

ESTUDIOS

A Lei Geral de Proteção de Dados Pessoais como proteção dos direitos da personalidade do docente: O tratamento de dados pessoais pelas instituições de ensino superior na avaliação do INEP

The General Personal Data Protection Law as protection of teacher's personality rights: the processing of personal data by higher education institutions in the INEP evaluation

Marcelo Negri Soares 

Wellington Junior Jorge 

Universidade Cesumar, Brasil

José Joaquim Pereira Melo 

Universidade Estadual de Maringá, Brasil

RESUMO O presente trabalho tem como premissa discutir a Lei Geral de Proteção de Dados Pessoais no que tange ao vazamento de dados por parte das instituições de ensino superior em relação ao procurador institucional, bem como os coordenadores e avaliadores, analisando o ordenamento jurídico considerando a Lei Geral de Proteção de Dados Pessoais e os direitos da personalidade. O problema da pesquisa é: qual a responsabilidade das instituições de ensino superior sobre a disponibilização dos dados pessoais dos docentes na avaliação da INEP? Considerou-se que o uso indiscriminado por parte dos avaliadores pode gerar várias consequências para o titular dos dados, como a violação dos seus direitos da personalidade. O método utilizado é o interpretativo racional, buscando entender a razão da norma e sua aplicação na temática, e o indutivo, considerando a observação de questões particulares que permitem conclusões gerais. De fato, essa lei é um marco para a sociedade moderna, porém muitas questões ainda precisam ser pesadas, considerando o compartilhamento de dados com terceiros e como o titular pode ser prejudicado com tal ação.

PALAVRAS-CHAVE Avaliação institucional, ensino superior, Lei Geral de Proteção de Dados Pessoais, INEP.

ABSTRACT The premise of this work is to discuss the General Personal Data Protection Law regarding data leakage by colleges about the institutional attorney, as well as coordinators and evaluators, analyzing the legal system considering the General Personal Data Protection Law and personality rights. The research problem is: what is the responsibility of colleges for making the personal data of teachers available in the INEP evaluation? It was considered that indiscriminate use by evaluators could generate several consequences for the data subject, such as the violation of their personality rights. The method used is rational interpretative, seeking to understand the reason for the standard and its application to the topic, and inductive, considering the observation of particular issues that allow general conclusions. This law is a milestone for modern society, however, many issues still need to be weighed, considering the sharing of data with third parties and how the data subject can be harmed by such action.

KEYWORDS Institutional evaluation, higher education, General Personal Data Protection Law, INEP.

Introdução

A rede mundial de computadores conecta o indivíduo com o mundo todo, além de empresas e instituições, sendo um espaço moderno de vida, onde é possível trabalhar, estudar, comprar, vender e conhecer outras pessoas por meio das redes sociais. Englobando inúmeras situações do cotidiano e estruturando uma nova interação social, a era da informação consolida a sociedade digital e a busca obter dados e informações de cada indivíduo que está presente em rede. Neste contexto, o ser humano se sente, muitas vezes, na obrigação de estar conectado a todo momento. Pensando nisso, empresas de tecnologia têm disponibilizado dados móveis para cada *smartphone* ou outro equipamento adequado que esteja conectado à internet, em muitos casos, sem qualquer custo direto, apesar da existência de custos indiretos.

É preciso compreender que por trás do que acontece na internet (de forma oculta, não explícita ou transparente) existem muitos interesses negociais e empresariais que se valem do que circula em rede para monetizar o que é apregoado como gratuito. Na prática, os dados que a pessoa entrega de forma voluntária, inadvertidamente ou, ainda, sendo enganada ilicitamente (tendo violada a sua privacidade), normalmente seguem dois destinos: vão para a circulação pública, podendo inclusive ser alvo de ilícitos criminais, ou seguem para os agentes do mercado, que os utilizam para fins de assédio indevido ao usuário, com vistas à prática de relações de consumo, o que não deixa de ser um ilícito civil.

De fato, a tecnologia digital permitiu ao usuário participar por meio das redes sociais de um universo antes impensado, além de poder contatar e transmitir para qualquer parte do planeta mensagens dos mais variados tipos. Os avanços no acesso à informação também têm alterado a maneira com que as pessoas se comportam nas

redes. Afinal, basta estar conectado para se ter acesso e adquirir comida, bebida, entretenimento, bem como pagar contas, conversar com a família por chamada e videoconferência. As interações com pessoas e coisas estão cada vez mais rápidas e intuitivas.

Diante desta perspectiva, a internet é um meio de comunicação em sentido horizontal, onde as pessoas, independentemente do *status* ou da classe social a que pertencem, em princípio podem acessar os mais diversos conteúdos, desde que tenham condições técnicas para tanto, configurada por aparelhos e com a conexão adequada. Vale ressaltar, entretanto, que conteúdo nem sempre é informação; que nem sempre é conhecimento; que nem sempre é sabedoria, mas que, atualmente, tal cenário exerce indubitavelmente uma espécie de magnetismo sobre as pessoas, envolvendo desde necessidades, como ter acesso a serviços públicos,¹ até futilidades, razão pela qual a interação entre as pessoas e o computador fez com que o comportamento destas restasse alterado de acordo com as novas possibilidades.

Assim, emergiu a preocupação quanto à existência de uma legislação específica para reger essa área, principalmente no que tange à questão do tratamento dos dados pessoais, o que ocorreu no Brasil com a Lei 13.709/18, a Lei Geral de Proteção de Dados Pessoais, norma que alterou substancialmente o marco civil da internet na Lei 12.965 de 2014. Surgiu para dar garantias e maior segurança na forma de como são tratados os dados, seja pelas empresas ou por particulares (por exemplo, profissionais liberais). Efetivou-se, então, uma padronização de normas e práticas, que promoveu a proteção de dados pessoais de maneira igualitária, sem olvidar outras garantias legais atinentes a direitos fundamentais e da personalidade.

Desta forma, a Lei Geral de Proteção de Dados Pessoais trouxe mudanças que não ficaram restritas apenas à atuação *online* de empresas e atingiram suas práticas *offline*. É o que ocorre com as instituições de ensino superior, as quais, no tocante à manipulação dos dados pessoais de seus docentes, serão objeto do presente trabalho, em quanto a forma como coletam, tratam e armazenam os dados deve ser pautada nas normativas existentes, com mais transparência em relação ao docente e às autoridades com poder de fiscalização, tudo a demonstrar que a lei em questão está sendo cumprida integralmente, seja nas atividades cotidianas relacionadas com sua esfera de ensino ou na área administrativa, seja no que se refere a terceiros (agentes de mercado, agentes reguladores como o Ministério da Educação, etcétera).

1. «A pesquisa do Comitê Gestor da Internet no Brasil (CGI.br) mostrou que, em 2021, 76% das organizações federais dos poderes executivo, legislativo, judiciário e do Ministério Público ofereceram pela internet os serviços públicos mais procurados pelos cidadãos, um aumento de vinte e dois pontos percentuais na comparação com 2019, período que antecedeu a crise sanitária provocada pela covid-19». Em «Prestação de serviços online por organizações públicas dá salto durante a pandemia, mostra 5.ª edição da TIC Governo Eletrônico», *Comitê Gestor da Internet do Brasil*, 26 de julho de 2022, disponível em <https://tipg.link/Mxqt>.

Dentro do campo educacional, a atuação da Lei Geral de Proteção de Dados Pessoais também precisa de uma atenção especial, pois, afinal, observa-se que as instituições de ensino superior obtêm a coleta de dados dos docentes desde a seleção para contratação, sendo que elas têm acesso a dados como o estado civil, a filiação (e o número de filhos) e o currículo (junto com as publicações e cursos realizados pelo participante). Na entrevista possuem liberdade para fazer perguntas a respeito da religião, da filiação em sindicato, da existência de outros familiares que também trabalham na instituições de ensino superior, das preferências individuais ligadas a aspectos culturais (por exemplo o hábito de leitura) e estilo musical, *hobbies*, etcétera. Igualmente, podem solicitar exame médico admissional e terem acesso a informações que indiquem se o candidato tem alguma patologia ou sinal de que possa vir a ter; ou seja, uma infinidade de informação que é considerada juridicamente dados pessoais (muitos deles, sensíveis).

Considerando a amplitude e a complexidade da Lei Geral de Proteção de Dados Pessoais, como foco central, refere-se neste trabalho a seguinte situação-problema: quais as consequências, em especial, os impactos que podem decorrer da disponibilização e da manipulação dos dados pessoais dos docentes quando das avaliações do Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira, uma vez que as instituições de ensino superior possuem esses dados e os disponibilizam para os avaliadores por meio de compartilhamento em nuvem? Trata-se de uma situação de risco diante da possibilidade de uso indiscriminado ou indevido, caracterizando ilicitude por parte das instituições de ensino superior ou de terceiros detentores desses dados, gerando consequências gravosas para o proprietário dos dados, embora sejam necessários estudos posteriores sobre o tema, considerando seu ineditismo.

Diante dos critérios de avaliação e dos indicadores, muito embora a instituições de ensino superior necessite divulgar esses dados e seja imprescindível o seu compartilhamento, o tratamento deles deve estar adequado aos preceitos constitucionais e da legislação específica. Por isso, tendo em vista um impacto direto ao docente (vulnerável) caso seus dados sejam indevidamente manipulados e expostos, é necessário um olhar atento quanto a tais exigências, diante da eventual exposição sem um protocolo adequado para evitar danos à pessoa e seus direitos da personalidade (privacidade, intimidade, dignidade humana, livre desenvolvimento da personalidade, dentre outros).

No que concerne à justificativa deste trabalho, esta se faz diante da existência de possíveis implicações com a publicação dos dados pessoais dos docentes nos processos de avaliação do Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (INEP). Assim, o presente trabalho tem como objetivo geral identificar como ocorre a manipulação da publicação dos dados pessoais dos docentes nas avaliações do INEP. Como objetivos específicos, considera-se importante distinguir a importância do trabalho docente na avaliação do INEP e examinar a necessidade

de correta aplicação da Lei Geral de Proteção de Dados Pessoais no tocante à coleta, à manipulação e à exposição dos dados dos docentes, bem como os reflexos no que concerne à responsabilidade civil em caso de coleta ou manipulação em desconformidade com a legislação.

A pesquisa tem como parâmetro permanente os direitos fundamentais e da personalidade, os quais podem ser violados diante deste cenário. A metodologia científica utilizada será a bibliográfica, bem como o método indutivo, que diante do percurso que será traçado na pesquisa possibilita uma análise acerca do tratamento de dados pelas instituições de ensino, permitindo, assim, conclusões gerais ou universais, referente aos eventuais impactos devido à possibilidade de uso indiscriminado. A partir, por exemplo, da divulgação dos dados dos docentes pelas instituições de ensino superior privadas com o uso indevido destes, os coordenadores, o procurador institucional e os avaliadores passam a ter acesso a tais informações, podendo gerar implicações nos direitos da personalidade, especificamente quanto à privacidade. Por isso, propõem-se a criação de um programa de *compliance* efetivo, que tenha condições de criar medidas internas para prevenir e minimizar riscos decorrentes da violação dos dados.

A Lei Geral de Proteção de Dados Pessoais no Brasil

A Lei 13.709/2018, promulgada em 14 de agosto de 2018 e com vigência a partir de 1 de agosto de 2021, passou a ser conhecida como Lei Geral de Proteção de Dados Pessoais, que tem como premissa dar um caráter legal à proteção de dados, sejam eles físicos ou do contexto *online*, objetivando a proteção destes e dos direitos e liberdades tanto das pessoas naturais quanto das jurídicas, podendo ainda ser de direito público ou privado, conforme descrito nos artigos primeiro e terceiro da referida lei (Garcia, 2020). A legislação estabeleceu, no Brasil, a Autoridade Nacional de Proteção de Dados, que será o órgão responsável pela fiscalização do inteiro cumprimento desta, conforme artigo quinto, inciso XIX, da Lei Geral de Proteção de Dados Pessoais.²

Cabe destacar que a Lei Geral de Proteção de Dados Pessoais visa proteger a privacidade dos dados de seus titulares, possibilitando que as empresas que detenham essas informações garantam o seu tratamento. Desta forma, entende-se que os dados pessoais são informações que possam identificar o sujeito, não se resumindo ao nome, mas a quaisquer dados que, ao serem cruzados, possibilitem a identificação, além de outras informações mais sensíveis, que determinem o sujeito por sua raça

2. «Artigo quinto. Para os fins desta lei, considera-se: XIX autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta lei em todo o território nacional». Lei 13.709, de 14 de agosto de 2018, disponível em <https://tipg.link/Mxyg>.

ou etnia, crenças religiosas, ideologias políticas, filosóficas, condição de saúde, vida sexual e dados genéticos ou biométricos (Galera, 2021).

Entretanto, cabe destacar que a Lei Geral de Proteção de Dados Pessoais não é a única a tratar sobre o tema. Exemplo disso é o Código de Defesa do Consumidor (Lei 8.078/1990), a Lei de Acesso à Informação (Lei 12.527/2011), o *habeas data* (artigo quinto, inciso LXXII, da Constituição Federal de 1988), o decreto do comércio eletrônico (decreto 7.962/2013), a Lei Carolina Dieckmann (Lei 12.373/2012) e o Pacote Anticrime (Lei 13.964/2019). Porém, o destaque a ser dado à Lei Geral de Proteção de Dados Pessoais no desenvolvimento deste trabalho é por ser uma lei específica quanto à coleta, o armazenamento, o compartilhamento e a exclusão de dados pessoais (Teixeira, 2021).

A referida legislação é um grande marco no que tange ao tratamento de dados, considerando que estes são algo valioso para quem os possui. Destaca-se que a lei traz dois tipos de dados, os pessoais e os sensíveis, conforme transcrito no artigo quinto, entendendo-se o primeiro a pessoa natural que venha ser possível identificar ou que seja identificável, enquanto o segundo envolve questões referentes à formação racial ou étnica, social, econômica e cultural, além de dados relacionados à saúde, à genética, à biométrica, ou seja, dados que de alguma forma estão vinculados à pessoa (Pinheiro, 2020).

Portanto, a partir do momento em que esses dados são preservados, dificultando assim a identificação, a pessoa física tem mais segurança; afinal, outras pessoas, sejam elas físicas ou jurídicas, terão maior dificuldade para utilizar esses dados e agir em forma indiscriminada. O mesmo ocorre com a preservação dos dados sensíveis, tendo em vista que assim é possível evitar perseguições por questões raciais, religiosas, políticas, bem como o mapeamento de genoma, de dados biométricos, da orientação sexual, dos dados sobre saúde, dentre outros (Burkart, 2021).

Quando se fala em Lei Geral de Proteção de Dados Pessoais, é necessário observar os princípios norteadores da referida lei, pois não basta armazenar os dados, mas sim protegê-los, conforme exposto no artigo sexto.³ Sendo assim, há todo um trabalho a

3. «Artigo sexto. As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; VI transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis

ser desenvolvido ao se receber esses dados, armazená-los e excluí-los, não podendo ser feito de qualquer forma, devendo seguir todo um tratamento, de acordo com as normativas presentes na lei (Galera, 2021).

Nesse contexto, o «tratamento» presente na legislação faz referência à operação realizada com dados pessoais, considerando todo o processo. O artigo sétimo estabelece em quais hipóteses esses dados poderão ser coletados; veja-se que se trata de um rol taxativo, uma vez que a legislação utiliza os termos «somente poderá». Assim, destaca-se, para efeitos desta lei, que o tratamento dos dados precisará ser feito mediante o consentimento do titular, com o cumprimento de obrigações pela administração pública, os órgãos de pesquisa, a execução de contrato, o exercício regular do direito, a proteção à vida, a tutela da saúde e dos interesses legítimos do controlador ou de terceiro e para a proteção do crédito (Pinheiro, 2020).

Serão delimitados, entre outros, os atores citados no artigo quinto da lei, apresentando-se neste contexto o controlador, que poderá ser tanto uma pessoa física quanto jurídica, e será o responsável por todas as decisões ligadas aos dados coletados. Também haverá o operador, pessoa física ou jurídica que realizará o tratamento dos dados em nome do controlador. Há, ainda, o encarregado de dados, que realizará os trâmites entre o controlador, os titulares e a Autoridade Nacional de Proteção de Dados. Por fim, o titular, poderá a qualquer momento solicitar quais dados a empresa detém, o porquê e, a depender, a exclusão destes dos arquivos da empresa (Galera, 2021).

A divisão de tarefas e a documentação realizada no procedimento serão essenciais caso haja algum vazamento de dados, tanto para demonstrar a boa-fé quanto para, em caso de condenação, separar a responsabilidade de cada setor, conforme o artigo quinto da Lei Geral de Proteção de Dados Pessoais em seus incisos VI, VII, VIII e IX, que deixam claro a função de cada um sobre o tratamento de dados (Pinheiro, 2020).

Por isso, dentro do contexto do presente trabalho, a Lei Geral de Proteção de Dados Pessoais coíbe o uso indevido de dados pessoais coletados ou adquiridos de forma lícita ou ilícita, para que os docentes que vão participar da avaliação institucional do INEP tenham garantias de que seus dados não serão usados de forma indiscriminada, ou seja, o uso de dados precisa estar dentro dos parâmetros legais, como previsto em lei, e essas informações, sejam elas sensíveis ou não, merecem cui-

sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; VII segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; VIII prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas». Em Lei 13.709, de 14 de agosto de 2018.

dado, tendo em vista todo o transtorno que isso pode acarretar. A legislação não está proibindo a utilização dos dados, porém, os envolvidos devem seguir normativas para salvaguardar que o usuário não será afetado de alguma forma com a exposição dessas informações, ainda mais sem o seu consentimento. Afinal, como a própria lei prescreve, e dando sequência à discussão, os dados são direitos fundamentais.

A preocupação com o uso indiscriminado dessas informações pessoais dos docentes vai além da Lei Geral de Proteção de Dados Pessoais, de modo que seria importante a existência de uma regulamentação por parte do INEP para promover meios pelos quais tais dados sejam analisados sem que o docente fique preocupado acerca de como estão tratando seus dados. Para cumprir esta lei, é fundamental tornar o processo de avaliação mais transparente e seguro, afinal, considerando que muitas informações presentes são de cunho pessoal, elas precisam ser resguardadas e com segurança. Além disso, todo o processo, até mesmo a fase de eliminação desses dados, deverá ser realizado de forma clara e objetiva, proporcionando ao titular o domínio (mesmo que indireto) e a condução das suas informações pessoais coletadas ou produzidas durante a graduação ou pós-graduação.

Para ser possível a atribuição de responsabilidade civil ao avaliador, essencial fazer uma analogia com a função do operador, dentro da previsão da Lei Geral de Proteção de Dados Pessoais, conforme artigo quinto, inciso VII, considerando ser uma pessoa natural de direito privado que, ao estar de posse dos documentos dos docentes, tem autonomia para fazer o tratamento. As instituições de ensino superior, por estar em posse e ter a condição de realizar o tratamento desses dados, compartilhar as informações com o INEP e ter o controle de quem terá o acesso no momento da avaliação, figura como controladora (inciso VII do mesmo artigo), tendo em vista a coleta, a utilização, a avaliação, dentre outros.

Fazer essa equivalência é conceder à pessoa lesada a equiparação de responsabilidade e, conseqüentemente, a reparação do dano. Porém, o avaliador institucional, dentre suas atribuições de operador, não possui a obrigação de informar aos docentes (titulares dos dados) que estes estão sendo utilizados para o preenchimento de indicadores, competindo ao controlador (procurador institucional) tal explanação. Embora o vínculo institucional no presente caso seja apenas do controlador, não exime o operador da prática do ato ilícito, seja por negligência, imprudência ou imperícia.

Atribuições dos docentes, responsabilidade civil e compliance nas avaliações do INEP

A formação de professores para a educação básica é feita pelo curso de licenciatura. De acordo com Biscaro (2023) esses cursos formam para que o docente venha a ter um desempenho adequado em sala de aula e sejam preparados para favorecer uma sólida formação inicial para que aprendam a ensinar.

No Brasil, a resolução CNE/CP número 2 de 2019, define as diretrizes curriculares nacionais para a formação inicial de professores para a educação básica e institui a base nacional comum para a formação inicial de professores da educação básica. Nele estabelece que as competências específicas são o conhecimento, prática e engajamento profissional.

No que tange ao conhecimento profissional, deve o docente dominar o conhecimento e saber ensiná-lo, reconhecer o contexto de vida dos discentes, conhecer a estrutura e governança dos sistemas educacionais. A prática profissional é composta por planejar as ações de ensino; gerir o ambiente de aprendizagem; avaliar o desenvolvimento dos alunos; conduzir pedagogicamente os objetos de conhecimento, competência e habilidades. Por fim, no que se refere ao engajamento profissional, a resolução estabelece que o docente deve se comprometer com seu próprio desenvolvimento profissional; comprometer-se com a aprendizagem dos discentes; participar de projetos pedagógicos; engajar-se com as famílias e comunidade visando melhorar o ambiente.

Verifica-se que a docência exige um compromisso ético-político com a educação. A formação dos professores deve ser um processo permanente, não devendo ser compreendida apenas enquanto formação inicial, necessitando de uma reflexão crítica, unindo a teoria e a prática (Aoyama, 2023). Assim, além das atribuições dos professores, há expectativas para suas capacidades, formação e atuação. Deve o professor realizar continuamente formações, ter habilidades emocionais, ser compreensivo e reflexivo, entre outras qualificações (Nogueira, 2023).

No que tange às avaliações do INEP, apesar da regulamentação da Lei Geral de Proteção de Dados Pessoais, diante da falta de um método eficaz para o compartilhamento da documentação dos docentes nas instituições de ensino existe o risco do vazamento de dados, que pode causar danos irreparáveis. Por isso, partindo da Lei 13.709/18, em caso de vazamento, deverá ser aplicada a responsabilidade civil, garantindo-se a reparação do titular, seja ela moral ou material (Godinho e outros, 2020). Neste sentido, medidas de governança, dentre elas, o *compliance*, precisam ser executadas para evitar danos aos titulares. Como explicitado anteriormente, a utilização dos dados dos docentes para a avaliação é necessária para que seja cumprida a atribuição da nota do indicador de credenciamento e credenciamento, assim como para o plano de cargos e salários, a titulação, o contrato de trabalho, o vínculo institucional, pontos avaliados e quanto aos quais os avaliadores precisam ter acesso.

Dito isso, os avaliadores do INEP, ao terem em posse os dados pessoais e sensíveis dos docentes, devem assumir algumas obrigações e cuidados para que as informações não tenham uma finalidade diversa da avaliação. Embora a Lei Geral de Proteção de Dados Pessoais traga as figuras do controlador, do operador e do encarregado, deve-se ter ciência de outras figuras que possuem o acesso, mesmo que provisório; no caso em questão, de terceiros (De Moraes, 2019).

Na presente pesquisa foi atribuída aos avaliadores a função de operador, tendo em vista que eles tratam tais dados e os utilizam para uma única função. Por isso, é necessário analisar pontos como protocolos estabelecidos de padrões de segurança, *compliance* e gestão de governança, para que seja possível a proteção dos dados pessoais ou ações que não violem os dados dos titulares, pois caso contrário, será necessária a aplicação da responsabilidade civil.

Segundo Cavalieri Filho, em seu sentido conceitual, falar em responsabilidade é exprimir uma ideia de obrigação, ter um encargo ou até mesmo uma contraprestação. Já no sentido jurídico, não segue a mesma linha. A essência da responsabilidade está direcionada à noção de algum desvio de conduta, ou seja, foi delineada para alcançar tipos de condutas praticadas de forma que lesione terceiros, sendo assim necessário reparar o prejuízo decorrente de uma violação de um dever jurídico. Desta forma, «responsabilidade civil é um dever jurídico sucessivo que surge para recompor o dano decorrente da violação de um dever jurídico originário» (Cavalieri Filho, 2012: 2).

Dentro do contexto da Lei Geral de Proteção de Dados Pessoais, é preciso pensar na atribuição de responsabilidade civil em caso de desvio de conduta, considerando que a atuação do avaliador deve ser estritamente analisar os documentos e atribuir uma nota nos indicadores relacionados aos docentes e, caso, venha ser realizada uma prática irregular, será necessária a reparação. Será discutido no próximo tópico que a proteção de dados está relacionada à proteção da vida privada do indivíduo, sendo assim um direito fundamental consagrado, além da dignidade da pessoa humana e dos direitos da personalidade, presentes na Constituição Federal de 1988. Registra-se que embora exista o consentimento por parte dos docentes, a utilização de seus dados por intermédio das instituições de ensino superior deverá ser feita com prudência.

A Lei Geral de Proteção de Dados Pessoais traz em seus artigos 42 a 45 regras sobre a responsabilidade civil para o controlador ou o operador, porém, há discussão doutrinária sobre a sua categoria objetiva ou subjetiva. Sendo assim, a proposta não é fazer uma diferenciação sobre os dados pessoais (sensíveis ou não), mas acerca de sua natureza. Antes da problematização, Silvio de Salvo Venosa (2022) pontua o conceito de responsabilidade civil objetiva, aplicando-a em casos além dos descritos em lei, ou seja, a partir do momento em que a atividade desenvolvida implicar em dano e trazer risco a outrem, sendo ela por dolo ou culpa. Já a subjetiva, a partir do momento em que for demonstrado o dano pelo agente (Venosa, 2022).

Neste sentido, não será explorada tal perspectiva (objetiva ou subjetiva), devido aos desdobramentos e a necessidade de análise mais apurada para o caso concreto, mas sim, compreender que havendo vazamento de dados dos docentes, deverá ser aplicada uma sanção e mensurado o impacto que tal ilicitude causou (Novakoski e Napolini, 2020). É notória a necessidade de tratar esses dados com responsabilidade, tendo em vista ser inevitável fazer tal averiguação sem o compartilhamento *online*.

Destaca-se que antes da pandemia da covid-19 as avaliações eram feitas *in loco*, porém, devido a restrições sanitárias na época, a atividade foi feita de forma virtual, com exceção dos cursos da saúde, que permaneceram com atividades presenciais.

Em termos gerais, o agente de tratamento de dados será responsabilizado por irregularidades, conforme artigo 42 e seguintes da Lei Geral de Proteção de Dados Pessoais, embora necessário o tratamento por parte do controlado e operador no caso em questão e, caso este não ocorra, e o titular sofra danos, violando-se a legislação, será necessária a reparação, prevista no artigo 44. Desta forma, caso não for possível a identificação do responsável pelo dano ou o descumprimento da legislação, haverá responsabilidade solidária, considerando a existência das instruções apresentadas pelo controlador, conforme artigo 42, § primeiro, incisos I e II. Porém, os agentes não serão responsabilizados caso provarem que não foi realizado o tratamento de dados, que não houve violação à legislação e, por fim, em caso de culpa exclusiva do titular.⁴

Embora a Lei Geral de Proteção de Dados Pessoais e sua aplicabilidade esteja ligada aos direitos fundamentais, como será discutido a seguir, a responsabilidade pelos danos causados deve ser analisada com cautela, considerando que a publicação dos dados é necessária, porém, para reduzir riscos, as instituições de ensino superior precisam criar métodos de governança, dentre eles, o *compliance*, para que os avaliadores tenham consciência e promovam medidas de segurança nas atividades que serão desenvolvidas.

Por isso, «é fundamental que haja uma tutela rigorosa dos dados sensíveis, pois esses transformaram-se em conteúdo essencial para a concretização do princípio da igualdade e da não discriminação» (Mulholland, 2020: 205). Com o avanço das tecnologias em várias esferas, toda precaução com a utilização de dados é fundamental, tendo em vista os riscos materiais e imateriais que podem afetar o titular e violações aos direitos da personalidade.

Para que os agentes de tratamento de dados minimizem possíveis danos no vazamento de dados nas avaliações do INEP, utilizar a gestão de governança, dentre elas, o *compliance*, pode ser uma alternativa. Porém, embora exista essa possibilidade, é utópico achar que atender a este quesito impede que os dados sejam vazados. Todavia, é essencial buscar alternativas por meio da tecnologia para prevenir os riscos de possíveis danos que o vazamento pode causar.

A partir deste entendimento, a estrutura de *compliance* analisará não apenas as leis, mas também as ações que são guiadas por princípios e valores da companhia,

4. «Artigo 43. Os agentes de tratamento só não serão responsabilizados quando provarem: I que não realizaram o tratamento de dados pessoais que lhes é atribuído; II que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados, ou III que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro». Em Lei 13.709, de 14 de agosto de 2018.

incluindo a ética. Ter um código de conduta é disponibilizar uma disciplina interna que, necessariamente não estão presentes em uma lei, cria padrões rigorosos equivalente à mesma (Wagatsuma e outros, 2020).

Muitas informações encaminhadas para os avaliadores não correspondem aos indicadores, por isso, ter um programa de *compliance* com procedimentos internos que consiga compreender o que é solicitado e encaminhar apenas isso pode minimizar uma possível irregularidade. Muitas vezes, com raras exceções, o departamento que possui toda a documentação dos docentes é o de recursos humanos e, quando as instituições de ensino superior vão passar por algum tipo de avaliação institucional, tais documentos são reunidos e colocados em compartilhamento pelo procurador institucional, que tem dentre suas atribuições, disponibilizar os dados dos docentes para que os avaliadores possam preencher os indicadores.

Não basta criar um procedimento para dificultar o acesso a tais informações, mas sim adotar processos que gerem responsabilidade e compromisso com toda equipe. Cada instituição tem as suas peculiaridades e riscos; por isso, cumprir com a legislação, criando regras e regulamentos, possibilita a todos os agentes trabalhar com segurança (Antonik, 2016).

Por se tratar de uma organização, as instituições de ensino superior precisam estar em conformidade com as exigências do Ministério da Educação e Cultura, cumprindo e criando regulamentos impostos pela legislação. De acordo com a Federação Brasileira de Bancos, o *compliance* está relacionado à função e direcionamentos de contribuir para a prevenção de riscos regulatório, sejam elas locais ou internacionais, além de danos que possam ser causados para imagem da instituição. Destaca-se que a prática do *compliance* está cada vez mais acentuada fazendo com que a missão, visão, valores e cultura organizacional estejam de acordo com as boas práticas do mercado.⁵

Por meio do *compliance*, o operador e o controlador do tratamento dos dados poderão reduzir os riscos de vazamento, considerando a política que as instituições de ensino superior definem, auxiliando na prevenção e na fiscalização de como serão manipulados esses dados no decorrer da avaliação. Além disso, são vários outros atos regulatórios que precisam ser seguidos para que as instituições de ensino superior ofereçam de forma permanente seus cursos de graduação e pós-graduação.

Essas técnicas fazem com que seja criado um clima organizacional capaz de proteger não apenas o docente que terá seus dados disponíveis para avaliação, mas também as próprias instituições de ensino superior diante de eventual responsabilidade, caso um dano venha a ser causado. É preciso deixar claro que o *compliance* não exime a responsabilidade, mas sim busca a prevenção e a redução de danos, passando maior credibilidade às instituições de ensino superior após sua implementação.

5. Federação Brasileira de Bancos, *Guia de boas práticas de compliance*. Edição revisada e atualizada 2018, disponível em <https://tipg.link/MynQ>.

O direito à proteção de dados pessoais como direito fundamental e da personalidade

Com o avanço da tecnologia e a praticidade das avaliações institucionais, o INEP, por meio da Portaria número 265, de 27 de junho de 2022, regulamentou a Avaliação Externa Virtual *in loco*, para que as comissões responsáveis tenham autonomia de realizar as visitas de forma remota. Com isso, o acesso aos dados dos docentes é necessário para a comprovação de vínculo institucional, do tempo de serviço, da função ou cargo e da titulação.

Ter acesso a tais informações possibilita que o avaliador consiga produzir o relatório por meio dos indicadores, fazendo com que a instituição tenha nota satisfatória no quesito da titulação dos docentes. Por isso, a questão referente à proteção de dados deve ser tratada de forma que as instituições de ensino superior tenham responsabilidade, desde o recebimento e a divulgação por meio do compartilhamento em nuvem até a exclusão, devendo ser feita de forma correta, de acordo com Lei Geral de Proteção de Dados Pessoais.

Os dados pessoais constituem algo intrínseco ao ser humano e, por essa razão, a utilização dos dados de forma incorreta ou abusiva pode acarretar vários danos para o titular, independentemente se o uso é feito pelas próprias instituições de ensino superior ou por terceiros, como avaliadores. Por esse motivo surge uma demanda no ordenamento jurídico: preservar a utilização desses dados, utilizados de forma correta ou com consentimento do titular, por isso, a necessidade de instrumentos capazes de protegê-los como direito fundamental (Doneda, 2011). Assim, é fundamental compreender a importância deste tema, tendo em vista que a proteção de dados pessoais «tem sido compreendida não como um direito à propriedade, mas como espécie de direito da personalidade; um direito de o indivíduo autodeterminar as suas informações pessoais» (Stelzer e outros, 2019: 3).

A Constituição Federal de 1988, embora não traga a terminologia «proteção de dados», uma vez que é um tema relativamente recente, não a deixa explícita como direito fundamental, sendo necessário compreender algumas menções que são relevantes; afinal, o artigo quinto da Constituição traz vários direitos, possibilitando que os indivíduos vivam de forma digna. O presente artigo traz a inviolabilidade e o sigilo da correspondência, podendo incluir até os meios digitais; salvo no inciso XII, são hipóteses específicas, ou seja, o indivíduo não pode ter seus dados e suas informações violados. Destaca-se a importância de se manter inviolável o sigilo, respeitando as particularidades.

Isso mostra que é possível compreender que o conteúdo deve ser destinado ao titular, não sendo autorizado que um terceiro colete a informação ali presente e dê destinação da forma que achar necessário, sem o consentimento do titular. De igual modo ocorre quanto aos dados pessoais, já que é necessário ter todo um cuidado e

responsabilidade para assegurar que tais informações não serão utilizadas de forma incorreta. Outra referência a dados que está relacionada aos direitos fundamentais é o *habeas data*, que embora tenha uma ação específica, é importante destacar a preocupação do legislador com os dados pessoais, permitindo ao titular ter conhecimento das informações presentes e, se assim desejar, retificar esses dados (Sarlet e Saavedra, 2020).

Desta forma, o *habeas data* tem como premissa proteger o indivíduo contra o abuso referente a seus dados, garantindo, assim, os direitos à informação, à intimidade e à privacidade. Neste caso, a presente ação tem como premissa assegurar o conhecimento das informações à pessoa solicitante, bem como retificá-las, caso não forem verdadeiras. Desta forma, pode, em alguns casos, ser estendida a terceiros, partindo do pressuposto de que exista algum interesse fundado no conhecimento ou na alteração dos dados armazenados. As pessoas, sejam elas físicas ou jurídicas, precisam tomar precaução ao obter dados de terceiros. Destaca-se, como já discutido anteriormente, considerando toda transformação tecnológica, que possuir dados se tornou uma mercadoria, em um cenário em que muitas empresas estão buscando obter o maior número de dados possíveis para seus próprios benefícios.

Falar em tratamento de dados exige certo cuidado, pelo fato de daqueles dados serem de uma pessoa e que violações podem resultar em diversos transtornos. Por isso, a Lei Geral de Proteção de Dados Pessoais proporciona uma legislação que garanta os direitos fundamentais do titular. Apesar das menções na Constituição Federal, em face da especificidade do assunto, é fundamental uma legislação específica que atenda e direcione a forma de tratamento desses dados (Sarlet e Saavedra, 2020).

A informação pessoal é algo que está atrelado ao sujeito, a qual toda organização social entende e identifica por meio dos dados, tornando-se elementar a proteção (Pinheiro, 2020). Na atual sociedade, as informações são a base das relações sociais, de modo que é necessário saber como tratar esses dados. Uma pessoa não pode ter a sua vida ameaçada pelo fato dos seus dados sensíveis terem sido publicados, afinal, todo sujeito tem como direito fundamental fazer parte de uma comunidade religiosa, filosófica, política, ter uma filiação sindical, ter uma vida sexual e informações sobre a sua saúde e sua genética preservadas (Marinho, 2020). Todas essas informações precisam de um cuidado especial para que o titular não tenha seus direitos violados.

De fato, a Lei Geral de Proteção de Dados Pessoais tem impactado todos os segmentos, sobretudo empresas que, muitas vezes, não tinham cuidado ao coletar dados. A partir de agora, começam a pensar em estruturar uma forma de tratar os dados coletados, dando-lhes uma finalidade e meios que possibilitem que o usuário tome ciência de como serão conduzidas as suas informações pessoais (Boff e outros, 2018). A lei em questão precisa ter, como essência, a preservação da dignidade da

pessoa humana, garantindo direitos fundamentais e de toda a sociedade, conforme presente no artigo segundo da referida lei.⁶

É necessário considerar que a regulamentação da Lei Geral de Proteção de Dados Pessoais precisa respeitar a privacidade e a liberdade e que o titular desses dados é o principal agente no que tange a suas próprias informações (Marinho, 2020). Tudo o que estiver relacionado aos seus dados, sendo eles sensíveis ou não, deverá observar seu consentimento. É comum falar apenas de dados no que diz respeito à lei, mas vale destacar que a preservação da imagem é algo também presente, como o próprio artigo demonstra, devendo esta ser protegida. Todo tratamento deve ser feito de uma forma que não venha a prejudicar o titular; a Lei Geral de Proteção de Dados Pessoais não tem como princípio prejudicar as instituições de ensino superior que possuem esses dados, mas sim assegurar que tenham uma consciência de que se algo for feito de forma que o titular não tenha conhecimento ou consentimento tal fato implicará em responsabilidade.

Diante das avaliações do INEP, após serem autorizadas no formato virtual *in loco*, as instituições de ensino superior tiveram que se adaptar. Com isso, toda a documentação precisou ser compartilhada em nuvem para que os avaliadores tivessem acesso, como já apresentado no tópico anterior. Todavia, não é possível ter o controle de como esses dados serão tratados durante e após a avaliação. Isso pode causar vários problemas para os docentes que tenham esses dados pessoais e sensíveis divulgados sem um devido tratamento. Destaca-se a previsão no Código Civil brasileiro de 2002, que apresenta um capítulo específico sobre os direitos de personalidade.⁷

As instituições de ensino superior, sejam elas faculdades, centros universitários ou universidades, para oferecerem cursos de nível superior (bacharelado, licenciatura ou tecnólogo), dependem da aprovação do INEP. Após a constituição da sociedade empresária de direito privado, elas precisam fazer o registro no Ministério da Edu-

6. «Artigo segundo. A disciplina da proteção de dados pessoais tem como fundamentos: I o respeito à privacidade; II a autodeterminação informativa; III a liberdade de expressão, de informação, de comunicação e de opinião; IV a inviolabilidade da intimidade, da honra e da imagem; V o desenvolvimento econômico e tecnológico e a inovação; VI a livre iniciativa, a livre concorrência e a defesa do consumidor, e VII os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais». Em Lei 13.709, de 14 de agosto de 2018.

7. «Artigo 21. Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo». Essa disposição faz referência clara aos direitos da personalidade. E «Artigo 11. Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária. Artigo 12. Pode-se exigir que cesse a ameaça, ou a lesão, a direito da personalidade, e reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei. Parágrafo único. Em se tratando de morto, terá legitimação para requerer a medida prevista neste artigo o cônjuge sobrevivente, ou qualquer parente em linha reta, ou colateral até o quarto grau». Em Lei 10.406, 10 de janeiro de 2002, disponível em <https://tipg.link/MyoL>.

cação e Cultura, para que tenham aprovado o início das suas atividades. Cabe a este ministério fiscalizar os processos de autorização, reconhecimento, credenciamento, reconhecimento e renovação de reconhecimento de cursos, de forma que, após o cadastro e a liberação de funcionamento, as instituições de ensino superior podem iniciar suas atividades como instituição de ensino.

As instituições de ensino superior não estão imunes ao tratamento de dados, tendo em vista que as informações de colaboradores, professores, técnicos, empresas que prestam serviço, enfim, todos os dados que são coletados e armazenados precisam ser tratados dentro das normas exigidas pela Lei Geral de Proteção de Dados Pessoais. Vale destacar que os dados presentes nas instituições de ensino não são apenas aqueles coletados em formato digital e que fichas cadastrais, laudos médicos, atestados e listas de presença são dados que precisam ser tratados dentro das normativas (Stelzer e outros, 2019: 4). Para entender a importância dos dados nas instituições de ensino superior é necessário compreender como esse tratamento deve ser realizado. Nesse sentido, a própria Lei Geral de Proteção de Dados Pessoais, em seu artigo quinto, inciso X, pontua uma definição sobre o que vem a ser o termo tratamento de dados, na Lei 13.709.

Considerando a legislação vigente sobre proteção de dados, cabe destacar que as instituições de ensino superior, objeto deste trabalho, não estão isentas de responsabilidades. Deve-se ter todo um cuidado quanto ao tratamento dos dados, conforme preconiza a Lei Geral de Proteção de Dados Pessoais, proporcionando que o meio acadêmico tenha garantias de que os seus dados serão tratados dentro das normativas legais e caso venha ocorrer alguma irregularidade é necessário apurar os fatos e tomar as medidas cabíveis (Luna, 2020).

Embora a Lei Geral de Proteção de Dados Pessoais determine como essa regulamentação deve ser feita dentro das pessoas jurídicas, a proposta desse trabalho é demonstrar a eventual responsabilidade por parte das instituições de ensino superior diante do vazamento de informações. Assim, haverá uma responsabilidade civil, prevista nos artigos 932 e 933, ambos do Código Civil.⁸

Deste modo, em uma possível ação de regresso, poderá as instituições de ensino superior responsabilizar cada um dos atores responsáveis, dentro de seu respectivo

8. «Artigo 932. São também responsáveis pela reparação civil: I os pais, pelos filhos menores que estiverem sob sua autoridade e em sua companhia; II o tutor e o curador, pelos pupilos e curatelados, que se acharem nas mesmas condições; III o empregador ou comitente, por seus empregados, serviçais e prepostos, no exercício do trabalho que lhes competir, ou em razão dele; IV os donos de hotéis, hospedarias, casas ou estabelecimentos onde se albergue por dinheiro, mesmo para fins de educação, pelos seus hóspedes, moradores e educandos; V os que gratuitamente houverem participado nos produtos do crime, até a concorrente quantia. Artigo 933. As pessoas indicadas nos incisos I a V do artigo antecedente, ainda que não haja culpa de sua parte, responderão pelos atos praticados pelos terceiros ali referidos». Em Lei número 10.406, 10 de janeiro de 2002.

trabalho (ou falta dele), a ser analisado no caso concreto. Por isso, é importante a implementação de um programa de *compliance* para arquivar toda a documentação feita no processo, descrevendo a participação de cada um, as informações sobre quais dados serão coletados e sua finalidade. Em caso de vazamento e judicialização será importante para comprovar que apesar do fatídico a empresa fez o melhor que podia para evitá-lo (Silva, 2019).

Conforme apresentado no decorrer deste trabalho, o vazamento de dados sensíveis ou não pode acarretar vários danos para o seu titular e a responsabilidade das instituições de ensino superior diante de prejuízos. A própria legislação é bem específica quanto à responsabilidade e à função de cada agente referente aos dados, porém, vale destacar que as pessoas jurídicas de direito privado têm a sua responsabilidade.⁹

O acesso aos dados dos docentes, além das implicações legais com o vazamento ou a utilização de forma indiscriminada, afeta diretamente os direitos da personalidade do indivíduo, dentre eles, a privacidade, considerando o acesso a informações pessoais que possuem os coordenadores, avaliadores, o procurador institucional e o próprio representante das instituições de ensino superior. Por isso, a importância da tutela do docente, considerando que «os dados pessoais não podem ser tratados como bens patrimoniais, que, uma vez fornecidos, podem ser livremente utilizados pelo destinatário» (Schreiber, 2014: 141). Desta forma, o acesso a tais dados precisa ser pensado de uma forma que proteja seu titular, diminuindo os riscos de um possível vazamento irregular.

É crucial considerar os atributos essenciais da pessoa humana, sobretudo que o seu ambiente de trabalho deve lhe proporcionar segurança. A utilização dos seus dados coletados no âmbito de avaliação pelas instituições de ensino superior não deve ser motivo de uso indiscriminado, como preconiza a Lei Geral de Proteção de Dados Pessoais. A proteção do docente não pode ficar restrita a aspectos físicos e deve abranger todos os desdobramentos inerentes a sua vontade. Toda essa proteção precisa ser pensada, tendo em vista que «os direitos da personalidade devem ser observados sempre em favor da proteção dos trabalhadores» (Da Silva e Pereira, 2013: 57). A violação do meio ambiente de trabalho do docente perpassa não apenas a violação da privacidade, com a exposição da sua imagem, voz, honra ou direitos autorais, mas também os seus dados pessoais.

9. «Artigo 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional». Em Lei 13.709, de 14 de agosto de 2018.

Conclusões

O presente trabalho procurou compreender o percurso da Lei Geral de Proteção de Dados Pessoais, sua importância no ordenamento jurídico e em que termos poderá ser acionado o judiciário em caso de vazamento de dados. Cabe destacar que a sociedade está em constante transformação e isso faz com que novas necessidades surjam. Consequentemente, essas demandas precisam de respaldo legal, exemplo disso são os casos de violação de dados pessoais, sobretudo porque a tecnologia permitiu que as pessoas se conectassem de uma maneira que potencializa sua vulnerabilidade e dificulta sua proteção.

Atualmente, fazer uma compra ou solicitar um acesso significa expor dados pessoais e isso vem se tornando cada dia mais comum, por isso, é necessária uma legislação capaz de proteger os indivíduos no que tange ao tratamento de seus dados.

Essa vulnerabilidade faz com que exista um desequilíbrio entre o titular dos dados e a pessoa jurídica que detém essas informações. Muitas vezes, solicitar uma correção ou a exclusão de dados é um processo muito burocrático. As empresas necessitam dos dados para oferecer os seus serviços, principalmente os considerados sensíveis; afinal, conhecer o consumidor na sua essência é fundamental para oferecer um produto ou um serviço.

Pensando em todos esses fatores, a Lei Geral de Proteção de Dados Pessoais surgiu como um instrumento regulatório para o tratamento de dados, buscando responsabilizar as pessoas físicas ou jurídicas que detêm esses dados, para que este processamento não seja feito de forma que venha a prejudicar o titular. Infelizmente, o uso indiscriminado está presente por toda parte e muitas empresas não se preocupam em como conduzir toda essa informação.

Por isso, ao compartilhar dados dos docentes para a avaliação da instituição ou curso, protocolos precisam ser pensados, considerando a vulnerabilidade do titular ao ter tais documentos nas mãos de terceiros, cujo uso de forma indiscriminada pode violar os direitos da personalidade, dentre eles, a privacidade.

Ao refletir sobre essas possibilidades, o presente trabalho trouxe a importância de se pensar sobre o eventual vazamento de dados das instituições de ensino superior e qual a sua responsabilidade perante o ordenamento jurídico. Afinal, documentos pessoais, carteira de trabalho, plano de carreira, contrato de trabalho, dentre outros, ficam disponíveis para a análise do vínculo que o docente tem com a instituição.

Por isso, mesmo com todas as dificuldades enfrentadas pelas instituições, estas não poderão deixar de formular projetos de segurança e ter um programa de *compliance* efetivo. O tratamento de dados pelas instituições de ensino superior é de sua responsabilidade e, conforme preconiza a Lei Geral de Proteção de Dados Pessoais, deverá ser seguido todo um protocolo acerca de como essas informações serão tratadas.

É importante deixar claro que a lei em questão não tem como finalidade fazer com que as empresas não trabalhem com os dados dos seus clientes, mas sim que elas tenham responsabilidade quanto ao modo como vão tratar esses dados, afinal, estes estão relacionados diretamente à dignidade da pessoa humana e danos neste sentido podem ser irreparáveis. Por isso, as pessoas que possuem esses dados, sejam elas pessoas físicas ou jurídicas, precisam ter conhecimento acerca da legislação e agir com responsabilidade.

Referências

- ANTONIK, Luis Roberto (2023). *Compliance, ética, responsabilidade social e empresarial: Uma visão prática*. Rio de Janeiro: Alta Books.
- AOYAMA, Kaori Aparecida (2023). «Contribuições freireanas para formação de professores: Uma investigação dos PPC dos cursos de licenciatura da UEMS/Dourados». *Anais do Seminário Formação Docente: Intersecção Entre Universidade e Escola*, 5 (5). Disponível em <https://tipg.link/MxGg>.
- BISCARO, Adriana de Fátima Vilela (2023). «O PIBID na UFGD: Contribuições para a formação inicial de professores». *Anais do Seminário Formação Docente: Intersecção Entre Universidade e Escola*, 5 (5). Disponível em <https://tipg.link/MxGl>.
- BOFF, Salete Oro, Vinícius Borges Fortes e Cinthia Obladen de Alemendra Freitas (2018). *Proteção de dados e privacidade: Dos direitos às novas tecnologias na sociedade da informação*. Rio de Janeiro: Lumen Juris.
- BURKART, Daniele Vincenzi Villares (2021). *Proteção de dados e o estudo da LGPD*. [Tese de mestrado]. Bauru: Universidade Estadual Paulista Júlio de Mesquita Filho.
- CAVALIERI FILHO, Sergio (2012). *Programa de responsabilidade civil*. 10.a ed. São Paulo: Atlas.
- DA SILVA, Leda Maria Messias e Marice Taques Pereira (2013). *Docência (in)digna: O meio ambiente labora do professor e as consequências em seus direitos da personalidade*. São Paulo: LTr.
- DA SILVA, Aline Gama, Paloma de Lavor Lopes, Renan Gomes de Moura e Marcus Vinicius Barbosa (2019). «Mecanismos de compliance em instituições de ensino superior». *Revista Valore*, 4: 317-330. DOI: [10.22408/rev402019373317-330](https://doi.org/10.22408/rev402019373317-330).
- DE MORAES, Maria Celina Bodin (2019). «LGPD: Um novo regime de responsabilização civil dito “proativo”». *Civilistica*, 8 (3): 1-6. Disponível em <https://tipg.link/MxHB>.
- DONEDA, Danilo (2011). «A proteção dos dados pessoais como um direito fundamental». *Espaço Jurídico*, 12 (2): 91-108. Disponível em <https://tipg.link/MxHo>.
- GALERA, Fernanda (2021). *Proteção de dados: Reflexões práticas e rápidas sobre a LGPD*. São Paulo: Expressa.
- GARCIA, Lara Rocha (2020). *Lei Geral de Proteção de Dados (LGPD): Guia de implantação*. São Paulo: Blucher.

- GODINHO, Adriano Marteleto, Genésio Rodrigues de Queiroga Neto e Rita de Cássia de Moraes Tolêdo (2020). «A responsabilidade civil pela violação a dados pessoais». *Revista IBERC*, 3 (1): 1-23. DOI: [10.37963/iberc.v3i1.105](https://doi.org/10.37963/iberc.v3i1.105).
- LUNA, Francisco Djalma Silva (2020). *Instituições de ensino superior brasileiras e sua jornada para a transformação digital*. [Dissertação de mestrado]. São Paulo: Universidade de São Paulo.
- MARINHO, Fernando (2020). *Os 10 mandamentos da LGPD: Como implementar a Lei Geral de Proteção de Dados em 14 passos*. São Paulo: Atlas.
- MULHOLLAND, Caitlin (2020). «Responsabilidade civil por danos causados pela violação de dados sensíveis e a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018)». Em Guilherme Magalhães Martins e Nelson Rosenvald (coordenadores), *Responsabilidade civil e novas tecnologias* (pp. 109-124). Indaiatuba: Foco.
- NOGUEIRA, Isadora de Souza (2023). «Reflexões sobre as atribuições docentes no Brasil e Paraguai». *Anais do Seminário Formação Docente: Intersecção Entre Universidade e Escola*, 5 (5). Disponível em <https://tipg.link/MxHD>.
- NOVAKOSKI, André Luis Mota e Samyra Haydêe dal Farra Napolini (2020). «Responsabilidade civil na LGPD: Problemas e soluções». *Conpedi Law Review*, 6 (1): 158-174. DOI: [10.26668/2448-3931_conpedilawreview/2020.v6i1.7024](https://doi.org/10.26668/2448-3931_conpedilawreview/2020.v6i1.7024).
- PINHEIRO, Patrícia Peck (2020). *Proteção de dados pessoais: Comentários à Lei número 13.709/2018 (LGPD)*. 2.a ed. São Paulo: Saraiva Educação.
- SARLET, Ingo Wolfgang e Giovani Agostini Saavedra (2020). «Fundamentos jusfilosóficos e âmbito de proteção do direito fundamental à proteção de dados pessoais». *Direito Público*, 17 (93): 33-57. Disponível em <https://tipg.link/MxHF>.
- SCHREIBER, Anderson (2014). *Direitos da personalidade*. 3.a ed. São Paulo: Atlas.
- STELZER, Joana e outros (2019). «A Lei Geral de Proteção de Dados Pessoais e os desafios das instituições de ensino superior para a adequação». Em *XIX Colóquio Internacional de Gestão Universitária*. Florianópolis: Universidade Federal de Santa Catarina.
- TEIXEIRA, Tarcísio (2021). *LGPD e e-commerce*. 2.a ed. São Paulo: Saraiva Educação.
- VENOSA, Sílvio de Salvo (2022). *Direito civil: Obrigações e responsabilidade civil*. 22.a ed. Barueri: Atlas.
- WAGATSUMA, Adriana Tocchet, Karina Nigri Cattan e Luciana Miliauskas Fernandes (2020). «Departamento de compliance: Independência e autonomia». Em Isabel Franco (organizadora), *Guia prático de compliance* (pp. 1-16). Rio de Janeiro: Forense.

Sobre os autores

MARCELO NEGRI SOARES é advogado e contabilista. É professor mestrado e doutorado UniCesumar. Doutor pela Pontifícia Universidade Católica de São Paulo e pós-doutor pela Universidade de Coimbra, Portugal. Orientador e pesquisador Instituto Cesumar de Ciência, Tecnologia e Inovação, Next Seti e Fundação de Amparo à Pesquisa do Estado de São Paulo. Editor da Springer Journal para E-Law e da *Revista Brasileira de Direitos da Personalidade*. Professor visitante da Coventry University em direito, administração e negócios. Seu correio eletrônico é negri@negrisoares.com.br.

 <http://orcid.org/0000-0002-0067-3163>.

JOSÉ JOAQUIM PEREIRA MELO é doutor e mestrado em história e sociedade pela Universidade Estadual Paulista Júlio de Mesquita Filho. Também é pós-doutorado em história da educação pela mesma instituição. Atualmente é professor associado da Universidade Estadual de Maringá. Seu correio eletrônico é pereirameloneto@hotmail.com.  <http://orcid.org/0000-0002-0743-8000>.

WELINGTON JUNIOR JORGE é mestre em educação pela Universidade Estadual de Maringá e mestrando em ciências jurídicas pela Universidade Cesumar. É bolsista institucional pela Universidade Cesumar, no Instituto Cesumar de Ciência, Tecnologia e Inovação. Seu correio eletrônico é prof.welingtonjorge@gmail.com.  <https://orcid.org/0000-0001-9684-7844>.

La *Revista Chilena de Derecho del Trabajo y de la Seguridad Social* es una publicación semestral del Departamento de Derecho del Trabajo y de la Seguridad Social de la Facultad de Derecho de la Universidad de Chile, y que tiene por objetivo el análisis dogmático y científico de las instituciones jurídico-laborales y de seguridad social tanto nacionales como del derecho comparado y sus principales efectos en las sociedades en las que rigen.

DIRECTOR

Luis Lizama Portal

EDITOR

Claudio Palavecino Cáceres

SECRETARIO DE REDACCIÓN

Eduardo Yañez Monje

SITIO WEB

revistatrabajo.uchile.cl

CORREO ELECTRÓNICO

pyanez@derecho.uchile.cl

LICENCIA DE ESTE ARTÍCULO

Creative Commons Atribución Compartir Igual 4.0 Internacional



La edición de textos, el diseño editorial
y la conversión a formatos electrónicos de este artículo
estuvieron a cargo de Tipografía
(www.tipografica.io)