LEI GERAL DE PROTEÇÃO DE DADOS NAS RELAÇÕES DE TRABALHO: UMA ANÁLISE DA RESPONSABILIDADE DA EMPRESA NO CASO DE VAZAMENTO DE DADOS PESSOAIS E SENSÍVEIS DO EMPREGADO[1]

GENERAL DATA PROTECTION LAW IN LABOR RELATIONS: AN ANALYSIS OF THE COMPANY'S RESPONSIBILITY IN THE EVENT OF LEAKAGE OF PERSONAL AND SENSITIVE EMPLOYEE DATA

Ana Carolina Faria TEREZA[2]

Iara Marthos ÁGUILA[3]

RESUMO
O presente estudo empreende uma análise jurídica do vazamento de dados de empregados no contexto das prerrogativas estabelecidas pela Lei Geral de Proteção de Dados (LGPD), considerando as influências normativas da General Data Protection Regulation (GDPR). A pesquisa aborda as implicações legais decorrentes dos vazamentos, a responsabilidade do empregador em consonância com os princípios de proteção de dados e privacidade. Além disso, explora a pertinência de um Sistema

[1] O presente artigo sintetiza a monografia de conclusão da pesquisa, realizada para o Programa Interno de Bolsas de Iniciação Científica (PIBIC 2022-2023) da Faculdade de Direito de Franca (FDF), Franca/SP.

[2] Graduanda da Faculdade de Direito de Franca/SP.

[3] Doutora e Mestre em Direito. Professora titular da Faculdade de Direito de Franca, na disciplina Direito do Trabalho e Processo do Trabalho. Advogada trabalhista.

ISSN 2675-0104 – v.8, n.1, dez. 2023

de Gestão de Segurança da Informática (SGSI) como medida estratégica na mitigação desses riscos, oferecendo uma perspectiva interdisciplinar que permeia os âmbitos jurídico, tecnológico e ético.
Palavras-Chave: vazamento de dados do empregado; lei geral de proteção de dados; *general data protection regulation*; sistema de gestão de segurança da informação.

ABSTRACT
The present study undertakes a legal analysis of employee data breaches in the context of the prerogatives established by the General Data Protection Law (LGPD), considering the normative influences of the General Data Protection Regulation (GDPR). The research addresses the legal implications arising from these breaches, the employer's responsibility in line with the principles of data protection and privacy. Additionally, it explores the relevance of an Information Security Management System (ISMS) as a strategic measure in mitigating these risks, offering an interdisciplinary perspective that encompasses legal, technological, and ethical realms.
Keywords: employee data breach; general data protection law; general data protection regulation; information security management system.

1 INTRODUÇÃO

Nos últimos anos, a intersecção entre a esfera digital e as relações laborais tem desencadeado uma complexa teia de desafios e oportunidades. A proteção dos dados pessoais e sensíveis dos empregados emerge como um imperativo ético e legal, catalisado pela promulgação da Lei Geral de Proteção de Dados (LGPD). A presente análise direciona seu foco para um aspecto vital e sensível: o vazamento de tais informações no contexto das relações de trabalho.

A "sociedade em rede", uma noção proeminente no pensamento de Manuel Castells, descreve um paradigma em que as estruturas sociais, culturais e econômicas são moldadas pelas tecnologias da informação e comunicação. Nesse ambiente, a troca veloz de dados e informações transcende as barreiras geográficas, criando uma teia interconectada que permeia todos os aspectos da vida moderna. Essa perspectiva se mostra especialmente relevante ao examinarmos o contexto das relações de trabalho, onde a digitalização tem transformado tanto os processos produtivos quanto a forma como os empregados interagem com as empresas.

Em meio a essa revolução digital, emerge um desafio considerável: a segurança dos dados pessoais e sensíveis dos empregados. O vazamento dessas informações, que podem variar desde dados de saúde até informações financeiras, potencialmente ameaça a privacidade e a

integridade dos indivíduos. Tais incidentes podem resultar em consequências graves, tanto para os empregados afetados quanto para as organizações responsáveis pela proteção desses dados. É nesse contexto que a análise das implicações da Lei Geral de Proteção de Dados (LGPD) nas relações de trabalho ganha relevância, proporcionando um arcabouço normativo e ético para lidar com essas situações complexas.

A Lei Geral de Proteção de Dados (LGPD), inspirada em iniciativas globais como a General Data Protection Regulation (GDPR) da União Europeia, consolida princípios essenciais para a coleta, processamento e armazenamento responsável de dados pessoais e sensíveis. A GDPR, implementada em 2018, estabeleceu um padrão internacional de proteção de dados, influenciando diretamente a abordagem adotada por diversos países, incluindo o Brasil, com a LGPD.

Neste contexto, o Sistema de Gestão de Segurança da Informação (SGSI) assume uma função crucial. O SGSI se configura como uma abordagem sistêmica que permite às organizações identificar, avaliar e mitigar riscos relacionados à segurança dos dados, conferindo maior confiabilidade aos processos de coleta, processamento e armazenamento de informações pessoais e sensíveis dos empregados. A integração do SGSI nas operações laborais não apenas assegura a conformidade com a LGPD, mas também confere uma vantagem competitiva ao zelar pela confiança e integridade dos colaboradores.

Este estudo tem como objetivo primordial a análise do vazamento de dados pessoais e sensíveis do empregado no contexto da LGPD, abordando suas implicações e repercussões. Dentre os objetivos específicos, destacam-se a influência da GDPR na LGPD, a investigação dos procedimentos de prevenção e resposta a vazamentos e a avaliação da aplicabilidade do Sistema de Gestão de Segurança da Informação (SGSI).

Para alcançar esses propósitos, esta pesquisa se utilizará de metodologia que engloba pesquisa bibliográfica, exemplificação de caso real de vazamentos dados e adotará uma abordagem qualitativa, valendo-se de análise documental e exemplificação de caso real acontecido no cenário brasileiro.

A intersecção entre a Lei Geral de Proteção de Dados e as relações de trabalho carrega implicações substanciais e multifacetadas. Este capítulo introdutório delineia as bases conceituais, os desafios emergentes e a abordagem metodológica que norteará a presente investigação. A pesquisa visa lançar luz sobre o tema complexo dos

ISSN 2675-0104 – v.8, n.1, dez. 2023

vazamentos de dados dos empregados, contribuindo para uma compreensão mais ampla e informada das implicações dessa questão na era digital e regulamentar contemporânea.

2 UNIVERSO DIGITAL: CONCEITOS FUNDAMENTAIS

O entendimento dos fundamentos do universo digital é essencial para contextualizar a análise da Lei Geral de Proteção de Dados (LGPD) nas relações de trabalho. Neste sentido são explorados conceitos que fundamentam a compreensão desse ambiente em constante evolução.

Uma das perspectivas que se pode analisar é a apresentada por Manuel Castells na teoria da "Sociedade em Rede" (Castells, 2002, p. 98-99). Castells destaca como as tecnologias da informação e comunicação moldaram uma sociedade onde as redes digitais são o cerne das interações humanas, afetando a economia, a cultura e a política. Essa abordagem proporciona insights sobre como o ambiente digital permeia várias esferas, incluindo as relações de trabalho.

A interrelação sociocultural e a evolução tecnológica demonstram como a digitalização impactou a maneira como as pessoas interagem e compartilham informações. A tecnologia transcendeu barreiras geográficas e temporais, promovendo uma integração global de culturas e perspectivas. Essa interconectividade afeta diretamente as relações de trabalho, à medida que os empregados operam em ambientes digitais diversos e interagem com colegas de diferentes partes do mundo.

No contexto digital, a privacidade e a salvaguarda de dados emergiram como direitos fundamentais. A proliferação de dados pessoais e sensíveis exige proteção, levando à formulação de regulamentações como a LGPD. A necessidade de garantir que os dados dos indivíduos sejam tratados com responsabilidade e respeito torna-se crucial em um ambiente onde a coleta e o compartilhamento de informações são onipresentes.

Ao alcançar o término do segundo milênio da Era Cristã, de acordo com Manuel Castells, observa-se uma trama de eventos de indubitável relevância histórica que promoveram uma metamorfose no quadro societário da experiência humana. Emergiu, nesse contexto, uma revolução tecnológica de cariz informacional que, focalizando-se nas tecnologias da informação, desencadeou uma reestruturação do substrato material da sociedade em uma cadência marcada pela rapidez. Os nexos

econômicos, por sua vez, transcenderam os limites nacionais, erigindo-se em uma interdependência global, engendrando, desse modo, uma nova matriz relacional entre economia, entidade estatal e agrupamento social, conformada segundo um padrão de geometria variável. O suceder dos eventos demanda, pois, um exame das implicações jurídicas que emergem desse panorama, especialmente no que concerne aos arranjos regulatórios e aos princípios de governança que se mostram intrínsecos a essa confluência de forças transformadoras (Castells, 2002, p. 39).

As ideias, crenças e valores foram grandes incentivadores para as mudanças na era da internet e tecnologias da informação, pois os indivíduos encontraram liberdade para agirem e modificarem sua realidade. Tal realidade encontrava-se em um mundo em constante transformação e avanço, o que gerou incessante busca pela identidade individual e coletiva. Tal fato gerou importância devido ao conflito da identidade permanecer ou não a mesma passando por tais mudanças, sendo que a identidade do homem sempre teve grande significado desde os primórdios da humanidade.

Posto isso, Castells preceituou que:

> [...] a identidade está se tornando a principal, e às vezes, única fonte de significado em um período histórico caracterizado pela ampla desestruturação das organizações, deslegitimação das instituições, enfraquecimento de movimentos sociais e expressões culturais efêmeras. Cada vez mais as pessoas organizam seu significado não em torno do que fazem, mas com base no que elas são ou acreditam que são. (2002, p. 41)

Analisando brevemente os fatos supramencionados e alicerçados nos pressupostos contemporâneos, nota-se que emerge um notório paradoxo entre a entidade da "Rede" e a essência do "Ser", fomentando uma intersecção que confronta a própria identidade do indivíduo. Esse enigma tem arquitetado uma mutação no enfoque do indivíduo, levando-o a uma desvalorização das dimensões de sua atividade e autenticidade, e, por outro lado, conferindo primazia à busca por uma construção volitiva de si e à projeção ostensiva daquilo que aspira aparentar ser.

Em breves passagens em que a inovação tecnológica se mostrou presente no contexto social, pode-se citar que em 1642, o filósofo francês

ISSN 2675-0104 – v.8, n.1, dez. 2023

Blaise Pascal criou um engenho mecânico que desempenhava a soma e a subtração de números de oito algarismos; em 1951 foi lançado o primeiro computador, chamado UNIVAC I, para a venda comercial; em 15 de janeiro de 2001 foi estreada a "Wikipédia", que se tornou a primeira enciclopédia online, podendo ser escrita por qualquer indivíduo em qualquer local do mundo em que estiver; e poucos dias após o lançamento desta, e dias após o atentado de 11 de setembro de 2001, Steve Jobs inovou lançando o "AirPod", que foi caracterizado pelo seu criador como "carregar mil músicas dentro do bolso" (Pinheiro, 2021, p.81-86).

O Direito Digital vem sendo considerado uma nova disciplina jurídica. Sua idade é estimada em duas décadas. Costuma-se dizer que a Portaria Interministerial 147, de 31 de maio de 1995, editada pelos ministros da Comunicação e da Ciência e Tecnologia, que regulou o uso de meios da rede pública de telecomunicações para o provimento e a utilização de serviços de conexão à Internet, foi o primeiro diploma legal desse ramo (Araújo, 2017, p. 17).

Em continuidade ao citado acima, Lotufo contextuou, sobre o espaço onde os crimes digitais acontecem:

> Por conseguinte, com o aumento da popularidade e a expansão da internet, a proliferação dos delitos digitais tem ocorrido de forma acelerada. Esse progresso é tão marcante que o domínio jurídico passou a instituir legislações específicas para abordar tais infrações, além de efetuar modificações nas normas já existentes, com o intuito de assegurar que as ações dos criminosos digitais não fiquem impunes. Essa é uma das áreas de enfoque do direito digital, no qual os crimes digitais têm ganhado protagonismo cada vez maior no cotidiano. A despeito de estarem em evolução constante, seus conceitos têm vindo a ser delimitados, recebendo tratamento especial no âmbito jurídico (2020, p. 02).

Gibson, em sua obra, conceituou o ciberespaço como: Uma ilusão compartilhada experimentada diariamente por inúmeros indivíduos autorizados, independentemente das fronteiras nacionais, inclusive por crianças que estão em processo de aprendizado de conceitos matemáticos avançados. Uma visualização gráfica de informações abstratas extraídas dos repositórios de dados presentes em todos os computadores do sistema

global humano. Uma intricada complexidade além do alcance da imaginação. Linhas luminosas que abrangem o espaço não tangível da mente; aglomerados nebulosos e incontáveis constelações de dados. Como marés de luzes na paisagem urbana (Gibson, 2003, p. 67).

Lévy propôs: Contrariamente ao possível, estático e já constituído, o virtual é como o complexo problemático, o nó de tendências ou de forças que acompanha uma situação, um acontecimento, um objeto ou uma entidade qualquer, e que chama um processo de resolução: a atualização (1996, p.16).

Em consonância com os ensinamentos de Lévy (1996), o conceito de virtual adquire, assim, o papel de um elemento que instaura as tensões essenciais para o processo criativo que abarca a atualização. Este não é algo previsível ou estático, assemelhando-se a uma simples transição entre o possível e o real. Essa compreensão do virtual parece estar vinculada à fecundidade textual alcançada através do exercício de desconstrução.

O ciberespaço é considerado como um domínio virtual, uma vez que se encontra latente, configurando um espaço que transcende limites geográficos. Este ambiente é intangível, porém se manifesta de maneira distinta, conferindo-lhe uma realidade própria. O ciberespaço ocupa uma posição indeterminada, situada em um território não definido, repleto de potenciais e opções em evolução. É inviável sustentar que o ciberespaço se limita a computadores ou redes, uma vez que, afinal, há questionamentos de onde se localiza o ciberespaço, para onde se desloca todo esse "domínio" quando os computadores são desligados. A fluidez intrínseca ao ciberespaço é o que o qualifica como virtual.

A conscientização sobre o gerenciamento adequado dos dados pessoais no ciberespaço é essencial. A adoção de medidas de segurança, regulamentações de proteção de dados e práticas de privacidade são meios importantes para garantir que os dados pessoais sejam tratados de maneira ética e responsável, preservando os direitos e segurança em um ambiente digital cada vez mais interconectado.

Portanto, devido ao avanço da tecnologia, a coleta e o uso de dados pessoais se tornaram mais frequentes e intrusivos, o que levou a uma maior preocupação com a privacidade e a proteção de dados pessoais.

A transformação tecnológica tem criado novos desafios e preocupações em relação à proteção de dados pessoais, o que levou à

ISSN 2675-0104 – v.8, n.1, dez. 2023

criação da LGPD como uma forma de garantir a privacidade e segurança desses dados.

3 LEI GERAL DE PROTEÇÃO DE DADOS

A proteção de dados pessoais tem se tornado cada vez mais importante na sociedade atual, diante dos inúmeros escândalos envolvendo o vazamento dessas informações. Com o objetivo de coibir incidentes e garantir os direitos fundamentais dos donos desses dados, muitos países têm regulamentado a coleta, uso e tratamento dessas informações. O Brasil seguiu o exemplo da União Europeia e aprovou a Lei Geral de Proteção de Dados (LGPD) em 2018.

A Lei Geral de Proteção de Dados é uma legislação completa sobre proteção de dados, que foi desenvolvida desde 2010 e coloca o Brasil na lista de países que possuem tais leis. Ela segue os princípios da Constituição Federal Brasileira de 1988, juntamente com o Código Civil e o Marco Civil da Internet, mas é mais atualizada e abrangente em relação à utilização de dados. A nova legislação enfatiza a importância do consentimento, exigindo que ele seja livre, informado e inequívoco, e serve como um guia para outras normas apresentadas pela legislação.

Sendo assim, o artigo 1º e alguns aspectos do artigo 2º da Lei Geral de Proteção de Dados deixam claro e reafirmam o compromisso desta legislação em relação aos princípios constitucionais que incluem a dignidade, privacidade, intimidade, honra e outros direitos pessoais.

Como mencionado, a Lei Geral de Proteção de Dados tem suas raízes na Constituição Federal de 1988, que estabelece em seu artigo 5º, X, a inviolabilidade da vida privada e da intimidade, bem como o artigo 5º, XII, que trata da interceptação de comunicações telefônicas, telegráficas ou de dados. Além disso, a Constituição estabelece o Habeas Data no inciso LXXII, um remédio constitucional que tem como objetivo garantir os direitos fundamentais de informação, privacidade e intimidade do indivíduo, permitindo o acesso a informações pessoais em registros ou bancos de dados.

José Afonso Silva preceitua em sua doutrina o seguinte:

> [...] um remédio constitucional que tem por objetivo proteger a esfera íntima dos indivíduos contra: (a)

> usos abusivos de registros de dados pessoais coletados por meios fraudulentos, desleais ou ilícitos; (b) introdução nesses registros de dados sensíveis (assim chamados os de origem racial, opinião política, filosófica ou religiosa, filiação partidária e sindical, orientação sexual, etc.); (c) conservação de dados falsos ou com fins diversos dos autorizados em Lei. (2005, p. 453)

Dessa forma, é importante salientar que a Lei Geral de Proteção de Dados é fundamentada na proteção da privacidade, liberdade, segurança e justiça das pessoas, além de promover o desenvolvimento econômico e social. A referida lei estabelece uma base legal para a proteção de dados sob tutela jurídica, garantindo que os dados pessoais dos indivíduos sejam tratados com respeito e segurança.

E de acordo com Santini, Valois, Cruz, Chung e Galvão (2019, p.17): "A Lei Geral de Proteção de Dados repercutirá diretamente no meio corporativo, sobretudo porque os seus destinatários são pessoas físicas ou jurídicas que realizem a captação e tratamento de dados pessoais de terceiros em solo nacional".

Embora a Lei Geral de Proteção de Dados represente uma grande mudança na forma como as empresas lidam com os dados, estar em conformidade com a lei pode trazer maior segurança jurídica para a governança de dados no Brasil. Para alcançar essa adaptação, é possível contar com normatizações que ajudam a alinhar as práticas necessárias para a proteção das informações pessoais coletadas.

A legislação de proteção de dados do Brasil, conhecida como Lei Geral de Proteção de Dados (LGPD) emergiu fundamentada em uma variedade de princípios, tendo sido influenciada pelo regulamento europeu de dados, que, por sua vez, impactou as legislações em muitos países ao redor do mundo.

O *Official Journal of the European* (União Europeia, 2018), por meio de seu artigo *"The history of the general data protection regulation"*, pode-se entender que a regulamentação europeia (EU) 2016/679, também conhecida como *General Data Protection Regulation* (GDPR), foi promulgada em 27 de abril de 2016 e passou a ser aplicada em toda a União Europeia em 25 de maio de 2018. A GDPR representa um marco significativo nos últimos anos para a União Europeia, uma vez que substituiu a Diretiva de Proteção de Dados de 1995, que tinha como

ISSN 2675-0104 – v.8, n.1, dez. 2023

propósito fundamental proteger os direitos dos indivíduos em relação ao processamento de seus dados pessoais e a livre circulação desses dados.

A GDPR surge como uma resposta ponderada às crescentes preocupações sobre a violação de dados, da privacidade e proteção de dados no contexto digital, substituindo uma legislação anterior e desatualizada.

O conceito de violação de dados, ou *"data breach"*, refere-se à exposição não autorizada de informações confidenciais e sensíveis. Especificamente, o termo *"data breach"* ou incidente de dados pessoais, conforme definido no artigo 4, alínea 12 do *General Data Protection Regulation* (GDPR), faz referência a "Uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento" (União Europeia, 2016).

Em suma, a legislação de proteção de dados no Brasil foi influenciada pelo regulamento europeu de dados e se fundamenta em princípios variados, dos quais a responsabilização é de suma importância, o que se pode ver notarialmente no art. 88 da *General Data Protection Regulation*.

Dessa forma, o supramencionado artigo dispõe da seguinte forma:

> Artigo 88. Tratamento no contexto laboral
>
> 1. Os Estados-Membros podem estabelecer, no seu ordenamento jurídico ou em convenções coletivas, normas mais específicas para garantir a defesa dos direitos e liberdades no que respeita ao tratamento de dados pessoais dos trabalhadores no contexto laboral, nomeadamente para efeitos de recrutamento, execução do contrato de trabalho, incluindo o cumprimento das obrigações previstas no ordenamento jurídico ou em convenções coletivas, de gestão, planeamento e organização do trabalho, de igualdade e diversidade no local de trabalho, de saúde e segurança no trabalho, de proteção dos bens do empregador ou do cliente e para efeitos do exercício e gozo, individual ou coletivo, dos direitos e

> benefícios relacionados com o emprego, bem como para efeitos de cessação da relação de trabalho.
>
> 2. As normas referidas incluem medidas adequadas e específicas para salvaguardar a dignidade, os interesses legítimos e os direitos fundamentais do titular dos dados, com especial relevo para a transparência do tratamento de dados, a transferência de dados pessoais num grupo empresarial ou num grupo de empresas envolvidas numa atividade económica conjunta e os sistemas de controlo no local de trabalho.
>
> 3. Os Estados-Membros notificam a Comissão das disposições de direito interno que adotarem nos termos do n.º 1, até 25 de maio de 2018 e, sem demora, de qualquer alteração subsequente das mesmas. (União Europeia, 2016)

O art. 88, acima transcrito, reflete o entendimento de que o equilíbrio entre a proteção dos dados pessoais e a gestão eficaz das relações de trabalho requer flexibilidade regulatória. Ao permitir ajustes nos termos do GDPR para acomodar as necessidades específicas das leis e práticas laborais de cada Estado-Membro, o regulamento busca garantir que a proteção de dados seja aplicada de maneira eficaz e equilibrada no contexto do emprego, salvaguardando os interesses dos titulares dos dados e assegurando a conformidade com as leis nacionais.

Na Lei Geral de Proteção de Dados (LGPD), há um artigo que possui uma função semelhante ao art. 88 da General Data Protection Regulation (GDPR) da União Europeia. O dispositivo correspondente na LGPD é o art. 7º, que trata das hipóteses em que o tratamento de dados pessoais pode ser realizado sem a necessidade de consentimento do titular.

Enquanto o art. 88 do GDPR trata das adaptações do regulamento para o ambiente de trabalho, o art. 7º da LGPD prevê situações em que o tratamento de dados pessoais pode ser realizado sem consentimento, como cumprimento de obrigação legal, proteção da vida, tutela da saúde, entre outras. Portanto, embora não seja exatamente um paralelo ao art. 88 do GDPR, o art. 7º da LGPD também aborda exceções à necessidade de consentimento do titular, em alinhamento com a ideia de equilibrar a proteção de dados com situações específicas. O art. 11, inciso II, da LGPD

ISSN 2675-0104 – v.8, n.1, dez. 2023

dispõe sobre as excções de consentimento e também destaca a importância de encontrar um equilíbrio sensato entre a necessidade de tratamento de dados sensíveis, proteção dos direitos individuais e as exceções de consentimento do titular, refletindo a complexidade e os desafios inerentes à regulação da privacidade em um mundo cada vez mais orientado por dados.

4 LEIS

No âmbito da proteção de dados nas relações de trabalho, a responsabilidade das empresas assume um papel central. Serão exploradas diversas facetas dessa responsabilidade, delineando o tratamento de dados laborais conforme o art. 88 da *General Data Protection Regulation* (GDPR). Para ilustrar os desafios do tema, um caso emblemático de vazamento de dados de empregados no Brasil é abordado, destacando as consequências legais e reputacionais enfrentadas pela empresa Record. Além disso, o tópico examina a importância da cibersegurança na proteção de dados por meio da implementação de um Sistema de Gestão de Segurança da Informática, reforçando a necessidade de abordagens estratégicas para mitigar riscos e assegurar a conformidade com regulamentações. Ao explorar esses aspectos interligados, este tópico oferece uma visão abrangente das implicações e desafios que as empresas enfrentam no contexto do tratamento de dados pessoais de empregados.

Conforme já exposto, o art. 88 do GDPR é uma disposição de notável importância, pois trata das exceções à sua aplicação no contexto de tratamento de dados no emprego e reconhece que Estados-Membros podem adotar leis específicas que ajustem as regras do GDPR em relação ao tratamento de dados pessoais em contexto de emprego. Isso possibilita a adaptação das regras gerais do GDPR para questões relacionadas a recursos humanos, emprego e relações de trabalho. Essas leis específicas devem respeitar os princípios gerais do GDPR e, em particular, garantir a proteção dos direitos e liberdades dos titulares dos dados.

O incidente de divulgação de dados constitui um dos prejuízos primários, entre diversos outros, potencialmente causados pela efetivação de uma ameaça bem-sucedida que afeta diretamente o sigilo, podendo também resultar no comprometimento da integridade e acessibilidade.

A Lei Geral de Proteção de Dados (LGPD) do Brasil não possui um artigo específico que trate exclusivamente do "vazamento de dados do empregado". No entanto, o tratamento de incidentes de segurança que envolvem vazamento de dados, incluindo os dados de empregados, é abordado principalmente no art. 48.

O referido artigo estabelece que, em caso de incidente de segurança que possa acarretar risco ou danos aos titulares dos dados, o controlador (a empresa ou organização que coleta e processa os dados) deve comunicar o ocorrido à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares dos dados afetados. Essa comunicação deve ocorrer de maneira rápida e eficaz, e o art. 48 também prevê informações específicas que devem ser incluídas na notificação.

Delineia-se, primordialmente, que o arcabouço da LGPD institui a responsabilidade civil do controlador ou operador de dados pessoais que, por sua ação ou omissão, resultar em danos a terceiros, cuja corolária é a obrigação de indenização. A emersão de um dano, consoante preceitua a norma, deflagra a obrigação do responsável pela operação dos dados a proceder a justa compensação àquele lesado. Sublinha-se que tal responsabilidade é de natureza objetiva, impondo-se independentemente de culpa, bastando a relação de causalidade entre a ação ou omissão do agente de tratamento e o dano sofrido.

Dentro desse espectro, vislumbra-se a possibilidade de instauração de demandas judiciais pelos empregados em face da ex-empregadora. Caso o nexo causal entre o vazamento de dados e o efetivo dano aos colaboradores seja comprovado, erige-se uma base sólida para o pleito de compensações financeiras, sejam elas de ordem moral ou material. O dano moral, em especial, decorrerá da violação dos atributos da personalidade, causando angústia, desconforto e abalo psicológico.

De igual monta, a LGPD inova ao prever, em seu bojo, a viabilidade da inversão do ônus da prova, conferindo ao titular de dados a prerrogativa de, ante a demonstração de verossimilhança em suas alegações, transferir ao agente de tratamento o encargo de demonstrar a inexistência do alegado dano. Tal dispositivo se erige como mecanismo hábil a reequilibrar a relação entre as partes, notadamente quando o detentor dos dados, em geral pessoa natural, se encontra em posição de vulnerabilidade perante entidades de grande envergadura econômica, como é o caso da empresa Record.

ISSN 2675-0104 – v.8, n.1, dez. 2023

Um exemplo, que ocorreu no cenário brasileiro, foi o caso da RecordTV Rádio e Televisão Record S/A, uma das maiores emissoras de televisão brasileira sofreu uma invasão e teve dados vazados.

Em 8 de outubro de 2022, a emissora Record sofreu uma invasão de seu sistema por meio de um ataque ransomware – uma modalidade de ciberataque que envolve o sequestro de arquivos por meio de criptografia – exigindo um pagamento para a liberação dos sistemas afetados (Veja, 2010).

O grupo de hackers identificado como BlackCat/Alphv assumiu a autoria da invasão e demandou um resgate de US$ 5 milhões (aproximadamente R$ 26 milhões). É notório que a emissora optou por não efetuar o pagamento.

No momento da invasão, a Record experimentou dificuldades para manter suas operações normais, a ponto de substituir o programa "Fala Brasil" pela série "Todo Mundo Odeia o Chris", uma vez que a ferramenta de edição do telejornal estava inacessível devido à criptografia. Isso resultou em alguns colaboradores sendo dispensados de suas atividades, já que a conexão à internet também estava afetada.

Em 10 de outubro de 2022, a equipe de Tecnologia e Segurança conseguiu restabelecer grande parte dos sistemas, provavelmente por meio de um processo de restauração a partir de backups, uma vez que os arquivos continuavam criptografados.

No início de novembro do mesmo ano – quase um mês depois da invasão -, a Record enfim distribuiu um comunicado por e-mail aos atuais empregados avisando que seus dados pessoais foram expostos.

Este aviso foi semelhante à carta recebida por ex-funcionários e constava que os seguintes dados haviam sido vazados: dados cadastrais para contato e comprovação de identidade; dados de saúde; dados referentes à relação empregatícia, incluindo informações de dependentes; dados sobre filiação sindical e dados financeiros.

Portanto, conclui-se que a Record, não obstante a diligência em informar o vazamento, não se exime de sua responsabilidade enquanto controladora de dados, devendo responder pelos danos que eventualmente sejam constatados. O ato ilícito, consubstanciado no vazamento de dados pessoais, em consonância com as disposições da LGPD, abre caminho para a propositura de ações pelos empregados, que, mediante comprovação, poderão buscar ressarcimento por danos morais e materiais decorrentes da transgressão de suas garantias fundamentais. Por ora, por se tratar de um

caso relativamente recente ainda não é possível determinar o posicionamento da Justiça do Trabalho sobre referido caso.

A inclusão de uma cláusula no contrato de trabalho que autoriza a empresa a divulgar dados sensíveis do empregado de acordo com a LGPD (Lei Geral de Proteção de Dados) deve ser realizada considerando os princípios e requisitos estabelecidos por essa lei. O art. 11 da LGPD, em particular, permite o tratamento de dados pessoais sensíveis nas situações em que o titular dos dados tenha fornecido o seu consentimento explícito e em determinadas circunstâncias, como para o cumprimento de obrigações legais e regulatórias. Portanto, a inclusão de uma cláusula nesse sentido no contrato de trabalho é possível, desde que esteja de acordo com a LGPD.

A segunda turma do Superior Tribunal de Justiça entendeu que apesar de representar uma falha indesejável no manuseio de informações de cunho pessoal, a ocorrência de um vazamento de dados não detém, por si só, a intrínseca capacidade de instaurar um contexto de ressarcimento por dano moral. Portanto, no caso de se formular uma demanda por compensação, torna-se imperativo que o detentor dos dados tangibilize um prejuízo efetivamente ocasionado pela divulgação dessas informações sensíveis, apresentando evidências claras e substanciais desse impacto negativo (Superior Tribunal De Justiça, 2023).

Nesse segmento, Sêmola afirmou:

> A conclusão a que podemos chegar depois dessa breve anamnese é a de que operar um negócio a partir de agora será mais arriscado e menos monótono do que um dia foi. Que os segredos e informações de negócio têm alto valor e serão alvos de ataques cada vez mais inteligentes, customizados e volumosos, originados por motivações diversificadas, que estarão atentando contra a estrutura de segurança da informação em contínuo desenvolvimento, amadurecimento e adaptação. (2020, p.76)

A Lei Geral de Proteção de Dados (LGPD) prevê a aplicação de sanções administrativas para infrações relacionadas ao tratamento de dados pessoais, incluindo o vazamento de dados. As multas podem variar de acordo com a gravidade da infração e o impacto causado pela violação, como dispõe o art. 52.

ISSN 2675-0104 – v.8, n.1, dez. 2023

A inserção de cláusulas específicas nos contratos laborais, delimitando com precisão os direitos e deveres das partes no que concerne ao manejo dos dados, consubstancia-se como uma abordagem apta a estruturar uma relação contratual que seja transparente e onde as responsabilidades estejam bem delineadas. Tais disposições contratuais podem englobar aspectos como os propósitos do tratamento, os limites de acesso, a confidencialidade e as finalidades buscadas.

Fomentar uma cultura organizacional voltada à conscientização dos colaboradores acerca da relevância da segurança da informação constitui um fundamento vital. Dentre os procedimentos adotados para evitar vazamento de dados dos empregados, também merece destaque a implementação de mecanismos internos de supervisão, tais como a designação de um Encarregado de Proteção de Dados (DPO), a execução de auditorias periódicas e o estabelecimento de protocolos de gestão de riscos. Essa confluência de práticas estabelece um ciclo constante de vigilância e monitoramento, solidificando a resiliência da organização no tocante ao tratamento das informações sensíveis.

Na moldura delineada, as estratégias preventivas emergem como pilares fundantes no esforço de resguardar a organização e seus trabalhadores das contingências decorrentes da administração inadequada dos dados laborais. A combinação de conformidade normativa, clareza contratual, conscientização e vigilância interna robustece a postura do empregador na observância de suas obrigações e na promoção de um ambiente laboral baseado na responsabilidade e na confiança recíproca, e tais fatos podem se dar devido a empresa estar com um exímio Sistema de Gestão de Segurança da Informação.

Lotufo, Bissoli e Siqueira preceituam sobre a necessidade atual dos Sistemas de Gestão de Segurança da Informação:

> Dentre as preocupações necessárias para o pleno funcionamento de uma empresa, a aplicação de um Sistema de Gestão de Segurança da Informação passou a ser uma obrigação para que todos os processos internos empresariais se mantenham seguros. Isso porque as ameaças cibernéticas têm crescido exponencialmente nos últimos anos, seja no volume dos ataques, seja na sofisticação dos mecanismos invasores. Tal situação tende a tornar-se

> ainda mais grave com a expansão da internet das coisas.
>
> Os Sistemas de Gestão de Segurança da Informação (SGSI) são sistemas corporativos que abrangem todos os processos organizacionais ou parte deles e buscam proteger as informações da empresa dentro dos critérios de confidencialidade, integridade e disponibilidade (CID) da organização. Neste sentido, os SGSI traduzem-se em planos, estratégias, políticas, medidas e controles voltados para a segurança da informação que têm o intuito de implementar, monitorar, analisar, manter e melhorar a segurança da informação corporativa. (2020, p. 41)

Nesse sentido, a norma técnica ISO/IEC 27001 desempenha um papel fundamental na orientação das práticas de gestão de segurança da informação. Ela oferece um conjunto abrangente de diretrizes que permite a criação e implementação de um Sistema de Gestão de Segurança da Informação (SGSI) eficaz. Além disso, a ISO/IEC 27001 possibilita a avaliação e certificação dos controles de segurança implementados, resultando em benefícios substanciais para as organizações.

Alguns benefícios com mais notoriedade associados à adoção da ISO/IEC 27001, de acordo com o Conselho Nacional do Ministério Público, incluem:

a) Estabelecimento de Melhores Práticas: A norma oferece uma estrutura sólida e bem definida para estabelecer práticas exemplares na gestão da segurança da informação. Ela orienta as organizações a identificar riscos, avaliar ameaças e implementar controles apropriados para proteger ativos de informação.

b) Aumento da Segurança: Ao seguir as orientações da ISO/IEC 27001, as organizações podem reforçar significativamente sua postura de segurança. Isso ajuda a minimizar a exposição a ameaças cibernéticas, vulnerabilidades e ataques maliciosos, protegendo assim os dados sensíveis e críticos da empresa.

c) Conformidade Regulatória: A adoção da norma auxilia as organizações a atenderem a requisitos legais e regulamentares relacionados à segurança da informação. A conformidade efetiva com esses regulamentos fortalece a credibilidade da empresa e reduz os riscos associados a multas e penalidades.

ISSN 2675-0104 – v.8, n.1, dez. 2023

d) Confiança dos Clientes: A implementação da ISO/IEC 27001 demonstra um compromisso sólido com a segurança da informação, o que melhora a confiança dos clientes. Os clientes têm mais tranquilidade ao lidar com uma organização que prioriza a proteção de seus dados e informações sensíveis.

e) Gestão de Riscos Aprimorada: A norma auxilia as organizações a adotarem uma abordagem mais estruturada para a identificação, avaliação e mitigação de riscos relacionados à segurança da informação. Isso resulta em uma gestão de riscos mais eficaz e informada.

f) Melhoria Contínua: A ISO/IEC 27001 incentiva a busca pela melhoria contínua no campo da segurança da informação. As organizações são estimuladas a revisar e atualizar regularmente seus controles de segurança, adaptando-se às ameaças em constante evolução.

g) Vantagem Competitiva: Empresas certificadas de acordo com a ISO/IEC 27001 podem ganhar uma vantagem competitiva no mercado, uma vez que a certificação demonstra compromisso com padrões internacionais de segurança, o que pode atrair novos clientes e parceiros comerciais.

h) Proteção da Reputação: A implementação bem-sucedida da norma protege a reputação da empresa, minimizando o risco de violações de dados e vazamentos de informações confidenciais. Isso também contribui para a construção de uma imagem positiva no mercado.

Em resumo, a ISO/IEC 27001 é uma norma técnica valiosa que oferece um roteiro claro para a criação de um Sistema de Gestão de Segurança da Informática eficaz, aprimorando a segurança da informação, a conformidade regulatória, a confiança dos clientes e a vantagem competitiva de uma organização. Seus benefícios abrangentes posicionam a norma como um guia essencial para a garantia da segurança da informação no ambiente empresarial moderno.

A cibersegurança, em meio à era digital, com tantos vazamentos de dados das empresas, emerge como um fator de extrema relevância para as organizações que buscam proteger seus ativos e informações sensíveis contra ameaças cibernéticas crescentes. O Sistema de Gestão de Segurança da Informação (SGSI) se estabelece como uma estrutura crucial para orquestrar e fortalecer as medidas de cibersegurança dentro de uma empresa.

O SGSI, fundamentado na norma técnica ISO/IEC 27001, que se encontra com o art. 7º do Marco Civil, surge como uma abordagem

estratégica e integrada para gerenciar riscos de segurança da informação. Ele procura compreender a complexa interação entre tecnologia, processos e pessoas, a fim de criar uma postura resiliente e proativa em relação à cibersegurança.

Em suma, o Sistema de Gestão de Segurança da Informação se apresenta como um arcabouço estratégico e abrangente para a cibersegurança nas organizações. Ao integrar a tecnologia, os processos e o capital humano, o SGSI capacita as organizações a enfrentarem os desafios da segurança cibernética de maneira proativa, adaptativa e eficaz, salvaguardando os ativos de informação e sustentando a confiança de clientes, parceiros e partes interessadas.

5 CONCLUSÃO

A conjuntura da sociedade em rede, na qual informações fluem livremente e a conectividade digital transcende fronteiras, confere à proteção de dados uma centralidade inegável. A análise da responsabilidade da empresa no caso de vazamento de dados pessoais e sensíveis dos empregados emerge como uma reflexão indispensável nesse contexto, tendo em vista as profundas implicações que tais incidentes acarretam.

A reputação de uma empresa, hoje mais do que nunca, está intrinsecamente ligada à sua capacidade de salvaguardar informações sensíveis. O vazamento de dados pessoais e sensíveis dos empregados, além de resultar em prejuízos financeiros, pode abalar a confiança de clientes e parceiros. A percepção de que uma empresa não zela adequadamente pela privacidade dos indivíduos com os quais se relaciona e que realizam o trabalho da mesma, pode desencadear efeitos deletérios na imagem da organização, afetando sua competitividade e posição no mercado.

A efetivação de uma estratégia de proteção de dados encontra respaldo no Sistema de Gestão de Segurança da Informação (SGSI), o qual se erige como um mecanismo essencial para assegurar a conformidade com a Lei Geral de Proteção de Dados (LGPD) e sua contraparte europeia, a *General Data Protection Regulation* (GDPR). O Sistema de Gestão de Segurança da Informação, embasado na norma técnica ISO/IEC 27001, oferece um arcabouço metodológico para identificação, avaliação e

ISSN 2675-0104 – v.8, n.1, dez. 2023

mitigação de riscos, bem como para a implementação de controles de segurança, fomentando uma cultura organizacional voltada à proteção da informação.

As sanções previstas na Lei Geral de Proteção de Dados, que podem incluir multas substanciais, reforçam a imperatividade de uma postura diligente das empresas na gestão dos dados de seus empregados. A Lei Geral de Proteção de Dados, inspirada pela *General Data Protection Regulation*, reforça a necessidade de consentimento informado, transparência no tratamento de dados, ação em casos de vazamentos e medidas de segurança adequadas. A *General Data Protection Regulation*, estabelecendo uma abordagem semelhante na União Europeia, serve como exemplo global de como regulamentações avançadas em proteção de dados podem influenciar normativas em nível nacional.

Diante disso, a análise da responsabilidade da empresa no caso de vazamento de dados pessoais e sensíveis dos empregados transcende a esfera meramente jurídica, abrangendo aspectos sociais, econômicos e éticos. A capacidade de gerir e proteger dados, mitigando os riscos inerentes à era da informação, é fundamental para a preservação da reputação empresarial, a manutenção de relações de confiança com os empregados e o cumprimento das diretrizes legais em um mundo cada vez mais conectado e orientado por dados.

Em conclusão, diante do cenário complexo e sensível das relações de trabalho no contexto da Lei Geral de Proteção de Dados, fica evidente que a responsabilidade do empregador pelo vazamento de dados pessoais e sensíveis do empregado é uma questão de fundamental importância. A análise realizada ao longo desta pesquisa reforça a necessidade de considerar o impacto abrangente das violações de dados nesse ambiente, levando em conta tanto os aspectos jurídicos quanto os impactos na reputação e confiança que a empresa exerce. Dessa forma, sustenta-se a ideia de que o empregador deve ser responsabilizado por tais danos, reforçando não apenas a conformidade com as regulamentações, mas também a importância de implementar medidas sólidas de proteção de dados e de estabelecer uma cultura organizacional que priorize a segurança da informação e o respeito aos direitos dos empregados.

6 REFERÊNCIAS

ARAÚJO, Marcelo Barreto de. **Comércio eletrônico; Marco Civil da Internet; Direito Digital**. Rio de Janeiro: Confederação Nacional do Comércio de Bens, Serviço e Turismo, 2017.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 31 jan. 2023.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 31 jan. 2023.

BRASIL. **Lei nº. 10.406, de 10 de janeiro de 2002.** Institui o Código Civil. Brasília, 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 11 maio 2023.

BRASIL. **Lei nº. 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 18 maio 2023.

CASTELLS, Manuel. **A sociedade em rede**. A Era da Informação: Economia, Sociedade e cultura. 6. ed. São Paulo: Paz e Terra, 2002.

DE BLASI, Bruno Gall; VENTURA, Felipe. Record confirma que dados pessoais de ex-funcionários também foram vazados. **Tecnoblog**. 2022. Disponível em: https://tecnoblog.net/noticias/2022/11/30/record-confirma-que-dados-pessoais-de-ex-funcionarios-tambem-foram-vazados/. Acesso em: 20 jul. 2023.

DINIZ, Maria Helena. **Curso de direito civil brasileiro**. volume 1: teoria geral do direito civil. São Paulo: Saraiva, 2012.

GIBSON, Willian. **Neuromancer**. São Paulo: Aleph, 2003.

GONÇALVES, Carlos Roberto **Direito civil brasileiro**,.volume 1 : parte geral / Carlos Roberto Gonçalves. 10. ed. São Paulo: Saraiva, 2012.

ISSN 2675-0104 – v.8, n.1, dez. 2023

HÄBERLE, Peter. **Hermenêutica constitucional**. A sociedade aberta dos intérpretes da Constituição: contribuição para a interpretação pluralista e "procedimental" da Constituição. Tradução de Gilmar Ferreira Mendes. Porto Alegre: Sergio Antonio Fabris, 2002.

INTERNATIONAL STANDARD. ISSO/IEC 27001. Information technology – Security techniques – Information security management systems – Requirements. **International Standad**. 2013. Disponível em: http://www.itref.ir/uploads/editor/42890b.pdf. Acesso em: 23 jun. 2023.

LÉVY, Pierre. **O Que é Virtual?**. Rio: Editora 34. 1996.

LOTUFO, Larissa; BISSOLI, Leandro; SIQUEIRA, Rafael. Como implementar uma cibersegurança corporativa? In: PINHEIRO, Patricia Peck (coord.) **Segurança Digital** – proteção de dados nas empresas. São Paulo: Gen/Atlas. 2020.

MENDES, G. F.; SARLET, I. W.; LTDA, I. C. E. P.; LTDA, I. C. E. P.; CANOTILHO, J. J. G.; LEONCY, L. F.; STRECK, L. L. **Comentários à constituição do Brasil**. 2. ed. São Paulo: Saraiva, 2017.

MENDES, L. S. **Privacidade, proteção de dados e defesa do consumidor** - Linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MIRANDA, Rosângelo Rodrigues. **A Proteção Constitucional da Vida Privada**. São Paulo: Led-Editora de Direito LTDA, 1996.

NAÇÕES UNIDAS ONU. **Declaração Universal dos Direitos Humanos de 1948**. Adotada e proclamada pela Assembleia Geral das Nações Unidas (resolução 217 A III) em 10 de dezembro 1948. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em: 15 jun. 2022.

PINHEIRO, Patricia Peck. **Direito digital**. 7. ed. São Paulo: Saraiva, 2021.

PINHEIRO, Patricia Peck. **Segurança Digital** - Proteção de Dados nas Empresas. São Paulo: Grupo GEN, 2018.

SANTINI, B.; CRUZ, H. V.; VALOIS, R.; CHUNG, R.; GALVÃO, R. A eficácia da Lei Geral de Proteção de Dados (LGPD). In: SALDANHA, P. M. (Org.). **O que estão fazendo com meus dados?** A importância da Lei Geral de

Proteção de Dados. (Recife: SerifaFina. 2019. p. 19-30.

SILVA, José Afonso da. **Curso de direito constitucional positivo**. São Paulo: Malheiros, 2005.

UNIÃO EUROPEIA. EUROPEAN DATA PROTECTION SUPERVISOR The history of the general data protection regulation. **Official Journal of the European Union**. p. 88, 2018. Disponível em: https://edps.europa.eu/data-protection/data-protection/legislation/ history-general-data-protection-regulation_en. Acesso em: 26 jul. 2023.

UNIÃO EUROPEIA. General Data Protection Regulation (GDPR). Art. 88 GDPR – Processing in the contexto of employment. **UNIÃO EUROPEIA**. 2018. Disponível em: https://gdpr-info.eu/art-88-gdpr/. Acesso em: 25 jun. 2023.

UNIÃO EUROPEIA. **Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016.** Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Regulamento Geral sobre a Proteção de Dados. UNIÃO EUROPEIA. 2016. Disponível em: https://eurlex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN. Acesso em: 26 jul. 2023.

https://www.cnmp.mp.br/portal/transparencia/lei-geral-de-protecao-de-dados-pessoais-lgpd/a-lgpd/fundamentos-e-principios#:~:text=Os%20seguintes%20princ%C3%ADpios%20