UNIVERSIDADE FEDERAL DE SANTA MARIA
CENTRO DE CIÊNCIAS SOCIAIS E HUMANAS
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO
MESTRADO EM DIREITO

Andrey Oliveira Lamberty

AUTODETERMINAÇÃO INFORMATIVA NO ÂMBITO DA JUSTIÇA DO TRABALHO: a proteção jurídica de dados pessoais do trabalhador em perspectiva comparada entre Brasil e Argentina

Santa Maria, RS
2019

Andrey Oliveira Lamberty

AUTODETERMINAÇÃO INFORMATIVA NO ÂMBITO DA JUSTIÇA DO TRABALHO: a proteção jurídica de dados pessoais do trabalhador em perspectiva comparada entre Brasil e Argentina

Dissertação apresentada ao Curso de Mestrado do Programa de Pós-graduação em Direito, na Área de Concentração Direitos Emergentes na Sociedade Global, com ênfase na Linha de Pesquisa Direitos na Sociedade em Rede, da Universidade Federal de Santa Maria (UFSM), como requisito parcial para obtenção do grau de **Mestre em Direito.**

Orientadora: Profª. Drª. Rosane Leal da Silva

Santa Maria, RS, Brasil
2019

Lamberty, Andrey Oliveira
AUTODETERMINAÇÃO INFORMATIVA NO ÂMBITO DA JUSTIÇA DO TRABALHO: a proteção jurídica de dados pessoais do trabalhador em perspectiva comparada entre Brasil e Argentina / Andrey Oliveira Lamberty.- 2019.
208 p.; 30 cm

Orientadora: Rosane Leal da Silva
Dissertação (mestrado) - Universidade Federal de Santa Maria, Centro de Ciências Sociais e Humanas, Programa de Pós-Graduação em Direito, RS, 2019

1. Autodeterminação informativa 2. Privacidade 3. Processo do trabalho 4. Proteção de dados pessoais 5. Sociedade em rede I. Silva, Rosane Leal da II. Título.

Sistema de geração automática de ficha catalográfica da UFSM. Dados fornecidos pelo autor(a). Sob supervisão da Direção da Divisão de Processos Técnicos da Biblioteca Central. Bibliotecária responsável Paula Schoenfeldt Patta CRB 10/1728.

Andrey Oliveira Lamberty

AUTODETERMINAÇÃO INFORMATIVA NO ÂMBITO DA JUSTIÇA DO TRABALHO: a proteção jurídica de dados pessoais do trabalhador em perspectiva comparada entre Brasil e Argentina

Dissertação apresentada ao Curso de Mestrado do Programa de Pós-graduação em Direito, na Área de Concentração Direitos Emergentes na Sociedade Global, com ênfase na Linha de Pesquisa Direitos na Sociedade em Rede, da Universidade Federal de Santa Maria (UFSM), como requisito parcial para obtenção do grau de **Mestre em Direito.**

Aprovado em 17 de dezembro de 2019:

Rosane Leal da Silva, Drª. (UFSM)
(Presidente/Orientadora)

Valéria Ribas do Nascimento, Drª. (UFSM)

Denise Fincato, Drª. (PUC/RS)

Santa Maria, RS
2019

Ao meu filho Arthur, à minha esposa Patricia e aos meus pais,
Maria de Lourdes e Salvador, meu eterno amor e gratidão!

AGRADECIMENTOS

Na vida, toda caminhada é repleta de pessoas que nos dão apoio e sustentação para seguir em frente. Terminada uma etapa desta jornada acadêmica, é importante expressar a gratidão a todos aqueles que, de uma forma ou de outra, me ajudaram nesta construção:

Ao meu filho amado Arthur, meu melhor amigo, a razão de todo o meu esforço, por me ensinar o verdadeiro sentido da vida.

À minha esposa Patricia, meu grande amor, companheira de todas as horas, por toda a dedicação, o carinho e o incentivo.

Aos meus pais, Maria de Lourdes e Salvador, meus alicerces, pelo apoio e o amor incondicional, pelo exemplo de caráter e pelas lições de vida.

À minha irmã Clarissa, minha segunda mãe, por estar sempre ao meu lado, mesmo distante.

À minha orientadora, profª. Rosane Leal da Silva, exemplo de profissionalismo e comprometimento, pela dedicação incansável, pela amizade e o apoio que sempre me ofereceu, e por todos os ensinamentos. Mais do que orientar o desenvolvimento deste trabalho, foi uma verdadeira orientadora para a vida.

Ao prof. Marcelo Barroso Kümmel, meu mestre e amigo, a quem tenho enorme gratidão e admiração, por ter sido o incentivador e orientador dos primeiros passos. Este trabalho tem muito da sua participação.

A todos os docentes do Programa de Pós-Graduação em Direito (PPGD/UFSM), pelos valorosos ensinamentos, que contribuíram para o meu crescimento como ser humano e para a ampliação dos horizontes acadêmicos.

Aos colegas Andreia Momolli, Ariani Avozani Oliveira, Isadora Forgiarini Balem, Jaqueline Bertoldo, Jéssica Freitas de Oliveira, Julia de David Chelotti, Pablo dos Santos Ritzel e Vitalinio Lannes Guedes, pela amizade, o companheirismo e a parceria durante todo o período de mestrado.

A todos os colegas do Programa de Pós-Graduação em Direito (PPGD/ UFSM), pela maravilhosa oportunidade de convivência, debates e trocas de experiências durante os últimos dois anos.

À Universidade Federal de Santa Maria (UFSM), pelo acolhimento e pela excelência no ensino público e gratuito.

À Universidade Franciscana (UFN), pela formação das bases teóricas e humanas que me deram sustentação para o desenvolvimento deste trabalho.

Às professoras Valéria Ribas do Nascimento e Denise Fincato, pela gentileza de terem aceitado o meu convite para compor as bancas de qualificação e de defesa, pelo olhar atento e pelas contribuições enriquecedoras ao meu trabalho.

Enfim, a todos aqueles que me acompanharam de alguma forma durante essa trajetória, minha mais sincera gratidão!

INTERTEXTO

Primeiro levaram os negros
Mas não me importei com isso
Eu não era negro

Em seguida levaram alguns operários
Mas não me importei com isso
Eu também não era operário

Depois prenderam os miseráveis
Mas não me importei com isso
Porque eu não sou miserável

Depois agarraram uns desempregados
Mas como tenho meu emprego
Também não me importei

Agora estão me levando
Mas já é tarde.
Como eu não me importei com ninguém
Ninguém se importa comigo.

(Bertolt Brecht)

RESUMO

AUTODETERMINAÇÃO INFORMATIVA NO ÂMBITO DA JUSTIÇA DO TRABALHO: a proteção jurídica de dados pessoais do trabalhador em perspectiva comparada entre Brasil e Argentina

AUTOR: Andrey Oliveira Lamberty
ORIENTADORA: Rosane Leal da Silva

A evolução tecnológica e o crescente uso das tecnologias da informação e da comunicação (TIC) trouxeram inegáveis avanços aos processos democráticos de uma sociedade em rede, frutos do estreitamento da relação entre Poder Público e cidadãos, a ampliação da eficiência administrativa, e a criação de canais de comunicação que possibilitam uma maior abertura e transparência governamental. Juntamente com estes benefícios, novas ameaças acabam sendo descortinadas, principalmente pela linha tênue que passa a separar o público e o privado em um mundo que rompe com os clássicos conceitos de privacidade, acrescentando uma vigilância implacável ao cotidiano dos cidadãos, já que todos tornam-se vigias e vigiados. Esse contexto impõe um olhar atento à problemática do trabalhador que ajuíza reclamação trabalhista para a tutela de seus direitos não satisfeitos e que, nesta situação, encontra-se em estado de acentuada vulnerabilidade tanto frente a outros particulares quanto em face do Poder Público, justamente pela divulgação de seus dados pessoais por meio dos portais institucionais da justiça laboral. As novas demandas passam a exigir um efetivo exercício do direito à autodeterminação informativa por parte do trabalhador, especialmente no campo do Processo do Trabalho, já que o reclamante não possui, de fato, controle sobre a destinação oferecida às informações que fornece ao Poder Judiciário. Se este é um problema que perturba o trabalhador brasileiro, já que a Justiça do Trabalho é justamente o ente responsável pela salvaguarda de seus direitos e ao mesmo tempo o agente que potencializa o risco da discriminação, também o é em diversos países latino-americanos. Por isso, diante da constatação de que a Argentina foi o primeiro país do Mercado Comum do Sul (MERCOSUL) a obter a certificação da União Europeia, que reconheceu a legislação daquele país com nível de proteção adequada e compatível à europeia e, considerando a recente edição, no Brasil, da Lei nº 13.709/2018, ainda em fase de *vacatio legis*, questiona-se: é possível afirmar, em perspectiva comparada, que a novel legislação brasileira confere nível de proteção compatível com o seu vizinho mercosulino, revelando-se adequada e suficiente para garantir a proteção do empregado em face da coleta e tratamento de dados realizadas em razão do ajuizamento da reclamatória trabalhista? O estudo vale-se do método de abordagem hipotético-dedutivo e dos métodos de procedimento comparativo e monográfico com o objetivo de analisar os sistemas jurídicos de proteção de dados pessoais na Argentina e no Brasil a fim de verificar se os dois países da América Latina garantem efetiva proteção ao trabalhador, tendo em vista a sua vulnerabilidade diante da coleta, manipulação e distribuição de dados pessoais no âmbito judicial, com o uso das Tecnologias da Informação e da Comunicação. Para tanto, utiliza-se das técnicas de pesquisa da análise documental, pesquisa bibliográfica e observação sistemática, direta e não-participante de *sites* e portais institucionais do Poder Judiciário trabalhista dos dois países vizinhos. Partindo das hipóteses inicialmente formuladas, os resultados conduziram a duas respostas adequadas à solução do problema, de forma complementar: 1) a nova lei de proteção de dados pessoais brasileira apresenta nível compatível com a legislação argentina, mas nenhuma delas mostra-se suficiente para garantir a proteção dos dados pessoais do trabalhador no âmbito da Justiça do Trabalho; e 2) independentemente do nível apresentado pela lei de proteção de dados de cada país, não é possível afirmar, de maneira direta, que a existência de uma lei específica condiciona as práticas protetivas de dados pessoais do trabalhador pelo Poder Judiciário trabalhista na divulgação das informações processuais.

Palavras-chave: Autodeterminação informativa. Privacidade. Processo do trabalho. Proteção de dados pessoais. Sociedade em rede.

ABSTRACT

INFORMATIONAL SELF-DETERMINATION IN THE SCOPE OF JUSTICE OF LABOR: the legal protection of worker's personal data in comparative perspective between Brazil and Argentina

AUTHOR: Andrey Oliveira Lamberty
ADVISOR: Rosane Leal da Silva

The technological developments and the increasing use of information and communication technologies (ICT) have undeniable advances in the democratic processes of a network society, as a result of the closer relationship between the Government and citizens, the expansion of administrative efficiency, and the creation of communication channels that enable greater government openness and transparency. Along with these benefits, new threats come to light, especially along the thin line that separates the public and the private in a world that breaks with the classic concepts of privacy, adding ruthless vigilance to the daily lives of citizens, as all become be watched and watched. This context imposes a close look at the problem of the worker who claims a labor claim for the protection of his unfulfilled rights and that, in this situation, is in a state of marked vulnerability both vis-à-vis other individuals and the Government, precisely because of disclosure of your personal data through the institutional portals of labor justice. The new demands now require an effective exercise of the right to informational self-determination by the worker, especially in the field of the Labor Process, since the claimant does not, in fact, have control over the destination of the information provided to the Judiciary. If this is a problem that disturbs the Brazilian worker, since the Labor Court is precisely the entity responsible for safeguarding their rights and at the same time the agent that increases the risk of discrimination, it is also in several Latin American countries. Therefore, given the fact that Argentina was the first country in the Southern Common Market (MERCOSUR) to obtain European Union certification, it recognized the legislation of that country with an adequate level of protection compatible with that of Europe and, considering the recent The publication, in Brazil, of Law Nº. 13.709 / 2018, still in the phase of vacatio legis, asks: is it possible to state, in comparative perspective, that the new Brazilian legislation confers a level of protection compatible with its neighbor mercosulino, revealing itself? adequate and sufficient to ensure the protection of the employee in the face of data collection and processing due to the filing of the labor claim? The study uses the hypothetical-deductive approach method and the comparative and monographic procedure methods in order to analyze the legal systems of personal data protection in Argentina and Brazil in order to verify if the two Latin American countries guarantee effective protection for workers, given their vulnerability to the collection, manipulation and distribution of personal data in the judicial sphere, through the use of Information and Communication Technologies. To this end, it uses the research techniques of document analysis, bibliographic research and systematic, direct and non-participant observation of websites and institutional portals of the Labor Judiciary of the two neighboring countries. Based on the hypotheses initially formulated, the results led to two appropriate responses to the solution of the problem, in a complementary way: 1) the new Brazilian personal data protection law has a level compatible with Argentine legislation, but none of them is sufficient to guarantee the protection of workers' personal data within the scope of Labor Justice; and 2) regardless of the level presented by the data protection law of each country, it is not possible to state directly that the existence of a specific law conditions the protective practices of personal data of the worker by the Labor Judiciary in the disclosure of procedural information.

Keywords: Informative self-determination. Privacy. Work process. Protection of personal data. Network society.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE GRÁFICOS

LISTA DE ABREVIATURAS E SIGLAS

ANPD – Autoridade Nacional de Proteção de Dados

CAGED – Cadastro Geral de Empregados e Desempregados

CLT – Consolidação das Leis do Trabalho

CNJ – Conselho Nacional de Justiça

CNT – Cámara Nacional de Apelaciones del Trabajo

CSJ – Corte Suprema de Justicia de la Nación argentina

CSJT – Conselho Superior da Justiça do Trabalho

CTPS – Carteira de Trabalho e Previdência Social

DPO – *Data Protection Officer*

EPD – Encarregado de Proteção de Dados

LAI – Lei de Acesso à Informação

LGPD – Lei Geral de Proteção de Dados brasileira (Lei 13.709/2018)

LPD – Ley de Proteccion de los Datos Personales argentina (Ley 25.326/2000)

MCI – Marco Civil da Internet

NIT - Número de Identificação do Trabalhador

NUDI – Núcleo de Direito Informacional

OCDE - Organização para a Cooperação e Desenvolvimento Econômico

OIT – Organização Internacional do Trabalho

ONU – Organização das Nações Unidas

PASEP - Programa de Formação do Patrimônio do Servidor Público

PIS – Programa de Integração Social

PJe – Processo Judicial eletrônico

PJN – Poder Judicial de la Nación argentina

RAIS – Relação Anual de Informações Sociais

RGPD – Regulamento Geral de Proteção de Dados da União Europeia

STF – Supremo Tribunal Federal

TIC – Tecnologias da Informação e da Comunicação

TRT – Tribunal Regional do Trabalho

TST – Tribunal Superior do Trabalho

UFSM – Universidade Federal de Santa Maria - RS

SUMÁRIO

INTRODUÇÃO

O crescente uso das Tecnologias da Informação e da Comunicação (TIC) impacta de forma significativa a sociedade contemporânea, uma sociedade em rede constituída de múltiplos nós interconectados, cujos fluxos multidirecionais de informações propagam-se simultaneamente, atingindo uma escala global. A *Internet* reduz distâncias, cria conexões, amplia possibilidades de comunicação e de conhecimento, mas também revela/descortina uma série de novos problemas, que podem afetar diretamente os direitos fundamentais dos seus usuários.

A origem dos direitos fundamentais, hoje previstos em posição de destaque no texto Constitucional, relaciona-se diretamente ao desenvolvimento do Estado, adotando um caráter protecionista frente às possíveis violações que dele decorrem. Atualmente entende-se que os efeitos da proteção dos direitos fundamentais vinculam diretamente os particulares, sendo a seara laboral um fértil terreno para a ocorrência de inúmeras violações a direitos que mereçam essa tutela. Com grande incidência, verifica-se uma série de interferências nos direitos fundamentais à intimidade e à vida privada do trabalhador, e o advento das novas tecnologias passou a ser um facilitador dessas agressões.

A sociedade em rede permite a implementação de novas estratégias de vigilância institucional antes inimagináveis, espalhadas de forma "líquida" e invisível, inclusive com a colaboração voluntária dos indivíduos para o fornecimento das informações de cunho pessoal. As TIC tornaram-se importantes ferramentas de manipulação, armazenamento e distribuição de dados pessoais, sendo que o problema enfrentado pelo obreiro é ainda mais perceptível, na medida em que seus dados são colocados à disposição do empregador, revestido de um poder diretivo cuja limitação não possui uma demarcação bem definida pelo ordenamento jurídico brasileiro. Tal fato se acentua ainda mais quando o trabalhador demanda a proteção de seus direitos ao Poder Judiciário, pois o exercício desse direito pode se converter em novas fontes de violação, a depender de como os dados processuais são divulgados por mecanismos de buscas e pelos próprios portais institucionais.

As informações publicizadas pelo Poder Judiciário trabalhista, por meio de ferramentas de consultas processuais e jurisprudenciais, com frequência abrangem dados pessoais (sensíveis ou não) que não estão abarcados pelo interesse público, deixando expostos os diversos sujeitos que integram a relação processual, sejam eles partes no processo ou terceiros, tais como as testemunhas ou pessoas relacionadas diretamente à demanda. A facilidade de acesso a essas informações pelos atores da sociedade em rede impõe que se atente para a proteção de dados

pessoais, especialmente do trabalhador que ajuíza ação para a tutela de seus direitos não satisfeitos e que, nesta situação, encontra-se em estado de acentuada fragilidade tanto frente a outros particulares quanto em face do Poder Público. Nesse contexto, há a necessidade de identificar as vulnerabilidades do trabalhador diante dos mecanismos que possibilitam o acesso e a transmissão de seus dados pessoais por entidades públicas e privadas, realizando um estudo comparado entre o tratamento jurídico conferido pela Argentina e pelo Brasil ao tema, a fim de verificar em que medida é efetiva a proteção do obreiro nesses países.

A escolha pela Argentina foi motivada por este ter sido, dentre os países integrantes do Mercosul à época da fundação do bloco[1], o primeiro a contar com uma lei protetiva de dados pessoais, somando-se ao fato de que o país obteve o reconhecimento da União Europeia quanto à adequação do nível de proteção de dados pessoais, nos termos da Diretiva 95/46/CE, do Parlamento Europeu e do Conselho, bem como pelo protagonismo que uma organização não governamental argentina (o *Instituto de Investigación para la Justicia Argentina*) teve na reunião que resultou na Carta de Heredia, o mais importante documento sobre a difusão de informação judicial na *Internet*.

Diante disso e considerando a recente edição, no Brasil, da Lei nº 13.709/2018, ainda em fase de *vacatio legis*, questiona-se: é possível afirmar, em perspectiva comparada, que a novel legislação brasileira confere nível de proteção compatível com o seu vizinho mercosulino, revelando-se adequada e suficiente para garantir a proteção do trabalhador em face da coleta e tratamento de dados realizadas em razão do ajuizamento da reclamatória trabalhista?

O estudo tem por escopo principal analisar os sistemas jurídicos de proteção de dados pessoais na Argentina e no Brasil a fim de verificar se os dois países da América Latina garantem efetiva proteção ao trabalhador, tendo em vista a sua vulnerabilidade diante da coleta, manipulação e distribuição de dados pessoais no âmbito judicial, com o uso das Tecnologias da Informação e da Comunicação. De maneira específica, busca-se identificar as vulnerabilidades do trabalhador diante do tratamento de dados pessoais no processo trabalhista, além de estudar a evolução do direito à proteção de dados pessoais e examinar o regramento existente na União Europeia, cotejando-o com os modelos existentes nos dois países latino-americanos.

Além disso, também são objetivos parciais do trabalho analisar e comparar o tratamento jurídico realizado na Argentina e no Brasil no que se refere à proteção de dados pessoais, com vistas a verificar qual sistema jurídico garante a maior proteção ao trabalhador, especialmente aquele que ajuizou reclamação trabalhista anteriormente e que se encontra em posição de

[1] Argentina, Brasil, Paraguai e Uruguai assinaram, em 26 de março de 1991, o Tratado de Assunção, dando origem ao Mercado Comum do Sul (Mercosul).

vulnerabilidade pela possibilidade de uso discriminatório de seus dados. Por fim, busca-se propor sugestões de medidas que podem ser adotadas pelo Poder Judiciário brasileiro para a tutela dos dados pessoais dos trabalhadores que ajuízam reclamatórias trabalhistas.

O marco teórico adotado conjuga autores que discutem os impactos das tecnologias da informação e da comunicação (TIC) na sociedade, tais como Manuel Castells, no que se refere à definição e ao estabelecimento das bases estruturais da sociedade em rede e às transformações do trabalho e do mercado de trabalho frente ao surgimento do paradigma informacional, Danilo Doneda, quanto ao estudo da privacidade e proteção de dados pessoais e Alice Monteiro de Barros, autora que trabalha com maior especificidade o tema da proteção de dados pessoais no âmbito das relações trabalhistas.

O aporte metodológico é composto pelo método de abordagem hipotético-dedutivo[2], estabelecendo-se premissas iniciais amplas e gerais, através da identificação e análise das vulnerabilidades do empregado diante da coleta, manipulação e distribuição de seus dados pessoais no âmbito da Justiça do Trabalho, bem como pelo estudo vinculação do Poder Público e dos particulares ao direito fundamental à privacidade e o reconhecimento da colisão de direitos na seara trabalhista, até que seja realizado o exame específico dos sistemas jurídicos de proteção de dados pessoais da Argentina e do Brasil, objetos do estudo proposto.

Para tanto, a pesquisa admite quatro hipóteses como possíveis soluções ao problema investigado: a) a nova lei de proteção de dados brasileira apresenta nível compatível com a legislação argentina, e ambas são suficientes para garantir a proteção dos dados pessoais do trabalhador que integram as reclamações trabalhistas; b) a nova lei de proteção de dados brasileira apresenta nível compatível com a legislação argentina, mas nenhuma delas mostra-se suficiente para garantir a proteção dos dados pessoais do trabalhador no âmbito da Justiça do Trabalho; c) a nova lei de proteção de dados brasileira revela nível protetivo inferior ao da legislação argentina, e por conta disso, não garante a proteção dos dados pessoais do trabalhador no âmbito da Justiça do Trabalho; e d) independentemente do nível apresentado pela lei de proteção de dados de cada país, não é possível afirmar, de maneira direta, que a existência de uma lei específica condiciona as práticas protetivas de dados pessoais do trabalhador pelo Poder Judiciário trabalhista na divulgação das informações processuais.

Quanto ao método de procedimento, é utilizado o comparativo, visando-se realizar um estudo comparado entre os sistemas jurídicos de proteção de dados pessoais do trabalhador

[2] Pelo método hipotético-dedutivo, "[...] partir-se-ia de conjecturas (hipóteses) formuladas na condição de respostas provisórias aos problemas apresentados, submetendo-as a um rigoroso processo de verificação (falseamento), de modo a aceitá-las ou refutá-las" (FINCATO; GILLET, 2018, p. 44).

instaurados na Argentina e Brasil, delimitando o campo de análise ao âmbito processual. O norte de condução do estudo comparado entre os sistemas jurídicos dos países em cotejo será fornecido pelas obras de René David e Marc Ancel, consagrados comparativistas que guiaram os parâmetros da metodologia empregada.

Aliado ao método comparativo, é utilizado o método monográfico, tendo em vista o estudo aprofundado acerca da proteção de dados pessoais do trabalhador na sociedade em rede, especialmente no que se refere aos dados pessoais que são discutidos e reportados nas decisões judiciais publicadas nos portais oficiais do Poder Judiciário e que dali migram para *sites* mantidos por empresas privadas.

As técnicas de pesquisa empregadas como ferramentas ao estudo do tema são a análise documental, pesquisa bibliográfica e a observação sistemática, direta e não-participante de *sites* e portais institucionais, o que é feito através da elaboração de fichamentos, resumos, tabelas e gráficos. Tais técnicas são aliadas tendo em vista que o desenvolvimento do trabalho demanda o exame de leis, decretos, súmulas, resoluções, *websites* e portais de *internet* da Argentina e do Brasil, bem como convenções e diretivas internacionais relacionadas à proteção de dados pessoais, juntamente com o estudo da doutrina pertinente ao tema.

Em consonância com a metodologia escolhida, o estudo foi estruturado em três capítulos, cada qual com subdivisões. No primeiro capítulo, procura-se identificar as vulnerabilidades do trabalhador diante do tratamento de dados pessoais no processo laboral, o que demanda uma abordagem inicial acerca da vigilância eletrônica em seus aspectos gerais, a partir das teorias que observavam o controle e a disciplina na sociedade industrial, evoluindo para as modernas doutrinas que se valem da utilização das tecnologias informacionais como instrumento de vigilância massiva em escala global.

Em um segundo momento, ainda no capítulo inicial, o foco da pesquisa volta-se ao uso que o Poder Público faz das tecnologias informacionais para a divulgação de informações processuais, o que conduz ao tratamento indevido de dados pessoais que são fornecidos em virtude do ajuizamento de reclamações trabalhistas. Diante de um possível conflito desvelado nesse contexto, que envolve o dever de transparência da Administração Pública, o direito à informação do empregador e o direito à privacidade do trabalhador, torna-se necessário estabelecer uma fronteira entre a informação pública e privada, o que é aprofundado neste ponto.

No segundo capítulo, emerge a abordagem jurídica do problema, iniciando-se por um estudo acerca da vinculação do Estado e dos particulares ao direito fundamental à privacidade, o que progride para um estudo deste direito em seus diversos aspectos e desdobramentos. O

tema demanda um necessário passeio histórico sobre as diferentes concepções de privacidade que acompanharam a evolução da sociedade, chegando-se à autodeterminação informativa enquanto direito ao controle das informações pessoais do indivíduo, ou direito à proteção de seus dados pessoais. Com isso, a sequência do capítulo ocupa-se em observar o modelo europeu de proteção de dados pessoais, padrão que vem influenciando a edição de diversas leis de proteção de dados pessoais na América Latina. O exame desse sistema, estruturado através de diretivas e regulamentos, permite que sejam estabelecidos os pilares que dão sustentação ao estudo dos modelos argentino e brasileiro, na sequência da dissertação.

O capítulo final adentra no estudo comparado dos sistemas jurídicos de proteção de dados pessoais do trabalhador dos dois países mercosulinos, partindo de parâmetros metodológicos delineados por consagrados autores comparativistas, e do estabelecimento de critérios prévios de análise a serem aplicados no exame legislativo e na observações dos portais institucionais do Poder Judiciário trabalhista de cada nação. A abordagem tem início pela análise do modelo da Argentina, o que demanda uma apresentação geral acerca da legislação pertinente ao tema, seguindo-se de um aprofundado exame da lei de proteção de dados pessoais do país, tudo à luz da doutrina pátria. Na sequência, a observação volta-se ao *site* do Poder Judicial de la Nación, visando alcançar as respostas com relação à efetividade de tas garantias legais no âmbito do processo laboral, preocupação que é o cerne da pesquisa.

O mesmo tratamento é oferecido ao Brasil, na sequência do capítulo. Após um necessário estudo das ferramentas de proteção de dados pessoais atualmente vigentes no ordenamento jurídico brasileiro e de um exame da sua nova lei de proteção de dados pessoais (o que envolve os caminhos percorridos até a edição da legislação), procura-se verificar qual é o atual panorama dos portais da Justiça do Trabalho no que se refere à divulgação de dados pessoais, escolhendo-se, para tal, o Tribunal Superior do Trabalho como modelo geral. O produto da observação e o cotejo com os demais resultados obtidos permite que se possa propor sugestões de medidas viáveis ao Brasil para uma maior proteção dos dados pessoais dos trabalhadores no processo do trabalho.

Diante disso, é importante ressaltar que se reconhece a vulnerabilidade de diversos outros sujeitos do processo do trabalho em face do tratamento de dados pessoais pela Justiça do Trabalho, dentre eles as testemunhas e terceiros diretamente relacionados às demandas. Entretanto, a presente pesquisa foca seu campo de observação aos problemas enfrentados pelo trabalhador, que sofre uma espécie de efeito colateral ao livre exercício do direito de ação. Percebe-se que o trabalhador possui a peculiaridade de enfrentar um dilema entre a busca da

reparação pelo dano sofrido no contrato de trabalho e a possibilidade de violações pelo próprio Poder Judiciário a que recorre, e essa particularidade justifica a escolha feita.

Dessa forma, ainda que este estudo eventualmente aborde outros atores de forma incipiente, um eventual aprofundamento abrangendo o tratamento de dados pessoais dos demais sujeitos vulneráveis do processo do trabalho, e até mesmo os dados do empregador (que também tem a sua vulnerabilidade, em alguma medida), serão contemplados em futuras pesquisas sobre o tema, até mesmo em sede de doutorado.

A pesquisa visa enfrentar os impactos advindos do crescente uso das tecnologias da informação e da comunicação nas relações trabalhistas, afetando não apenas os direitos de personalidade, mas também repercutindo nos direitos sociais do obreiro, que está inserido nesta sociedade de fluxos informacionais. Além disso, repensa o papel do Poder Público na divulgação de informações processuais, estabelecendo um limite para o exercício de seu dever de transparência. Com isso, o tema insere-se no âmbito das pesquisas feitas pelo Núcleo de Direito Informacional da UFSM (NUDI), mostrando-se em perfeita sintonia com a linha de pesquisa “Direitos na Sociedade em Rede” do Programa de Pós-Graduação em Direito da Universidade Federal de Santa Maria, na medida em que conduz a um olhar frente aos novos problemas que se desvelam na sociedade em rede, e propondo soluções para a plena tutela dos direitos do trabalhador.

1 QUANDO O ACESSO À JUSTIÇA SE CONSTITUI EM UM RISCO AO JURISDICIONADO: vulnerabilidades do trabalhador diante do tratamento de dados pessoais no processo do trabalho

As mudanças representadas pela progressiva inserção das Tecnologias da Informação e da Comunicação (TIC) no cotidiano das pessoas vão muito além do encurtamento das distâncias e das facilidades de comunicação. Vive-se, atualmente, em uma sociedade cujas interações sociais ocorrem, em grande parte, no *ciberespaço*[3], através de um intenso fluxo de informações entre os diferentes atores no ambiente virtual. Esses fluxos informacionais são correntes de informação processados por conjuntos de nós interconectados, formando estruturas comunicativas (CASTELLS, 2015, p. 66).

Na sociedade em rede, definida por Manuel Castells (2015, p. 70) como "uma sociedade cuja estrutura social é construída em torno de redes ativadas por tecnologias de comunicação e de informação processadas digitalmente e baseadas na microeletrônica", o espaço de fluxos permite a dissolução do tempo sequencial, redefinindo as noções de tempo e espaço através da simultaneidade de eventos. Há, portanto, o rompimento da lógica tradicional tempo/espaço (CASTELLS, 2015, p. 81), através da conversão do tempo local e cronológico a um tempo mundial e universal (VIRILIO, 1995, p. 95).

Através dos fluxos informacionais, o controle da comunicação, e por consequência, a informação, passam a ter enorme valor, não somente econômico, mas como fonte de poder. Não é à toa que Castells (2015, p. 99) define o poder na sociedade em rede como sendo o poder da comunicação. Nas palavras do autor (2015, p. 29), as relações de poder "[...] são amplamente construídas na mentalidade das pessoas através de processos de comunicação".

O poder, anteriormente vinculado ao uso da força, passa agora a ser definido pela capacidade de utilização das informações para a manipulação e o controle das atividades dos cidadãos, o que se torna possível pela transformação de informações dispersas em informações de massa e organizadas (SÁNCHEZ BRAVO, 2010, p. 17). O processamento automatizado de informações converte-se, portanto, em fonte de poder à disposição daqueles que detém o poderio tecnológico.

---

[3] Pierre Lévy (1999, p. 92) conceitua o ciberespaço como "[...] o espaço de comunicação aberto pela interconexão mundial dos computadores e das memórias dos computadores", definição que "inclui o conjunto dos sistemas de comunicação eletrônicos [...], na medida em que transmitem informações provenientes de fontes digitais ou destinadas à digitalização".

A informação digitalizada é capaz de ser processada em grande quantidade, de forma automática, precisa e extremamente veloz (LÉVY, 1999, p. 52), o que possibilita que esses fluxos informacionais se propaguem intensamente, carregando uma enorme quantidade de conhecimento. À medida em que o *ciberespaço* permite o livre acesso às informações, bem como a liberdade de expressão e comunicação incomparável com outros períodos históricos, também intensifica a interdependência e a interligação entre seus atores (LÉVY, 2002, p. 29-30), favorecendo a eliminação das tradicionais fronteiras nacionais.

A transposição dos espaços físicos e das barreiras nacionais, próprias do fenômeno da globalização e da expansão das TIC, proporciona o surgimento de novos centros de poder não estatais. O poder passa a migrar em direção aos atores públicos, vinculados às grandes potências mundiais, e aos atores privados, papel exercido pelas empresas transnacionais que possuem o monopólio das tecnologias da informação (MENEZES NETO; MORAIS; BEZERRA, 2017, p.196). Esses atores passam a exercer uma vigilância suavizada sob a ótica do consumo e legitimada pela ideia de "mal necessário" diante da ameaça do terrorismo. Nesse sentido, Marcelo Cardoso Pereira (2005, p. 167) lembra que os países que mantêm sistemas eletrônicos de vigilância, quando admitem que o fazem, costumam justificá-los em virtude do combate ao terrorismo, especialmente após os atentados de 11 de setembro de 2001, nos Estados Unidos da América.

A vigilância e a disciplina, que remetem aos primórdios da sociedade industrial, através do controle sobre os próprios corpos dos indivíduos, são reinventadas na contemporaneidade, ganhando novos contornos com a utilização das modernas tecnologias informacionais. Práticas de monitoramento foram incorporadas ao dia a dia dos indivíduos, que assimilaram o fornecimento de informações pessoais sem o conhecimento dos riscos a que podem ser submetidos. Cita-se os exemplos dos *Smartphones* conectados à *Internet* que são carregados junto ao corpo, sendo capazes de indicar a localização onde quer que se vá, dos *scanners* corpóreos em aeroportos, das câmeras de vigilância, dos *check-ins* para acesso de redes *wi-fi*, dos cadastros e das senhas fornecidas em compras *on-line* e dos *cookies*, pequenos arquivos de dados que são enviados por *sites* e ficam armazenados no computador do usuário, permitindo o acesso à informações sobre os hábitos de navegação da pessoa.

Uma das principais funções do *ciberespaço* é a transferência de dados ou *upload*, que ocorre mediante a cópia de um pacote de informações de uma memória digital para outra (LÉVY, 1999, p. 94). Em um mundo marcado pela informação incessante e pelo consumo, dados pessoais são coletados a todo instante, abastecendo bancos de dados que armazenam as mais diversas informações pessoais de indivíduos conectados ao redor do mundo. Todas essas

informações que navegam no *ciberespaço*, sejam dados pessoais ou metadados[4], constituem-se em insumo nas mãos desses atores sociais, convertendo-se em instrumento de controle e manipulação.

O *ciberespaço* amplifica o potencial danoso da informação que circula na rede, especialmente quando essa informação relaciona-se à vida privada dos indivíduos, uma vez que permite a sua rápida difusão pelos milhões de computadores interconectados, atingindo uma enorme capacidade de projeção (FARINHO, 2006, p. 70). Esse grau de risco é potencializado pelo cruzamento dos bancos de dados, resultando em informação diversa dos dados inicialmente coletados, cuja utilização pelo poder público pode se dar com o intuito restritivo à liberdade do cidadão, ou por entidades privadas, para fins discriminatórios (GONÇALVES, 2003, p. 82). Mas não apenas o governo e as grandes empresas privadas, a sociedade em rede possibilita que qualquer pessoa com acesso à *Internet* receba e divulgue informações, coletando, armazenando e transferindo dados pessoais.

Todas essas mudanças repercutem no mundo do trabalho, já que a utilização de um arsenal de ferramentas disponibilizadas pelas tecnologias inseridas nos sistemas produtivos converte a empresa em um banco de dados pessoais do obreiro, muitas vezes por imposição legal e outras vezes pela ânsia do empregador em salvaguardar a sua propriedade. A vigilância eletrônica nas relações laborais é exercida por meio de dispositivos cada vez mais discretos e sofisticados, que operam silenciosamente, coletando dados pessoais do empregado e controlando todos os seus movimentos dentro e fora do sistema de produção.

O desenvolvimento tecnológico permite que o poder fiscalizatório do empregador, antes restrito ao ambiente laboral, ultrapasse a esfera empresarial e atinja o trabalhador nos seus momentos de lazer. A coleta de dados pessoais do trabalhador por outros particulares, portanto, torna-se uma ameaça aos direitos de personalidade do obreiro, especialmente os direitos à privacidade e à igualdade, tendo em vista que a utilização de seus dados pessoais para fins desvirtuados dos objetivos da coleta original pode conduzir a um tratamento discriminatório durante a contratualidade ou antes mesmo de sua formação.

Quando este empregado busca o Poder Judiciário visando a tutela de direitos não satisfeitos durante o contrato de trabalho, ou a reparação por eventual dano sofrido, depara-se com nova situação de risco: a coleta e a divulgação de dados pessoais no âmbito judicial para

[4] Metadados são informações sobre a própria informação (dado sobre dado), que não dizem respeito ao seu conteúdo e que, desvinculadas do contexto, podem parecer inofensivas, mas ao serem catalogadas, reordenadas e analisadas levam à identificação do indivíduo, de suas preferências e hábitos, colocando em risco os seus direitos à privacidade, à liberdade e à igualdade. (NETO; MORAIS; BEZERRA, 2017, p.191-3).

fins para os quais não houve consentimento, alheios à prestação jurisdicional. Neste caso, o Poder Público atua como colaborador e propulsor das violações sofridas pelo obreiro, na medida em que permite a transmissão de dados pessoais sem a devida autorização, possibilitando a terceiros que obtenham acesso a informações indesejadas pelo trabalhador.

Todas essas ferramentas facilitam as práticas de vigilância implementadas pelos atores públicos e privados de uma sociedade em rede, trazendo diversas ameaças ao trabalhador, que se mostra em situação de extrema vulnerabilidade diante do processamento indevido de dados pessoais que integram os processos judiciais. Faz-se necessário, com isso, um estudo dos principais modelos teóricos sobre a vigilância, desde aqueles autores tradicionais que debruçaram seus estudos sobre este tema antes do advento das TIC até as teorias que trabalham sob o viés da vigilância eletrônica massiva em escala global, a *surveillance,* identificando os seus impactos no mundo do trabalho.

1.1 A SOFISTICAÇÃO DA VIGILÂNCIA NA SOCIEDADE EM REDE: novas tensões ao mundo do trabalho

A ascensão burguesa, na virada do Século XVIII, e com ela o intenso processo de industrialização e o crescimento das cidades e do proletariado urbano, trouxeram consigo a necessidade de controle e disciplina sobre a massa populacional, que representava a força de trabalho necessária ao desenvolvimento capitalista. Ainda que a vigilância seja uma prática que remete ao surgimento da própria civilização ocidental, passa a adquirir maior força na modernidade em virtude da necessidade de organização própria do modelo estatal moderno (MENEZES NETO; MORAIS; BEZERRA, 2017, p. 187).

Nesse contexto, a disciplina passa a ser exercida através do controle sobre o próprio corpo do indivíduo, tornando-o submisso, obediente e dócil. Os “corpos dóceis”, na teoria de Michel Foucault (1998a, p. 118-9), são corpos que podem ser utilizados, transformados e aperfeiçoados, mostrando-se fortes em termos econômicos de utilidade (aptidão), mas fracos em termos políticos de obediência (dominação acentuada). Os processos disciplinares encontram-se em funcionamento nas diversas instituições que acompanham o indivíduo desde o seu nascimento, seja nas escolas, hospitais, quartéis e fábricas, moldando o corpo necessário ao funcionamento da sociedade industrial.

No âmbito das oficinas e fábricas, os processos disciplinares visam à fabricação do operário obediente através da submissão dos corpos por meio das práticas de controle. Foucault (1998a, p. 147) entende que o aumento da complexidade do aparelho de produção torna as

tarefas de controle cada vez mais necessárias e de difícil execução, sendo que a vigilância torna-se uma parte do processo produtivo e uma engrenagem do poder disciplinar. O poder disciplinar é descrito pelo autor (1998b, p. XVII-XVIII) como um instrumento de poder, um sistema político de dominação, exercido através da distribuição e da organização dos indivíduos no espaço, do controle do tempo e da vigilância, que permite a tudo ver sem ser visto. Este poder permite que se extraia dos corpos tempo e trabalho, mais do que bens e riqueza (FOUCAULT, 1998b, p. 187).

O modelo do "panóptico" é o instrumento idealizado por Jeremy Bentham (2008, p. 20) para viabilizar essa vigilância hierárquica. Trata-se da construção de uma estrutura circular que permitiria ao observador, situado no centro e mantendo-se invisível aos prisioneiros por meio de uma cortina, ter o controle de todas as celas ao mesmo tempo. Esta construção arquitetônica, aplicável a presídios, hospícios, hospitais, escolas e indústrias, conforme Foucault (1998a, p. 166-7), induziria no detento "um estado consciente e permanente de visibilidade que assegura o funcionamento automático do poder", ainda que o próprio observador não estivesse em período integral na condição de vigilante. Com isso, o prisioneiro nunca sabe ao certo se está sendo observado, mas tem certeza que pode estar sendo vigiado a qualquer momento.

Na literatura, George Orwell previu um mundo de controle e vigilância mediada pela tecnologia, antes mesmo do advento das TIC. Publicado em 1949, o romance distópico "1984" (2009), o último escrito pelo autor, apresenta o personagem Winston Smith como refém de um Estado opressivo (Oceânia), vigiado por um Grande Irmão (*Big Brother*) onipresente, líder do "Partido" que controla a tudo e a todos. Dentro desse Estado, inexiste lei, e a única regra a ser seguida é a obediência irrestrita tanto em ações como em pensamento (ORWELL, 2009, p. 382).

A visionária obra apresenta uma metáfora ao controle governamental exercido nos dias atuais, mediado pelas tecnologias da informação, apresentando as "teletelas" como uma espécie de televisores (descrito como uma "placa de metal semelhante a um espelho fosco") que seriam capazes de receber e transmitir informações, capturando o som ambiente e monitorando os indivíduos de Oceânia, que vivem sob a ameaça de que "O GRANDE IRMÃO ESTÁ DE OLHO EM VOCÊ" (ORWELL, 2009, p. 12-3, grifo do autor). Tal como o modelo do panóptico, o *Big Brother* inibe o desejo de fuga no prisioneiro, tendo em vista que este poderia estar sendo vigiado a qualquer momento (MENEZES NETO; MORAIS; BEZERRA, 2017, p. 196).

A crise e o declínio das sociedades disciplinares e a sua substituição por "sociedades de controle" é defendida por Gilles Deleuze, em seu artigo intitulado "Post-scriptum sobre as

Sociedades de Controle", publicado no *L'Autre Journal* n. 1, em maio de 1990 (DELEUZE, 1992). Para Deleuze (1992, p. 223), diferentemente das sociedades antigas, que manejavam máquinas simples, e das sociedades disciplinares, que utilizavam máquinas energéticas, as sociedades de controle "operam por máquinas de uma terceira espécie, máquinas de informática e computadores, cujo perigo passivo é a interferência, e, o ativo, a pirataria e a introdução de vírus".

As sociedades de controle representam a substituição de uma sociedade baseada no confinamento por um novo regime de dominação próprio do sistema capitalista, com o *marketing* assumindo o papel de instrumento de controle social. A fábrica foi substituída pela empresa, uma empresa invisível composta apenas por gerentes, onde o salário fixo passa a ser trocado pelo sistema de prêmios e metas, que fazem com que o empregado seja o próprio fiscal de si mesmo. Com isso, o confinamento deu lugar ao endividamento como ferramenta de controle social (DELEUZE, 1992, p. 221-4).

Revisitando o modelo do panóptico, a partir do desenvolvimento dos meios de comunicação de massa, especialmente a televisão, Mathiesen (1997) desenvolve o conceito do sinóptico, em que muitos vigiam poucos. Este modelo, complementar ao panóptico como uma via de mão dupla, surge no contexto de uma sociedade espectadora, a partir da identificação de que os meios de comunicação tradicionais levam centenas de milhões de pessoa a ver e admirar algumas poucas celebridades (MATHIESEN, 1997).

Nos dias atuais, entretanto, o desenvolvimento da *Internet* e dos meios de autocomunicação de massa (CASTELLS, 2015) permitem a qualquer pessoa com acesso à rede a possibilidade de emitir e receber mensagens, bem como acessar informações de qualquer parte do mundo. A disseminação das redes sociais e necessidade de ver e ser visto por todos impõem a atualização dos antigos conceitos, motivo que leva Fernanda Bruno (2013) a propor o termo "palinóptico", que designa uma sociedade em que muitos vigiam muitos. Para Bruno (2013, p. 47):

> Nem panóptico nem sinóptico, mas um modelo reticular e distribuído onde muitos vigiam muitos ou onde muitos veem e são vistos de variadas formas. Algo como um palinóptico, para brincar com o radical grego palin, que designa processos de dupla via. Ver e ser visto ganham aqui sentidos atrelados à reputação, pertencimento, admiração, desejo, conferindo à visibilidade uma conotação prioritariamente positiva, desejável, que ressoa nos sentidos sociais que a vigilância assume hoje. Ser visto e ser vigiado, assim como ver e vigiar, são progressivamente incorporados no repertório perceptivo, afetivo, atencional, social, e associados a processos de prazer, diversão, sociabilidade.

Assim, com as diversas mudanças proporcionadas pelo uso massivo das Tecnologias da Informação e da Comunicação, inclusive com novas formas de controle social, os modelos teóricos tradicionais de vigilância apresentam-se inadequados ao contexto que se apresenta diante de novas características que são inerentes à sociedade contemporânea: a fluidez, a descentralização e a desterritorialização (MENEZES NETO; MORAIS; BEZERRA, 2017, p. 187). Por isso, Menezes Neto, Morais e Bezerra (2017, p. 187) defendem a superação da ideia de mera "vigilância" pelo emprego da expressão "*surveillance*", terminologia que contempla as tecnologias da informação como condição de possibilidade das interações humanas, referindo-se à "[...] vigilância eletrônica e em massa global" (FAVERA, 2018, p. 7).

A *surveillance* contemporânea não é uma prática disseminada somente no âmbito das agências de inteligências vinculadas ao governo, podendo também ser efetuada por empresas e indivíduos ou grupos. Sua execução demanda uma atuação organizada, rotineira e habitual, através da observação sistemática de dados pessoais, visando objetivos específicos, que vão desde o controle até a influência de grupos sociais (FAVERA, 2018, p. 15).

Menezes Neto, Morais e Bezerra (2017, p. 187) destacam o modelo proposto por Kevin D. Haggerty e Richard V. Ericson, no artigo intitulado "*The surveillant assemblage*", analisando a multiplicidade de sistemas individuais de coletas de dados distintas, que recombinadas de diferentes formas, funcionam em conjunto formando uma unidade. Esse modelo, que destaca o fluxo discreto de dados, é chamado de *dataveillance*. Para Ericson e Haggerty (2000, p. 606), a *surveillant assemblage* funciona através da abstração dos corpos humanos de suas configurações territoriais, e posterior separação em uma série de fluxos discretos de dados, que serão reagrupados e direcionados para intervenção.

A *dataveillance,* cuja tradução literal seria "vigilância de dados" relaciona-se ao fluxo discreto de dados que é coletado de forma massiva, mas transparente, inserida do cotidiano das pessoas, seja ao realizar uma compra *on-line*, ao assistir um filme via *streaming*, ou pelo simples fato de portar um celular conectado à *Internet* na rua. Esses dados (ou metadados), posteriormente, podem ser reconstruídos conforme a demanda, formandos novos significados e trazendo sérias ameaças aos direitos fundamentais dos usuários (MENEZES NETO; MORAIS; BEZERRA, 2017, p. 187-8).

Diante da coleta massiva de dados pessoais por parte de entidades públicas e privadas para fins de segurança pública, Carlos Alberto Molinaro e Ingo Wolfgang Sarlet reconhecem a existência de um novo modelo de Estado, denominado "Estado de Vigilância", que constitui-se em "uma forma de contaminação da democracia caracterizada pela intrusão dos governos e das corporações na liberdade e na privacidade de terceiros, sejam estes atores públicos ou

privados" (MOLINARO; SARLET, 2013, p. 65). Este modelo de Estado, próprio de uma sociedade em rede, evidencia a forma como o poder é exercido por meio do controle da informação, e como os governos e entidades privadas adquirem este poder por meio da vigilância e da mineração de dados, com a justificativa da "Guerra ao Terror".

Assim, a privacidade encontra-se entre a liberdade e a segurança, especialmente diante das ameaças terroristas e da insegurança gerada pela sofisticação dos *cibercrimes*, o que leva a um permanente Estado de vigilância, atualizando o próprio modelo do panóptico de Benthan (MOLINARO; SARLET, 2013, p. 69-70). Através da mineração de dados, e a sua respectiva manipulação, concatenação e análise, os governos vigilantes visam não somente à antecipação de possíveis ameaças, mas especialmente o interesse mercadológico, tendo em vista que informação representa poder.

Em face do paradigma informacional da pós-modernidade (e sua liquidez), Zygmunt Bauman e David Lyon (2013, p. 12) apresentam o conceito de "vigilância líquida" como um "pós-panóptico", no qual mobilidade e nomadismo passam a ser valorizados, e o observador pode estar em qualquer lugar, inacessível. Essa vigilância, característica de uma sociedade moderna que carece de vínculos duradouros, se manifesta no estado "líquido", na medida em que é exercida de forma diluída através de novos meios de monitoramento que estão inseridos de forma silenciosa e invisível no dia a dia das pessoas, mas está atenta a todos os seus movimentos. A vigilância líquida é exercida de forma imperceptível, suavizada e móvel, através do uso das TIC, sem que haja qualquer resistência por parte de quem está sendo observado, diminuindo a possibilidade de identificação do observador, e, ao contrário, aumentando infinitamente a possibilidade de controle por parte das organizações de vigilância.

A vigilância é justificada, especialmente, sob o argumento da segurança e se espalha silenciosa no âmbito do consumo. Ferramentas de monitoramento (os chamados *cookies*[5]) permitem que as ofertas sejam direcionadas ao consumidor selecionado, aquele que já demonstrou interesse pelo tipo de produto ofertado. O usuário sente-se "agradecido" pela oferta amigável, quase um conselho dirigido por um amigo, e voluntariamente (e até com certo entusiasmo) dispõe de seus dados pessoais, tornando a vigilância ainda mais eficaz. Além disso, o sentimento de insegurança coletiva, característica marcante da sociedade pós-11 de setembro, induzem os próprios indivíduos ao fornecimento de dados pessoais de forma voluntária, fazendo parte do cotidiano o preenchimento de cadastros, o uso de senhas de acesso,

[5] *Cookies* são pequenos arquivos de dados enviados por um *website* e armazenados no computador do usuário, possibilitando que o *site* tenha acesso ao seu histórico de navegação (TOURIÑO, 2014, p. 57).

a prática de *check-ins* para o uso de redes sem fio, a submissão a *scanners* corpóreos, entre outros.

Assim, Zygmunt Bauman e David Lyon (2013, p. 29) referem que "[...] o aspecto mais notável da edição contemporânea da vigilância é que ela conseguiu, de alguma maneira, forçar e persuadir opositores a trabalhar em uníssono e fazê-los funcionar de comum acordo, a serviço de uma mesma realidade". Ao contrário dos prisioneiros do panóptico, cujo medo e a ameaça de estarem sendo observados eram utilizados como ferramenta de vigilância pelo carcereiro, o indivíduo pós-moderno busca a exposição a todo momento, tornando-se uma presa ainda mais fácil às organizações de vigilância. Os "corpos dóceis" da teoria de Foucault, passam a ser moldados de forma imperceptível, ao gosto do consumidor.

O embate entre ética e segurança permeia a questão da "adiaforização" da sociedade atual, em que os processos distanciam-se de questões morais, efetivando-se melhor à distância, na medida em que afasta o indivíduo das consequências de sua ação. No que se refere à vigilância, os dados pessoais coletados são sugados para bancos de dados a fim de processamento e análise, sendo posteriormente replicados e fragmentados. Nesse processo, tornam-se informações frias, desvinculadas do ser humano titular, e, na sociedade atual, acabam por inspirar mais confiança do que a própria pessoa (BAUMAN; LYON, 2013, p. 15).

Tal preocupação já podia ser percebida na obra de Deleuze (1992, p. 222), que em 1990 observava que os indivíduos tornaram-se divisíveis, em amostras, dados, mercados, ou "bancos". No mesmo sentido, Menezes Neto, Morais e Bezerra (2017, p. 191) lembram de Kafka, e seu clássico "O Processo", para demonstrar uma analogia com a coleta de dados nos dias atuais, e a consequente "dissolução do ser humano em uma rede composta por práticas padronizadas, procedimentos secretos e a incapacidade de interação com aqueles que definem os critérios de processamento das informações".

Outro problema a ser destacado refere-se à categorização social realizada pelos mecanismos de vigilância, o que atinge as liberdades civis e os direitos humanos. Apesar de uma aparente eventualidade, pessoas de determinados grupos étnicos recebem tratamento diferenciado em aeroportos, sendo rotulados como indesejadas a partir de processos de estereotipia que visam à exclusão social (BAUMAN; LYON, 2013, p. 13). No âmbito do consumo, da mesma forma que o sistema seleciona os consumidores que lhe interessam, exclui e marginaliza aqueles que não se encaixam em sua política.

Além disso, as mídias sociais estão sendo responsáveis por uma mudança de paradigma à privacidade, confundindo os limites entre a esfera privada e pública. A exposição (e o consumo) de informações de cunho pessoal na *Internet*, acessíveis a "amigos" que são

verdadeiros desconhecidos, acaba tornando-se a lógica das redes sociais. Os usuários, ávidos pela exposição de sua intimidade, tornam a rede mundial de computadores uma plataforma própria para suas confissões pessoais. Essa característica da sociedade atual faz com que Bauman e Lyon (2013, p. 28) cheguem a falar em uma "morte do anonimato" trazida pela *Internet*, afirmando que "submetemos à matança nossos direitos de privacidade por vontade própria".

Preocupado não apenas com relação à exposição voluntária nas redes sociais, mas também com o fornecimento de dados pessoais que são coletados por aplicativos na rede, Manuel Castells (2003, p. 143-5) anuncia um "fim da privacidade", afirmando que as pessoas abrem mão do seu direito à privacidade para poder utilizar a *Internet*, e advertindo para a criação de um sistema eletrônico de vigilância governamental. O autor (2003, p. 148) traz para os dias atuais o conceito de panóptico, e diz que viver em um panóptico eletrônico é o equivalente a ter metade da vida exposta a monitoramento, na medida em que grande parcela da interação pessoal, o trabalho e o lazer ocorrem na *Internet*, e que a maior parte da atividade econômica, social e política é um híbrido de interação *on line* e física.

Entretanto, a vigilância na modernidade líquida distingue-se do panóptico na medida em que não visa mais ao confinamento (manter dentro), mas sim à exclusão (manter afastado). A vigilância realizada no âmbito do controle fronteiriço entre estados nacionais, por exemplo, está ligada à segurança, e ao objetivo de manter o afastamento dos indivíduos indesejados, e não propriamente ao aprisionamento e à disciplina que caracterizava o modelo de Bentham e Foucault (BAUMAN; LYON, 2013, p. 64-5). Partindo deste paradigma, Didier Bigo redefine o conceito de panóptico à partir do termo "ban-óptico", que indica a maneira como a tecnologia de elaboração de perfis é utilizada para banir certos grupos em nome de seu potencial futuro comportamento, funcionando como uma forma de (in)segurança em nível transnacional (BIGO, 2006, p. 35). Este modelo, para Bauman e Lyon (2013, p. 63), evidencia quais indivíduos são bem-vindos ou não, criando categorias de pessoas excluídas, seja pelo próprio Estado, seja por outras potências globais.

A coleta de fluxo de dados com o uso das TIC converte-se em instrumento de segregação social, afetando não somente o direito à privacidade, mas também atingindo a liberdade e a igualdade, o que se observa desde a concessão de benefícios de forma discriminatória até a restrição na utilização de transporte aéreo a algumas pessoas (MENEZES NETO; MORAIS; BEZERRA, 2017, p. 196-7). Na sociedade contemporânea, além das violações à intimidade, a ameaça à liberdade, representada pelo emprego de tecnologias de controle individual e coletivo, e à igualdade, que toma forma desde a segregação entre aqueles que tem acesso ao poder

informático e os que são alijados do seu uso, são os reflexos de um paradigma tecnológico imposto ao cidadão desde o seu nascimento (PÉREZ LUÑO, 2012, p. 23).

Se o controle eletrônico exercido pelos governos tradicionais representa grande preocupação à maioria dos ciberativistas, as novas formas de poder surgem como ameaças ainda mais alarmantes. A ingênua transparência possibilitada pelas redes oculta a atuação dos buscadores, firmas de inteligência de mercado e agências de avaliação creditícia, que exercem grande influência na vida das pessoas ao acessarem livremente as suas informações pessoais, mas, em contrapartida, não apresentam qualquer transparência em suas operações (LANIER, 2015, p. 359-360).

O mesmo perigo sofre o trabalhador em relação à vigilância no âmbito da relação laboral, que costuma ser implementada em todas as etapas do contrato de trabalho, desde antes mesmo da sua formação. Diversas são as informações pessoais fornecidas por força do contrato de trabalho, e as mais variadas práticas de monitoramento inseridas nos sistemas produtivos, dentro e fora do ambiente laboral, conduzem a uma coleta exacerbada de dados pessoais. Por outro lado, a atuação empresarial nem sempre é revestida de transparência no que se refere ao tratamento dessas informações, ocultando do trabalhador as finalidades da coleta e a sua destinação, frequentemente discriminatórias.

A persistência de práticas autoritárias de vigilância no local de trabalho é uma preocupação para Castells[6], que entende ser este o ambiente "mais importante de nossas vidas". O autor afirma que à medida que os trabalhadores tornaram-se cada vez mais dependentes da interconexão *online*, as empresas passaram a monitorar o uso das redes por parte de seus funcionários, gerando, inclusive, despedidas pelo uso impróprio da *Internet*. Segundo estudos trazidos pelo sociólogo espanhol, 73,5% das companhias dos EUA exerciam, no ano de 2000, alguma forma de vigilância sobre o uso da *internet* de seus empregados (CASTELLS, 2003, p. 143). É provável que a maior parcela destes funcionários sequer desconfiasse desse monitoramento no ambiente empresarial, e, ainda que o fizessem, muitos teriam dificuldade de se insurgir contra esta prática em virtude da assimetria que é própria da relação trabalhista, obstáculo que dificulta o acesso do trabalhador ao Poder Judiciário até a atualidade.

[6] Com relação às modificações do trabalho e do mercado de trabalho frente à evolução tecnológica, Manuel Castells considera que o principal instrumento de impacto do paradigma informacional e do processo de globalização na sociedade é a transformação tecnológica e administrativa do trabalho e das relações de produção existentes dentro e em torno da empresa emergente em rede (CASTELLS, 2005, p. 265). Certamente que o surgimento de novos postos de trabalho à distância, monitorados pelo uso das TIC, representa um dos principais aspectos dessa mudança. Para maiores aprofundamentos sobre o teletrabalho, sugere-se a leitura de Fincato (2003).

Os instrumentos de controle tendem a tornar-se parte da própria estrutura do sistema nas empresas, perdendo sua natureza autônoma. Com isso, os trabalhadores estão cientes de que, ao utilizarem o seu terminal de trabalho, estarão sendo vigiados a cada atividade desenvolvida, sem a necessidade de uma estrutura especificamente destinada para isso. O aparato eletrônico de vigilância monitora os tempos, os ritmos de trabalho, os intervalos, estando à disposição de quem tenha interesse em avaliar os funcionários (RODOTÁ, 2008, p. 112).

O incremento das novas tecnologias de processamento automático trouxe diversos riscos ao trabalhador, que permanece em constante supervisão imposta por um sistema de informação representado por um mecanismo inacessível, disponível somente ao empregador (SANDEN, 2014, p. 26). Tal qual o panóptico, a vigilância eletrônica nos dias atuais confere ao obreiro a incerteza de estar sendo continuamente vigiado através do tratamento massivo de seus dados pessoais, ampliando a pressão sobre a sua atividade, independentemente do conhecimento exato sobre o funcionamento e as funcionalidades do sistema.

O corriqueiro processamento e o fluxo de dados convertem o empregador em um verdadeiro repositório de informações pessoais do trabalhador, sendo que o avanço tecnológico elimina o problema do espaço físico para armazenamento. Com isso, os dados pessoais (e seus fragmentos) estão sempre disponíveis para o tratamento, podendo ser livremente combinados e reagrupados, de acordo com os diferentes contextos e objetivos que possa ter o empregador, muitas vezes de forma alheia às finalidades para os quais foram obtidos, na medida em que as tecnologias da informação permitem que se quebre a relação com o propósito original da coleta (SANDEN, 2014, p. 23-4).

Além da possibilidade de lesão a dados sensíveis[7] do trabalhador, e da utilização para fins diversos da coleta, a utilização das novas tecnologias no processamento de informações pessoais traz consigo o perigo de que as decisões do empregador estejam sendo tomadas por processos totalmente automatizados (SANDEN, 2014, p. 26), o que viola o direito fundamental da proteção em face da automação, consagrado pelo artigo 7°, XXVII, da Carta Magna (BRASIL, 1988).

A evolução tecnológica também possibilita o deslocamento geográfico das atividades tradicionais da empresa e a prestação de serviços de locais remotos (SÁNCHEZ BRAVO, 2010, p. 26), permitindo que o controle do empregado possa ser exercido também fora do ambiente empresarial, de forma portátil, difusa e ainda mais eficaz. A velocidade com que as informações

[7] Dados sensíveis são determinados tipos de informação que possuem potencial de utilização discriminatória, tais como as relativas à raça, crenças religiosas e políticas, vida sexual, saúde e dados genéticos de um indivíduo (DONEDA, 2006, p. 160-1).

são disseminadas e a facilidade de deslocamento dos dispositivos eletrônicos, cada vez menores e mais potentes, ampliaram as possibilidades de controle patronal, não mais sendo necessário o ambiente fechado para a implantação da disciplina aos trabalhadores. Ao contrário, os dispositivos móveis tornam a vigilância ainda mais sufocante ao trabalhador, na medida em que ele passa a carregar os seus próprios panópticos pessoais junto ao corpo (BAUMAN; LYON, 2013, p. 61).

A *Internet* converte-se em um dos principais instrumentos da vigilância permanente que pode ser exercida por diversos atores, expondo os dados pessoais do trabalhador a qualquer pessoa que possua acesso à rede mundial de computadores e interesse em pesquisar sobre a vida pregressa do indivíduo. Uma das principais formas de operar esta vigilância é pelo acesso às informações processuais divulgadas pelos portais dos Tribunais do Trabalho, ou por *sites* que realizam a busca e o agrupamento de trâmites judiciais, tornando-se ferramentas discriminatórias nas mãos do empregador que busca referências sobre o candidato a uma vaga de emprego. Com isso, acentua-se a relevância de uma efetiva proteção aos dados pessoais como forma de garantia da liberdade e da igualdade dos titulares, impedindo a criação de obstáculos ao mercado de trabalho, posição que é sustentada por Tepedino e Teffé (2019, p. 288):

> O desenvolvimento de mecanismos destinados a regular o tratamento dos 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 análise de dados não informadas ao titular e sob critérios não transparentes.

Nesse cenário, as modernas possibilidades de acesso e armazenamento de informações pessoais do trabalhador podem repercutir em fatores impeditivos para sua contratação, ainda que as informações coletadas não contenham qualquer relação com o objeto do contrato de trabalho (WEINSCHENKER, 2013, p. 65). São recorrentes na justiça laboral ações que se insurgem contra a prática de condutas discriminatórias pelas reclamadas, especialmente através da elaboração e divulgação de listas contendo nomes de trabalhadores que tenham proposto ação judicial contra seus empregadores, as chamadas "listas discriminatórias" ou "listas negras[8]", conforme denomina Weinschenker (2013, p. 58). Trata-se de bancos de dados com informações desabonatórias de ex-empregados, na quais constam, além das reclamações

[8] Entende-se que a utilização da expressão "lista negra" é inapropriada, pois seu conteúdo semântico pode reforçar a carga discriminatória da própria prática reprovável. Opta-se pela adoção dos termos "listas discriminatórias" ou "listas sujas".

trabalhistas ajuizadas anteriormente pelo trabalhador, outras informações de cunho discriminatório como antecedentes criminais, restrições de crédito e a participação em movimentos paredistas, visando à retaliação de seus componentes pelo empresariado, o que atinge não somente a privacidade, mas também o direito do trabalhador à igualdade, conforme refere Limberger (2007, p. 62).

O processo de seleção e contratação é a fase em que o empregador necessita de maior número de informações do candidato, necessárias para a aferição de seu nível de conhecimento, aptidões e capacidades. Torna-se, com isso, um momento especialmente delicado do ponto de vista da proteção de dados pessoais do trabalhador, já que alguns dados relacionados ao perfil profissional do trabalhador são indissociáveis de sua vertente pessoal ou privada. Esse tratamento de dados ocorre em um contexto em que o candidato encontra-se em posição de vulnerabilidade ainda mais acentuada que o trabalhador já contratado, principalmente porque sabe que a oposição de resistências aos questionamentos feitos pelo contratante em entrevistas de emprego certamente levarão à sua preterição (VILLALÓN, 2019, p. 9-10). Somado a isso, nesta fase a empresa costuma realizar uma verdadeira "varredura" na vida pregressa do candidato, buscando informações relacionadas aos seus antecedentes, prática que, nas últimas décadas, ganhou o incremento da *Internet* como principal ferramenta.

Essa investigação prévia feita pela empresa costuma atingir os dados sensíveis do trabalhador, já que as pesquisas incluem antecedentes laborais, preparação para o desempenho de tarefas (estudos, títulos e experiências anteriores), trabalho anterior e razão do desligamento, situação familiar, preferências pessoais e políticas, crenças religiosas, filiação sindical, origem étnica e antecedentes criminais do empregado. Entretanto, o critério utilizado pelo empregador na sua busca deve restringir-se à avaliação da aptidão do candidato à realização das funções relacionadas ao cargo que ocupará, sob pena de violação do direito à intimidade do obreiro. Nesse sentido, indagações plausíveis seriam relativas às experiências obtidas, certificados, diplomas, local de trabalho anterior e demais assuntos ligados à capacidade profissional do candidato (BARROS, 2009, p. 68), parâmetro que deve nortear eventuais pesquisas realizadas na rede mundial de computadores.

Portanto, a investigação dos antecedentes do trabalhador, inclusive a avaliação prévia de sua atividade nas redes sociais, prática bastante utilizada quando se trata do candidato jovem, até poderiam ser cogitadas desde que a sua finalidade fosse estritamente a de contratar trabalhadores com reais condições de assumir determinada atividade (FRANCO FILHO, 2016, p. 24). Ainda assim, a utilização desses dados para fins de seleção de pessoal somente poderia ser considerada legítima quando o interessado houver divulgado as informações por vontade

própria, para fins profissionais e não privados, devendo ser informado sobre qualquer operação de tratamento antes do início do processo de seleção, separando-se os dados que exigem o seu consentimento (VILLALÓN, 2019, p. 67).

O que se observa, justamente ao contrário, é a utilização de tais ferramentas com o intuito discriminatório, satisfazendo os pré-conceitos pessoais do empregador que o levam a uma seletividade arbitrária, principalmente quando se trata da consulta ao histórico de ajuizamentos de reclamações trabalhistas do obreiro. Essa prática atinge o trabalhador que figurou como reclamante na Justiça do Trabalho não somente pela obstrução do acesso à uma vaga de emprego, mas também pela coleta de dados sensíveis que integram os despachos e decisões judiciais, revelando informações de saúde, orientação sexual, crenças religiosas, preferências políticas, hábitos pessoais, etc., o que apresenta enorme potencial discriminatório também para outros sujeitos do processo do trabalho, como as testemunhas e terceiros envolvidos na lide.

Ainda que seja legítimo o direito à informação patronal, esse direito fundamental não pode ser exercido sem limitações e tampouco abrange toda e qualquer informação que integre os processos judiciais. É evidente que não cabe ao empregador a delimitação entre a informação que deve ou não ser publicizada pelo Poder Público (discussão que será abordada no tópico seguinte), e, portanto, a empresa não pratica ilegalidade alguma pelo simples fato do acesso a dados que são fornecidas por fontes oficiais. Entretanto, o tratamento de dados pelo empregador deve seguir alguns parâmetros, tais como a necessidade de informação ao demandante de emprego sobre tipo de tratamento de dados que está sendo realizado para fins de seleção profissional, incluindo o detalhamento acerca das finalidades para os quais os dados serão utilizados (VILLALÓN, 2019, p. 71), bem como a observância dos princípio da não discriminação (que integra a maioria das normativas relativas à proteção de dados pessoais na América Latina e na União Europeia), e da própria boa-fé, sob pena da devida responsabilização civil no caso de danos gerados aos titulares.

No caso em que o empregador busca em portais dos tribunais trabalhistas ou em buscadores na *Internet* o conhecimento acerca de dados alheios à finalidade contratual, que em nada justificam a sua coleta, utilizando-os para fins discriminatórios, não só o Poder Público, encarregado pelo armazenamento das informações, mas a empresa que mantém o buscador que reproduz, organiza e fornece acesso a esses dados pessoais e o próprio empresário tornam-se responsáveis, direitos ou indiretos, pela violação a direitos fundamentais do obreiro.

Fato é que quando o trabalhador recorre à Justiça do Trabalho, ente responsável pela salvaguarda de direitos que foram descumpridos durante o contrato de trabalho, é surpreendido

por nova violação no curso do processo trabalhista, emanada pelo próprio Poder Judiciário, que expõe seus dados pessoais ao livre acesso público na rede mundial de computadores, sem o consentimento específico para esta finalidade. Essa constatação impõe a necessidade de um estudo específico sobre a utilização das tecnologias informacionais pela administração pública e a divulgação de dados pessoais no processo do trabalho, buscando-se estabelecer os limites entre a informação de interesse público e a informação de caráter privado, que merece um regime protetivo mais rigoroso.

1.2 O USO DAS TIC PELO PODER JUDICIÁRIO: a divulgação de dados pessoais no âmbito da Justiça do Trabalho

O uso abusivo de dados pessoais do empregado por outros particulares desvela um efeito colateral do legítimo exercício do direito de ação pelo obreiro, cujo responsável passa a ser o próprio Poder Público. O empregado que ajuíza reclamação trabalhista buscando a satisfação de obrigações não cumpridas pelo contratante torna-se vulnerável diante do acesso de terceiros a informações que podem obstaculizar a contratação por outro empregador, ou até mesmo da violação de sua privacidade mediante a divulgação de dados sensíveis que passam a integrar as atas de audiência e decisões judiciais, muitas vezes disponíveis pelo *site* do tribunal ou por mecanismos de busca na *Internet*.

Com frequência a via jurisdicional representa a última esperança do trabalhador a fim de fazer cessar uma violação sofrida durante o contrato de trabalho, o que pode, inclusive, decorrer de um ato discriminatório, como são os casos envolvendo despedidas discriminatórias e assédio moral. Entretanto, ao buscar o Poder Judiciário, o reclamante torna-se novamente vítima, através da exposição pública de aspectos de sua intimidade (até mesmo com a reprodução das próprias ofensas sofridas), o que se torna acessível a qualquer pessoa que consultar o inteiro teor da decisão judicial por meio da rede mundial de computadores (SILVA, R., 2019, p. 163), repercutindo e potencializando o surgimento de novas discriminações.

Diversas são as formas de relacionamento entre os cidadãos e o Estado, através da prestação dos mais diversos serviços públicos, o que eleva o Poder Público à condição de grande produtor e coletor de dados pessoais. Todas essas informações interessam, e muito, ao mercado, e aos próprios cidadãos, financiadores e usuários dos serviços ofertados (CARVALHO; CABRAL, 2019, p. 59). O Poder Judiciário, enquanto órgão responsável pela tutela jurisdicional, está compreendido dentro do dever de publicidade administrativo, e utiliza o aparato estatal neste intuito. Aqui, entretanto, importa que se reconheçam os limites para a

publicização das informações processuais.

Existem duas formas de abastecimento dos bancos de dados: seja pela coleta direta através do titular, ou por meio da transferência de informações armazenadas em outros bancos de dados. A transmissão de dados pessoais ocorre mediante o repasse de dados da pessoa ou entidade que realiza o tratamento para terceiros, o que pode ocorrer com ou sem o consentimento do titular dos dados (DONEDA; VIOLA, 2009, 94-5). Os bancos de dados mantidos pelo Poder Judiciário são alimentados pelo fornecimento de dados pessoais diretamente pelos seus titulares, mediante o ajuizamento de ações judiciais. Entretanto, essas informações acabam sendo disponibilizadas para terceiros por meio dos portais institucionais, ou reproduzidas por empresas privadas, responsáveis pela manutenção de *sites* que realizam buscas envolvendo trâmites judiciais na *Internet,* sem o consentimento do jurisdicionado.

O indivíduo que fornece seus dados pessoais ao Poder Judiciário o faz na confiança de que o tratamento e a distribuição desses dados será limitada ao estritamente necessário à tutela jurisdicional. Ao permitir que esses dados sejam coletados e replicados por entidades privadas, o Estado contribui com a violação de direitos que pretende combater, amplificando o potencial discriminatório dos dados divulgados e originando novas demandas futuras. Uma vez prejudicado no contrato de trabalho, o empregado acaba sendo atingido novamente ao buscar guarida na Justiça do Trabalho.

A publicização da atividade jurisdicional do Estado em si é algo positivo e necessário, fundamentado pelo dever de transparência da administração pública, próprio de um Estado Democrático de Direito. O problema consiste na possibilidade de livre acesso às informações contidas no processo, sendo que o nome é um direito da personalidade indisponível ao Estado, incorporando não só o direito à privacidade como também o direito à não-discriminação, e o seu tratamento necessita do prévio consentimento do titular, algo que somente poderia ser dispensado diante do interesse direto ou por questões de interesse público (LIMBERGER; RUARO, 2011, p. 130).

A difusão das sentenças e despachos judiciais na *Internet* foi tema de uma reunião, ocorrida em julho de 2003 em Heredia, na Costa Rica, promovida pelo *Instituto de Investigación para la Justicia Argentina*, com o apoio da Corte Suprema de Justiça da Costa Rica e patrocínio da *International Development Research Centre* do Canadá. Na ocasião, o debate culminou na formulação do principal documento existente a respeito da difusão da informação judicial na *Internet*, a "Carta de Heredia" ou "Regras de Heredia" (INSTITUTO..., 2003), que estabelece regras mínimas a serem adotadas pelos organismos responsáveis por esta divulgação.

O documento visa nortear governos e poderes judiciais do mundo quanto ao tratamento de dados pessoais em seus *sites* visando a transparência das atividades judiciais e proteção da privacidade e intimidade dos demandantes no Poder Judiciário (GREGÓRIO; PAIVA, 2005, p. 01). Com isso, a Carta de Heredia pode servir como modelo a ser adotado pelos tribunais dos países da América Latina, podendo ser incorporados pelo regulamento interno de cada tribunal.

Carlos Gregório e Mário Paiva (2005, p. 12), que foram palestrantes no evento em Heredia e participaram da elaboração das regras, assim denunciam os prejuízos sofridos por trabalhadores em virtude do acesso de decisões judiciais pela *Internet* no Brasil:

> No Brasil, por exemplo, vários trabalhadores tiveram o seu direito a livre acesso ao emprego vetado pelo futuro empregador em virtude da disponibilização de consulta por nome dos reclamante (*sic*) nos sites dos tribunais. Tal procedimento trouxe reconhecidos e concretos prejuízos a milhares de trabalhadores tanto que foi admitido pelos próprios tribunais que alguns anos mais tarde resolveram abolir este tipo de pesquisa.

As regras evidenciam uma preocupação em estabelecer um equilíbrio entre o direito à privacidade e a transparência e direito de acesso à informação pública, o que poderá ser instrumentalizado por meio de duas proposições, previstas na Regra 7: a) a utilização de motores de buscas capazes de ignorar nomes e dados pessoais nas bases de dados e sentenças; e b) a utilização do número do processo como critério de busca nas bases de dados de informações processuais (INSTITUTO..., 2003).

O direito de acesso à informação pública, que teve o seu reconhecimento enquanto direito fundamental através do artigo XIX da Declaração Universal dos Direitos Humanos, proclamada pela Assembleia Geral das Nações Unidas em 1948 (ASSEMBLEIA...,1948), "[...] consiste na faculdade que possuem as pessoas, físicas e jurídicas de solicitar documentação oficial e informação que se encontra em mãos do Estado, de consultá-la, tomar conhecimento dela e obter sua reprodução"[9] (LAVALLE COBO, 2009, p. 33).

Este direito fundamenta-se na ideia de que a informação que está em mãos do Poder Público pertence à própria sociedade. A democratização do acesso à informação garante, assim, um diálogo entre governantes e sociedade civil, permitindo a abertura, transparência e participação, bases de qualquer democracia (MENDEL, 2009, p. 1). Nos últimos anos, diversos países latino-americanos têm adotado legislações regulamentando o acesso à informação, sendo que a Argentina foi um dos mais recentes, através da edição da Lei nº 27.275/16, cujo âmbito

[9] Do original: "El derecho de acceso a la información pública consiste em la faculdad de las personas, físicas y jurídicas de solicitar documentación oficial e información que se encuentre en manos del Estado, de consultarla, tomar conocimiento de ella y obtener su reproducción".

de aplicação abrange os Poderes Executivo, Legislativo e Judiciário[10] (ARGENTINA, 2016c).

No Brasil, o acesso à informação alcançou a categoria de direito fundamental pelo artigo 5°, incisos XIV e XXXIII da Constituição da República Federativa do Brasil, que garantem a todos o acesso à informação e o direito de receber dos órgãos públicos informações de interesse particular, coletivo ou geral. A Carta Magna contempla, ainda, a publicidade como um dos princípios gerais da administração pública (artigo 37, caput) (BRASIL, 1988).

A Lei nº 12.527/2011 (Lei de Acesso à Informação - LAI), que rege o direito à informação[11] no país, determina a "observância da publicidade como preceito geral e do sigilo como exceção" (artigo 3º, I) (BRASIL, 2011b). A lei impõe ao Poder Público o dever de transparência, no seu duplo viés: o da transparência passiva, que consiste no dever de responder às solicitações enviadas por qualquer pessoa que manifeste o interesse por meio de uma solicitação; e o da transparência ativa, que diz respeito ao dever de divulgar as informações de forma proativa e rotineira, antecipando-se às eventuais solicitações dos cidadãos (CONTROLADORIA-GERAL..., 2013, p. 6).

Entretanto, a transparência pelo Poder Público não pode ser exercida de forma indiscriminada, devendo observar alguns critérios para não atingir os direitos de personalidade das pessoas envolvidas com a informação que se pretende dar publicidade. A própria LAI, em seu artigo 31, prevê a obrigatoriedade do tratamento das informações pessoais ser feito de forma transparente, respeitando a intimidade e a vida privada dos titulares dos dados, estabelecendo a necessidade de previsão legal ou consentimento para a sua divulgação ou acesso por terceiros (BRASIL, 2011b).

Publicidade e transparência são dois conceitos distintos, mas que caminham no mesmo sentido: enquanto a transparência possibilita ao cidadão ter acesso à informação pública, a publicidade é a exteriorização dos atos da administração pública para a coletividade, fortalecendo o próprio Estado Democrático de Direito (LIMBERGER, 2016, p. 45-46). Além da transparência das decisões governamentais, o princípio da publicidade visa facilitar o seu conhecimento pelos administrados, tornando efetivo o acesso à informação (LAVALLE COBO, 2009, p. 7). Ocorre que nem toda informação que é "publicizada" na *Internet* pela

[10] Antes da publicação da Lei nº 27.275/16, o direito de acesso à informação na Argentina era disciplinado pelo Decreto Presidencial nº 1.172/03, aplicável somente no âmbito do Poder Executivo (OYHANARTE; KANTOR, 2015, p. 259).

[11] O direito à informação pode ser observado sob três diferentes aspectos: o direito de informar, o direito de ser informado e o direito de se informar. Enquanto o direito de informar diz respeito à possibilidade de transmitir informações e comunicar acontecimentos, o direito de ser informado vincula-se à faculdade de receber informações de órgãos públicos ou de bancos de dados que mantenham registros sobre o indivíduo e o direito de se informar confere à pessoa a faculdade de buscar essas informações sem obstáculos (MORAES, 2018, p. 27-9).

administração pública faz parte do exercício da transparência, o que passa pela delimitação da tênue fronteira entre o público e o privado (LIMBERGER; RUARO, 2011, p. 125).

A delimitação de fronteiras entre o público e o privado é uma árdua tarefa que há muito ocupa as reflexões doutrinárias. Para a filósofa Hannah Arendt (2007, p. 47-8), a era moderna representou uma diluição da antiga divisão entre privado e político, alterando significativamente o sentido dos dois termos e a sua importância aos indivíduos. A privatividade moderna (hoje tida como um círculo de intimidade) opõe-se à esfera social, esta desconhecida dos antigos, que passa a ser ampliada, "devorando" as antigas esferas do político e do privado (ARENDT, 2007, p. 55).

A autora define a esfera pública sob dois fenômenos: significa dizer, em primeiro lugar, que tudo que é público pode ser visto e ouvido por todos, constituindo a realidade. A realidade relaciona-se, portanto, à aparência. Em segundo lugar, a esfera pública representa o mundo comum, que separa e estabelece relações entre os homens (ARENDT, 2007, p. 59-62). A esfera privada, por outro lado, representa ao indivíduo a privação dessas características essenciais do ser humano: ser privado da realidade proveniente de ser visto e ouvido pelos demais indivíduos, privado da relação objetiva que estabelece com as outras pessoas por meio de um mundo comum, além de ser privado da realização de algo que transcenda a limitação temporal de sua própria vida (ARENDT, 2007, p. 68).

Portanto, a distinção ente o público e privado, na perspectiva de Hannah Arendt, "[...] equivale à diferença entre aquilo que deve e pode ser mostrado – o visível – e aquilo que pode e deve ser ocultado (LAFER, 1991, p. 261). Em síntese, na visão da autora o público representa o comum, que está ao alcance dos olhos, e o privado é o que diz respeito somente ao indivíduo enquanto ser singular, e que por conta disso deve ficar distante da publicidade. Dessa forma, a defesa da intimidade torna-se uma medida necessária contra a banalização da esfera pública, diante da invasão do público pelo íntimo (LAFER, 1991, p. 271).

Apresentando uma proposta de delimitação entre a informação pública e privada, Dolores Lavalle Cobo (2009, p. 9) define como informação pública toda aquela que está em poder do Estado, o que pode coincidir ou não com a documentação administrativa, e cujo acesso não é expressamente vedado pela legislação. A autora argentina (2009, p. 10-1) lembra que o alcance deste conceito pode variar conforme a legislação de cada país, o que pode se dar de acordo com o sujeito que detém a informação em seu poder ou segundo a matéria relativa ao conteúdo da informação. Assim, algumas legislações garantem somente o direito de acesso aos documentos administrativos, vinculados restritivamente ao Poder Executivo, enquanto as legislações mais modernas estendem este direito à atividade administrativa dos órgãos do Poder

Legislativo e Judiciário.

Ainda acerca da dicotomia público/privado, Sônia Aguiar do Amaral Vieira (2002, p. 90) compreende os dados públicos como aqueles que dizem respeito à toda sociedade, e cuja publicação cumpre com o dever de informar e ser informado, tais como resultados eleitorais, orçamento nacional, declaração patrimonial de servidores públicos e até mesmo alguns dados pessoais que permitam a identificação do titular, tais como nome, domicílio, estado civil, filiação, cédula de identidade, etc. A evolução das ferramentas de coleta e manipulação de dados que permitem, na atualidade, uma vigilância massiva global, impõe a necessidade de atualização deste entendimento da autora, na medida em que novos dados podem surgir a partir do reagrupamento de informações pessoais, ainda que aparentemente inofensivas em seu aspecto original, o que demanda uma ampliação do conceito de dado sensível. A esse respeito defende Ana Frazão (2018b):

> Tais reflexões ajudam a mostrar que a linha distintiva entre dados pessoais e dados pessoais sensíveis pode não ser tão nítida, até porque a perspectiva de análise deve ser dinâmica e não estática. Dessa maneira, há boas razões para sustentar que são sensíveis todos os dados que permitem que se chegue, como resultado final, a informações sensíveis a respeito das pessoas.

Adentrando na discussão acerca da delimitação entre os dados cadastrais passíveis de veiculação pelo Poder Público, Matos e Ruzyk (2019, p. 211) entendem que o endereço residencial integra um espaço de privacidade que não pode ser exposto sem o consentimento prévio de seu titular, uma vez que inexiste interesse público em sua divulgação, sendo este um item dispensável ao controle dos atos administrativos pelos cidadãos. Para eles, o mesmo tratamento não deve ser ofertado aos números de RG, CPF e cadastros profissionais de pessoas que contratam, celebram convênios ou se beneficiam direta, individual e voluntariamente dos atos da Administração Pública, já que esta identificação compõe o dever de transparência pública (MATOS; RUZYK, 2019, p. 211).

Assim, buscando uma definição teórica, os autores estabelecem um conceito indeterminado de interesse público em matéria de dados pessoais, que compreende "[...] aquilo que atende ao direito fundamental assegurado no inciso XXXIII do artigo 5º, conjugado com o artigo 37 da Constituição, ou seja, aquilo que é necessário para o controle social da transparência pública" (MATOS; RUZYK, 2019, p. 212).

É inegável que existem algumas situações em que o interesse público se sobrepõe ao particular, justificando a limitação da intimidade (VIEIRA, 2002, p. 27). A própria Lei de Acesso à Informação admite exceções à necessidade de expresso consentimento para a

divulgação de informações privadas, tais como: quando houver necessidade para a prevenção e diagnóstico médico, ao cumprimento de ordem judicial e à defesa de direitos humanos, dentre outros (BRASIL, 2011b). Mesmo nestes casos, eventual flexibilização do direito à privacidade somente seria justificado diante da inexistência de outros mecanismos para a garantia do acesso à informação, conforme a lição de Vieira (2002, p. 28):

> [...] é imperioso que o interesse público a sobrepujar o particular, em termos de vida privada, seja indispensável, ou seja, só se justifica o sacrifício, na exata medida da necessidade e se o interesse superior não puder ser satisfeito por outra forma, seja ele de natureza pública ou privada.

Importa salientar que alguns dados pessoais que são divulgadas por meio das consultas processuais e jurisprudenciais, especialmente os sensíveis, são informações que "[...] se ocultadas, não prejudicam a ninguém, porém, se reveladas, podem ocasionar prejuízos" (VIEIRA, 2002, p. 89), violando o direito à privacidade do jurisdicionado. Encontram-se nessa categoria de dados, conforme a classificação de Vieira (2002, p. 89), a orientação sexual, a religião, ideias sócio-políticas, situação econômica, raça, senha do *e-mail* e número de telefone. A essa lista podem ser incluídos as informações de saúde, informações creditícias, sindicais, e outras categorias capazes de conduzir ao tratamento discriminatório de seu titular.

Portanto, é imperioso que se reconheça a diferença de tratamento que deve ser ofertado às informações relativas à divulgação de contas, gestão administrativa, financeira e mesmo a produção de resultados pelo Poder Judiciário, cujo interesse público é evidente, com relação à divulgação de dados personalíssimos que foram fornecidos para a instrução de processos judiciais, de natureza sensível, que não se enquadram no conceito de interesse público (SILVA, R., 2018, p. 335).

Nesses casos, não há como se observar o interesse público a justificar o sacrifício de direitos fundamentais do jurisdicionados, ainda mais quando existem diversos mecanismos que possibilitam a ocultação dos trechos de caráter privado e a publicização das informações essenciais, cumprindo com o objetivo da transparência sem prejuízos (anonimização de dados, desindexação dos termos de busca, etc). Não existe, portanto, o caráter indispensável da divulgação e tampouco a informação essencial não pode ser franqueada de outra forma. Informações protegidas pela intimidade devem ser resguardadas, na medida em que a publicidade "[...] em tal caso busca satisfazer a simples curiosidade pública, sem propósitos de informação legítima" (RODRIGUES, 2014, p. 113).

É evidente que as novas tecnologias informacionais geraram ganhos de eficiência ao

setor público no tratamento das informações, permitindo o recolhimento de maior número de dados e, por consequência, uma maior informação e conhecimento nos processos decisórios, viabilizando também a coordenação e descentralização das atividades vinculadas ao serviços públicos (GONÇALVES, M. E., 2003, p. 113). O desenvolvimento tecnológico, especialmente da *Internet,* facilita a comunicação do Estado com a sociedade civil, potencializando a publicidade das atividades governamentais e proporcionando o acesso à informação ao cidadão por meio dos *sites* institucionais (LAVALLE COBO, 2009, p. 2).

No caso do Poder Judiciário, não são apenas as informações administrativas que possuem relevância aos cidadãos, mas também a sua atividade jurisdicional. Via de regra, entende-se que a atividade administrativa do Poder Judiciário deve ser pública. Com relação à função jurisdicional, entre as informações que devem ser publicizadas pela administração pública estão: estatísticas de causas ingressadas, pendentes e conclusas; sentenças; acesso a processos relacionados com crimes contra a administração pública; e a transparência nas sessões dos tribunais (BERAZATEGUI; EMANUELE, 2017, p. 262-3).

Em todos esses casos, tanto no que se refere à atividade administrativa ou jurisdicional, a limitação quanto ao tratamento de dados sensíveis deve ser observada pelo tribunal. Apesar de integrarem a categoria de arquivos públicos (com algumas exceções), os arquivos judiciais incorporam grande quantidade de informações pessoais, sejam informações básicas de identificação (nome, endereço, data de nascimento, etc), ou dados relacionados a condições médicas, estilo de vida, estado financeiro, desempenho laboral, dentre outros, que podem relacionar-se não apenas às partes, mas também a terceiros com implicação no processo (NISSEBAUM, 2010, p. 67).

Não se questionam os proveitos assegurados pelo implemento da informatização no Poder Judiciário, otimizando a atividade jurisdicional, facilitando o acesso às informações processuais e aumentando a economia e produtividade dos procedimentos, inclusive com a redução dos espaços de armazenamento e a diminuição de distâncias não apenas ao jurisdicionado, mas à toda sociedade (ABRÃO, 2011, p. 18). Reconhece-se, portanto, "[...] que o processo eletrônico foi criado para trazer vantagens àqueles que ao processo se encontram vinculados, como celeridade, praticidade e economia" (COLOMBO; DUARTE, 2019, p. 84).

No que diz respeito à democratização do acesso à justiça, as TIC possibilitam uma maior circulação das informações, aproximando o direito e a justiça dos cidadãos através de movimentos de abertura e transparência. Facilitam o acesso às bases de dados jurídicos, permitindo ao cidadão o exercício facilitado de direitos e deveres, seja através da apresentação de requerimentos, recebimento de informações, pagamento de taxas e impostos ou da consulta

processual (SANTOS, 2005, p. 9). Entretanto, não se pode perder de vista que os seus impactos aos operadores do direito e aos jurisdicionados não estão limitados aos benefícios.

A evolução do governo eletrônico, com todos os aspectos positivos que lhe são decorrentes, inclusive o implemento da eficiência administrativa e a ampliação da participação popular nos processos decisórios, não pode desvincular-se de uma blindagem das garantias individuais do cidadão, preocupação que é debatida por Rodotá (2008, p. 275):

> Freqüentemente é prometido aos cidadãos um futuro pleno de eficiência administrativa e oculta-se um presente no qual se multiplicam os instrumentos de um controle cada vez mais invasivo e ramificado. Chega a parecer que estão sendo construídos dois mundos não comunicantes, e que o *e-government*, a administração eletrônica possam evoluir sem levar em consideração os direitos individuais e coletivos. [...]

O processo judicial eletrônico representou uma mudança de paradigma em relação ao processo físico. No caso do processo em papel, ainda que o acesso seja público, existem diversas limitações que restringem o âmbito de alcance das informações, tais como deslocamento, formato dos autos, regras de consulta forense, etc. O processo eletrônico rompe definitivamente com essas barreiras, possibilitando que uma pessoa localizada em qualquer lugar do mundo, desde que incluída digitalmente, tenha completo acesso às informações produzidas pelas partes e pelo Poder Judiciário, o que abrange os dados pessoais sensíveis que integram os autos (GONÇALVES, V. H., 2015, p. 202). Ao permitir tamanha intrusão, a administração pública acaba por invadir a esfera privada do jurisdicionado, violando os dados que lhe compete proteger e extrapolando o seu dever de transparência.

Diante disso, a privacidade não se presta a atuar como forma de fuga, escapismo ou negação das novidades tecnológicas (que são, diga-se de passagem, inevitáveis e até necessárias, diante da multiplicação de demandas próprias de uma sociedade plural, exigentes de respostas cada vez mais rápidas e eficazes). Pelo contrário, a privacidade, nas palavras de Rodotá (2008, p. 275-6) opera como uma verdadeira "[...] pré-condição para o pleno exercício das liberdades e dos direitos. Repetimos mais uma vez: como um elemento precioso da liberdade e da cidadania".

O processo eletrônico, portanto, fortalece-se enquanto instrumento democrático na medida em que existe o respeito às liberdades individuais do jurisdicionado, algo que deve permear a atuação de todos os operadores do direito, sejam procuradores, juízes e serventuários. O dever de transparência da administração pública encontra sua limitação no direito à privacidade, e esse respeito revigora o sistema como um todo, que não pode ser compreendido

como um elemento isolado.

A informatização judicial no Brasil foi um processo histórico que teve início pela edição da Lei nº 11.419/2006, que regulamenta o uso de instrumentos eletrônicos na tramitação de processos judiciais, comunicação de atos e transmissão de documentos processuais, aplicando-se de maneira indistinta aos processos civil, penal e trabalhista, bem como aos juizados especiais, nos termos de seu artigo 1º, *caput* e parágrafo 1º (BRASIL, 2006).

A lei limitava, em seu artigo 11, parágrafo 6º, o acesso aos documentos digitalizados juntados em processo eletrônico às partes, seus procuradores e ao Ministério Público, com exceção das situações de sigilo e segredo de justiça (BRASIL, 2006). O recente advento da Lei nº 13.793, de 3 de janeiro 2019, modificou a redação do parágrafo, incluindo a prerrogativa de acesso aos advogados que não contam com procuração nos autos (BRASIL, 2019a). A restrição de acesso aos autos imposta pela lei evidencia um respeito ao direito à intimidade do jurisdicionado (CLEMENTINO, 2012, p. 98), ainda que a norma dirija-se à íntegra dos processos, o que inclui as petições e documentos protocolados pelas partes, mas não às decisões e acórdãos, que também contém dados pessoais e são livremente publicizados.

Além disso, o artigo 12, parágrafo 1º da Lei nº 11.419/2006 demonstra uma preocupação com relação à proteção dos autos dos processos eletrônicos, o que deve ser feito por meio de sistemas de segurança de acesso e armazenamento em meio que garanta a preservação e integridade dos dados (BRASIL, 2006). O mesmo cuidado não é oferecido à segurança e confidencialidade de dados que são transmitidos por meio da publicação de informações processuais e replicados por sistemas de busca na *Internet*, conhecidos como robôs (tais como o próprio *Google*), que vasculham a rede à procura de termos específicos (ALMEIDA FILHO, 2011, p. 226), questão que não foi contemplada pela lei.

A adesão oficial da Justiça do Trabalho ao Processo Judicial Eletrônico (PJe) ocorreu em 29 de março de 2010, através da celebração do Termo de Acordo de Cooperação Técnica nº 51/2010 entre o Conselho Nacional de Justiça (CNJ), o Tribunal Superior do Trabalho (TST) e o Conselho Superior da Justiça do Trabalho (CSJT). O acordo de Cooperação Técnica nº 01/2010, assinado na mesma data pelo Tribunal Superior do Trabalho, o Conselho Superior da Justiça do Trabalho e os vinte e quatro Tribunais Regionais do Trabalho selou a participação de todos os órgãos da Justiça do Trabalho no projeto (BRASIL, 2019d).

O sistema adotado pelo Poder Judiciário brasileiro para a divulgação de dados processuais eletrônicos na *Internet* foi regulamentado pela Resolução nº 121 do Conselho Nacional de Justiça (CNJ), de 5 de outubro de 2010. A norma reforça, em seus "Considerandos", a adoção do princípio da publicidade como garantia da prestação de contas

da atividade jurisdicional, ancorando-se no princípio da transparência e no direito de acesso à informação, o que deve observar a preservação do direito à intimidade, à vida privada, à honra e à imagem das pessoas (CONSELHO..., 2010).

O quinto "Considerando" que embasa o documento reconhece expressamente a estigmatização das partes pela disponibilização na *Internet* de dados relacionados aos processos judiciais criminais, cíveis e trabalhistas em que figuraram como partes (CONSELHO..., 2010). Por conta disso, em 30 de novembro de 2011, o CNJ editou a Resolução nº 143 (CONSELHO..., 2011), que alterou o artigo 4º da Resolução nº 121/2010[12] no sentido de restringir as consultas processuais trabalhistas ao número do processo, ao nome do advogado ou ao seu registro na Ordem dos Advogados do Brasil.

Vale ressaltar que o artigo 2º da Resolução nº 121 do CNJ classifica como dados básicos de livre acesso aqueles relacionados ao número, classe e assuntos do processo; nome das partes e de seus advogados; movimentação processual; e inteiro teor das decisões, sentenças, votos e acórdãos (CONSELHO..., 2010). Todos esses dados serão disponibilizados na *Internet* e estarão acessíveis a toda e qualquer pessoa, independentemente de prévio cadastramento ou de demonstração de interesse, por força do artigo 1º, com exceção dos processos que tramitam em sigilo ou segredo de justiça[13] (parágrafo único) (CONSELHO..., 2010), ainda que, nas ações ajuizadas na Justiça do Trabalho, a consulta processual possa ter critérios de busca mais

---

[12] "Art. 4.º As consultas públicas dos sistemas de tramitação e acompanhamento processual dos Tribunais e Conselhos, disponíveis na rede mundial de computadores, devem permitir a localização e identificação dos dados básicos de processo judicial segundo os seguintes critérios: (Redação dada pela Resolução nº 143, de 30.11.2011)
I – número atual ou anteriores, inclusive em outro juízo ou instâncias;
II – nomes das partes;
III – número de cadastro das partes no cadastro de contribuintes do Ministério da Fazenda;
IV – nomes dos advogados;
V – registro junto à Ordem dos Advogados do Brasil.
§ 1º. A consulta ficará restrita às seguintes situações: (Redação dada pela Resolução nº 143, de 30.11.2011)
I - ao inciso I da cabeça deste artigo, nos processo (sic) criminais, após o trânsito em julgado da decisão absolutória, da extinção da punibilidade ou do cumprimento da pena; (Redação dada pela Resolução nº 143, de 30.11.2011)
II - aos incisos I, IV e V da cabeça deste artigo, nos processo sujeitos à apreciação da Justiça do Trabalho. (Redação dada pela Resolução nº 143, de 30.11.2011)
§ 2º. Os nomes das vítimas não se incluem nos dados básicos dos processos criminais" (CONSELHO..., 2010).

[13] Segundo o artigo 189 do Código de Processo Civil: "Os atos processuais são públicos, todavia tramitam em segredo de justiça os processos:
I - em que o exija o interesse público ou social;
II - que versem sobre casamento, separação de corpos, divórcio, separação, união estável, filiação, alimentos e guarda de crianças e adolescentes;
III - em que constem dados protegidos pelo direito constitucional à intimidade;
IV - que versem sobre arbitragem, inclusive sobre cumprimento de carta arbitral, desde que a confidencialidade estipulada na arbitragem seja comprovada perante o juízo.
§ 1º O direito de consultar os autos de processo que tramite em segredo de justiça e de pedir certidões de seus atos é restrito às partes e aos seus procuradores.
§ 2º O terceiro que demonstrar interesse jurídico pode requerer ao juiz certidão do dispositivo da sentença, bem como de inventário e de partilha resultantes de divórcio ou separação" (BRASIL, 2015).

restritos.

Os parâmetros para a implementação e o funcionamento do Sistema Processo Judicial Eletrônico (PJe) na Justiça do Trabalho foram estabelecidos pela Resolução nº 94/2012 do Conselho Superior da Justiça do Trabalho (CONSELHO..., 2012). Dois anos depois, a diretriz foi revogada por meio da edição da Resolução nº 136/2014 (CONSELHO..., 2014a), com o intuito de adequação à Resolução nº 185/2013, do CNJ (CONSELHO..., 2013), que apresentava maior flexibilidade com relação ao cronograma de instalação do PJe-JT (BRASIL, 2019d).

Os preceitos definidos pelo artigo 27 da Resolução nº 185/2013 do CNJ indicam que a consulta ao inteiro teor dos documentos do PJe somente serão disponibilizados via *Internet*, estando acessíveis para as respectivas partes, advogados em geral, Ministério Público e para os magistrados, podendo, ainda, serem visualizados nas Secretarias das Varas do Trabalho, com exceção daqueles que tramitam em segredo de justiça. Em todos esses casos, com exceção da hipótese de visualização em secretaria, exige-se o credenciamento no sistema (CONSELHO..., 2013).

Em 24 de junho de 2014, o Conselho Superior da Justiça do Trabalho editou a Resolução nº 139 (CONSELHO..., 2014b), determinando a adoção de medidas mínimas pelos Tribunais Regionais do Trabalho a fim de mitigar o acesso automatizado a dados dos reclamantes constantes dos processos judiciais no âmbito do Poder Judiciário trabalhista para fins de elaboração das "listas sujas" (artigo 1°, caput). As medidas, indicadas no anexo da resolução, direcionam-se a uma tentativa de evitar o rastreamento e indexação de conteúdos por serviços de busca, bem como inibir a captura de dados por meio de consultas públicas.

Entretanto, ainda que os *sites* dos Tribunais Regionais do Trabalho possam ter sido adequados após a Resolução nº 139/2014[14], atualmente, uma pesquisa rápida pelo nome da pessoa em buscadores na *Internet* pode facilmente revelar informações sobre a existência de processos judiciais trabalhistas, permitindo o acesso ao número do processo, nomes das partes, informações sobre a tramitação e até reproduções das decisões judiciais, afrontando diretamente os direitos fundamentais do trabalhador.

Em 2017, foi editada a Resolução nº 185 do CSJT, que segue as determinações da Resolução nº 185 do CNJ e define os parâmetros para governança, infraestrutura, gestão e prática eletrônica de atos processuais do Sistema Processo Judicial Eletrônico (PJe) na Justiça do Trabalho. O documento determina que o acesso dos advogados ao PJe seja realizado através da identificação do usuário pelo seu certificado digital (artigo 5º, "caput"), e traz a possibilidade

[14] Os Tribunais Regionais do Trabalho possuíam o prazo de 180 (cento e oitenta) dias para adequação dos seus sites às orientações da Resolução nº 139/2014, conforme o artigo 1°, parágrafo 2° (CONSELHO..., 2014b).

das partes atribuírem segredo de justiça a algumas peças processuais, desde que devidamente fundamentado nas hipóteses legais (artigo 22, parágrafo 2º) (CONSELHO..., 2017).

As diretrizes que regulamentam o PJe não revelam maiores cuidados com relação ao acesso de trâmites e documentos processuais por terceiros (consulta pública), por meio do *site* dos tribunais, sem a necessidade de utilização de *login* e senha, bastando o conhecimento do número do processo pelo usuário. Ao abordar a questão da autenticidade de documentos, em seu artigo 3º, parágrafo 1º, por exemplo, a Resolução nº 185/CSJT prevê que as cópias extraídas de autos eletrônicos devem conter elementos que permitam a verificação de sua autenticidade no endereço referente à consulta pública no PJe, com acesso disponibilizado nos *sites* do Conselho Superior da Justiça do Trabalho (CSJT) e dos Tribunais Regionais do Trabalho (TRTs). Como se percebe, a proteção à privacidade e aos dados pessoais dos litigantes parece ser uma questão secundária diante da garantia de acesso a essas informações, pelo teor das normas editadas até então.

Por conta disso, em 26 de abril de 2019, foi editada pelo Conselho Nacional de Justiça a Portaria nº 63, que institui o Grupo de Trabalho com a finalidade de elaboração de estudos acerca da política de acesso às bases de dados processuais dos tribunais, com especial atenção à utilização dessas informações para fins comerciais (CONSELHO..., 2019). Um dos objetivos é a edição de uma norma para disciplinar o acesso a dados pessoais extraídos de sistemas de tribunais, tornando sigilosos trechos de processos judiciais com informações reveladoras da privacidade e da intimidade dos jurisdicionados (BRÍGIDO, 2019), o que não se concretizou até o momento. Ainda se aguardam resultados concretos resultantes das reuniões do grupo de trabalho, fato é que são necessárias medidas urgentes para disciplinar o tratamento de dados pelo Poder Judiciário, e o CNJ parece estar atento a isso.

O incremento das práticas de vigilância por meio do tratamento de dados pessoais no âmbito da justiça laboral torna-se, como visto, uma ameaça aos direitos fundamentais do trabalhador, exigindo novas formas de proteção condizentes com as demandas de uma sociedade em rede. Tamanha facilidade no acesso a esses dados impõe a necessidade de um estudo aprofundado acerca dos mecanismos jurídicos de tutela dos dados pessoais do empregado. Passa-se a examinar, na sequência da dissertação, os fundamentos da proteção jurídica de dados pessoais, mediante o estudo da evolução histórica dos direito à privacidade e à igualdade, além de um panorama geral acerca das normativas existentes na União Europeia, que serviram como paradigma à recente legislação brasileira protetiva de dados pessoais.

2 A PROTEÇÃO JURÍDICA DE DADOS PESSOAIS NO PROCESSO DO TRABALHO DA SOCIEDADE EM REDE

Os atores de uma sociedade em rede transitam em um novo espaço de comunicação virtual, desenvolvido paralelamente ao ambiente físico, cuja estrutura e amplitude transcende as fronteiras do Estado-nação. O rompimento do paradigma do tempo/espaço sequencial possibilita uma troca incessante de informações ao redor do planeta, o que gera uma série de efeitos positivos, tais como a ampliação das comodidades e a aproximação das distâncias, mas revela novas ameaças aos direitos fundamentais dos indivíduos, especialmente pelo tratamento de seus dados pessoais.

Nas relações laborais, o próprio contrato de trabalho estimula a coleta de dados do obreiro, legitimando a manipulação patronal sobre uma série de informações pessoais do empregado, tais como informações de saúde, previdenciárias e fiscais. Alguns dados pessoais sensíveis que estão ao alcance do empregador, no entanto, não possuem qualquer relação com o contrato de trabalho, trazendo violações aos direitos fundamentais do trabalhador, como é o caso das informações que integram os processos judiciais ajuizados anteriormente, e que acabam sendo divulgadas pelo Poder Público sem o seu consentimento.

A concepção de direitos fundamentais como direitos de defesa em face do Estado remonta ao modelo liberal burguês, voltado à tutela das liberdades individuais frente aos arbítrios da monarquia. Em pleno Estado democrático de Direito, com o desvelar de novos direitos emergentes de uma sociedade em rede, é necessário que se estabeleça uma teoria que reconheça também a vinculação dos particulares aos direitos fundamentais, especialmente aos direitos à privacidade e à igualdade, principais direitos do trabalhador atingidos pelo tratamento automatizado de seus dados pessoais.

O direito à privacidade, por muito tempo ligado a uma ideia de isolamento e solidão, evoluiu para um direito relacionado ao controle das informações que dizem respeito ao indivíduo, adotando nuances dinâmicas e transcendendo o paradigma individualista que o caracterizou nos primórdios do seu reconhecimento, tendo em vista que os dados pessoais são desmembrados e reagrupados de diferentes formas, exigindo uma nova forma de proteção, coerente com as exigências de uma sociedade em rede.

Ao assumir as feições de um direito à autodeterminação informativa, a privacidade passa a salvaguardar o trabalhador com relação à distribuição indevida de seus dados pessoais e a utilização para fins diversos daqueles que foram informados na coleta. Da mesma forma, o direito à igualdade, protege o trabalhador do uso discriminatório das informações que foram

disponibilizadas nos processos trabalhistas. Diante disso, encaminha-se para um estudo inicial acerca da vinculação dos particulares e do Poder Público aos direitos fundamentais, identificando como ocorre a colisão de direitos fundamentais nestas esferas e examinando a evolução histórica do direito à privacidade, de um direito a estar só à autodeterminação informativa, e de seus desmembramentos no contexto do tratamento informatizado de dados pessoais pela Justiça do Trabalho.

2.1 EFICÁCIA DO DIREITO FUNDAMENTAL À PRIVACIDADE NAS RELAÇÕES TRABALHISTAS: a autodeterminação informativa do trabalhador e seus desdobramentos.

Os direitos humanos foram construídos de acordo com a evolução representada pelos diversos contextos históricos da humanidade, acompanhando as necessidades, os interesses e as lutas de cada época. O reconhecimento dos direitos do homem, conforme Norberto Bobbio (2004, p. 25), foi ocorrendo de forma gradual, "não todos de uma vez e nem de uma vez por todas", refletindo determinados períodos históricos e as suas circunstâncias próprias, através das lutas em defesa de novas liberdades contra antigos poderes.

A concepção contemporânea de direitos humanos foi introduzida em 10 de dezembro de 1948, após as barbáries que assolaram o mundo na Segunda Guerra Mundial, com a proclamação da Declaração Universal dos Direitos Humanos (ASSEMBLEIA..., 1948) pela Assembleia Geral das Nações Unidas, reafirmando o respeito aos direitos humanos fundamentais, à dignidade e ao valor do ser humano e à igualdade de direitos entre homens e mulheres. Dentre os direitos elencados na Declaração, o respeito à vida privada foi previsto no artigo XII, que garante também a proteção contra interferência na família e no lar, o sigilo de correspondências e a tutela da honra e da reputação.

A inovação representada pela concepção contemporânea de direitos humanos diz respeito ao caráter universal e indivisível de tais direitos. Enquanto o atributo da universalidade é relacionado à extensão ampla e geral dos direitos humanos, reconhecendo-se a condição de pessoa (enquanto ser essencialmente moral e dotado de dignidade), como único requisito para a sua titularidade, a indivisibilidade deriva da composição de uma unidade indivisível e interdependente de direitos, através da conjugação do catálogo de direitos civis e políticos com os direitos sociais, econômicos e culturais (PIOVESAN, 2006, p. 13). Mesmo com todos esses atributos, na concepção de Hunt (2009, p. 19), os direitos humanos somente tornam-se significativos quando ganham conteúdo político, já que se dirigem às relações humanas em sociedade. São, portanto, "[...] direitos que requerem uma participação ativa daqueles que os

detém" (HUNT, 2009, p. 19).

A Declaração de 1948 é um dos pilares que, em conjunto com o Pacto Internacional dos Direitos Civis e Políticos (ASSEMBLEIA..., 1966a) e o Pacto Internacional dos Direitos Econômicos, Sociais e Culturais (ASSEMBLEIA..., 1966b), ambos aprovados em 1966, estruturam o sistema global de proteção dos direitos humanos, conferindo carga axiológica ao Direito Internacional dos Direitos Humanos. Esse sistema é integrado por tratados internacionais que refletem a consciência ética contemporânea global, atuando complementarmente aos sistemas regionais para compor o arcabouço protetivo dos direitos humanos no plano internacional (PIOVESAN, 2006, p. 13-4).

A fragmentação dos direitos humanos em dois grupos refletiu o contexto político e a ruptura ideológica existente entre os cinco países vencedores do conflito bélico global, confrontando ideais liberais e socialistas (LEÃO, 2001, p. 33). Resultou, portanto, de um compromisso diplomático, servindo para conciliar os interesses das potências ocidentais (que insistiam no reconhecimento das liberdades individuais clássicas, tão somente) e dos países do bloco comunista e jovens países africanos (que preferiam destacar os direitos sociais e econômicos) (COMPARATO, 2003, p. 276).

Apesar da elaboração de dois tratados distintos, que leva alguns países a privilegiarem os direitos civis e políticos em detrimento dos direitos econômicos, sociais e culturais, o caráter indivisível e interdependente dos direitos humanos é reforçado pelos preâmbulos dos dois pactos, cuja redação é semelhante, ao assegurarem que "[...] o ideal do ser humano livre, liberto do medo e da miséria não pode ser realizado a menos que sejam criadas condições que permitam a cada um desfrutar dos seus direitos econômicos, sociais e culturais, bem como dos seus direitos civis e políticos" (ASSEMBLEIA..., 1966b). Tratou-se de uma divisão artificial, evidenciada, inclusive, pelo reconhecimento de alguns direitos de forma idêntica nos dois tratados, tais como o direito à autodeterminação dos povos e o direito de sindicalização, além da própria identidade entre os preâmbulos (COMPARATO, 2003, p. 276).

Apontando uma embasada crítica a essa dissociação, por reconhecer a interdependência entre economia e direitos humanos e entender que a universalidade advém do conjunto dos direitos enunciados, e não pela prevalência de um em detrimento de outro (DELMAS-MARTY, 2003, p. 39), enquanto a dignidade humana representa o núcleo valorativo de todo e qualquer direito humano, Mireille Delmas-Marty (2003, p. 40) lembra que:

> [...] a indivisibilidade não exclui toda hierarquia entre os direitos, vez que admite limitações temporárias ou permanentes, mas esta hierarquia é, em si, transversal, vez que remete aos valores subjacentes; em suma, o direito à igual dignidade tem

> implicações às vezes civis e políticas e, ainda, econômicas, sociais e culturais, pois ela exclui a tortura e a escravidão e, mais largamente, as penas ou tratamentos cruéis, inumanos ou degradantes.

Na posição de Celso Lafer (1991, p. 129), esta divisão em dois pactos distintos pode ser explicada pela heterogeneidade jurídica que diferencia as liberdades clássicas dos direitos de crédito. Isso porque em caso de violação, os direitos civis e políticos comportam o peticionamento individual a um organismo internacional, enquanto os direitos econômicos-sociais e culturais, na condição de objetivos programáticos a serem progressivamente implementados por meio da atuação estatal, possuem maiores dificuldades de aplicação imediata. Assim, no plano internacional, estes direitos são tutelados por meio de relatórios sobre a situação de grupos ou coletividades, e não na forma de reparação individual (LAFER, 1991, p. 129).

Qualquer que seja o posicionamento adotado, indiscutível é o papel representado pela dignidade da pessoa humana na condução da concepção moderna de direitos humanos. O respeito à dignidade humana pressupõe, na visão de Kant (1997, p. 68), que todo ser racional existe como um fim em si mesmo, jamais como um meio; ou seja, o indivíduo jamais pode ser utilizado como mero instrumento para o uso arbitrário da vontade de alguém. O postulado kantiano indica que a dignidade "[...] constitui a condição só graças à qual qualquer coisa pode ser um fim em si mesma, não tem somente um valor relativo, isto é um preço, mas um valor íntimo" (KANT, 1997, p. 77).

Portanto, a compreensão contemporânea de dignidade humana, inaugurada com o pensamento clássico e cujos principais marcos são a tradição judaico-cristã, o Iluminismo e o período pós-Segunda Guerra Mundial, assenta-se em uma visão metafísica, através do pressuposto de existência de um valor intrínseco em cada ser humano, que ocupa posição destacada no universo (BARROSO, 2013, p. 13-4). O seu respeito deve existir sempre, em todos os lugares e de forma igualitária a todos os indivíduos, de tal maneira que o crescimento econômico e material que for conseguido às custas de ofensas à dignidade humana terá valor negativo, não sendo merecedor de respeito (DALLARI, 2004, p. 15).

A proteção da dignidade, enquanto valor intrínseco ao ser humano, constitui-se em objetivo a ser perseguido pelos Estados na busca da concretização dos direitos humanos, de acordo com as concepções existentes nos diversos períodos históricos da humanidade. Reconhecendo a importância da dignidade humana na gênese da moderna teoria dos direitos do homem, Pérez Luño (2005, p. 50) define os direitos humanos como "un conjunto de facultades e instituciones que, en cada momento histórico, concretan las exigencias de la dignidad, la

libertad y la igualdad humana, las cuales deben ser reconocidas positivamente por los ordenamientos jurídicos a nível nacional e internacional".

Entretanto, deve-se atentar para a distinção existente entre as expressões "direitos humanos" e "direitos fundamentais". Os direitos humanos, conforme leciona Ingo Sarlet (2001, p. 33), possuem caráter supranacional e validade universal, referindo-se àquelas posições jurídicas que são reconhecidas ao ser humano como tal, independente da vinculação com determinada ordem constitucional (relacionam-se aos documentos de direito internacional). Os direitos fundamentais, por sua vez, aplicam-se aos direitos do ser humano que são reconhecidos e positivados no âmbito do direito constitucional positivo de um Estado em específico.

Certamente existem grandes aproximações entre os conceitos de "direitos humanos" e "direitos fundamentais", e não apenas pelo fato de que os direitos fundamentais, em alguma medida, são sempre direitos humanos (ainda que representado por um ente coletivo, o titular do direito, ao cabo, será um ser humano), mas também porque grande parte das Constituições que vieram após a Segunda Grande Guerra inspiraram-se na Declaração Universal dos Direitos Humanos de 1948, bem como nos documentos internacionais que a seguiram (SARLET, 2001, p. 33-5).

Os direitos fundamentais sofreram diversas transformações ao longo da história, acompanhando a própria evolução do Estado, desde o seu reconhecimento nas primeiras Constituições liberais até o modelo de Estado Democrático de Direito. Diante de tal evolução histórica, a doutrina costuma falar da existência de três, quatro ou até mesmo cinco gerações[15] de direitos fundamentais progressivos. Este trabalho, entretanto, filia-se à concepção de Ingo Sarlet (2001, p. 49), que utiliza a expressão "dimensões de direitos fundamentais", por entender que o termo "gerações" causa a impressão errônea de que há a substituição gradativa de uma geração por outra ao longo do tempo, quando na verdade, há uma coexistência de direitos fundamentais em diferentes esferas.

Observa-se que a dignidade humana, na condição de valor e princípio, pressupõe e exige que sejam reconhecidos e respeitados os direitos fundamentais de todas as dimensões identificadas, na medida em que a negação aos direitos fundamentais inerentes à pessoa representa a negação de sua própria dignidade (SARLET, 2015, p. 125). A dignidade, portanto, além de vetor a orientar a aplicação de todos os direitos fundamentais, está presente, direta ou indiretamente, no âmago de cada um desses direitos.

[15] Vide Bonavides (2012, p. 598) e Wolkmer (2012, p. 29).

Os direitos fundamentais, criação originária do Estado Liberal, surgiram da necessidade de impor limitações ao poder do Estado, de forma a garantir à burguesia emergente a liberdade, a propriedade individual, a igualdade e segurança jurídica, valores ligados a uma concepção racional própria da sociedade capitalista emergente. Substituía-se o antigo modelo estatal absolutista, calcado em um poder de origem divina atribuído à figura do soberano, por um modelo liberal-racionalista, em busca da almejada segurança que seria proporcionada pela Constituição e pela separação dos poderes.

O modelo liberal de Estado surgiu com a ascensão burguesa, no final do século XVIII, que não mais contentou-se em ser detentora apenas do poder econômico e passou a querer para si o poder político, limitando os poderes da monarquia. Para isso, sustentou-se em uma Constituição como expressão jurídica do acordo político que dá origem ao Estado (BOLZAN DE MORAIS; STRECK, 2006, p. 51).

Assim, os direitos fundamentais foram concebidos como invenção do constitucionalismo liberal, estabelecendo-se como limites ao poder estatal, representado pela figura do soberano. Restringiam-se, portanto, à relação indivíduo-Estado, de forma a salvaguardar o burguês dos abusos (arbitrariedades) provenientes do monarca (STEINMETZ, 2004, p. 64). Essa preocupação foi levada às constituições liberais, através da consagração dos direitos fundamentais de primeira dimensão, liberdades individuais que garantiam a defesa do indivíduo em face do poderio do Estado.

Juntamente com a separação dos poderes, o reconhecimento dos direitos fundamentais é um dos pilares estruturantes das declarações de direito e das constituições liberais. O constitucionalismo liberal desenvolveu-se, portanto, através de constituições escritas que consolidaram a ascensão da burguesia liberal, constituindo-se em um mecanismo de garantia das liberdades burguesas (STEINMETZ, 2004, p. 67). A respeito das constituições liberais, Canotilho (2003, p. 110) afirma que elas:

> [...] costumavam ser consideradas como «códigos individualistas» exaltantes dos direitos individuais do homem. A noção de indivíduo, elevado à posição de sujeito unificador de uma nova sociedade, manifesta-se fundamentalmente de duas maneiras: (1) a primeira acentua o desenvolvimento do sujeito moral e intelectual livre; (2) a segunda parte do desenvolvimento do sujeito econômico livre no meio da livre concorrência.

Os direitos fundamentais de primeira dimensão, assim entendidos os direitos à vida, à liberdade, à propriedade e à igualdade perante a lei, próprios dessa fase do constitucionalismo liberal, são direitos de cunho negativo, ou seja, direitos de defesa os quais exigem do Estado

uma abstenção, demarcando uma zona de não-intervenção do estado e delimitando o campo da autonomia individual em face da atuação estatal (SARLET, 2001, p. 50). Reconhecendo-se a relação vertical de poder existente entre o Estado e o indivíduo, o ordenamento jurídico impõe uma limitação à atuação dos governantes em relação aos governados, o que a doutrina costuma denominar de eficácia vertical dos direitos fundamentais (LEITE, 2011, p. 34).

Entretanto, em pleno Estado Democrático de Direito, diante do surgimento de megagrupos industriais, comerciais, financeiros e midiáticos, que rivalizam, em alguns aspectos, com o poder do Estado, o Estado deixa de ser o único a condicionar, restringir ou eliminar as liberdades individuais (STEINMETZ, 2004, p. 87-8). No âmbito da sociedade da informação, esse conflito toma uma proporção relevante, na medida em que grandes grupos multimídia constantemente apropriam-se de dados pessoais para fins obscuros, violando direitos fundamentais constitucionalmente assegurados.

Nesse contexto, conforme leciona Limberger (2007, p. 39), os conflitos deslocaram-se da esfera Estado x cidadão para o âmbito das relações grupo x indivíduo, fazendo-se necessário o reconhecimento da vinculação dos particulares aos direitos fundamentais, ou a "eficácia dos direitos fundamentais nas relações entre particulares", também conhecida por "eficácia horizontal dos direitos fundamentais"[16].

Vale destacar que alguns autores, dentre eles Bilbao Ubillos (2006, p. 304) e Têmis Limberger (2007, p. 39), criticam a terminologia "eficácia horizontal" por entender que, mesmo nas relações privadas, existem situações na qual se configura igualmente uma relação assimétrica, de forma que não se poderia falar em uma horizontalidade, tais como as relações de emprego e de consumo. Trata-se de um evidente acerto dos doutrinadores, especialmente no que diz respeito às relações trabalhistas e a vulnerabilidade do empregado diante do seu acentuado caráter de dependência. Por conta disso, este trabalho filia-se a esta posição, evitando o uso da expressão "eficácia horizontal dos direitos fundamentais", ainda que reconheça a existência de opiniões divergentes, tais como Steinmetz (2004, p. 58), que defende a sua utilização como sinônima das demais terminologias referentes à vinculação dos particulares a direitos fundamentais.

A respeito da extensão com que as normas de direitos fundamentais produzem efeitos na relação cidadão/cidadão, Robert Alexy (2008, p. 529) faz a distinção acerca de três teorias

[16] Pode-se citar, ainda, o uso das expressões "eficácia frente a terceiros", "eficácia externa", "eficácia social", "eficácia privada" (STEINMETZ, 2004, p. 53-4), bem como a expressão alemã "drittwirkung" (LIMBERGER, 2007, p. 39 e STEINMETZ, 2004, p. 31)

existentes[17]: a teoria dos efeitos indiretos perante terceiros, a teoria dos efeitos diretos e a teoria dos efeitos mediados por direitos em face do Estado.

De acordo com a teoria dos efeitos indiretos perante terceiros, ou teoria da eficácia mediata ou indireta (*mittelbare Drittwirkung*), conforme refere André Rufino do Vale (2004, p. 140), os direitos fundamentais, enquanto valores constitucionais, entranham-se no direito privado por meio de cláusulas gerais, a serem interpretadas conforme os ditames da própria legislação civil. Os direitos fundamentais, sendo assim, poderiam servir como princípios interpretativos das cláusulas gerais, sempre dentro do "espírito" do direito privado.

Para a teoria da eficácia mediata, os direitos fundamentais não ingressam no âmbito privado como direitos subjetivos, invocáveis a partir da Constituição, mas sim por meio dos próprios mecanismos do direito privado (SARMENTO; GOMES, 2011, p. 66-8). Alexy (2008, p. 529) refere, com relação a esta teoria, que os direitos fundamentais seriam dotados de um efeito irradiador que "deve fundamentar o dever de levar em consideração a influência dos direitos fundamentais nas normas de direito privado, quando de sua interpretação". Nesse sentido, Virgílio Afonso da Silva (2005, p. 84) afirma que os direitos fundamentais, enquanto sistema de valores, infiltrariam-se no direito privado por meio das cláusulas gerais.

A teoria dos efeitos diretos perante terceiros, ou teoria da eficácia imediata ou direta (*unmittelbare Drittwirkung*) defende a aplicabilidade direta dos direitos fundamentais nas relações privadas, sem a necessidade de nenhuma ação intermediária a fim de serem concretizados nas relações entre particulares (SILVA, V. A., 2005, p. 86). Bilbao Ubillos (2006, p. 318) afirma que a teoria da eficácia imediata "implica que, con normativa legal de desarrollo o sin ella, es la norma constitucional la que se aplica como "razón primaria y justificadora" (no necesariamente la única) de uma determinada decisión".

De acordo com Alexy (2008, p. 530), as normas de direitos fundamentais possuem um caráter objetivo e vinculante, produzindo, conforme a teoria da eficácia imediata, efeitos na relação cidadão/cidadão porque deles flui diretamente direitos subjetivos privados que vinculam os indivíduos (ao contrário da teoria da eficácia mediata, em que o efeito é decorrente de uma interpretação das normas de direito privado).

Por fim, a teoria dos efeitos mediados por direitos em face do Estado[18] ou eficácia produzida por direitos frente ao Estado ou, ainda, teoria dos deveres de proteção do Estado em

[17] Além das três teorias aqui apresentadas, merecem referência também a doutrina norte-americana do *State Action* (STEINMETZ, 2004, p. 178 e SARMENTO; GOMES, 2011, p. 63) e a teoria integradora proposta por Alexy (2008, p. 533).

[18] Alexy (2008, p. 530) refere a existência de uma versão extrema dessa teoria, proposta por Schwabe (teoria da imputação ao Estado), também citada por Steinmetz (2004, p. 175), segundo a qual o Estado, na medida em que

relação aos direitos fundamentais, traz a ideia de que os direitos fundamentais vinculam diretamente apenas o poder público, e não os sujeitos de direito privado, cabendo ao Estado a proteção dos direitos fundamentais do indivíduo ameaçado por outros particulares (SARMENTO; GOMES, 2011, p. 75). Portanto, o poder público, além da dimensão negativa, de abstenção, e do dever de criar as condições para a concretização dos direitos fundamentais, possuiria a obrigação de proteger os indivíduos de violações entre si (VALE, 2004, p. 150-1).

Steinmetz (2004, p. 151-2) sustenta que, segundo a teoria dos direitos fundamentais como direitos à proteção, caberia ao poder estatal (Poder Legislativo, em um primeiro momento, e Poder Judiciário, de forma subsidiária) a proteção dos direitos fundamentais das violações provocadas por outros particulares, figurando como sujeito passivo e intervindo de forma excepcional e justificada, na medida em que ocorram violações unilaterais e recíprocas entre os particulares.

O reconhecimento de uma aplicabilidade direta dos direitos fundamentais parece ser a perspectiva mais adequada diante da posição que é adotada pela Constituição da República Federativa do Brasil, ao expressar, em seu artigo 5°, parágrafo 1°, que "as normas definidoras dos direitos e garantias fundamentais têm aplicação imediata" (BRASIL, 1988). Além disso, ao elencar um rol de direitos sociais, a Carta Magna oferece uma outra indicação da vinculação imediata dos particulares aos direitos fundamentais, uma vez que tais direitos possuem não apenas um caráter prestacional por parte do Estado, mas também denotam garantias que atingem o âmbito das relações entre particulares, especialmente as normas relacionadas ao contrato de trabalho, exigindo do Estado apenas o controle da sua efetividade.

A par da existência das teorias anteriormente referidas, Barroso (2010, p. 372) defende a aplicabilidade direta e imediata dos direitos fundamentais no contexto brasileiro, através de um critério de ponderação entre os princípios constitucionais e/ou direitos fundamentais, devendo ser levados em conta elementos do caso concreto. No mesmo sentido, Ingo Sarlet (2001, p. 241) sustenta a aplicabilidade imediata de todos os direitos fundamentais constantes no Catálogo constitucional (artigos 5° a 17), bem como os localizados em outras partes da Constituição Federal e nos tratados internacionais, amparado pelo artigo 5°, parágrafo 1°, da Carta Magna.

Esse também parece ser o entendimento do Supremo Tribunal Federal brasileiro, conforme se observa no julgamento paradigmático do Recurso Extraordinário número 201.819-8 (BRASIL, 2005). Na ocasião, o STF reconheceu a eficácia imediata dos direitos fundamentais

---

cria e impões um sistema de direito privado, seria ele próprio responsável pelas violações a direitos fundamentais ocorridas entre particulares, uma vez que resultante de uma permissão estatal ou de uma não-proibição estatal.

em controvérsia envolvendo a exclusão de um sócio de uma entidade privada (a União Brasileira de Compositores), sem terem sido oportunizadas as garantias do contraditório e da ampla defesa.

Partindo do reconhecimento da vinculação dos particulares aos direitos fundamentais, observa-se que estes direitos não são absolutos e ilimitados. Algumas peculiaridades que diferenciam as relações entre indivíduo e Estado das relações estritamente particulares devem ser analisadas, uma vez que, diferentemente do que ocorre na relação Estado-particular, na relação entre particulares ambas as partes são detentoras de direitos fundamentais, conforme lembra Virgílio Afonso da Silva (2005, p. 18), configurando a colisão de direitos fundamentais. Tal colisão se manifesta "[...] quando, *in concreto*, o exercício de um direito fundamental por um titular obstaculiza, afeta ou restringe o exercício de um direito fundamental de outro titular, podendo tratar-se de direitos idênticos ou de direitos diferentes [...]" (STEINMETZ, 2001, p. 139).

Algumas características próprias do contrato de trabalho demonstram a necessidade de atuação dos direitos fundamentais no âmbito das relações trabalhistas, especialmente a relação de dependência existente entre empregador e empregado, que cede sua força de trabalho em prol de uma atividade cujo proveito não reverte diretamente em seu benefício, sofrendo limitações em sua liberdade (AMARAL, 2014, p. 100). Nesse contexto, a vigilância eletrônica no âmbito laboral materializa a colisão entre direitos fundamentais do empregado e o direito à propriedade do empregador, exercido através do seu poder de direção[19].

A coleta e o processamento de dados pessoais do trabalhador, principalmente na fase pré-contratual, quando o contratante busca referências para a admissão do funcionário, pode representar a materialização desta colisão de direitos fundamentais: de um lado o empregador, com a necessidade da informação sobre aspectos relevantes para a formação de seu convencimento acerca da contratação, e do outro, o obreiro, dispondo de aspectos de sua privacidade, na medida em que presta informações de cunho pessoal. Entretanto, importa salientar que o exercício do direito de informação do empregador é limitado pelos princípios da

[19] Apesar da ressalva de que, atualmente, em inúmeros estabelecimentos e empresas, o poder diretivo não é exercido pelo mesmo titular do direito de propriedade. Dessa forma, além da teoria da propriedade privada, outras correntes explicam o poder de direção do empregador, conforme leciona Delgado (2013, p. 672): a teoria institucionalista, segundo a qual o poder diretivo decorre do fato de o empregado estar inserido na instituição (empresa), que possui estrutura hierarquizada, e assim fundamenta o direito de punir disciplinarmente pela própria necessidade de direção da empresa para a sua finalidade econômico-social; a teoria publicística, que concebe o poder diretivo como uma delegação do poder público; e a teoria contratualista, com o fundamento de que o poder diretivo decorre do contrato de trabalho, onde o empregado submete-se à vontade do empregador, conforme livremente pactuado.

boa-fé e da não discriminação, já que o tratamento de dados não se presta ao objetivo segregacional.

No campo processual, sob o enfoque da atuação do Poder Público, a discriminação do empregado que demandou judicialmente por seus direitos, em virtude da divulgação de informações judiciais pelos mecanismos de busca na Internet e/ou pelos próprios *sites* dos tribunais, materializa a colisão de direitos fundamentais sob outro aspecto: os direitos à privacidade e à igualdade do empregado colidem com o direito à informação, o princípio da publicidade e o dever de transparência da Administração Pública. A esse respeito, Limberger e Ruaro (2011, p. 126) pensam que o desafio se estabelece "na busca do equilíbrio entre o dever de informar, o conteúdo da informação e o direito à proteção de dados", balizamento que deverá ser realizado à luz dos princípios e normas atinentes à proteção de dados no ordenamento jurídico nacional, conforme observam Doneda e Monteiro (2015):

> Assim, o estabelecimento de limitações para o dever geral de transparência do poder público é resultado da consideração de outros direitos e interesses que, eventualmente, possam se chocar com o princípio da transparência. Casos em que a privacidade, a dignidade ou a isonomia de cidadãos estejam em jogo são exemplos de fundamentos destas exceções, que costumam ser feitas a partir da consideração de normas específicas de proteção de dados pessoais, nos países que possuem normativas deste gênero, ou da consideração de outras normas e princípios presentes no ordenamento jurídico.

Como proposta metodológica para a solução do conflito entre direitos fundamentais, a doutrina costuma apontar a ponderação de bens, operacionalizada por meio da aplicação do princípio da proporcionalidade, método que é adotado por Steinmetz (2001, p. 143). Este princípio se manifesta sob três máximas parciais: a adequação, a necessidade e a proporcionalidade em sentido estrito. As máximas da necessidade e da adequação são decorrentes da natureza dos princípios como mandamentos de otimização diante das possibilidades fáticas existentes, enquanto a máxima da proporcionalidade em sentido estrito, ou seja, a exigência de um sopesamento no caso concreto, decorre do fato de que os princípios são mandamentos de otimização face às possibilidades jurídicas (ALEXY, 2008, p. 117-8).

Em linhas gerais, o princípio da adequação (ou da conformidade) ordena que se verifique se a medida restritiva do direito fundamental é apta para alcançar a finalidade pretendida; o princípio da necessidade (ou da intervenção mínima) questiona acerca da existência ou não de outra medida igualmente adequada e eficaz, mas menos prejudicial ao direito fundamental em questão; enquanto a proporcionalidade em sentido estrito é a ponderação de bens propriamente dita, examinando a relação de proporcionalidade entre a

decisão normativa e a finalidade perseguida (STEINMETZ, 2001, p. 149-153).

Ainda que reconheça tratarem-se de princípios autônomos, Steinmetz (2001, p. 186) lembra que existe uma visível tendência doutrinária no Brasil que trata os princípios da proporcionalidade e da razoabilidade como equivalentes, ou identifica entre eles uma relação de inclusão (um estaria incluso no outro). A tese da equivalência deve ser refutada, optando-se pela proporcionalidade como critério para a solução da colisão de direitos fundamentais, uma vez que o conflito é estruturado através de uma relação de meio-fim, não sendo o caso de verificar a razoabilidade da aplicação de uma norma geral a uma situação específica. Além disso, somente a proporcionalidade apresenta indicadores concretos mediante a aplicação das três máximas anteriormente referidas: a adequação, a exigibilidade e a proporcionalidade em sentido estrito (STEINMETZ, 2001, p. 187-192).

Ainda que a razoabilidade não seja o critério mais apropriado para o conflito de direitos fundamentais, sua aplicação é indispensável na seara laboral, sendo definida por Plá Rodriguez (1996, p. 251) como a "[...] afirmação essencial de que o ser humano, em suas relações trabalhistas, procede e deve proceder conforme a razão". Assim, este princípio figura como espécie de contrapeso ao princípio da proteção (CAMINO, 1999, p. 61), estabelecendo-se como ponto de equilíbrio que pode ser invocado como critério de orientação para as questões atinentes ao contrato de trabalho e às relações entre empregado e empregador.

Portanto, qualquer restrição a um direito fundamental do empregado somente poderá ser considerada válida se for compatível com o princípio da proporcionalidade em seus três desdobramentos: deve ao menos contribuir para a promoção de interesse legítimo do trabalhador (adequação), deve ser o meio mais suave para a promoção daquele interesse, mantendo a mesma intensidade (necessidade), sendo que a promoção do objetivo buscado pelo empregador não pode demandar sacrifício superior ao direito do obreiro (proporcionalidade em sentido estrito) (SARMENTO, 2011, p. 96). Todos esses subprincípios serão utilizados, cumulativamente, como critério de verificação pelo Poder Judiciário trabalhista, a fim de verificar se há proporcionalidade entre a medida utilizada e a finalidade pretendida.

Essa harmonização entre os direitos fundamentais conflitantes mostra significativa relevância quando se observa o contexto de uma sociedade em rede, cuja fronteira entre público e privado não apresenta contornos bem definidos e a informação passa a ter mais valor do que a própria vida privada dos envolvidos. A evolução das relações sociais exige que o próprio direito sofra mutações, desvelando novas roupagens mais adequadas aos tempos contemporâneos, como é o caso das mutações sofridas pelo direito à privacidade.

O tratamento automatizado de dados pessoais impõe um necessário rompimento com um paradigma defasado, amparado em uma noção estática de privacidade que não mais atende às demandas dos novos tempos. O reconhecimento de um direito autônomo à proteção de dados pessoais implica na identificação de seus diversos desmembramentos, especialmente nas relações laborais, em que o uso discriminatório das informações do empregado evidencia que a privacidade não é o seu único direito impactado, mas também o direito à igualdade. A evolução de ambos os direitos merece ser analisada com maior atenção.

O marco inicial de reconhecimento de um direito à privacidade costuma ser associado doutrinariamente ao artigo de autoria de Samuel Warren e Louis Brandeis, intitulado "*The Right to Privacy*" (WARREN; BRANDEIS, 1890), publicado em 15 de dezembro de 1890 pela Revista *Harvard Law Review*. Partindo dos direitos à liberdade e à propriedade, os autores formularam uma construção teórica que definiu a privacidade como sendo a "faculdade de se determinar ordinariamente em que medida seus pensamentos, sentimentos e emoções devem ser comunicados a outrem", dissociando-o da esfera da propriedade privada.

Este modelo de privacidade, de cunho individualista, até mesmo egoísta, remete ao paradigma do *zero-relationship*, como isolamento do indivíduo com relação aos demais (DONEDA, 2006, p. 8-9). A partir do final do Século XIX, entretanto, o direito à privacidade passa a desvincular-se da concepção liberal que caracterizam os direitos fundamentais de primeira dimensão, deixando de ser considerado um bem de pleno domínio do indivíduo, de cunho patrimonial, para começar a ser considerado um direito de personalidade. O direito à privacidade[20] torna-se uma manifestação do direito à liberdade, consistindo em espécie de direito humano fundamental da personalidade que visa à proteção da dignidade humana (BARBOSA JUNIOR, 2008, p. 62).

Assim, Sarlet (2015, p. 130) defende o reconhecimento da dignidade humana como necessário para que se possa admitir um direito ao livre desenvolvimento da personalidade, concretizado, dentre outras dimensões, pela privacidade. Os direitos de personalidade, no ensinamento de Bittar (2001, p. 1) são aqueles "reconhecidos à pessoa humana tomada em si mesma e em suas projeções na sociedade, previstos no ordenamento jurídico exatamente para a defesa de valores inatos ao homem [...]", dentre os quais se encontra a intimidade. O autor (2001, p. 107) identifica que o direito à intimidade vem assumindo, de forma gradativa, maior

[20] Em face da diversa gama de expressões utilizada pela doutrina para representar a privacidade, tais como vida privada, intimidade, segredo, sigilo, recato, reserva, intimidade da vida privada (DONEDA, 2006, p. 101), este trabalho seguirá a posição defendida por Danilo Doneda (2006, p. 111-2), utilizando a terminologia "privacidade" como conceito amplo e adequado ao contexto das novas tecnologias informacionais, abrangendo os valores expressos pelos termos intimidade e vida privada.

importância em virtude da contínua expansão das técnicas de comunicação e do desenvolvimento tecnológico.

O Brasil consagrou expressamente os direitos à intimidade e à vida privada através da Constituição da República de 1988 (BRASIL, 1988), em seu artigo 5°, X, sendo que a dignidade da pessoa humana é um princípio fundamental elencado com destaque no artigo 1º, III, que cumpre uma "função hermenêutica", constituindo-se em parâmetro de aplicação, interpretação e integração não só dos direitos fundamentais, mas de todo o ordenamento jurídico (SARLET, 2015, p. 103). No âmbito infraconstitucional, os direitos de personalidade foram inseridos no Capítulo II do Código Civil brasileiro (BRASIL, 2002), dentre os quais a inviolabilidade da vida privada é uma garantia do artigo 21.

Ressalta-se que o legislador brasileiro não fez uso do termo "privacidade", optando pelas expressões "vida privada" e "intimidade", para tratar de diferentes aspectos da privacidade, tendo em vista que a doutrina pátria[21] costuma referir-se à vida privada como um conceito mais amplo, que envolve a convivência familiar e as relações sociais próximas, enquanto a intimidade denotaria uma esfera de âmbito mais reservado. Com isso, coaduna-se à doutrina alemã das esferas concêntricas, de Hubmann, referida por Doneda (2006, p. 108), que representa os diversos graus de manifestação da privacidade através da ideia de círculos que se sobrepõem: a esfera da intimidade (ou do segredo) é a camada mais interna, a esfera privada a camada intermediária, e a esfera pessoal (que abrangeria a vida pública) é a camada externa, revestindo as demais.

Entretanto, o advento das Tecnologias da Informação e da Comunicação (TIC) e a evolução do paradigma informacional trouxeram significativas mudanças à caracterização da privacidade na sociedade em rede, levando Pérez Luño (2012, p. 115) a defender uma "metamorfose da intimidade", que se manifesta através de um duplo deslocamento: 1) ultrapassando a esfera da solidão e do isolamento e atingindo a esfera social e coletiva; e 2) transcendendo a condição de integrante de direito da personalidade à orbita do direito patrimonial. Os tradicionais atributos próprios dos direitos de personalidade, quais sejam, inviolabilidade, irrenunciabilidade, e inalienabilidade, teriam sido mitigados diante da conversão da intimidade em mercadoria, sujeita aos modismos e às leis do mercado e podendo ser objeto das mais diversas violações consentidas. Sua condição de direito de personalidade

[21] Para Marcelo Pereira (2005, p. 111-5), a intimidade representa o núcleo mais íntimo, o mais interior da pessoa, seus pensamentos, ideias e emoções, enquanto a vida privada seria tudo o que não pertença a esse âmbito íntimo, mas que, por sua vez, não ultrapasse à esfera pública, consistindo na convivência familiar, com os companheiros de trabalho e com os amigos mais próximos.

permaneceria intocável somente para os menores de idade (PÉREZ LUÑO, 2012, p. 120-1).

Tamanha transformação exige uma redefinição do já obsoleto conceito de privacidade, que abandonou a esfera da solidão característica de um "direito de ser deixado só", para incorporar um viés dinâmico, relacionado à possibilidade do sujeito conhecer, controlar, endereçar e interromper ativamente o fluxo de informações a seu respeito. A definição mais apropriada para a privacidade, nesse novo contexto, passa a ser "o direito de manter o controle sobre as próprias informações" (RODOTÁ, 2008, p. 92).

O titular do direito à privacidade acaba por concretizar o seu direito através da exigência de formas de "circulação controlada" (sequência pessoa-informação-circulação-controle), e não mais somente interrompendo o fluxo das informações (pessoa-informação-sigilo) (RODOTÁ, 2008, p. 93). Assim, algumas das transformações representadas pelo novo panorama tecnológico, para Stefano Rodotá (2008, p. 128), são o aumento do valor agregado das informações pessoais e sua transformação em mercadoria, relegando-se a pessoa humana e sua dignidade a uma posição de menor importância, além de tornar cada vez mais sutil a fronteira entre a esfera pública e a esfera privada.

Nesse contexto, a proteção de dados pessoais passa a ser um dos aspectos mais importantes da privacidade, enquanto direito ao controle das informações que dizem respeito ao indivíduo. Têmis Limberger (2007, p. 61) conceitua dado pessoal como "uma informação que permite identificar uma pessoa de maneira direta", seguindo a definição estabelecida por diversas normativas europeias. A autora (2007, p. 61) apresenta a necessidade de uma proteção mais rigorosa para alguns tipos de dados, que possuem conteúdo especial, referindo-se a questões de ordem religiosa, ideológica, sexual, racial, de crença ou de saúde, os denominados "dados sensíveis"[22], cuja obtenção pode gerar uma diferença de tratamento discriminatória, em especial nas relações de trabalho.

O reconhecimento de um direito autônomo e específico para a proteção de dados pessoais, definido pela doutrina alemã como o direito à autodeterminação informativa[23] (*informationelle selbstestimmung*), foi consolidado pelo Tribunal Constitucional Federal da Alemanha (*Bundesverfassungsricht*) em 1983, por meio de uma célebre sentença relacionada

[22] Identificando a demanda por um nível protetivo distinto para os diversos tipos de dados, Fernandéz Delpech (2004, p. 292) classifica os dados pessoais em duas categorias: os dados pessoais públicos e os dados pessoais íntimos, classe em que se encontram os dados sensíveis e os dados não sensíveis.

[23] É possível elencar algumas características próprias do direito à autodeterminação informativa: 1) trata-se de um direito originário, inerente ao indivíduo; 2) é subjetivo privado, permitindo o livre exercício das faculdades individuais; 3) absoluto, oponível a terceiros; 4) personalíssimo, exercível somente pelo seu titular; 5) irrenunciável, não podendo ser afastado pela vontade; 6) variável, pois seu conteúdo é flexível e desenvolve-se conforme as circunstâncias; 7) imprescritível, permanecendo inalterável com o decurso do tempo; e interno, pois insere-se na particularidade do sujeito, no âmbito de sua consciência (JUÁREZ, 2003, p. 68-9).

ao tratamento de dados pelo censo do país (DONEDA, 2006, 192-6). Compreendida como um direito fundamental, a autodeterminação informativa foi identificada pela Corte Constitucional alemã como o "[...] direito de um indivíduo controlar a obtenção, a titularidade, o tratamento e a transmissão de dados relativos à sua pessoa" (DONEDA, 2011, p. 95).

A doutrinadora portuguesa Catarina Sarmento e Castro (2011, p. 11) relaciona a autodeterminação informativa com a "[...] liberdade de controlar a utilização das informações que lhe respeitem (desde que sejam pessoais), e na proteção perante agressões derivadas do uso dessas informações". Esta garantia nasce para salvaguardar um direito à intimidade no que diz respeito ao tratamento de dados pessoais (CASTRO, 2005, p. 25), atuando como uma proteção ao indivíduo em todos os aspectos da privacidade na sociedade em rede, tendo em vista que seus dados pessoais são fragmentos e espalhados por diversos bancos de dados e registros eletrônicos.

Este direito representa a superação do modelo de segmentação que caracterizava a "Teoria das Esferas", uma vez que inexistem dados pessoais irrelevantes diante das diversas possibilidades tecnológicas de manipulação e reagrupamento de dados (SILVA, C. B., 2014, p. 41). A noção de privacidade dividida em camadas bem definidas acaba entrando em defasagem diante da coleta massiva de dados pessoais por meios eletrônicos, sendo que o tratamento de dados aparentemente anônimos e inofensivos pode levar à identificação de seu titular, revelando informações sensíveis, o que requer a autonomia do indivíduo no controle da circulação de todos os seus dados pessoais, e não apenas daqueles mais reservados.

Partindo dessa linha evolutiva, alguns autores, como é o caso de Ana Frazão, passam a compreender a noção atual de privacidade como um conceito amplo, que abrange não só o aspecto clássico da intimidade e do segredo, mas também o direito ao controle e autodeterminação informativa, incorporando ainda importantes direitos e garantias fundamentais, como o direito à não discriminação, a liberdade, a igualdade e a própria cidadania, na medida em que os dados pessoais podem ser utilizados para todo tipo de manipulação, inclusive política (FRAZÃO, 2019, p. 108-9).

Carlos Eduardo Saltor (2013. p. 56), por sua vez, entende que o direito à autodeterminação informativa integra o aspecto subjetivo do direito à intimidade. Dessa forma, a intimidade tutelada pelo direito à autodeterminação seria dotada de uma proteção política e coletiva, superando os esquemas defasados que mantinham em compartimentos estanques o individual e o social, o pessoal e o coletivo, o público e o privado. Por conta disso, o direito à intimidade mantém relação direta com outras liberdades individuais, já que os danos

decorrentes da utilização indevida das novas tecnologias afeta direitos fundamentais como a liberdade ou a igualdade (SALTOR, 2013, p. 60).

Já Bruno Bioni defende que o direito à proteção de dados pessoais[24] seria dotado de autonomia própria (trata-se de um novo direito da personalidade, que não deve ser amarrado a uma categoria específica). Assim, ao afastar-se da dicotomia do público/privado, o direito à proteção de dados pessoais transcende a ideia de uma mera evolução do direito à privacidade, na medida em que tutela a dimensão relacional do ser humano, o que está atrelado à diversas liberdades individuais, inclusive os direitos à igualdade e à não discriminação, extrapolando o âmbito de tutela do direito à privacidade. Para o autor, os diversos direitos fundamentais que estão diretamente vinculados ao direito à proteção de dados não são abarcados pelo direito à privacidade (BIONI, 2019, p. 98-9).

A partir de todos esses conceitos doutrinários, o presente trabalho pretende adotar alguns parâmetros de nomenclatura, sistematizado da seguinte forma:

1) Compreende-se a privacidade em seu sentido amplo, como "expressão guarda-chuva" dotada de diversos aspectos (dimensões, cuja significação ganhou conteúdo de acordo com cada contexto histórico, mas coexistentes entre si) que vão desde a sua noção individualista, ligada a um direito de estar só, de cunho negativo (incluindo o segredo, a intimidade e a vida privada em seus conceitos tradicionais), chegando a uma compreensão contemporânea, de ordem positiva, relacionada ao direito de controle sobre o fluxo de informações que dizem respeito ao indivíduo (autodeterminação informativa, ou direito à proteção de dados pessoais). As noções de igualdade e liberdade, embora imbricadas e indissociáveis do direito à privacidade, extrapolam o seu âmbito de abrangência.

2) Utiliza-se as expressões "direito à autodeterminação informativa" e "direito à proteção de dados pessoais" como expressões sinônimas, para designar um direito dotado de sentido próprio e autonomia, que tutela o fluxo informacional do indivíduo e possui desdobramentos na esfera relacional, com impactos não só nos direitos à privacidade, mas também na possibilidade de ser vítima de práticas discriminatórias ou restritivas, o que repercute em diversos direitos civis, políticos e sociais. Dentre as manifestações da autodeterminação informativa, encontram-se o direito ao esquecimento, o direito à

[24] Diante da multiplicidade de termos que tratam de conteúdo semelhante, tais como "direito à proteção de dados", "liberdade informática" e "autodeterminação informativa", ainda que possam existir adeptos de uma ou outra nomenclatura e reconhecendo a validade de seus argumentos, Carlos Bruno Ferreira da Silva (2014, p. 74-5) defende a utilização das expressões "direito à proteção de dados" e "direito à autodeterminação informativa" como sinônimas, posição que é adotada por este trabalho.

"extimidade"[25], o direito à anonimização de dados, o direito ao acesso, direito à retificação, direito à portabilidade, etc. Por isso, a autodeterminação informativa passa a ser uma das principais facetas do direito à privacidade na sociedade em rede, mas que abrange também aspectos do direito à igualdade e à liberdade, ainda que não se confunda com tais direitos. Em síntese: compreende-se o direito à autodeterminação informativa como um direito autônomo cujo espectro protetivo contempla não só a privacidade, em sua dimensão positiva, mas também fragmentos da igualdade e da liberdade.

No âmbito laboral, a autodeterminação informativa permite ao trabalhador o controle das informações que são coletadas e armazenadas pela empresa, estabelecendo-se como o principal limite ao poder diretivo patronal (SÍMON, 2000, p. 165). Essa garantia confere ao empregado não apenas a faculdade de opor-se à coleta de dados e a possibilidade de conhecimento e acesso aos bancos de dados mantidos pela empresa, mas também de retificação e exclusão de dados incorretos ou indesejados. Estão dentro do âmbito protetivo do direito à autodeterminação informativa, portanto, os dados coletados por meio das entrevistas de emprego, os dados coletados por força do contrato de trabalho e também as informações relacionadas ao trabalhador que servem como fonte de convencimento em processos seletivos, ainda que não fornecidas pelo obreiro, depositadas e mantidas em bancos de dados patronais.

É neste ponto que insere-se outro aspecto importante da proteção de dados pessoais: o direito ao esquecimento, vinculado à expressão norte-americana "*right to be forgotten*"[26], que confere ao usuário a possibilidade de deletar dados e informações pessoais na *internet* (FORTES, 2016, p. 186). Antonio Rulli Júnior e Antonio Rulli Neto (2012, p. 426) definem o direito ao esquecimento como "[...] aquele em que se garante que os dados sobre uma pessoa somente serão conservados de maneira a permitir a identificação do sujeito a eles ligado, além de somente poder ser mantido durante o tempo necessário para suas finalidades".

Ainda que não se confunda com o direito à privacidade, o direito ao esquecimento manifesta-se como uma de suas várias facetas (PARENTONI, 2015, p. 577), relacionando-se, nas palavras de Parentoni (2015, p. 577), à:

> [...] faculdade de obstar o processamento informatizado, a transferência ou publicação de dados pessoais, além de exigir que sejam apagados, sempre que a sua preservação esteja causando constrangimento ao sujeito envolvido, desde que não exista razão de interesse público que justifique a preservação.

[25] Para maiores aprofundamentos acerca do "direito à extimidade", sugere-se a leitura de Bolesina (2015).
[26] Conforme Parentoni (2015, p. 546), a doutrina costuma utilizar diversas expressões para definir o direito ao esquecimento: *right to forget*, *right to forgotten*, *right to erasure*, *right to delete*, *right to oblivion* (termo que o autor considera adequado), e até mesmo *right to be let alone,* expressão vinculada ao sentido originário do direito à privacidade, conforme anteriormente referido.

Aparentemente em sentido diverso, Anderson Schreiber (2019, p. 374) defende que o direito ao esquecimento não se relaciona tanto à privacidade, mas sim ao direito à identidade pessoal. Para ele (2019, p. 374), a interpretação deste como um direito de apagar os dados do passado é equivocada, já que representa um direito individual de "[...] se opor à recordação opressiva de determinados fatos perante a sociedade (recordações públicas nesse sentido), que lhe impeça de desenvolver plenamente sua identidade pessoal, por enfatizar perante terceiros aspectos de sua personalidade que não mais refletem a realidade".

Ocorre que, a partir da definição conceitual de privacidade já apresentada, e das noções de direito ao esquecimento acima referidas, pode-se verificar que ambas as concepções conduzem a um mesmo ponto: a de que o direito ao esquecimento vincula-se à esfera relacional do indivíduo e à possibilidade de fortalecimento de sua identidade pessoal, o que será efetivado mediante o controle do fluxo de seus dados pessoais. Portanto, o que se defende neste trabalho é a classificação do direito ao esquecimento como um dos aspectos da autodeterminação informativa do sujeito, que como visto, possui reflexos diretos no seu direito à construção e reconstrução da identidade pessoal.

O direito ao esquecimento, que nos primórdios de seu reconhecimento pelo Superior Tribunal de Justiça brasileiro ganhou o sentido de "direito de não ser lembrado contra sua vontade", relacionando-se a fatos desabonadores na esfera criminal (SCHREIBER, 2019, p. 371), ganhou novos contornos no contexto da *Internet*, passando a dizer respeito à possibilidade de desindexação dos resultados emitidos pelos mecanismos de busca na rede, para que as pesquisas em buscadores não remetam ao nome da pessoa quando relacionadas àquele conteúdo que não se quer propagar. É o que defende Ruaro e Machado (2017, p. 225), ao afirmar que "O diferencial da tutela direito ao esquecimento na internet recai no fato de que, além de englobar a tutela clássica desse direito enquanto óbice a uma veiculação de uma nova reportagem sobre fato antigo, ela abarca a chamada desindexação".

Este direito muitas vezes conflitua com o direito de acesso à informação pública, na medida que algumas informações possuem interesse público na sua divulgação. Em outras situações, o fato não possui qualquer relevância para a coletividade, submetendo o indivíduo a uma exposição desnecessária. É o caso das informações relacionadas à vida privada do trabalhador (as quais não compõe a esfera do interesse público, tampouco interessando ao seu empregador), que tenham sido registradas e armazenadas no meio virtual, tornando-se de livre acesso ao público, estejam elas depositadas em redes sociais, sistemas de busca ou, especialmente, em mecanismos que deveriam garantir o sigilo dessas informações, como os "e-

jus" trabalhistas, sistemas de armazenamento eletrônicos de informações judiciais que, eventualmente, podem estar disponíveis na *Internet* por descuido (FINCATO; GUIMARÃES, 2019, p. 278).

A essas bases de dados incluem-se os bancos de jurisprudência mantidos pelo Poder Judiciário e divulgados na rede mundial de computadores por meio de consultas *on-line,* franqueando ao público em geral as minúcias de caráter íntimo que são relatadas em muitas das reclamações trabalhistas, permanecendo acessíveis pela *web* por muito tempo, mesmo após o término do processo. Tamanha facilidade na coleta de dados sensíveis confere ao empregador a possibilidade de ter em suas mãos um dossiê completo sobre a vida pregressa do candidato, onde podem constar antecedentes laborais e criminais, preferências pessoais, orientação sexual, histórico de doenças, etc. Todas essas informações podem ser (e com frequência, o são) utilizadas como critério discriminatório de um postulante a vaga de emprego, como descrevem Fincato e Gumarães (2019, p. 281):

> Os empregadores naturalmente recorrem a sistemas de busca da internet e *sites* de relacionamento antes de contratar um empregado. Algumas empresas, sem pudores, solicitam ao candidato sua senha nos sites de relacionamento, quando da entrevista de seleção ao emprego (caso tal sítio seja protegido ou restrito). A tomada de decisão sobre a contratação (ou não), passará, então, por critérios que não perquirem apenas da habilidade e formação do candidato, podendo pautar-se em suas opções pessoais (partidárias, religiosas, de orientação sexual, entre outras).

Com isso, o tratamento de dados pessoais do trabalhador repercute na violação não apenas da sua dignidade humana, mas também do direito à igualdade, já que as informações são utilizadas como fator de discriminação social. Revisitando a formação histórica dos direitos fundamentais, observa-se que a bandeira de defesa da igualdade remete à Revolução Francesa, movimento burguês que visava romper com os privilégios de um modelo monárquico à partir da inspiração em ideais de liberdade, igualdade e fraternidade. Com o estabelecimento de um Estado de feições liberais, a igualdade formal, despreocupada com particularidades de grupos minoritários, tomou a forma de direito civil e político que protegia os indivíduos contra as arbitrariedades do Estado, sendo incorporada pelo constitucionalismo liberal, destacando-se a iniciativa pioneira da Constituição Francesa de 1793 (PERES, 2014, p. 22-3).

A concepção de igualdade meramente formal começou a ruir juntamente com o liberalismo. O aprofundamento das contradições do próprio modelo, as consequências da Revolução Industrial, tais como as péssimas condições de trabalho e o crescimento de uma massa de trabalhadores desempregados e a morte de milhares de pessoas na Primeira Guerra Mundial colocaram em crise sobre a concepção de igualdade formalista presente nas

Constituições e declarações de direitos. O fim da Segunda Guerra Mundial representou a consolidação de uma noção de igualdade material, a partir de um sistema protetivo dos direitos humanos no cenário internacional, cuja atenção passa a direcionar-se aos grupos minoritários (PERES, 2014, p. 24-7).

O princípio da igualdade passa a proibir tratamentos diferenciados fundados exclusivamente em razões arbitrárias ou critérios contrários à dignidade humana, garantindo que ninguém seja prejudicado ou beneficiado em virtude de realidades específicas, tais como ascendência, sexo, raça, língua, religião, etc. Assume, com isso, o papel de motor de uma igualdade jurídico-material idealizada, que se busca promover através da imposição de uma obrigação ao Poder Público, qual seja a de compensar desigualdades socialmente construídas por meio de discriminações positivas, refletindo-se na sua política econômica, fiscal, dentre outras (GARCIA, 2005, p. 18-22).

O aspecto material da igualdade demanda o reconhecimento do indivíduo enquanto ser social, exigindo do Estado uma atuação positiva, de forma a assegurar às minorias as condições adequadas de saúde, trabalho, educação, etc. Preocupada com a discriminação nas relações empregatícias, a Organização Internacional do Trabalho (OIT) editou a Convenção nº 111 (OIT, 1958), conhecida como "Convenção sobre a Discriminação (Emprego e Profissão)". A convenção, que foi adotada em 1958 e ratificada pelo Brasil em 26 de novembro de 1965, visa o compromisso dos países signatários com a adoção de medidas que promovam a igualdade de oportunidade e tratamento no acesso à formação profissional, ao emprego, às diferentes profissões e às condições de emprego, com o objetivo de eliminar toda distinção, exclusão ou preferência que possa ser fundada na raça, sexo, religião, opinião política, ascendência ou origem social, o que se relaciona com os dados pessoais sensíveis do trabalhador (OIT, 1958).

No âmbito das Nações Unidas, os dados pessoais do empregado são tutelados pelo Repertório de Recomendações Práticas sobre a Proteção dos Dados Pessoais dos Trabalhadores, adotado pela OIT em 1997. O Repertório determina, dentre os princípios gerais elencados, que o tratamento de dados pessoais deva ser motivado somente por razões diretamente relevantes para o emprego do trabalhador (5.1), e que o processamento de dados não tenha efeito discriminatório na relação laboral (5.10) (OIT, 1997). Apesar de não possuir força vinculativa, este documento traz diversas recomendações que podem servir como orientação para o desenvolvimento das legislações internas de cada país, ou mesmo de acordos, convenções coletivas e regulamentos empresariais, estabelecendo, por exemplo, limites aos questionamentos patronais nas entrevistas de emprego e vedando a transferência de dados

pessoais do empregado para terceiros, para fins comerciais ou publicitários (SANDEN, 2014, p. 35-6).

Se há nas Nações Unidas um repertório de recomendações que oriente a edição de normas relacionadas à tutela dos dados pessoais do trabalhador em todos os seus Estados-Membros, a preocupação com a eliminação de práticas discriminatórias é reforçada e conduzida pelas cartas constitucionais de cada nação, especialmente nos países do Mercosul, onde inexiste um sistema de harmonização de normas nos moldes da União Europeia. A Argentina, país que é objeto do estudo comparado desenvolvido neste trabalho, consagra a igualdade, em seu aspecto formal, por meio do artigo 16 da Constituição da Nação[27], reconhecendo a igualdade de todos os seus habitantes perante a lei (ARGENTINA, 1994). A reforma constitucional de 1994 trouxe alguns dispositivos que inseriram a noção de igualdade material ao texto constitucional, tais como os artigos 37[28] e 75, inciso 23[29], representando "[...] a recepção de um paradigma de igualdade que promulga a superação de barreiras fáticas que impedem a plena realização dos direitos daqueles que integram grupos desfavorecidos"[30] (TREACY, 2012, p. 273).

No ordenamento jurídico brasileiro, diversas são as garantias constitucionais que estabelecem o direito à igualdade e à não discriminação, a começar pelos objetivos da República Federativa do Brasil, elencados no artigo 3° da Constituição de 1988, que em seu inciso IV visa a promoção do bem de todos, "sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação". Além disso, a Carta Magna assegura o direito à igualdade (artigo 5°, *caput*), e a punição a qualquer discriminação que atente contra os direitos e liberdades fundamentais (art. 5°, XLI) (BRASIL, 1988).

---

[27] "Artículo 16.- La Nación Argentina no admite prerrogativas de sangre, ni de nacimiento: no hay en ella fueros personales ni títulos de nobleza. Todos sus habitantes son iguales ante la ley, y admisibles en los empleos sin otra condición que la idoneidad. La igualdad es la base del impuesto y de las cargas públicas" (ARGENTINA, 1994).

[28] "Artículo 37.- Esta Constitución garantiza el pleno ejercicio de los derechos políticos, con arreglo al principio de la soberanía popular y de las leyes que se dicten en consecuencia. El sufragio es universal, igual, secreto y obligatorio.

La igualdad real de oportunidades entre varones y mujeres para el acceso a cargos electivos y partidarios se garantizará por acciones positivas en la regulación de los partidos políticos y en el régimen electoral" (ARGENTINA, 1994).

[29] "Artículo 75.- Corresponde al Congreso: [...] 23. Legislar y promover medidas de acción positiva que garanticen la igualdad real de oportunidades y de trato, y el pleno goce y ejercicio de los derechos reconocidos por esta Constitución y por los tratados internacionales vigentes sobre derechos humanos, en particular respecto de los niños, las mujeres, los ancianos y las personas con discapacidad.

Dictar un régimen de seguridad social especial e integral en protección del niño en situación de desamparo, desde el embarazo hasta la finalización del período de enseñanza elemental, y de la madre durante el embarazo y el tiempo de lactancia" (ARGENTINA, 1994).

[30] Do original: "Ambas disposiciones significan la recepción de un paradigma de igualdad que promulga la superación de barreras fácticas que impidan la realización plena de los derechos de quienes integran grupos desaventajados" (TREACY, 2012, p. 273).

Outros direitos fundamentais que protegem o trabalhador contra a utilização de seus dados pessoais para fins discriminatórios na seleção de emprego encontram-se elencados no rol dos direitos sociais. A Constituição brasileira garante, em seu artigo 7°, XXX, a proibição de diferenças salariais, de exercício de funções e de critérios de admissão fundados em motivos de sexo, idade, cor ou estado civil, e veda, no artigo 7°, XXXI, qualquer discriminação salarial ou relativa a critérios de admissão do trabalhador portador de deficiência (BRASIL, 1988).

O princípio da igualdade vincula-se ao tratamento de dados sensíveis do trabalhador, na medida em que o conhecimento anterior dessas informações pela empresa pode gerar quebra da isonomia. É o que ocorre, por exemplo, quando o empregador descobre doença grave que acomete o obreiro, tal como a AIDS, por meio do acesso a prontuário médico, dispensando-o imotivadamente ou mesmo deixando de admiti-lo em virtude disso (LIMBERGER, 2007, p. 203).

Por essa razão, a Lei nº 9029/95, com nítida inspiração na Convenção nº 111 da OIT, proíbe a adoção de práticas discriminatórias na seleção de emprego, bem como no contrato de trabalho, sejam elas motivadas por orientação sexual, aspectos raciais, cor da pele, estado civil, deficiência, entre outros (artigo 1°). A lei garante ao trabalhador despedido por ato discriminatório, além da reparação pelo dano moral, a faculdade de a reintegração com ressarcimento integral do período de afastamento, ou a percepção, em dobro, da remuneração do período de afastamento, com os devidos juros e correção monetária (artigo 4°) (BRASIL, 1995).

Amparada pelo princípio da igualdade e da não discriminação nas relações laborais, a jurisprudência espanhola[31] formulou o instituto da garantia de indenidade, que visa proteger o trabalhador que exerce o direito fundamental de ação contra a despedida imotivada. A garantia de indenidade seria um instrumento de efetivação desse direito, vedando a retaliação ou vingança pela pessoa pública ou privada obrigada a atender a demanda, tornando nulo qualquer ato de represália. Essa garantia geraria efeitos não apenas no caso de despedida imotivada, mas nas diversas formas de represália que possa sofrer o empregado, inclusive antes ou depois da vigência do contrato de trabalho (CARVALHO, 2013, p. 112-3).

Portanto, a garantia de indenidade poderia ser invocada pelo candidato preterido de uma vaga de emprego pelo fato de ter em seu histórico o ajuizamento de ação trabalhista contra ex-

[31] A formulação embrionária da garantia de indenidade é imputada ao Tribunal Constitucional espanhol, que na STD n. 6/1988 reconheceu que a celebração do contrato de trabalho não possui o condão de privar o trabalhador dos direitos fundamentais constitucionalmente assegurados, ainda que tal contrato possa condicionar o exercício da liberdade (CARVALHO, 2013, p. 123).

empregador, resguardando o direito fundamental de ação deste trabalhador em face de uma possível retaliação na etapa pré-contratual. Sua aplicação, neste caso, está relacionada ao uso não discriminatório dos dados pessoais que compõe processos judiciais trabalhistas acessíveis pela rede mundial de computadores.

A efetivação dessa garantia demanda o controle do indivíduo com relação aos seus dados pessoais constantes em bancos de dados públicos e privados, incluindo a possibilidade de retificação ou exclusão de informações indesejadas, tais como os dados sensíveis que integram os processos judiciais ajuizados. O reconhecimento de um direito à autodeterminação informativa passa a ser uma necessidade impulsionada pela evolução tecnológica, que submete os indivíduos a uma vigilância massiva imposta pelos Estados Nacionais e por organizações privadas, e que, com relação ao trabalhador, revela-se ainda mais ameaçadora, exigindo uma proteção jurídica condizente com a sofisticação dos instrumentos de coleta e distribuição de dados pessoais.

Sintonizada com esse novo paradigma, a União Europeia tomou a dianteira na edição de normativas que oferecem robusta tutela aos dados pessoais de seus cidadãos, apresentando um modelo de regulação estruturado em um sistema protetivo unificado e uma principiologia vanguardista que serviu como parâmetro de aplicação para diversos países ao redor do mundo, o que será desenvolvido na seção seguinte.

2.2 A UNIÃO EUROPEIA COMO MODELO PARADIGMÁTICO

Os primeiros passos para a construção de um sistema de proteção de dados pessoais na União Europeia (atualmente unificado em torno do Regulamento Geral de Proteção de Dados), foram dados pela adoção de leis nacionais de proteção de dados pelos Estados-Membros. A produção normativa europeia de proteção de dados teve início em 1970, através da experiência alemã no *Land* de Hesse, com a tentativa de elaboração de um sistema de proteção de dados pessoais[32]. Na ocasião, foi instituído o primeiro comissário de proteção de dados, autoridade autônoma que deveria reportar-se ao Parlamento do *Land*. Alguns anos depois, em 1973, a Suécia foi a pioneira na edição da primeira lei nacional de proteção de dados pessoais, denominando um órgão autônomo encarregado de zelar pela sua aplicação (DONEDA, 2006, p. 228). Observa-se, desde as primeiras iniciativas, uma preocupação com a designação de uma autoridade responsável pelo controle e fiscalização da lei de proteção de dados.

[32] A legislação pioneira do *Land* de Hesse abrangia somente os arquivos digitais de titularidade pública (LIMBERGER, 2009, p. 36).

Outros países europeus vieram a legislar acerca da proteção de dados pessoais[33] até que, no final dos anos 1970, com a identificação de que as legislações focadas no direito interno não seriam suficientes tendo em vista o caráter transnacional da coleta e tratamento de dados, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) organizou discussões acerca da uniformização legislativa supranacional. A iniciativa culminou na elaboração das Diretrizes sobre a Proteção da Privacidade e o Fluxo de Dados Pessoais Transfronteiriços (*Guiderlines on the Protecion of Privacy and Transborder Flows of Personal Data*), adotadas em 1980, que possuía uma forte preocupação com o tráfego de dados e não propriamente com a sua proteção. Apesar de seus enunciados não serem vinculantes, as diretrizes estabeleceram os princípios que passaram a nortear a regulação da proteção de dados pessoais (DONEDA, 2006, p. 230-1).

Em 1981 foi editada pelo Conselho da Europa a Convenção para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais nº 108/1981 ou Convenção de Strasbourg (CONSELHO..., 1981), que representou o primeiro passo para a construção de um sistema europeu integrado de proteção de dados pessoais, inserindo a proteção de dados na esfera dos direitos humanos (DONEDA, 2006, p. 231-2). A Convenção nº 108 é o único instrumento internacional juridicamente vinculativo adotado até hoje no âmbito da proteção de dados pessoais, tendo sido ratificada por todos os Estados-Membros da União Europeia e sendo aberta também para a adesão de países não-membros do Conselho da Europa[34] (AGÊNCIA...; CONSELHO..., 2018, p. 24-6).

Ambos os documentos (Diretrizes sobre a Proteção da Privacidade e o Fluxo de Dados Pessoais Transfronteiriços e Convenção nº 108 do Conselho da Europa) deram origem a muitos dos princípios e normas válidas até hoje, servindo de inspiração na elaboração de diversas legislações que os seguiram no plano internacional, estruturados na ideia de minimização dos riscos do processamento automático de informações e na vedação da coleta injustificada de dados pessoais (SANDEN, 2014, p. 29). Inspirado na principiologia proposta por estes marcos regulatórios, Doneda (2015, p. 376) assim sintetizou os princípios aplicáveis para o tratamento

[33] A evolução das legislações internas dos países europeus no tocante à proteção de dados pessoais permite a sua classificação em três gerações de leis: a fase inicial, caracterizada por uma criação mais rigorosa de arquivos automatizados, abrange a lei do *Land* de Hesse alemão, de 1970, a lei sueca de 1973, a lei da República Federal Alemã de 1977, a lei dinamarquesa de 1978 e a lei austríaca de 1978. A segunda geração, que demonstra maior preocupação com a proteção de direitos fundamentais, compreende as leis editadas no final dos anos 70 e início dos anos 80, tais como a lei francesa de 1978, a lei de Luxemburgo de 1979, a lei suíça de 1981 e a lei da Islândia de 1981. A terceira fase, marcada pela unificação do direito europeu, tem início através da Convenção de Estrasburgo de 1981, destacando-se a lei do Reino Unido de 1984, a nova lei alemã de 1990, a primeira lei de Portugal de 1991, a lei espanhola de 1992 e a lei italiana de 1996 (LIMBERGER, 2009, p. 36).

[34] O Uruguai foi o primeiro país não europeu a formalizar sua adesão à Convenção 108, fato que ocorreu em agosto de 2013 (AGÊNCIA...; CONSELHO..., 2018, p. 26).

de dados pessoais: princípio da transparência ou publicidade, princípio da qualidade, princípio da finalidade, princípio do livre acesso, princípio da segurança física e lógica, princípio da proporcionalidade e princípio da necessidade.

O princípio da finalidade orienta o procedimento relacionado ao tratamento de dados pessoais, relacionando-o, de forma expressa e limitada, a finalidade a que foram coletados, observados os critérios da proporcionalidade e adequação entre os meios e os fins utilizados (KLEE; MARTINS, 2015, p. 319). Este princípio tem importância fundamental no que diz respeito à destinação dos dados pessoais fornecidos pelo empregado ao Poder Judiciário em virtude do ajuizamento de reclamação trabalhista, e que acabam sendo disponibilizadas na *Internet* e utilizados para outros fins, servindo como um dos vetores interpretativos deste estudo.

Por possuir um conteúdo demasiadamente generalista, admitindo exceções a muitos desses princípios, a Convenção nº 108/1981 não representou uma ferramenta jurídica suficiente o bastante para garantir a almejada compatibilização legislativa, fundamental para a livre circulação de dados no interior do mercado europeu (GONÇALVES, 2003, p. 98). Em virtude disso, foi adotada em 1995, no âmbito da União Europeia, a Diretiva 95/46 CE, do Parlamento Europeu e do Conselho (PARLAMENTO..., 1995), que visava justamente a harmonização das legislações protetivas de dados dos Estados-Membros, tornando equivalentes os níveis de proteção em um patamar elevado (AGÊNCIA...; CONSELHO..., 2018, p. 29).

Diferentemente da Convenção nº 108 do Conselho da Europa, a Diretiva 95/46 impôs aos legisladores o dever de produzir normas internas que atingissem o patamar protetivo delineado em suas diretrizes[35]. A diretiva apresentava um duplo viés de atuação: se por um lado buscava a proteção do sujeito titular dos dados pelo tratamento de suas informações pessoais, por outro mostrava clara preocupação com as exigências mercadológicas, visando o fomento do comércio através do livre fluxo de dados entre os países do bloco, o que somente seria possível através da harmonização nas regras protetivas de dados (DONEDA, 2006, p. 236).

A proteção de dados pessoais foi alçada à categoria de direito fundamental autônomo em 07 de dezembro de 2000, através da Carta de Direitos Fundamentais da Europa[36] (UNIÃO

[35] As diretivas são atos legislativos que fixam um objetivo geral a ser alcançado por todos os Estados-Membros da União Europeia, cabendo a cada país tomar as medidas necessárias para a adequação de sua legislação interna (PARLAMENTO..., 2018).

[36] "Artigo 8° - Proteção de dados pessoais
1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.
2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação.

EUROPEIA, 2000), conhecida como Carta de Nice, que incorporou os direitos civis, políticos, econômicos e sociais comuns aos Estados-Membros. Este documento tornou-se juridicamente vinculativa como direito primário da União Europeia com a entrada em vigor do Tratado de Lisboa, em dezembro de 2009 (AGÊNCIA...; CONSELHO..., 2018, p. 28).

Em 2002 foi editada a Diretiva 2002/58/CE (PARLAMENTO EUROPEU E CONSELHO, 2002), que dispõe de forma mais específica sobre o tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas. Apesar de não representar uma real inovação em relação à Diretiva 95/46 CE, esta diretiva tinha o intuito de adequar o modelo regulatório à realidade tecnológica das comunicações em rede (DONEDA, 2006, p. 239), restringindo-se ao tratamento de dados realizado nesse contexto.

O Tratado que estabelece uma Constituição para a Europa (UNIÃO EUROPEIA, 2004), adotado pelo Conselho Europeu em 18 de junho 2004 em Bruxelas, e assinado em Roma, em 29 de outubro do mesmo ano, contempla a proteção de dados pessoais em dois de seus dispositivos. O artigo I-51, que está inscrito no capítulo "Vida democrática da União Européia", volta-se às instituições, órgãos e organismos da União Europeia e seus Estados-Membros. Já o artigo II-68 inscreve-se no capítulo das "Liberdades", dirigindo suas atenções para o consentimento no fornecimento de dados, bem como o direito de acesso e retificação (FORTES, 2016, p. 156). O projeto acabou fracassando pela ausência de ratificação por todos os Estados-Membros, tendo em vista que foi rejeitado por França e Holanda em seus respectivos referendos nacionais (PARLAMENTO EUROPEU, 2019).

Todas as normativas anteriormente referidas evidenciam uma forte preocupação com relação ao estabelecimento de um nível adequado de proteção em todos os países do bloco, com um viés protetivo voltado ao titular dos dados, algo que exigia uma atualização legislativa a fim de adaptar-se à rápida evolução tecnológica. Assim, em janeiro de 2012, foi proposto pela Comissão Europeia uma reforma legislativa visando a modernização da legislação do bloco europeu, adaptando-a ao contexto econômico e social da era digital (AGÊNCIA...; CONSELHO..., 2018, p. 29-30).

Esta proposta culminou na edição do Regulamento[37] (UE) 2016/679 do Parlamento Europeu e do Conselho (UNIÃO EUROPEIA, 2016), ou Regulamento Geral sobre Proteção de Dados (RGPD), de 27 de abril de 2016, que se tornou aplicável em 25 de maio de 2018,

3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente" (UNIÃO EUROPEIA, 2000).

[37] Diferentemente das diretivas, os regulamentos são atos legislativos vinculativos, aplicando-se na sua integralidade aos Estados-Membros da União Europeia (PARLAMENTO..., 2018).

revogando a Diretiva 95/46/CE e convertendo-se no principal instrumento jurídico de proteção de dados no âmbito da União Europeia. Embora seu âmbito de atuação limite-se ao contexto da União Europeia, na prática o Regulamento possui verdadeiro alcance mundial, diante da relevância do bloco europeu na economia internacional e da integração global proporcionada pela *Internet* (SCHREIBER, 2019, p. 369). Soma-se a isso a exigência mantida pelo bloco europeu com relação ao nível adequado da legislação protetiva de dados pessoais dos países que mantém trocas comerciais com seus Estados-Membros e tem-se um Regulamento que repercute no mundo em sua totalidade.

O escopo de aplicação do RGPD abrange o tratamento de dados pessoais por meios automatizados (total ou parcialmente) e não automatizados (artigo 2º, 1), apresentando caráter extraterritorial, ou seja, é aplicável tanto quando o tratamento dos dados ocorre no contexto das atividades de uma empresa estabelecida na União Europeia, independentemente do local do tratamento (artigo 3º, 1) quanto no caso do tratamento de dados pessoais ser realizado por empresa não estabelecida no bloco europeu, desde que vise a oferta de bens e serviços[38], ainda que gratuita, ou o controle do comportamento de pessoas que se encontrem no território da União Europeia (artigo 3º, 2) (UNIÃO EUROPEIA, 2016).

Além de oferecer uma ampla cartela de princípios destinados ao tratamento de dados pessoais[39] (repetindo o modelo da Diretiva 95/46/CE, com alguns acréscimos, tais como o princípio da transparência), o RGPD apresenta seis hipóteses taxativas[40] que autorizam o

[38] Nessa hipótese, a incidência extraterritorial do RGPD demanda a apuração da real intenção de ofertar bens ou serviços a pessoas que se encontrem em território da União Europeia, o que pode ser feito pela observância de algumas atitudes por parte da empresa, tais como: listagem de número de telefone internacional para contato, *website* com domínios próprios da Europa, portais e aplicativos traduzidos aos idiomas oficiais da União, propaganda voltada para o público que se encontra no território do bloco, etc. (LIMA, 2018, p. 36).

[39] O artigo 5º do RGPD estabelece como princípios relativos ao tratamento de dados pessoais a licitude, lealdade, transparência, limitação da finalidade, minimização dos dados, exatidão, integridade e confidencialidade (UNIÃO EUROPEIA, 2016).

[40] "Artigo 6.º
Licitude do tratamento
1.O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações:
a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;
b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados;
c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;
d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;
e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento;
f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.
O primeiro parágrafo, alínea f), não se aplica ao tratamento de dados efetuado por autoridades públicas na prossecução das suas atribuições por via eletrônica" (UNIÃO EUROPEIA, 2016).

tratamento de dados, das quais o consentimento é a principal. Ao estabelecer, em seu artigo 4º, 10, o consentimento como "[...] uma manifestação de vontade, livre, específica, informada e explícita [...]" (UNIÃO EUROPEIA, 2016), o regulamento garante ao titular não apenas a possibilidade de realizar uma escolha verdadeira, podendo recusar ou retirar o consentimento livremente, sem sofrer qualquer prejuízo por conta disso, como lhe permite ter o conhecimento necessária para a tomada de uma decisão consciente, que deverá ser manifestada de forma inequívoca e específica para cada operação de tratamento de dados realizada pelo *controller*[41] (VAINZOF, 2018, p. 72-4).

A fim de garantir esta possibilidade de escolha real, o consentimento não pode estar vinculado a uma parte não negociável da execução do contrato. Ou seja, para que o consentimento seja tido como uma manifestação de vontade espontânea e livre, a ausência de consentimento não poderá privar o titular dos dados do acesso ao serviço (MELO, 2019, p. 41). Com relação às formas de manifestação do consentimento por meio da *Internet*, o RGPD estabeleceu parâmetros de atuação aos *sites* que realizam a coleta de dados, exigindo a adequação das empresas às suas definições e estabelecendo novas diretrizes que repercutem nas legislações do mundo todo. Nesse sentido, o Considerando 32 do RGPD (UNIÃO EUROPEIA, 2016) estabelece que:

> O consentimento pode ser dado validando uma opção ao visitar um sítio web na Internet, selecionando os parâmetros técnicos para os serviços da sociedade da informação ou mediante outra declaração ou conduta que indique claramente nesse contexto que aceita o tratamento proposto dos seus dados pessoais. O silêncio, as opções pré-validadas ou a omissão não deverão, por conseguinte, constituir um consentimento.

Ainda, dentre as bases legais que permitem o tratamento de dados, encontram-se duas hipóteses diretamente relacionadas aos dados pessoais fornecidos ao Poder Judiciário em virtude do ajuizamento de ação: a do artigo 6º, 1, alínea "c", que estabelece a licitude do tratamento quando "[...] for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito" e a alínea "e", quando o "[...] tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento" (UNIÃO EUROPEIA, 2016). Nesses dois

[41] *Controller*, ou responsável pelo tratamento, é "[...]a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro", conforme o artigo 4º, 7 (UNIÃO EUROPEIA, 2016).

casos, a definição do fundamento jurídico caberá ao direito da União Europeia ou de cada Estado-Membro (artigo 6º, 3), sempre observando o objetivo de interesse público e a proporcionalidade ao objetivo legítimo prosseguido. Tal fundamento jurídico pode prever disposições específicas, quais sejam (UNIÃO EUROPEIA, 2016):

> [...] as condições gerais de licitude do tratamento pelo responsável pelo seu tratamento; os tipos de dados objeto de tratamento; os titulares dos dados em questão; as entidades a que os dados pessoais poderão ser comunicados e para que efeitos; os limites a que as finalidades do tratamento devem obedecer; os prazos de conservação; e as operações e procedimentos de tratamento, incluindo as medidas destinadas a garantir a legalidade e lealdade do tratamento [...]

Assim como as normativas que o antecederam, o RGPD também oferece um padrão mais elevado de tutela aos dados sensíveis (artigo 9º, 1), definidas como uma categoria especial de dados, os quais incluem dados relativos à origem racial, etnia, opiniões políticas, convicções religiosas, filosóficas, filiação sindical, dados genéticos, biométricos, dados relativos à saúde, vida sexual ou orientação sexual (UNIÃO EUROPEIA, 2016). Apresentando a vedação ao tratamento de dados sensíveis como regra geral, a normativa apresenta dez hipóteses que permitem o tratamento desses dados (artigo 9º, 2), das quais duas chamam a atenção:

> f) Se o tratamento for necessário à declaração, ao exercício ou à defesa de um direito num processo judicial ou sempre que os tribunais atuem no exercício da suas (*sic*) função jurisdicional;
> g) Se o tratamento for necessário por motivos de interesse público importante, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados;

Algumas considerações podem ser feitas a partir da leitura dos regramentos acima referidos: em primeiro lugar, há a permissão de tratamento de dados sensíveis necessários ao exercício de direitos em processos judiciais, mas também a autorização ao Poder Judiciário de manipular e processar esses dados, sempre que atuar no exercício da sua função jurisdicional. O regulamento não deixa dúvidas ao delimitar o campo de tratamento de dados pelos Tribunais ao exercício de sua função jurisdicional, função esta que se restringe à resolução do conflito de interesses, e não abrange os atos posteriores, especialmente aqueles que não estão abarcados pelo dever de transparência da administração pública, já que envolvem informações de natureza privada, sem qualquer interesse público. Portanto, o tratamento de dados sensíveis pelos Tribunais, ao extrapolarem os da sua função jurisdicional, são vedados pelo RGPD, a não ser

que o titular forneça o seu consentimento específico para esta finalidade, nos termos do art. 9º, 2, "a" (UNIÃO EUROPEIA, 2016).

Com relação à alínea "g", que justifica o tratamento de dados sensíveis com base no interesse público relevante, é importante a disposição quanto ao tratamento proporcional ao objetivo buscado, e a necessidade de previsão de medidas específicas aptas à defesa dos direitos fundamentais do titular. Com isso, ainda que o interesse público possa autorizar o tratamento de dados em determinadas situações, como é o caso das informações divulgadas pelo Poder Judiciário no exercício da publicidade administrativa, deverão ser adotadas medidas que conduzam à salvaguarda dos direitos dos titulares, tais como a própria anonimização de dados ou a desindexação dos resultados nas consultas processuais e jurisprudenciais.

Outro direito importante para um efetivo controle do titular com relação ao fluxo de informações a seu respeito é o direito ao apagamento de dados, ou direito ao esquecimento, contemplado no artigo 17º do RGPD. Devido à importância deste direito como garantidor das liberdades individuais do cidadão no contexto da *Internet*, Lemos *et al.* (2018) defendem que a sua previsão no RGPD visa "[...] garantir maior proteção aos indivíduos na era digital, e ao mesmo tempo garantir segurança jurídica e a devida proteção à liberdade de expressão e ao interesse público".

Ainda que tal direito não constitua propriamente uma inovação no solo europeu, já que a Diretiva 95/46 tratava da possibilidade de apagamento de dados, e os tribunais já reconheciam este direito há algum tempo (MALDONADO, 2018, p. 100), destaca-se para a utilização da expressão "direito a ser esquecido" pelo próprio diploma legal. Assim, dentre os motivos que autorizam o apagamento dos dados, sem demora injustificada, estão a perda da necessidade para a finalidade que motivou o recolhimento, a retirada do consentimento e o exercício do direito de oposição[42] pelo titular, ou o tratamento ilícito dos dados (UNIÃO EUROPEIA, 2016).

O item 3 do artigo 17º trata das hipóteses em que não se aplica o direito ao esquecimento, dentre as quais encontra-se o tratamento necessário ao exercício da liberdade de expressão (alínea "a") e para fins de declaração, exercício ou defesa de direitos em processo judicial (alínea "e"). Ou seja, o direito ao apagamento de dados relativos à processos judiciais somente será aplicável nas hipóteses em que não se configura o interesse público (dados sensíveis, por exemplo) e, ainda assim, se essas informações não forem necessárias para fins de defesa em

[42] O direito de oposição está inscrito no artigo 21ºdo RGPD, permitindo ao titular dos dados que se oponha ao tratamento, o que obriga o responsável a cessá-lo, a não ser que possua razões imperiosas para que este tratamento sobreponha-se aos direitos, liberdades e interesses do titular, ou que ele seja necessário para fins de declaração, exercício ou defesa de um direito em processo judicial (UNIÃO EUROPEIA, 2016).

processo ou exercício do direito de ação (como as decisões divulgadas em ferramentas de busca jurisprudencial).

Uma das principais inovações do RGPD em relação à Diretiva 46/95 é a expressa positivação do *privacy by design,* metodologia que, conforme a definição de Lima e Bioni (2015, p. 277), consiste em levar em consideração a privacidade como um elemento condutor dos processos de concepção e desenvolvimento de produtos e serviços. Este conceito, que foi idealizado por Ann Cavoukian na década de 1990, visa "[...] proteger a privacidade do usuário desde a concepção de quaisquer sistemas de tecnologia da informação ou de práticas de negócio que sejam concernentes ao ser humano", através da incorporação da privacidade à arquitetura técnica dos produtos/serviços (JIMENE, 2018, p. 173-4).

O RGPD incorpora o conceito de *privacy by design* em seu artigo 25, ao afirmar que o responsável pelo tratamento deverá aplicar "[...] tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização [...]" (UNIÃO EUROPEIA, 2016). O dispositivo faz referência à pseudonimização[43], uma das técnicas da anonimização de dados (BIONI, 2019, p. 71), que pode ser útil no processo de construção de *sites* pelo Poder Judiciário, com vista a dificultar/impedir a identificação entre um dado e o jurisdicionado a ele atrelado.

Além do direito à portabilidade de dados, cuja incidência impacta mais diretamente o âmbito do Direito do Consumidor, outra grande novidade elencada pelo RGPD é a figura do *data protection officer* (DPO), ou "encarregado de proteção de dados", sujeito responsável pela cooperação e o aconselhamento dos responsáveis pelo tratamento e dos trabalhadores que tratem os dados pessoais acerca de suas obrigações, além da orientação acerca da avaliação de impacto sobre a proteção de dados, constituindo-se em um ponto de contato para a autoridade de controle sobre questões relacionadas com o tratamento, conforme estabelece o Art. 39, 1 (UNIÃO EUROPEIA, 2016).

O DPO atua como um canal de comunicação entre os agentes de tratamento, os titulares e a autoridade de controle, que poderá ser um funcionário ou consultor externo especialista em proteção de dados pessoais (LEMOS *et al.*, 2018). Esta pessoa não poderá ser responsabilizada por eventual descumprimento do RGPD pelos agentes de tratamento, já que sua

[43] O artigo 4º, 5 do RGPD descreve a técnica da pseudonimização como "[...] o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável (UNIÃO EUROPEIA, 2016).

responsabilidade pessoal limita-se ao exercício de função consultiva em matéria de proteção de dados junto ao agente de tratamento contratante (CHAVES, 2018, p. 136).

O RGPD é taxativo quanto às hipóteses que exigem a designação de um DPO pelo controlador ou operador, dentre elas os casos em que "[...] for efetuado por uma autoridade ou um organismo público, excetuando os tribunais no exercício da sua função jurisdicional" (UNIÃO EUROPEIA, 2016), nos termos de seu artigo 37, 1, "a". Mais uma vez observa-se a referência expressa ao tratamento de dados no exercício da função jurisdicional pelo Poder Judiciário, atividade que prescinde da nomeação de um encarregado de proteção de dados. Este dispositivo deve ser interpretado no sentido de que o tratamento de dados em atividades que não estão abarcadas pelo estrito desempenho da função jurisdicional do Tribunal exigem a designação de uma pessoa, pela própria administração pública, para receber reclamações e comunicações de titulares e órgãos competentes, prestar esclarecimentos, adotar providências e orientar funcionários, etc.

É importante observar que o RGPD prevê a criação de uma autoridade de controle totalmente independente (DPA), designada pelos Estados-Membros, que não se submeterá a influências externas, diretas ou indiretas na execução de suas funções e no desempenho dos seus poderes, conforme garante o artigo 52. Este órgão é responsável pelo controle e execução das normas regulamentares, dispondo de poderes investigativos, corretivos e consultivos (UNIÃO EUROPEIA, 2016).

Chama atenção que, mesmo com relação ao âmbito de atuação das autoridades de controle, existe regramento expresso prevendo que não são competentes para controlar operações de tratamento efetuadas por tribunais que atuem no exercício da sua função jurisdicional. Portanto, há clara orientação no RGPD flexibilizando a atuação dos agentes de tratamento no caso de estrito exercício da função jurisdicional pelo Estado (seja pela desnecessidade de designação de um encarregado de proteção de dados, seja porque estes dados não estão sob a competência de uma autoridade de controle), o que indica que as demais situações que envolvam o tratamento de dados pelo Poder Judiciário devem submeter-se à todos os dispositivos gerais de proteção elencados pelo RGPD.

Sem a intenção de exaurir o conteúdo do RGPD a partir deste apanhado histórico que acompanhou o desenvolvimento da proteção de dados pessoais na União Europeia, observa-se que toda essa evolução normativa vem trazendo reflexos positivos aos países da América Latina. A Argentina foi pioneira ao inspirar-se na Diretiva 95/46 CE para a edição de sua já sedimentada lei de proteção de dados pessoais, o que lhe rendeu o reconhecimento do bloco europeu. O Brasil, na esteira de uma tendência internacional, editou recentemente sua nova Lei

Geral de Proteção de Dados, com forte influência do recente Regulamento Geral de Proteção de Dados europeu. Mesmo antes da entrada em vigor da nova lei, os efeitos do RGPD são sentidos no Brasil, conforme lembram Ronaldo Lemos *et al.* (2018):

> A GDPR também poderá produzir efeitos sobre práticas nacionais, em razão da influência que pode exercer sobre o entendimento de autoridades judiciais e administrativas a respeito do alcance das normas vigentes no Brasil de proteção de dados pessoais. Em outras palavras, poderão ser intensificadas práticas nas quais o quadro legal vigente – em especial as regras do Código de Defesa do Consumidor, Marco Civil da Internet e de seu Decreto regulamentador – é interpretado como se espelhasse disposições da GDPR.

Diante disso, o próximo capítulo da dissertação propõe-se a realizar um estudo comparado acerca dos sistemas protetivos de dados pessoais dos dois países mercosulinos (Brasil e Argentina), com enfoque no tratamento de dados pessoais pela Justiça do Trabalho, o que demanda a análise das legislações aplicáveis e dos portais institucionais das Cortes Superiores da justiça laboral de cada país.

3 OS SISTEMAS DE PROTEÇÃO DE DADOS PESSOAIS EM PERSPECTIVA COMPARADA: aproximações e distanciamentos entre Argentina e Brasil

O modelo europeu de proteção de dados pessoais evidencia a necessidade de se pensar um sistema transnacional de tutela, que possa oferecer uma resposta adequada às demandas de uma sociedade em rede, estabelecendo-se um alto patamar protetivo em todos os países que negociam entre si. O estabelecimento de pautas jurídicas comuns entre os Estados torna-se uma necessidade, na medida em que as lesões a direitos individuais oriundas do tratamento automatizado de dados pessoais transbordam os limites nacionais (SILVA, C. B., 2014, p. 124).

Embora se reconheça a insuficiência dos mecanismos de controle estatais para a proteção adequada dos direitos humanos diante do fenômeno da globalização, da descentralização do poder e da expansão das tecnologias informacionais (MENEZES NETO; MORAIS; BEZERRA, 2017, p. 196), a existência de uma legislação adequada é extremamente necessária para estabelecer os parâmetros da tutela dentro de cada estado-nação, o que nas relações trabalhistas se mostra ainda mais relevante, na medida em que o tratamento de dados pessoais impacta diretamente no contrato de trabalho.

Tendo em vista que a produção normativa sobre o tema revela-se extremamente dinâmica e mutável, especialmente pelo conteúdo vinculado ao avanço tecnológico, que passa por constante transformação, também os mecanismos regulatórios relacionados à informação acabam revelando características especiais, capazes de permitir uma aplicação legal não rígida (GONÇALVES, 2003, p. 26). Isso explica o papel fundamental exercido pelo conjunto principiológico que norteia as legislações que regulam a proteção de dados pessoais em diversos países do mundo.

Além do sistema europeu, verifica-se a existência de outros dois modelos distintos de proteção de dados pessoais no mundo: o sistema latino-americano e o sistema dos Estados Unidos[44]. O sistema latino-americano, foco da análise deste capítulo, baseia-se principalmente na ação de *Habeas Data* e possui forte influência da Diretiva 95/46/CE, visando o reconhecimento europeu quanto ao nível de adequação das legislações, o que passa a ser uma

[44] O sistema norte-americano de proteção de dados pessoais fundamenta-se, principalmente, em mecanismos de autorregulação, diante da acentuada limitação que o direito à privacidade possui no país, muito em função do valor atribuído à liberdade de expressão. O modelo dos Estados Unidos desenvolveu-se a partir de decisões jurisprudenciais, culminando na edição do *Privacy Act,* de 1974, cujo alcance é limitado ao tratamento de dados pelo Governo Federal (CARRASQUILLA, 2012, p. 128-9). Por não fazer parte do campo de estudo desta dissertação, o sistema norte-americano não será analisado com maior profundidade, optando-se pelo modelo da União Europeia como paradigma, na medida em que representou uma influência direta às leis editadas na Argentina e no Brasil.

demanda para a realização de negócios que impliquem a transferência internacional de dados (CARRASQUILLA, 2012, p. 128-130).

Na América Latina, não há um sistema integrado de proteção de dados semelhante ao do bloco europeu. Ao contrário, o modelo latino-americano é pautado pela regulação no âmbito interno de cada país, apresentando um grande desnível evolutivo entre nações. Este modelo passou recentemente por um período de transição, saindo de uma fase cuja regulamentação encontrava-se predominantemente nas cartas constitucionais para a edição de leis que regulamentam o tratamento de dados de modo integral, compreendendo o processamento de informações tanto pelo Poder Público como pelo setor privado (SILVA A., 2012, p. 169-170).

Com a finalidade de estabelecer regras homogêneas sobre proteção de dados pessoais nos países ibero-americanos[45] e facilitar o fluxo de dados entre os países da região, a Rede Ibero-Americana de Proteção de Dados (RIPD)[46] aprovou, em 20 de junho de 2017, durante a realização do XV Encontro Ibero-Americano de Proteção de Dados, os "Padrões de Proteção de Dados dos Estados Ibero-Americanos". Este documento consiste em um conjunto de diretrizes orientadoras, que visa servir como modelo normativo para as futuras regulações de proteção de dados pessoais na região ibero-americana, no caso dos países que não contam com esses ordenamentos, ou para atuar como parâmetro na modernização e atualização das legislações já existentes (REDE IBERO-AMERICANA..., 2017, p. 3-4).

Sem o caráter vinculante do RGPD da União Europeia, os "Padrões de Proteção de Dados dos Estados Ibero-Americanos", não procuram infringir o direito interno de cada país, propondo uma série de padrões flexíveis que possam facilitar sua adoção entre os Estados Ibero-Americanos (REDE IBERO-AMERICANA..., 2017, p. 5). Com isso, suas diretrizes orientadoras certamente serviram como inspiração para a edição da recente Lei Geral de Proteção de Dados brasileira, que entrará em vigor em 2020. Vale ressaltar que ao longo das duas últimas décadas, outros países da América Latina, tais como Argentina (ARGENTINA, 2000) e Uruguai (URUGUAI, 2008), já haviam adotado leis específicas que abordam a proteção

[45] Integram a Rede Ibero-Americana de Proteção de Dados, na condição de membros, entidades dos seguintes países: Andorra, Argentina, Chile, Colômbia, Costa Rica, Espanha, México, Peru, Portugal e Uruguai. Ocupam a categoria de observadores entidades da Argentina, Brasil, Equador, El Salvador, Guatemala, Honduras, México, Paraguai, República Dominicana, OEA, FIIAPP-EUROSOCIAL (Fundação Internacional e Ibero-Americana de Administração e Políticas Pública), EDPS, Conselho da Europa, Cabo Verde e São Tomé e Príncipe. Participam como representantes brasileiros a Ouvidoria-Geral da União, Ministério da Transparência, Fiscalização e Controladoria-Geral da União (REDE IBERO-AMERICANA..., 2019).

[46] A Rede Ibero-Americana de Proteção de Dados é um grupo de cooperação resultado do acordo firmado entre os representantes de quatorze países ibero-americanos que participaram do Encontro Ibero-americano de Proteção de Dados (EIPD), realizado em Antígua, Guatemala, entre os dias 1 e 6 de junho de 2003 (REDE IBERO-AMERICANA..., 2018, p. 1).

de dados pessoais de modo integral. Estes países, juntamente com o Brasil, eram membros integrantes do Mercado Comum do Sul (Mercosul) à época de sua fundação, em 1991, realizada através do Tratado de Assunção (BRASIL, 1991).

A Argentina mostrou seu pioneirismo em diversas iniciativas que evidenciam que a preocupação do país com relação à proteção de dados pessoais já vem de longa data. Além de ter sido o primeiro país mercosulino a contar com uma lei de proteção de dados pessoais (lei 25.326/2000), o país obteve o reconhecimento da União Europeia (COMISSÃO EUROPEIA, 2003) quanto à adequação do nível de proteção de dados pessoais[47], nos termos da Diretiva 95/46/CE, do Parlamento Europeu e do Conselho. Soma-se a isso a participação direta de um organismo não governamental argentino, na organização da reunião que resultou na Carta de Heredia, principal documento elaborado na América Latina sobre a difusão de informação judicial na *Internet,* que data de 2003.

Identificando-se a consolidação do modelo argentino, a partir dos predicados acima elencados, faz-se necessário examinar a legislação protetiva de dados pessoais vigente no país, especialmente no que se refere à tutela do trabalhador diante do tratamento de dados pelo Poder Judiciário, bem como os demais mecanismos que integram o sistema jurídico de proteção de dados pessoais no âmbito do processo laboral, estabelecendo-se um comparativo com o modelo brasileiro, cuja legislação ainda encontra-se em período de *vacatio legis.*

3.1 APORTE METODOLÓGICO DA PESQUISA COMPARATIVA: categorias de análise para o estudo comparado dos sistemas jurídicos de proteção de dados pessoais da Argentina e Brasil

O estabelecimento de um contraste entre os modelos argentino e brasileiro implica um necessário aprofundamento sobre o método comparativo aplicado à abordagem de sistemas jurídicos. A professora Ana Lucia de Lyra Tavares (2006, p. 61-2), pesquisadora do direito comparado, considera que este ramo do direito

> [...] se caracteriza pela aplicação do método comparativo a dois ou mais ordenamentos jurídicos nacionais, pertencentes, ou não, ao mesmo sistema jurídico. Busca identificar semelhanças e diferenças quanto a pontos específicos (microcomparação) ou em relação a traços diferenciais, estruturais ou históricos, de dois ou mais sistemas jurídicos (macrocomparação).

[47] A análise feita pela Comissão Europeia na certificação do nível de proteção adequado observa o respeito aos princípios protetivos de dados pessoais e aos direitos dos titulares, bem como a existência de meios compatíveis para garantir a aplicação da lei (SILVA, C. B., 2014, p. 130).

O estudo deve começar pela delimitação conceitual sobre o que se compreende por um sistema jurídico. A definição de sistema jurídico adotada pelos autores comparativistas, tais como René David (1998), é a de um "[...] conjunto mais ou menos amplo de legislações nacionais, unidas por uma comunidade de origem, de fontes, de concepções fundamentais, de métodos e de processos de desenvolvimento" (ANCEL, 2015, p. 58). Este conceito transcende a concepção restritiva de sistema jurídico enquanto o conjunto do direito de uma nação, formado por uma hierarquia que tem início pelas regras de direito e passa pela instituição, chegando, enfim, ao sistema jurídico nacional (ANCEL, 2015, p. 56).

Partindo da definição mais abrangente, René David (1998, p. 17) defende a existência de três sistemas jurídicos[48] proeminentes no mundo contemporâneo: a família romano-germânica, a família da *common law* e a família dos direitos socialistas, classificação que é acompanhada por Marc Ancel (2015, p. 60-3). Tendo a Europa como berço, a família romano-germânica expandiu-se por diversos países do mundo devido à conquista de territórios, o que incluiu não apenas o Brasil[49] e a Argentina, mas toda a América Latina (DAVID, 1998, p. 25).

A família romano-germânica agrupa os países cuja ciência do direito estruturou-se sob os pilares do direito romano, atribuindo um importante papel à lei, sistematizada por meio de codificações (DAVID, 1998, p. 17-8). Apesar do papel primordial atribuído à legislação, outras fontes do direito são reconhecidas pelos países adeptos desse sistema jurídico, quais sejam: o costume, a jurisprudência, a doutrina e os princípios gerais (DAVID, 1998, p. 91). Nesse sentido insere-se a lição de Caio Mário da Silva Pereira (1955, p. 37-8):

> O direito, ainda nos países de direito escrito como o Brasil, onde sua fonte primordial está na lei, não se limita a esta. Basta atentar em que a norma legislativa tem na verdade o sentido que a interpretação jurisprudencial lhe dá, para se ver que fará trabalho incompleto quem pretenda tirar conclusões do cotejo apenas de textos legais, com abstração da atividade das côrtes (*sic*) de justiça. Demais disso a doutrina, a elaboração científica, voando mais alto do que o legislador, e mais desembaraçada do que o juiz, formula a elaboração dogmática das instituições, dando mais idéia (*sic*) do estado de evolução do sistema jurídico.

[48] René David (1998, p. 17) utiliza a expressão "família de direito" para referir-se a cada um dos diferentes sistemas jurídicos da contemporaneidade.

[49] Ana Lucia de Lyra Tavares (1990, p. 56) lembra que o direito brasileiro, enquanto ordem jurídica secundária, ou seja, construído por influência de sistemas exportadores de direito, sempre recorreu ao direito comparado (em sentido estrito), o que fez com que René David por algum tempo o compreendesse como uma síntese de direitos europeus, vindo a rever a sua posição anos mais tarde para reconhecer a sua originalidade.

Além das fontes formais do direito, as fontes materiais[50] emergem dos fatos sociais, políticos, econômicos, culturais, éticos e morais de um determinado povo em cada período histórico, tornando-se fontes potenciais também ao processo trabalhista (LEITE, 2015, p. 60). Ao Direito comparado, portanto, importa observar a realidade dos sistemas jurídicos em seu conjunto, o que compreende não só a legislação, mas também a jurisprudência, o conhecimento do meio social, a prática contratual e a tendência da técnica jurídica (PEREIRA, C. M., 1955, p. 37).

Por conta disso, a abordagem de diferentes sistemas jurídicos, através da utilização do método comparativo, deve pautar-se por duas ordens de direção: inicialmente, pela apreensão global do sistema, seguindo-se por uma análise particular (ANCEL, 2015, p. 66). Nas palavras de Ancel (2015, p. 69), a "[...] compreensão global do sistema, em seus dados históricos e nas suas condições sócio-econômicas de aplicação, torna-se, destarte a condição primeira para uma utilização verdadeiramente científica do método comparativo". Mais do que uma análise das regras e instituições de um sistema, o estudo comparado demanda uma análise das formas do pensamento jurídico, na maneira pelo qual advogados, juízes e usuários do sistema o compreendem e o vivem (ANCEL, 2015, p. 69).

Nessa senda, um estudo que se proponha a investigar e comparar os sistemas jurídicos de proteção de dados pessoais no Brasil e na Argentina deve, além do confronto entre a legislação vigente nos dois países, aprofundar-se no exame dos instrumentos de disponibilização de informações processuais na *Internet*, cuja utilização permite a coleta de dados pessoais do trabalhador por terceiros alheios ao processo, principal ponto de atenção da pesquisa ora realizada. É por conta disso que se impõe a necessidade de observação e comparação entre os *sites* do Poder Judiciário trabalhista dos dois países latino-americanos, compreendendo-se a forma como cada país realiza a divulgação de informações processuais no âmbito da Justiça do Trabalho.

Ao final deste estudo comparado, pretende-se verificar se a novel legislação brasileira confere nível de proteção compatível com o seu vizinho mercosulino, revelando-se adequada e suficiente para garantir a proteção do trabalhador em face da coleta e tratamento de dados realizadas em razão do ajuizamento da reclamatória trabalhista, o que somente será possível através da análise conjunta dos resultados obtidos.

---

[50] Ainda que este trabalho aborde as fontes do direito de forma ampla, convém lembrar que existem posições em sentido contrário, como a de Miguel Reale (2002, p. 140-1), que não reconhece as fontes materiais como fontes do direito, por entender que toda fonte de direito pressupõe uma estrutura normativa de poder, enquanto as fontes materiais estariam ligadas ao fundamento ético ou social das normas jurídicas, situando-se fora do campo da Ciência do Direito.

No âmbito da pesquisa legislativa, o primeiro passo foi o estabelecimento de sete critérios de análise das Leis de Proteção de Dados Pessoais, escolhidos de acordo com a pertinência com o tema ora dissertado, quais sejam: 1) escopo de aplicação; 2) bases legais para o tratamento de dados; 3) tratamento de dados sensíveis; 4) direitos dos titulares dos dados; 5) princípios de proteção dos dados; 6) órgão regulador de proteção de dados e 7) tratamento de dados pelo Poder Público. Definidas estas categorias, o modelo pioneiro da Argentina será colocado em contraste com o modelo brasileiro e a sua *novel* legislação, à luz das contribuições doutrinárias pátrias.

Todo o aparato normativo examinado representa uma garantia em face do tratamento indevido de dados pessoais do trabalhador, mas a sua eficácia depende de providências que possam assegurar ao texto legal sua concretude. Ao tratarem informações pessoais de cunho sensível, os Tribunais de Justiça precisam observar critérios que possam impedir a utilização excessiva desses dados e a consequente violação de direitos fundamentais do jurisdicionado, o que se reflete nas formas de divulgação de informações pelos portais institucionais.

Na sequência, parte-se para uma observação sistemática, direta e não participante[51] dos portais dos tribunais judiciais trabalhistas do Brasil e Argentina, a fim de verificar em que medida os dois países garantem efetiva proteção ao trabalhador, especialmente aquele que ajuizou reclamação trabalhista anteriormente e que se encontra em posição de vulnerabilidade pela possibilidade de uso discriminatório de seus dados, divulgados ou repassados a terceiros pelo Poder Judiciário. Como a recente lei protetiva de dados pessoais brasileira encontra-se em período de *vacatio legis*, o estudo aqui apresentado tem o condão de identificar as falhas existentes no atual sistema brasileiro, que podem ser futuramente corrigidas com a correta aplicação e fiscalização da Lei nº 13.709/2018.

Como o estudo visa traçar um panorama geral acerca da forma como os Poderes Judiciários laborais da Argentina e do Brasil divulgam as informação pessoais dos trabalhadores, optou-se pela delimitação do campo de análise aos portais das Cortes Superiores do Poder Judiciário trabalhista dos dois países, quais sejam, o *site* do Poder Judicial de la Nación argentina (www.pjn.gov.ar) (ARGENTINA, 2019a), mediante a opção pela consulta dos julgados da Cámara Nacional de Apelaciones del Trabajo, e o *site* do Tribunal Superior do Trabalho brasileiro (www.tst.jus.br) (BRASIL, 2019c).

[51] A observação sistemática, também conhecida como "planejada", "estruturada" ou "controlada" é a técnica científica efetuada em condições controladas que busca responder a finalidades previamente definidas. Esta modalidade de observação será realizada de modo direto quando demanda a aplicação imediata dos sentidos sobre o fenômeno em análise. Na observação não participante, o observador aparece como um elemento externo, que vê o objeto como um espectador (RAMPAZZO, 2011, p. 111-3).

Para a avaliação dos *sites*, serão utilizadas três categorias de análise: 1) possibilidade de pesquisa pelo nome do reclamante, tanto na consulta processual como jurisprudencial; 2) adoção de solução de *captcha* para consultas em processos, acórdãos e jurisprudências, visando inibir a captura de dados por meio de consultas públicas, conforme recomendação da Resolução CSJT 139/2014 (CONSELHO..., 2014b); e 3) divulgação de dados sensíveis por meio da pesquisa jurisprudencial[52].

Com o objetivo de responder ao terceiro critério de análise elencado, optou-se pela eleição de uma palavra-chave que costuma conduzir ao tratamento de dados sensíveis, qual seja, "despedida discriminatória", no Brasil e "despido discriminatorio", na Argentina. Posteriormente, os resultados encontrados serão categorizados de acordo com os diferentes tipos de dados sensíveis, a fim de se observar o percentual de incidência de cada categoria nas consultas jurisprudenciais.

Por fim, diante da verificação de que, no Brasil, é possível o acesso a informações processuais, documentos, despachos e decisões em inteiro teor por meio de buscadores administrados por empresas privadas, de forma mais facilitada do que a própria divulgação dos Tribunais, serão observadas as principais funcionalidades do *site* "Escavador" (www.escavador.com) (ESCAVADOR, 2019), identificando-se a sua parcela de contribuição à violação de direitos fundamentais do trabalhador. A análise conjunta dos resultados alcançados levará ao estabelecimento de um panorama amplo e geral sobre os sistemas jurídicos de proteção de dados pessoais do trabalhador existentes em cada país, delimitando-se o objeto de estudo ao tratamento de dados que integram os processos judiciais disponibilizados no meio eletrônico.

3.2 O PIONEIRISMO DA ARGENTINA NA PROTEÇÃO DE DADOS PESSOAIS: da promessa normativa à realidade dos portais institucionais do Poder Judiciário trabalhista.

Ao tratar da proteção de dados pessoais em perspectiva comparada, a constatação de que a Argentina possui regulamentação específica deste tema desde o início da década de 2000 conduz ao seguinte questionamento: será possível vincular a existência de uma lei geral ao nível

[52] Optou-se pela delimitação do campo de pesquisa dos dados sensíveis ao âmbito da consulta jurisprudencial tendo em vista que não seria viável a utilização de nomes reais de reclamantes no campo de pesquisa processual. Ainda assim, é notório que a pesquisa processual dos *sites* dos Tribunais possibilita o acesso a despachos e decisões judiciais que contém informações pessoais do trabalhador, restando saber se essas informações estão disponíveis de forma facilitada a qualquer pessoa, nos casos em que é possível o acesso à tramitação processual por meio da pesquisa pelo nome do reclamante, ou não.

de proteção oferecido pelo Poder Judiciário trabalhista aos dados pessoais de seus jurisdicionados? Este será o debate enfrentado ao longo deste capítulo, tendo como ponto de partida um olhar sobre a evolução histórica da proteção de dados pessoais no país, e do sistema normativo atualmente vigente, com especial atenção à Lei nº 25.326/2000 (Lei de Proteção de Dados Pessoais).

3.2.1 O panorama normativo da proteção de dados pessoais na Argentina

A precursora legislação argentina protetiva de dados pessoais foi o fruto de uma construção histórica que teve início com o reconhecimento constitucional do direito à privacidade. O artigo 18 da Constituição da Nação Argentina, sancionada em 1853 (e que sofreu diversas reformas, nos anos de 1860, 1866, 1898, 1957 e 1994), contempla a inviolabilidade do domicílio e da correspondência, e o artigo 19 assegura que "As ações privadas dos homens que de nenhum modo ofendem a ordem pública e a moralidade, ou prejudicam um terceiro, são reservadas somente a Deus e isentas da autoridade dos magistrados[53]" (ARGENTINA, 1994). Estes dispositivos protegem uma concepção de privacidade ligada ao direito de ser deixado em paz, afastando as ingerências de terceiros sobre a vida privada do indivíduo.

Em 1994, a proteção constitucional da privacidade sintonizou-se ao novo paradigma informacional. A inserção do artigo 43 à Constituição da Nação argentina introduziu a garantia do *Habeas Data*[54], remédio constitucional que possibilita ao cidadão que tome conhecimento dos dados a ele referentes existentes em registros ou bancos de dados públicos, ou privados destinados ao fornecimento de informações, bem como seja informado acerca das finalidade da coleta de tais dados, com a possibilidade de exigir a exclusão, retificação, confidencialidade ou atualização dos registros (ARGENTINA, 1994). Trata-se de um duplo objetivo: por um lado, tomar conhecimento da existência de bancos de dados referentes à pessoa e suas finalidades; por outro, o direito de tomar as medidas cabíveis em caso de falsidade ou discriminação (SALTOR, 2013, p. 381).

---

[53] As traduções da legislação argentina utilizadas neste trabalho são traduções livres do autor. Do original: "Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados".

[54] A Constituição argentina não faz referência expressa ao termo *Habeas Data*, que é amplamente utilizado pela doutrina e jurisprudência pátria. Por isso, Gozaíni (2003, p. 166) defende que o *Habeas Data* não existe na Argentina, mas sim um subtipo de amparo na sua vertente protetora do dado, diferentemente da Constituição brasileira, em que foi incorporado como uma garantia autônoma. Ainda assim, Saltor (2013, p. 366) considera que a Constituição do Brasil de 1988 serviu como inspiração aos reformadores constitucionais argentinos para a introdução do artigo 43 à Carta Magna do país. O autor (2013, p. 376) classifica esta garantia como uma ação de *Habeas Data* inominada.

A inclusão do artigo 43 à Constituição da República argentina representa uma solução de compatibilização entre o direito à intimidade e o direito à informação, garantido pelo artigo 14 da Carta Magna. A colisão desses direitos fundamentais demanda uma proteção especial à intimidade, que resguarda o indivíduo do tratamento abusivo de seus dados pessoais, enquanto o direito à informação atua no sentido oposto, buscando justamente a coleta dessas informações (FERNÁNDEZ DELPECH, 2004, p. 279-80). Portanto, o *Habeas Data* resguarda o direito à intimidade do indivíduo, já que a vulnerabilidade do titular em virtude da utilização indevida e da publicidade de seus dados pessoais afeta seus direitos fundamentais, especialmente diante do avanço das tecnologias informacionais (SALTOR, 2013, p. 380).

No que se refere à legitimidade passiva da ação de *Habeas Data*, a Constituição não prevê exceções aos bancos de dados públicos, sendo cabível em face dos arquivos mantidos pela Administração Pública centralizada, descentralizada, autarquias, empresas públicas e sociedades estatais, em âmbito nacional, provincial e municipal. Quanto aos registros mantidos por entidades privadas, a norma estabelece que somente aqueles destinados a fornecer relatórios são acessíveis por meio da ação constitucional. Seu alcance abrange especialmente as empresas cuja atividade tem por finalidade o fornecimento de relatórios comerciais e financeiros a bancos e instituições de créditos, mas também podem ser incluídas os sindicatos, estabelecimentos de ensino e clubes desportivos (ALTMARK; QUIROGA, 1996, p. 1256-7).

No âmbito infraconstitucional, a inclusão do artigo 1071 bis[55] no Código Civil da República Argentina pela Lei nº 21.173, de 1975, representou o marco normativo inicial de proteção à intimidade (FERNÁNDEZ DELPECH, 2004, p. 283). O dispositivo utiliza a expressão "vida aleja" para referir-se às intromissões à intimidade e a violação de direitos personalíssimos da pessoa afetada, abrangendo sua imagem, dignidade, crenças, ideologia e documentação de caráter privado, devendo, necessariamente, implicar em alguma espécie de perturbação (SALTOR, 2013, p. 371). O Código Civil argentino de 1869 sofreu inúmeras modificações ao longo do tempo, até ser revogado, em 1° de agosto de 2015, pela Lei nº 26.994, com a entrada em vigor do atual Código Civil e Comercial da Nação (ARGENTINA, 2014).

No novo Código Civil e Comercial da Nação argentina, o direito à intimidade está inserido no capítulo 3, que trata dos Direitos e atos personalíssimos. A inviolabilidade da pessoa

[55] Art.1071 bis.- El que arbitrariamente se entrometiere en la vida ajena, publicando retratos, difundiendo correspondencia, mortificando a otros en sus costumbres o sentimientos, o perturbando de cualquier modo su intimidad, y el hecho no fuere un delito penal, será obligado a cesar en tales actividades, si antes no hubieren cesado, y a pagar una indemnización que fijará equitativamente el juez, de acuerdo con las circunstancias; además, podrá éste, a pedido del agraviado, ordenar la publicación de la sentencia en un diario o periódico del lugar, si esta medida fuese procedente para una adecuada reparación (ARGENTINA, 1975).

humana e o reconhecimento da sua dignidade constituem a base sobre a qual se alicerça todo o capítulo, devendo ser o guia norteador do alcance de todos os direitos personalíssimos ali elencados (CÁNEPA, 2015, p. 42). O artigo 52, que trata das afetações à dignidade, "direitos à personalidade espiritual", como denomina Rivera (2012, p. 152), ou "direitos da integridade espiritual", vide Navarro Floria (2012, p. 110), elenca a proteção da "intimidade pessoal ou familiar", introduzindo o elemento de proteção à família, com a garantia da prevenção e reparação dos danos sofridos. A reparação de danos também possui previsão no artigo 1740, garantindo que no caso de ofensa à intimidade o juiz poderá, a pedido da parte, ordenar a publicação da sentença ou das suas partes pertinentes às custas do responsável (ARGENTINA, 2014).

A proteção específica da intimidade encontra-se no artigo 1770 do Código Civil e Comercial da Nação, que garante a proteção da vida privada, com a devida indenização (ARGENTINA, 2014). Observa-se que o legislador preocupou-se em descrever algumas formas de violação da intimidade, tais como a intromissão arbitrária na vida alheia, a publicação de fotos, a divulgação de correspondências e a lesão aos costumes e sentimentos de outra pessoa, mas este não se trata de um rol exaustivo, já que expressamente veda a perturbação da intimidade de qualquer outro modo. Tal como ocorre na legislação brasileira, o Código Civil e Comercial da Nação argentina utiliza os termos "intimidade" e "vida privada", mas não faz uso da expressão "privacidade".

Com relação à legislação trabalhista na Argentina, a Lei nº 20.744 (ARGENTINA, 1974), sancionada em setembro de 1974 (Lei do Contrato de Trabalho), é uma normativa geral que regula as relações de trabalho, sistematizando os diferentes regulamentos sobre o contrato de trabalho que anteriormente estavam dispersos na legislação. A Lei do Contrato de Trabalho é uma espécie de "núcleo" regulatório, sendo complementada por estatutos especiais específicos, destinados a regulamentar algumas categorias profissionais, ou por leis esparsas, tal como a Lei nº 11.544/1929 (ARGENTINA, 1929), conhecida como a Lei da Jornada de Trabalho.

Na Lei do Contrato de Trabalho argentina, algumas normas podem ser diretamente relacionadas à proteção de dados pessoais do empregado[56]. Merece um primeiro destaque o artigo 17, que proíbe qualquer tipo de discriminação do trabalhador motivada por sexo, raça,

[56] Além dos dispositivos referidos, merece menção o artigo 70 da Lei nº 20.744, cuja abordagem direciona-se aos sistemas de controle pessoal do trabalhador, destinados à proteção dos bens do empregador, os quais devem ser praticados com discrição, por meio de seleção automática entre todos os funcionários, de forma a proteger a dignidade do trabalhador. As práticas devem ter o conhecimento do trabalhador, nos termos do artigo 71 (ARGENTINA, 1974).

nacionalidade, religião, política, associações ou idade (ARGENTINA, 1974). Ao garantir o direito à igualdade e à não discriminação do trabalhador, o dispositivo vai ao encontro das normativas europeias de proteção de dados, que erigiram o princípio da não discriminação como um de seus norteadores, garantindo a proteção dos dados sensíveis do trabalhador. A lei, no artigo 17 bis, também faz menção implícita ao princípio da proteção do trabalhador e à busca por igualdade material, ao dispor que as desigualdades criadas pela lei em favor de uma das partes são formas de compensar desigualdades criadas, por si só, na própria relação de trabalho (ARGENTINA, 1974).

Assim, a norma deve ser aplicada em conjunto com o artigo 63, que estabelece o princípio da boa-fé nas relações de trabalho, o que pode ser estendido ao tratamento de dados pessoais do empregado no âmbito do contrato laboral. O texto legal faz menção expressa à obrigatoriedade de se agir com boa-fé tanto na celebração do contrato de trabalho (fase pré-contratual), durante a sua execução e após a sua extinção (fase pós-contratual) (ARGENTINA, 1974). Da conjugação dos dispositivos em tela, pode-se inferir que os princípios da não discriminação e da boa-fé devem conduzir a tomada de decisões do empregador em todas as etapas do contrato laboral, o que contempla o tratamento de dados pessoais antes mesmo da contratação (etapa em que ocorrem os processos seletivos e a busca de informações pessoais do candidato).

Por esse motivo, o artigo 73 determina que o empregador não pode, no momento da contratação, durante a vigência do contrato, ou na dissolução contratual, realizar questionamentos sobre preferências políticas, religiosas, sindicais, culturais ou sexuais do trabalhador. O dispositivo garante ainda o direito à liberdade de expressão do empregado, que poderá expressar livremente suas opiniões sobre tais aspectos no local de trabalho, desde que isso não interfira no desenvolvimento normal das tarefas (ARGENTINA, 1974). Trata-se de regulamentação que assegura a proteção de dados sensíveis do empregado, especialmente no que se refere às ingerências diretas do empregador. Este artigo, somado à proibição da discriminação e à previsão da boa-fé, possuem importante papel na proteção da privacidade do trabalhador, que muitas vezes se vê alvo de intromissões que podem constituir-se em ameaças a seus direitos de personalidade.

Em 04 de outubro de 2000 foi sancionada a Lei nº 25.326 (ARGENTINA, 2000), conhecida como Lei de Proteção de Dados Pessoais, que estabeleceu um marco normativo para a proteção de dados pessoais na Argentina[57]. A lei foi regulamentada pelo Decreto

[57] O sistema federativo argentino também permite às províncias legislarem acerca da proteção de dados pessoais e do Habeas Data (DONEDA, 2006, p. 347). Observa-se, por exemplo, que a cidade de Buenos Aires possui a sua

Regulamentar nº 1558/2001, editado em 29 de novembro de 2001 (ARGENTINA, 2001). Esta iniciativa foi precursora na América Latina, tornando-se a primeira lei a regular a proteção de dados pessoais no continente e assumindo grande influência da Diretiva 46/95 CE, do Parlamento e do Conselho Europeu e da lei de proteção de dados espanhola (lei orgânica 15/1999)[58] (FERNÁNDEZ DELPECH, 2004, p. 286).

Seus dispositivos desenvolvem e ampliam as garantias constitucionais, dispondo, a exemplo da normativa da União Europeia, sobre princípios gerais relativos à proteção de dados pessoais, direitos dos titulares dos dados, responsabilidade sobre os arquivos, registros e bancos de dados e sanções, dentre outros, além de disciplinar o *Habeas Data* (ação de proteção de dados pessoais), conforme o artigo 43 da Constituição da Nação Argentina.

É importante destacar que a legislação argentina não dispõe de normas especiais para a regulamentação do direito de privacidade na *Internet*, objeto principal de estudo da presente dissertação. A jurisprudência argentina oferece aos direitos de *Internet* o mesmo tratamento outorgado a outros meios, tais como televisão e imprensa, equiparando a rede mundial de computadores e os serviços nela prestados aos arquivos, bancos de dados e outros meios técnicos de tratamento de dados, termos encontrados na redação do artigo 1º da Lei nº 25.326/2000 (CARRASQUILLA, 2012, p. 144). Feita esta ressalva, a Lei de Proteção de Dados argentina será analisada a partir das sete categorias anteriormente definidas, visando um posterior contraste com a novel legislação brasileira, a começar pelo escopo de aplicação.

No que se refere ao âmbito de aplicação material, o artigo 1º da Lei de Proteção de Dados Pessoais argentina inspira-se no artigo 43 da Constituição do país, delimitando a sua abrangência aos bancos de dados públicos e privados destinados a fornecer informações (ARGENTINA, 2000). Interpretando este dispositivo em cotejo com o artigo 24 da mesma normativa e com o Decreto Regulamentar nº 1558/2001, Fernández Delpech (2004, p. 287-8), sustenta que estão ao abrigo da lei todas as bases de dados que não se destinam ao uso estritamente pessoal, o que contempla todos os arquivos que alcancem pessoas distintas do seu

própria Lei de Proteção de Dados Pessoais, a Lei nº 1845, de 24 de novembro de 2005 (BUENOS AIRES, 2005). A lei regula o tratamento de dados pessoais dentro do âmbito da capital argentina, relacionando-se às informações que se encontrem em arquivos, registros ou bancos de dados do setor público da cidade (artigo 1°).

[58] Por entender que a Lei nº 25.326/2000 sofreu principal influência da lei espanhola de 1999, própria da segunda geração de leis de proteção de dados, e menos na Diretiva 95/46 CE, normativa representativa da terceira fase, ainda que esta tenha impulsionado a iniciativa de sua regulamentação, Fernando Maresca (2003, p. 284-5) afirma que a legislação argentina já nasceu obsoleta. Para o doutrinador argentino (2003, p. 285-6), a diretiva europeia demonstrava preocupação com o desenvolvimento comercial dos países-membros por meio do estabelecimento de um equilíbrio entre o padrão protetivo das legislações diante do papel fundamental exercido pela informação na nova economia, o que não faz a lei da Argentina.

titular, incluindo as bases de dados relativas a atividades sociais ou econômicas e aquelas que prevejam a transferência gratuita ou onerosa de dados a terceiros.

Com o mesmo entendimento, Pablo Palazzi (2003, p. 129-31) defende uma interpretação ampla do dispositivo legal, estendendo o âmbito de aplicação da lei a todos os dados que excedam o uso pessoal, sem que necessariamente façam parte de banco de dados destinado especificamente a fornecer informações a terceiros. É o que ocorre, por exemplo, com os dados de empregados mantidos nos sistemas empresariais, os dados sensíveis de pacientes mantidos por hospitais, sanatórios e médicos e o armazenamento de dados de navegação dos usuários por *sites* de *Internet*. A lição doutrinária permite inferir que estão sob a proteção legal não apenas os dados pessoais tratados pelo Poder Judiciário, mas também aqueles que são disponibilizados por *sites* jurídicos, contemplando integralmente o objeto deste estudo.

Ainda que a lei seja omissa quanto ao seu alcance territorial[59], é possível deduzir que sua proteção compreende somente as bases de dados existentes dentro do território argentino, sejam seus titulares nacionais ou estrangeiros, residentes ou não no país (FERNÁNDEZ DELPECH, 2004, p. 288). Por se tratar de uma normativa mais antiga, a lei argentina apresenta uma defasagem em relação ao novo Regulamento Geral de Proteção de Dados da União Europeia, que apresenta um âmbito de aplicação extraterritorial, garantindo maior proteção ao cidadão europeu diante do caráter transnacional[60] que passa a ter a coleta de dados pessoais com o avanço tecnológico.

Adentrando-se na análise do segundo critério estipulado, qual seja, as bases legais para o tratamento de dados, o artigo 5º, inciso 1º[61] estabelece o consentimento livre, expresso e

---

[59] O artigo 44, que trata do âmbito de aplicação da lei, estipula apenas que as normas contidas nos Capítulos I, II, II e IV e o artigo 32 são aplicáveis em todo o território nacional. Com isso, os capítulos V, parte do VI e o VII, que se referem ao órgão de controle, sanções administrativas e à ação de proteção de dados pessoais (Habeas Data), poderão ser regulados pelas leis provinciais, ou da Cidade Autônoma de Buenos Aires, no caso da base de dados não abranger mais de uma jurisdição (FERNÁNDEZ DELPECH, 2004, p. 288).

[60] O artigo 12 da Lei nº 25.326/2000 (ARGENTINA, 2000) veda a transferência internacional de dados para países que não possuem uma legislação adequada ao nível da Lei argentina, o que assemelha-se à exigência do Regulamento Geral europeu.

[61] "ARTICULO 5° — (Consentimiento).
1. El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias.
El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el artículo 6° de la presente ley.
2. No será necesario el consentimiento cuando:
a) Los datos se obtengan de fuentes de acceso público irrestricto;
b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal;
c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio;
d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necessários para su desarrollo o cumplimiento;

informado do titular como o principal requisito para a licitude do tratamento. Esta manifestação poderá ser feita por escrito ou por outro meio equiparável, de forma destacada de outras declarações (ARGENTINA, 2000). O Decreto Regulamentar nº 1558/2001 disciplinou a possibilidade de revogação do consentimento, prevista no artigo 11, inciso 2, da lei, o que poderá ocorrer a qualquer tempo, sem efeitos retroativos (ARGENTINA, 2001).

O consentimento prévio do trabalhador é um requisito para as atividades de vigilância implementadas pela empresa no ambiente laboral, dentre elas o monitoramento dos *sites* visitados pelo empregado, ou o controle de seu correio eletrônico. A estes casos, é cabível a aplicação dos dispositivos previstos no artigo 5º e 6º da Lei de Proteção de Dados argentina (CABANELLAS DE LAS CUEVAS; PALAZZI, 2012, p. 53). Semelhante tratamento deve ser estendido ao processamento dos dados fornecidos ao Poder Judiciário, que necessita se submeter ao expresso consentimento do jurisdicionado, específico com relação à finalidade de divulgação pública em seus portais institucionais, via consultas processuais e jurisprudenciais

O conteúdo essencial do requisito de consentimento prévio, no entendimento de Esteban Ruiz Martínez (2003, p. 102), é a proteção dos demais direitos[62] afetados diretamente pelo tratamento de dados pessoais, tais como a própria intimidade ou a liberdade. É o que ocorre nas situações que envolvem a divulgação de dados pessoais sensíveis, por exemplo. Nos demais casos, quando não há a tutela expressa de um direito determinado, o consentimento atua como ferramenta de prudência para o exercício do direito de controlar as informações pessoais (MARTÍNEZ, 2003, p. 103).

Além do consentimento, o inciso 2º do artigo 5º estabelece outras hipóteses que autorizam o tratamento de dados pessoais, quais sejam: a) quando os dados forem obtidos de fontes de acesso público irrestrito; b) sua coleta for necessária para o exercício de funções próprias dos poderes do Estado ou em virtude de uma obrigação legal; c) os arquivos limitarem-se ao nome, documento de identidade, identificação tributária ou previdenciária, ocupação, data de nascimento e domicílio; d) derivem de uma relação contratual, científica ou profissional do proprietário dos dados e forem necessários para o seu desenvolvimento ou cumprimento; e) no caso de operações realizadas por instituições financeiras e as informações recebidas de seus clientes (ARGENTINA, 2000).

---

e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley 21.526" (ARGENTINA, 2000).

[62] Carlos Bruno Ferreira da Silva (2014, p. 76) ressalta que o caráter instrumental do direito à autodeterminação informativa como ferramenta protetiva de outros direitos não deve servir de obstáculo para que se reconheça a sua autonomia, especialmente quando todos os direitos fundamentais são, de alguma forma, instrumentais à dignidade da pessoa humana, ao passo que são igualmente autônomos.

Algumas críticas podem ser feitas às exceções listadas pelo artigo, a começar pela alínea "a", que permite o tratamento de dados sem consentimento nos casos em que forem obtidos de fontes de acesso público irrestrito. Para Basterra (2004, p. 16), as fontes de acesso público irrestrito são aquelas que não trazem impedimentos formais ou tampouco substanciais para que qualquer interessado as consulte. A autora considera que esses bancos de dados podem conter informações que reconheçam certas restrições de acesso, tais como os dados sensíveis, sendo, neste caso, necessário o consentimento do titular, não em virtude do registro, mas sim da qualidade do dado (BASTERRA, 2004, p. 16).

No caso do tratamento de dados pela Justiça do Trabalho, este dispositivo refere-se aos dados que compõe o seu dever de publicidade e transparência, incluindo informações administrativas e até mesmo processuais, mas de forma alguma pode abarcar os dados pessoais dos jurisdicionados, especialmente os sensíveis ou aqueles que combinados podem levar à sua discriminação, pois tratam-se de informações não dotadas de interesse público. Some-se a isso o fato de que a administração pode atingir o mesmo resultado utilizando-se de técnicas menos lesivas ao jurisdicionado, como a dissociação de dados, definida pela lei em seu artigo 2º como todo o tratamento de dados pessoais de modo que a informação obtida não possa ser associada a uma pessoa identificada ou identificável (ARGENTINA, 2000).

Com relação à alínea "b", que contempla os dados coletados pela administração pública para o exercício das suas funções, percebe-se um dispositivo vago que acaba por delegar ao próprio Estado a definição de quais dados são necessários ou não para o exercício de suas funções. O dispositivo deve ser interpretado de maneira restritiva, lembrando que "La actividad estatal no significa que todos los organismos estén libres de requerir autorización, sino, que sólo podrá exceptuarse en los términos estrictos que la propia ley estabelece (BASTERRA, 2004, p. 18). Portanto, Basterra (2004, p. 18-9) defende uma interpretação conjunta deste dispositivo com o artigo 23 inciso 2º, entendendo ser cabível o tratamento de dados sem consentimento somente para os casos que envolvam defesa nacional, segurança pública ou repressão de delitos, excetuando-se os dados sensíveis, cujo tratamento jamais poderia ser autorizado (somente após o procedimento de dissociação de dados).

Ainda que o dispositivo possa justificar o tratamento de dados pelo Poder Judiciário, sem o consentimento do reclamante, vale lembrar que este deve limitar-se às finalidades de interesse público, o que abrange tão somente a função jurisdicional, devendo ser informado e consentido pelo titular qualquer outra espécie de tratamento. Outro ponto controverso é a previsão da alínea "c", que autoriza o tratamento de informações pessoais do titular, tais como nome, número de documentos pessoais, profissão e endereço, sem o seu devido consentimento,

o que pode facilmente ser convertido em ameaça aos dados sensíveis por meio da mineração de dados. Acerca desses dados, Piccirilli e Quiroga (2015, p. 232) ponderam:

> A primera vista este tipo de datos personales parecen comunes, no obstante no debemos subestimarlos dado que con ellos puede tenerse un mapa casi completo del comportamento de un ciudadano. Es por ello que incluso un número de DNI puede permitir inmiscuirse en la esfera de la privacidad de una persona (del cual podrán desprenderse otros datos como ser: domicilio completo, lugar de trabajo, tenencia de cuentas bancarias, bienes muebles e inmuebles y/o servicios a su nombre, entre otras).

Portanto, as regras acima referidas acabam por flexibilizar o tratamento de dados pela Justiça do Trabalho, já que não indicam qualquer restrição ou cuidado a serem tomados, o que demonstra um baixo nível protetivo dispensado aos dados pessoais dos jurisdicionados, especialmente diante de seu alto potencial discriminatório.

Uma vez examinado o segundo critério, passa-se para a terceira categoria de análise, relacionada ao tratamento de dados sensíveis, que são definidos pelo artigo 2º da lei[63] como aqueles "[...] que revelam origens raciais e étnicas, opiniões políticas, convicções religiosas, filosóficas ou morais, afiliação sindical e informação referente à saúde ou à vida sexual[64]". Os dados sensíveis apresentam-se sob um regime de proteção mais severo, havendo a expressa garantia de que ninguém é obrigado a fornecê-los (artigo 7º, inciso 1º), além da proibição com relação à coleta, tratamento e formação de arquivos, bancos ou registros que armazenem informações que direta ou indiretamente revelem dados sensíveis (incisos 2º e 3º do artigo 7º) (ARGENTINA, 2000). Com isso, a lei adota o princípio da proibição da coleta de dados sensíveis, estabelecendo a responsabilidade objetiva dos registros no caso de danos causados aos titulares, como a sua divulgação ilegal (SALTOR, 2013, p. 396).

A primeira permissão legal ao tratamento de dados sensíveis (exceção à regra geral de vedação ao tratamento) é o caso de existência de razões de interesse geral autorizadas por lei[65],

---

[63] Fernández Delpech (2003, p. 147) defende o caráter taxativo do enunciado legal, não podendo ser incluídos no conceito de dados sensíveis outros que não estejam especificamente mencionados no artigo 2º. O autor ressalva, entretanto, que os dados pessoais íntimos não sensíveis, ainda que não se enquadrem em uma das hipóteses legais, contam com a proteção legal dentro do regime geral de proteção de dados, na medida em que seu conteúdo pode originar condutas discriminatórias.

[64] Do original: "Datos sensibles: Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

[65] "ARTICULO 7° — (Categoría de datos).

1. Ninguna persona puede ser obligada a proporcionar datos sensibles.

2. Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares.

conforme o artigo 7º, inciso 2º (ARGENTINA, 2000). Diante do direito do titular de negativa ao fornecimento de dados sensíveis, previsto no inciso 1º, esta exceção deve ser interpretada no sentido de que é possível o recolhimento de dados sensíveis se existirem circunstâncias definidas pelo Estado como de interesse geral (o que pode ser visto como um ponto abstrato e nebuloso da lei), ressalvado o direito do titular de negar-se a proporcioná-los, ainda que possam ser distribuídos por terceiros (FERNÁNDEZ DELPECH, 2003, p. 155).

Esse dispositivo atribui poderes ao Estado na definição das circunstâncias que seriam ou não de interesse geral, o que se mostra uma ameaça aos direitos individuais dos cidadãos, vulneráveis aos alvedrios do Poder Público. A imprecisão da norma atende aos interesses de governos autoritários, revelando uma perigosa porta de entrada para práticas antidemocráticas, incluindo a vigilância eletrônica e o tratamento de dados para fins de categorização social. A outra exceção[66] prevista pelo artigo 7º, inciso 2º (ARGENTINA, 2000), que diz respeito ao tratamento para finalidades estatísticas ou científicas, quando os seus titulares não puderem ser identificados, também é passível de críticas, na medida em que, atualmente, diante das diversas possibilidades tecnológicas de manipulação de dados pessoais, qualquer dado, ainda que aparentemente anônimo, pode levar à identificação de seu titular quando recombinado ou reagrupado.

A análise conjunta do artigo 7º com o artigo 5º da Lei nº 25.326/2000, que trata da licitude do tratamento de dados mediante o consentimento do titular, permite concluir que nem mesmo o consentimento expresso autoriza o tratamento e a formação de arquivos, bancos e registros de dados sensíveis nos casos não relacionados pela normativa, já que não há a previsão legal do consentimento como uma das exceções elencadas no rol taxativo (FERNÁNDEZ DELPECH, 2003, p. 154). Com isso, ainda que o empregado autorizasse expressamente a distribuição de dados sensíveis que integram os processos judiciais em *sites* da internet, a legislação argentina vedaria expressamente essa prática. O tema é controverso e encontra posições doutrinárias divergentes, como a de Gustavo Tanús (2003, p. 243), que entende ser

3. Queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles. Sin perjuicio de ello, la Iglesia Católica, las asociaciones religiosas y las organizaciones políticas y sindicales podrán llevar un registro de sus miembros.
4. Los datos relativos a antecedentes penales o contravencionales sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas" (ARGENTINA, 2000).

[66] Os incisos 3º e 4º do artigo 7º da lei de proteção de dados argentina trazem mais duas exceções à proibição de formação de arquivos, registros ou bancos de dados sensíveis, referindo-se, respectivamente, aos registros mantidos por associações religiosas, políticas e sindicais e aos antecedentes penais ou contravencionais. Além disso, o artigo 8º da mesma lei permite o tratamento de dados relativos à saúde de pacientes, mantidos por estabelecimentos públicos e privados de saúde e profissionais ligados a esta área (ARGENTINA, 2000).

possível a inclusão de informações sensíveis de uma pessoa em bases de dados, mediante o consentimento livre, expresso, informado e por escrito do titular.

Os direitos dos titulares dos dados, quarta categoria de análise elencada, estão previstos no Capítulo III da Lei nº 25.326, que contempla os direitos de informação (artigo 13), acesso (artigo 14), retificação, atualização ou supressão (artigo 16). Portanto, a lei garante ao titular o direito de ser informado com relação à existência de bancos de dados e suas finalidades, podendo obter informações sobre os seus dados armazenados por entidades públicas e/ou privadas, o que deve ser respondido no prazo de dez dias após a solicitação, e ainda requerer a retificação ou a atualização de dados incorretos, bem como a supressão ou a confidencialidade de dados que não deseja divulgar. O procedimento de retificação ou supressão de dados incorretos deve ser cumprido pelo responsável pelo tratamento dos dados em até cinco dias úteis do recebimento da reclamação, sendo que o descumprimento da solicitação autoriza o titular dos dados a impetrar a ação de *Habeas Data*, nos termos do artigo 16 (ARGENTINA, 2000).

Estes dispositivos contemplam uma etapa extrajudicial para o exercício do direito de acesso, através de solicitação direta ao titular do banco de dados. Por outro lado, havendo negativa expressa ou o silêncio do responsável pelo tratamento, ou quando houver o acesso por terceiros a dados sensíveis sem o consentimento do titular, é possível o ajuizamento da ação judicial de proteção de dados pessoais (*Habeas Data*), prevista no capítulo VII da lei (SALTOR, 2013, p. 427). Portanto, o texto legal permite a interpretação de que o ingresso do *Habeas Data* pressupõe o prévio esgotamento das tentativas pela via administrativa (ALBUQUERQUE; PALAZZI, 2003, p. 556).

O artigo 16, inciso 5, estipula duas exceções ao direito de supressão de dados: quando puder causar prejuízo a interesse legítimo de terceiros, ou quando houver uma obrigação legal de conservação dos dados (ARGENTINA, 2000). Ainda que se pudesse entender como legítimo o interesse do cidadão em ter acesso aos dados judiciais, as informações pessoais dos jurisdicionados não são de interesse público e o seu acesso por terceiros viola direitos fundamentais, o que garante o direito do trabalhador de ter seus dados pessoais ocultados das decisões divulgadas pela *Internet*.

A quinta categoria de análise é referente aos princípios de proteção de dados, que podem ser extraídos do Capítulo II da Lei nº 25.326/2000: princípio da pertinência ou princípio da proporcionalidade e qualidade dos dados (artigo 4º, inciso 1º), princípio da finalidade (artigo 3º, parágrafo 2º), princípio da utilização não abusiva (art. 4º, inciso 3º), princípio da exatidão

(artigo 4º, incisos 4º e 5º), princípio do direito ao esquecimento[67] ou princípio da limitação no tempo (artigo 4º, inciso 7º), princípio da legalidade ou princípio da limitação da coleta (artigo 4º, inciso 2º), princípio da segurança (artigo 9º, inciso 2º) e princípio do consentimento (artigo 5º) (TANÚS, 2003, p. 247-253). Os princípios gerais relativos à proteção de dados pessoais determinam que os dados pessoais devem ser certos, adequados, pertinentes e não excessivos em relação às finalidades da coleta; recolhidos de modo leal e não fraudulento; utilizados somente para os fins que motivaram a coleta; exatos e atualizados (no caso de serem total ou parcialmente inexatos, devem ser suprimidos, substituídos ou completados), incluindo a exigência de consentimento como elemento central da lei (PALAZZI, 2003, p. 550).

Para Saltor (2013, p. 406), o princípio da boa-fé figura junto ao lógico objetivo legal de proteger os dados pessoais, já que é coerente a exigência do consentimento do titular para a cessão de dados, salvo casos excepcionais. Tanto a boa-fé como os demais princípios elencados no capítulo II da lei são vetores interpretativos que devem guiar o tratamento de dados pessoais por parte do empregador e o Poder Público, ainda que a inexistência de mecanismos específicos de regulação acabem por dificultar o seu concreto cumprimento pelos diversos atores que realizam armazenam e repassam dados pessoais do reclamante no decurso de um processo laboral.

Ademais, apesar de apresentar uma carta de princípios progressistas e protecionistas, a quantidade de exceções previstas na lei dificulta o amparo dos direitos personalíssimos, sendo esta uma deficiência legal denunciada por Piccirilli e Quiroga (2015, p. 238). Nesse sentido, as bases de dados públicas tendem a reunir maior número de informações sobre os cidadãos (quantitativa e qualitativamente, já que abrange grande quantidade de dados sensíveis), resultando também ser as detentoras do maior número de exceções ao consentimento do titular, o que exige o incremento do controle sobre os bancos de dados públicos (PICCIRILLI; QUIROGA, 2015, p. 243).

Se a lei contempla a expressa previsão dos princípios da proporcionalidade, finalidade e utilização não abusiva, determinando que a coleta e o tratamento de dados devem ser proporcionais à finalidade perseguida, sem que a sua utilização seja vinculada a propósitos distintos daqueles informados ao titular dos dados (TANÚS, 2003, p. 247-8), tal disposição deve ser observada pela Justiça do Trabalho quando manipula os dados de jurisdicionados, já que a publicidade da sua atuação não é justificativa para a exposição pública de informações de

[67] Puccinelli (2012, p. 9) defende que o direito ao esquecimento foi expressamente incluído na Lei 25.326/2000 através de seu artigo 4º, inciso 7º, que determina que: "Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados" (ARGENTINA, 2000).

caráter íntimo do trabalhador. Ao ingressar com uma demanda judicial, o reclamante, via de regra, demonstra total desconhecimento com relação ao tratamento que será oferecido às informações disponibilizadas, e certamente não o faz imaginando a divulgação pública desses dados via *Internet*.

Outro dispositivo que carece de uma maior aplicação prática é o que está inserido no artigo 4º, inciso 7º da lei, ao estabelecer um princípio do direito ao esquecimento ou princípio da limitação no tempo, já que determina a destruição dos dados após deixarem de ser necessários ou pertinentes para as finalidades de sua coleta (ARGENTINA, 2000). A norma refere-se à prática habitual de formação lícita de bancos de dados de grande capacidade, sem que haja o devido descarte dos dados após a sua utilização, o que contraria o dispositivo legal, conforme destacam Piccirilli e Quiroga (2015, p. 231). Os autores (2015, p. 231) entendem que este problema evidencia uma deficiência legal, que habilita a retenção ilícita de dados, por isso a importância de se exercer um controle sobre a duração do armazenamento dos dados[68]. Vale ressaltar que a lei não regula com especificidade o tempo de duração do armazenamento de dados, limitando-se a vinculá-lo às finalidades da coleta. É este o caso das informações sensíveis que integram processos que há muito foram extintos e seguem indexadas aos seus nomes em bancos de jurisprudência disponibilizados na *Internet*, não se encontrando qualquer necessidade para a sua manutenção, o que contraria expressamente o texto legal.

Além dos citados, o artigo 6º da LPD ainda estabelece o princípio da informação, que consiste na necessidade do responsável franquear ao titular dos dados todas as informações relacionadas ao tratamento, incluindo as suas finalidades, a existência de bancos de dados ou qualquer outra forma de registro, bem como a identidade e domicílio do responsável, o caráter obrigatório ou facultativo das respostas ao questionário, as consequências de proporcionar os dados, da sua negativa ou de sua inexatidão e a possibilidade do interessado exercer os direitos de acesso, retificação e supressão dos dados (ARGENTINA, 2000). Este princípio acaba por ser o elemento central do exercício da autodeterminação informativa pelo titular, sem o qual o direito de acesso e a própria proteção de dados pessoais resultam utópicos, uma vez que o conhecimento acerca da manutenção de bancos de dados a seu respeito, e a identificação dos responsáveis, são fatores indispensáveis para que o titular possa ter a mínima possibilidade de avaliar se os registros possuem as características de qualidade, tais como adequação, exatidão, pertinência e vinculação à finalidade da coleta (PICCIRILLI; QUIROGA, 2015, p. 234).

[68] Piccirilli e Quiroga (2015, p. 244) sugerem a realização de controles periódicos por parte da autoridade de aplicação, a fim de certificar a vigência da finalidade que permitiu a coleta dos dados, analisando se é o caso de proceder a destruição dos dados ou se é cabível que o tratamento subsista por tempo maior.

É justamente para garantir a correta aplicação e vigilância do cumprimento de tais dispositivos legais que reside a importância do estabelecimento de um órgão de fiscalização da lei, entidade que figura nas principais normativas editadas na União Europeia e que foi, por conta disso, incluída como quinta categoria de análise deste trabalho. Nesse diapasão, o artigo 29 da Lei nº 25.326/2000 estabelece a criação de um órgão de controle responsável pelas ações necessárias ao cumprimento da lei, tais como o assessoramento das pessoas acerca dos meios disponíveis para a proteção de seus dados pessoais[69], a criação de normas e regulamentações visando o desenvolvimento das atividades compreendidas pela lei, o controle da observância das normas de integridade e segurança dos dados por parte dos arquivos, registros ou bancos de dados e a imposição de sanções administrativas no caso de violações à lei, dentre outros (ARGENTINA, 2000).

A criação de um órgão de controle proposta pela Lei de Proteção de Dados Pessoais argentina é uma iniciativa pioneira na América Latina, conforme reconhece Danilo Doneda (2006, p. 351). Verifica-se que a redação original do artigo 29, 2 da Lei nº 25.326/2000 previa que o órgão seria dotado de autonomia funcional, atuando de forma descentralizada, ligado à estrutura do Ministério da Justiça e Direitos Humanos da Nação (ARGENTINA, 2000). Entretanto, o ponto foi vetado pelo Poder Executivo[70], sob o argumento de que a incorporação de um órgão descentralizado implicaria em um aumento nas despesas estatais, o que não estava previsto no orçamento governamental. Assim, o órgão opera, atualmente, no âmbito da Secretaria de Assuntos Registrais, sob a dependência do Ministério da Justiça e Direitos Humanos (FERREYRA, 2019, p. 18).

Com isso, ao atuar de forma vinculada ao Poder Executivo nacional (ALBUQUERQUE; PALAZZI, 2003, p. 559), integrando um de seus Ministérios, o órgão de controle tem comprometida a sua independência, tão necessária ao cumprimento das atribuições fiscalizatórias, especialmente com relação ao tratamento de dados pelo Poder Público, o que repercute diretamente na (in)efetividade da lei. Trata-se de um ponto crucial que diferencia os modelos implementados na Argentina e na União Europeia, já que o RGPD garante a completa independência das autoridades de controle da estrutura do Poder Executivo dos Estados-Membros.

---

[69] É importante observar que a legislação argentina não prevê a figura do Encarregado de Proteção de Dados (ou DPO) (SALTOR, 2013, p. 150), diferentemente do que faz a União Europeia em seu RGPD e, recentemente, o Brasil em sua LGPD.

[70] As seções 2 e 3 do artigo 29 da Lei nº 25.326/2000 foram vetadas pelo Decreto nº 995/2000 do Poder Executivo da Nação, extirpando da lei uma ferramenta de controle de caráter independente e imparcial, enquanto foram promulgadas especificações que autorizam a remoção do Diretor Nacional de Proteção de Dados Pessoais por mau desempenho de suas funções, precarizando ainda mais liberdade de atuação do órgão (SALTOR, 2013, p. 422).

Observa-se que a criação de uma autoridade de controle independente do Estado costuma encontrar fortes resistências políticas. Assim, a vinculação das entidades reguladoras ao Poder Público tem demonstrado uma grande ineficiência e incapacidade de atingir suas finalidades. As experiências vivenciadas América Latina indicam a utilização destes órgãos como fonte de emprego a ser distribuída entre a clientela eleitoral de governantes ou como caixa de suborno de concessionárias (SALTOR, 2013, p. 147), práticas que evidenciam a seríssima necessidade de sua autonomia funcional.

Na Argentina, a ausência de uma autoridade de controle independente do governo central (chamada de Direção Nacional de Proteção de Dados) reflete em uma política ineficiente de proteção do direito à autodeterminação informativa dos cidadãos, incluindo a baixa divulgação sobre os direitos dos titulares e a escassa quantidade de sanções leves aplicadas, de acordo com os dados encontrados no *site* do órgão (SALTOR, 2013, p. 148). Com isso, o próprio marco operativo da autoridade de aplicação contribui para a insuficiência da proteção de dados do titular (PICCIRILLI; QUIROGA, 2015, p. 238). Certamente que essa tímida atuação repercute na ausência de adaptação dos portais do Poder Judiciário às exigências legais de proteção de dados, conforme será observado na sequência da dissertação.

Por fim, o último e mais importante dos critérios de pesquisa elencados diz respeito ao tratamento de dados pelo Poder Público, já que a existência de normas específicas para a regulação da distribuição de dados pessoais pela administração pública são cruciais para que o cidadão seja munido de ferramentas contra as violações que lhe são impostas. É neste ponto que se observa uma das maiores fragilidades da Lei de Proteção de Dados argentina, na medida em que não existem regras específicas disciplinando o tratamento de dados quando os responsáveis são os próprios órgãos estatais, especialmente no caso da cessão de dados a terceiros.

O artigo 22, que aborda os arquivos, registros ou bancos de dados públicos, limita-se a exigir que as normas envolvendo a criação, modificação ou supressão de arquivos ou bancos de dados pertencentes a organismos públicos sejam precedidas da publicação de disposição geral no Boletim Oficial da Nação ou em diário oficial. Quando for o caso da supressão de registros informatizados, deverão ser informados a destinação dos arquivos ou as medidas adotadas para a sua destruição, conforme o inciso 3º (ARGENTINA, 2000).

Ainda que exista a carência de uma disciplina mais específica voltada à atuação do Estado, o artigo 11 da lei estabelece que a cessão dos dados pessoais objetos de tratamento só pode ser realizada em atendimento aos interesses legítimos do cedente e do cessionário, mediante prévio consentimento do titular, através da prévia informação das finalidades da

cessão. Este dispositivo sofreu regulamentação pelo Decreto nº 1558/2001, determinando que na hipótese de arquivos ou bancos de dados públicos vinculados a um organismo oficial destinado à difusão ao público em geral, em razão de suas funções específicas, considera-se implícito o interesse legítimo do cessionário às razões de interesse geral que motivaram o acesso público irrestrito dos dados (ARGENTINA, 2001).

Dentre as exceções ao consentimento para a cessão de dados pessoais, estão as situações em que o tratamento for realizado nas dependências dos órgãos estatais, de forma direta e no cumprimento de suas respectivas competências (inciso 3º, alínea "c"). Este dispositivo demonstra, na opinião de Piccirilli e Quiroga (2015, p. 232), uma cabal deficiência da normativa, na medida em que permite a aquisição de dados por entidade distinta daquela que realizou a coleta, sem informar ao titular, provavelmente com um propósito diferente daquele que originou a necessidade de tratamento por parte do cedente.

Outra importante exceção legal à regra do consentimento contempla os casos em que for aplicado um procedimento de dissociação da informação, impossibilitando a identificação de seus titulares (inciso 3º, alínea "e") (ARGENTINA, 2000). A partir desta regra, entende-se que a prática de dissociação deveria ser utilizada como regra geral pelo Poder Judiciário na cessão de dados pessoais para outros órgãos ou entidades públicas ou privadas, já que a justiça laboral não dispõe de um mecanismo de coleta do consentimento dos jurisdicionados para a publicização das informações fornecidas em virtude do ajuizamento da ação e/ou produzidas durante o trâmite processual.

Diante desse panorama, revela-se a importância do dispositivo previsto no inciso 4º do artigo 11, ao estabelecer a responsabilidade solidária do cedente e do cessionário perante o organismo de controle e o titular dos dados sujeitos ao tratamento, submetendo-se às mesmas obrigações legais e regulamentares (ARGENTINA, 2000). A norma em apreço impõe que se atente para a possibilidade de responsabilização solidária do Poder Público (cedente dos dados pessoais que são disponibilizados em seus portais de consulta processual e bancos de jurisprudência) e o cessionário (empregador que coleta os dados pessoais por meio do acesso à *Internet*) em face da violação da privacidade do jurisdicionado e das repercussões em seus direitos sociais. Vale lembrar que o artigo 1757 do Código Civil e Comercial da Nação[71] (ARGENTINA, 2014) estabelece a cláusula de responsabilidade civil objetiva para as pessoas

[71] "ARTICULO 1757.- Hecho de las cosas y actividades riesgosas. Toda persona responde por el daño causado por el riesgo o vicio de las cosas, o de las actividades que sean riesgosas o peligrosas por su naturaleza, por los medios empleados o por las circunstancias de su realización.
La responsabilidad es objetiva. No son eximentes la autorización administrativa para el uso de la cosa o la realización de la actividad, ni el cumplimiento de las técnicas de prevención" (ARGENTINA, 2014).

que causarem danos provenientes do exercício de atividade de risco, como pode ser considerado o caso do tratamento de dados sensíveis.

Todas as garantias previstas na Lei de Proteção de Dados argentina, ora identificadas, revelam um grande arcabouço principiológico, fruto de sua influência das normativas europeias, e o papel central oferecido ao consentimento no tratamento de dados pessoais. Por outro lado, ao não regulamentar de forma específica a atuação do Poder Público, verifica-se uma falha no sistema protetivo que acaba prejudicando diretamente o trabalhador que busca guarida na Justiça do Trabalho, já que a atuação do Poder Judiciário enquanto órgão controlador dos dados acaba carecendo de um maior balizamento, ainda mais quando violações são cometidas em nome da publicidade de seus atos.

Feito este exame da legislação argentina voltada à proteção de dados pessoais, com especial destaque à sua consolidada lei de proteção de dados, o foco do trabalho volta-se à observação do portal institucional da Corte Superior do Poder Judiciário trabalhista da Argentina, qual seja, o *site* do Poder Judicial de la Nación argentina (www.pjn.gov.ar) (ARGENTINA, 2019a), mediante a opção pela consulta dos julgados da Cámara Nacional de Apelaciones del Trabajo. O estudo será desenvolvido a partir dos critérios de análise anteriormente elencados, buscando encontrar vinculações entre a promessa protetiva feita pela legislação e a efetiva proteção dos dados do trabalhador no âmbito do processo trabalhista do país.

3.2.2 Pesquisa empírica: as ferramentas de consulta processual e jurisprudencial no *site* do Poder Judicial de la Nación argentina

Antes de adentrar na investigação do portal argentino, é importante a compreensão da organização judiciária no país. O sistema de justiça na Argentina é formado pelo Poder Judiciário da Nação (composto pela Corte Suprema de Justiça da Nação, o Conselho da Magistratura da Nação, os Tribunais de Primeira Instância e as Câmaras de Apelação) e pelos Poderes Judiciários de cada uma das províncias. Dentro do Poder Judiciário da Nação existem diferentes jurisdições, separadas em razão da matéria, tais como direito civil, direito comercial, direito do trabalho, etc., onde atuam os Tribunais de Primeira Instância e as Câmaras de Apelação (MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS, 2019). Dessa forma, a Justiça Nacional do Trabalho é exercida pelos juízes nacionais de primeira instância do trabalho e pela Câmara Nacional de Apelações do Trabalho, nos termos do artigo 1º da Lei 18345/1969, que dispõe sobre a organização da justiça laboral no país (ARGENTINA, 1969).

A justiça argentina é administrada de forma concorrente pelo Poder Judiciário da nação e pelos Poderes Judiciários provinciais. O artigo 116 da Constituição argentina (ARGENTINA, 1994) estabelece a competência da Corte Suprema e dos Tribunais Inferiores da Nação para a apreciação de demandas que versem sobre pontos regidos pela Constituição, pelas leis da nação ou por tratados internacionais, resguardando-se a competência das jurisdições provinciais (MINISTERIO DA JUSTIÇA E SEGURANÇA PÚBLICA, 2019).

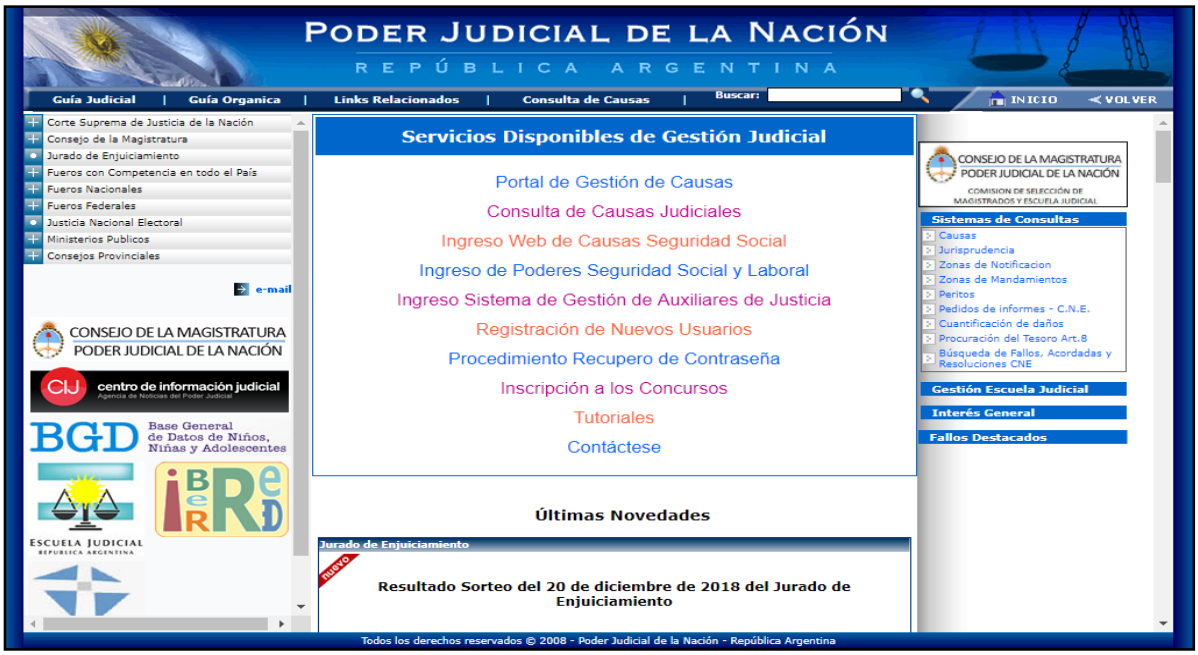
Cada província é responsável pela administração e organização judiciária em seu território, atribuição que lhes é outorgada pelo artigo 5º da Constituição argentina (ARGENTINA, 1994). Aos Tribunais provinciais compete, originariamente, o julgamento das causas que dispõem sobre direitos previstos nos Códigos Civil, Comercial, Penal, do Trabalho e Seguridade Social[72], sendo que, nesses casos, a Corte Suprema atuará somente em sede recursal (MINISTERIO DA JUSTIÇA E SEGURANÇA PÚBLICA, 2019).

Após esta introdução acerca da estruturação do Poder Judiciário na Argentina, parte-se para a observação direta do *site* do Poder Judicial de la Nación[73] (www.pjn.gov.ar), realizada no dia 02 de fevereiro de 2019. O portal apresenta, na sua tela inicial (Figura 1), a opção de "Consulta de causas judiciales", que remete ao "Sistema de Consulta Web", sistema unificado que integra a consulta processual da Corte Suprema, das Câmaras Nacionais de Apelações, das Câmaras Federais e da Justiça Federal das Províncias. A pesquisa jurisprudencial é acessível no menu "Sistema de consultas", situado à direita na tela inicial do *site* (Figura 1) (ARGENTINA, 2019a) remetendo a outra seção do portal, aparentemente menos rebuscada.

[72] Nos termos do artigo 75, da Constituição: "Corresponde al Congreso: [...] 12. Dictar los Códigos Civil, Comercial, Penal, de Minería, y del Trabajo y Seguridad Social, en cuerpos unificados o separados, sin que tales códigos alteren las jurisdicciones locales, correspondiendo su aplicación a los tribunales federales o provinciales, según que las cosas o las personas cayeren bajo sus respectivas jurisdicciones; y especialmente leyes generales para toda la Nación sobre naturalización y nacionalidad, com sujeción al principio de nacionalidad natural y por opción en beneficio de la argentina: así como sobre bancarrotas, sobre falsificación de la moneda corriente y documentos públicos del Estado, y las que requiera el establecimiento del juicio por jurados" (ARGENTINA, 1994).

[73] Além do *site* do Poder Judicial de la Nación, a Corte Suprema de Justiça da Nação conta com o portal Centro de Información Judicial (cij.gov.ar) (ARGENTINA, 2019b), que divulga informações relacionadas à atividade do Poder Judiciário argentino em geral. Por meio desta página, é possível realizar buscas processuais, o que remete à consulta de expedientes do portal do Poder Judicial de la Nación.

Figura 1 – Página inicial – Poder Judicial de La Nación (ARGENTINA, 2019a)



Como a pesquisa é limitada à Cámara Nacional de Apelaciones del Trabajo, esta opção foi selecionada em todas as buscas realizadas através de aba disponibilizada pelo *site*, tanto na consulta de expedientes quanto na consulta jurisprudencial, como é possível observar nas Figura 2 e 3.

Figura 2 – Consulta de expedientes (ARGENTINA, 2019a)

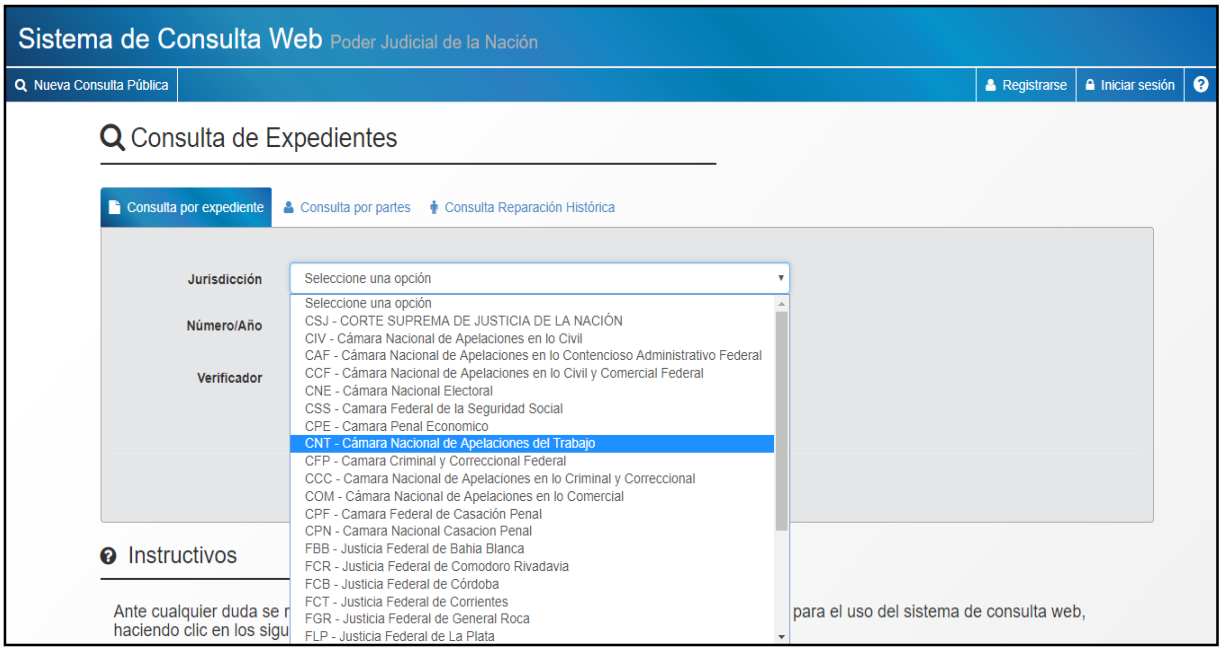
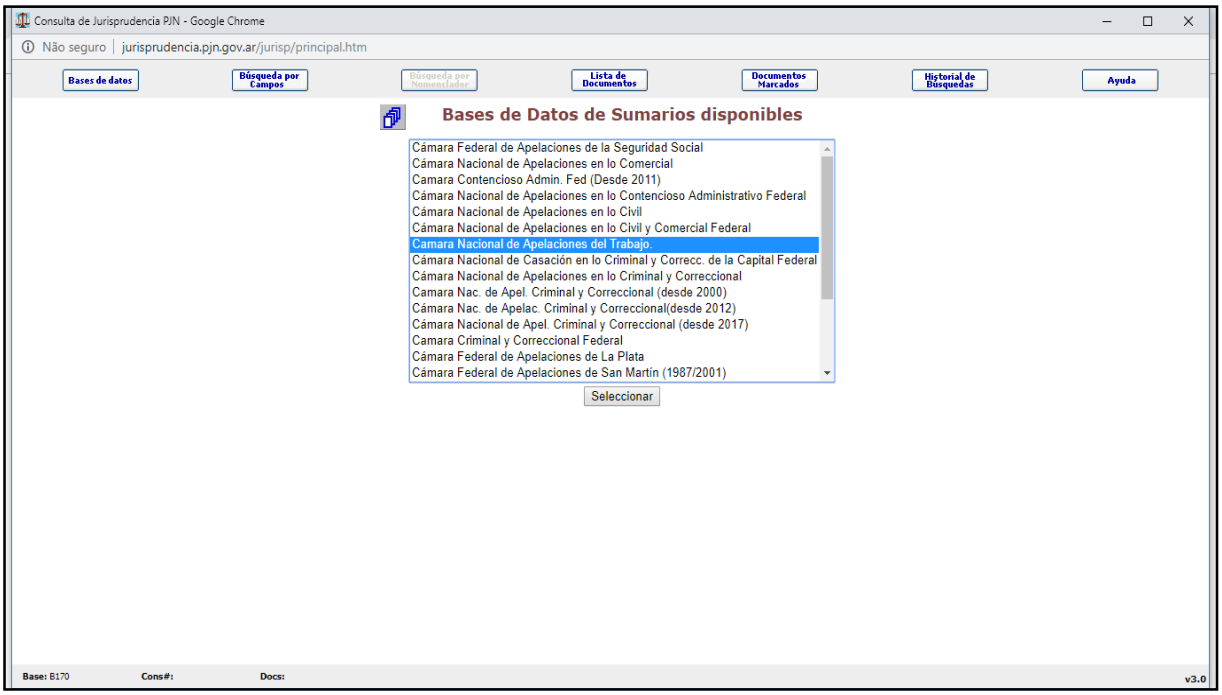


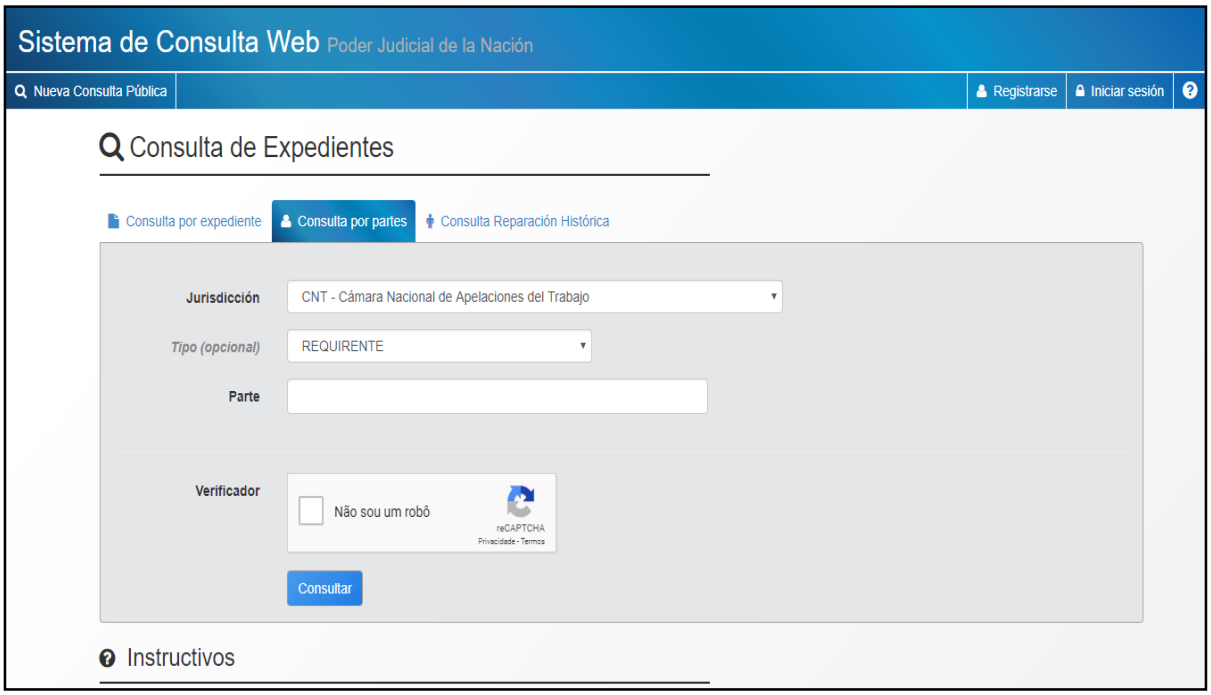
Figura 3 – Consulta de jurisprudência (ARGENTINA, 2019a)



Em resposta ao primeiro critério de análise, qual seja, a possibilidade de pesquisa pelo nome do reclamante, observa-se que o *site* permite o acesso aos processos em andamento através da pesquisa pelo nome do autor ou de qualquer das partes em "Consulta de expedientes" (Figura 4). A ferramenta, por si só, viola dispositivos expressos na Lei de Proteção de dados, já que o artigo 7º, 2 determina que dados sensíveis somente podem ser tratados havendo razões de interesse geral autorizadas por lei (ARGENTINA, 2000), o que não é o caso dos dados reportados em reclamatórias trabalhistas, e a possibilidade de consulta pública por meio do nome do trabalhador conduz ao uso discriminatório dessas informações.

Vale lembrar a posição do doutrinador argentino Horacio Fernández Delpech (2003, p. 154), que entende que nem mesmo o consentimento expresso do titular eliminaria a proibição expressa à formação de bancos de dados sensíveis. Dessa forma, ao facilitar o acesso público a bancos de dados com este conteúdo, o Poder Judiciário incorre em uma dupla violação. Em primeiro lugar, a utilização dos dados para finalidades distintas da coleta e a manutenção de bancos de dados com informações sensíveis mesmo após o término do tratamento. E por outro lado, a publicização das informações, com a possibilidade de acesso facilitado ao público em geral aos bancos de dados repletos de informações sensíveis, direcionando-se a busca diretamente ao nome da pessoa.

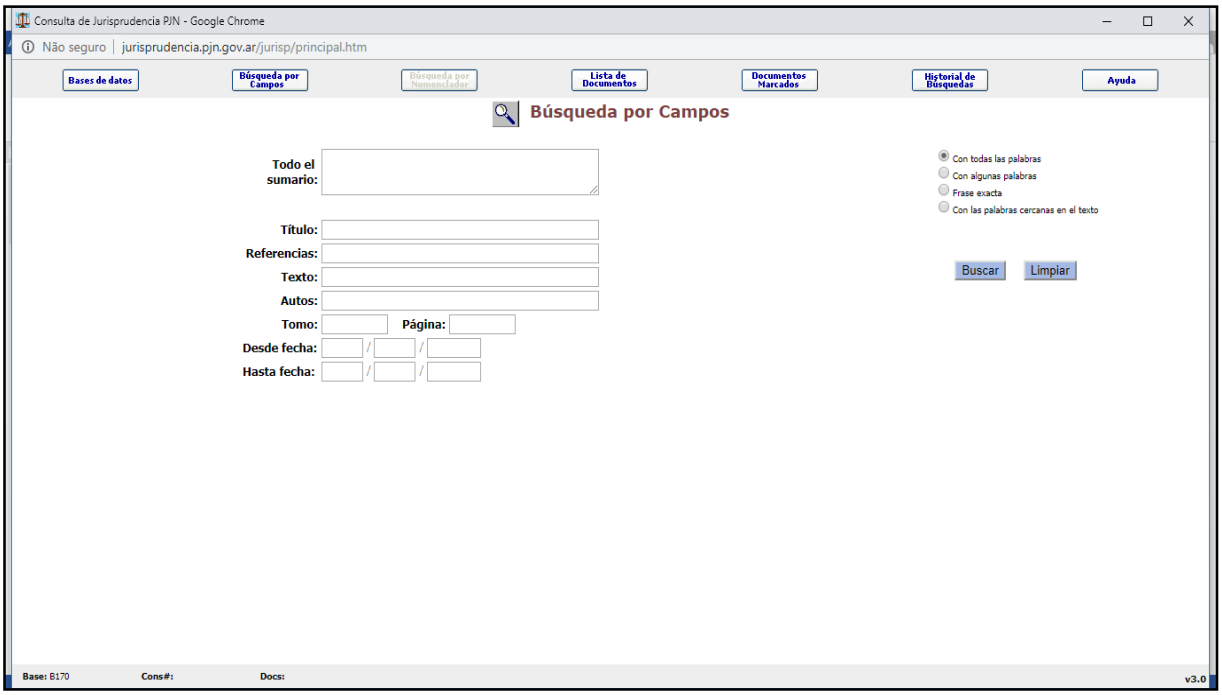
Figura 4 – Consulta por partes (ARGENTINA, 2019a)



O portal não impõe nenhuma restrição ao acesso do conteúdo, sendo disponibilizado a qualquer usuário da *Internet* que disponha do nome completo do trabalhador. Este ponto representa a principal vulnerabilidade do modelo argentino, organizado em torno de um sistema unificado de buscas que permite o livre acesso de qualquer indivíduo aos dados pessoais do trabalhador, em que pese exista a previsão do consentimento como base legal para o tratamento de dados no país.

O mesmo pode ser dito da pesquisa jurisprudencial (Figura 5), que permite a utilização do nome das partes como palavras-chave, conduzindo ao acesso de acórdãos com informações sensíveis de pessoas específicas, bastando que os termos buscados sejam coincidentes com os resultados reportados no banco de dados.

Figura 5 – Pesquisa jurisprudencial: busca por campos (ARGENTINA, 2019a)



E para superar a vulnerabilidade aberta pelo sistema, seria possível ao Poder Judicial da Nação argentina tomar a medida de desindexação dos nomes integrantes de acórdãos para que a busca não obtivesse resultados encontrados. A esse respeito, Marcel Leonardi (2012, p. 145) explica o funcionamento dos mecanismos de busca na *Internet*, informando que é possível impedir a indexação de partes ou de todo o conteúdo de um *site*, já que os buscadores são configurados para seguir as orientações a respeito de quais arquivos devem ou não ser indexados que estão contidas no *Robot Exclusion Standard,* ou "Protocolo de Exclusão de Robôs" (arquivo "robots.txt"), localizado no diretório raiz de um servidor *Web*. Esse procedimento impede que as informações sejam indexadas, mas mantém a possibilidade de acesso a quem utilizar o endereço eletrônico correto (LEONARDI, 2012, p. 145). Não é o que se observa no portal atual do Poder Judicial de la Nación, que não possui qualquer filtro aos resultados da busca jurisprudencial, bastando que a palavra-chave procurada coincida com qualquer termo existente nas decisões mantidas em seu banco de dados.

Dessa forma, ao divulgar informações de cunho sensível do jurisdicionado sem o seu expresso consentimento, que deveria ser acompanhado da ampla informação acerca da finalidade da cessão, e ainda permitir a busca vinculada ao seu nome, a Corte Suprema do Poder Judiciário trabalhista argentino acaba por violar o artigo 11 da Lei de Proteção de Dados, que somente admite a dispensa de tal consentimento mediante a realização de um procedimento de

dissociação da informação (artigo 11, inciso 3º, alínea “e”) (ARGENTINA, 2000), justamente visando impedir a identificação de seus titulares.

A primeira categoria analisada indicou, portanto, uma alta preocupação de transparência por parte do Poder Judiciário argentino, mas uma atenção reduzida à privacidade dos jurisdicionados, desconectando-se dos preceitos indicados pela Lei nº 25.326/2000 ao tratamento de dados pessoais, o que se torna um preço alto a ser pago pelo trabalhador. Entende-se que a pesquisa pelo nome do reclamante, tanto processual como jurisprudencial, amplifica o acesso a informações com alto potencial discriminatório, devendo-se adotar um padrão mais rígido de proteção para estes dados.

O segundo critério de observação é a adoção de solução de *captcha* para consultas em processos, acórdãos e jurisprudências, categoria que foi definida tendo como inspiração uma orientação sugerida pela Resolução nº 139/2014 do Conselho Superior da Justiça do Trabalho brasileira (CONSELHO..., 2014b), com vistas a inibir a captura automatizada de dados de reclamantes e reclamados por meio de consultas públicas na Justiça do Trabalho. Considerando ser este um importante mecanismo contra a utilização de ferramentas de automação para a coleta de dados pessoais que integram o processo judicial eletrônico, optou-se por incorporá-lo como uma categoria de análise também do portal argentino.

O termo *captcha* é uma sigla derivada da expressão "Completely Automated Public Turing test to tell Computers and Humans Apart" (teste de Turing público completamente automatizado para diferenciação entre computadores e humanos), e representa uma ferramenta empregada contra a atuação de robôs programados para a execução de tarefas automatizadas na *Internet*. Costuma ser utilizado como anti-*spam* ou por *sites* que promovem o tratamento de dados sensíveis, visando obstar o acesso a essas informações (SINGH; PAL, 2014, p. 2242).

A observação da seção de “Consulta de Expedientes”, ferramenta de consulta processual integrada do Poder Judicial da la Nación (Sistema de Consulta Web) indicou a adoção do verificador *captcha* como requisito prévio para a busca pelo nome das partes, conforme é possível observar na Figura 4, o que evidencia uma preocupação com a segurança em face do tratamento automatizado de dados pessoais. Por outro lado, o mesmo cuidado não é oferecido à pesquisa jurisprudencial, que não faz uso da ferramenta, permitindo o acesso facilitado aos resultados de busca (Figura 5). Diante disso, o portal cumpre parcialmente com o segundo critério de análise, uma vez que falha ao permitir que dados pessoais do trabalhador que fazem parte do banco de jurisprudência do Tribunal sejam plenamente acessíveis por sistemas automatizados cuja finalidade costuma ser justamente a coleta massiva de dados pessoais e o posterior reagrupamento para fins comerciais e/ou discriminatórios.

O próximo critério de observação, relacionado à divulgação de dados sensíveis, restringe-se ao âmbito da pesquisa jurisprudencial, diante da inviabilidade da utilização de nomes reais de reclamantes no campo de pesquisa processual. Não resta dúvidas de que a pesquisa processual dos portais dos Tribunais possibilita o acesso a trâmites processuais, bem como a despachos e decisões judiciais contendo informações pessoais do trabalhador, por isso importava apenas descobrir se essas informações estão disponíveis de forma facilitada a qualquer pessoa por meio da pesquisa pelo nome do reclamante, o que consistiu no primeiro critério analisado.

Visando examinar[74] o recurso da pesquisa jurisprudencial, optou-se pela eleição de uma palavra-chave que costuma conduzir ao tratamento de dados sensíveis, qual seja, "despido discriminatorio", através de consulta realizada no dia 01 de julho de 2019. A pesquisa concentrou-se no período de 27/04/2016 a 27/04/2019, com o preenchimento do campo "Todo el sumario" e a opção de "Frase exacta", resultando em 43 (quarenta e três) julgados. A data escolhida como termo inicial da busca coincide com a data de edição do Regulamento Geral de Proteção de Dados Pessoais da União Europeia, normativa que exerce grande influência nos países da América Latina, em virtude das trocas comerciais que envolvem a circulação de dados pessoais e a necessidade de adequação da legislação desses países.

É importante destacar que a pesquisa não encontrou julgados posteriores ao ano de 2017. Mostra-se, portanto, um sistema evidentemente desatualizado, inclusive pela própria ferramenta de busca, que apresenta poucas opções de filtragem, não permitindo a escolha entre processos físicos ou eletrônicos. As únicas opções disponibilizadas para a filtragem dos resultados são, além do campo de pesquisa livre (sumário, título, referências e texto), o número dos autos, o tomo/página da decisão e o período de pesquisa. Além disso, o portal não divulga os julgados na íntegra, disponibilizando o acesso somente à ementa. Diante de tantas limitações, o sistema de pesquisa jurisprudencial acaba tornando-se mais protetivo ao trabalhador em virtude de sua precariedade, e não por uma política do Tribunal.

Dentre os resultados encontrados, verificou-se um número excessivo de julgados em repetição, 18 (dezoito) no total. Em resposta à terceira categoria de análise, observou-se que das 25 (vinte e cinco) decisões diferentes encontradas, 21 (vinte e uma) reportaram algum tipo de dado sensível, sendo que em 15 (quinze) resultados houve a divulgação de informação

[74] A observação dos dados deve ter como primeira etapa a análise temática transversal, que consiste em uma fase de preparação e de ordenamento das informações coletadas, através do estabelecimento de temas comuns e da codificação e classificação dos dados recolhidos (ALAMI; DESJEUX; GARABUAU-MOUSSAOUI, 2010, p. 122).

relacionada à saúde ou vida sexual do trabalhador, ou de terceiro[75] (vide apêndice C, quadro 3), algo que pode ser atribuído ao predomínio de ações envolvendo o pedido de reintegração ou indenização do empregado(a) despedido(a) em função de doença ou em estado de gravidez[76].

Se o sistema apresenta suas falhas e limitações, ao menos adotou, em 11 (onze) dos resultados distintos (44% do total, excluídas as repetições), a prática de disponibilizar somente as iniciais do nome do trabalhador. Não foram encontradas justificativas aparentes para que essa diferenciação tenha ocorrido, já que julgados de matéria similar encontram tratamentos distintos e não há a indicação de segredo de justiça. A utilização das iniciais de nome e sobrenome para a designação do reclamante é um procedimento que reduz a exposição do trabalhador aos riscos de tratamento discriminatório e, por conta disso, deve ser louvado, ainda que urgente a sua adoção como regra geral, e não somente em alguns casos.

Alguns julgados merecem destaque a título exemplificativo. É o caso da ação n. 29865/2013/CA1, ajuizada por M.L.M.[77] em face de M.C.F. AS em virtude de despedida discriminatória motivada pelo estado de saúde da trabalhadora. O acórdão, julgado em 21/12/16, foi assim divulgado pelo Poder Judicial de la Nación (ARGENTINA, 2016b):

> Despido discriminatorio
> **Trabajadora con insuficiência cardíaca**. Ausencias e incumplimientos de horario a raíz de los controles que le imponía su enfermedad. Discriminación de las personas discapacitadas
>
> **Como consecuencia de un trasplante cardiológico al que fue sometida la actora quedó en un delicado estado de salud que la obligaba a incurrir en ausencias e incumplimientos de horários laborales**. Probado a través de la testimonial que su despido no obedeció a cuestiones de restructuración de la empresa, tal como alegó la demandada, cabe concluir que el distracto obedeció a sus inconvenientes de salud. La discriminación arbitraria que se evidencia en el caso es un acto prohibido por la ley 23.592, motivo por el cual no se realiza de manera explícita, sino de manera solapada, porque quien conoce la ilegitimidad de su actuar intenta disimularlo o directamente ocultarlo. Por ello, de acuerdo a todo un plexo normativo que resulta aplicable al caso, en especial la ley 22431 que instituyó el Sistema de Protección Integral de las Personas Discapacitadas, **al haber sido segregada la actora de su comunidad laboral por tener problemas prolongados de salud**, impidiéndole de esta manera uma igualdad real de oportunidades y de trato, así como el pleno goce y ejercicio de los derechos reconocidos por el bloque de constitucionalidad federal, la preceptiva supralegal y legal vigente en la materia, corresponde resarcir el daño moral del que fuera objeto [grifo nosso].

[75] Os dados encontrados foram categorizados conforme as diferentes classes de dados sensíveis elencadas pelo artigo 5º, II da LGPD brasileira - Lei nº 13.709/2018 (BRASIL, 2018a), adotando-se este padrão para o comparativo entre Argentina e Brasil.

[76] Dentre os 15 (quinze) resultados em que houve a divulgação de dados relacionados à saúde ou vida sexual, 2 (dois) deles relacionaram-se à trabalhadora gestante.

[77] Ainda que grande parte dos julgados encontrados na pesquisa jurisprudencial argentina tenha divulgado o nome completo das partes, optou-se pela utilização das letras iniciais como regra geral em todas as jurisprudências citadas neste trabalho, como forma de minimizar o potencial discriminatório das informações aqui tratadas.

Como se observa, a obreira foi despedida em virtude das constantes ausências e descumprimento de horários decorrentes de transplante cardiológico a que se submeteu, em função de ser portadora de insuficiência cardíaca, informações sensíveis que integraram a ementa. Somando-se os fatos de que houve a divulgação do nome completo da reclamante (a íntegra do julgado divulgada pelo *site* do Poder Judicial de la Nación apresentava os nomes completos das partes, que foram abreviados pelo autor visando reduzir o potencial discriminatório das informações), seu estado de saúde, e as recorrentes ausências ao trabalho em virtude do transplante, o tratamento dessas informações por terceiros podem resultar em consequências ainda mais devastadoras à trabalhadora.

Além da incômoda situação de ter seu problema cardíaco completamente exposto na *Internet,* qualquer empregador que realizar uma pesquisa *online* poderá ser informado de que a candidata costumava faltar ao serviço por conta dos problemas prolongados de saúde, o que provavelmente irá inviabilizar a sua futura contratação, isso se a discriminação não vier pelo simples fato de ter ajuizado a reclamação trabalhista. Torna-se perceptível que a Justiça do Trabalho procura compensar uma situação de desigualdade gerada durante o contrato de trabalho, mas acaba criando um efeito colateral capaz de potencializar a discriminação ao trabalhador.

Os dados de saúde são tutelados pelo artigo 8º da Lei nº 25.326/2000[78] (ARGENTINA, 2000), que se vincula ao tratamento no âmbito dos estabelecimentos sanitários e por profissionais da área da saúde. Mesmo quando incorporadas às páginas de um processo judicial eletrônico, essas informações compõe verdadeira história clínica do paciente, definida por Tanús (2003, p. 244) como "[...] un conjunto de registros en los que se asientan en forma detallada y ordenada las observaciones, diagnósticos y hallazgos relacionados con la salud de una persona".

Portanto, assim como todos os dados sensíveis, esses dados estão submetidos a um regime de proteção mais restrito que os demais (TANÚS, 2003, p. 243), já que a regra geral legal é a da vedação ao tratamento desta categoria de dado, se não houver razão de interesse geral autorizada em lei. No caso da divulgação de informações de saúde pela Justiça laboral argentina, evidente a desnecessidade na exposição integral de laudos e prontuários médicos, bem como detalhamentos sobre o estado de saúde do trabalhador (como a própria insuficiência

[78] "ARTICULO 8° — (Datos relativos a la salud).
Los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando los princípios del secreto professional" (ARGENTINA, 2000).

cardíaca acima referida), bastando a referência ao número dos documentos eletrônicos, preferencialmente após um processo de dissociação dos dados, na forma do artigo 2º da lei (ARGENTINA, 2000).

Mas os dados sensíveis encontrados na busca realizada não se limitaram aos dados relativos à saúde do trabalhador. Além de 4 (quatro) resultados envolvendo a divulgação de dados relativos à filiação sindical ou à organização política e 1 (um) relacionado à opinião política, encontrou-se 1 (um) julgado relacionado à origem racial ou étnica. Trata-se do processo de número 48.965/2009/CA1, movido por T.R.I. em face de P.P. ICSA (ARGENTINA, 2016a). A ementa do acórdão, que data de 25/10/16, apresentou o seguinte teor:

> Despido discriminatorio
> **Trabajadora discriminada por su condición de mujer y por su parentesco con personas de origen boliviano**. Dictamen proveniente del INADI. Resarcimiento civil. Daño moral.
>
> La conducta lesiva traducida en la presión a la que se vio sometida la actora, implicó un proceder que afectó la dignidade de la persona humana, reconocida en los tratados internacionales de derechos humanos, e incluso reconocida recientemente en el nuevo Código Civil que ha mutado así a un criterio humanista al abandonar el patrimonialista del viejo código. Esa conducta agraviante o lesiva del honor del trabajador se enmarca em responsabilidad extracontractual por daños, en tanto que ese proceder de la empleadora exorbitó el marco contractual contemplado en la L.C.T.. Al resultar demostrado que la empleadora incurrió en responsabilidad extracontractual, pues cometió actos reprobables (por acción u omisión) en perjuicio de la trabajadora, ésta resulta civilmente resarcible aún em ausencia de vínculo laboral (conf. arts. 1068, 1078 y 1.109 del anterior Código Civil), y cabe asimismo condenar a aquélla a um resarcimiento adicional por daño moral [grifo nosso].

O julgado refere-se a pedido indenizatório por dano moral proveniente de tratamento discriminatório de uma trabalhadora em virtude da sua condição de mulher (discriminação por motivo de gênero) e da descendência boliviana (discriminação por motivo de raça/etnia). A conjugação dos dados referentes à origem étnica da obreira, considerados sensíveis pela Lei de Proteção de Dados Pessoais do país[79], com o nome da trabalhadora, publicado junto à decisão, conduzem a uma violação do direito à privacidade pela distribuição de informações sem o devido consentimento, uma vez que a reclamante certamente não buscou o Poder Judiciário imaginando que tal publicização fosse ocorrer.

[79] Embora exista certa confusão acerca do significado das expressões "origem racial" e "etnia", frequentemente utilizados como sinônimas, Fernández Delpech (2003, p. 149) estabelece uma diferença básica, considerando que etnia é um modo de organização da sociedade com base em certas características comuns, dentre as quais se encontra a raça.

Quanto às possibilidades de manifestação do consentimento no processo judicial eletrônico, é valiosa a contribuição de Basterra (2004, p. 7), ao lembrar que a lei deixa aberta a possibilidade de utilização da assinatura eletrônica, ao admitir o consentimento por outros meios que se equiparem à forma escrita, de acordo com as circunstâncias. A assinatura eletrônica é um meio de garantir as transações realizadas pela *Internet*, permitindo a prova da identidade do remetente, a integridade e a confidencialidade do conteúdo (BASTERRA, 2004, p. 9). Com isso, o procurador do reclamante, com procuração protocolada nos autos poderia manifestar o consentimento do titular por meio de simples petição, assinada digitalmente, discriminando-se as finalidades do tratamento autorizado, o que bastaria para evitar a divulgação involuntária de dados sensíveis como os reportados no julgado acima, que envolviam discriminações por motivo de sexo e etnia.

O problema envolvendo a discriminação por motivo de sexo na Argentina é uma preocupação desde a edição das primeiras leis laborais, já que em 1907 a Lei nº 5.291 já ofereceu uma proteção especial à mulher, tutela que historicamente buscou proteger tanto a condição da mulher em si mesma (na sua condição física), no seu papel de mãe e como base da família (GRISOLIA, HIERREZUELO, 2013, p. 8). Atualmente, a Lei do Contrato de Trabalho destina uma seção (título VII) à proteção da mulher, vedando qualquer espécie de discriminação motivada por sexo, em seu artigo 172 (ARGENTINA, 1974).

A legislação argentina também veda toda e qualquer forma de discriminação por motivo de raça, religião, nacionalidade, ideologia, opinião política ou sindical, sexo, posição econômica, condição social ou características físicas, através da Lei nº 23.592/1988 (ARGENTINA, 1988). Com relação à nacionalidade, trata-se de uma informação de conteúdo altamente discriminatório, que com frequência leva à estigmatização, classificação, pré-julgamentos, comprometendo inclusive a segurança dos seus titulares (DONEDA; MONTEIRO, 2015). Esses dados demandam um nível mais elevado de proteção, já que enquadram-se em uma categoria que, mesmo parecendo inofensivos isoladamente, ao serem conjugados com outras informações podem conduzir à discriminação da pessoa humana (KONDER, 2019, p. 455).

Em que pese aparente uma certa contradição o estabelecimento de tratamento sigiloso a informações aparentes como a raça, cor e sexo, ou ainda preferências políticas ou religiosas, que somente podem ser manifestadas em público, o tratamento diferenciado a esses dados se justifica como uma estratégia preventiva antidiscriminação (ACUÑA, 2005, p. 26), já que mesmo dados ordinários podem converter-se em dados sensíveis através de seu uso ou tratamento discriminatório (PICCIRILLI; QUIROGA, 2015, p. 237).

Os julgados aqui colacionados como exemplos indicam uma falha no sistema argentino de proteção de dados pessoais do trabalhador, contrariando os dispositivos legais relacionados ao tratamento de dados sensíveis, principalmente diante da inexistência de interesse público a autorizar a sua divulgação irrestrita e da ausência de expresso consentimento do reclamante, específico para esta finalidade. Ao não oferecer maiores cuidados às informações pessoais que são publicadas em suas ferramentas de busca processual e jurisprudencial, o Poder Judiciário argentino evidencia um verdadeiro descaso para com o jurisdicionado, principal afetado com essa política.

Vale lembrar que a Lei nº 25.326/2000 regulamenta o *Habeas Data*, ação de proteção de dados pessoais que permite ao titular pleitear o cancelamento de dados quando a sua utilização não corresponde à finalidade para a qual foram coletados, justamente a situação observada na pesquisa jurisprudencial. Como se tratam de bancos de dados públicos, a Administração Pública possui um dever permanente de atualização, a fim de garantir a confidencialidade dos dados sensíveis e a supressão dos dados que se tornarem desnecessários (GOZAÍNI, 2003, p. 214), o que é o caso das informações sensíveis dos jurisdicionados que são reportadas nos autos das reclamações trabalhistas e que esgotam a sua finalidade com a tutela jurisdicional, sendo descabida a sua reprodução nas jurisprudências divulgadas pela *Internet*. Dentre os dispositivos relacionados à ação de *Habeas Data*, a lei traz a previsão de que o juiz poderá determinar o bloqueio provisório do arquivo quando o dado pessoal for dotado de manifesto caráter discriminatório (ARGENTINA, 2000), medida que pode ser impetrada pelo jurisdicionado para a proteção de seus dados sensíveis.

A ausência de uma regulamentação específica acerca do tratamento de dados por parte do Poder Público na Lei de Proteção de Dados, somada à inobservância do Poder Judiciário com relação à alguns dos dispositivos legais, dentre eles o tratamento de dados sensíveis em situações não autorizadas pela lei, permitem inferir que a Argentina, apesar das quase duas décadas de implantação de uma legislação específica regulando o tema, não garante uma efetiva proteção de dados pessoais do trabalhador que busca a guarida da Justiça laboral. Além da insuficiência de sua legislação, pelas próprias incompletudes já apontadas, o resultado da análise realizada no portal do Poder Judicial de la Nación indica uma ausência de aplicação das disposições legalmente estabelecidas, permitindo o tratamento de dados sensíveis do reclamante sem maiores cuidados que pudessem evitar a identificação individual.

Parte-se agora para a análise do modelo brasileiro, notadamente quando se comemora no país o advento de uma nova lei geral de proteção de dados pessoais, que será observada em conjunto com o portal do Tribunal Superior do Trabalho, Corte Superior do Poder Judiciário

trabalhista do país. O próximo ponto avaliará a suficiência ou não desse instrumento legal para garantir uma proteção ao trabalhador diante do uso abusivo de seus dados pessoais no âmbito da Justiça do Trabalho, em cotejo com os paradigmas anteriormente apresentados.

3.3 A NOVA LEI DE PROTEÇÃO DE DADOS BRASILEIRA ENTRE EXPECTATIVAS E A REALIDADE: é possível falar em efetividade da proteção dos dados pessoais do trabalhador no atual contexto da Justiça do Trabalho?

Enquanto o Brasil aguarda a entrada em vigor de uma lei específica que venha a regular a proteção de dados de maneira ampla, muito se discute no país sobre os procedimentos a serem tomados visando a adequação empresarial às exigências da nova lei. Com relação ao Poder Público não é diferente, e muitas práticas terão de ser revistas diante do expressivo número de dados pessoais que são tratados pelos organismos governamentais. Este tópico propõe-se a analisar o panorama atual da divulgação de dados pessoais dos jurisdicionados pelo *site* do Tribunal Superior do Trabalho, à luz dos preceitos estabelecidos pela nova Lei de Proteção de Dados Pessoais, começando por uma estudo de legislação atualmente vigente no país.

3.3.1 A legislação brasileira protetiva de dados pessoais com o advento do novo marco normativo

No Brasil, foi longo o caminho percorrido até a edição de um marco regulatório para a proteção de dados pessoais. O avanço tecnológico e as pressões do mercado internacional trouxeram a necessidade de uma normativa que assegure ao país um nível adequado de sua legislação. Além das garantias constitucionais, vinculadas à proteção da intimidade e da dignidade da pessoa humana, a legislação infraconstitucional vigente mostra-se fragmentária e direcionada a temas específicos, não abrangendo a tutela de dados pessoais em todos os seus aspectos.

O princípio da dignidade da pessoa humana, expresso no artigo 1°, III da Constituição da República Federativa do Brasil constitui-se no verdadeiro fundamento da ordem constitucional, vetor interpretativo de todos os direitos fundamentais. A Carta Magna não prevê expressamente o direito à proteção de dados pessoais, mas tutela os direitos fundamentais à intimidade e à vida privada em seu artigo 5º, inciso X, garantindo também o direito à indenização pelos danos morais ou materiais decorrentes da sua violação. Além disso, o artigo

5°, inciso XII garante a inviolabilidade de dados, referindo-se à interceptação de correspondências e comunicações telefônicas (BRASIL, 1988).

A Constituição de 1988 estabelece, ainda, a figura do *Habeas Data* como remédio constitucional previsto no artigo 5 º, inciso LXXII (BRASIL, 1988), destinado a proteção dos dados pessoais, por meio do direito de acesso e de retificação das informações constantes de registros ou bancos de dados de entidades governamentais ou de caráter público. O *Habeas Data* é apontado por Pérez Luño (2005, p. 357) como ferramenta apta para a proteção jurisdicional do direito à autodeterminação informativa, que traduz-se em uma nova faceta do direito à privacidade, e, como tal, requer novos instrumentos jurídicos para se tornar efetivo.

Observa-se que o Brasil foi o primeiro dentre os países latino-americanos a introduzir o *Habeas Data* em sua Carta Magna, sendo seguido por diversos outros, dentre eles a Argentina. Ao contrário do vizinho mercosulino, entretanto, o *writ* constitucional no Brasil existe como figura autônoma (GOZAÍNI, 2003, p. 166), que veio a ser regulamentada pela Lei nº 9.507/1997, disciplinando o seu rito processual.

No que se refere ao âmbito de aplicação, a normativa define, em seu artigo 1º, parágrafo único, como de caráter público "[...] todo registro ou banco de dados contendo informações que sejam ou que possam ser transmitidas a terceiros ou que não sejam de uso privativo do órgão ou entidade produtora ou depositária das informações" (BRASIL, 1997). Com isso, a ação poderá direcionar-se tanto os bancos de dados públicos, vinculados diretamente à Administração Pública direta ou indireta, bem como aos titulares de bancos de dados privados (SILVA, C. B., 2014, p. 232) que contenham informações que podem ser repassadas a terceiros, o que inclui a possibilidade de impetração no âmbito das relações trabalhistas (SIMÓN, 2000, p. 196).

O *Habeas Data* emerge como a principal ferramenta à disposição do jurisdicionado com vistas a uma ampla tutela de seus dados pessoais, especialmente o acesso e o apagamento de dados armazenados em bancos de dados mantidos pelo Poder Judiciário. A regulamentação deste remédio constitucional no Brasil coincide com um período de maior preocupação dos Estados Modernos com relação à ampla transparência dos atos administrativos, própria dos modelos democráticos, sem descuidar da garantia dos direitos individuais, nos quais insere-se a intimidade e a vida privada. Diante dessa realidade, Ruaro, Rodriguez e Finger (2011, p. 58) relatam que:

> [...] os Estados modernos, promovem mais e mais a garantia de respeito à dignidade da pessoa humana bem como a transparência nos atos da Administração Pública e isto porque, dentro desta perspectiva, hoje é impensável deixar de reconhecer o direito do

> cidadão de dispor dos seus dados pessoais da mesma forma que tem direito de dispor livremente do seu corpo. Há a consciência de que o armazenamento de dados em computadores e outros tipos de bancos de dados pode significar uma agressão à intimidade da vida privada e, também, ofender outros bens jurídicos fundamentais.

No plano infraconstitucional, os direitos de personalidade estão elencados no Capítulo II do Código Civil de 2002[80], que prevê a inviolabilidade da vida privada em seu artigo 21 (BRASIL, 2002). Até a entrada em vigor de uma normativa que regulamente de forma ampla a proteção de dados pessoais no país, diversos dispositivos esparsos[81] podem ser evocados, especialmente no que se refere à tutela de dados do consumidor, tais como o artigo 43 da Lei nº 8.078/1990, Código de Defesa do Consumidor (BRASIL, 1990), e os artigos 3°, 5° e 14 da Lei nº 12.414/2011, Lei do Cadastro Positivo (BRASIL, 2011a), que trata da formação e consulta a bancos de dados com informações de adimplemento.

Com relação à divulgação de informações pelo Poder Público, merece destaque a já referida lei 12.527/2011, Lei de Acesso à Informação, que disciplina o direito de acesso à informação pública, dispondo, em seu artigo 31, sobre a obrigatoriedade do tratamento das informações pessoais ser feito de forma transparente, respeitando a intimidade, vida privada, honra e imagem das pessoas, havendo a possibilidade da autorização da divulgação ou do acesso dessas informações somente mediante previsão legal ou consentimento expresso do titular dos dados (BRASIL, 2011b).

A lei, que vincula tanto os órgãos integrantes da Administração Pública direta, abrangendo os Poderes Executivo, Legislativo e Judiciário, além dos Tribunais de Contas e do Ministério Público, quanto as entidades da administração indireta e as entidades privadas sem fins lucrativos que recebam verbas públicas, estabelece, em seu artigo 31, parágrafo 2º, a responsabilização daqueles que obtiverem acesso às informações pessoais pelo seu uso indevido (BRASIL, 2011b), justamente o que ocorre quando informações que foram fornecidas para a finalidade específica da prestação jurisdicional são utilizadas para fins discriminatórios.

Além do mais, o artigo 34, "caput", assevera que os órgãos e entidades públicas deverão responder diretamente pelos danos decorrentes da divulgação não autorizada ou da utilização indevida de informações pessoais, cabendo eventual direito de regresso em caso de culpa ou dolo do agente público (BRASIL, 2011b). Este dispositivo consagra a responsabilidade civil

---

[80] O artigo 8°, parágrafo 1° do Decreto-lei nº 5.452, de 1943 (BRASIL, 1943), a Consolidação das Leis do Trabalho (CLT), com a alteração promovida pela Lei 13.467/2017, estabelece a aplicação subsidiária do direito comum ao direito do trabalho.

[81] Atualmente, existem mais de trinta leis setoriais vigentes que regulam diversos aspectos da proteção de dados no Brasil. Como essas normativas continuarão existindo após a entrada em vigor da nova Lei Geral de Proteção de Dados, caberá à Autoridade Nacional de Proteção de Dados e ao Poder Judiciário a solução dos eventuais conflitos normativos que possam surgir (LIMA, 2018, p. 27).

objetiva do Estado pelos danos suportados pelo trabalhador no caso da divulgação de trâmites processuais e decisões judiciais que contenham dados pessoais de caráter íntimo, já que a destinação ofertada a essas informações não obteve o consentimento do titular, tratando-se de uma das hipóteses legais ensejadoras de acesso restrito.

Outra normativa de especial relevância é a Lei nº 12.965, de 23 de abril de 2014, conhecida como o "Marco Civil da Internet", que regulamenta o uso da *Internet* no país, estabelecendo princípios, garantias, direitos e deveres, e elencando, em seu artigo 3°, II e III, a proteção da privacidade e dos dados pessoais como princípios que disciplinam o uso da rede mundial de computadores no Brasil (BRASIL, 2014). Até a entrada em vigor da nova Lei Geral de Proteção de Dados Pessoais, esta normativa representa a principal regulamentação relativa à proteção de dados pessoais no país, ainda que se dirija especialmente ao âmbito da *Internet*.

O Marco Civil da Internet sustentou-se sob os pilares da privacidade e da proteção de dados, temas que ganharam protagonismo no texto legal como forma de oferecer uma resposta rápida aos usuários da rede no Brasil, após as revelações de Edward Snowden acerca da vigilância implementada pelo governo norte-americano (LIMA; BIONI, 2015, p. 265). Um dos seus pontos de destaque é o estabelecimento de uma longa adjetivação ao consentimento (informado e expresso) exigido para a coleta, tratamento e utilização dos dados pessoais, o que pode ser considerado como um avanço importante dentro do contexto em que foi editada, apesar da omissão quanto à maneira pela qual o usuário pode expressar este consentimento (LIMA; BIONI, 2015, p. 286-7).

É possível constatar que todas as normas que regem o sistema protetivo de dados pessoais do MCI orbitam sob a figura central do usuário, e este, uma vez cientificado do tratamento, poderá exercer o controle (desde a fase da coleta de dados até o término da relação junto ao fornecedor de produtos e serviços de *Internet*) por meio do consentimento. Diante disso, resta evidente que a autodeterminação informativa representou o parâmetro normativo adotado pelo MCI na tutela de dados pessoais (BIONI, 2019, p. 132).

A lei disciplina, em seu artigo 7°, os direitos e garantias dos usuários, dentre eles o direito de obter informações claras e completas sobre a coleta, uso, armazenamento, tratamento e proteção de dados pessoais, sendo que a sua utilização está condicionada às finalidades que justifiquem a sua coleta, o que possui relação com os princípios da transparência, da finalidade e da proporcionalidade no tratamento de dados pessoais, bem como o respeito ao contexto com que os dados foram coletados. Tais finalidades não poderão, ainda, ser vedadas pela legislação, e deverão estar especificadas no contrato firmado ou nos termos de uso do *site* acessado (BRASIL, 2014).

Todas essas disposições apontaram o norte para o qual deveria seguir a regulamentação da proteção de dados pessoais no Brasil, galgando os primeiros passos rumo à edição de uma lei que contemplasse o nível protetivo almejado para a inserção do país no padrão europeu. Entretanto, nas palavras de Tepedino e Teffé (2019, p. 290), "[...] esse arcabouço regulatório mostrava-se pouco preciso e não oferecia garantias adequadas às partes, o que, além de gerar insegurança jurídica, acabava tornando o País menos competitivo no contexto de uma sociedade cada vez mais movida a dados".

Os debates para a construção do tão aguardado marco regulatório para a proteção de dados pessoais no Brasil tiveram início em 2010, por iniciativa do Ministério da Justiça, que lançou a primeira consulta pública de um Anteprojeto de Lei (BIONI, 2018). As iniciativas tomaram forma na Câmara dos Deputados, através do Projeto de Lei nº 4060/2012 (BRASIL, 2012a) de autoria do deputado Milton Monti, e do Projeto de Lei nº 5276/2016 (BRASIL, 2016a), resultado das diversas consultas públicas que foram retomadas em 2015, por meio de uma plataforma *online,* com o recebimento de contribuições de toda a sociedade (BIONI, 2015, p. 8). Depois de tramitar em regime de urgência por um período, o PL nº 5276/2016 acabou apensado ao PL nº 4060/2012, e assim permaneceu até a pauta ser retomada no país, após o escândalo envolvendo a Cambridge Analytica[82], e com a entrada em vigor do Regulamento Geral sobre Proteção de Dados (RGPD) da União Europeia.

Após alguns anos de tramitação na Câmara dos Deputados, no dia 29 de maio de 2018 foi aprovado o texto legal que rumou ao Senado Federal sob o número 53/2018 (BRASIL, 2018c), poucos dias após a eficácia plena do GDPR[83], demonstrando a tentativa apressada de adequação nacional aos padrões exigidos internacionalmente, até porque a normativa europeia veda a transferência internacional de dados a países sem a devida adequação legislativa, como era o caso brasileiro naquele momento.

No Senado Federal, o PLC n° 53/2018 foi apensado ao PLS n° 330, de 2013 (BRASIL, 2013), de autoria do Senador Antônio Carlos Valadares, obtendo sua aprovação em 10 de julho de 2018. A Lei Geral de Proteção de Dados (LGPD) brasileira, que ganhou o número 13.709/2018, foi sancionada pelo então presidente Michel Temer no dia 14 de agosto de 2018,

[82] O escândalo foi deflagrado pelo jornal The New York Times, em 17 de março de 2018, que revelou que mais de 50 milhões de usuários do Facebook tiveram seus dados pessoais tratados pela Cambridge Analytica, sem o devido consentimento, com o objetivo de manipulação das eleições presidenciais norte-americanas de 2016, em favor do então candidato Donald Trump (THE NEW YORK TIMES, 2018).
[83] O RGPD, de 27 de abril de 2016, tornou-se plenamente aplicável em 25 de maio de 2018.

e entrará em vigor após decorridos vinte e quatro meses de sua publicação, ou seja, em agosto de 2020[84] (BRASIL, 2019b).

Juntamente com o respeito à privacidade, a liberdade de expressão, de informação, de comunicação e de opinião e a inviolabilidade da intimidade, da honra e da imagem, dentre outros, a lei estabeleceu expressamente a autodeterminação informativa como um de seus fundamentos (artigo 2º) (BRASIL, 2018a), incorporando definitivamente este direito ao ordenamento jurídico brasileiro, em consonância com a ampla doutrina nacional e com as normativas europeias. Para Cots e Oliveira (2018, p. 64), o fundamento da autodeterminação informativa concilia a exteriorização da vontade do titular com a obrigação do controlador[85] em informar a respeito do tratamento oferecido aos seus dados pessoais.

Feito este destaque inicial, a análise da LGPD demanda a retomada dos critérios elencados anteriormente, a começar pelo âmbito de aplicação. No que se refere ao escopo de aplicação material[86], a normativa abrange de forma ampla e geral a toda e qualquer atividade que envolva a utilização de dados pessoais (coleta, armazenamento, compartilhamento, exclusão etc.), seja por pessoa natural ou pessoa jurídica de direito público ou privado (artigo 3°, *caput*). Inspirado no Regulamento Geral de Proteção de Dados europeu, a lei brasileira apresenta aplicação extraterritorial, ou seja, é aplicável também para empresas que não possuam estabelecimento no Brasil, desde que o tratamento[87] seja realizado em território nacional (art. 3º, I), o tratamento tenha por finalidade a oferta de bens ou serviços ao mercado consumidor brasileiro ou o tratamento de dados de indivíduos localizados no país (artigo 3º, II), ou que os dados tenham sido coletados no território nacional (artigo 3º, III) (BRASIL, 2018a).

O exame das hipóteses previstas nos incisos do artigo 3º permite concluir que se o tratamento ocorrer no território brasileiro, não importa que seja realizado apenas com dados

---

[84] O período de *vacatio legis* da Lei Geral de Proteção de Dados foi alterado pela Lei nº 13.853/2019 (BRASIL, 2019b), que ampliou o prazo geral de dezoito meses para vinte e quatro meses. Além disso, a lei estabeleceu um prazo diferenciado para as normas disciplinadas no Capítulos IX, que dizem respeito à Autoridade Nacional de Proteção de Dados e ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, que passaram a vigorar no dia 28 de dezembro de 2018. Com isso, foi convertida em lei a Medida Provisória nº 869, de 2018 (BRASIL, 2018b), que havia sido editada pelo presidente Jair Bolsonaro em 27 de dezembro de 2018.

[85] O artigo 5º, IV conceitua a figura do controlador como sendo a "[...] pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais" (BRASIL, 2018a).

[86] As hipóteses de não incidência da LGPD estão previstas no artigo 4º, abrangendo o tratamento de dados para fins de uso particular (inciso I), fins exclusivamente jornalísticos, artísticos ou acadêmicos (inciso II), fins de interesse público relacionados à segurança e defesa nacional (inciso II) e o tratamento de dados oriundos do exterior que não sejam objeto de comunicação ou compartilhamento com agentes brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência (inciso III) (BRASIL, 2018a).

[87] Por tratamento, entende-se "[...] 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", nos termos do artigo 5º, X (BRASIL, 2018a).

colhidos de pessoas naturais estrangeiras, aplica-se a lei. Por outro lado, a LGPD protege qualquer indivíduo que se localize em território nacional do tratamento de dados que tenha por objetivo a oferta de produtos ou serviços a este mercado, ainda que possa tratar-se de estrangeiro em breve passagem pelo país (COTS; OLIVEIRA, 2018, p.79).

Partindo para o segundo critério de análise, qual seja, a identificação das bases legais para o tratamento de dados, verifica-se que o artigo 7º da LGPD estabelece dez hipóteses[88] que autorizam o tratamento de dados pessoais, a começar do consentimento do titular. A lei não demonstra distinção hierárquica entre as hipóteses autorizadoras do tratamento de dados pessoais, mas ainda assim é possível considerar o consentimento como o vetor principal das demais bases legais de tratamento de dados pessoais, inclusive porque os princípios elencados pela lei focam-se no protagonismo do indivíduo no controle do fluxo de suas informações pessoais (BIONI, 2019, p. 134).

Alguns autores, tais como Cots e Oliveira (2018, p. 114), defendem a natureza jurídica contratual do consentimento, tendo em vista que representa a manifestação de vontade do agente em realizar o tratamento para determinada finalidade, com a anuência do titular. Tal entendimento é tido como inadequado por Tepedino e Teffé (2019, p. 299), já que reforçaria uma relação de troca de natureza econômica entre o titular de dados e o responsável pelo tratamento, fomentando a aplicação de uma lógica inerente aos direitos de propriedade à tutela de dados pessoais. Diante disso, compartilha-se da posição de Tepedino e Teffé (2019, p. 299), por entender que o consentimento é um instrumento vinculado aos direitos de personalidade, que compreende a liberdade de escolha e reforça a esfera de autonomia individual, e que, portanto, não possui natureza negocial.

---

[88] "Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
I - mediante o fornecimento de consentimento pelo titular;
II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente" (BRASIL, 2018a).

O consentimento, que o artigo 5º, XII da lei define como a "[...] manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada", deverá ser fornecido por escrito (em cláusula destacada das demais), ou por qualquer outro meio capaz de demonstrá-lo de forma inequívoca, especificando-se as finalidades determinadas, e poderá ser revogado a qualquer tempo, conforme as determinações do artigo 8º, *caput* e parágrafos (BRASIL, 2018a). Ao permitir o fornecimento do consentimento por quaisquer outros meios, além dos escritos, que permitam a sua demonstração inequívoca, a lei admite a manifestação do consentimento através de arquivos de áudio e vídeo, *e-mail* ou SMS, dentre outros, desde que devidamente relacionado aos termos do tratamento de dados especificado (COTS; OLIVEIRA, 2018, p. 115).

Visando impedir as "políticas de tudo ou nada" (TEPEDINO; TEFFÉ, 2019, p. 300), em que o usuário não dispõe de outra opção a não ser o consentimento ou não será fornecido o acesso ao produto ou serviço, a lei dispõe, em seu artigo 9º, parágrafo 3º, que se o tratamento de dados for condição para o fornecimento de produto, serviço ou para o exercício de direito, o titular deverá ser informado de maneira destacada sobre esse fato e sobre os meios pelos quais poderá exercer os direitos elencados pelo artigo 18 (BRASIL, 2018a). Esse dispositivo incentiva a possibilidade de manifestação de consentimento de forma modular, emitindo autorizações fragmentadas de acordo com as diferentes funcionalidades ofertadas (TEPEDINO; TEFFÉ, 2019, p. 301).

Assim, tomando-se como exemplo o tema central desta pesquisa, dentre as diversas formas de expressar o consentimento do reclamante com relação ao tratamento de seus dados em ação judicial, uma das mais viáveis seria o protocolo no Processo Judicial Eletrônico (PJe) de manifestação assinada pelo reclamante, especificando-se as finalidades do tratamento de dados, mas também poderiam ser admitidas a juntada de arquivo de áudio ou vídeo, ou até a manifestação oral em audiência. Entretanto, o consentimento específico com relação à divulgação de dados pessoais em portais institucionais na *Internet* pela Justiça do Trabalho não poderia ser uma exigência indispensável ao ajuizamento da ação, diante da cláusula inscrita no artigo 9º, parágrafo 3º da LGPD, adotando-se o modelo de configurações personalizáveis da privacidade para diferentes categorias de tratamento.

Ainda que o consentimento seja o principal requisito, a LGPD inovou ao estabelecer diversas outras hipóteses que permitem o tratamento de dados pessoais, mesmo sem a

manifestação de vontade do titular[89]. No caso das relações empregatícias, algumas situações decorrentes do contrato de trabalho impõem a necessidade de coleta de dados do empregado, tais como a ficha de registro e o encaminhamento de informações à Previdência Social, FGTS, Receita Federal e Ministério do Trabalho, incluindo o Cadastro Geral de Empregados e Desempregados (Caged) e a Relação Anual de Informações Sociais (Rais), etc. O processamento dessas informações é autorizado pelo artigo 7º inciso II, que se refere ao cumprimento de obrigação legal ou regulatória. Além disso, os dados que integram os exames de saúde admissionais, periódicos e demissionais e os programas de Saúde Ocupacional (PCMSO, PPRA, PPP, etc.), foram contempladas pelo 7º inciso III, que permite o tratamento de dados visando a tutela da saúde, em procedimento realizado por profissionais da área ou por entidades sanitárias (BRASIL, 2018a).

No que se refere ao tratamento de dados pessoais no âmbito processual trabalhista, principal foco deste estudo, o primeiro destaque deve ser feito ao inciso VI do artigo 7º, que permite o tratamento de dados quando for necessário para o exercício regular de direitos em processo judicial, administrativo ou arbitral (BRASIL, 2018a). Este dispositivo, para Ana Frazão (2018a), é "[...] fundamental para deixar claro que a proteção aos dados pessoais não compromete o necessário direito que as partes têm de produzir provas umas contra as outras, ainda que estas se refiram a dados pessoais do adversário". Garante, com isso, ao empregador que for demandado judicialmente, o direito de defender-se levando ao processo as informações que dispuser do trabalhador, tais como cadastros, exames médicos, atestados, cartões-ponto, etc., sem a necessidade de consentimento do titular dos dados.

Entretanto, do ponto de vista do reclamante em processo laboral, tal dispositivo dispensa o seu consentimento com relação ao tratamento dos dados que são fornecidos em virtude do exercício do direito de ação, o que se mostraria uma medida razoável não fosse o fato de que os dados acabam sendo utilizados para finalidades distintas das quais foram fornecidos. Justamente por conta disso, o artigo 21 da lei estabelece que os dados pessoais tratados com a finalidade de exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo (BRASIL, 2018a), determinação que não poderia ser desrespeitada pela divulgação de dados pessoais (sensíveis ou não) do obreiro pelos portais institucionais da justiça laboral, já que as consequências dessa publicização não lhe trazem qualquer benefício, muito pelo contrário.

[89] É dever do controlador e do operador manter registro das operações de tratamento (artigo 37), devendo eliminar de imediato os dados que não estejam devidamente justificados por uma das bases legais de tratamento de dados (VAINZOF, 2019, p. 123).

Não fosse o bastante, o inciso IX do artigo 7º autoriza o tratamento de dados pessoais quando se mostrar necessário para atender aos interesses legítimos do controlador ou de terceiro (o que poderia incluir a própria prestação jurisdicional como função precípua da Justiça do Trabalho, incluindo o seu dever de publicidade), mas excetua os casos em que prevalecerem direitos e liberdades fundamentais que exijam a proteção de seus dados pessoais (BRASIL, 2018a), como é o caso da privacidade atingida pela divulgação dessas informações. Observa-se que o conceito de "legítimo interesse" disposto na lei é vago, abrindo espaço para as mais diversas interpretações. A cláusula aberta, inspirada em regramento semelhante do RGPD da União Europeia, suscitou debates também no direito europeu, por conta do receio de flexibilização do conteúdo protetivo da lei (BUCAR; VIOLA, 2019, p. 467).

Na tentativa de definição de um conteúdo à cláusula geral de interesse legítimo, conclui-se pela sua interpretação e preenchimento no caso concreto, utilizando-se a ponderação de interesses para o sopesamento no caso de colisão entre direitos (BUCAR; VIOLA, 2019, p. 472-4). Entretanto, havendo conflito entre interesses patrimoniais e existenciais, torna-se evidente a prevalência destes, já que a dignidade humana prepondera sobre interesses econômicos, que devem ser funcionalizados à proteção da pessoa (BUCAR; VIOLA, 2019, p. 483). É possível, por exemplo, que se interprete ser um interesse legítimo, fundado no direito de acesso à informação e no direito à propriedade, o da empresa que coleta informações públicas, agrupa e divulga através de ferramentas de busca na *Internet* (a exemplo dos portais Escavador e Jus Brasil). Neste caso, o próprio artigo traz a limitação, tendo em vista ser esse um interesse patrimonial de terceiro que esbarra nos direitos fundamentais do jurisdicionado.

Ademais, o artigo 10, § 1° estabelece a observância do princípio da necessidade como requisito para o tratamento de dados na hipótese de interesse legítimo do controlador, ou seja, somente os dados pessoais estritamente necessários poderão ser tratados (BRASIL, 2018a), o que significa dizer que, neste caso, ainda que pudesse ser dispensado o consentimento do titular, não poderia haver a transferência, distribuição ou divulgação de dados que excedam as finalidades para os quais foram coletadas.

O terceiro critério de análise foca nos dados sensíveis, cujo tratamento torna o titular suscetível à toda sorte de discriminações, como a estigmatização, a exclusão ou a segregação, atingindo a sua dignidade humana, sua identidade pessoal e privacidade (KONDER, 2019, p. 455). Estes dados são definidos pela lei como relacionados à "[...] origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (BRASIL, 2018a), conceito que foi utilizado como

parâmetro para a categorização das pesquisas jurisprudenciais realizadas neste trabalho. O própria legislador reconhece que este não é um rol taxativo (KONDER, 2019, p. 455), na medida em que estende o mesmo rigor de tutela a todos os dados pessoais que, ainda que não sejam sensíveis em uma primeira análise, possam revelarem-se sensíveis após o tratamento, c com isso causar danos a seu titular, conforme dispõe o parágrafo 1º do artigo 11 (BRASIL, 2018a).

Além do consentimento do titular, que deverá ser fornecido de forma específica e destacada, direcionado a finalidades específicas[90] (Art. 11, I), a lei restringe o rol de hipóteses que autorizam o tratamento de dados sensíveis sem a sua anuência (artigo 11, II) (BRASIL, 2018a), adotando um catálogo mais fechado em relação ao tratamento de dados pessoais em geral, disposto no artigo 7° (BIONI, 2019, p. 229). Dentre os dispositivos afastados (bases legais cujo tratamento é autorizado para os dados pessoais em geral, mas não reproduzidas na seção referente ao tratamento de dados sensíveis) estão o tratamento necessário para a execução de contrato, o necessário para atender aos interesses legítimos do controlador ou de terceiro e o necessário para a proteção do crédito, todas hipóteses que envolvem interesses patrimoniais, o que não justificaria o risco intrínseco da manipulação de dados sensíveis (KONDER, 2019, p. 458).

Dentre as bases legais elencadas pelo artigo 11, chama a atenção o fato de que mesmo os dados sensíveis poderão ser objeto de tratamento, ainda que sem o consentimento, quando necessários para o exercício regular de direitos em processo judicial. Ou seja, no caso de informações sensíveis do trabalhador reportadas em processos judiciais, tais como aquelas relacionadas à sua saúde ou sexualidade, eventual tratamento de dados sem o consentimento do titular poderia ser autorizado por tal disposição, esbarrando apenas na regra estabelecida pelo artigo 21, que veda a utilização desses dados em prejuízo do reclamante (BRASIL, 2018a).

Ao dispor de diversas situações que dispensam o consentimento do titular em face de tratamento de seus dados sensíveis, em grande parte em hipóteses que envolvem um suposto interesse público, a lei acaba por realizar uma evidente ponderação de interesses, dando prevalência aos interesses de natureza pública em face dos interesses do titular, ainda que se tratem de direitos fundamentais (MULHOLLAND, 2018, p. 168). Diante de tal discrepância, Mulholland (2018, p. 168) tece críticas ao posicionamento legislativo, por entender que a tutela

[90] O consentimento para o tratamento de dados sensíveis, além da necessidade de ser livre, informado e inequívoco (conforme preceitua o artigo 5º, XII, para os dados pessoais em geral), também deverá ser específico e destacado, para finalidades específicas, exigências adicionais elencadas pelo artigo 11, I (BRASIL, 2018a).

dos dados pessoais sensíveis pressupõe o pleno exercício de direitos fundamentais, especialmente os da igualdade, liberdade e privacidade.

No mesmo sentido, Rosane Leal da Silva (2018, p. 336) aponta uma inconsistência na lei brasileira diante da hipótese que permite o tratamento de dados sensíveis para o exercício de direitos em processos judiciais, já que o legislador não se preocupou em estabelecer qualquer restrição ou obrigação aos Tribunais no tratamento dessas informações, especialmente na divulgação de informações processuais por meio de seus portais institucionais. O legislador demonstra, com esta omissão, que este risco é invisível aos seus olhos, ou ainda, que os direitos dos jurisdicionados não são importantes para o Poder Judiciário (SILVA, R., 2018, p. 336).

Vale ressaltar que a LPGD inspira-se em larga escala no RGPD da União Europeia, que também permite o tratamento de dados sensíveis quando necessários ao exercício ou à defesa de direitos em processo judicial (UNIÃO EUROPEIA, 2016), mas naquele caso a normativa delimita o tratamento de dados pelo Poder Judiciário às situações em que os tribunais atuem no exercício de sua função jurisdicional, o que não foi contemplado pela lei brasileira. Ao não disciplinar, de forma pontual e específica, as atribuições e os limites da atuação do Estado no tratamento de dados sensíveis que são deixados ao seu abrigo pelo ajuizamento de ações, a LGPD permite um amplo espaço para interpretações das mais diversas, abrindo caminho para a discricionariedade.

Justamente por conta de seu potencial de utilização para finalidades discriminatórias, e visando a garantia de plenitude à esfera pública, determinadas categorias de dados sensíveis (tais como opiniões políticas e sindicais, raça ou credo religioso) devem ser submetidos a rigorosas condições de circulação[91] (inclusive com a restrição de coleta a determinados sujeitos, como os empregadores) (RODOTÁ, 2008, p. 96). Dessa forma, o grande número de situações que autorizam o tratamento de dados sensíveis pela legislação brasileira representa um ponto falho neste sistema protetivo, inclusive pela considerável abertura semântica, como é o caso, por exemplo, dos dados necessários ao exercício regular de direitos.

Se a lei brasileira falha por demonstrar um baixo caráter protetivo em relação aos dados sensíveis, o mesmo não pode ser dito com relação aos direitos garantidos aos titulares (quarta categoria de análise), disciplinados pelo Capítulo III da LGPD. Além de reiterar, em seu artigo 17, as garantias constitucionais da liberdade, da intimidade e da privacidade, a lei assegura, dentre outros, os direitos de acesso, correção, anonimização, bloqueio e eliminação de dados

[91] Rodotá (2008, p. 129) visualiza um paradoxo na tutela especial atribuída às opiniões políticas e sindicais, na medida em que se tratam de dados que, especialmente em Estados democráticos, deveriam caracterizar a esfera pública, mas que recebem o máximo de proteção privada, frente às possíveis discriminações sofridas pelo titular.

desnecessários, excessivos ou tratados em desconformidade com a lei, bem como o direito de revogação do consentimento, todos eles no artigo 18 (BRASIL, 2018a).

Todo esse catálogo de direitos nada mais faz do que especificar, através da enunciação de "remédios", os conteúdos representativos da noção contemporânea de privacidade, qual seja, a autodeterminação informativa (SOUZA; SILVA, 2019, p. 262). Ora, se a autodeterminação informativa diz respeito ao direito atribuído ao titular de gerir o fluxo de seus dados pessoais, assim o faz através da adoção de medidas e procedimentos que lhe garantam a possibilidade de descobrir a existência de bancos de dados em seu nome, de ter acesso à esses dados, de retificá-los e de solicitar o cancelamento do tratamento, quando entender necessário.

Todas essas medidas, definidas pela LGPD como direitos do titular, tratam-se, conforme o entendimento de Souza e Silva (2019, p. 265), de mecanismos instrumentais voltados à viabilização da tutela dos direitos propriamente ditos (tais como a própria privacidade), e por isso não devem corresponder a um fim em si mesmo, posição que é compartilhada por esta pesquisa, ainda que se possa estabelecer uma exceção para o direito à eliminação de dados, por constituir-se em um dos elementos do direito ao esquecimento, dotado de autonomia.

Com relação ao direito de eliminação de dados pessoais, previsto no artigo 18, VI da LGPD, e que já integrava o rol de direitos do usuário no Marco Civil da *Internet*, Guedes e Meireles (2019, p. 227-8) fazem questão de estabelecer uma distinção conceitual com o direito ao esquecimento, tal como entendido pela jurisprudência, que se relaciona muito mais à possibilidade de fatos do passado não sofrerem uma eterna veiculação pública, por meio da desindexação de determinados termo, do que propriamente pela eliminação dos dados após o término do tratamento, ou pela revogação do consentimento. Para os autores, o verdadeiro fundamento do direito ao esquecimento no ordenamento jurídico brasileiro é a própria Carta Magna, e não a LGPD ou o MCI (GUEDES; MEIRELES, 2019, p. 228). Compartilhando de opinião semelhante, Bioni e Mendes (2019, p. 810) acreditam que o direito ao esquecimento não está claro no texto da LGPD, apesar de constar expressamente no RGPD europeu.

Com posicionamento mais radical, Schreiber (2019, p. 380) entende que nem a LGPD e tampouco o RGPD europeu (ainda que utilize a expressão "direito a ser esquecido") trabalham com o direito ao esquecimento propriamente dito, entendido pelo autor como "direito do indivíduo de se opor à recordação pública e opressiva de fatos que já não mais refletem sua identidade pessoal", mas sim referem-se ao direito à eliminação de dados, cujo conteúdo e finalidades seriam diferenciados. Por outro lado, Fincato e Guimarães (2019, p. 281) visualizam uma insuficiência normativa na LGPD, já que o país não conta com um direito regulamentado que permita a opção de escolha entre a divulgação ou não de determinados episódios de sua

vida. Para as autoras (2019, p. 281), somente a não postagem garantiria a efetividade e a eficácia do direito ao esquecimento.

A par destes posicionamentos, e mesmo reconhecendo-se que o direito à desindexação é a principal forma de efetivação do direito ao esquecimento na contemporaneidade, optou-se, para fins conceituais, pela filiação à definição estabelecida por Fortes (2016, p. 186), adequada à terminologia utilizada pelo RGPD da União Europeia, compreendendo o direito do usuário de deletar dados pessoais na *Internet* dentro da esfera de abrangência deste direito. Entende-se, com isso, que o artigo 18, VI da LGPD contempla, de forma expressa, assim como faz a lei argentina, o reconhecimento do direito ao esquecimento no ordenamento jurídico pátrio, como um dos aspectos da autodeterminação informativa, ainda que possa ser discutível a efetividade deste direito diante da velocidade de propagação dessas informações no meio virtual.

Dentre o rol de direitos listado no artigo 18, o direito à anonimização de dados deve ser observado com atenção, já que se trata de medida não extremada que pode permitir o tratamento de dados sem oferecer uma consequência tão nociva ao seu titular, oferecendo uma resposta com melhor custo benefício à sociedade nos casos envolvendo a divulgação de informações necessárias à transparência pública. A anonimização é descrita pela LGPD, em seu artigo 5º, XI, como a "[...] 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", enquanto os dados anonimizados[92], decorrentes do processo de anomização, são conceituados pelo artigo 5º, III, da lei como dados relativos "[...] a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento" (BRASIL, 2018a).

Ressalta-se que o Brasil, inspirado pelo RGPD europeu, também adotou expressamente a metodologia do *privacy by design*, ao determinar, em seu artigo 46, parágrafo 2º, que as medidas de segurança e de sigilo de dados deverão ser observadas "[...] desde a fase de concepção do produto ou do serviço até a sua execução". Este conceito, que parte da ideia de que a proteção de dados deve conduzir a concepção de um produto ou serviço à partir da utilização de tecnologias que facilitem o controle e a proteção de dados pessoais desde a sua arquitetura, tem na anonimização de dados uma de suas técnicas capazes de proteger a privacidade dos cidadãos (BIONI, 2019, p. 176-7).

Tanto a anonimização como os demais direitos listados, especialmente os direitos ao bloqueio ou eliminação de dados excessivos e a eliminação dos dados tratados com ou sem o

[92] A LGPD não considera o dado anonimizado como um dado pessoal, resultando na inaplicabilidade da sua regulamentação para os dados que passaram pelo procedimento de anonimização (VAINZOF, 2019, p. 95).

consentimento do titular garantem ao jurisdicionado uma ampla gama de ferramentas que podem ser invocados visando não só a exclusão definitiva das informações disponibilizadas na *Internet*, mas a desindexação de seus dados reportados nos julgados ou mesmo a impossibilidade de identificação do titular. Para tanto, o titular deverá formular um requerimento expresso endereçado ao agente de tratamento, que poderá acolher o pedido ou negá-lo, comunicando que não é o agente responsável pelo tratamento e indicando o agente correto ou indicando as razões que impedem a adoção das providências solicitadas (§§3° e 4°) (BRASIL, 2018a). Além disso, o titular possui o direito de peticionar perante a Autoridade Nacional de Proteção de Dados (ANPD) (§1°) (BRASIL, 2018a), o que lhe confere a possibilidade de buscar o cumprimento dos direitos legalmente previstos pela via administrativa.

Vale lembrar que a previsão de requerimento expresso do titular ao agente de tratamento ou à própria Autoridade Nacional de Proteção de Dados não afasta a legitimidade do Ministério Público do Trabalho[93] ou mesmo dos Sindicatos[94] para peticionarem em prol dos interesses de determinada categoria ou grupos de trabalhadores. A atuação de tais entes pode suprir os déficits (principalmente o informacional) que costumam reduzir a efetividade da tutela individual buscada pelo titular dos dados (SOUZA; SILVA, 2019, p. 278-9).

Existe, ainda, a possibilidade do titular dirigir-se ao encarregado de proteção de dados, figura inspirada no DPO (*data protection officer*) do RGPD europeu, que consiste em uma "[...] 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, 2018a), nos termos do artigo 5º, VIII da lei. Ao encarregado são atribuídas as funções de receber reclamações e comunicados dos titulares e da autoridade nacional, prestando esclarecimentos e adotando providências, conforme dispõe o artigo 41 da lei (BRASIL, 2018a). Dentre as suas atividades, incluem-se também o auxílio no desenvolvimento de produtos e serviços por meio da adoção de metodologias como o próprio *privacy by design* (XAVIER; XAVIER; SPALER, 2019, p. 493).

---

[93] A atuação do Ministério Público do Trabalho (MPT) é de extrema importância para a efetivação do direito à autodeterminação informativa dos reclamantes no âmbito do processo laboral, através de uma atuação judicial e extrajudicial na defesa de interesses difusos e coletivos, inclusive pleiteando a adequação dos *sites* dos Tribunais trabalhistas às diretrizes legais de proteção de dados.

[94] Nos casos envolvendo ações coletivas em matéria de tutela de dados pessoais, quando a Administração Pública figurar no polo passiva e houverem pedidos relacionados à divulgação de informações pessoais do jurisdicionado pelos portais institucionais dos Tribunais, a decisão judicial deverá determinar modificações com vista a implementar uma reforma estrutural na forma de tratamento de dados pessoais sensíveis (as chamadas decisões estruturantes), ocasionando decisões em cascata (ROQUE; BAPTISTA; ROCHA, 2019, p. 767-8).

Feita esta observação acerca dos direitos garantidos ao titular e das vias de requerimento para buscar o seu cumprimento, observa-se que o legislador brasileiro (assim como também fez o argentino) optou por uma técnica regulamentar minuciosa, com base em instrumentos rígidos e não pela via das cláusulas gerais, que poderiam ser mais adequadas a acompanhar as rápidas mudanças tecnológicas, na posição de Souza e Silva (2019, p. 281). Sustenta-se, entretanto, que a técnica legislativa utilizada na construção de um catálogo rígido de direitos, revestidos como verdadeiras ferramentas à disposição do titular, somada às cláusulas gerais elencadas na formas de princípios que norteiam a interpretação da lei, foi apropriada, já que pode oferecer melhor resposta às demandas dos titulares de dados pessoais do que um conjunto de direitos de conteúdo eminentemente aberto, diante da necessidade por instrumentos que forneçam concretude às promessas legais.

Ainda é cedo para avaliar se tais mecanismos serão eficazes, proporcionando uma resposta célere e adequada, especialmente com relação às informações disponibilizadas pelo próprio Poder Público. Entretanto, levando-se em consideração as promessas feitas pela lei, no que se refere aos direitos garantidos aos titulares de dados pessoais, há um avanço importante em direção ao pleno exercício de um direito à autodeterminação informativa do jurisdicionado, já que poderia dispor livremente de seus dados pessoais, com a possibilidade de anonimização das informações que são divulgadas nas consultas processuais e jurisprudenciais, eliminação de informações sensíveis que não possuem qualquer interesse público e até mesmo oposição ao tratamento em caso de violação dos dispositivos legais.

Na sequência dos critérios a serem analisados estão os princípios de proteção dos dados, tópico que apresenta especial relevância diante do acentuado caráter principiológico demonstrado pela LGPD brasileira, em consonância com as normativas da União Europeia e com a própria lei argentina. Influenciada em larga escala por estes regramentos, o artigo 6° da LGPD elenca dez princípios, que deverão ser guiados pela boa-fé enquanto máxima de conduta: finalidade, adequação, necessidade, livre acesso, qualidade, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas.

Embora não tenha constado no rol de princípios específicos da proteção de dados pessoais elencados pela lei, mas sim no *caput* do artigo, não se discute a importância da boa-fé objetiva enquanto princípio geral a guiar os tratamento de dados pessoais, especialmente quando grande parte das bases legais que autorizam este tratamento possuem natureza contratual, incluindo o próprio consentimento (COTS; OLIVEIRA, 2018, p. 99). Tal é a importância da boa-fé nas relações negociais de um Estado Democrático (e Social) de Direito, enquanto limitador dos princípios liberais oitocentistas que serviam de diretrizes ao direito

contratual, que Rulli Neto (2011, p. 117) a define como uma nova forma de pensar que visa dar continuidade aos negócios jurídicos, visando a manutenção da confiança e a segurança das pessoas e da coletividade, o que é uma exigência do multiculturalismo, dos direitos sociais, dos direitos fundamentais, da pós-modernidade e da evolução social.

É nesse contexto que se inserem todos os demais princípios relacionados pelo artigo 6° da LGPD, a começar pela finalidade (inciso I), segundo o qual o tratamento deve ser realizado com vistas à execução de propósitos legítimos, específicos, explícitos e informados ao titular dos dados, sendo vedado o tratamento posterior de forma incompatível com estas finalidades (BRASIL, 2018a). Enquanto o objeto do princípio da finalidade é a regularidade dos fins que se buscam atingir com o tratamento, o princípio da adequação (inciso II) volta-se ao procedimento adotado para se chegar a tal finalidade (COTS; OLIVEIRA, 2018, p. 101). Este princípio determina que exista uma compatibilidade do tratamento com as finalidades que foram informadas ao titular, conforme o contexto do tratamento, relacionando-se ao princípio da necessidade (inciso III), que limita o tratamento ao mínimo necessário para a realização de tais objetivos, dispensando-se os dados excessivos (BRASIL, 2018a).

Na concepção de Regina Ruaro e Carlos Alberto Molinaro (2017, p. 32), o princípio da finalidade tem como função precípua resguardar "[...] o titular dos dados de uso por terceiros não legitimados na relação estabelecida com quem coleta os dados pessoais". Sua razão constitui-se na própria concepção de autodeterminação informativa, enquanto direito que se desdobra de uma concepção ampla de privacidade, oferecendo ao titular dos dados a proteção contra a utilização indevida de suas informações pessoais.

Observa-se que a finalidade específica da coleta de dados pelo Poder Judiciário é a própria prestação jurisdicional[95], não cabendo a posterior divulgação desses dados para terceiros via *Internet*, especialmente sem o consentimento do jurisdicionado e diante da possibilidade de utilização dessas informações para os fins mais diversos, que em nada dizem respeito aos propósitos do processo no qual o empregado figurou como parte, o que configura uma utilização excessiva dos dados pessoais, violando não somente o princípio da finalidade, mas também a própria boa-fé objetiva e o princípio da necessidade.

Não existem justificativas plausíveis para que as decisões judiciais reproduzam o completo detalhamento da vida íntima ou de aspectos da saúde do trabalhador, que já tiveram

[95] A jurisdição é um método heterocompositivo de resolução de conflitos, cujo exercício funda-se na soberania estatal e, no Brasil, legitima-se na Constituição de 1988, especialmente nos direitos fundamentais materiais e processuais (MARINONI; ARENHART; MITIDIERO, 2017, p. 178). A inafastabilidade da jurisdição é garantida pelo artigo 5º, XXXV da Carta Magna, ao determinar que "[...] a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito" (BRASIL, 1988).

a sua finalidade atingida ao longo do processo, através da formação do convencimento do julgador (SILVA, R., 2018, p. 336). A violação ao princípio da necessidade, cujo postulado indica a "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, 2018a), decorre da existência de outra soluções aptas a produzir o mesmo resultado, como seria, por exemplo, a simples medida de reportar na decisão o número do documento ou prova (SILVA, R., 2018, p. 336), ou seja, a indicação do ID no Processo Judicial Eletrônico, sem a necessidade de especificação dos pormenores.

Somado a isso, considere-se que o artigo 6°, IX estabelece o princípio da não discriminação, vedando o tratamento de dados pessoais para finalidades discriminatórias, ilícitas ou abusivas (BRASIL, 2018a). Este princípio coaduna-se ao regime jurídico mais protetivo oferecido pela lei brasileira ao tratamento de dados sensíveis, vinculando-se muito mais à proteção do direito à igualdade do que da intimidade propriamente dita (FRAZÃO, 2019, p. 107). Visa, dessa forma, "[...] garantir a ausência de traços diferenciais nas relações sociais, a fim de possibilitar que o indivíduo desenvolva livremente a sua personalidade" (BIONI, 2019, p. 86).

À luz do princípio da não discriminação, o empregador que obtiver, por meio da rede mundial de computadores, o acesso a dados pessoais de um candidato a vaga de emprego, tais como a notícia de que ele já ajuizou reclamações trabalhistas no passado, não poderá valer-se desta informação para oferecer tratamento distinto ao candidato, sob pena da reparação cabível pelo dano causado ao trabalhador, quando comprovado o ato ilícito (prova esta que representa uma enorme dificuldade para o obreiro).

Todos esses princípios devem orientar a atuação do controlador de dados (a própria Justiça do Trabalho, em um primeiro momento, bem como os buscadores e empregadores que fazem uso desses dados após a sua divulgação pela *Internet*), guiando todas as ações que envolvem o tratamento, assim consideradas as elencadas no art. 5°, X: "[...] coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração" (BRASIL, 2018a).

A nova lei, ao inserir uma cartela de princípios em seu artigo 6º, reitera diversos princípios do tratamento de dados que já podiam ser extraídos da legislação esparsa, impondo agora obrigações legais aos responsáveis pelo tratamento de dados, o que é importante para a concretização desse conteúdo axiológico, já que, como afirmam Oliveira e Lopes (2019, p. 60-1):

> [...] não basta conhecer e indicar os princípios de proteção aos dados pessoais. As forças do mercado e da administração pública reclamam que a lei contenha meios de proteção tangíveis, em disposições específicas e explícitas, para assegurar a proteção de dados pessoais, além de fornecer a segurança jurídica em seu tratamento.

Assim, ao invés de superar a legislação que a antecede, a LGPD passa a integrar, juntamente com as demais leis (incluindo o Marco Civil da Internet, o Código de Defesa do Consumidor e a Lei de Acesso à Informação) e os respectivos dispositivos, um verdadeiro sistema brasileiro de proteção de dados pessoais, norteado por essa principiologia (OLIVEIRA; LOPES, 2019, p. 82).

É importante, dessa forma, que seja instituído um órgão de controle capaz de fiscalizar a aplicação da lei, autoridade que, como se viu, foi implementada pela União Europeia e também pela Argentina. É neste ponto que se insere a quinta categoria de análise, qual seja, a existência ou não de um órgão regulador de proteção de dados. Observa-se que a criação de uma Autoridade Nacional de Proteção de Dados foi, inicialmente, vetada pelo então presidente Michel Temer, na edição da Lei nº 13.709/2018, sob o argumento da existência de um vício de iniciativa: a criação de uma autoridade como essa deveria partir de uma iniciativa do Poder Executivo e não do Poder Legislativo.

Entretanto, após a edição da Medida Provisória nº 869/2018, foi sancionada pelo presidente Jair Bolsonaro a Lei nº 13.853, de 8 de julho de 2019, que alterou a LGPD em diversos pontos, além de criar a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, responsável por zelar pela aplicação da lei, fiscalizando e aplicando sanções em caso de tratamento de dados realizado em descumprimento à legislação e editando regulamentos e procedimentos acerca da proteção de dados pessoais e privacidade (BRASIL, 2019b). Assim como ocorreu na Argentina, o órgão de controle brasileiro vincula-se ao Poder Executivo (no caso do Brasil, será integrado à Presidência da República), o que limita em muito a sua liberdade de atuação, em que pese a lei garanta uma "[...] autonomia técnica e decisória à ANPD" (BRASIL, 2019b).

Diante disso, o modelo proposto pela lei não garante a autonomia e independência funcional, administrativa e financeiras necessárias ao exercício autoridade reguladora, já que o "Mero enunciado normativo de autonomia técnica não afasta as exigências fáticas que caracterizam uma entidade de fato autônoma" (VASCONCELOS; PAULA, 2019, p. 731). Dentre os principais problemas da vinculação da ANPD à Presidência da República, é previsível a redução da capacidade fiscalizatória com relação ao tratamento de dados pelo Poder Público,

além da ausência da autonomia necessária e exigida por outros países, tais como os Estados-Membros da União Europeia, para assegurar a cooperação jurídica internacional com relação ao fluxo de dados transnacionais (VASCONCELOS; PAULA, 2019, p. 732). Soma-se isto à revogação dos parágrafos 1º e 2º do artigo 7º pela Lei nº 13.853/2019, que estabeleciam ao Poder Público obrigações de transparência ao titular dos dados, e vislumbra-se uma preocupante possibilidade de utilização indevida dos dados pessoais de cidadãos pelos órgãos da administração pública, suspeita que é partilhada por Vasconcelos e Paula (2019, p. 733).

A importância de autoridades de controle livres de influências externas nos estado ibero-americanos é destacada pelo Padrão de Proteção de Dados Pessoais para os Estados Ibero-Americanos (REDE IBERO-AMERICANA..., 2017, p. 11), em seu considerando 24:

> Admitindo a necessidade imperiosa de que cada Estado Ibero- Americano conte com autoridade de controle independente e imparcial em suas faculdades, cujas decisões somente possam ser recorríveis pelo controle judicial, alheia a qualquer influência externa, com poderes de supervisão e investigação em matéria de proteção de dados pessoais, e encarregada de zelar pelo cumprimento da legislação nacional na matéria, que possua recursos humanos e materiais suficientes para garantir o exercício de seus poderes e o desempenho efetivo de suas funções;

A garantia de um órgão de controle dotado de independência e autonomia também importa diante da sua competência para apreciar petições apresentadas pelo titular contra o controlador, em caso de infrutífera a reclamação diretamente ao controlador (art. 55-J, V), bem como solicitar às entidades do poder público informações específicas acerca das operações de tratamento de dados pessoais por elas realizadas, incluindo o âmbito e a natureza dos dados (art. 55-J, XI) (BRASIL, 2019b). Todas essas atribuições, caso sejam devidamente executadas, poderão representar uma perspectiva positiva em relação à implementação da LGPD no Brasil, já que os setores público e privado deverão, em tese, passar por um reajuste profundo a fim de adequarem-se aos preceitos legais, o que precisará ser supervisionado pela Autoridade (e por isso a sua liberdade é tão importante).

Cumpre referir que a lei estabelece um "poder de autocontrole administrativo" (TASSO, 2019, p. 284) ao determinar, no artigo 31, a possibilidade de a autoridade nacional enviar informes ao órgão público, contendo medidas cabíveis para fazer cessar a violação (BRASIL, 2018a), orientação que não encontra dispositivo semelhante com relação às pessoas jurídicas de direito privado. Além disso, dentre as atribuições da ANPD, estão a solicitação da publicação de relatórios de impacto à proteção de dados pessoais aos agentes administrativos e a sugestão da adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder

Público (artigo 32) (BRASIL, 2019b), medidas que serão imprescindíveis para a adequação dos *sites* do Poder Judiciário a um modelo que pensa a privacidade desde o seu projeto.

Com isso, adentra-se no último critério de análise da lei, qual seja, o tratamento de dados pelo Poder Público, disposto no Capítulo IV da LGPD. Trata-se de matéria que exige uma disciplina mais protetiva ao titular, diante da assimetria de poder existente entre cidadão e Estado, inclusive pela manutenção administrativa de uma série de bancos de dados potencialmente sensíveis (TASSO, 2019, p. 245-6). É este o caso dos bancos de dados mantidos pelo Poder Judiciário, indispensáveis à consecução de sua atividade precípua, mas que demandam cuidado por conter um grande número de informações sensíveis dos jurisdicionados. Portanto, ainda que a coleta de dados pela administração pública seja medida necessária ao desenvolvimento e execução das políticas públicas, o tratamento não pode ser realizado de maneira indiscriminada, cabendo ao Poder Público submeter-se aos preceitos legais (MENEZES; COLAÇO, 2019, p. 162). Diante disso, a abordagem específica realizada neste trabalho procura verificar quais são os regramentos especificamente aplicáveis ao tratamento de dados pela Justiça do Trabalho, no âmbito do processo judicial eletrônico.

Em uma primeira observação, verifica-se que não há um dispositivo específico relacionado à divulgação de dados que integram os processos judiciais. Dentre as disposições gerais, o artigo 23, I, da LGPD indica que as entidades públicas deverão informar as hipóteses de tratamento de dados, incluindo as finalidades (vinculadas à persecução do interesse público), procedimentos e práticas utilizadas para a execução dessas atividades, preferencialmente em seus *sites* na *Internet*. O mesmo artigo, em seu inciso III, indica a necessidade de nomeação de um encarregado de proteção de dados pela administração pública, quando houver o tratamento de dados pessoais (BRASIL, 2018a), sem estabelecer uma distinção para os dados que forem tratados pelo Poder Judiciário no âmbito de sua função jurisdicional, como faz o RGPD europeu.

Com relação à transferência de dados para o setor privado, o parágrafo 1° do artigo 26 proíbe o Poder Público de transferir para entidades privadas os dados pessoais existentes em bases de dados a que tenha acesso, excetuando, no inciso III, os casos em que os dados forem acessíveis publicamente (BRASIL, 2018a). É justamente este o fundamento utilizado para justificar a atuação de buscadores, tais como os *sites* Escavador e Jus Brasil, que coletam e concatenam informações processuais que são publicamente acessíveis nos próprios portais do Poder Judiciário. Ocorre que os dados pessoais (sensíveis ou não) não perdem a sua natureza ou o padrão protetivo legal por integrarem bases de dados públicos. Portanto, ainda que acessíveis publicamente, não pode haver transferência de dados para entidade privada sem que

exista uma finalidade pública sendo atendida ou se esteja perseguindo o cumprimento de interesse público (TASSO, 2019, p. 280).

Assim, mesmo nos casos em que o consentimento do titular dos dados não é obrigatório, a utilização dessas informações pela administração pública deve ser vinculada à prestação ou melhoria deste ou daquele serviço especificamente, sendo vedada qualquer destinação para a qual não foi fornecido consentimento. Por isso, nesse sentido, não pode haver cessão dos dados para entidades privadas, nem mesmo para outros órgãos públicos que prestam outros serviços diferentes daquele que motivaram a coleta, a não ser por ordem judicial (LEMOS; ADAMI; SUNDFELD, 2018). Outro problema reside no fato de que as informações processuais trabalhistas possuem restrições de pesquisa, impostas aos Tribunais Regionais do Trabalho pela já referida Resolução nº 121 do CNJ, orientação que não é seguida por estas empresas, que após a coleta dos dados nos bancos de dados públicos mantém a divulgação aberta das informações na *Internet*.

Para disciplinar o tratamento de dados pessoais que possuem acesso público, o parágrafo 3° do artigo 7° da lei prevê a necessidade de observância da finalidade, da boa-fé e do interesse público que justificaram sua disponibilização. Neste ponto, a LGPD estabelece uma distinção entre os dados tidos como públicos e os dados "tornados manifestamente públicos pelo titular", os quais dispensam a exigência do consentimento (artigo 7°, parágrafo 4°), o que não afasta a necessidade de observância dos princípios gerais do tratamento de dados pessoais e da garantia dos direitos do titular, nos termos do parágrafo 6° do mesmo artigo (BRASIL, 2018a).

Portanto, o tratamento de informações processuais divulgadas via *Internet* pelo Poder Judiciário deve ser realizado para fins não discriminatórios (princípio da não discriminação), limitando-se aos propósitos específicas da coleta fins (princípios da finalidade e adequação) e atendendo ao efetivo interesse público, orientações que deverão nortear a atuação dos *sites* que realizam buscas processuais, já que são os principais disseminadores desses dados. Para isso, caberia também ao Poder Público a elaboração de políticas de privacidade, dispondo sobre o correto tratamento das informações coletadas no âmbito *on-line*, visando a concretização do princípio da transparência administrativa (XAVIER; XAVIER; SPALER, 2019, p. 499).

Nesse caso, o exame da (i)legalidade do tratamento será definido com base na sua compatibilidade com a finalidade e o interesse público que justificaram a divulgação pública dos dados, a partir de uma análise contextualizada (a destinação oferecida aos dados deve ser compatível com a razão pelas quais os dados foram tornados públicos) (BIONI, 2019, p. 270-1). Se os dados são utilizados com vistas à segregação social, evidentemente a destinação não é compatível com o objetivo da divulgação pública, demonstrando não só a ilegalidade do

tratamento, mas também a necessidade de um regime ainda mais rigoroso para determinadas categorias de dados que são manipuladas pela administração pública.

Por fim, com relação à responsabilidade civil do Poder Público pelo tratamento de dados, observa-se que o artigo 42 da LGPD estabelece uma cláusula geral de responsabilidade civil, indicando que "O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo" (BRASIL, 2018a). Se esta é uma diretriz que se volta tanto à administração pública quanto às empresas de natureza privada quando desempenham o papel de controladores ou operadores de dados[96], a lei vai mais fundo ao determinar a responsabilização solidária de ambos os agentes de tratamento nos casos envolvendo mais de um controladores que gerem danos ao titular (artigo 42, II). Resta, portanto, expressa a responsabilidade solidária entre o Poder Judiciário, agente responsável originariamente pelo tratamento de dados dos jurisdicionados, e os *sites* que coletam essas informações e realizam um tratamento secundário, figurando ainda assim como controladores.

Em que pese o pouco tempo decorrido desde a edição da lei, já existem divergências doutrinárias com relação à interpretação dos dispositivos referentes à responsabilidade civil pelos danos decorrentes do tratamento de dados. Enquanto uns sustentam que a LGPD adotou o modelo da responsabilidade objetiva, inspirando-se no CDC, outros defendem a responsabilidade subjetiva, já que a lei estabelece diversos deveres de cuidado no tratamento de dados, que não fariam sentido se a responsabilização do agente fosse imputada independentemente da existência de culpa (GUEDES; MEIRELES, 2019, p. 231).

Com relação ao tratamento de dados sensíveis, Guedes e Meireles (2019, p. 238) defendem a aplicação da cláusula geral de responsabilidade objetiva prevista no parágrafo único do artigo 927 do Código Civil[97], quando a atividade do agente enquadrar-se como atividade de risco nos termos ali descritos. Entretanto, quando se refere ao tratamento de dados pessoais pelo Poder Público (sejam eles dados sensíveis ou não), o presente estudo sustenta a aplicação da

[96] "[...] VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;[...]" (BRASIL, 2018a).

[97] Art. 927 [...] Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem (BRASIL, 2002).

teoria do risco administrativo[98] a amparar a responsabilidade objetiva do Estado pelos danos causados aos titulares, nos termos do artigo 36, parágrafo 6º da Constituição Federal[99].

Ademais, destaca-se que toda a disciplina da LGPD brasileira relativa ao tratamento de dados pelo Estado deve observar os prazos e procedimentos previstos na Lei de Acesso à Informação, incluindo a limitação à publicidade das informações privadas, o que exige o diálogo entre as fontes, conforme destacam Sousa, Barrancos e Maia (2019, p. 249):

> Observa-se, desse modo, que a regulação do tratamento de dados pessoais pelo poder público está intimamente ligado aos procedimentos previstos na Lei de Acesso à Informação, verificando-se a necessidade de que haja o diálogo entre as fontes jurídicas conforme decisões já reconhecidas anteriormente pelos tribunais superiores, em que se permite a aplicação simultânea, coerente e coordenada das plúrimas fontes, por haver influência recíproca, aplicação conjunta das duas normas ao mesmo tempo e ao mesmo caso.

Não havendo regramento específico com relação ao tratamento de dados pelo Poder Judiciário, há uma evidente perda de oportunidade pelo legislador de contemplar um conteúdo urgente e carente de disciplina. Optou-se pelas normas de caráter geral, cujo conteúdo é maleável às mudanças temporais (instrumentos adequados à uma lei que envolve tecnologias tão mutáveis), mas cuja imprecisão dos termos e abertura semântica permite com que as disposições sejam interpretadas ao alvedrio dos interesses.

Observados os regramentos da nova legislação protetiva de dados pessoais no Brasil, ainda em período de *vacatio legis*, ressalta-se que o ordenamento jurídico brasileiro conta com algumas ferramentas que protegem o trabalhador contra a discriminação nas relações trabalhistas, especialmente a Lei nº 9.029/1995, que pode ser utilizado para obstar o acesso e a utilização de dados sensíveis do trabalhador. O seu artigo 1°, proíbe a adoção de práticas discriminatórias na seleção de emprego, bem como no contrato de trabalho, inclusive relacionando alguns dados sensíveis do trabalhador que não podem dar causa a qualquer discriminação, como sexo, raça, deficiência, etc. (BRASIL, 1995).

A Consolidação das Leis do Trabalho (CLT) não traz nenhum dispositivo específico que se refira aos dados pessoais do obreiro. No entanto, em seu artigo 9º, determina a nulidade de todos os atos do empregador cujo objetivo seja o de desvirtuar a aplicação dos preceitos

---

[98] A teoria do risco administrativo reconhece os riscos inerentes à função da administração pública, decorrentes de atividades que visam o interesse público e a organização social, propondo que, assim como os seus benefícios são coletivos, os ônus das atividades administrativas também devem ser socializados (BOLESINA, 2019, p. 588-9).

[99] "Art. 37 [...]§ 6º As pessoas jurídicas de direito público e as de direito privado prestadoras de serviços públicos responderão pelos danos que seus agentes, nessa qualidade, causarem a terceiros, assegurado o direito de regresso contra o responsável nos casos de dolo ou culpa" (BRASIL, 1988).

protetivos da legislação do trabalho. Gustavo Carvalho Chehab (2015, p. 118) considera que este artigo seria aplicável para evitar a coleta de dados do trabalhador com desvio de sua finalidade original, sendo a decisão de dispensá-lo ou não contratá-lo, com base neste único critério, passível de nulidade.

No que se refere à discriminação do reclamante na Justiça do Trabalho, a Portaria nº 367 do Ministério do Trabalho e Emprego (MINISTÉRIO..., 2002), de 18 de setembro de 2002, determinou que toda denúncia formalmente dirigida ao MTE, referente à ocorrência de prática discriminatória por parte de empresa que recuse a contratação de empregado que tenha ingressado com ação judicial trabalhista, será encaminhada à chefia de fiscalização da respectiva Delegacia Regional do Trabalho para apuração, recebendo tratamento prioritário pelo MTE. A portaria foi elaborada após a Promotoria do Trabalho ter conduzido 182 investigações em 20 Estados brasileiros relacionadas à formação de cadastros com o nome de empregados que ajuizaram ações judiciais ("listas sujas"), formados com a utilização de informações de trâmites processuais retiradas da *Internet* e disponíveis ao acesso dos empresários que buscavam informações sobre os candidatos a uma vaga de emprego, para fins discriminatórios (LIMBERGER, 2007, p. 207).

Todos esses instrumentos normativos reforçam o conteúdo da LGPD, que tem na não discriminação um de seus principais princípios. Se serão ou não efetivas todas as promessas apresentadas pela nova lei, somente será possível saber com clareza após a sua entrada em vigor, em agosto de 2020. Por enquanto, é importante observar a forma como são divulgadas as informações processuais pelo Poder Judiciário trabalhista do Brasil, estabelecendo-se um comparativo com um país que possui uma lei de proteção de dados pessoais vigente e estabelecida, como é o caso da Argentina, já analisada no capítulo anterior. Através do estudo será possível verificar se a existência de uma lei específica condiciona as práticas protetivas de dados pessoais do obreiro, visando a proposição de alternativas que possam ser adotadas pela Justiça do Trabalho brasileira.

3.3.2 Pesquisa empírica: as ferramentas de consulta processual e jurisprudencial no *site* do Tribunal Superior do Trabalho e no portal Escavador

A observação direta do *site* do Tribunal Superior do Trabalho (www.tst.jus.br) foi realizada no dia 26 de junho de 2019, a partir das categorias de análise previamente elencadas e descritas. O portal disponibiliza uma barra lateral de acesso rápido em sua página inicial

(Figura 6), que permite o acesso às pesquisas jurisprudencial e processual por meio das opções "Pesquisa de Jurisprudência" e "Processos do TST", respectivamente (BRASIL, 2019c).

Além disso, as opções de consulta pública também são acessíveis por meio do menu disponibilizado no cabeçalho da página inicial, na aba "Jurisprudência", que armazena o *link* "Pesquisa de Jurisprudência (novo)", e na seção "Serviços", que contém o item "Serviços Processuais", e nele a ferramenta de "Consulta Processual no TST". Ressalta-se que o *site* mantém acessíveis dois sistemas de consulta jurisprudencial: uma versão desatualizada, modelo que era utilizada no passado (o próprio portal alerta ao usuário que se trata de um sistema muito antigo), chamado de "Consulta Unificada (sistema antigo)", e o atual sistema de pesquisa jurisprudencial, que foi implementado em substituição ao anterior, e será objeto de análise deste estudo.

Figura 6 – Página inicial – Tribunal Superior do Trabalho (BRASIL, 2019c)

O primeiro critério de observação diz respeito à possibilidade de pesquisa pelo nome do reclamante, em ambas as formas de consulta. Com relação à pesquisa processual, observa-se que o *site* permite a consulta pelo número do processo, pelo nome do empregador ou pelo nome do advogado, mas não pelo nome do trabalhador (Figura 7) (BRASIL, 2019c). Neste ponto, se comparado ao portal argentino anteriormente examinado, o Tribunal brasileiro demonstra um maior nível protetivo, ainda que, de fato, a conduta não reverta em maiores ganhos ao trabalhador, devido à atuação dos buscadores que divulgam as informações processuais de

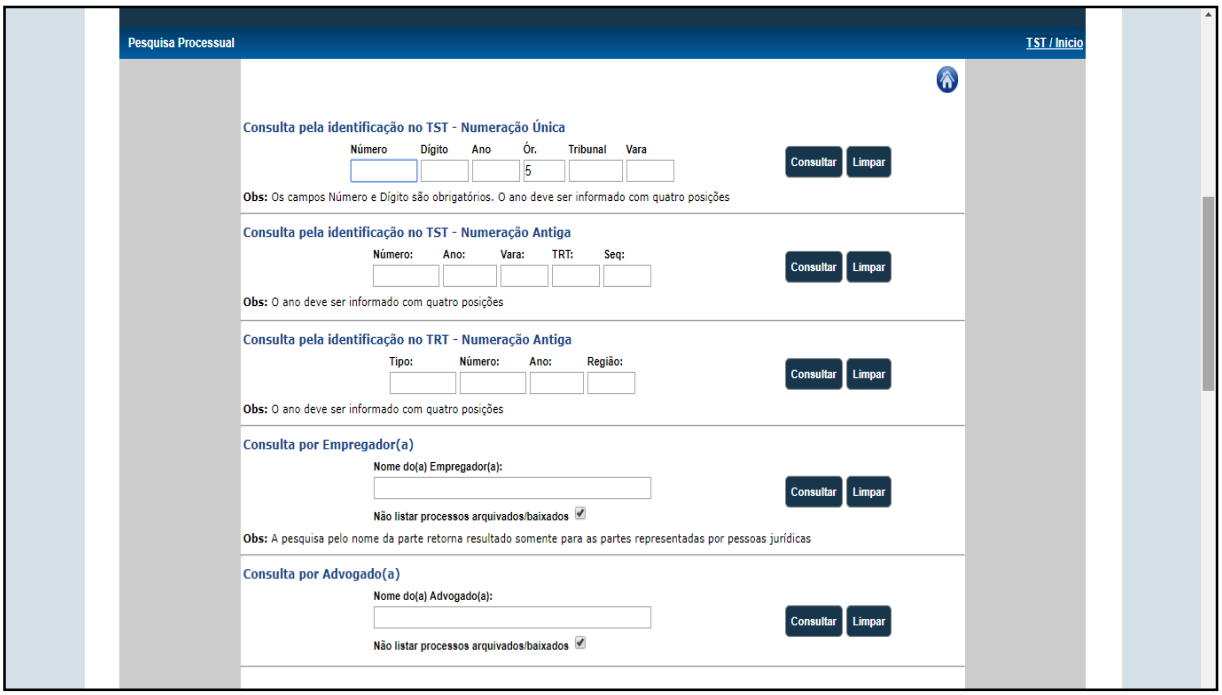
forma indiscriminada na *Internet*, a exemplo do portal Escavador, conforme será referido e analisado na sequência do trabalho.

Ademais, a própria divulgação de inteiro teor de decisões judiciais, sem o consentimento do titular, viola os princípios regentes da *novel* Lei Geral de Proteção de Dados pessoais brasileira. É justamente essa a preocupação de Rosane Leal da Silva (2018, p. 334) ao alertar que:

> Em que pese a consulta pelos sistemas de busca não ocorrer pelo nome das partes, o que é muito importante 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 (art. 2º), importante direito que se constitui num dos fundamentos da recente Lei nº 13.709, de 14 de agosto de 2018 (Lei de Proteção de Dados) [...]

Não fosse o bastante, o próprio fato de permitir que a consulta seja realizada pelo nome do empregador ou pelo nome do advogado já evidenciam uma fragilidade do sistema, diante de tamanha facilidade com que se pode chegar ao conhecimento dessas informações. Vale destacar que a ferramenta oferecida pelo tribunal afronta o artigo 4°, parágrafo 1º, II, da Resolução nº 121/2010 do CNJ, com redação dada pela Resolução 143/2011 (CONSELHO..., 2011), que veta a pesquisa pelo nome das partes (o que inclui, portanto, reclamante e reclamadas) nos processo sujeitos à apreciação da Justiça do Trabalho.

Figura 7 – Pesquisa processual (BRASIL, 2019c)



Com relação à pesquisa de jurisprudência, o portal recentemente passou por reformulações em sua ferramenta de busca. O novo sistema (Figura 8) permite a utilização de diversos filtros de pesquisa, tais como órgão judicante, ministro, classe processual, data de publicação de data de julgamento, além da possibilidade de escolha do tipo de documento (BRASIL, 2019c). Observa-se, entretanto, que não há qualquer limitação à pesquisa pelo nome do trabalhador, já que a ferramenta realiza a ampla busca de todos os termos pesquisados no banco de jurisprudência do Tribunal, sem a anonimização dos resultados ou a desindexação dos nomes que integram as decisões.

Assim, é essencial ao Poder Público a criação de outros mecanismos de proteção à privacidade, visando a uma nova geração de serviços públicos eficientes sem atentar contra as garantias fundamentais, como a chamada "privacidade por desenho" ou *privacy by design* (LEMOS; ADAMI; SUNDFELD, 2018), que deveria ser aplicada pelo Poder Judiciário desde o processo de construção de seus *sites* institucionais, sendo que a anonimização é uma de suas principais modalidades. Este processo, por sua vez, pode ser implementado por diferentes técnicas, tais como a supressão, a generalização[100], a randomização[101] e a pseudoanonimização[102] (BIONI, 2019, p. 71).

Sem o escopo de aprofundamento em cada uma dessas técnicas, entende-se que a sua aplicação conjunta é necessária para a redução do grau de identificabilidade do reclamante em processos trabalhistas, a depender do tipo de informação a ser divulgada, especialmente as técnicas da supressão (ocultamento completo da informação), generalização (divulgação parcial ou generalizada, apenas de elementos que não permitam a identificação direta) e/ou pseudoanonimização (utilização de pseudônimo para a designação dos identificadores diretos do indivíduo, ao invés do nome, CPF, etc). Esta última, para alguns autores, não é considerada uma técnica de anonimização, já que a pessoa continua sendo identificável por pseudônimos (ex. números aleatórios) (BIONI, 2019, p. 71), mantendo-se o caráter de pessoalidade do dado (VAINZOF, 2019, p. 96), o que não impede a sua utilização integrada com outros métodos.

---

[100] A generalização consiste em diluir ou generalizar dos atributos dos titulares, modificando a respectiva escala ou ordem de magnitude (ex. uma região em vez de uma cidade, um mês em vez de uma semana) (ARTICLE 29 DATA PROTECTION..., 2014, p. 16).

[101] A randomização é um conjunto de técnicas (tais como a aplicação de ruído, permutação e privacidade diferenciada) que altera a veracidade dos dados para remover o vínculo existente entre os dados e o titular (ARTICLE 29 DATA PROTECTION..., 2014, p. 12).

[102] Para os efeitos da LGPD, nos termos de seu artigo 13, parágrafo 4º, considera-se pseudonimização o "[...] 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, 2018a).

Assim, vale referir um exemplo geral sugerido por Bruno Bioni (2019, p. 71-2) para a redução do grau de identificabilidade de uma base de dados: supressão de CPF (já que a sua disponibilização, ainda que parcial, pode levar à identificação do indivíduo), generalização do nome completo (disponibilização somente do prenome), generalização da localização geográfica (divulgação de alguns dígitos do CPF), generalização da idade (divulgação da faixa etária). Apesar de estudos demonstrarem que este é um processo falível (*vide* Bioni, 2019, p. 73; Konder, 2019, p. 452-3 e Vainzof, 2019, p. 98), já que a garantia integral de anonimato torna-se impossível diante das diversas ferramentas de manipulação e associação com outros dados, a utilização dessas técnicas, de forma combinada[103], pode minimizar os riscos a que se submete o trabalhador com a divulgação integral de seus dados em decisões judiciais, submetendo-se aos mesmos cuidados os dados da reclamada e os próprios fatos narrados na demanda.

Neste caso, torna-se evidente que os acórdãos divulgados pelo Poder Judiciário deveriam passar por um processo de anonimização prévio, removendo-se, ocultando-se ou generalizando-se os dados pessoais e as informações que permitam a identificação de seu titular, na medida em que são desnecessários para as finalidades às quais são divulgados. Esse processo deve ser realizado através de técnicas que não permitam a sua reversão, conforme observam Lemos, Adami e Sundfeld (2018):

> Há casos, também, em que um sensor ou dispositivo poderia obter dados pessoais, mas o regime de proteção de dados é afastado, uma vez que as informações coletadas são "anonimizadas", ou seja, qualquer indicativo da titularidade é mascarado definitivamente por técnicas de criptografia. Essa anonimização deve ser obrigatoriamente de alto nível, impedindo a reversão ou reidentificação dos usuários.

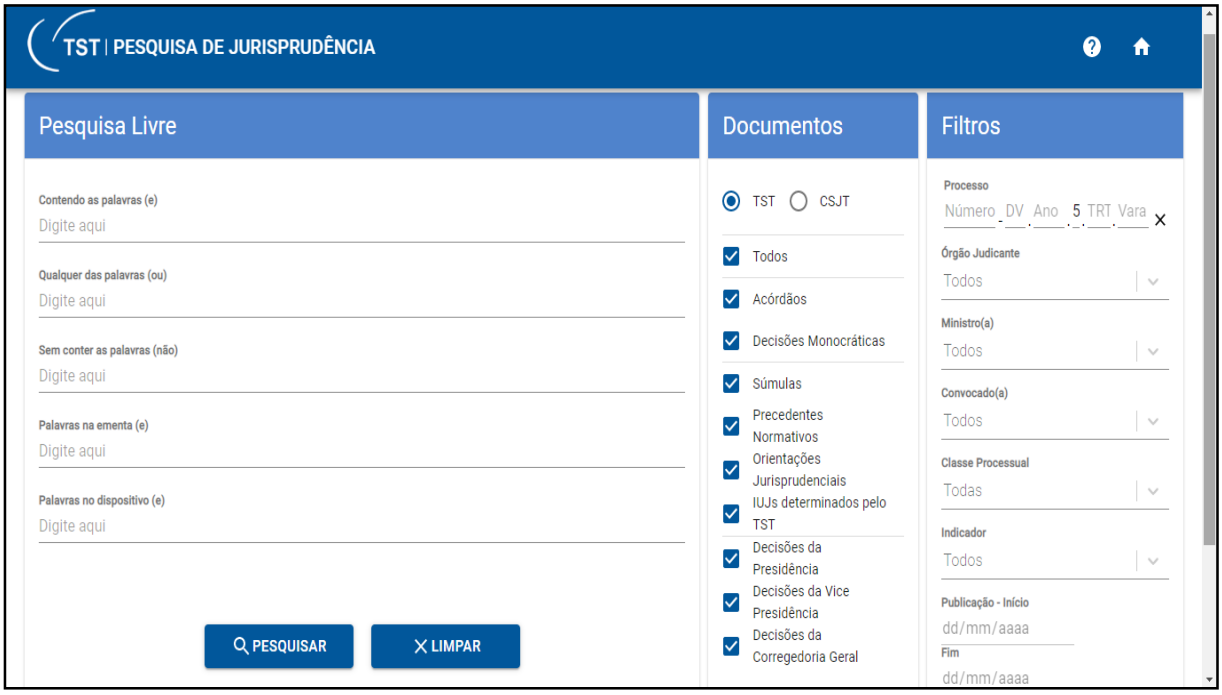
Não são poucos os debates acerca de quais são as informações que integram efetivamente o interesse público, devendo ser divulgadas pela Administração em seu exercício de transparência, tema que foi abordado no item 1.2 deste trabalho. Buscando estabelecer uma padrão distintivo, Matos e Ruzyk (2019, p. 210) chegam à seguinte premissa: com relação aos dados pessoais não anonimizados, somente poderão ser veiculados aqueles que sejam indispensáveis ao atendimento da transparência pública, mantendo-se o sigilo sobre os demais; com relação aos dados anonimizados, é possível a divulgação desde que o tratamento não torne

[103] De acordo com Vainzof (2019, p. 98), "[...] a solução ideal deve ser decidida caso a caso, possivelmente usando uma combinação de diferentes técnicas, sempre levando em consideração que um conjunto de dados anonimizados ainda pode apresentar riscos para os seus titulares".

novamente possível a identificação de seus titulares, por meio de razoável esforço do agente responsável pelo tratamento, atendendo-se ao disposto no artigo 12 da LGPD[104].

Assim, estabelecendo-se uma aplicação do critério de proporcionalidade entre os bens jurídicos lesados, não é razoável a violação de direitos fundamentais dos jurisdicionados diante da existência de outros meios capazes de atingir resultado semelhante, como são os processos de anomização e desindexação dos resultados de busca, plenamente aplicáveis pelos tribunais para a construção das ferramentas de consultas jurisprudenciais de seus *sites*, através da utilização do método do *privacy by design*.

Figura 8 – Pesquisa jurisprudencial (BRASIL, 2019c)



Diante dos elementos expostos, o Tribunal Superior do Trabalho atende parcialmente ao primeiro critério de observação, apresentando uma resposta razoavelmente satisfatória no que se refere à impossibilidade de pesquisa pelo nome do trabalhador no campo de consulta processual (ainda que não totalmente adequada à Resolução nº 121 do CNJ, já que permite a pesquisa pelo nome do empregador), mas não demonstrando o mesmo cuidado com a pesquisa jurisprudencial.

[104] "Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido" (BRASIL, 2018a).

O segundo critério de análise parte de uma diretriz do Conselho Superior da Justiça do Trabalho[105] brasileira (Resolução CSJT nº 139/2014), qual seja, a adoção de solução de *captcha* para consultas em processos, acórdãos e jurisprudências. Ainda que tal recomendação seja direcionada aos Tribunais Regionais do Trabalho (que, na sua grande maioria, adotam a prática), o próprio Tribunal Superior do Trabalho do país não utiliza a ferramenta em seu *site*, tanto na pesquisa jurisprudencial como na consulta processual.

Conforme referido anteriormente, o dispositivo *captcha* é utilizado para evitar o preenchimento automático de formulários por robôs, protegendo os dados pessoais contidos nas decisões judiciais disponibilizadas na *Internet* contra o tratamento automatizado, o que se coaduna à ideia de *privacy by design*. Vale ressaltar que a privacidade incorporada ao *design* é um dos princípios norteadores desta metodologia (SOUZA, 2019, p. 429), o que torna necessária a preocupação do Poder Judiciário inclusive com o *layout* de seus portais na rede mundial de computadores, e com a utilização de mecanismos que protejam a privacidade dos jurisdicionados, usuários do serviço público, como é o caso do dispositivo *captcha*.

Ao dispensar a sua utilização, o Tribunal Superior do Trabalho demonstra não estar em sintonia com as orientações estabelecidas pelo órgão administrativo, o que revela uma preocupante falta de cuidado com a proteção dos dados pessoais publicados em seu portal. O TST, na condição de Cortes Superior do Poder Judiciário trabalhista brasileiro, deveria ser modelo a ser seguido pelos Tribunais Regionais, apresentando um sistema impecável para a ampla tutela do trabalhador, o que, de fato, não ocorre.

A terceira categoria de observação volta-se à divulgação ou não de dados sensíveis por meio da pesquisa jurisprudencial (Figura 8). A realização das buscas teve como ponto de partida a eleição de uma palavra-chave que costuma conduzir ao tratamento de dados sensíveis, optando-se pelo termo "despedida discriminatória". A consulta foi realizada no dia 07 de julho de 2019, limitando-se aos acórdãos com tramitação eletrônica julgados pelas Turmas do TST, em sede de Recurso de Revista, e publicados entre 27/04/2016 e 27/04/2019, indicando 42 (quarenta e dois) resultados encontrados. A opção pela data de 27/04/2016 como termo inicial da busca, assim como na pesquisa realizada na Argentina, foi motivada pela data de edição do Regulamento de Proteção de Dados Pessoais da União Europeia, com influência determinante

[105] O Conselho Superior da Justiça do Trabalho é um órgão vinculado ao Tribunal Superior do Trabalho, que exerce a função de "[...] supervisão administrativa, orçamentária, financeira e patrimonial da Justiça do Trabalho de primeiro e segundo graus, como órgão central do sistema, cujas decisões terão efeito vinculante", nos termos do artigo 111-A, parágrafo 2º, II da Constituição da República Federativa do Brasil, conforme redação incluída pela Emenda Constitucional 45/2004 (BRASIL, 2004).

na lei de proteção de dados pessoais brasileira e nas práticas protetivas implementadas no país desde então.

Ressalta-se que o Recurso de Revista é a modalidade recursal destinada a impugnar decisão que afronta a literalidade de lei federal ou da Constituição Federal, seja pela violação direta à norma ou pela divergência de interpretação com outro Tribunal Regional ou com a Seção de Dissídios Individuais do TST (MALGARIN, 2016, p. 260). Trata-se do recurso cabível nos dissídios individuais em face das decisões proferidas pelos Tribunais Regionais do Trabalho em grau de recurso ordinário, e seu julgamento compete às Turmas do Tribunal Superior do Trabalho, nos termos do artigo 896, "caput", da CLT, com redação dada pela lei 9.756/1998 (BRASIL, 1998). Diante disso, a limitação de pesquisa é pertinente na medida em que serve de amostragem dos dissídios individuais envolvendo despedidas discriminatórias, especialmente nos processos eletrônicos.

Em resposta ao quesito em análise, verificou-se que 27 (vinte e sete) dos 42 (quarenta e dois) resultados encontrados continham alguma categoria de dado sensível do trabalhador ou de terceiro. Ainda que a porcentagem de julgados com divulgação de dados sensíveis tenha atingido o índice de 64,28% dos resultados coletados, não se pode considerar essa informação como significativa para indicar se há ou não, de fato, uma preocupação institucional em ocultar essas informações em determinadas situações. Na verdade, o recorte feito nesta pesquisa busca estabelecer um panorama geral sobre a forma como é feita a divulgação de jurisprudências pelos *sites* dos Tribunais trabalhistas de cada país, ciente de que os resultados encontrados devem ser considerados sob um enfoque amplo e contextualizado.

A exemplo do que foi constatado na pesquisa de jurisprudências realizada na Corte argentina, a busca no Tribunal Superior do Trabalho do Brasil indicou que grande parte dos dados sensíveis divulgados nos acórdãos são relacionados à saúde. Dos 27 (vinte e sete) resultados em que foi detectada a divulgação de dados sensíveis, 24 (vinte e quatro) relacionaram-se a doença ou estado gravídico do(a) reclamante. Este é um número expressivo que se relaciona ao grande quadro de reclamações trabalhistas pleiteando a reintegração da empregada gestante[106] ou do trabalhador portador de doença grave que suscite estigma ou preconceito, através da incidência da Lei 9.029/1995 e da Súmula 443 do TST[107].

---

[106] A empregada gestante possui estabilidade provisória que se estende da confirmação da gravidez até 5 (cinco) meses após o parto, nos termos do artigo 10, II, "b" do Ato das Disposições Constitucionais Transitórias (BRASIL, 1988). A despedida da trabalhadora durante este período, ainda que por desconhecimento do estado gravídico pelo empregador, autoriza o pedido de reintegração, conforme entendimento jurisprudencial, manifesto na Súmula 244 do TST (BRASIL, 2012b). Dos 24 (vinte e quatro) resultados em que houve divulgação de dados relativos à saúde ou vida sexual, 4 (quatro) foram relacionados à gravidez da trabalhadora.

[107] "Súmula nº 443 do TST

Dentre as categorias de dados sensíveis encontradas, somente 1 (um) resultado relacionou-se à filiação a sindicato ou organização religiosa, filosófica ou política, baixo número que pode estar associado mais às palavras-chave adotadas do que ao número de processos buscando a reintegração do dirigente sindical, abundante na justiça laboral. Acerca dos dados relacionados à filiação partidária, Matos e Ruzyk (2019, p. 212) lembram que tais informações, ainda que elencados como sensíveis pela LGPD, não podem ser mantidas em sigilo, já que, por óbvio, o conhecimento público é inerente à pretensão do titular. Entretanto, assim como os dados relativos à filiação sindical, tais informação podem ser utilizadas para finalidades discriminatórias no âmbito laboral, seja pela orientação partidária contrária ao contratante, ou porque trabalhadores que foram dirigentes sindicais possuem maiores dificuldades para inserir-se no mercado de trabalho, o que justifica uma proteção mais restritiva em determinadas situações, como é o caso da divulgação em processos judiciais.

Outro ponto importante a ser considerado é que todos os julgados encontrados na pesquisa jurisprudencial brasileira mencionaram o nome completo do trabalhador, não havendo resultados cujos dados tenham sido anonimizados ou que se tenha utilizado as iniciais do nome do reclamante. No Brasil, a abreviatura dos nomes das partes é uma prática restrita aos processos que tramitam em segredo de justiça, disciplinados pelo artigo 189 do Código de Processo Civil[108] (BRASIL, 2015), dos quais destacam-se as ações relativas ao Direito de Família (causas que versem sobre casamento, separação de corpos, divórcio, separação, união estável, filiação, alimentos e guarda de crianças e adolescentes), ainda que, mesmo nesses casos, o teor dos julgados disponibilizados pelos tribunais acabe, muitas vezes, divulgando informações sensíveis dos jurisdicionados e permitindo a sua identificação.

É importante destacar que o artigo 189, inciso III, do CPC (BRASIL, 2015) assegura aos processos em que constem dados protegidos pelo direito à intimidade a tramitação em

---

DISPENSA DISCRIMINATÓRIA. PRESUNÇÃO. EMPREGADO PORTADOR DE DOENÇA GRAVE. ESTIGMA OU PRECONCEITO. DIREITO À REINTEGRAÇÃO - Res. 185/2012, DEJT divulgado em 25, 26 e 27.09.2012

Presume-se discriminatória a despedida de empregado portador do vírus HIV ou de outra doença grave que suscite estigma ou preconceito. Inválido o ato, o empregado tem direito à reintegração no emprego" (BRASIL, 2012c).

[108] "Art. 189. Os atos processuais são públicos, todavia tramitam em segredo de justiça os processos:

I - em que o exija o interesse público ou social;

II - que versem sobre casamento, separação de corpos, divórcio, separação, união estável, filiação, alimentos e guarda de crianças e adolescentes;

III - em que constem dados protegidos pelo direito constitucional à intimidade;

IV - que versem sobre arbitragem, inclusive sobre cumprimento de carta arbitral, desde que a confidencialidade estipulada na arbitragem seja comprovada perante o juízo.

§ 1º O direito de consultar os autos de processo que tramite em segredo de justiça e de pedir certidões de seus atos é restrito às partes e aos seus procuradores.

§ 2º O terceiro que demonstrar interesse jurídico pode requerer ao juiz certidão do dispositivo da sentença, bem como de inventário e de partilha resultantes de divórcio ou separação" (BRASIL, 2015).

segredo de justiça, acompanhando a regra constitucional prevista no artigo 5º, LX, que garante que "[...] a lei só poderá restringir a publicidade dos atos processuais quando a defesa da intimidade ou o interesse social o exigirem" (BRASIL, 1988). É justamente esse o caso dos processos trabalhistas cujo conteúdo costuma envolver, frequentemente, a divulgação de dados de caráter privado com alto potencial discriminatório, como são, por exemplo, as questões envolvendo a saúde do trabalhador, amplamente dissecadas nos autos que tramitam na Justiça laboral, e que, por conta disso, deveriam contar com uma tramitação diferenciada, aumentando-se o nível protetivo no tráfego dessas informações.

A reforçar esta posição está o princípio da proteção, que, conforme a lição de Plá Rodriguez (1996, p. 30), visa a alcançar a igualdade substancial entre as partes da relação empregatícia, restabelecendo o desequilíbrio existente entre empregado e empregador e orientando o intérprete para uma proteção jurídica favorável ao obreiro. Assim, sua finalidade "[...] consiste em tentar corrigir desigualdades, criando uma superioridade jurídica em favor do empregado, diante da sua condição de hipossuficiente" (BARROS, 2016, p. 122). Alguns doutrinadores, tais como Carlos Henrique Bezerra Leite (2018, p. 112), Manoel Antonio Teixeira Filho (2009, p. 93-97) e Wagner D. Giglio (2007, p. 83) defendem uma aplicação do princípio protecionista do trabalhador, próprio da relação de direito material, ao ramo do direito processual do trabalho, concebendo o princípio da proteção processual (ou princípio da correção da desigualdade) como um de seus princípios peculiares.

Dessa forma, o princípio da proteção processual busca o estabelecimento de uma igualdade jurídica entre as partes (MALGARIN, 2016, p. 27), o que deriva da própria razão de ser do processo do trabalho enquanto instrumento de efetivação do direito laboral (LEITE, 2018, p. 112). Diante de tal desequilíbrio, observado inclusive no campo processual[109], um regime de tutela especial ao trabalhador deveria ser aplicada também às informações que são levadas pelo reclamante à Justiça do Trabalho e que, ao fim e ao cabo, visam assegurar ao trabalhador a garantia de direitos não satisfeitos durante o contrato de trabalho.

A fim de exemplificar a vulnerabilidade do trabalhador diante da exposição pública de

[109] O estabelecimento de um protecionismo temperado, mitigado ou relativizado no processo laboral visa compensar eventuais dificuldades do trabalhador ao procurar a Justiça do Trabalho (PEREIRA, L., 2014, p. 76), manifestando-se, por exemplo, por meio da possibilidade de inversão do ônus da prova, da gratuidade judiciária, e do impulso processual *ex officio* (GIGLIO; CORRÊA, 2007, p. 85). Os dois últimos exemplos citados foram limitados pelas recentes alterações impostas pela lei 13.467/2017 (BRASIL, 2017), que ampliou os obstáculos ao acesso do obreiro à justiça. Por conta disso, Bezerra Leite (2018, p. 115) entende que a lei "[...] desferiu um duro golpe no princípio de proteção processual ao trabalhador [...]", citando os exemplos da obrigatoriedade do depósito recursal ao reclamante e a possibilidade de condenação em honorários advocatícios e periciais mesmo sendo beneficiário da justiça gratuita, alterações que impuseram novas dificuldades ao trabalhador demandante na justiça laboral.

informações de cunho pessoal, dois resultados obtidos na consulta jurisprudencial efetuada no Tribunal Superior do Trabalho serão mencionados a título exemplificativo. Começa-se pelo Recurso de Revista nº TST-RR-10524-33.2014.5.15.0031, julgado em 28 de fevereiro de 2018, com relatoria do Ministro Breno Medeiros, em que foi recorrente E.L.E.[110] e recorrida a empresa V.R.N.E.C. LTDA. O fato que originou a demanda foi a despedida sem justa causa de um empregado que enfrentava problemas com a dependência química, circunstância que foi assim narrada no acórdão (BRASIL, 2018d):

> **Alegou que é dependente químico e que sofreu uma recaída no dia 22.09.2013** (seu dia de folga), não tendo condições de comparecer ao trabalho no dia 23.09.2013. Disse, ainda, que no dia seguinte, sua esposatentou [*sic*] explicar o ocorrido e entregar um atestado médico na empresa, que não o aceitou. No dia 25.09.2013, o obreiro se dirigiu ao escritório da reclamada na tentativa de entregar o documento, informar o ocorrido e requerer os documentos necessários para pleitear, junto ao INSS, seu afastamento do trabalho, **haja vista a necessidade de permanecer em clínica de reabilitação por pelo menos 6 meses**, oportunidade em que a Sra. S. lhe pediu que retornasse no dia seguinte, ou seja, no dia 26.09.2013 para entregar o atestado médico e retirar os documentos requeridos. Ao retornar ao escritório no dia solicitado, foi surpreendido com a notícia de que estava sendo demitido sem justa causa, com afastamento desde o dia 24.09.2013, sendo dito pela funcionária que o atendeu que sequer aceitariam seu atestado médico pois não precisariam mais de seus serviços [grifo nosso].

Diante do pedido de reintegração do reclamante, a reclamada alegou em defesa "[...] que desconhecia o fato do autor ser dependente químico, pois o único atestado médico entregue na empresa ocorreu no dia 20.05.2013, em função de uma gastro colite de origem infecciosa" (BRASIL, 2018d). Sobreveio sentença declarando nula a dispensa imotivada do reclamante e restabelecendo o vínculo de emprego entre as partes. Em sede de Recurso Ordinário, o Tribunal Regional da 15ª Região, reexaminou as provas produzidas pelas partes, manifestando-se com a seguinte constatação (BRASIL, 2018d):

> Da análise dos documentos carreados aos autos verifica-se que o atestado sob ID 2891658 comprova que foi solicitado 15 dias de afastamento ao autor a partir de 23.09.2013, por motivo de doença. Posteriormente, **no dia 26.09.2013, houve o encaminhamento do obreiro para internação em clínica para tratamento de crack** (ID 2891658) [grifo nosso].

[110] Ainda que todos os julgados encontrados na pesquisa jurisprudencial no portal brasileiro tenha divulgado o nome completo das partes, optou-se pela utilização das letras iniciais como regra geral para todas as jurisprudências citadas neste trabalho, como forma de minimizar o potencial discriminatório das informações aqui tratadas. O mesmo cuidado foi oferecido aos nomes de partes, testemunhas, médicos e terceiros relacionados às demandas, que apesar de divulgados na íntegra nos acórdãos, não terão seus nomes completos aqui reproduzidos.

Considerando que o autor não se desincumbiu do ônus de provar a dispensa discriminatória e eventuais vexames ou constrangimentos, diante da ausência de provas testemunhais, o Tribunal Regional deu provimento ao apelo da reclamada, para afastar a reintegração do reclamante no emprego. O trabalhador interpôs Recurso de Revista, indicando contrariedade à Súmula 443 do TST, o qual foi conhecido e provido, reconhecendo como presumível a dispensa discriminatória do empregado portador de patologia grave capaz de suscitar estigmas ou preconceitos, como é o caso da dependência química (BRASIL, 2018d).

Da análise do acórdão, verifica-se uma completa exposição da enfermidade que acomete o trabalhador, a dependência do crack, inclusive com menção à necessidade de internação em clínica de tratamento, e até mesmo de doença gástrica, através da revelação dos conteúdos de atestados médicos emitido pelo empregado em momento anterior. Certamente que se reconhece ser inevitável que todos esses dados se façam presentes no processo ajuizado pelo reclamante, já que a enfermidade compõe justamente o cerne da demanda e resolução do litígio impõe o manejo dos dados pelas partes, procuradores, servidores e magistrado. O que é questionável é a ampla publicização dessas informações por meio da rede mundial de computadores, ainda mais em sede de pesquisa jurisprudencial, com possibilidade de busca pelo nome do trabalhador, sem o seu consentimento. Esta problemática é identificada por Rosane Leal da Silva (2019, p. 159), ao sustentar que:

> [...] muitos desses elementos figuram em processos, muitas vezes integrando o mérito da discussão, como ocorre nos pedidos de reintegração no emprego em razão de despedida discriminatória. O problema ocorre, portanto, quando tais decisões são publicadas nos portais do Poder Judiciário, revelando a terceiros elementos que deveriam ser mantidos na esfera privada do trabalhador, como no caso de doenças como HIV, problemas mentais, determinadas dependências e até a orientação sexual da pessoa".

Vale lembrar que a nova Lei Geral de Proteção de Dados Pessoais, que ainda aguarda sua vigência plena, exige o expresso consentimento do titular dos dados, o qual deverá ser vinculado à finalidade específica do tratamento. Neste ponto, o advento de uma normativa que venha a disciplinar os parâmetros para o tratamento de dados poderá exigir uma readequação por parte do Poder Público com relação ao modo como procede a divulgação de informações processuais, sob pena de incorrer nas sanções administrativas legalmente previstas.

Se o problema envolvendo a violação da privacidade do trabalhador já é grave o suficiente, a ausência de cuidado com os dados pessoais na Justiça laboral não se limita aos jurisdicionados, já que outros sujeitos que participam do processo do trabalho também sofrem uma exposição desnecessária, como são os casos das testemunhas e outras pessoas referidas na

reclamação trabalhista, como o assediador, em caso de assédio moral ou sexual, e os colegas de trabalho do reclamante. Um dos julgados encontrados na pesquisa jurisprudencial ilustra essa problemática com perfeição. Trata-se do Recurso de Revista nº TST-RR-205000-15.2008.5.02.0073, julgado em 10 de Agosto de 2016, com relatoria da Ministra Dora Maria da Costa, em que foi recorrente a empresa C.G.S.P. e recorrido J.M. (BRASIL, 2016b).

Trata-se de demanda provocada pela despedida sem justa causa, alegadamente discriminatória, de empregado que encaminhou ao Comitê de Ética da empresa uma denúncia de assédio sexual promovido pelo seu superior hierárquico (diretor da empresa) em face de outra funcionária, subordinada ao reclamante. A empresa, por sua vez, justificou a despedida sob a alegação de que o perfil do cargo não estaria adequado ao funcionário. O fato foi assim descrito no acórdão, que transcreve trecho da decisão proferida pelo Tribunal Regional da 2ª Região em sede de recurso ordinário: "Indiscutível nos autos o fato gerador da demissão do recorrente: na qualidade de superior hierárquico da empregada S.V.M., acompanhou-a na apresentação de denúncia de assédio sexual praticado pelo Diretor L. A., seu superior hierárquico; [...]" (BRASIL, 2016b).

Ao examinar as provas, o Tribunal Regional verificou que a vítima do assédio havia ingressado com reclamação trabalhista na 79ª Vara do Trabalho de São Paulo, recuperando trechos de seu depoimento e da oitiva de testemunha realizada naquele processo, conforme se observa na passagem a seguir (BRASIL, 2016b):

> Sem delongas, vejamos a prova dos autos acerca da imputação dessa prática ao preposto da empresa, acima nominado: a vítima S. V. M. ajuizou reclamatória em face da ré (proc. 01977-2007-079-02-00-6) e no seu depoimento prestado perante a MM. 79ª Vara do Trabalho de São Paulo, declarou que
> "(...) *que a partir de fevereiro de 2006 a depoente passou a ser assediada pelo Sr. L. A. que não era o chefe imediato da depoente, mas com quem a depoente se encontrava cerca de duas vezes por dia em função das atividades desempenhadas; que o assédio era de ordem sexual e moral; (...) que a testemunha J. M. presenciou uma vez tal assédio sexual, ocorrido na sala do Sr. L. que no* tocante ao assédio moral este ocorria na frente de todos do setor, inclusive aos empregados que se reportavam à depoente; (...) que ambos os tipos de assédio aconteciam quase que diariamente (...)" – fl. 217.(grifei).
> Nessa reclamação trabalhista foi colhido o depoimento da primeira testemunha da autora, médico psiquiatra que atendeu a sra. S., a pedido da reclamada, que afirmou: "(...) que o pedido de que a reclamante fosse atendida foi formulado pelo Dr. F. S., médico da reclamada (...); que o Dr. F. narrou ao depoente que a reclamante se afastou em virtude de úlcera na córnea e de dano provocado por queda de cavalo e que também a reclamante havia dito que estava sendo vítima de assédio moral e sexual; (...) que a reclamante apresentava quadro de ansiedade e depressão que o depoente concluiu terem nexo causal com um conjunto de fatores consistentes no assédio moral e sexual por parte de um dos diretores (...)" – fl. 218. [abreviaturas pelo autor].

A prova testemunhal colhida pelo *juízo a quo* também foi reanalisada pelo Tribunal, com a reprodução dos depoimentos, conforme o seguinte trecho transcrito no acórdão (BRASIL, 2016b):

> Vejamos agora como tal denúncia foi efetuada e se tem ligação com a demissão do autor: para tanto, convém aqui transcrever trechos do depoimento da testemunha do reclamante, Sr. D. L. F., colhido por meio de Carta Precatória, anexa aos presentes autos (fls. 97/98):
> "(...) que na época o reclamante era gerente da área de gás na cidade de São Paulo/SP; que não sabe se o cargo do reclamante era de gerente, mas era o responsável na área indicada; que o reclamante deixou de trabalhar para reclamada porque denunciou um caso de assédio sexual, o reclamante foi despedido porque denunciou o caso; que a reclamada tem um comitê de ética e na época do presidente deste comitê era L. D., que também era presidente da reclamada; (...) que foi relatado ao depoente que havia uma empregada de nome S. gostaria de denunciar o assédio e estaria com medo; sendo questionado ao depoente como poderia ser denunciado o caso; que o depoente então informou que a denúncia deveria ser feita ao comitê de ética da reclamada; (...) que o depoente levou o caso ao presidente da BG e a dois superintendentes da reclamada, R. L. e A.; que depois de um mês da despedida do reclamante o Sr. D. chamou o depoente e lhe despediu; [abreviaturas pelo autor].

Constatando que o trabalhador havia recebido diversas promoções ao longo da carreira, com desempenho elogiável, inclusive alguns meses antes de ser despedido, e que a dispensa foi consequência direta e imediata da denúncia feita, o Tribunal Regional deu provimento ao Recurso Ordinário, a fim de reformar a decisão de origem e declarar nula de pleno direito a despedida. Interposto o Recurso de Revista pela empresa, a 8ª turma do Tribunal Superior do Trabalho entendeu que não houve comprovação de nexo entre a dispensa e a denúncia feita pelo reclamante, restabelecendo a sentença em relação ao indeferimento dos pedidos de reintegração e indenização por danos materiais e morais (BRASIL, 2016b).

O conteúdo do julgado revela que diversos sujeitos tiveram seus dados pessoais divulgados sem o devido consentimento: além da reclamação trabalhista discorrer acerca de uma suposta prática de assédio sexual que não envolvia o reclamante diretamente (expondo nominalmente o assediador e a vítima), outras pessoas foram citadas, tais como os colegas de trabalho e diretores da empresa. O julgado chegou até mesmo a referir uma úlcera na córnea que acomete a trabalhadora vítima do assédio sexual, que não é parte neste processo, com a transcrição do depoimento do médico que serviu como testemunha naquela ocasião, tudo isso com a divulgação dos nomes completos de todas essas pessoas.

Esta é a síntese de um problema corriqueiro dos processos trabalhistas, cujas demandas geralmente envolvem diversos sujeitos tão vulneráveis quanto o reclamante, já que a prova testemunhal é a mais utilizada para a comprovação de práticas discriminatórias, e o trabalhador que figura como testemunha também costuma ser alvo de represálias. Resta urgente a adoção

de medidas capazes de mitigar o acesso a informações que não são de interesse público, já que em nada contribuem para uma maior transparência do processo, muito pelo contrário, acabam violando direitos fundamentais dos trabalhadores e de terceiros, o que repercute inclusive nos seus direitos sociais. Se a informação divulgada em nada acrescenta aos cidadãos, por que não ocultar trechos das decisões disponibilizadas nos portais? Além da anonimização dos acórdãos, a restrição de acesso aos bancos de jurisprudência aos advogados a partir da utilização de assinatura eletrônica é uma alternativa viável, capaz de, ao menos, minimizar o problema.

A retaliação sofrida pelo trabalhador que figurou como reclamante na Justiça do Trabalho é uma prática que há muito vem sendo adotada pelas empresas, seja pela despedida discriminatória, caso permaneça o vínculo empregatício com a reclamada, ou após a despedida, pela elaboração e repasse das "listas sujas" e através das pesquisa *on-line,* situações em que a simples divulgação do nome é suficiente para a produção do dano. A título exemplificativo, basta citar que a busca jurisprudencial no *site* do TST indicou dentre os resultados 2 (dois) acórdãos que abordavam a despedida discriminatória de empregados pelo ajuizamento de reclamações trabalhistas, o que evidencia ser este um problema frequente que surge como obstáculo ao acesso à justiça do trabalhador.

Quando se trata do trabalhador que foi preterido de uma vaga de emprego por ter em seu histórico o ajuizamento de demandas trabalhistas em vínculos passados, a dificuldade de comprovação se torna intransponível ao reclamante, o que impede uma eventual reparação pela via judicial. O Poder Judiciário, na medida em que divulga essas informações, surge como um dos responsáveis pela lesão imposta ao trabalhador, sendo que nem ao menos é capaz de repará-la diante da impossibilidade de comprovação pela vítima. As condutas do Poder Público (agente que divulga os dados pessoais, sem o consentimento do obreiro), e do empregador (agente que coleta os dados e utiliza para fins discriminatórios) entretanto, não são as únicas a causarem danos ao trabalhador.

Todos os pontos analisados até aqui indicaram uma divulgação indiscriminada das informação jurisprudenciais e um maior número de limitações ao acesso de informações processuais pelo portal do Tribunal Superior do Trabalho (restringindo-se, ao menos, a busca pelo nome do trabalhador). Ocorre que, mesmo a preocupação de não disponibilização da ferramenta de busca pelo nome do reclamante, presente na Resolução nº 121 do CNJ, esvazia-se perante a atuação de buscadores de informações processuais, que realizam a tarefa de indexação e organização de dados, que se tornam facilmente acessíveis por qualquer pessoa. É o caso do *site* escavador (www.escavador.com), que colabora solidariamente com o Poder

Público na violação à privacidade do reclamante e, por conta disso, será observado na sequência da dissertação.

Figura 9 – *Site* "Escavador" – página inicial (ESCAVADOR, 2019)

O portal (ESCAVADOR, 2019) apresenta-se como o "Seu assistente jurídico", uma ferramenta de busca que vasculha os orgãos oficiais de todo o Brasil, coletando informações processuais, agrupando, organizando e disponibilizando ao usuário os dados encontrados. Por conta disso, a tela inicial do *site* (Figura 9) já remete a um campo de buscas que permite a pesquisa por pessoas, empresas, Diários Oficiais, partes em processos e jurisprudência.

A pesquisa direta pelo nome da pessoa ou empresa aponta como resultados todos os processos indexados ao termo buscado, com indicação de nomes das partes, advogados, número do processo e movimentações, que são organizadas por data, oferecendo acesso direto às notas de expedientes publicadas nos Diários Oficiais (ESCAVADOR, 2019), tudo de forma reorganizada e sistematizada. Se a restrição de acesso aos processos trabalhistas por meio da busca por nome do reclamante atinge os Tribunais do Trabalho, o mesmo não se pode dizer do Escavador, já que seu objetivo é justamente permitir, da forma mais facilitada possível, o amplo acesso a toda informação relacionada a pessoas físicas ou jurídicas que é disponibilizada nos bancos de dados do Poder Público.

Portanto, o seu funcionamento assemelha-se ao de outros mecanismos de buscas na *Internet*, já que envolve a utilização de palavras-chave fornecidas pelo usuário, que são

buscadas em índices a partir da navegação automatizada a diferentes *sites* por meio de robôs (*softwares* criados para esta finalidade). Quando as palavras-chave coincidem com este índice, o usuário recebe uma lista contendo os links a ela relacionados, possibilitando o acesso às informações de acordo com o termo pesquisado (LEONARDI, 2012, p. 289).

Assim, conforme explica a Ministra Nancy Andrighi (2012, p. 70) a atividade dos buscadores é dividida em três etapas: (i) as páginas da *web* são identificadas por uma espécie de robô; (ii) após a identificação, a página passa por um processo de indexação, com a catalogação e o mapeamento de cada palavra existente, formando a base de dados para as buscas; (iii) realizada a pesquisa pelo usuário, os critérios de busca são comparados com as informações indexadas por um processador, e posteriormente inseridas na base de dados do provedor, apresentando o resultado com a determinação das páginas relevantes.

A situação do Portal Escavador assemelha-se à do *site* "Tudo Sobre Todos", por meio do qual era possível o acesso a informações pessoais como endereço, telefone e nome dos ascendentes mediante a busca pelo nome do indivíduo, sem qualquer consentimento por parte do titular, e por conta disso teve seu acesso suspenso por decisão liminar da 1ª Vara Federal do Rio Grande do Norte, proferida em julho de 2015 (SOUZA, 2019, p. 422). Assim como operava o *site* "Tudo Contra Todos", o portal Escavador também se vale de informações supostamente públicas para divulgar dados pessoais de forma irrestrita, sem o consentimento do titular, além da prática da comercialização de informações que não são disponibilizadas em sua versão gratuita.

Ao comercializar dados pessoais dos cidadãos (a empresa mantém, inclusive, planos pagos que permitem um maior monitoramento de dados), o portal Escavador desvia-se completamente da finalidade da coleta original dessas informações pelo Poder Público, uma vez que o interesse público não pode ser utilizado para justificar o objetivo unicamente comercial de uma empresa privada no tratamento de dados pessoais, em grande parte sensíveis. Com isso, a atividade viola o princípio da finalidade, no momento em que o *site* realiza o tratamento de informações com fins lucrativos, e possivelmente o da não discriminação, já que a maioria dos acessos a esse tipo de ferramenta pela *Internet* possui propósitos não legítimos, frequentemente segregacionistas.

Outro ponto a ser observado, e que diferencia o Escavador e o próprio portal Jus Brasil de outros mecanismos de busca na *Internet*, como o *Google*, é que esses buscadores de informações processuais não apenas direcionam o usuário para a página relacionada à palavra-chave buscada, mas também reproduzem as informações, alojando-as em seu próprio *site.* Assim, o tratamento fornecido pelos buscadores processuais a esses dados amplifica o seu

potencial lesivo na medida em que os reorganiza, transformando uma informação fragmentada e dispersa em uma nova informação, agrupada e dissecada. Tamanha facilidade de acesso a um conteúdo altamente discriminatório é uma preocupação para Leal (2019, p. 161), já que:

> [...] basta lançar o nome da pessoa no Google que este remete a 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.

Não fosse o bastante, o *site* Escavador ainda disponibiliza ao usuário a opção de compartilhamento nas redes sociais (*Facebook*, *Twitter* e *Google* Plus) das informações de cada processo, ou de todos os resultados indexados a uma pessoa determinada (incluindo um resumo de seu histórico) (ESCAVADOR, 2019), uma ferramenta que não possui qualquer função que não seja a de expor o jurisdicionado, atentando violentamente contra a sua privacidade, sem que exista uma justificativa plausível para isso. Ao permitir a transmissão de dados pessoais por meio de uma ferramenta de compartilhamento, o *site* não só atua solidariamente com o Poder Público na divulgação de informações sem o consentimento do jurisdicionado como permite que terceiros repercutam os dados em inúmeras redes que podem se multiplicar instantaneamente, atingindo um grande número de pessoas e tomando uma proporção imprevisível, de forma ainda mais nefasta ao trabalhador do que as já antiquadas "listas sujas".

Além do botão "Compartilhar", o sistema oferece a função de monitoramento[111], opção em que o usuário cadastra-se para receber atualizações futuras, sendo informado acerca de qualquer nova movimentação ou atualização de processo, nome de pessoa ou empresa, através do acompanhamento de Diários Oficiais de todo o Brasil (ESCAVADOR, 2019). A ferramenta permite que um termo de busca seja pré-fixado e que novas atualizações sejam enviadas automaticamente ao usuário, inclusive com andamentos processuais, o que amplia a vulnerabilidade do trabalhador à vigilância eletrônica implementada pelos diversos atores de uma sociedade em rede.

Diante de tantas ferramentas intrusivas, o portal disponibiliza, ao menos, uma opção ao titular dos dados pessoais para a remoção das informações, bastando o envio de um documento que confirme sua identidade. A opção é selecionável tanto na tela que apresenta os resultados

[111] Além de opções básicas que podem ser acessadas sem o cadastramento do usuário (que permite o monitoramento de apenas um termo de busca), o *site* Escavador oferece planos de assinatura, que progressivamente permitem o monitoramento de uma maior quantidade de termos em Diários Oficiais (até o limite máximo de cinquenta), a depender do valor da mensalidade (ESCAVADOR, 2019).

gerais da busca relacionada a uma pessoa, contendo os resultados indexados ao seu nome, como na tela relativa a um processo em específico (ESCAVADOR, 2019). Ainda que esta medida não seja suficiente para impedir o dano causado, já que o jurisdicionado, na maioria das vezes, nem tem o conhecimento dessa divulgação, mostra-se um paliativo que aparentemente tem a finalidade de permitir uma rápida remoção de conteúdo sem a necessidade da interpelação pela via judicial.

A enorme assimetria existente entre o jurisdicionado, titular dos dados pessoais, e o portal Escavador, pessoa jurídica de direito privado que, ao exercer sua atividade econômica, figura na condição de controlador do tratamento desses dados, é agravada pelo fato de que muitos trabalhadores sequer têm acesso ao uso das tecnologias, seja para tomar conhecimento da existência do banco de dados a seu respeito, seja para adotar qualquer tipo de atitude visando a exclusão dessas informações. O tema deve ser analisado à luz dos direitos fundamentais e da vinculação dos particulares a esses direitos, reconhecendo-se a preponderância da dignidade humana e dos direitos personalíssimos do trabalhador diante da utilização de seus dados pessoais com finalidade meramente econômica pelos *sites* de busca.

O *site* ainda apresenta uma opção de pesquisa jurisprudencial, que vasculha os bancos de dados dos Tribunais Superiores, através da opção de filtragem por tribunal (TST, STJ ou STF), Estado de origem do processo, tipo de documento, relator, órgão julgador, classe do recurso/ação, distância entre termos e data de julgamento (ESCAVADOR, 2019). Nesta opção, o sistema nada mais faz do que sistematizar os dados disponibilizados pelos tribunais, sem agregar maiores funcionalidades, e com alguns problemas de funcionamento no motor de busca. Prova disso é que a pesquisa pela palavra-chave "despedida discriminatória" não obteve resultados encontrados, ao contrário da pesquisa diretamente no portal do Tribunal Superior do Trabalho.

É importante observar que o portal Escavador é alimentado por meio de informações divulgadas pelo Poder Público, sem alteração dos conteúdos originais, conforme é explicado na seção "Quem somos" (ESCAVADOR, 2019):

> TODO o conteúdo do site foi coletado automaticamente de fontes públicas, seja pela Lei de Acesso à Informação ou de fontes jurídicas e de instituições públicas
>
> Portanto, o Escavador não produz ou altera nenhum dos conteúdos exibidos, assim como não substitui as fontes originárias da informação,e não garante a veracidade nem a atualização dos dados.

Ocorre que mesmo os dados cujo acesso é público não podem sofrer um uso indiscriminado, devendo ser observados o contexto em que a informação foi disponibilizada, bem como a existência de compatibilidade entre o uso e as circunstâncias pelas quais a informação foi publicizada (TEPEDINO; TEFFÉ, 2019, p. 304). Além do mais, a proteção de dados pessoais não deve se submeter à lógica binária do público/privado, já que mesmo os dados cujo acesso é público subordinam-se a um regime protetivo necessário para evitar a formação de perfis discriminatórios, tal como relatam Bioni e Ribeiro (2015):

> De qualquer forma, não seria difícil imaginar um caso de compilação de dados pessoais sensíveis, apesar de serem de acesso público irrestrito – indexados na rede por exemplo - como a orientação política, sexual e religiosa. Por conseguinte, tais compilações de dados estariam fora do escopo de controle dos cidadãos, abrindo-se uma porta perigosa para a desproteção de dados pessoais. Isto porque, no final das contas, pode haver um volume de informações detalhado sobre uma pessoa a compor um perfil muito preciso sobre a sua personalidade.

Assim, o risco de se operar na dicotomia reducionista entre o público e privado reside no esvaziamento da esfera de controle do cidadão sobre seus dados pessoais, o que faz ainda menos sentido diante do fenômeno do *Big Data* e das modernas possibilidades de reagrupamento de dados. Não há dúvidas de que o pleno exercício de um direito à autodeterminação informativa pelo cidadão implica em estabelecer um nível protetivo equivalente aos dados tidos como públicos ou privados (BIONI; RIBEIRO, 2015).

Não é à toa que a LGPD incluiu, em seu artigo 7º, parágrafo 3º, uma cláusula expressa determinando que "O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização" (BRASIL, 2018a). Na hipótese em tela, não existe qualquer interesse público na divulgação de informações pessoais por entres privados, cuja atividade exercida é de cunho eminentemente econômico, utilizando-se de dados pessoais como insumo para o desenvolvimento de seu negócio particular, tornando-se completamente despropositada a justificativa oferecida pelo *site*.

Diante disso, é importante a reflexão acerca do grau de responsabilidade de um portal que organiza e reverbera as informações transmitidas por fontes públicas pelos danos gerados aos cidadãos afetados por essa divulgação. Ainda que o Marco Civil da *Internet* assegure que os provedores de aplicação de *Internet* somente poderão ser responsabilizados civilmente por danos decorrentes de conteúdo gerado por terceiros nos casos em que não tomar as providências para tornar indisponível o conteúdo ilícito após ordem judicial, dentro do prazo estabelecido (artigo 19) (BRASIL, 2014), no caso dos buscadores processuais não há apenas o

direcionamento à outros endereços, mas sim a reprodução e a reorganização das informações na própria página, o que envolve o tratamento de dados sensíveis, coletados e distribuídos sem o consentimento do titular, para finalidades distintas daquelas para as quais foram coletados.

Portanto, o artigo 942 do Código Civil (BRASIL, 2002) é claro ao afirmar que, quando a conduta de dois ou mais agentes contribuir para o dano, todos os partícipes possuem o dever de indenizar. É justamente esta a situação observada no caso em tela, em que concorrem decisivamente para o dano as condutas do Poder Público, da entidade privada (Escavador ou qualquer outro motor de busca de informações processuais) e do próprio empregador, quando coleta, armazena e faz uso desta informação com finalidade discriminatória.

A utilização indevida de dados pessoais por entidades públicas e privadas é tema contemplado pelo artigo 34 da Lei de Acesso à Informação, que responsabiliza os órgãos e entidades públicas pelos danos causados, o que também se aplica "[...] à pessoa física ou entidade privada que, em virtude de vínculo de qualquer natureza com órgãos ou entidades, tenha acesso a informação sigilosa ou pessoal e a submeta a tratamento indevido (BRASIL, 2011). Estes dispositivos permitem, atualmente, a responsabilização solidária do Poder Público juntamente com as empresas que mantém os provedores de pesquisa, pelas lesões impostas aos jurisdicionados. Esta responsabilidade, de natureza objetiva, é amparada pelas doutrinas do risco-administrativo, no caso do tratamento de dados pelo Estado, e do risco-proveito[112], no que se refere ao tratamento realizado pelos buscadores de *Internet,* já que o tratamento de dados sensíveis (incluindo a sua divulgação pública) deve ser classificado como uma atividade de risco, sendo que a única finalidade buscada por essas empresas com a propagação de informações pessoais é o lucro, desvinculando-se completamente do interesse público.

Somado a isso, considere-se que, com a entrada em vigor da LGPD, passará também a viger a sua disciplina com relação à responsabilidade civil e o ressarcimento de danos pelas operações de tratamento de dados, que obriga o controlador ou o operador responsáveis pela geração de dano patrimonial, moral, individual ou coletivo à devida reparação (artigo 42). A lei estabelece, ainda, a responsabilidade solidária quando houver mais de um controladores diretamente envolvidos no tratamento (artigo 42, II) (BRASIL, 2018a). Vale lembrar que o termo "controlador" é definido pela lei, em seu artigo 5º, VII, como a "[...] pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais" (BRASIL, 2018a), o que abarca tanto o Poder Público como as pessoas

[112] A teoria do risco-proveito determina que "[...] todo aquele que, de modo habitual, organizado e profissional ou empresarial, desenvolve atividade e dela retira proveito ou vantagem (econômica ou não), deverá responder pelos danos advindos da sua atividade, independentemente de culpa" (BOLESINA, 2019, p. 466).

jurídicas de direito privado. Também será possível ao lesado, com a entrada em vigor da LGPD, além de eventual reparação civil na esfera judicial, buscar o bloqueio, a anonimização ou a retirada das informações pela via administrativa, através do peticionamento à Autoridade Nacional de Proteção de Dados.

Por outro lado, como responsabilizar o empregador que faz uso de informação disponibilizada pelo próprio Poder Público? Não há dúvidas de que os dados pessoais devem ser tratados conforme os princípios da boa-fé objetiva, finalidade e não discriminação, preceitos expressos pela LGPD. Entretanto, sendo essas informações publicizadas pelo Poder Judiciário em seus portais institucionais, com livre acesso a qualquer pessoa, torna-se uma tarefa ingrata ao reclamante o ônus de comprovar o nexo causal existente entre o dano e a conduta patronal. De qualquer forma, havendo a comprovação de que houve a utilização indevida das informações pessoais por parte da empresa, é cabível a sua responsabilização solidária juntamente aos demais autores da ofensa.

A análise da legislação vigente, somado ao exame das ferramentas de pesquisa processual e jurisprudencial disponibilizadas pelo Tribunal Superior do Trabalho, indicam que o Brasil não garante ao trabalhador uma efetiva proteção de seus dados pessoais, tanto pela insuficiência normativa quanto porque permite a divulgação de dados sensíveis do jurisdicionado na *Internet* por meio de buscas de jurisprudência, sem a ocultação do nome do reclamante e, principalmente, pela ausência de controle com relação aos *sites* que coletam e reproduzem dados divulgados pelo Poder Judiciário, tais como o Escavador. Ainda assim, em um comparativo com o que foi observado na Argentina, verificou-se que, mesmo sem uma lei vigente regulando a proteção de dados no país, o atual sistema de proteção de dados pessoais brasileiro mostra-se, no mínimo, no mesmo patamar protetivo do vizinho mercosulino, já que problemas semelhantes foram detectados naquele país.

O estudo da Lei Geral de Proteção de Dados Pessoais, que entrará em vigor no próximo ano, indicou melhores perspectivas ao trabalhador, já que a *novel* legislação dispõe de um rol de direitos e garantias ao titular e de um amplo arcabouço principiógico, demontrando um nível protetivo compatível à legislação argentina. Não restam dúvidas quanto ao avanço representado pela nova normativa, mas já é possível evidenciar pontos críticos no que diz respeito à submissão da Autoridade Nacional de Proteção de Dados ao Poder Executivo, prejudicando-se a sua autonomia, e à carência de regulamentações específicas com relação à divulgação de informações processuais pelo Poder Público, tema que foi completamente esquecido pela lei, a exemplo do que já havia ocorrido com o vizinho latino-americano.

Ainda que a lei seja o primeiro passo para a criação de uma cultura de privacidade no país, diversas outras medidas são necessárias para uma efetiva proteção do trabalhador, a começar pela fiscalização constante e atuação inibitória concreta das autoridades administrativas e judiciárias. Somado a isso, é imprescindível a instituição de políticas públicas e campanhas de esclarecimento quanto às consequências do compartilhamento de informações na *Internet*, visando a conscientização do cidadão na tomada de medidas de autoproteção da privacidade (FINCATO; GUIMARÃES, 2019, p. 281).

A liquidez contemporânea desvela novos desafios impostos à sociedade, dificultando o acompanhamento pelo legislador, preso a soluções estáticas. Esses conflitos demandam variadas formas de regulamentação, a partir de uma atuação integrada entre o Poder Público, o setor privado e a sociedade, em busca de um objetivo comum: o fortalecimento da segurança das relações jurídicas. Ainda é cedo para se mensurar quais serão, de fato, os impactos da LGPD na atuação empresarial e administrativa, já que ainda pairam diversas dúvidas de ordem prática quanto à sua implementação. Certo é que as velhas práticas deverão ser revistas, sob pena da manutenção dos velhos paradigmas que sustentam a sua lógica de desenvolvimento às custas de direitos individuais e sociais.

CONCLUSÃO

Não são poucos os impactos representados pelo rápido avanço tecnológico na sociedade, especialmente nas últimas décadas. Novas ferramentas permitem a comunicação instantânea entre pontos opostos do globo, saciam o impulso consumista de uma sociedade movida pela novidade, e dão conforto a uma população obcecada pela segurança. Mas tudo tem um preço, e se a moeda representou um avanço histórico ao homem, facilitando as relações de troca, o insumo mais valioso nos dias atuais são os dados pessoais. São eles que movem o comércio internacional, alimentando governos e empresas transnacionais e gerando poder através do controle da informação e o implemento de práticas de vigilância em escala global.

Se o incremento da vigilância por meio das tecnologias da informação e da comunicação representa uma ameaça aos direitos fundamentais dos cidadãos que transitam nesta sociedade em rede, pode-se lembrar que esta prática não é uma novidade desta era, ainda que os métodos tenham se sofisticado ao longo dos tempos. Práticas de controle e disciplina inseridos nos sistemas fabris garantiam a efetividade de um modelo de monitoramento característico do período industrial, submetendo os trabalhadores através da docilização de seus próprios corpos e da restrição de sua liberdade.

A sociedade atual carrega consigo novas formas de submissão dos corpos, ainda que travestidas de uma liberdade aparente. No mundo do trabalho, as tecnologias silenciosamente inseridas nos sistemas produtivos permitem não só o controle interno do ambiente laboral, como também o monitoramento do trabalhador quando está fora dele, em sua vida privada. Se este é um problema para o empregado, vigiado e controlado diuturnamente, maior ainda são os impactos para aquele que busca a tutela de seus direitos no Poder Judiciário, já que o ente responsável pela sua proteção é o primeiro a divulgar pela *Internet* as informações que lhe foram confiadas, repercutindo em novas violações. Diante das circunstâncias que se apresentam, não restam opções ao reclamante se não ceder seus dados pessoais à Justiça do Trabalho, ainda que não expresse o consentimento com qualquer forma de utilização diversa do que a própria resolução da lide.

Se o Brasil ainda se encontra em um estágio incipiente enquanto aguarda a entrada em vigor de uma lei que tutele os dados pessoais de forma ampla, o mesmo não se pode dizer de outros países da América Latina, como a Argentina, cuja legislação sedimentou-se ao longo das últimas duas décadas. Diante dessa disparidade, a proposta desta dissertação foi justamente estabelecer um comparativo entre os sistemas jurídicos existentes nos dois países, de forma a

poder compreender se as legislações vigentes impactam positivamente nas práticas protetivas de dados pessoais pelos tribunais trabalhistas.

Estruturada em três capítulos, a pesquisa buscou cumprir com os objetivos específicos inicialmente delineados. No capítulo inaugural, intitulado "Quando o acesso à justiça se constitui em um risco ao jurisdicionado: vulnerabilidades do trabalhador diante do tratamento de dados pessoais no processo do trabalho", alcançou-se o objetivo de identificar as vulnerabilidades do trabalhador diante do tratamento de dados pessoais no processo trabalhista, observando a problemática do trabalhador sob um duplo viés: a vigilância exercida pelas entidades privadas e os impactos da inserção das TIC no mundo do trabalho, em um primeiro momento, e o tratamento de dados pessoais pelo próprio Poder Público na publicização de trâmites e informações processuais.

No segundo capítulo, denominado "A proteção jurídica de dados pessoais no processo do trabalho da sociedade em rede", o foco de atenção voltou-se à problemática jurídica, momento em que se efetuou o estudo evolutivo do direito à proteção de dados pessoais, desde seus primórdios enquanto um direito estritamente pessoal e de cunho individualista até a concepção atual, vinculado à autodeterminação informativa e à possibilidade de controle das informações pessoais por parte dos cidadãos, reconhecendo a vinculação do Poder Público e dos particulares a este direito fundamental da sociedade em rede. No mesmo capítulo, cumpriu-se o objetivo específico de examinar o regramento existente na União Europeia, a fim de utilizá-lo como paradigma para a análise normativa dos países latino-americanos, a ser realizada no capítulo seguinte.

O exame e o comparativo entre os sistemas protetivos de dados pessoais do Brasil e da Argentina foi realizado no terceiro capítulo, intitulado "Os sistemas de proteção de dados pessoais em perspectiva comparada: aproximações e distanciamentos entre Argentina e Brasil", ocasião em que se buscou verificar qual sistema jurídico garante a maior proteção ao trabalhador, especialmente aquele que ajuizou reclamação trabalhista anteriormente e que se encontra em posição de vulnerabilidade pela possibilidade de uso discriminatório de seus dados.

Dessa forma, retomando-se os sete critérios previamente elencados para a análise das leis protetivas de dados pessoais, a partir de um cruzamento das informações coletadas em cada um dos países, chega-se às seguintes constatações em perspectiva comparada:

Categoria 1 – "Escopo de aplicação": a legislação brasileira, por ser mais recente, incorpora o caráter extraterritorial presente no RGPD da União Europeia. O modelo apresentado pela Argentina mostra-se menos protetivo neste quesito, uma vez que não contempla os bancos de dados localizados fora do país, fragilizando o jurisdicionado com

relação à coleta de dados por empresas multinacionais e organismos estrangeiros.

Categoria 2 – "Bases legais para o tratamento de dados": a lei brasileira apresenta um maior número de hipóteses autorizadoras do tratamento de dados pessoais sem o consentimento do titular, o que pode representar uma menor proteção ao cidadão em geral. Ambas as legislações, entretanto, apresentam dispositivos vagos e permitem o tratamento de dados pelo Poder Judiciário sem maiores restrições ou indicação de cuidados a serem tomados, seja o dispositivo da lei argentina que permite o tratamento pela administração pública para o exercício das suas funções, seja o da lei brasileira que trata do exercício regular de direitos em processo judicial. Neste ponto, as leis equivalem-se em relação ao baixo nível protetivo dispensado aos dados pessoais dos jurisdicionados.

Categoria 3 – "Tratamento de dados sensíveis": a lei brasileira mostra-se menos protetiva em relação aos dados sensíveis, ao ampliar abusivamente o espaço para tratamento dessas informações. Ambas as leis de proteção de dados merecem críticas pela generalidade das cláusulas, deixando espaço para interpretações amplas e perdendo a oportunidade de delimitação quanto aos deveres específicos dos agentes responsáveis pelo tratamento de dados sensíveis, especialmente no âmbito do Poder Judiciário.

Categoria 4 - "Direitos dos titulares dos dados": a normativa brasileira mostra-se mais adequada às novas exigências de uma sociedade em rede, altamente informatizada e em constante transformação, contemplando algumas inovações inspiradas pelo Regulamento Geral de Proteção de Dados da União Europeia, tais como o direito à portabilidade de dados. Do ponto de vista das garantias oferecidas ao reclamante para a tutela de seus dados em face do uso abusivo pelo Poder Judiciário, ambas as leis demonstram possuir uma cartela satisfatória de direitos, cabendo o seu efetivo implemento e fiscalização pela respectiva autoridade fiscalizatória.

Categoria 5 – "Princípios de proteção dos dados": tanto a legislação brasileira como a argentina evidenciam uma grande influência do arcabouço de princípios delineados pelas normativas da União Europeia. Consistem em legislações com forte conteúdo principiológico, com adequado nível protetivo nesse aspecto. A existência de uma carta de princípios, dotados de força normativa, contribui para que se busque uma maior proteção dos dados pessoais do reclamante diante da total vulnerabilidade que se apresenta no campo do processo trabalhista.

Categoria 6 – "Órgão regulador de proteção de dados": a efetividade de uma política nacional de proteção de dados pessoais passa, em larga escala, pela existência de uma autoridade independente, responsável pela fiscalização e pelo controle do atendimento das exigências legais junto aos órgãos responsáveis pelo tratamento de dados. Ao estabelecerem a

vinculação destes órgãos ao Poder Executivo, tanto Brasil quanto Argentina comprometem a sua autonomia e liberdade de fiscalização, dificultando a sua atuação frente ao tratamento de dados pelos próprios entes estatais (incluindo o Poder Judiciário), o que se afasta do modelo de sucesso do RGPD da União Europeia.

Categoria 7 – "Tratamento de dados pelo Poder Público": a normativa do Brasil disciplina de maneira mais abrangente o tratamento de dados pelo Poder Público em relação à de seu país vizinho. Ambas, entretanto, são insuficientes para garantir a proteção dos dados pessoais dos jurisdicionados, na medida em que falham em não estabelecer regras específicas para o tratamento e o repasse de informações processuais (no caso da lei brasileira, esses dados acabam inserindo-se na exceção que permite a transferência a entidades privadas de dados acessíveis publicamente, vulnerabilizando o jurisdicionado).

Após o exame normativo, seguiu-se a observação sistemática e não participante dos *sites* das Cortes Superiores do Poder Judiciário trabalhista da Argentina e do Brasil, o que permitiu o estabelecimento de um panorama geral acerca da forma como os tribunais da justiça laboral dos dois países divulgam as informações pessoais dos trabalhadores. A conjugação comparativa dos dados coletados, a partir da definição de três categorias de análise, levou aos seguintes resultados:

Categoria 1 – "Possibilidade de pesquisa pelo nome do reclamante, tanto na consulta processual como jurisprudencial": enquanto o portal argentino permite a consulta pública por meio do nome do reclamante tanto na consulta processual quanto na jurisprudencial, no s*ite* brasileiro somente a consulta jurisprudencial pode ser efetuada por meio da utilização do nome como palavra-chave. Ainda que, quanto a esse quesito, o portal brasileiro apresente-se mais protetivo ao trabalhador, o Tribunal Superior do Trabalho permite a pesquisa processual pelo nome do empregador, o que pode facilitar o acesso a informações de seus ex-funcionários.

A análise conjunta dos resultados evidencia que a pesquisa jurisprudencial não costuma ser objeto de maiores preocupações com relação à proteção de dados pessoais dos sujeitos do processo, já que os portais não apresentam qualquer tipo de restrição de busca de jurisprudência em ambos os países, bastando que haja a coincidência entre a palavra-chave buscada e os termos encontrados na decisão.

No Brasil, soma-se a isso a atuação dos buscadores, como o Escavador, que oferecem a possibilidade de acesso rápido e organizado a todos os processos ajuizados pelo cidadão, inclusive com ferramentas de compartilhamento nas redes sociais e monitoramento de processos. A existência desses mecanismos representa uma porta aberta para grande número de violações aos direitos fundamentais do trabalhador, principalmente pelo grande fluxo de dados

sensíveis que integram as decisões judiciais e tornam-se facilmente acessíveis a qualquer pessoa que tenha acesso à rede mundial de computadores.

Categoria 2 – "Adoção de solução de *captcha* para consultas em processos, acórdãos e jurisprudências, visando inibir a captura de dados por meio de consultas públicas": ainda que esta prática seja sugerida pelo Conselho Superior da Justiça do Trabalho brasileira, visando ser implementada pelos Tribunais Regionais do Trabalho do país, a própria Corte Superior trabalhista do Brasil não faz uso da ferramenta, enquanto na Argentina o dispositivo é utilizado na consulta processual. Como consequência, o jurisdicionado brasileiro apresenta-se mais suscetível aos riscos advindos da coleta massiva de dados pessoais por meio de sistemas informatizados. Vale ressaltar que a adoção desse dispositivo coaduna-se à metodologia do *privacy by design,* que deve nortear as práticas protetivas de dados pessoais no país a partir da entrada em vigor da LGPD.

Categoria 3 – "Divulgação de dados sensíveis por meio da pesquisa jurisprudencial": a divulgação de dados sensíveis é uma prática adotada pelos portais de ambos os tribunais, que não fazem uso da anonimização de dados em sua consulta jurisprudencial, com uma ressalva: no tribunal argentino, em 44% do total de julgados encontrados (excluídas as repetições), somente as iniciais do nome do reclamante foram disponibilizadas, o que se torna um ponto positivo a favor da Argentina. Não foram encontradas justificativas aparentes para que essa diferenciação tenha ocorrido, pois julgados de matéria similar encontram tratamentos diferentes, e não há a indicação de segredo de justiça.

Além disso, o tribunal argentino também não realiza a divulgação dos julgados na íntegra, somente a ementa, o que pode ser considerado um outro aspecto positivo à privacidade do trabalhador, já que as informações divulgadas são menos detalhadas (ainda que contenham informações expressivas sobre aspectos da vida privada do trabalhador). O baixo número de julgados diferentes encontrados (grande quantidade de julgados repetidos) e a ausência de resultados após o ano de 2017 evidencia que o sistema utilizado pelo Poder Judicial de la Nación da Argentina encontra-se em desuso. A partir dessas constatações, é possível concluir que a ferramenta de consulta jurisprudencial do tribunal argentino acaba se tornando mais protetiva em virtude de sua precariedade, e não por uma política do Tribunal.

Dentre as categorias de dados sensíveis encontradas nas buscas realizadas nos dois países, há um evidente predomínio dos dados relacionados à saúde do trabalhador, o que pode ser explicado pela grande quantidade de ações envolvendo o pedido de reintegração do empregado(a) despedido(a) em função de doença ou gravidez. No Brasil, ainda que apresente um menor índice de julgados com a divulgação de dados sensíveis em relação ao país vizinho

na busca realizada (64,28%, contra 84% da Argentina), o Tribunal brasileiro não demonstra, de fato, uma preocupação institucional em ocultar essas informações, além de divulgar os acórdãos na íntegra e publicar o nome completo do trabalhador em todos os resultados encontrados, tornando-se menos protetivo ao trabalhador neste ponto.

Com relação às ferramentas disponibilizadas pelos *sites* em si, o sistema de consulta jurisprudencial do Tribunal Superior do Trabalho do Brasil mostra-se mais moderno (sofreu recente atualização) e melhor formatado em relação ao portal do tribunal argentino, apresentando grande número de parâmetros de busca e não indicando resultados em repetição, constatações que são positivas do ponto de vista da eficiência do Poder Judiciário, mas que não revertem em ganhos à privacidade do jurisdicionado brasileiro.

Assim, diante da análise legislativa comparada e de todos os dados coletados empiricamente, e tendo em vista que o Brasil ainda aguarda a entrada em vigor de sua nova Lei Geral de Proteção de dados pessoais, pode-se chegar a duas conclusões preliminares:

1) A legislação vigente atualmente no Brasil, por óbvio, mostra-se menos protetiva ao trabalhador em face da existência de uma lei específica na Argentina. Entretanto, é possível inferir que a existência de uma lei específica não necessariamente condiciona, ao menos de forma direta, as práticas protetivas de dados pessoais do trabalhador pela Justiça do Trabalho na divulgação das informações processuais. Ainda que possua uma lei sedimentada e reconhecida como de alto nível protetivo, inclusive pela União Europeia, a existência de tal arcabouço normativo na Argentina não refletiu em garantia ampla de proteção aos dados pessoais dos jurisdicionados, ao menos com relação às pesquisas processuais e jurisprudenciais disponibilizadas no portal do Poder Judicial da Nação.

2) O estudo da *novel* legislação brasileira, comparativamente à legislação argentina, mostrou que o Brasil encontra-se em sintonia com os padrões delineados pelas normativas da União Europeia, especialmente o Regulamento Geral de Proteção de Dados Pessoais europeu, apresentando-se em um nível compatível ao de seu vizinho mercosulino. Essa constatação, entretanto, não é motivo para animação em ambos os países, diante da vinculação das respectivas Autoridades Nacionais de Proteção de Dados ao Poder Executivo, comprometendo a autonomia de um órgão que é responsável pela fiscalização da lei, e da ausência de normas específicas que disciplinem o tratamento de dados pelo Poder Judiciário, principal foco de estudo deste trabalho.

Portanto, mesmo com a entrada em vigor da nova lei, as perspectivas para o futuro não indicam uma melhora significativa nas práticas protetiva dos dados pessoais que estão ao abrigo da justiça laboral brasileira. Ainda no panorama atual, a ausência normativa não pode ser

utilizado como justificativa para as violações à privacidade do trabalhador, já que os princípios constitucionais são dotados de força vinculante e a legislação infraconstitucional, ainda que timidamente, estabelecem os regramentos que deveriam ser respeitados pelos entes públicos e privados. Por conta disso, é possível afirmar, com boa dose de convicção, que a Autoridade Nacional de Proteção de Dados pessoais desempenhará papel fundamental para que mudanças significativas possam ocorrer, já que controle e fiscalização parecem ser os principais elementos ausentes na atualidade. Para isso, a necessária autonomia técnica e decisória, prevista expressamente na lei brasileira, precisará passar da mera letra fria para a efetividade, já previstas as dificuldades pela subordinação do órgão à Presidência da República.

Com base nas conclusões parciais acima elencadas, é possível responder ao problema de pesquisa, que consiste na pergunta: "é possível afirmar, em perspectiva comparada, que a novel legislação brasileira confere nível de proteção compatível com o seu vizinho mercosulino, revelando-se adequada e suficiente para garantir a proteção do trabalhador em face da coleta e tratamento de dados realizadas em razão do ajuizamento da reclamatória trabalhista?" Dentro das respostas previamente elencadas como possíveis solução ao problema, duas encontram-se adequadas: b) a nova lei de proteção de dados brasileira apresenta nível compatível com a legislação argentina, mas nenhuma delas mostra-se suficiente para garantir a proteção dos dados pessoais do trabalhador no âmbito da Justiça do Trabalho; e d) independentemente do nível apresentado pela lei de proteção de dados de cada país, não é possível afirmar, de maneira direta, que a existência de uma lei específica condiciona as práticas protetivas de dados pessoais do trabalhador pelo Poder Judiciário trabalhista na divulgação das informações processuais.

Por fim, em resposta ao último objetivo específico estabelecido, são propostas algumas sugestões de medidas que podem ser adotadas pelos Tribunais brasileiros para a tutela dos dados pessoais dos trabalhadores que ajuízam reclamatórias trabalhistas:

a) Restrição de acesso a bancos de jurisprudência a profissionais da área do direito. Esta providência impediria o acesso indiscriminado às pesquisas jurisprudenciais, evitando o uso discriminatório de informações do trabalhador. Dessa forma, o acesso às ferramentas de busca seria limitado aos advogados, servidores e magistrados, mediante certificação digital.

b) Anonimização de dados, buscando-se a diminuição do grau de identificabilidade do reclamante através das técnicas da supressão e da generalização de seus dados pessoais (RG, CPF, CTPS, PIS/PASEP/NIT, endereço, etc), bem como de informações ou relatos que permitam a identificação do trabalhador. A pseudonimização também consiste em uma alternativa viável, substituindo-se o nome do reclamante e seus identificadores diretos por um pseudônimo/número aleatório. Outra medida cabível é a utilização das letras iniciais dos nomes

das partes como regra geral aplicável aos processos trabalhistas, visando impedir a identificação imediata dos litigantes, tal como ocorre em outros ramos do Poder Judiciário, como as Varas de Família.

c) Ocultação de trechos de acórdãos e decisões judiciais que contenham dados sensíveis. Procedimento semelhante ao que ocorre com o tratamento da informação parcialmente sigilosa pelo Poder Público, regulamentado pelo artigo 7º, VII, § 2º da Lei de Acesso à Informação (BRASIL, 2011), limitar-se-ia o acesso a informações que possam violar o direito à privacidade dos jurisdicionados, assegurando a publicização do restante das informações.

d) Desindexação de dados em sistemas de busca na *Internet*. Procedimento necessário para a desvinculação dos resultados de busca aos nomes dos jurisdicionados, evitando que a consulta realizada por meio de buscadores de conteúdo, como o próprio *Google*, ou buscadores especificamente destinados a consultas processuais, como o *site* Escavador e o JusBrasil, realizem o agrupamento dos dados pessoais do trabalhador e impedindo as buscas por meio do nome do reclamante.

e) Implementação de mecanismo de consentimento no sistema PJe da Justiça do Trabalho. A medida consistiria na inserção pelo Tribunal de termo de consentimento no processo eletrônico, informativo quanto às finalidades do tratamento de dados e destacado das demais informações (atendendo ao requisito do artigo 8º, §1º da LGPD), que poderia ter o aceite do trabalhador, por meio de seu procurador, no ato de ajuizamento da reclamação trabalhista, não consistindo em um critério impeditivo à propositura da ação, já que poderia ser solicitado o consentimento específico para a divulgação de informações processuais na *Internet*, que poderia ser negado pelo reclamante. Outra opção mais adequada aos preceitos da LGPD, que evitaria o consentimento fornecido indiretamente, seria a exigência de juntada de termo de consentimento pelo reclamante, mediante declaração assinada pelo trabalhador e protocolada no próprio Processo Judicial Eletrônico (PJe), especificando-se as finalidades do tratamento de dados autorizadas.

f) Desenvolvimento, pela Justiça do Trabalho, de campanhas nacionais de esclarecimento com relação ao compartilhamento de informações e utilização de redes sociais pelo trabalhador, visando fomentar as práticas de autoproteção de sua privacidade. Essa medida implicaria na redução do fluxo de informações de cunho pessoal distribuídas pela *Internet*, ampliando a autodeterminação informativa do trabalhador, e minimizando os riscos desses dados serem utilizadas em detrimento do reclamante em processos judiciais.

A adoção de medidas de resguardo ao trabalhador, tais como as que foram sugeridas, é indispensável para que sejam levados a cabo os avanços representados pela nova lei, já que as

garantias legais precisam ser sentidas no campo prático, sob pena de tornarem-se inócuas. Além disso, ressalta-se a importância de uma efetiva observância, por parte de entidades públicas e privadas, do conteúdo principiológico legal, já que o desvio de destinação dos dados pessoais coletados torna-se o responsável central pelas consequências que acaba sofrendo o reclamante.

Justamente por conta disso, a atuação de uma Autoridade Nacional de Proteção de Dados (ANPD) torna-se peça central deste quebra-cabeça, uma vez que possui competência para fiscalizar a aplicação da lei, receber petições do titular dos dados e aplicar sanções em caso de tratamento realizado em descumprimento à legislação (inclusive ao Poder Público, se for ele o responsável pelo tratamento). Somente uma atuação diligente deste órgão poderá garantir ao trabalhador a segurança de buscar seus direitos no Poder Judiciário sem uma imediata exposição de sua intimidade na rede mundial de computadores.

A transparência pública é um dos avanços de um Estado Democrático de Direito, extremamente salutar para que o povo possa participar da gestão pública, inclusive através de um governo eletrônico. Entretanto, a divulgação de informações processuais não se presta a satisfazer a curiosidade pública (muito diferente do conceito de interesse público) ou, ainda pior, os preconceitos de terceiros que nenhuma relação possuem com o processo. Ao respeitar a privacidade do reclamante, o Estado não dará um passo atrás em relação à transparência de seus atos (a própria lei de acesso à informação ampara as informações privadas), ao contrário, avançará enquanto instituição democrática que garante aos seus cidadãos a proteção necessária para a busca de direitos sociais com o resguardo das suas liberdades individuais.

REFERÊNCIAS

ABRÃO, Carlos Henrique. *Processo eletrônico*: processo digital. 3. ed. rev. atual. e ampl. São Paulo: Atlas, 2011.

ACUÑA, Juan Manuel et al. La protección de datos personales y la autodeterminación informativa como respuesta desde el derecho ante el poder informático. *OPENAIRE*, 2005. Disponível em: http://scripta.up.edu.mx/xmlui/bitstream/handle/123456789/1178/R0053117.pdf?sequence=1&isAllowed=y. Acesso em: 01 nov. 2019.

AGÊNCIA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA; CONSELHO DA EUROPA. *Handbook on European data protection law - 2018 edition*. Disponível em: https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law. Acesso em: 01 jan. 2018.

ALAMI, Sophie; DESJEUX, Dominique; GARABUAU-MOUSSAOUI, Isabelle. *Os métodos qualitativos*. Petrópolis: Vozes, 2010.

ALBUQUERQUE, Roberto Chacon de; PALAZZI, Pablo A. Necesidad de armonizar el derecho a la protección de datos personales em el Mercosur. *In:* PALAZZI, Pablo Andrés (coord.). *Derecho y nuevas tecnologias*. Buenos Aires: Ad-Hoc, 2003, p. 545-580.

ALEXY, Robert. *Teoria dos direitos fundamentais*. Trad. Virgílio Afonso da Silva. São Paulo: Malheiros, 2008.

ALMEIDA FILHO, José Carlos de Araújo. *Processo eletrônico e teoria geral do processo eletrônico*: a informatização judicial no Brasil. 4. ed. rev. e atual. Rio de Janeiro: Forense, 2011.

ALTMARK, Daniel Ricardo; QUIROGA, Eduardo Molina. Protección de datos personales y reforma constitucional. *Informática y Derecho:* Revista iberoamericana de derecho informático, Mérida, n. 12-15, p. 1237-1260, 1996. Disponível em: https://dialnet.unirioja.es/descarga/articulo/249244.pdf. Acesso em: 28 dez. 2018.

AMARAL, Júlio Ricardo de Paula. *Eficácia dos direitos fundamentais nas relações trabalhistas*. 2. ed. São Paulo: LTr, 2014.

ANCEL, Marc. *Utilidade e métodos do direito comparado*. Elementos de introdução geral ao estudo comparado dos direitos. Reimp. Porto Alegre: Fabris, 2015.

ANDRIGHI, Fátima Nancy. A responsabilidade civil dos provedores de pesquisa via internet. *Revista do Tribunal Superior do Trabalho*, Brasília, v. 78, n. 3, p. 64-75, jul/set. 2012. Disponível em: https://juslaboris.tst.jus.br/bitstream/handle/20.500.12178/34301/003_andrighi.pdf?sequence=1&isAllowed=y . Acesso em: 1 nov. 2019.

ARENDT, Hannah. *A condição humana*. 10 ed. Rio de Janeiro: Forense Universitária, 2007.

ARGENTINA. Cámara Nacional de Apelaciones del Trabajo. *Processo nº 48.965/2009/CA1*. T.R.I. e P.P. ICSA. Buenos Aires, 25 de outubro de 2016a. Disponível em: http://jurisprudencia.pjn.gov.ar/documentos/jurisp/verdoc.jsp?db=B170&td=8&qn=1. Acesso em: 01 jul. 2019a.

ARGENTINA. Cámara Nacional de Apelaciones del Trabajo. *Processo nº 29865/2013/CA1*. M.L.M. e M.C.F. SA. Buenos Aires, 21 de dezembro de 2016b. Disponível em: http://jurisprudencia.pjn.gov.ar/documentos/jurisp/verdoc.jsp?db=B170&td=13&qn=1. Acesso em: 01 jul. 2019b.

ARGENTINA. *Código Civil de la República Argentina*, 29 de septiembre de 1869. Disponível em: https://www.oas.org/dil/esp/Codigo_Civil_de_la_Republica_Argentina.pdf. Acesso em: 28 maio 2018.

ARGENTINA. *Constitución de la Nación Argentina*. Ley n. 24.430 - Ordénase la publicación del texto oficial de la Constitución Nacional (sancionada en 1853 con las reformas de los años 1860, 1866, 1898, 1957 y 1994). Disponível em: http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/804/norma.htm. Acesso em: 2 jun. 2018.

ARGENTINA. *Decreto nº 1558/2001 de 29 de noviembre de 2001*. Reglamentación de la ley de protección de datos personales. Disponível em: http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70368/norma.htm. Acesso em: 2 jun. 2018.

ARGENTINA. *Ley nº 11.544, de 12 de setiembre de 1929*. Ley da Jornada de Trabajo. Disponível em: http://www.ilo.org/dyn/travail/docs/975/Ley%2011.544.pdf. Acesso em: 2 jun. 2018.

ARGENTINA. *Ley nº 18.345, de 12 de setiembre de 1969.* Organizacion y procedimento de la justicia nacional del trabajo. Disponível em: http://servicios.infoleg.gob.ar/infolegInternet/anexos/45000-49999/48890/norma.htm. Acesso em: 3 fev. 2019.

ARGENTINA. *Ley nº 20.744, de 20 de setiembre de 1974*. Ley de Contrato de Trabajo. Disponível em: http://servicios.infoleg.gob.ar/infolegInternet/anexos/25000-29999/25552/texact.htm. Acesso em: 2 jun. 2018.

ARGENTINA. *Ley nº 21.173, de 22 de octubre de 1975*. Modifica ley 340 y derroga ley 20889 sobre derecho a la intimidade. Disponível em: http://www.informaticalegal.com.ar/1975/09/30/ley-21-173-introduccion-del-articulo-1071-bis-al-codigo-civil/. Acesso em: 2 jun. 2018.

ARGENTINA. *Ley nº 23.592, de 23 de agosto de 1988*. Penalización de actos discriminatorios. Disponível em: http://servicios.infoleg.gob.ar/infolegInternet/anexos/20000-24999/20465/texact.htm. Acesso em: 1 nov. 2019.

ARGENTINA. *Ley nº 25.326 de 04 de octubre de 2000*. Ley de Protección de los Datos Personales. Disponível em: http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm. Acesso em: 2 jun. 2018.

ARGENTINA. *Ley nº 26.994 de 7 de octubre de 2014*. Codigo Civil y Comercial de la Nación. Disponível em: http://servicios.infoleg.gob.ar/infolegInternet/anexos/235000-239999/235975/norma.htm. Acesso em: 2 jun. 2018.

ARGENTINA. *Ley nº 27.275, de 14 de septiembre de 2016c.* Derecho de acceso a la información pública. Disponível em: http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/265949/norma.htm. Acesso em: 12 fev. 2019.

ARGENTINA. *Portal Poder Judicial de la Nación*. Disponível em: http://www.pjn.gov.ar/. Acesso em: 2 fev. 2019a.

ARGENTINA. *Portal Centro de Información Judicial*. Disponível em: http://cij.gov.ar/inicio.html. Acesso em: 13 fev. 2019b.

ASSEMBLEIA GERAL DAS NAÇÕES UNIDAS. *Declaração Universal dos Direitos Humanos*. 1948. Disponível em: http://www.onu.org.br/img/2014/09/DUDH.pdf. Acesso em: 18 jun. 2018.

ASSEMBLEIA GERAL DAS NAÇÕES UNIDAS. Pacto Internacional de Direitos Civis e Políticos. Adotado pela XXI Sessão da Assembleia-Geral das Nações Unidas, em 16 de dezembro de 1966a. Disponível em: http://www.refugiados.net/cid_virtual_bkup/asilo2/2pidcp.html. Acesso em: 16 mar. 2019.

ASSEMBLEIA GERAL DAS NAÇÕES UNIDAS. Pacto Internacional de Direitos Econômicos, Sociais e Culturais. Adotado e aberto à assinatura, ratificação e adesão pela resolução 2200A (XXI) da Assembléia Geral das Nações Unidas, de 16 de Dezembro de 1966b. Disponível em: http://www.unfpa.org.br/Arquivos/pacto_internacional.pdf. Acesso em: 16 mar. 2019.

ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 05/2014 on Anonymisation Techniques*. 10 abr. 2014. Disponível em: https://www.pdpjournals.com/docs/88197.pdf. Acesso em: 25 out. 2019.

BARBOSA JÚNIOR, Floriano. *Direito à intimidade*: direito fundamental e humano na relação de emprego. São Paulo: LTr, 2008.

BARROS, Alice Monteiro de. *Proteção à intimidade do empregado*. 2. ed. São Paulo: LTr, 2009.

BARROS, Alice Monteiro de. *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.

BARROSO, Luís Roberto. *A dignidade da pessoa humana no direito constitucional contemporâneo*: a construção de um conceito jurídico à luz da jurisprudência mundial. 1. reimp. Belo Horizonte: Fórum, 2013.

BASTERRA, Marcela I. El consentimiento del afectado en el proceso de tratamiento de datos personales. *Jurisprudencia Argentina–Lexis Nexis*. Número Especial, v. 28, 2004. Disponível em: http://marcelabasterra.com.ar/wp-content/uploads/2016/11/HD.-El-consentimiento-del-afectado-en-el-proceso-de-tratamiento-de-datos-personales.pdf. Acesso em: 29 out. 2019.

BAUMAN, Zygmunt; LYON, David. *Vigilância líquida*. Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013.

BENTHAM, Jeremy. *O Panóptico*. 2. ed. Belo Horizonte: Autêntica, 2008.

BERAZATEGUI, María Emilia; EMANUELE, Germán. La casa del herrero. El acceso a la información pública en el Poder Judicial. *In: Poder Ciudadano*: corrupción y transparencia: informe 2016-2017. Ciudad Autónoma de Buenos Aires: Eudeba, 2017. p. 260-8. Disponível em: https://www.mpf.gob.ar/pia/files/2017/10/11.InformePoderCiudadano2017.pdf#page=260. Acesso em: 13 fev. 2019.

BIGO, Didier. Globalized (in) security: the field and the ban-opticon. *Illiberal practices of liberal regimes*: the (in) security games, p. 5-49, 2006. Disponível em: http://criticaltheoryindex.org/assets/bigo%2C-didier-globalized-(in)security-the-field-and-the-ban-opticon.pdf. Acesso em: 21 out. 2019.

BILBAO UBILLOS, Juan María. ¿Em qué medida vinculan a los particulares los derechos fundamentales?. In: SARLET, Ingo Wolfgang (Org.) *Constituição, direitos fundamentais e direito privado*. 2. ed. rev. e ampl. Porto Alegre: Livraria do Advogado, 2006.

BIONI, Bruno Ricardo. *Xeque-mate*: O tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. São Paulo, 2 jul. 2015. Disponível em: https://www.researchgate.net/profile/Bruno_Bioni/publication/328266374_Xeque-Mate_o_tripe_de_protecao_de_dados_pessoais_no_xadrez_das_iniciativas_legislativas_no_Brasil/links/5bc21d22a6fdcc2c91fb6f4b/Xeque-Mate-o-tripe-de-protecao-de-dados-pessoais-no-xadrez-das-iniciativas-legislativas-no-Brasil.pdf?origin=publication_detail. Acesso em: 30 jan. 2019.

BIONI, Bruno Ricardo. *De 2010 a 2018*: a discussão brasileira sobre uma lei geral de proteção de dados. 3 jul. 2018. Disponível em: https://www.nic.br/noticia/na-midia/de-2010-a-2018-a-discussao-brasileira-sobre-uma-lei-geral-de-protecao-de-dados. Acesso em: 01 fev. 2019.

BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e os limites do consentimento. 3. reimp. Rio de Janeiro: Forense, 2019.

BIONI, Bruno Ricardo; RIBEIRO, Márcio Moretto. A transposição da dicotomia entre o público e o privado: uma questão fundamental para a proteção dos dados pessoais. *Jota*, 25 de setembro de 2015. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-transposicao-da-dicotomia-entre-o-publico-e-o-privado-25092015. Acesso em: 14 out. 2019.

BIONI, Bruno Ricardo; MENDES, Laura Schertel. Regulamento europeu de proteção de dados pessoais e a lei geral brasileira de proteção de dados: mapeando convergências na direção de um nível de equivalência. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA,

Milena Donato (coord.). *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019, p. 797-820.

BITTAR, Carlos Alberto. *Os direitos da personalidade*. 5. ed. rev. atual. e aum. Rio de Janeiro: Forense Universitária, 2001.

BOBBIO, Norberto. *A era dos direitos*. Tradução de Carlos Nelson Coutinho. Rio de Janeiro: Elsevir, 2004.

BOLESINA, Iuri. Direito à extimidade no ciberespaço e a transformação do binômio público-privado. *In*: Mostra de pesquisa de direito civil constitucionalizado. 3., 2015, Rio Grande do Sul. *Anais eletrônicos*... Santa Cruz do Sul: Unisc, 2015. Disponível em: http://online.unisc.br/acadnet/anais/index.php/ecc/article/view/14341/2783. Acesso em: 6 out. 2019.

BOLESINA, Iuri. *Responsabilidade civil*. Erechim: Deviant, 2019.

BOLZAN DE MORAIS, José Luis; STRECK, Lenio Luiz. *Ciência política e teoria do estado*. 5. ed. rev. e atual. Porto Alegre: Ed. Livraria do Advogado, 2006.

BONAVIDES, Paulo. *Curso de direito constitucional*. 27. ed., São Paulo: Editora Malheiros, 2012.

BRASIL. Código Civil. *Lei nº 10.406, de 10 de janeiro de 2002*. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm. Acesso em: 2 jun. 2018.

BRASIL. Código de Processo Civil. *Lei nº 13.105, de 16 de março de 2015*. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2015/Lei/L13105.htm. Acesso em: 7 fev. 2019.

BRASIL. Consolidação das Leis do Trabalho. *Decreto-lei nº 5.452, de 1°de maio de 1943*. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del5452.htm. Acesso em: 2 jun. 2018.

BRASIL. *Constituição da República Federativa do Brasil*. Brasília: Senado Federal, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituiçao.htm. Acesso em: 2 jun. 2018.

BRASIL. *Decreto nº 350, de 21 de novembro de 1991*. Promulga o Tratado para a Constituição de um Mercado Comum entre a República Argentina, a República Federativa do Brasil, a República do Paraguai e a República Oriental do Uruguai (TRATADO MERCOSUL). Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0350.htm. Acesso em: 2 jun. 2018.

BRASIL. *Emenda Constitucional nº 45, de 30 de dezembro de 2004*. Altera dispositivos dos arts. 5º, 36, 52, 92, 93, 95, 98, 99, 102, 103, 104, 105, 107, 109, 111, 112, 114, 115, 125, 126, 127, 128, 129, 134 e 168 da Constituição Federal, e acrescenta os arts. 103-A, 103B, 111-A e 130-A, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc45.htm. Acesso em: 28 jun. 2019.

BRASIL. *Lei nº 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/l8078.htm. Acesso em: 2 jun. 2018.

BRASIL. *Lei nº 9.029, de 13 de abril de 1995*. Proíbe a exigência de atestados de gravidez e esterilização, e outras práticas discriminatórias, para efeitos admissionais ou de permanência da relação jurídica de trabalho, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9029.HTM. Acesso em: 2 jun. 2018.

BRASIL. *Lei nº 9.507, de 12 de novembro de 1997*. Regula o direito de acesso a informações e disciplina o rito processual do habeas data. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L9507.htm. Acesso em: 2 jun. 2018.

BRASIL. *Lei nº 9.756, de 17 de dezembro de 1998*. Dispõe sobre o processamento de recursos no âmbito dos tribunais. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L9756.htm. Acesso em: 7 jul. 2019.

BRASIL. *Lei nº 11.419, de 19 de dezembro de 2006*. Dispõe sobre a informatização do processo judicial; altera a Lei no 5.869, de 11 de janeiro de 1973 – Código de Processo Civil; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11419.htm. Acesso em: 17 maio 2019.

BRASIL. *Lei nº 12.414, de 9 de junho de 2011a*. 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: 6 maio 2018.

BRASIL. *Lei nº 12.527, de 18 de novembro de 2011b*. 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: 6 maio 2018.

BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Consolidação das Leis do Trabalho. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 6 maio 2018.

BRASIL. *Lei nº 13.467, de 13 de julho de 2017*. Altera a Consolidação das Leis do Trabalho (CLT), aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943, e as Leis n º 6.019, de 3 de janeiro de 1974, 8.036, de 11 de maio de 1990, e 8.212, de 24 de julho de 1991, a fim de adequar a legislação às novas relações de trabalho. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13467.htm. Acesso em: 16 maio 2019.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018a*. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em:

http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 28 set 2018.

BRASIL. *Lei nº 13.793, de 3 de janeiro de 2019a*. Altera as Leis n os 8.906, de 4 de julho de 1994, 11.419, de 19 de dezembro de 2006, e 13.105, de 16 de março de 2015 (Código de Processo Civil), para assegurar a advogados o exame e a obtenção de cópias de atos e documentos de processos e de procedimentos eletrônicos. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13793.htm. Acesso em: 29 jun. 2019.

BRASIL. *Lei nº 13.853, de 8 de julho de 2019b*. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art1. Acesso em: 8 ago. 2019.

BRASIL. *Medida provisória nº 869, de 27 de dezembro de 2018b*. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Mpv/mpv869.htm. Acesso em: 28 jan. 2019.

BRASIL. *Portal Tribunal Superior do Trabalho*. Disponível em: http://www.tst.jus.br/. Acesso em: 2 fev. 2019c.

BRASIL. *Projeto de Lei nº 4060, de 13 de junho de 2012*. Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Brasília: Câmara dos Deputados, 2012a. Disponível em: http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=548066&ord=1. Acesso em: 6 maio 2018.

BRASIL. *Projeto de Lei do Senado nº 330, de 2013*. Dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências. Brasília: Senado Federal, 2013. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=3927883&ts=1548431640805&disposition=inline. Acesso em: 6 maio 2018.

BRASIL. *Projeto de lei nº 5276, de 13 de maio de 2016*. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Brasília: Câmara dos Deputados, 2016a. Disponível em: http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1457459&filename=PL+5276/2016. Acesso em: 6 maio 2018.

BRASIL. *Projeto de lei da Câmara nº 53, de 2018*. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Brasília: Senado Federal, 2018c. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=7738646&disposition=inline. Acesso em: 24 jul. 2018.

BRASIL. Supremo Tribunal Federal. 2ª Turma. *Recurso extraordinário nº 201.819-8*. União Brasileira de Compositores - UBC e Arthur Rodrigues Villarinho. Relatora Min. Ellen Gracie. Brasília. 11 out. 2005. Disponível em www.stf.gov.br. Acesso em: 6 maio 2018.

BRASIL. Tribunal Superior do Trabalho. 8ª Turma. *Recurso de Revista nº TST-RR-205000-15.2008.5.02.0073*. C.G.S.P. e J.M.. Relator Dora Maria da Costa. Brasília. 10 ago. 2016b. Disponível em: https://jurisprudencia-backend.tst.jus.br/rest/documentos/802720301cf8b23426309ef5ee6dad3. Acesso em: 7 jul. 2019.

BRASIL. Tribunal Superior do Trabalho. 5ª Turma. *Recurso de Revista nº TST-RR-10524-33.2014.5.15.0031*. E.L.E. e V.R.N.E.C. LTDA. Relator Breno Medeiros. Brasília. 28 fev. 2018d. Disponível em: https://jurisprudencia-backend.tst.jus.br/rest/documentos/5335df162b8d9112d9629134ee883c58. Acesso em: 7 jul. 2019.

BRASIL. Tribunal Superior do Trabalho. *Súmula nº 244 do TST*. GESTANTE. ESTABILIDADE PROVISÓRIA (redação do item III alterada na sessão do Tribunal Pleno realizada em 14.09.2012) - Res. 185/2012, DEJT divulgado em 25, 26 e 27.09.2012b. Disponível em: http://www3.tst.jus.br/jurisprudencia/Sumulas_com_indice/Sumulas_Ind_201_250.html. Acesso em: 14 jul. 2019.

BRASIL. Tribunal Superior do Trabalho. *Súmula nº 443 do TST.* DISPENSA DISCRIMINATÓRIA. PRESUNÇÃO. EMPREGADO PORTADOR DE DOENÇA GRAVE. ESTIGMA OU PRECONCEITO. DIREITO À REINTEGRAÇÃO - Res. 185/2012, DEJT divulgado em 25, 26 e 27.09.2012c. Disponível em: http://www3.tst.jus.br/jurisprudencia/Sumulas_com_indice/Sumulas_Ind_201_250.html. Acesso em: 14 jul. 2019.

BRASIL. Tribunal Superior do Trabalho. *O que é o PJe. Histórico*. Disponível em: http://www.tst.jus.br/web/pje/historico. Acesso em: 31 maio 2019d.

BRÍGIDO, Carolina. CNJ deve tornar sigilosos trechos de processos com informações pessoais e reveladoras sobre as partes. *O Globo*. Rio de Janeiro, 27 maio 2019. Disponível em: https://oglobo.globo.com/brasil/cnj-deve-tornar-sigilosos-trechos-de-processos-com-informacoes-pessoais-reveladoras-sobre-as-partes-23696229. Acesso em: 28 out. 2019.

BRUNO, Fernanda. *Máquinas de ver, modos de ser*: vigilância, tecnologia e subjetividade. Porto Alegre: Sulina, 2013. Disponível em: https://comunicacaoeidentidades.files.wordpress.com/2014/07/pg-18-a-51-maquinas-de-ver-modos-de-ser.pdf. Acesso em: 21 out. 2019.

BUCAR, Daniel; VIOLA, Mario. Tratamento de dados pessoais por "legítimo interesse do controlador": primeiras questões e apontamentos. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019, p. 465-484.

BUENOS AIRES. *Ley nº 1845, de 24 de noviembre de 2005*. Ley de Protección de Datos Personales. Disponível em: http://www.cpdp.gob.ar/index.php?option=com_content&view=article&id=53&Itemid=65. Acesso em: 2 jun. 2018.

CABANELLAS DE LAS CUEVAS, Guillermo; PALAZZI, Pablo. Derecho de internet em la Argentina. *In:* CABANELLAS DE LAS CUEVAS, Guillermo; MONTES DE OCA, Ángel (coords.). *Derecho de internet*. 3. ed. Buenos Aires: Heliasta, 2012, p. 9-64.

CAMINO, Carmen. *Direito individual do trabalho*. 2. ed. Porto Alegre: Síntese, 1999.

CÁNEPA, Ivana Cajigal. Acerca de la incorporación de los derechos y actos personalíssimos em el Código Civil y Comercial de la Nación. *Perspectivas*, v. 5, n. 1, 2015. Disponível em: https://cerac.unlpam.edu.ar/index.php/perspectivas/article/view/3636/3748. Acesso em: 17 mar. 2019.

CANOTILHO, José Joaquim Gomes. *Direito constitucional e Teoria da Constituição*. 7. ed. – 2. reimp. Coimbra: Almedina, 2003.

CARRASQUILLA, Lorenzo Villegas. Protección de datos personales en América Latina: retención y tratamiento de datos personales en el
mundo de Internet. *In:* BERTONI, Eduardo Andrés (coord.). *Hacia una internet libre de censura:* propuestas para América Latina. Buenos Aires: Universidad de Palermo, 2012, p. 125-164.

CARVALHO, Augusto César Leite de. *Garantia de indenidade no Brasil*: o livre exercício do direito fundamental de ação sem o temor de represália patronal. São Paulo: LTr, 2013.

CARVALHO, Mariana Martins de; CABRAL, Rodolfo de Carvalho. Dilemas entre transparência e proteção de dados: as requisições dos órgãos de controle e o sigilo estatístico. *Esferas*, n. 14, p. 54-67, 2019.

CASTELLS, Manuel. *A galáxia da Internet*: reflexões sobre a Internet, negócios e a sociedade. Traduzido por Maria Luiza X. de A. Borges. Rio de Janeiro: Jorge Zahar, 2003.

CASTELLS, Manuel. *A sociedade em rede*. V. 01. 8. ed. rev. e ampl. São Paulo: Paz e Terra, 2005.

CASTELLS, Manuel. *O Poder da Comunicação*. São Paulo: Paz e Terra, 2015.

CASTRO, Catarina Sarmento e. *Direito da informática, privacidade e dados pessoais*. Coimbra: Edições Almedina, 2005.

CASTRO, Catarina Sarmento e. *O direito à autodeterminação informativa e os novos desafios gerados pelo direito à liberdade e à segurança no pós 11 de Setembro. 2011*. Disponível em: http://www.egov.ufsc.br/portal/sites/default/files/anexos/5544-5536-1-PB.pdf. Acesso em: 5 maio 2018.

CHAVES, Luis Fernando Prado. Responsável pelo tratamento, subcontratante e DPO. *In:* MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coords.). *Comentários ao GDPR*: Regulamento geral de proteção de dados da União Europeia. São Paulo: Revista dos Tribunais, 2018, p. 111-138.

CHEHAB, Gustavo Carvalho. *A privacidade ameaçada de morte*. São Paulo: LTr, 2015.

CLEMENTINO, Edilberto Barbosa. Processo judicial eletrônico. 1. ed. 2. reimp. Curitiba: Juruá, 2012.

COLOMBO, Juliano; DUARTE, Luiz Filipe. Processo eletrônico e seus impactos na experiência brasileira: sociedade, tempo e saúde. *In:* FINCATO, Denise Pires; VIDALETTI, Leiliane Piovesani (coords.). *Novas tecnologias, processo e relações de trabalho III*. Porto Alegre: Magister, 2019, p. 83-98.

COMISSÃO EUROPEIA. *Decisão da Comissão de 30 de junho de 2003 nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de protecção de dados pessoais na Argentina*. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32003D0490&from=PT. Acesso em: 2 jun. 2018.

COMPARATO, Fábio Konder. *A afirmação histórica dos direitos humanos*. 3. ed. rev. ampl. São Paulo: Saraiva, 2003.

CONSELHO DA EUROPA. *Convenção para a protecção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal*. 1981. Disponível em: http://www.fd.unl.pt/docentes_docs/ma/MEG_MA_5900.pdf. Acesso em: 6 maio 2018.

CONSELHO NACIONAL DE JUSTIÇA. *Resolução n. 121, de 5 de outubro de 2010*. Dispõe sobre a divulgação de dados processuais eletrônicos na rede mundial de computadores, expedição de certidões judiciais e dá outras providências. Disponível em: http://www.cnj.jus.br/images/atos_normativos/resolucao/resoluo%20121_2010.pdf. Acesso em: 1 jun. 2018.

CONSELHO NACIONAL DE JUSTIÇA. *Resolução nº 143, de 30 de novembro de 2011*. Altera a redação do art. 4º, § 1º, da Resolução CNJ no 121, de 5 de outubro de 2010. Disponível em: http://www.cnj.jus.br///images/atos_normativos/resolucao/resolucao_143_30112011_10102012202834.pdf. Acesso em: 1 jun. 2018.

CONSELHO NACIONAL DE JUSTIÇA. *Resolução nº 185, de 18 de dezembro de 2013*. Institui o Sistema Processo Judicial Eletrônico - PJe como sistema de processamento de informações e prática de atos processuais e estabelece os parâmetros para sua implementação e funcionamento. Disponível em: http://www.cnj.jus.br/busca-atos-adm?documento=2492. Acesso em: 31 maio 2019.

CONSELHO NACIONAL DE JUSTIÇA. *Portaria nº 63, de 26 de abril de 2019*. Institui Grupo de Trabalho destinado à elaboração de estudos e propostas voltadas à política de acesso às bases de dados processuais dos tribunais e dá outras providências. Disponível em: http://www.cnj.jus.br/atos-normativos?documento=2890. Acesso em: 01 jun. 2019.

CONSELHO SUPERIOR DA JUSTIÇA DO TRABALHO. *Resolução nº 94/2012*. Institui o Sistema Processo Judicial Eletrônico da Justiça do Trabalho – PJe-JT como sistema de processamento de informações e prática de atos processuais e estabelece os parâmetros para sua implementação e funcionamento. Disponível em: https://juslaboris.tst.jus.br/bitstream/handle/20.500.12178/21077/2012_res0094_csjt_rep04.pdf?sequence=22&isAllowed=y. Acesso em: 31 maio 2019.

CONSELHO SUPERIOR DA JUSTIÇA DO TRABALHO. *Resolução nº 136/2014a*. Institui o Sistema Processo Judicial Eletrônico da Justiça do Trabalho – PJe-JT como sistema de processamento de informações e prática de atos processuais e estabelece os parâmetros para sua implementação e funcionamento. Disponível em: https://juslaboris.tst.jus.br/bitstream/handle/20.500.12178/39001/2014_res0136_csjt_rep02.pdf?sequence=14&isAllowed=y. Acesso em: 31 maio 2019.

CONSELHO SUPERIOR DA JUSTIÇA DO TRABALHO. *Resolução nº 139/2014b*. Dispõe sobre medidas a serem adotadas pelos Tribunais Regionais do Trabalho para impedir ou dificultar a busca de nome de empregados com o fim de elaboração de "listas sujas". Disponível em: https://siabi.trt4.jus.br/biblioteca/direito/legislacao/atos/federais/res_csjt_2014_139.pdf. Acesso em: 8 jun. 2018.

CONSELHO SUPERIOR DA JUSTIÇA DO TRABALHO. *Resolução nº 185/2017*. Dispõe sobre a padronização do uso, governança, infraestrutura e gestão do Sistema Processo Judicial Eletrônico (PJe) instalado na Justiça do Trabalho e dá outras providências. Disponível em: https://juslaboris.tst.jus.br/bitstream/handle/20.500.12178/102716/2017_res0185_csjt_compilado.pdf?sequence=4&isAllowed=y. Acesso em: 31 maio 2019.

CONTROLADORIA-GERAL DA UNIÃO. *Manual da lei de acesso à informação para Estados e Municípios*. Brasília: 2013. Disponível em: http://www.cgu.gov.br/Publicacoes/transparencia-publica/brasil-transparente/arquivos/manual_lai_estadosmunicipios.pdf. Acesso em 06 fev. 2019.

COTS, Márcio; OLIVEIRA, Ricardo. *Lei geral de proteção de dados pessoais comentada*. São Paulo: Revista dos Tribunais, 2018.

DALLARI, Dalmo de Abreu. *Direitos humanos e cidadania*. 2. ed. reform. São Paulo: Moderna, 2004.

DAVID, René. *Os grandes sistemas do direito contemporâneo*. 3. ed. São Paulo: Martins Fontes, 1998.

DELEUZE, Gilles. *Conversações, 1972 – 1990*. Tradução de Peter Pál Pelbart. Rio de Janeiro: 34, 1992.

DELGADO, Mauricio Godinho. *Curso de direito do trabalho*. 12. ed. São Paulo: LTr, 2013.

DELMAS-MARTY, Mireille. *Três desafios para um direito mundial*. Tradução de Fauzi Hassan Choukr. Rio de Janeiro: Lumen Juris, 2003.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. São Paulo, Renovar, 2006.

DONEDA, Danilo; VIOLA, Mario. Risco e informação pessoal: o princípio da finalidade e a proteção de dados no ordenamento brasileiro. *Revista Brasileira de Risco e Seguro,* v. 5, n. 10, p. 85-102, out. 2009/mar. 2010. Disponível em: http://www.rbrs.com.br/arquivos/RBRS10-4%20Danilo%20Doneda.pdf. Acesso em: 31 dez. 2018.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *EJJL – Espaço Jurídico Journal of Law*, v. 12, n. 2, p. 91-108, jul./dez. 2011. Disponível em: https://editora.unoesc.edu.br/index.php/espacojuridico/article/view/1315/658. Acesso em: 31 dez. 2018.

DONEDA, Danilo. Princípios de proteção de dados pessoais. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira (coords.). *Direito e Internet III*: Marco Civil da Internet III – tomo I. São Paulo: Quartier Latin, 2015, p. 369-384.

DONEDA, Danilo; MONTEIRO, Marília. Acesso à informação e privacidade no caso da Universidade Federal de Santa Maria. *Jota*, 02 de julho de 2015. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/acesso-a-informacao-e-privacidade-no-caso-da-universidade-federal-de-santa-maria-02072015. Acesso em: 14 out. 2019.

ERICSON, Richard; HAGGERTY, Kevin. The surveillant assemblage. *British Journal of Sociology*, London, v. 51, n. 4, p. 605-622, dez. 2000.

ESCAVADOR. Disponível em: https://www.escavador.com/. Acesso em: 19 jul. 2019.

FARINHO, Domingos Soares. *Intimidade da vida privada e media no ciberespaço*. Coimbra: Almedina, 2006.

FAVERA, Rafaela Bolson Dalla. *Surveillance e direitos humanos*: o tratamento jurídico do tema nos EUA e no Brasil, a partir do caso Edward Snowden. Rio de Janeiro: Lumen Juris, 2018.

FERNÁNDEZ DELPECH, Horacio. Los datos sensibles em la ley de protección de datos personales. *In:* PALAZZI, Pablo Andrés (coord.). *Derecho y nuevas tecnologias*. Buenos Aires: Ad-Hoc, 2003, p. 135-163.

FERNÁNDEZ DELPECH, Horacio. *Internet, su problemática jurídica*. 2. ed. Buenos Aires: Abeledo-Perrot, 2004.

FERREYRA, Eduardo. *Legislación argentina sobre protección de datos personales*. Disponível em: https://adcdigital.org.ar/wp-content/uploads/2017/01/Legislacion-argentina-sobre-proteccion-de-datos-personales-ADC.pdf. Acesso em 20 out. 2019.

FINCATO, Denise Pires. *Teletrabalho*: uma análise juslaboral. Revista Justiça do Trabalho. Porto Alegre, v.20, n. 236, 2003.

FINCATO, Denise Pires; GILLET, Sérgio Augusto da Costa. *A pesquisa jurídica sem mistérios*: do projeto de pesquisa à banca. Porto Alegre: Fi, 2018.

FINCATO, Denise Pires; GUIMARÃES, Cíntia Ione Santiago. Relações líquidas e direito ao esquecimento: novos desafios de proteção nas relações de trabalho. *In:* FINCATO, Denise Pires; VIDALETTI, Leiliane Piovesani (coords.). *Novas tecnologias, processo e relações de trabalho III*. Porto Alegre: Magister, 2019, p. 268-283.

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

FOUCAULT, Michel. *Vigiar e punir*: nascimento da prisão. 18. ed. Petrópolis: Vozes, 1998a.

FOUCAULT, Michel. *Microfísica do Poder*. 13. ed. Rio de Janeiro: Graal, 1998b.

FRANCO FILHO, Georgenor de Souza. *Intimidade e privacidade do trabalhador* – direito internacional e comparado. São Paulo: LTr, 2016.

FRAZÃO, Ana. Nova LGPD: as demais hipóteses de tratamento de dados pessoais. *Jota*, 26 de setembro de 2018a. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-as-demais-hipoteses-de-tratamento-de-dados-pessoais-19092018. Acesso em: 14 out. 2019.

FRAZÃO, Ana. Nova LGPD: o tratamento dos dados pessoais sensíveis. *Jota*, 26 de setembro de 2018b. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-o-tratamento-dos-dados-pessoais-sensiveis-26092018. Acesso em: 14 out. 2019.

FRAZÃO, Ana. Objetivos e alcance da lei geral de proteção de dados. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019, p. 99-129.

GARCIA, Maria da Glória F.P.D. *Estudos sobre o princípio da igualdade*. Coimbra: Almedina, 2005.

GIGLIO, Wagner D.; CORRÊA, Claudia Giglio Veltri. *Direito processual do trabalho*. 16. ed. rev. ampl. adap. São Paulo: Saraiva, 2007.

GONÇALVES, Maria Eduarda. *Direito da informação*: novos direitos e formas de regulação na sociedade da informação. Lisboa: Almedina, 2003.

GONÇALVES, Victor Hugo Pereira. Direito fundamental à exclusão digital. *In:* DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira (coords.). *Direito e Internet III*: Marco Civil da Internet III – tomo I. São Paulo: Quartier Latin, 2015, p. 187-206.

GOZAÍNI, Osvaldo A. El proceso de habeas data en la nueva ley de protección de datos personales. *In:* PALAZZI, Pablo Andrés (coord.). *Derecho y nuevas tecnologias*. Buenos Aires: Ad-Hoc, 2003, p. 165-238.

GREGÓRIO, Carlos; PAIVA, Mário Antônio Lobato de. Proteção de dados pessoais no âmbito judicial. *Lex – Jurisprudência do Supremo Tribunal Federal*, ano 27, n. 313, jan. 2005. Disponível em: http://sisnet.aduaneiras.com.br/lex/doutrinas/arquivos/Prot-dados.pdf. Acesso em: 1 jul. 2018.

GRISOLIA, Julio Armando; HIERREZUELO, Ricardo Diego. La discriminación en el derecho del trabajo: el caso argentino. *Revista internacional y comparada de relaciones laborales y derecho del empleo*, v. 1, n. 1, jan./mar. 2013. Disponível em: http://ejcls.adapt.it/index.php/rlde_adapt/article/view/72/124. Acesso em: 17 mar. 2019.

GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau. Término do tratamento de dados. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019, p. 219-241.

HUNT, Lynn. *A invenção dos direitos humanos*: uma história. 1. reimp. São Paulo: Companhia das Letras, 2009.

INSTITUTO DE INVESTIGACIÓN PARA LA JUSTICIA. *Regras de Heredia*. 2003. Disponível em: http://www.iijusticia.org/heredia/Regras_de_Heredia.htm. Acesso em: 8 jul. 2018.

JIMENE, Camilla do Vale. Reflexões sobre privacy by design e privacy by default da idealização à positivação. LIMA. *In:* MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coords.). *Comentários ao GDPR*: Regulamento geral de proteção de dados da União Europeia. São Paulo: Revista dos Tribunais, 2018, p. 169-183.

JUÁRES, Noé A. Riande. Privacidad, autodeterminación informativa y la responsabilidad de proteger los bienes de uso común. *In:* PALAZZI, Pablo Andrés (coord.). *Derecho y nuevas tecnologias*. Buenos Aires: Ad-Hoc, 2003, p. 63-70.

KANT, Immanuel. *Fundamentação da metafísica dos costumes*. Lisboa: Edições 70, 1997.

KLEE, Antonia Espíndola Longoni; MARTINS, Guilherme Magalhães. A privacidade, a proteção dos dados e dos registros pessoais e a liberdade de expressão: algumas reflexões sobre o Marco Civil da Internet no Brasil (Lei n°12.965/2014). *In:* DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coords.). *Direito & Internet III*: Marco Civil da Internet – Tomo I (Lei n. 12.965/2014) – São Paulo: Quartier Latin, 2015, p. 291-367.

KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da lei 13.709/2018. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019, p. 445-463.

LAFER, Celso. *A reconstrução dos direitos humanos*: um diálogo com o pensamento de Hannah Arendt. 1. reimp. São Paulo: Companhia das Letras, 1991.

LANIER, Jaron. *Quién controla el futuro*. 1. ed. Buenos Aires: Debate, 2015.

LAVALLE COBO, Dolores. *Derecho de acceso a la información pública*. Buenos Aires: Astrea, 2009.

LEÃO, Renato Zerbini Ribeiro. *Os direitos econômicos, sociais e culturais na América Latina e o protocolo de San Salvador*. Porto Alegre: Sergio Antonio Fabris Editor, 2001.

LEITE, Carlos Henrique Bezerra. Eficácia horizontal dos direitos fundamentais nas relações de emprego. *Revista Brasileira de Direito Constitucional*, n. 17, jan./jun. 2011. Disponível em: http://www.esdc.com.br/RBDC/RBDC-17/RBDC-17-033-

Artigo_Carlos_Henrique_Bezerra_Leite_(Eficacia_Horizontal_dos_Direitos_Fundamentais_na_relacao_de_Emprego).pdf. Acesso em: 21 jan. 2019.

LEITE, Carlos Henrique Bezerra. *Curso de direito processual do trabalho*. 13. ed. São Paulo: Saraiva, 2015.

LEITE, Carlos Henrique Bezerra. *Curso de direito processual do trabalho*. 16. ed. São Paulo: Saraiva, 2018.

LEMOS, Ronaldo; ADAMI, Mateus Piva; SUNDFELD, Philippe. Proteção de dados na Administração Pública. *Jota*, 14 de maio de 2018. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/dados-administracao-publica-14052018. Acesso em: 14 out. 2019.

LEMOS, Ronaldo *et al.* GDPR: a nova legislação de proteção de dados pessoais da Europa. *Jota*, 25 de maio de 2018. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/gdpr-dados-pessoais-europa-25052018. Acesso em: 14 out. 2019.

LEONARDI, Marcel. *Tutela e privacidade na Internet*. São Paulo: Saraiva, 2012.

LÉVY, Pierre. *Cibercultura*. Traduzido por Carlos Irineu da Costa. 2. ed. São Paulo: Editora 34, 1999.

LÉVY, Pierre. *Ciberdemocracia*. Lisboa: Instituto Piaget, 2002.

LIMA, Caio César Carvalho. Objeto, aplicação material e aplicação territorial. *In:* MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coords.). *Comentários ao GDPR*: Regulamento geral de proteção de dados da União Europeia. São Paulo: Revista dos Tribunais, 2018, p. 23-36.

LIMA, Cíntia Rosa Pereira; BIONI, Bruno Ricardo. A proteção dos dados pessoais na fase de coleta: apontamentos sobre a adjetivação do consentimento implementada pelo artigo 7, incisos VIII e IX, do Marco Civil da Internet a partir da Human Computer Interaction e da Privacy By Default. *In:* DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira. *Direito e Internet III*: Marco Civil da Internet III – tomo I. São Paulo: Quartier Latin, 2015, p. 263-290.

LIMBERGER, Têmis. *O direito à intimidade na era da informática*. Porto Alegre: Livraria do Advogado, 2007.

LIMBERGER, Têmis. Da evolução do direito a ser deixado em paz à proteção dos dados pessoais. *Novos Estudos Jurídicos - NEJ*, v. 14, n. 2, p. 27-53, maio/ago. 2009. Disponível em: http://www.egov.ufsc.br/portal/conteudo/da-evolu%C3%A7%C3%A3o-do-direito-ser-deixado-em-paz-%C3%A0-prote%C3%A7%C3%A3o-dos-dados-pessoais. Acesso em: 31 dez. 2018.

LIMBERGER, Têmis; RUARO, Regina. Administração pública e novas tecnologias: o embate entre o público e o privado – análise da Resolução 121/2010 do CNJ. *Revista NEJ – Eletrônica*, v. 16, n. 2, p. 121-134, mai./ago. 2011. Disponível em:

https://siaiap32.univali.br/seer/index.php/nej/article/view/3276/2059. Acesso em: 07 jun. 2018.

LIMBERGER, Têmis. *Cibertransparência*: informação pública em rede: a virtualidade e suas repercussões na realidade. Porto Alegre: Livraria do advogado, 2016.

MALDONADO, Viviane Nóbrega. Direitos dos titulares de dados. *In:* MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coords.). *Comentários ao GDPR*: Regulamento geral de proteção de dados da União Europeia. São Paulo: Revista dos Tribunais, 2018, p. 85-109.

MALGARIN, Claudio Alves. *Direito processual do trabalho*: processo do trabalho: como seria e como é. São Paulo: LTr, 2016.

MARINONI, Luiz Guilherme; ARENHART, Sérgio Cruz; MITIDIERO, Daniel. Novo Curso de processo civil: teoria do processo civil volume 1. 3. ed. rev. atual. e ampl. São Paulo: Revista dos Tribunais, 2017.

MATHIESEN, Thomas. *The viewer society*: Michel Foucault's 'panopticon' revisited. *In*: Theoretical Criminology, May. 1997, vol. 1, n. 2, pp. 215-234. Disponível em: https://pdfs.semanticscholar.org/99cc/d5c5e27f2f1332c5f2247ba2881bed20560c.pdf. Acesso em: 21 out. 2019.

MATOS, Ana Carla Harmatiuk; RUZYK, Carlos Eduardo Pianovski. Diálogos entre a lei geral de proteção de dados e a lei de acesso à informação. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019, p. 199-218.

MARESCA, Fernando. Marketing y privacidad. *In:* PALAZZI, Pablo Andrés (coord.). *Derecho y nuevas tecnologias*. Buenos Aires: Ad-Hoc, 2003, p. 278-297.

MARTÍNEZ, Esteban Ruiz. Breve ensayo sobre el derecho a controlar la información personal. *In:* PALAZZI, Pablo Andrés (coord.). *Derecho y nuevas tecnologias*. Buenos Aires: Ad-Hoc, 2003, p. 71-119.

MELO, Ana Sofia Medeiros. *Regulamento Geral de Proteção de Dados*: um novo paradigma regulatório. 2019. Dissertação, Mestrado em Mestrado em Ciências Jurídico-Forenses, Faculdade de Direito, Universidade de Coimbra, Coimbra, 2019. Disponível em: https://estudogeral.sib.uc.pt/handle/10316/86570. Acesso em: 8 set. 2019.

MENDEL, Toby. *El Derecho a la Información en América Latina*: comparación juridica. Quito: UNESCO, 2009. Disponível em http://unesdoc.unesco.org/images/0018/001832/183273s.pdf. Aceso em 21 jul. 2018.

MENEZES, Joyceane Bezerra de; COLAÇO, Hian Silva. Quando a lei geral de proteção de dados não se aplica? *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019, p. 156-197.

MENEZES NETO, Elias Jacob de; MORAIS, Jose Luis Bolzan de; BEZERRA, Tiago José de Souza Lima. O projeto de lei de proteção de dados pessoais (PL 5276/2016) no mundo do big data: o fenômeno da dataveillance em relação à utilização de metadados e seu impacto nos direitos humanos. *Revista Brasileira de Políticas Públicas*, Brasília, v. 7, n. 3, 2017, p. 184-198. Disponível em: https://www.publicacoesacademicas.uniceub.br/RBPP/article/download/4840/3636. Acesso em: 30 jun. 2019.

MINISTERIO DA JUSTIÇA E SEGURANÇA PÚBLICA. *Argentina*. Disponível em: http://www.justica.gov.br/sua-protecao/cooperacao-internacional/cooperacao-juridica-internacional-em-materia-penal/orientacoes-por-pais/argentina. Acesso em: 31 jan. 2019.

MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS. *La justicia argentina*. Disponível em: https://www.argentina.gob.ar/justicia/argentina. Acesso em: 31 jan. 2019.

MINISTÉRIO DO TRABALHO E EMPREGO. *Portaria nº 367, de 18 de setembro de 2002*. Disponível em: http://www.trtsp.jus.br/geral/tribunal2/ORGAOS/MTE/Portaria/P367_02.htm. Acesso em: 09 jun. 2018.

MOLINARO, Carlos Alberto; SARLET, Ingo Wolfgang. Sociedade em rede, internet e Estado de vigilância: algumas aproximações. *Revista da AJURIS*, Porto Alegre, v. 40, n. 132, dez. 2013. Disponível em: http://www.ajuris.org.br/OJS2/index.php/REVAJURIS/article/view/249/184. Acesso em: 16 jul. 2018.

MORAES, Melina Ferracini. *Direito ao esquecimento na internet*: das decisões judiciais no Brasil. Curitiba: Juruá, 2018.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). *Rev. Dir. Gar. Fund., Vitória*, v. 19, n. 3, p. 159-180, set./dez. 2018. Disponível em: http://dx.doi.org/10.18759/rdgf.v19i3.1603. Acesso em: 6 set. 2019.

NAVARRO FLORIA, Juan G. *Los derechos personalísimos*. Buenos Aires: El Derecho, 2012. Disponível em: https://repositorio.uca.edu.ar/handle/123456789/2865. Acesso em: 17 mar. 2019.

NISSENBAUM, Helen. *Privacidad amenazada.* Tecnología, política y la integridad de la vida social. México: Oceano, 2010.

OIT. ORGANIZAÇÃO INTERNACIONAL DO TRABALHO. *Convenção nº 111, de 1958*. Convenção sobre a Discriminação (Emprego e Profissão). Disponível em: http://www.ilo.org/brasilia/convencoes/WCMS_235325/lang--pt/index.htm. Acesso em: 30 jun. 2018.

OIT. ORGANIZAÇÃO INTERNACIONAL DO TRABALHO. *Protection of workers' personal data:* an ILO code of practice, 1997. Commentary on the Code of Practice. Disponível em:

http://www.ilo.org/wcmsp5/groups/public/@ed_protect/@protrav/@safework/documents/normativeinstrument/wcms_107797.pdf. Acesso em: 30 jun. 2018.

OLIVEIRA, Marco Aurélio Bellizze; LOPES, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela lei 13.709/2018. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019, p. 53-83.

ORWELL, George. *1984*. São Paulo: Companhia das Letras, 2009.

OYHANARTE, Marta; KANTOR, Mora. El derecho de acceso a la información pública en la Argentina. Un análisis de su situación normativa y su efectividad. *In: Poder Ciudadano:* corrupción y transparência. Informe 2014. Buenos Aires, 2015. p. 253-80. Disponível em: http://acij.org.ar/sin_corrupcion/wp-content/uploads/2016/10/Libro_PoderCiudadano_CapVII-Acceso-a-la-informacion-publica.pdf. Acesso em: 12 fev. 2019.

PALAZZI, Pablo Andrés. Ámbito de aplicación de la ley de protección de datos personales. *In:* PALAZZI, Pablo Andrés (coord.). *Derecho y nuevas tecnologias*. Buenos Aires: Ad-Hoc, 2003, p. 121-134.

PARENTONI, Leonardo Netto. O Direito ao esquecimento (Right to oblivion). *In:* DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira. *Direito e Internet III*: Marco Civil da Internet III – tomo I. São Paulo: Quartier Latin, 2015, p. 539-618.

PARLAMENTO EUROPEU. *Projecto de tratado que estabelece uma constituição para a Europa (não ratificado)*. Acesso em: http://www.europarl.europa.eu/about-parliament/pt/in-the-past/the-parliament-and-the-treaties/draft-treaty-establishing-a-constitution-for-europe. Acesso em: 21 jan. 2019.

PARLAMENTO EUROPEU E CONSELHO. *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/PDF/?uri=CELEX:31995L0046&from=PT. Acesso em: 6 maio 2018.

PARLAMENTO EUROPEU E CONSELHO. *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 (Directiva relativa à privacidade e às comunicações electrónicas)*. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32002L0058&from=PT. Acesso em: 6 maio 2018.

PARLAMENTO EUROPEU E CONSELHO. *Regulamentos, diretivas e outros atos legislativos*. Bruxelas, 2018. Disponível em: https://europa.eu/european-union/eu-law/legal-acts_pt. Acesso em: 2 jan. 2019.

PEREIRA, Caio Mário da Silva. Direito comparado e seu estudo. *Revista da Faculdade de Direito da Universidade Federal de Minas Gerais,* Belo Horizonte, v. 7, p. 35-51, 1955.

Disponível em: https://www.direito.ufmg.br/revista/index.php/revista/article/view/889/832. Acesso em: 05 maio 2019.

PEREIRA, Marcelo Cardoso. *Direito à intimidade na Internet*. Curitiba: Juruá, 2005.

PEREIRA, Leone. *Manual de processo do trabalho*. 3. ed. São Paulo, SP: Saraiva, 2014.

PERES, Célia Mara. *A igualdade e a não discriminação nas relações de trabalho*. São Paulo: LTr, 2014.

PÉREZ LUÑO, Antonio Enrique. *Derechos humanos, estado de derecho y constituición*. Novena edición. Madrid: Tecnos, 2005.

PÉREZ LUÑO, Antonio Enrique. *Los derechos humanos en la sociedad tecnológica*. Madrid: Universitas, 2012.

PICCIRILLI, María Eugenia; QUIROGA, Eduardo Molina. Principios nacionales e internacionales en el marco de la protección de datos personales: deficiencias, recomendaciones. *In: Simposio Argentino de Informática y Derecho*. Rosario, 2015. Disponível em: http://sedici.unlp.edu.ar/bitstream/handle/10915/58627/Documento_completo.pdf?sequence=1. Acesso em: 17 mar. 2019.

PIOVESAN, Flávia. *Direitos humanos e justiça internacional*: um comparativo dos sistemas regionais europeu, interamericano e africano. São Paulo: Saraiva, 2006.

PLÁ RODRIGUEZ, Américo. Princípios de direito do trabalho. São Paulo, SP: Ltr, 1996.

PUCCINELLI, Oscar R. El "derecho al olvido" en el derecho de la protección de datos. El caso argentino. *Revista Internacional de Protección de Datos Personales*. Bogotá, n. 1, dez. 2012. Disponível em: https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/ok8_-Oscar-Puccinelli_FINAL.pdf. Acesso em: 17 mar. 2019.

RAMPAZZO, Lino. *Metodologia científica*: para alunos dos cursos de graduação e pós-graduação. São Paulo: Edições Loyola, 2011.

REALE, Miguel. *Lições preliminares de direito*. 27. ed. São Paulo: Saraiva, 2002.

REDE IBERO-AMERICANA DE PROTEÇÃO DE DADOS. *Padrões de proteção de dados pessoais para os Estados ibero-americanos*. 20 jun. 2017. Disponível em: http://www.redipd.es/documentacion/common/Estandares_PORTUGUES.pdf. Acesso em: 28 out. 2019.

REDE IBERO-AMERICANA DE PROTEÇÃO DE DADOS. *Regulamento da RIPD*. 30 nov. 2018. Disponível em: http://www.redipd.es/documentacion/common/REGLAMENTO_RIPD_REV30_11_18_PT.pdf. Acesso em: 28 out. 2019.

REDE IBERO-AMERICANA DE PROTEÇÃO DE DADOS. *Relación de entidades acreditadas RIPD*. Disponível em: http://www.redipd.es/la_red/Miembros/index-idpt-idphp.php. Acesso em: 28 out. 2019.

RIVERA, Júlio César. Derechos y actos personalísimos en el proyecto de Código Civil y Comercial. *Revista Pensar en Derecho*, 2012. Disponível em: http://www.derecho.uba.ar/publicaciones/pensar-en-derecho/revistas/0/derechos-y-actos-personalisimos-en-el-proyecto-de-codigo-civil-y-comercial.pdf. Acesso em: 17 mar. 2019.

RODOTÁ, Stéfano. *A vida na sociedade de vigilância*: a privacidade hoje. São Paulo: Renovar, 2008.

RODRIGUES, João Gaspar. *Publicidade, transparência e abertura na administração pública*. Revista de Direito Administrativo (RDA), Rio de Janeiro, v. 266, p.89-123, maio/ ago. 2014. Disponível em: http://bibliotecadigital.fgv.br/ojs/index.php/rda/article/view/32142/30937. Acesso em: 08 set. 2019.

ROQUE, Andre Vasconcelos; BAPTISTA, Bernardo Barreto; ROCHA, Henrique de Moraes Fleury da. A tutela processual dos dados pessoais na LGPD. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019, p. 741-775.

RUARO, Regina Linden; MACHADO, Fernando Inglez de Souza. Ensaio a propósito do direito ao esquecimento: limites, origem e pertinência no ordenamento jurídico brasileiro. *Revista do Direito Público*, Londrina, v. 12, n. 1, p. 204-233, abr. 2017. Disponível em: http://repositorio.pucrs.br/dspace/bitstream/10923/11549/2/Ensaio_a_proposito_do_direito_ao_esquecimento_limites_origem_e_pertinencia_no_ordenamento_juridico_brasileiro.pdf. Acesso em: 16 mar. 2019.

RUARO, Regina Linden; MOLINARO, Carlos Alberto. Conflito real ou aparente de interesses entre o direito fundamental à proteção de dados pessoais e o livre mercado. *In:* RUARO, Regina Linden; MAÑAS, José Luis Pinãr; MOLINARO, Carlos Alberto. *Privacidade e proteção de dados pessoais na sociedade digital*. Porto Alegre: Fi, 2017.

RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro; FINGER, Brunize. O direito à proteção de dados pessoais e a privacidade. *Revista da Faculdade de Direito UFPR*, v. 53, 2011. Disponível em: https://revistas.ufpr.br/direito/article/view/30768. Acesso em: 24 set. 2019.

RULLI JUNIOR, Antonio; RULLI NETO, Antonio. Direito ao esquecimento e o superinformacionismo: apontamentos no direito brasileiro dentro do contexto da sociedade da informação. *Revista do Instituto do Direito Brasileiro*, v. 1, n. 2012, p. 419–434, 2012. Disponível em: https://www.cidp.pt/publicacoes/revistas/ridb/2012/01/2012_01_0419_0434.pdf. Acesso em: 27 abr. 2018.

RULLI NETO, Antonio. *Função social do contrato*. São Paulo: Saraiva, 2011.

SALTOR, Carlos Eduardo. *La protección de datos personales*: estudio comparativo Europa-América con especial análisis de la situación argentina. 2013. Tese, Doutorado Em Direito, Faculdad de derecho, Universidad Complutense de Madrid, 2013. Disponível em: https://eprints.ucm.es/22832/1/T34731.pdf. Acesso em: 17 mar. 2019.

SÁNCHEZ BRAVO, Álvaro. *A nova sociedade tecnológica*: da inclusão ao controle social: a Europ@ é exemplo? Santa Cruz do Sul: EDUNISC, 2010.

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.

SANTOS, Boaventura de Sousa. Os tribunais e as novas tecnologias de comunicação e de informação. *Sociologias*, Porto Alegre, n. 13, jun. 2005. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1517-45222005000100004&lng=pt&nrm=iso. Acesso em 31 out. 2019.

SARLET, Ingo Wolfgang. *A eficácia dos direitos fundamentais*: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 2. ed. rev. e atual. Porto Alegre: Livraria do Advogado, 2001.

SARLET, Ingo Wolfgang. *Dignidade (da pessoa) humana e direitos fundamentais na Constituição Federal de 1988*. 10. ed. rev. atual. e ampl. Porto Alegre: Livraria do Advogado, 2015.

SARMENTO, Daniel; GOMES, Fábio Rodrigues. *A eficácia dos direitos fundamentais nas relações entre particulares*: o caso das relações de trabalho. Revista do Tribunal Superior do Trabalho, São Paulo, v. 77, n. 4, p. 60-101, out./dez. 2011. Disponível em: https://hdl.handle.net/20.500.12178/28342. Acesso em: 19 ago. 2018.

SCHREIBER, Anderson. Direito ao esquecimento e proteção de dados pessoais na lei 13.709/2018: distinções e potenciais convergências. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019, p. 99-129.

SILVA, Alberto J. Cerda. Protección de datos personales y prestación de servicios en línea en América Latina. *In:* BERTONI, Eduardo Andrés (coord.). *Hacia una internet libre de censura:* propuestas para América Latina. Buenos Aires: Universidad de Palermo, 2012, p. 165-180.

SILVA, Carlos Bruno Ferreira da. *Proteção de dados e cooperação transnacional*: teoria e prática na Alemanha, Espanha e Brasil. Belo Horizonte: Arraes Editores, 2014.

SILVA, Rosane Leal da. A vulnerabilidade do trabalhador em face da lei nº 13.709/2018: quando o acesso à justiça pode violar dados pessoais sensíveis. *In:* GUIMARÃES, Cíntia; FELTEN, Maria Cláudia; ROCHA, Mariângela Guerreiro Milhoranza da (coord.). *Temas polêmicos de direito e processo do trabalho*: estudos em homenagem à professora Denise Fincato. Porto Alegre: Livraria do Advogado, 2018.

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 *et al*. (coord.). *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.

SILVA, Virgílio Afonso da. *A constitucionalização do direito*: os direitos fundamentais nas relações entre particulares. São Paulo: Malheiros, 2005.

SIMÓN, Sandra Lia. *A proteção constitucional da intimidade e da vida privada do empregado*. São Paulo: LTr, 2000.

SINGH, Ved Prakash; PAL, Preet. Survey of different types of CAPTCHA. *International Journal of Computer Science and Information Technologies*, v. 5, n. 2, p. 2242-5, 2014. Disponível em: https://pdfs.semanticscholar.org/4cb1/c8d9b8d7712779b3f2ab401586833a72db61.pdf. Acesso em: 24 jun. 2019.

SOUSA, Rosilene Paiva Marinho de; BARRANCOS, Jacqueline Echeverría; MAIA, Manuela Eugênio. Acesso à informação e ao tratamento de dados pessoais pelo Poder Público. *Informação & Sociedade*, v. 29, n. 1, 2019. Disponível em: https://search.proquest.com/openview/f40645edbedfbae2e4097746d036aeeb/1?pq-origsite=gscholar&cbl=2030753. Acesso em: 8 set. 2019.

SOUZA, Carlos Affonso Pereira de. Segurança e sigilo dos dados pessoais: primeiras impressões à luz da lei 13.709/2018. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019, p. 417-441.

SOUZA, Eduardo Nunes; SILVA, Rodrigo da Guia. Direitos do titular de dados pessoais na Lei 13.709/2019: uma abordagem sistemática. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019, p. 241-286.

STEINMETZ, Wilson Antônio. *Colisão de direitos fundamentais e princípio da proporcionalidade.* Porto Alegre: Livraria do Advogado, 2001.

STEINMETZ, Wilson Antônio. *A vinculação dos particulares a direitos fundamentais*. São Paulo: Malheiros. 2004.

TASSO, Fernando Antonio. Capítulo IV - Do tratamento de dados pessoais pelo poder público. *In:* MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coords.). *LGPD*: lei geral de proteção de dados comentada. São Paulo: Thomson Reuters Brasil, 2019, p. 245-285.

TAVARES, Ana Lucia de Lyra. O direito comparado na história do sistema jurídico brasileiro. *Revista de Ciência Política*, v. 33, n. 1, p. 56-90, 1990. Disponível em: http://bibliotecadigital.fgv.br/ojs/index.php/rcp/article/viewFile/59810/58140. Acesso em: 12 maio 2019.

TAVARES, Ana Lucia de Lyra. Contribuição do direito comparado às fontes do direito brasileiro. *Prisma Jurídico*, São Paulo, v. 5, p. 59-77, 2006. Disponível em: http://www.redalyc.org/pdf/934/93400504.pdf. Acesso em: 05 maio 2019.

TANÚS, Gustavo D. La protección de los datos personales de salud y la ley 25.326. *In:* PALAZZI, Pablo Andrés (coord.). *Derecho y nuevas tecnologias*. Buenos Aires: Ad-Hoc, 2003, p. 239-278.

TEIXEIRA FILHO, Manoel Antonio. *Curso de direito processual do trabalho, vol. I*: processo de conhecimento 1: compreendendo temas de teoria geral do processo. São Paulo: LTR, 2009.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. Consentimento e proteção de dados pessoais na LGPD. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019, p. 287-322.

THE NEW YORK TIMES. *How Trump Consultants Exploited the Facebook Data of Millions*. Nova York, 17 mar. 2018. Disponível em: https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=first-column-region. Acesso em: 1 fev. 2019.

TOURIÑO, Alejandro. *El derecho al olvido y a la intimidad en Internet*. Madrid: Catarata, 2014.

TREACY, Guillermo. La convergencia de criterios interpretativos en materia de derecho a la igualdad en el derecho internacional de los derechos humanos y el derecho interno argentino. *In:* CAPALDO, Griselda; SIECKMANN, Jan; CLÉRICO, Laura. *Internacionalización del derecho constitucional, constitucionalización del derecho internacional*. Buenos Aires: Eudeba, 2012, p. 271-286.

URUGUAI. *Lei nº 18.331 de 11 de agosto de 2008*. Protección de datos personales y acción de "Habeas Data". Disponível em: https://www.agesic.gub.uy/innovaportal/v/302/1/agesic/ley-n%C2%B0-18331-de-11-de-agosto-de-2008.html. Acesso em: 8 jun. 2018.

UNIÃO EUROPEIA. *Carta dos direitos fundamentais da União Europeia*. 2000. Disponível em: http://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 6 maio 2018.

UNIÃO EUROPEIA. *Tratado que estabelece uma Constituição para a Europa*. 2004. Disponível em: https://europa.eu/european-union/sites/europaeu/files/docs/body/treaty_establishing_a_constitution_for_europe_pt.pdf. Acesso em: 6 maio 2018.

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*. Disponível em: https://publications.europa.eu/pt/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-pt. Acesso em: 6 maio 2018.

VAINZOF, Rony. Dados pessoais, tratamento e princípios. *In:* MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coords.). *Comentários ao GDPR*: Regulamento geral de proteção de dados da União Europeia. São Paulo: Revista dos Tribunais, 2018, p. 37-83.

VAINZOF, Rony. Capítulo I – Disposições preliminares. *In:* MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coords.). *LGPD*: Lei geral de proteção de dados comentada. São Paulo: Revista dos Tribunais, 2019, p. 19-177.

VALE, André Rufino do. *Eficácia dos direitos fundamentais nas relações privadas*. Porto Alegre: Sergio Antonio Fabris, 2004.

VASCONCELOS, Beto; PAULA, Felipe de. A autoridade nacional de proteção de dados: origem, avanços e pontos críticos. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019, p. 717-739.

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

VILLALÓN, Jesús Cruz. *Protección de datos personales del trabajador en el proceso de contratación*: facultades y límites de la actuación del empleador. Sevilla: Editorial Bomarzo, 2019.

VIRILIO, Paul. *La velocidad de liberación*. Buenos Aires: Manantial, 1995.

XAVIER, Luciana Pedroso; XAVIER, Marília Pedroso; SPALER, Mayara Guibor. Primeiras impressões sobre o tratamento de dados pessoais nas hipóteses de interesse público e execução de contratos. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019, p. 485-503.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. *Harward LR*, Harward, v. 4, n. 5, p. 193-220, 1890. Disponível em: http://www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf. Acesso em: 24 abr. 2018.

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. Introdução aos fundamentos de uma teoria geral dos "novos" direitos. *In:* WOLKMER, Antonio Carlos; LEITE, José Rubens Morato. *Os "novos" direitos no Brasil*: natureza e perspectivas – uma visão básica das novas conflituosidades jurídicas. São Paulo: Saraiva, 2012, p. 15-48.

APÊNCIDES

APÊNDICE A – ANÁLISE DA LEGISLAÇÃO

Tabela 1 – Comparativo entre as leis de proteção de dados pessoais de Argentina e Brasil

COMPARATIVO ENTRE AS LEIS DE PROTEÇÃO DE DADOS PESSOAIS			
Categorias de análise	**Ley nº 25.326/2000 (Argentina)**	**Lei nº 13.709/2018 (Brasil)**	**Comentário**
1) Escopo de aplicação	- Material: Destina-se à proteção dados pessoais armazenados em arquivos, registros e bancos de dados públicos ou privados destinados a fornecer informações (artigo 1º). - Territorial: Lei é omissa quanto a esse quesito.	- Material: É aplicável a toda atividade que envolva a utilização de dados pessoais, seja por pessoa natural ou pessoa jurídica de direito público ou privado (artigo 3°, caput). - Territorial: Possui aplicação tanto para empresas sediadas no Brasil como para empresas que não possuam estabelecimento no país, desde que o tratamento seja realizado em território nacional (art. 3º, I), o tratamento tenha por finalidade a oferta de bens ou serviços ao mercado consumidor brasileiro ou o tratamento de dados de indivíduos localizados no país (artigo 3º, II), ou que os dados tenham sido coletados no território nacional (artigo 3º, III).	A legislação brasileira, por ser mais recente, incorpora o caráter extraterritorial presente no RGPD da União Europeia. O modelo apresentado pela Argentina mostra-se menos protetivo neste quesito, uma vez que não contempla os bancos de dados localizados fora do país.
2) Bases legais para o tratamento de dados	Além do consentimento, o inciso 2º do artigo 5º estabelece outras cinco hipóteses que autorizam o tratamento de dados pessoais, quais sejam: a) quando os dados forem obtidos de fontes de acesso público irrestrito; b) sua coleta for necessária para o exercício de funções próprias dos poderes do Estado ou em virtude de uma obrigação legal; c) os arquivos limitarem-se ao nome, documento de	Assim como ocorre na Argentina, a lei estabelece um rol de hipóteses (nove, no total) que, além do consentimento, autorizam o tratamento de dados pessoais (todas elas em seu artigo 7º). Destacam-se o cumprimento de obrigação legal pelo controlador (II); a execução de políticas públicas pela administração pública (III); o exercício regular de direitos em processo judicial, administrativo ou arbitral (VI); e quando necessário para atender aos	Estabelecendo-se um comparativo entre ambas as legislações, é possível observar que a lei brasileira apresenta um maior número de hipóteses autorizadoras do tratamento de dados pessoais sem o consentimento do titular, o que pode representar uma menor proteção ao cidadão em geral. As duas legislações, entretanto, apresentam dispositivos vagos e permitem o

	identidade, identificação tributária ou previdenciária, ocupação, data de nascimento e domicílio; d) derivem de uma relação contratual, científica ou profissional do proprietário dos dados e forem necessários para o seu desenvolvimento ou cumprimento; e) no caso de operações realizadas por instituições financeiras e as informações recebidas de seus clientes	interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (IX).	tratamento de dados pelo Poder Judiciário sem maiores restrições ou indicação de cuidados a serem tomados, seja a hipótese da lei argentina que permite o tratamento pela administração pública para o exercício das suas funções, seja a da lei brasileira que trata do exercício regular de direitos em processo judicial. Neste ponto, as leis equivalem-se em relação ao baixo nível protetivo dispensado aos dados pessoais dos jurisdicionados.
3) Tratamento de dados sensíveis	A lei, como regra geral, estabelece que nenhuma pessoa é obrigada a fornecer dados sensíveis (artigo 7º). Entretanto, estabelece duas exceções autorizadoras do tratamento: quando existirem de razões de interesse geral autorizadas por lei; e para finalidades estatísticas ou científicas, quando os seus titulares não puderem ser identificados (artigo 7º, inciso 2º). Alguns autores, como Delpech (2003, p. 154) entendem que nem mesmo o consentimento expresso autoriza o tratamento e a formação de arquivos, bancos e registros de dados sensíveis nos casos não relacionados pela normativa, já que não há a previsão legal do consentimento como uma das exceções elencadas no rol taxativo.	A lei estabelece um rol de hipóteses que autorizam o tratamento de dados sensíveis, ainda que sem o consentimento do titular (artigo 11, II). O dispositivo repete grande parte dos itens do artigo 7°, excluindo algumas situações, como é o caso do interesse legítimo do controlador ou de terceiro. Permite, por exemplo, o tratamento de dados sensíveis em casos que envolvam o exercício regular de direitos em processo judicial, administrativo ou arbitral.	A lei brasileira mostra-se menos protetiva em relação aos dados sensíveis, ao ampliar abusivamente o espaço para tratamento dessas informações. Ambas as leis merecem críticas pela generalidade das cláusulas, deixando espaço para interpretações amplas e perdendo a oportunidade de delimitação quanto aos deveres específicos dos agentes responsáveis pelo tratamento de dados sensíveis, especialmente no âmbito do Poder Judiciário.
4) Direitos dos titulares dos dados	Estão previstos no Capítulo III da lei, que contempla os direitos de informação	A lei estabelece uma ampla gama de direitos aos titulares, dos quais	A LGPD brasileira mostra-se mais adequada às novas exigências de uma

	(artigo 13), acesso (artigo 14), e retificação, atualização ou supressão (artigo 16). Além disso, o artigo 11, inciso 2, garante ao titular dos dados o direito à revogação do consentimento.	destacam-se os direitos de acesso (II), correção (III), anonimização, bloqueio e eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a lei (IV), portabilidade (V), informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados (VII), bem como o direito de revogação do consentimento (IX), todos eles no artigo 18.	sociedade em rede, altamente informatizada e em constante transformação, contemplando algumas inovações inspiradas pelo RGPD da União Europeia, tais como o direito à portabilidade de dados. Do ponto de vista das garantias oferecidas ao reclamante para a tutela de seus dados em face do uso abusivo pelo Poder Judiciário, ambas as leis demonstram possuir uma cartela satisfatória de direitos, cabendo o seu efetivo implemento e fiscalização pela respectiva autoridade fiscalizatória.
5) Princípios de proteção dos dados	Os princípios de proteção de dados foram incorporados pela lei 25.326/2000 em seu Capítulo II. Gustavo Tanús (2003, p. 247-253), doutrinador argentino, classifica tais princípios em: princípio da pertinência ou princípio da proporcionalidade e qualidade dos dados (artigo 4º, inciso 1º), princípio da finalidade (artigo 3º, parágrafo 2º), princípio da utilização não abusiva (art. 4º, inciso 3º), princípio da exatidão (artigo 4º, incisos 4º e 5º), princípio do direito ao esquecimento ou princípio da limitação no tempo (artigo 4º, inciso 7º), princípio da legalidade ou princípio da limitação da coleta (artigo 4º, inciso 2º), princípio da segurança (artigo 9º, inciso 2º) e princípio do consentimento (artigo 5º).	A LGPD elenca, em seu artigo 6°, dez princípios, que deverão ser guiados pela boa-fé enquanto máxima de conduta: finalidade, adequação, necessidade, livre acesso, qualidade, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas.	Ambas as legislações sofrem influência do arcabouço de princípios delineados pelas normativas da União Europeia. Consistem em legislações com forte conteúdo principiológico, com adequado nível protetivo nesse aspecto.

6) Órgão regulador de proteção de dados	O artigo 29 da Lei nº 25.326/2000 estabelece, de forma pioneira na América Latina, a criação de um órgão de controle responsável pelas ações necessárias ao cumprimento da lei, tais como o assessoramento das pessoas acerca dos meios disponíveis para a proteção de seus dados pessoais, a criação de normas e regulamentações visando o desenvolvimento das atividades compreendidas pela lei, o controle da observância das normas de integridade e segurança dos dados por parte dos arquivos, registros ou bancos de dados e a imposição de sanções administrativas no caso de violações à lei, dentre outros. A autoridade opera no âmbito da Secretaria de Assuntos Registrais, vinculada ao Ministério da Justiça e Direitos Humanos.	A Autoridade Nacional de Proteção de Dados (ANPD), instituída pelo artigo 55-A da lei, é um órgão da administração pública federal, integrante da Presidência da República. Dentre suas principais atribuições estão: zelar pela aplicação da lei, fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação e editar regulamentos e procedimentos acerca da proteção de dados pessoais e privacidade.	A efetividade de uma política nacional de proteção de dados pessoais passa pela existência de uma autoridade independente, responsável pela fiscalização e pelo controle do atendimento das exigências legais junto aos órgãos responsáveis pelo tratamento de dados. Ao estabelecerem a vinculação destes órgãos ao Poder Executivo, Brasil e Argentina impõe barreiras à sua autonomia e liberdade de fiscalização, especialmente com relação ao tratamento de dados pelo Poder Público, afastando-se do modelo de sucesso do RGPD da União Europeia.
7) Tratamento de dados pelo Poder Público.	A lei não apresenta regramento específico disciplinando o tratamento de dados quando os responsáveis são os próprios órgãos estatais, especialmente no caso da cessão de dados a terceiros. O artigo 22, que aborda os arquivos, registros ou bancos de dados públicos, limita-se a exigir que as normas envolvendo a criação, modificação ou supressão de arquivos ou bancos de dados pertencentes a organismos públicos sejam precedidas da publicação de disposição geral no Boletim Oficial da Nação	Apesar de contar com um capítulo voltado ao tratamento de dados pelo Poder Público (capítulo IV), não há na lei um dispositivo específico relacionado à divulgação de dados que integram os processos judiciais. O artigo 23, I, da LGPD indica que as entidades públicas deverão informar as hipóteses de tratamento de dados, incluindo as finalidades (vinculadas à persecução do interesse público), procedimentos e práticas utilizadas para a execução dessas atividades, preferencialmente pela Internet Além disso, o	A lei brasileira disciplina de maneira mais abrangente o tratamento de dados pelo Poder Público em relação à normativa da Argentina. Ambas, entretanto, são insuficientes para garantir a proteção dos dados pessoais dos jurisdicionados, na medida em que falham em não estabelecer regras específicas para o tratamento e o repasse de informações processuais (no caso da lei brasileira, esses dados acabam sendo abarcados pela exceção que permite a transferência a entidades privadas de

	ou em diário oficial. Quando for o caso da supressão de registros informatizados, deverão ser informados a destinação dos arquivos ou as medidas adotadas para a sua destruição, conforme o inciso 3º.	parágrafo 1° do artigo 26 proíbe o Poder Público de transferir para entidades privadas os dados pessoais existentes em bases de dados a que tenha acesso, excetuando, no inciso III, os casos em que os dados forem acessíveis publicamente. Obs. Necessária a aplicação conjunta da Lei de Acesso à Informação.	dados acessíveis publicamente).

Fonte: elaborado pelo autor a partir de Argentina (2000) e Brasil (2018a).

APÊNDICE B – OBSERVAÇÃO DOS PORTAIS DOS TRIBUNAIS TRABALHISTAS

Tabela 2 – Comparativo entre os portais das Cortes Superiores do Poder Judiciário trabalhista de Argentina e Brasil

	ARGENTINA	**BRASIL**
Data da observação	02/02/2019	26/06/2019
Órgão analisado	Cámara Nacional de Apelaciones del Trabajo	Tribunal Superior do Trabalho
Link do site analisado	www.pjn.gov.ar	www.tst.jus.br
1) Possibilidade de pesquisa pelo nome do reclamante	Sim. Tanto na consulta processual quanto na jurisprudencial.	Parcialmente. A consulta processual não pode ser realizada através do nome do reclamante, mas a pesquisa jurisprudencial sim.
2) Adoção de solução de *captcha* para consultas públicas em processos, acórdãos e jurisprudências	Parcialmente. Somente a consulta processual adota a solução *captcha*, a pesquisa jurisprudencial não.	Não. A solução não é utilizada nem na consulta processual e nem na jurisprudencial.
3) Divulgação de dados sensíveis por meio da pesquisa jurisprudencial	Sim.	Sim.
Comentários	O *site* do Poder Judicial de la Nación mostra-se o mais transparente com relação à divulgação de informações processuais, possuindo um sistema de consulta de expedientes que permite a pesquisa pelo nome das partes. Por consequência, não apresenta um nível adequado de proteção aos dados pessoais do trabalhador.	Apesar de não adotar a solução de *captcha* sugerida pela Resolução CSJT nº 139/2014, o que o torna mais vulnerável à coleta automatizada de dados, o *site* do TST não permite a consulta processual pelo nome do reclamante, conforme determina a Resolução nº 121 do Conselho Nacional de Justiça. Ainda assim, o tribunal permite a pesquisa processual pelo nome do empregador, o que pode facilitar o acesso a informações de seus ex-funcionários. Somado a isso, a consulta jurisprudencial pode ser realizada por meio do nome de qualquer das partes, o que acaba revelando os dados sensíveis do trabalhador.

Fonte: elaborado pelo autor a partir de Argentina (2019a) e Brasil (2019c).

APÊNDICE C – PESQUISA JURISPRUDENCIAL - DIVULGAÇÃO DE DADOS PESSOAIS

Tabela 3 – Comparativo entre os portais das Cortes Superiores do Poder Judiciário trabalhista de Argentina e Brasil, com relação à divulgação de dados pessoais do trabalhador por meio da consulta jurisprudencial

	ARGENTINA	**BRASIL**
Data da observação	01/07/2019	07/07/2019
Órgão analisado	Cámara Nacional de Apelaciones del Trabajo	Tribunal Superior do Trabalho
Link do site analisado	www.pjn.gov.ar	www.tst.jus.br
Palavras-chave utilizadas	"despido discriminatorio"	"despedida discriminatória"
Período de abrangência da pesquisa	27/04/2016 a 27/04/2019	27/04/2016 a 27/04/2019 (data de publicação)
Processos físicos e/ou eletrônicos?	Não disponibiliza esta opção	Somente eletrônicos
Acórdãos e/ou decisões monocráticas?	Não disponibiliza esta opção	Somente acórdãos
Parâmetros de busca	- Frase exata	- Contendo as palavras (e); - Documentos: acórdãos - Órgão judicante: todas as Turmas; - Classe processual: Recursos de Revista; - Indicador: Tramitação eletrônica.
Total de resultados encontrados	43 resultados	42 resultados
Número de resultados repetidos	18 resultados	0 resultados
Total de julgados diferentes encontrados	25 resultados	42 resultados
Julgados com divulgação do nome completo do trabalhador	14 resultados	42 resultados
Total de julgados com divulgação de dados sensíveis[113]	21 resultados	27 resultados
Número percentual dos julgados em que houve divulgação de dados sensíveis	84%	64,28%
Julgados com divulgação de dados sobre origem racial ou étnica	1 resultado	0 resultados
Julgados com divulgação de dados sobre convicção religiosa	0 resultados	0 resultados
Julgados com divulgação de dados sobre opinião política	1 resultado	1 resultado
Julgados com divulgação de dados sobre filiação	4 resultados	1 resultado

[113] Com base nas categorias de dados sensíveis elencadas pelo artigo 5º, II da Lei nº 13.709/2018 (BRASIL, 2018a).

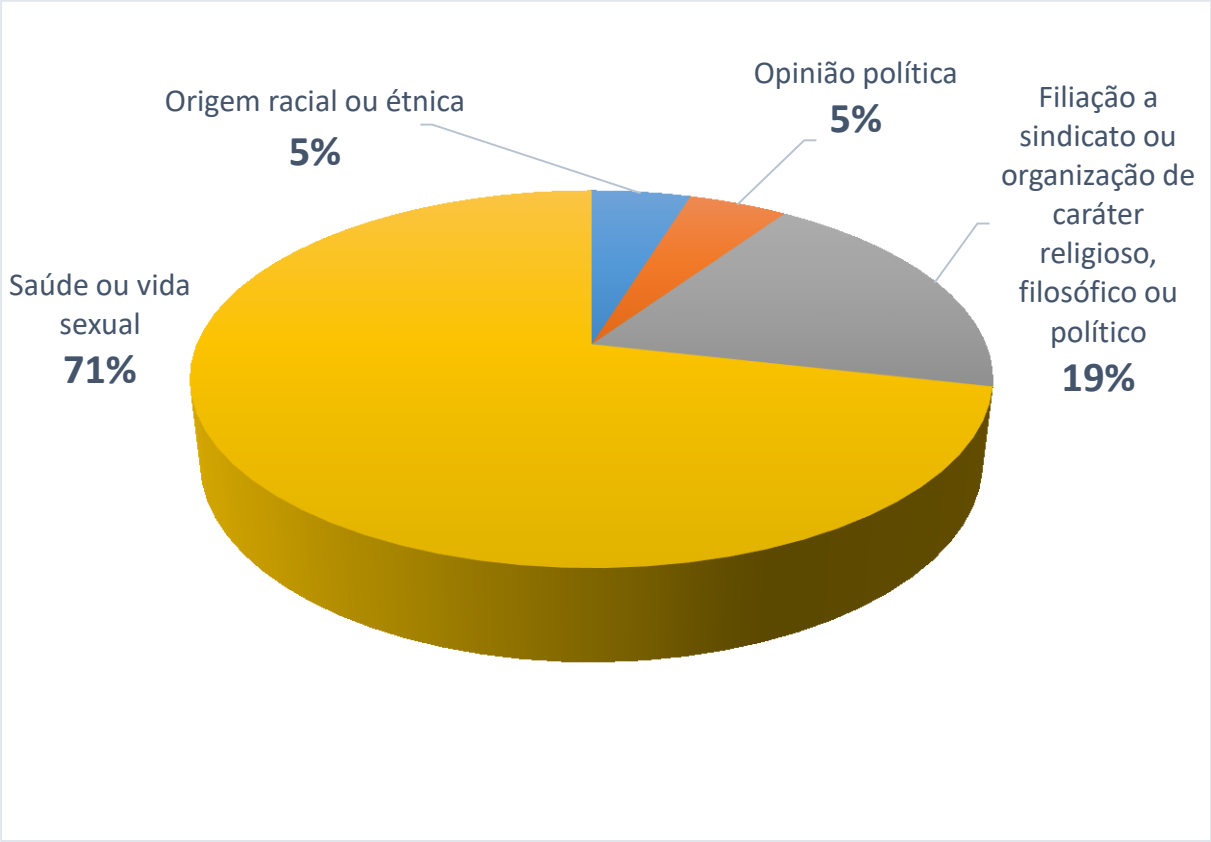
a sindicato ou a organização de caráter religioso, filosófico ou político		
Julgados com divulgação de dados referentes à saúde ou à vida sexual	15 resultados* *Deste resultado, 2 julgados continham dados relacionados ao estado de gravidez da trabalhadora.	25 resultados* *Deste resultado, 4 julgados continham dados relacionados ao estado de gravidez da trabalhadora.
Julgados com divulgação de dados genéticos ou biométricos	0 resultados	0 resultados
O julgado é disponibilizado na íntegra?	Não. Somente a ementa é disponibilizada.	Sim. Disponibiliza o acórdão na íntegra.
Há a disponibilização de dados pessoais de terceiros?	Sim	Sim
Comentários	O baixo número de julgados diferentes encontrados e a ausência de resultados após o ano de 2017 evidencia que o sistema encontra-se em desuso. Diante do predomínio das ações envolvendo o pedido de reintegração do empregado despedido em função de doença ou gravidez, dados relacionados à saúde do trabalhador foram os mais encontrados na busca realizada. Ressalta-se que em mais da metade dos julgados houve a divulgação do nome completo do trabalhador, enquanto no restante (44% do total, excluídas as repetições) somente as iniciais foram disponibilizadas. Não foram encontradas justificativas aparentes para que essa diferenciação tenha ocorrido, pois julgados de matéria similar encontram tratamentos diferentes, e não há a indicação de segredo de justiça.	Assim como na Argentina, a pesquisa indicou a maioria absoluta de julgados contendo dados relacionados à saúde do trabalhador. Ainda que apresente um menor índice de julgados com a divulgação de dados sensíveis em relação ao país vizinho na busca realizada, o Tribunal brasileiro realizou a divulgação do nome completo do trabalhador em todos os resultados encontrados, tornando-se menos protetivo ao trabalhador neste ponto.
Avaliação de pesquisa jurisprudencial	Pontos positivos: - Não realiza a divulgação dos julgados na íntegra, somente a ementa; - Em alguns casos, não divulga o nome completo do trabalhador, somente as iniciais.	Pontos positivos: - Sistema de busca mais moderno e melhor formatado em relação ao argentino, apresenta grande número de parâmetros de pesquisa e não indica resultados em repetição, constatações que são positivas do

	Pontos negativos: - Sistema defasado, não disponibiliza opções refinadas de busca. Acaba se tornando mais protetivo em virtude de sua precariedade, e não por uma política do Tribunal. - Apresenta grande número de resultados repetidos.	ponto de vista da eficiência do Poder Judiciário, mas não revertem em ganhos à privacidade do jurisdicionado. - Com relação às buscas realizadas, demonstrou uma menor porcentagem de julgados em que houve a divulgação de dados sensíveis em relação ao Tribunal da Argentina, ainda que isso não seja decorrente de uma política de não divulgação do Tribunal. Pontos negativos: - Falha ao priorizar a ampla publicidade na divulgação de informações processuais em detrimento da privacidade do jurisdicionado, publicando os acórdãos na íntegra e revelando os nomes dos reclamantes em todos eles.

Fonte: elaborado pelo autor a partir de Argentina (2019a) e Brasil (2019c).

APÊNDICE D – CATEGORIAS DE DADOS SENSÍVEIS ENCONTRADAS NA PESQUISA JURISPRUDENCIAL (POR PERCENTUAL) – CÁMARA NACIONAL DE APELACIONES DEL TRABAJO (ARGENTINA)

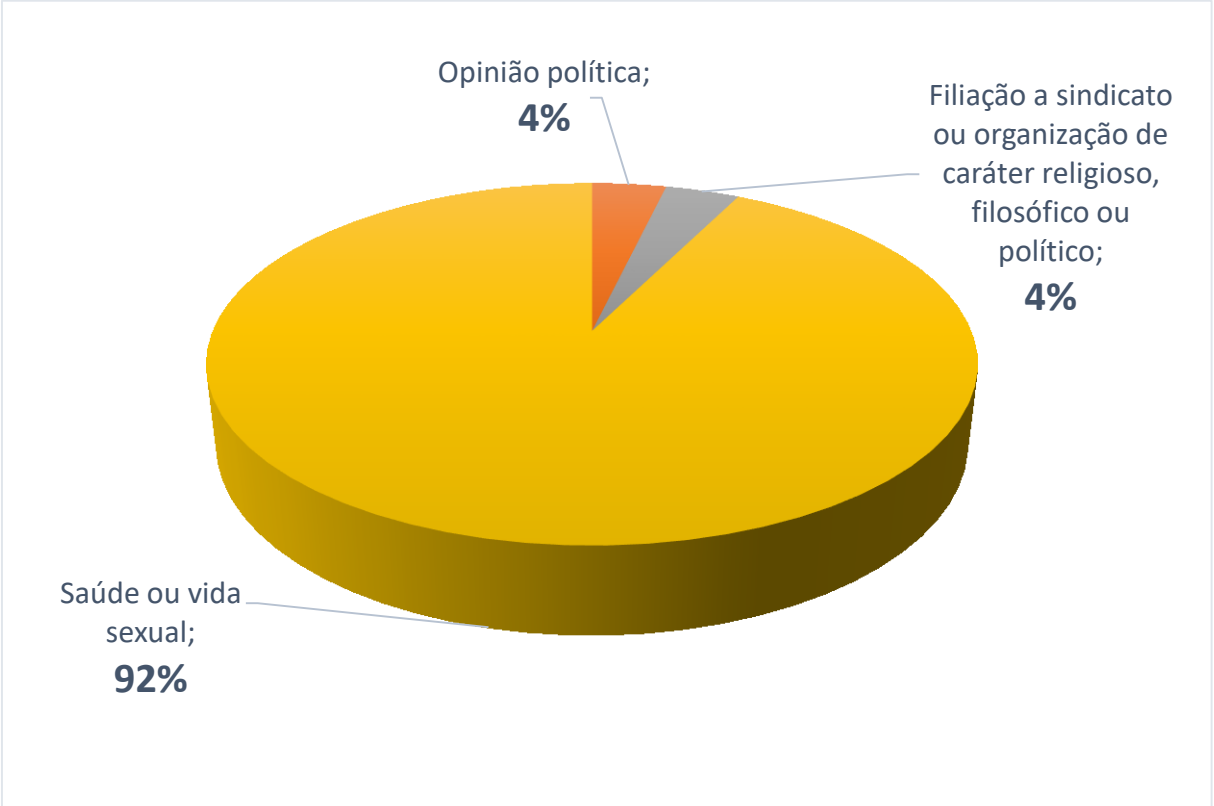
Gráfico 1 – Categorias de dados sensíveis – pesquisa jurisprudencial realizada na Cámara Nacional de Apelaciones del Trabajo (Argentina)



Fonte: elaborado pelo autor a partir de Argentina (2019a).

APÊNDICE E – CATEGORIAS DE DADOS SENSÍVEIS ENCONTRADAS NA PESQUISA JURISPRUDENCIAL (POR PERCENTUAL) – TRIBUNAL SUPERIOR DO TRABALHO (BRASIL)

Gráfico 2 – Categorias de dados sensíveis – pesquisa jurisprudencial realizada no Tribunal Superior do Trabalho (Brasil)



Fonte: elaborado pelo autor a partir de Brasil (2019c).

APÊNDICE F – OBSERVAÇÃO DO *SITE* "ESCAVADOR"

Tabela 4 – Análise do *site* "Escavador" (www.escavador.com)

FUNCIONALIDADE	OBSERVAÇÃO
Consulta por Pessoas, Empresas, Diários Oficiais ou Partes em processos	Aponta como resultados todos os processos indexados ao termo buscado, com indicação de nomes das partes, advogados, número do processo e movimentações, que são organizadas por data, oferecendo acesso direto às notas de expedientes publicadas nos Diários Oficiais.
Consulta de jurisprudência	Vasculha os bancos de dados dos Tribunais Superiores, através da opção de filtragem por tribunal (TST, STJ ou STF), Estado de origem do processo, tipo de documento, relator, órgão julgador, classe do recurso/ação, distância entre termos e data de julgamento. A pesquisa pela palavra-chave "despedida discriminatória" não obteve resultados encontrados, ao contrário da pesquisa diretamente no portal do Tribunal Superior do Trabalho, o que evidencia que o motor de busca apresenta problemas de funcionamento.
Compartilhamento	Permite o compartilhamento nas redes sociais (*Facebook*, *Twitter* e *Google Plus*) das informações de cada processo ou de todos os resultados indexados a uma pessoa determinada (incluindo um resumo de seu histórico).
Monitoramento	Possibilita ao usuário cadastrar-se para receber atualizações futuras, sendo informado acerca de qualquer nova movimentação ou atualização de processo, nome de pessoa ou empresa, através do acompanhamento de Diários Oficiais de todo o Brasil.
Remover informações	Faculta ao titular dos dados a remoção de conteúdo determinado, bastando o envio de um documento que confirme sua identidade. A opção é selecionável tanto na tela que apresenta os resultados gerais da busca relacionada a uma pessoa, contendo os resultados indexados ao seu nome, como na tela relativa a um processo em específico.

Fonte: elaborado pelo autor a partir de Escavador (2019).