PUC-SP

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO

FACULDADE DE DIREITO

Daniel Beneti Baldini

LGPD E SEUS IMPACTOS NO DIREITO BRASILEIRO,NAS RELAÇÕES INTERSOCIAIS E PROFISSIONAIS:

Como uma única Lei pode impactar tantos âmbitos da sociedade, não só do ponto de vista jurídico, mas também social e profissional

Projeto de Pesquisa do Trabalho de Conclusão de Curso, como requisito parcial para obtenção do título de bacharel em Direito, sob orientação do Prof. Rogério José Ferraz Donnini

São Paulo

2024

1 TEMA E JUSTIFICATIVA DA ESCOLHA

A monografia a ser desenvolvida terá como tema

“LGPD E SEUS IMPACTOS NO DIREITO BRASILEIRO, BEM COMO NAS RELAÇÕES INTERSOCIAIS E PROFISSIONAIS:”

A Lei Geral de Proteção de Dados (LGPD) representa um marco significativo no cenário jurídico brasileiro, estabelecendo diretrizes para o tratamento de dados pessoais por parte de organizações públicas e privadas. Sua promulgação em 2018 reflete a necessidade de adaptação do ordenamento jurídico nacional aos avanços tecnológicos e à crescente preocupação com a privacidade e segurança das informações pessoais.

A escolha deste tema para a minha Monografia em Direito é respaldada pela sua relevância no contexto atual. A LGPD não apenas redefine o modo como as instituições lidam com os dados pessoais, mas também impacta diretamente as relações intersociais e profissionais. Entender os aspectos legais e práticos dessa legislação é essencial para profissionais do direito, gestores de empresas e indivíduos em geral.

A LGPD introduz uma série de obrigações legais para as organizações, incluindo a necessidade de obtenção de consentimento explícito para o tratamento de dados pessoais, a garantia de transparência nas práticas de coleta e utilização de informações, além da obrigação de implementação de medidas de segurança adequadas. Além disso, estabelece sanções para o descumprimento das normas, podendo gerar multas significativas e até mesmo a responsabilização civil e penal das empresas e seus gestores.

Dessa forma, a LGPD demanda uma revisão das políticas internas das organizações, a fim de garantir conformidade com as novas exigências legais. Sendo assim, surge uma nova classe de advogados especializados em proteção de dados, que assumem um papel crucial na orientação de seus clientes sobre as melhores práticas para evitar litígios e sanções, bem como de se perceber eventuais irregularidades no âmbito digital que possa prejudicá-lo ou beneficiá-lo

No que diz respeito às relações intersociais, a LGPD promove uma conscientização maior sobre a importância da privacidade e proteção de dados pessoais. Indivíduos passam a ter mais controle sobre suas informações e a exigir maior transparência por parte das organizações. Isso impacta diretamente a forma como empresas e instituições se relacionam com seu público, fortalecendo a confiança e a reputação das marcas que adotam práticas transparentes e responsáveis de tratamento de dados.

No ambiente profissional, a LGPD impõe desafios adicionais às empresas, que precisam garantir a segurança e conformidade das informações de seus colaboradores e clientes. Programas de treinamento e conscientização se tornam essenciais para educar funcionários sobre as melhores práticas de proteção de dados e evitar incidentes de vazamento ou uso indevido de informações pessoais.

A LGPD representa um avanço significativo na proteção da privacidade e dos direitos dos cidadãos brasileiros em um mundo cada vez mais digitalizado. Seus impactos no direito brasileiro e nas relações intersociais e profissionais são profundos e requerem uma abordagem multidisciplinar para garantir sua efetiva implementação e cumprimento. Este tema oferece uma oportunidade única para explorar os desafios e oportunidades que surgem com a entrada em vigor dessa legislação e contribuir para o desenvolvimento de uma cultura de proteção de dados no Brasil.

2. OBJETIVOS DA PESQUISA

Os objetivos desta pesquisa são múltiplos e interconectados. Em primeiro lugar, busca-se compreender de forma abrangente os dispositivos legais estabelecidos pela LGPD e sua aplicabilidade no contexto do direito brasileiro, analisando os impactos jurídicos e regulatórios decorrentes de sua implementação. Além disso, pretende-se investigar os efeitos da LGPD nas relações intersociais, explorando como a conscientização sobre a proteção de dados pessoais influencia as interações entre indivíduos e organizações. Por fim, a pesquisa visa identificar as melhores práticas para garantir a conformidade com a LGPD no ambiente profissional, examinando os desafios enfrentados pelas empresas na adaptação às novas exigências legais e as estratégias mais eficazes para mitigar riscos e promover uma cultura de proteção de dados.

3. DESENVOLVIMENTO

O estudo do tema objeto da pesquisa será desenvolvido, a princípio, em conformidade com o índice abaixo:

LGPD E SEUS IMPACTOS NO DIREITO BRASILEIRO, BEM COMO NAS RELAÇÕES INTERSOCIAIS E PROFISSIONAIS

RESUMO

A pesquisa teve como objetivo geral compreender os dispositivos legais da LGPD e sua aplicabilidade no direito brasileiro, analisando os impactos jurídicos e regulatórios decorrentes de sua implementação. Especificamente, investigou os efeitos da LGPD nas relações intersociais, explorando a influência da conscientização sobre a proteção de dados; identificou melhores práticas para garantir a conformidade no ambiente profissional; e examinou os desafios e estratégias das empresas na adaptação às novas exigências legais. Utilizou-se o método bibliográfico, com coleta de dados através de periódicos, livros, artigos eletrônicos, revistas jurídicas e jurisprudências, adotando um enfoque exploratório para desenvolver o tema. Com o estudo foi possível concluir que a LGPD precisa ser continuamente atualizada para acompanhar as evoluções tecnológicas e novas formas de coleta e processamento de dados. O diálogo constante entre legisladores, autoridades reguladoras, empresas e a sociedade civil é crucial para manter a relevância e eficácia da legislação na proteção dos dados pessoais. A LGPD marca uma era de maior proteção e responsabilidade no tratamento de dados pessoais no Brasil, com impactos profundos no direito brasileiro e nas relações sociais e profissionais. A lei fortalece os direitos fundamentais de privacidade e promove uma cultura de respeito e responsabilidade no tratamento de dados pessoais. Sua implementação eficaz é essencial para alinhar o Brasil às melhores práticas globais de proteção de dados e privacidade, garantindo um ambiente mais seguro e confiável para todos.

Palavras-chave: LGPD; segurança de dados; relações trabalhistas.

ABSTRACT

The general objective of the research was to understand the legal provisions of the LGPD and their applicability in Brazilian law, analyzing the legal and regulatory impacts resulting from its implementation. Specifically, it investigated the effects of the LGPD on intersocial relationships, exploring the influence of awareness about data protection; identified best practices to ensure compliance in the professional environment; and examined the challenges and strategies of companies in adapting to new legal requirements. The bibliographic method was used, with data collection through periodicals, books, electronic articles, legal magazines and case law, adopting an exploratory approach to develop the theme. The study made it possible to conclude that the LGPD needs to be continually updated to keep up with technological developments and new forms of data collection and processing. Constant dialogue between legislators, regulatory authorities, companies and civil society is crucial to maintain the relevance and effectiveness of legislation in protecting personal data. The LGPD marks an era of greater protection and responsibility in the processing of personal data in Brazil, with profound impacts on Brazilian law and social and professional relations. The law strengthens fundamental privacy rights and promotes a culture of respect and responsibility in the processing of personal data. Its effective implementation is essential to align Brazil with the best global data protection and privacy practices, ensuring a safer and more reliable environment for everyone.

Keywords: LGPD; data security; working relationships.

SUMARIO

INTRODUÇÃO

A monografia a ser desenvolvida terá como tema “LGPD e seus impactos no direito brasileiro, bem como nas relações intersociais e profissionais”.

A Lei Geral de Proteção de Dados (LGPD) representa um marco significativo no cenário jurídico brasileiro, estabelecendo diretrizes para o tratamento de dados pessoais por parte de organizações públicas e privadas. Sua promulgação em 2018 reflete a necessidade de adaptação do ordenamento jurídico nacional aos avanços tecnológicos e à crescente preocupação com a privacidade e segurança das informações pessoais.

A escolha deste tema é respaldada pela sua relevância no contexto atual. A LGPD não apenas redefine o modo como as instituições lidam com os dados pessoais, mas também impacta diretamente as relações intersociais e profissionais. Entender os aspectos legais e práticos dessa legislação é essencial para profissionais do direito, gestores de empresas e indivíduos em geral.

A LGPD introduz uma série de obrigações legais para as organizações, incluindo a necessidade de obtenção de consentimento explícito para o tratamento de dados pessoais, a garantia de transparência nas práticas de coleta e utilização de informações, além da obrigação de implementação de medidas de segurança adequadas. Além disso, estabelece sanções para o descumprimento das normas, podendo gerar multas significativas e até mesmo a responsabilização civil e penal das empresas e seus gestores. Dessa forma, a LGPD demanda uma revisão das políticas internas das organizações, a fim de garantir conformidade com as novas exigências legais. Sendo assim, surge uma nova classe de advogados especializados em proteção de dados, que assumem um papel crucial na orientação de seus clientes sobre as melhores práticas para evitar litígios e sanções, bem como de se perceber eventuais irregularidades no âmbito digital que possa prejudicá-lo ou beneficiá-lo

No que diz respeito às relações intersociais, a LGPD promove uma conscientização maior sobre a importância da privacidade e proteção de dados pessoais. Indivíduos passam a ter mais controle sobre suas informações e a exigir maior transparência por parte das organizações. Isso impacta diretamente a forma como empresas e instituições se relacionam com seu público, fortalecendo a

confiança e a reputação das marcas que adotam práticas transparentes e responsáveis de tratamento de dados. No ambiente profissional, a LGPD impõe desafios adicionais às empresas, que precisam garantir a segurança e conformidade das informações de seus colaboradores e clientes. Programas de treinamento e conscientização se tornam essenciais para educar funcionários sobre as melhores práticas de proteção de dados e evitar incidentes de vazamento ou uso indevido de informações pessoais. A LGPD representa um avanço significativo na proteção da privacidade e dos direitos dos cidadãos brasileiros em um mundo cada vez mais digitalizado. Seus impactos no direito brasileiro e nas relações intersociais e profissionais são profundos e requerem uma abordagem multidisciplinar para garantir sua efetiva implementação e cumprimento. Este tema oferece uma oportunidade única para explorar os desafios e oportunidades que surgem com a entrada em vigor dessa legislação e contribuir para o desenvolvimento de uma cultura de proteção de dados no Brasil.

A implementação da LGPD enfrenta desafios significativos em termos de adequação e conformidade por parte das empresas e órgãos públicos, a falta de clareza em alguns aspectos da legislação e a necessidade de equilibrar a proteção de dados pessoais com a inovação tecnológica e a eficiência empresarial. Além disso, a insuficiente conscientização e capacitação sobre a lei entre profissionais e cidadãos pode comprometer a eficácia da proteção de dados pessoais e a confiança nas práticas de tratamento de dados. Assim, o problema a ser investigado é: Como a aplicação da LGPD pode ser efetivamente implementada no Brasil para garantir a proteção dos dados pessoais, ao mesmo tempo em que se equilibra a inovação tecnológica e a eficiência empresarial, e se assegura a conscientização e capacitação adequadas de todos os stakeholders envolvidos?

O objetivo geral da pesquisa é compreender, de forma abrangente, os dispositivos legais estabelecidos pela LGPD e sua aplicabilidade no contexto do direito brasileiro, analisando os impactos jurídicos e regulatórios decorrentes de sua implementação. Como objetivos específicos, pretende-se investigar os efeitos da LGPD nas relações intersociais, explorando como a conscientização sobre a proteção de dados pessoais influencia as interações entre indivíduos e organizações; identificar as melhores práticas para garantir a conformidade com a LGPD no ambiente profissional; examinar os desafios enfrentados pelas empresas na adaptação às

novas exigências legais e as estratégias mais eficazes para mitigar riscos e promover uma cultura de proteção de dados

Na pesquisa utilizou-se o método bibliográfico, no qual a coleta de dados se deu através de periódicos; livros; artigos eletrônicos; revistas jurídicas; jurisprudências relacionadas, entre outros, com base na utilização do método exploratório para assim, adquirir considerável contribuição para o desenvolvimento do tema escolhido.

1 LGPD

Em 14 de agosto de 2018, foi sancionada a Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD). Essa iniciativa representa um marco regulatório significativo no tema, como será discutido neste capítulo. A LGPD quebra um paradigma na cultura de proteção da privacidade, que antes era tratada de forma puramente formal, ao introduzir uma nova fase em que a proteção física dos dados pessoais, processados dentro ou fora de um ambiente, é imposta digitalmente (Frazão, 2018).

Embora houvesse legislação para regulamentar a proteção de dados no contexto das relações digitais estabelecidas pela Internet, essa legislação era incompleta. A proteção de dados já era parcialmente regida pela Lei nº 12.965/2014, conhecida como Marco Civil da Internet (Cavalcanti; Santos, 2018). Contudo, com a chegada da LGPD, a abordagem tornou-se mais abrangente e específica, proporcionando uma estrutura legal mais robusta e detalhada para a proteção dos dados pessoais.

1.1 Base Legal

A LGPD, em seu artigo 7º, prevê expressamente dez hipóteses que autorizam o tratamento de dados pessoais, além de estabelecer os requisitos necessários para a execução desse procedimento. Essas hipóteses são conhecidas como bases legais para o tratamento de dados pessoais.

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - mediante o fornecimento de consentimento pelo titular;
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019) Vigência
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.
> § 1º (Revogado). (Redação dada pela Lei nº 13.853, de 2019)
> § 2º (Revogado). (Redação dada pela Lei nº 13.853, de 2019) Vigência
> § 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.
> § 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.
> § 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.
> § 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.
> § 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei. (Incluído pela Lei nº 13.853, de 2019) Vigência

Nos casos em que o tratamento de dados não se baseia no consentimento, é possível compartilhar dados com órgãos públicos ou transferi-los a terceiros fora do setor público. Nesses casos, os agentes de tratamento devem comunicar claramente aos titulares dos dados sobre as operações executadas, garantindo-lhes os direitos previstos no artigo 18 da LGPD, como acesso, retificação, oposição, eliminação e informação sobre as entidades envolvidas no uso compartilhado dos dados. Essa comunicação deve ser renovada em caso de alteração da finalidade ou de qualquer operação de tratamento, incluindo novos compartilhamentos ou transferências. Além disso, deve-se verificar se os princípios da necessidade e adequação estão sendo cumpridos. Quando o tratamento de dados se baseia no consentimento, cada nova operação deve ser autorizada novamente, incluindo o compartilhamento com outras entidades, dentro ou fora da administração pública federal. O compartilhamento dentro da administração pública para a execução de políticas públicas não exige consentimento específico, mas o órgão que coleta os dados deve informar claramente

sobre o compartilhamento e suas partes envolvidas. O órgão que solicita o acesso deve justificar a necessidade com base em uma política pública específica e descrever o uso pretendido dos dados. Informações protegidas por sigilo continuam sujeitas a normativos e regras específicas (Governo Digital, 2020).

1.3 Processo Legislativo que levou à Promulgação da LGPD

Por volta de 1970, surgiram decisões jurídicas e legislações que reconheceram os dados pessoais como uma projeção da personalidade do indivíduo, merecendo assim proteção jurídica. As regulamentações sobre proteção de dados evoluíram em diversas fases até o momento atual, quando o direito à proteção de dados é reconhecido como um direito fundamental, com legislações específicas e abrangentes como a LGPD e a GDPR. A regulamentação da proteção de dados pessoais passou por quatro gerações distintas, que começaram com leis mais técnicas e restritas e evoluíram para disposições mais amplas e adequadas às tecnologias modernas (Lugati; Almeida, 2020).

A primeira geração de leis surgiu no contexto do Estado Moderno, onde o controle da população se dava por meio da obtenção massiva de informações. O Estado era o principal destinatário desses regulamentos, que se direcionavam à própria tecnologia. Um exemplo dessa primeira geração é o Privacy Act dos Estados Unidos, de 1974. Essa fase se estendeu até a implementação da Bundesdatenschutzgesetz, a lei federal alemã sobre proteção de dados pessoais, de 1977, época em que várias leis sobre proteção de dados foram implementadas na Alemanha. A primeira geração de leis, baseada somente em autorizações governamentais, tornou-se obsoleta com o avanço da tecnologia, já que o tratamento de dados passou a ser feito também por entes privados. Esse cenário levou à segunda geração de leis, onde o consentimento do usuário lhe conferia o poder de participar do processo de tratamento de dados em fases como coleta, uso e compartilhamento (Lugati; Almeida, 2020).

A terceira geração de leis focou mais na tutela do direito à privacidade, buscando garantir a efetividade desse direito e ampliando a participação do indivíduo em todas as fases do tratamento de dados. Este período introduziu o conceito de

"autodeterminação informativa". No entanto, essa abordagem ainda abrangia apenas uma parcela de indivíduos, mostrando-se insuficiente. Para superar essas limitações, surgiu a quarta geração, que prevalece até hoje. As leis atuais priorizam os titulares dos dados em relação a terceiros que possam manipular suas informações pessoais, buscando proteger de maneira mais abrangente os direitos dos indivíduos (Lugati; Almeida, 2020).

1.4 Objetivos da LGPD

A LGPD, Lei nº 13.709 de 14 de agosto de 2018, é a Lei de Proteção de Dados Pessoais que regulamenta o tratamento de dados pessoais, incluindo nos meios digitais, por pessoas naturais e jurídicas, tanto de direito público quanto privado. Seu objetivo é proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural (pessoa física).

Diferentemente do Marco Civil da Internet, que focava no usuário da internet de modo geral, a LGPD tem um foco mais direcionado à pessoa natural (Mèlo, 2019).

2 IMPACTO DA LGPD NO DIREITO BRASILEIRO

2.1. Linha do Tempo do tratamento aos dados

O artigo 5º, inciso X, da Constituição da República Federativa do Brasil de 1988 (CRFB/88) garante abstratamente o direito constitucional à privacidade. Esse direito pode ser entendido como a pretensão do indivíduo de não ser observado por terceiros e de manter seus assuntos, informações pessoais e características particulares protegidos de exposição a terceiros ou ao público em geral (Carvalho; Pedrini, 2019).

A proteção de dados já era tratada de forma indireta em legislações dispersas, como o Código de Defesa do Consumidor, a Lei do Cadastro Positivo (Lei nº 12.414/2011) e o Marco Civil da Internet. No entanto, não havia uma regulamentação específica que abordasse diretamente a problemática da proteção de dados, o que ressaltou a importância de uma legislação dedicada a esse tema. Durante esse período, outros países também estavam implementando suas próprias leis de proteção de dados. A União Europeia, que já tinha um histórico de legislações como a Convenção 108 e a Diretiva 95/46, implementou a *General Data Protection Regulation* (GDPR), uma legislação abrangente que regulamenta o tratamento de dados pessoais pelos países signatários. A criação da GDPR serviu como catalisador global, inspirando outros países a desenvolverem suas próprias legislações específicas. Nesse contexto, o Brasil promulgou, em 2018, a Lei Geral de Proteção de Dados (LGPD) (Lugati; Almeida, 2020).

A LGPD entrou em vigor no Brasil em agosto de 2020, dezessete anos após a criação da Rede Ibero-americana de Proteção de Dados (RIPD) em junho de 2003.

A Rede Ibero-americana de Proteção de Dados (RIPD) é um fórum integrador que reúne atores dos setores público e privado para desenvolver iniciativas e projetos relacionados à proteção de dados no espaço ibero-americano. Seu objetivo é manter e fortalecer o intercâmbio de informações, experiências e conhecimentos, promovendo desenvolvimentos legislativos que garantam uma regulação avançada do direito à proteção de dados pessoais em um contexto democrático. Desde o I Encontro Ibero-americano de Proteção de Dados (EIPD) em 2002, na Espanha, a RIPD tem trabalhado para coordenar ações e vontades, oficializando sua formação

em 2003, na Guatemala. Ao longo dos anos, a RIPD contribuiu significativamente para o desenvolvimento de regimes de proteção de dados em diversos países da América Latina, impulsionando políticas e iniciativas. Em 2017, a aprovação dos ‘Standards de proteção de dados pessoais para os países ibero-americanos’ consolidou esse esforço, servindo como modelo para futuras regulações e atualização de legislações existentes na região (CNPD, 2024)

2.2 Marco Civil da Internet

O Marco Civil da Internet é uma iniciativa legislativa criada em 2009, com o objetivo de estabelecer princípios, direitos e deveres para o uso da Internet no Brasil. Conforme destacam Lincoln Macário e Elisabel Ferriche, o Marco Civil da Internet possui três pontos principais:

> (...) a proteção à privacidade, a garantia de liberdade do internauta e a neutralidade de rede, que tem sido o principal alvo de tensões entre os parlamentares e pode inviabilizar a votação da proposta no plenário da Câmara. (...) A neutralidade de rede garante que os provedores de conexão tratem todos os dados de forma igual, não podendo privilegiar determinados sites ou conteúdos com quem tenham acordo comercial (Macário; Ferriche, 2014, p. 1).

O direito à privacidade, protegido pela Constituição Federal de 1988, é frequentemente violado, especialmente em relação às informações divulgadas pelos meios de comunicação. Com o Marco Civil da Internet, o Brasil tornou-se um dos poucos países a estabelecer a neutralidade da rede como norma. A Lei nº 12.965/2014, conhecida como o Marco Civil da Internet, em seu artigo 1º, inciso III, determina:

> Art. 1º Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.
> (...)
> III - proteção dos dados pessoais, na forma da lei;

A neutralidade da rede, estabelecida pelo Marco Civil da Internet, visa proteger os usuários contra a redução de sua velocidade de conexão por motivos econômicos.

Dessa forma, as empresas não podem mais diminuir a velocidade para serviços de voz por IP, como Skype, ou reduzir a banda de produtos de empresas concorrentes (Wireless Brasil, 2012). A neutralidade da rede é uma regra e qualquer provedor que discriminar o tráfego deve prestar explicações. Segundo o artigo 11 da Lei nº 12.965/2014, existem exceções à coleta de dados pessoais onde pode ocorrer discriminação, mas os requisitos técnicos para essas exceções devem ser definidos por decreto presidencial.

> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
> (...)
> § 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.

O Marco Civil da Internet reforçou o direito à privacidade dos usuários ao estabelecer que "informações pessoais e registros de acesso só poderão ser vendidos se o usuário autorizar expressamente a operação comercial" (Agência Brasil, 2014). Antes disso, grandes empresas utilizavam os dados dos internautas para fins comerciais e publicitários, acessando suas preferências para anunciar produtos direcionados ao público-alvo.

A Lei nº 13.709, de 14 de agosto de 2018, regulamenta o tratamento de dados pessoais no Brasil, abrangendo tanto o setor público quanto o privado. Conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), essa legislação visa proteger a privacidade dos usuários e seus dados pessoais. Para entender melhor a nova lei, Patrícia Peck Pinheiro, especialista em Direito Digital, explica: "A Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018, é a legislação brasileira que regula as atividades de tratamento de dados pessoais e altera os artigos 7º e 16 do Marco Civil da Internet" (Pinheiro, 2018, p. 37).

2.3 Direitos abordados pela Lei Geral de Proteção de dados e seu amparo constitucional

Os princípios de proteção de dados são aplicados de forma prática, facilitando sua integração nas políticas de proteção (Cavalcanti; Santos, 2018). Esses princípios, desenvolvidos por meio de ferramentas transnacionais e internacionais, são fundamentais para os cidadãos e devem ser implementados por instituições que manipulam dados pessoais. A pesquisa destaca os princípios da finalidade, transparência, qualidade dos dados e segurança como essenciais para a eficácia dos demais.

O princípio da finalidade exige que o uso de dados pessoais esteja claramente relacionado à finalidade comunicada aos proprietários no momento da coleta, restringindo o acesso de terceiros e garantindo a adequação e razoabilidade do uso. A transparência requer que os bancos de dados sejam públicos, combatendo práticas abusivas e reforçando a compatibilidade com um Estado de direito democrático. As empresas devem divulgar informações sobre seus bancos de dados para cumprir este princípio.

O princípio da qualidade dos dados exige que as informações sejam tratadas de maneira justa, atualizadas, precisas e objetivas. As empresas devem gerenciar dados com atenção, garantindo acesso e direitos de retificação e cancelamento. O princípio de segurança exige meios eficazes para proteger os dados contra perda, destruição, modificação e desvio não autorizado, além de assegurar a responsabilidade pelos danos causados pela violação da privacidade.

Programas de conformidade são recomendados para superar desafios de adequação e minimizar riscos legais e de reputação. A implementação requer uma estrutura tecnológica para segurança da informação, governança regulatória e contratual, além de treinamento de equipes (Cabral; Caprino, 2015; Veríssimo, 2017).

3 INFLUÊNCIA DA LGPD NAS RELAÇÕES DE TRABALHO

Desde a entrada em vigor da Lei nº 13.709/2018, em setembro de 2020, houve mudanças significativas nas rotinas das empresas, destacando a importância de implementar um programa de adequação à Lei Geral de Proteção de Dados (LGPD). A LGPD visa proteger os direitos fundamentais de liberdade e privacidade, indo além das relações trabalhistas. O compliance trabalhista, no entanto, é crucial para garantir que a empresa esteja em conformidade com a legislação vigente, como a CLT e acordos coletivos.

Nas relações trabalhistas, é necessário armazenar e tratar dados pessoais. No entanto, a LGPD afeta todas as relações jurídicas que envolvem o manuseio de dados e informações entre pessoas naturais e jurídicas (Santos, 2019, p. 43).

A Lei Geral de Proteção de Dados (LGPD) impactou diretamente as relações comerciais, pois todas as empresas utilizam dados pessoais para fins comerciais ou para cumprir obrigações legais. Embora a LGPD tenha trazido mudanças, seu objetivo não é complicar as relações de trabalho, mas sim garantir maior cuidado na coleta e tratamento de dados pessoais e sensíveis.

Os impactos da lei podem ser minimizados através de práticas cuidadosas desde a seleção de candidatos, passando pela relação contratual, até o término ou rescisão do contrato de trabalho, abrangendo colaboradores terceirizados, celetistas e prestadores de serviços (Mattia, 2021).

Todo o processo de contratação, manutenção e demissão de empregados deve ser revisado à luz da LGPD, definindo claramente quais dados devem ser coletados e como serão armazenados e tratados.

3.1 Consentimento

A fase pré-contratual, comumente conhecida como “processo de recrutamento e seleção”, envolve necessariamente a coleta e o tratamento de dados pessoais dos candidatos. A LGPD, em seu artigo 7º, inciso V, permite a utilização desses dados

quando necessário para a execução do contrato ou de procedimentos preliminares relacionados ao contrato do qual o titular faz parte. (Giuntini et al, 2021).

Todavia, as empresas devem solicitar o consentimento expresso do candidato e informá-lo de maneira clara que seus dados serão utilizados para recrutamento, avaliação e seleção. Se a empresa decidir utilizar esses dados para outra finalidade, isso deve ser claramente informado e o consentimento expresso do titular deve ser obtido. (Giuntini et al, 2021).

É importante destacar que, durante o processo de recrutamento e seleção, se a empresa contratar agências especializadas, estas devem ser claramente identificadas aos candidatos e explicar como seus dados pessoais serão utilizados. Na elaboração dos documentos trabalhistas, é necessária a adequação das cláusulas contratuais que envolvem o tratamento de dados pessoais, podendo ser necessário incluir novas cláusulas conforme os princípios da LGPD, apresentados no artigo 6º. (Giuntini et al, 2021).

3.2 Segurança de dados

O tratamento de dados e a adequação à LGPD nas relações de trabalho devem começar desde o anúncio da vaga e continuar em todas as fases contratuais – antes, durante e após o término do contrato, respeitando os prazos prescricionais estabelecidos pela legislação trabalhista. A LGPD regula a utilização dessas informações na fase pré-contratual, permitindo o tratamento de dados quando necessário para a execução do contrato ou em procedimentos preliminares, conforme o artigo 7º, inciso V (Oliveira, 2021; Estevão; Lima; Silva, 2022).

Desde o anúncio da vaga, as empresas devem solicitar apenas informações essenciais, respeitando o princípio da necessidade e limitando a solicitação de dados ao mínimo necessário. Elas devem evitar a coleta de dados não pertinentes ou excessivos e garantir que o tratamento dos dados não fira o princípio da não discriminação. As empresas não podem discriminar candidatos e devem evitar a coleta de dados com fins discriminatórios, independentemente do método de coleta. (Oliveira, 2021; Estevão; Lima; Silva, 2022).

Na fase pré-contratual, é necessário obter o consentimento expresso do candidato e informá-lo claramente sobre o uso de suas informações pessoais para recrutamento, avaliação e seleção. Se as empresas quiserem usar os dados para outros fins, isso deve ser claramente comunicado e o consentimento do candidato deve ser solicitado, mesmo para uso em campanhas de marketing ou compartilhamento de informações com outras empresas do mesmo grupo econômico. Além disso, se o candidato não for selecionado, os dados devem ser eliminados, a menos que haja consentimento expresso para mantê-los armazenados. Isso garante a transparência, o livre acesso, a qualidade dos dados e a segurança da informação. (Oliveira, 2021; Estevão; Lima; Silva, 2022).

Também é essencial que o empregador tenha cuidado com a guarda de documentos, garantindo a segurança do armazenamento, incluindo backups, especialmente no caso de documentos eletrônicos (Giuntini et al, 2021; Estevão; Lima; Silva, 2022).

3.3 Tratamento de dados pessoais sensíveis

Sobre os dados pessoais, estes se referem a direitos que protegem as pessoas contra intromissões externas, como o sigilo das correspondências e a privacidade. Portanto, a proteção dos dados pessoais é, na verdade, a proteção da personalidade, ou seja, de um conjunto de elementos fundamentais que formam a identidade de uma pessoa. (Giuntini et al, 2021).

Dados pessoais sensíveis são uma categoria especial de dados pessoais que, além de serem pessoais, podem causar discriminação se tratados de forma inadequada. Esses dados implicam riscos e vulnerabilidades aos direitos e liberdades dos titulares, necessitando de cuidados especiais em seu tratamento. São dados pessoais sensíveis: Dados biométricos: imagens faciais, impressão digital; Dados genéticos: relativos às características genéticas, hereditárias ou adquiridas de uma pessoa que tragam informações únicas sobre a sua fisiologia ou saúde. A coleta de dados pessoais sensíveis deve observar rigorosamente a finalidade, ou seja, o motivo do recolhimento desses dados, conforme indicado pela Lei nº 13.709. Esse tratamento rigoroso é necessário devido ao potencial de discriminação que esses dados podem

causar ao titular. No entanto, existem situações em que o tratamento desses dados é imprescindível, como informações sobre religião, que podem influenciar a disponibilidade para trabalhar em determinados dias, ou sobre filiações sindicais. (Giuntini et al, 2021).

A regra geral para que uma empresa trate qualquer dado pessoal é a observância da finalidade, pois quanto maior a quantidade de dados coletados, maior será o investimento necessário em seu tratamento e segurança (Giuntini et al, 2021).

3.4 Tratamento a dados de crianças e adolescentes

As empresas que empregam funcionários menores de idade precisam ter uma atenção especial com os dados desses indivíduos. De acordo com o artigo 14 da LGPD, os dados de crianças e adolescentes devem ser tratados visando o seu melhor interesse. Esse tratamento deve ser realizado mediante consentimento específico e destacado, fornecido por pelo menos um dos pais ou responsável legal. (Giuntini et al, 2021).

O § 1º do art. 14 da LGPD estabelece que o tratamento de dados pessoais de crianças deve ser realizado com consentimento específico e destacado, fornecido por pelo menos um dos pais ou responsável legal. Já o § 3º do mesmo artigo permite a coleta de dados de crianças sem esse consentimento quando for necessário para contatar os pais ou responsável legal ou para a proteção da criança. (Giuntini et al, 2021).

Há uma controvérsia significativa entre acadêmicos, profissionais da área e representantes da sociedade civil sobre a interpretação desses dispositivos, resultando em incerteza jurídica para os agentes de tratamento. Alguns órgãos públicos defendem que o consentimento é a única base legal adequada para o tratamento de dados de crianças, enquanto outros acreditam que outras hipóteses legais, como execução de políticas públicas e realização de estudos por órgãos de pesquisa, também podem legitimar o compartilhamento de dados. Além dessas interpretações, alguns atores sociais equiparam os dados de crianças e adolescentes a dados sensíveis, sugerindo que seu tratamento só poderia ocorrer com base nas hipóteses legais previstas no art. 11 da LGPD (ANPD, 2022).

3.5 Transferência de dados

A LGPD se aplica a todas as operações realizadas com dados pessoais, sejam online ou offline, abrangendo atividades como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, modificação, comunicação, transferência, difusão e extração (Sousa, 2021).

Figura 1: Operações realizadas com dados pessoais, sejam online ou offline

Fonte: Sousa, 2021, p. 12

A Lei nº 13.709/2018 não abrange os problemas relacionados à captação, tratamento e compartilhamento de dados na esfera penal. Ela exclui de seu âmbito os dados coletados exclusivamente para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, para os quais é necessária a edição de uma legislação específica. Na prática, isso deixa a interpretação dos ditames normativos sem um controle fundamental. Na esfera penal, os procedimentos de coleta, guarda, processamento, utilização ou transferência de dados pessoais abrangem não apenas os dados do autor ou da vítima

de uma infração, mas também os de outros agentes envolvidos, como testemunhas, peritos e terceiros sem relação direta com o fato, todos sujeitos à interferência do Estado (Ponte, 2022).

3.6 Responsabilidade civil sobre eventuais vazamentos

A responsabilidade civil na LGPD, regulamentada na Seção III do Capítulo VI, abrange a violação da "legislação de proteção de dados", que constitui um microssistema com normas previstas em diversas leis e normas administrativas. Essas normas podem ceder espaço a outras específicas, como o Código de Defesa do Consumidor, conforme o artigo 45 da LGPD. A responsabilidade surge do exercício da atividade de proteção de dados que viole essa legislação (Capanema, 2020). É necessário interpretar o artigo 42, caput, em conjunto com o artigo 44, parágrafo único, que dispõe: “Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano” (Capanema, 2020, p. 165).

O art. 46 da LGPD exige que os agentes de tratamento adotem medidas de segurança, técnicas e administrativas para proteger dados pessoais. Essas normas podem ser editadas pela ANPD e devem seguir padrões reconhecidos, como as normas ISO. A responsabilidade civil na LGPD pode surgir de duas situações: violação de normas jurídicas do microssistema de proteção de dados e violação de normas técnicas de segurança e proteção de dados pessoais. A responsabilidade civil só ocorre se essas violações causarem dano material ou moral ao titular ou à coletividade. O art. 42 limita a responsabilidade ao controlador ou ao operador, mas permite solidariedade em casos específicos, como quando o operador descumpre a legislação ou as instruções do controlador. A LGPD não menciona a responsabilidade do encarregado, mas esta pode surgir em relações consumeristas. O § 2º permite a inversão do ônus da prova a favor do titular dos dados, reconhecendo a hipossuficiência do titular e estabelecendo a responsabilidade civil objetiva, onde não se discute a culpa do agente (Capanema, 2020).

4 COMPARAÇÃO DA LGPD COM LEIS SIMILARES EM OUTROS PAÍSES

4.1 União Europeia e GDPR

Em 1981, a Convenção 108 reuniu membros do Conselho da Europa, como Islândia, Irlanda, Itália, Holanda e Noruega, para ampliar a proteção dos direitos e liberdades fundamentais, especialmente o direito à privacidade, em resposta ao crescente fluxo de dados pessoais transfronteiriços. Em 1995, a Diretiva 46 da Europa abordou temas semelhantes, estabelecendo legislações duradouras. Em abril de 2016, o Conselho Europeu aprovou o GDPR, com um período de dois anos para adequação. Em 2018, entrou em vigor o Regulamento 679/2016, conhecido como *General Data Protection Regulation* (GDPR), aprovado pelo congresso europeu em abril de 2016. Este regulamento aplica-se a todos os países membros da União Europeia e a qualquer empresa que ofereça bens e serviços aos residentes da UE, permitindo um período de adaptação até 25 de maio de 2018. Este regulamento inspirou diversas legislações globais, incluindo a Lei 13.709/2018 no Brasil, a CCPA na Califórnia, EUA, e a *Ley General de Protección de Datos Personales* no México. Atualmente, há mais de 100 leis de proteção de dados no mundo, que devem criar 75.000 empregos, com 28.000 concentrados na Europa (Soares; Silva, 2021).

Nos Estados Unidos, as leis de proteção de dados não são tão abrangentes quanto a LGPD e o GDPR, devido à estrutura federativa do país, onde estados têm autonomia sobre legislações sensíveis como pena de morte, legalização de drogas e proteção de dados. Em 1998, entrou em vigor a lei federal de Proteção à Privacidade de Crianças Online (COPPA). Em 2004, a Califórnia implementou a *California Online Privacy Protection Act* (CalOPPA), uma precursora do CCPA, que trata de dados online. A CalOPPA se aplica a qualquer site comercial que coleta informações pessoais de residentes na Califórnia, enquanto a CCPA é mais restritiva, aplicando-se a empresas que vendem dados pessoais, têm uma renda bruta de pelo menos 25 milhões de dólares, tratam dados de mais de 50 mil californianos ou obtêm 50% de sua receita da comercialização de dados pessoais (Soares; Silva, 2021).

4.2 Japão e APPI

A principal lei de proteção de dados no Japão é o Ato em Proteção da Informação Pessoal (APPI), promulgado em 2003, para proteger os direitos e interesses dos indivíduos. O APPI impõe obrigações para empresas e agentes que processam dados pessoais, conhecidos como Operadores de Negócios. A lei é dividida em setores privado e público, com subdivisões no setor público (Silva, 2023).

O APPI classifica informações pessoais em três categorias: informações pessoais gerais, dados pessoais, e dados pessoais retidos (mantidos por mais de 6 meses). A definição de informações pessoais foi ampliada em 2016 para incluir dados sensíveis e informações confidenciais, estabelecendo normas para o uso de dados anônimos e regulamentando a transferência de dados pessoais para o exterior. (Silva, 2023).

O APPI inclui disposições para aplicação extraterritorial e cooperação internacional. A Comissão de Proteção da Informação Pessoal (PPC) monitora o uso correto de dados pessoais. A lei é revisada sistematicamente a cada três anos para garantir que continue a atender às necessidades atuais de proteção de dados. (Silva, 2023).

4.3 Argentina e PDPA

A Lei de Proteção de Dados Pessoais 25.326 (PDPA) da Argentina, executada em 2000, visa proteger a privacidade dos dados pessoais e permitir acesso individual a informações em bancos de dados e registros públicos e privados. A Agência Argentina de Acesso à Informação Pública (AAIP) é responsável pela aplicação desta lei. A PDPA está alinhada com o modelo legislativo europeu e a Argentina foi o primeiro país da América Latina a obter uma qualificação de “adequação” para transferências de dados da UE. Em 2016, a AAIP emitiu a Provisão 60 E/2016, regulando as transferências internacionais de dados pessoais e aprovando formulários baseados no modelo europeu para controladores e processadores de dados.

Em julho de 2018, a Agência Argentina de Acesso à Informação Pública (ADPA) emitiu a Disposição 47/2018, que substituiu a Disposição N.º 11/2006 da Lei de Proteção de Dados Pessoais (PDPA). A nova Disposição 47 recomenda medidas de segurança alinhadas com as melhores práticas e padrões internacionais para proteger a confidencialidade e integridade dos dados pessoais desde a coleta até a exclusão. A resolução atualizou a lista de medidas e controles para a gestão, planejamento, controle e melhoria da segurança no processamento de dados pessoais, incluindo categorias como coleta de dados, controles de acesso, backup e recuperação, gestão de vulnerabilidade e incidentes de segurança. Também inclui medidas específicas para "dados confidenciais" (Monteiro et al, 2019).

5 APLICAÇÃO JURISPRUDENCIAL SOBRE CASOS RELACIONADOS À LGPD

O relator Wolney de Macedo Cordeiro, em 2022, julgou um mandado de segurança, abaixo descrito:

> MANDADO DE SEGURANÇA. DADOS SENSÍVEIS DO RECLAMANTE. ARTS. 2º, I e IV, e 5º, II, da LEI GERAL DE PROTEÇÃO DE DADOS (LGPD). SEGREDO DE JUSTIÇA APENAS SOBRE PEÇAS DA AÇÃO TRABALHISTA. SEGURANÇA PARCIALMENTE CONCEDIDA. Cabe ao julgador harmonizar a publicidade dos atos processuais com a proteção à vida privada do litigante, somente limitando a mencionada publicidade, nos lindes estritamente necessários à tutela dos direitos da personalidade das partes (arts. 5º, LXXIX, e 93, IX, da CF, c/c art. 2º, I e IV, da LGPD – Lei nº 13.709/2018). No caso em exame, não há necessidade de decretação de sigilo sobre a integralidade da reclamatória, ficando rechaçada a pretensão da parte impetrante nesse particular. Todavia, em relação a documentos que envolvam dados sensíveis do trabalhador (art. 5º, II, da LGPD), o sigilo se impõe. É que tais escritos dizem respeito à esfera de privacidade e intimidade do ora impetrante, sendo cabível a restrição de acesso a essas peças processuais específicas. Em todo caso, o controle de visibilidade dos documentos sigilosos deve permitir que ambas as partes, bem como os auxiliares da justiça (art. 149 do CPC), consigam visualizar os escritos. Segurança parcialmente concedida. (TRT-13 - MSCiv: 00004508620225130000, Relator: WOLNEY DE MACEDO CORDEIRO, Tribunal Pleno - Gabinete do Desembargador Wolney de Macedo Cordeiro)

Esta jurisprudência refere-se a um mandado de segurança no qual se discute a proteção de dados sensíveis do reclamante em uma ação trabalhista. A decisão se baseia na necessidade de harmonizar a publicidade dos atos processuais com a proteção à vida privada do litigante, conforme previsto na Constituição Federal e na Lei Geral de Proteção de Dados (LGPD). O julgador deve equilibrar a publicidade dos atos processuais com a proteção à vida privada dos litigantes, limitando a publicidade apenas nos limites necessários para proteger os direitos de personalidade das partes, conforme os artigos 5º, LXXIX, e 93, IX, da Constituição Federal, combinados com os artigos 2º, I e IV, da LGPD. No caso em questão, não é necessária a decretação de sigilo sobre a totalidade da ação trabalhista, rejeitando-se a pretensão da parte impetrante nesse aspecto. No entanto, documentos que contenham dados sensíveis do trabalhador devem ser mantidos em sigilo. Dados sensíveis, conforme o artigo 5º, II, da LGPD, referem-se a informações que afetam a esfera de privacidade e

intimidade do indivíduo, justificando a restrição de acesso a essas peças processuais específicas. O controle de visibilidade dos documentos sigilosos deve garantir que ambas as partes e os auxiliares da justiça (conforme o artigo 149 do CPC) tenham acesso aos escritos, assegurando o devido processo legal. A segurança foi parcialmente concedida, estabelecendo sigilo apenas sobre os documentos que envolvem dados sensíveis do trabalhador, enquanto o restante da ação permanece público.

Entende-se que a decisão demonstra a aplicação prática da LGPD em contextos judiciais, equilibrando a publicidade dos atos processuais com a proteção da privacidade e intimidade dos litigantes. O sigilo é imposto apenas sobre documentos que contenham dados sensíveis, garantindo o direito à privacidade do trabalhador, enquanto permite a transparência processual nos demais aspectos. Esta abordagem assegura a proteção dos direitos fundamentais dos indivíduos sem comprometer a integridade do processo judicial.

Em decisão proferida pelo relator Carlos Rodrigues Zahlouth Junior no ano de 2023 sobre o tema:

> OBTENÇÃO DA GEOLOCALIZAÇÃO DO CELULAR DO EMPREGADO COMO MEIO DE PROVA NO ÂMBITO DO PROCESSO DO TRABALHO. PRINCÍPIO DA PROPORCIONALIDADE. DIREITO À INVIOLABILIDADE DO SIGILO DOS DADOS E DAS COMUNICAÇÕES TELEFÔNICAS. DIREITO CONSTITUCIONAL FUNDAMENTAL DE ÍNDOLE INDIVIDUAL. CLÁUSULA PÉTREA (ART. 60, § 4º, INCISO IV, DA CF). NECESSIDADE DE CONSENTIMENTO DO EMPREGADO. O artigo 5º, inciso XII, da Constituição Federal, assegura a inviolabilidade do sigilo dos dados e das comunicações telefônicas, ressalvando apenas, quanto à última, a quebra do sigilo por ordem judicial em instrução processual penal ou em investigação criminal. Apesar de não ser absoluto, trata-se de direito constitucional fundamental de índole individual, além de cláusula pétrea, nos termos do artigo 60, § 4º, inciso IV, da CF. No plano infraconstitucional, a Lei Geral de Proteção de Dados assegura o respeito à privacidade à inviolabilidade da intimidade, notadamente quanto aos dados pessoais e sensíveis, nos termos dos artigos 2º, Ie IV, e 5º, Ie II, da Lei 13.709/18. No caso dos autos, a quebra de sigilo determinada viola o dispositivo constitucional por não ter por objetivo a instrução de processo penal ou a investigação criminal, tampouco direito postulado no juízo trabalhista que possa configurar ilícito de natureza penal. Assim, entende-se que a medida se mostra desproporcional e afrontosa à privacidade do trabalhador. Nesse diapasão, fixa-se a seguinte tese jurídica: "Não pode haver a quebra da geolocalização do celular do empregado sem a sua autorização, a fim de fazer prova em processo trabalhista, por violação aos direitos e garantias fundamentais do trabalhador." (TRT da 8ª Região; Processo: 0000613-07.2022.5.08.0000 IRDR; Data: 11/12/2023; Órgão Julgador: Pleno; Relator: CARLOS RODRIGUES ZAHLOUTH JUNIOR)

A jurisprudência em questão trata da obtenção da geolocalização do celular do empregado como meio de prova em processos trabalhistas. A análise gira em torno do princípio da proporcionalidade, do direito à inviolabilidade do sigilo dos dados e das comunicações telefônicas, e da necessidade de consentimento do empregado para tais medidas. O artigo 5º, inciso XII, da Constituição Federal, garante a inviolabilidade do sigilo dos dados e das comunicações telefônicas, excetuando apenas a quebra de sigilo por ordem judicial em instrução processual penal ou em investigação criminal. Este direito é considerado um direito constitucional fundamental de índole individual e é protegido como cláusula pétrea pelo artigo 60, § 4º, inciso IV, da Constituição, o que significa que não pode ser alterado por emendas constitucionais. A Lei Geral de Proteção de Dados (LGPD), Lei 13.709/18, reforça a proteção à privacidade e à inviolabilidade da intimidade, especialmente em relação a dados pessoais e sensíveis, conforme os artigos 2º, I e IV, e 5º, I e II. No caso analisado, a quebra do sigilo da geolocalização foi determinada fora do contexto de uma instrução processual penal ou investigação criminal. Não havia, portanto, base legal suficiente para tal medida no âmbito de um processo trabalhista. A medida foi considerada desproporcional e violadora da privacidade do trabalhador, pois não atendia aos critérios legais estabelecidos para a quebra de sigilo. A tese jurídica estabelecida é que não pode haver a quebra da geolocalização do celular do empregado sem a sua autorização para fazer prova em processo trabalhista. Isso se baseia na violação dos direitos e garantias fundamentais do trabalhador.

Assim, entende-se que a obtenção da geolocalização do celular do empregado sem consentimento no âmbito de processos trabalhistas é considerada desproporcional e afronta os direitos fundamentais de privacidade e sigilo de dados. A jurisprudência reforça a necessidade de consentimento explícito do empregado para tais medidas, protegendo assim os direitos constitucionais e as garantias previstas na LGPD.

Em outra decisão proferida pelo relator Ministro Edson Fachin, em 2024:

> EMENTA: AGRAVO REGIMENTAL NO RECURSO EXTRAORDINÁRIO COM AGRAVO. INTERPOSIÇÃO EM 10.03.2023. AÇÃO CIVIL PÚBLICA. INVESTIGAÇÃO. EXPLORAÇÃO DO TRABALHO DE CRIANÇAS E DE ADOLESCENTES. REQUISIÇÃO MINISTERIAL. FORNECIMENTO DE

> DADOS CADASTRAIS DE CLIENTE DE OPERADORA DE TELEFONIA. ALEGADA OFENSA AO ART. 5º, XII, DA CRFB. IMPROCEDÊNCIA. INAPLICABILIDADE DO TEMA 1148 DA REPERCUSSÃO GERAL. NOVA LEI GERAL DE PROTEÇÂO DE DADOS – LGPD. LEI Nº 13.709/2018. INOVAÇÃO EM SEDE DE AGRAVO REGIMENTAL. INVIABILIDADE. 1. A orientação jurisprudencial do STF assinala que a proteção a que se refere o art. 5º, XII, da Constituição da República é da comunicação de dados e, não, dos dados em si mesmos. 2. O acórdão vergastado está alinhado à jurisprudência desta Corte, que reconhece a diferença entre conteúdo de comunicações telemáticas e o mero registro de dados cadastrais de conta telefônica. 3. Inaplicável, portanto, o Tema 1148 da sistemática da repercussão geral, cujo paradigma é o RE 1.301.250-RG, ocasião em que foi reconhecida a repercussão geral da questão “limites para decretação judicial da quebra de sigilo de dados telemáticos, no âmbito de procedimentos penais, em relação a pessoas indeterminadas”. 4. A jurisprudência desta Corte é pacífica no sentido da impossibilidade de inovação em sede recursal. Precedentes. 5. Agravo regimental a que se nega provimento. Sem honorários, por se tratar de ação civil pública (art. 18 da Lei 7.347/1985). (STF - ARE: 1391865 MG, Relator: Min. EDSON FACHIN, Data de Julgamento: 14/02/2024, Segunda Turma, Data de Publicação: PROCESSO ELETRÔNICO DJe-s/n DIVULG 20-02-2024 PUBLIC 21-02-2024)

Esta decisão trata de um agravo regimental interposto em um recurso extraordinário com agravo, relacionado a uma ação civil pública que investiga a exploração do trabalho de crianças e adolescentes. O caso envolve a requisição ministerial de fornecimento de dados cadastrais de um cliente de operadora de telefonia. O recorrente alegou ofensa ao artigo 5º, XII, da Constituição Federal, que protege a inviolabilidade das comunicações telegráficas, de dados e das comunicações telefônicas, salvo por ordem judicial em instrução criminal ou investigação penal. O Supremo Tribunal Federal (STF) orienta que a proteção referida no art. 5º, XII, da Constituição, diz respeito à comunicação de dados e não aos dados em si. Ou seja, a inviolabilidade garantida é sobre o conteúdo das comunicações, e não sobre os registros cadastrais. O acórdão reafirma a jurisprudência que distingue entre o conteúdo das comunicações telemáticas (protegido pelo sigilo) e os dados cadastrais (não protegidos pelo sigilo). Neste caso, a solicitação envolvia apenas dados cadastrais de contas telefônicas, não violando assim o artigo 5º, XII. A jurisprudência não aplica o Tema 1148 da repercussão geral, relacionado aos limites para decretação judicial da quebra de sigilo de dados telemáticos em procedimentos penais. O caso em questão não envolve a quebra de sigilo de comunicações telemáticas, mas apenas o fornecimento de dados cadastrais. O STF reafirma que não é permitido introduzir novas questões em sede recursal, conforme precedentes jurisprudenciais. O agravo regimental foi negado, mantendo-se a decisão anterior,

sem concessão de honorários, dado tratar-se de uma ação civil pública conforme o artigo 18 da Lei 7.347/1985.

Entende-se que a decisão analisada reflete a posição do STF de que a proteção constitucional do sigilo das comunicações não se estende aos dados cadastrais. Assim, a requisição ministerial de dados cadastrais para investigação de exploração do trabalho infantil não viola o artigo 5º, XII, da Constituição. Além disso, não é possível inovar em sede recursal, mantendo-se a decisão de fornecer os dados cadastrais sem violação de direitos fundamentais ou da LGPD.

CONCLUSÃO

A Lei Geral de Proteção de Dados Pessoais (LGPD), sancionada pela Lei nº 13.709/2018, representa uma transformação significativa no panorama jurídico brasileiro e nas relações sociais e profissionais. Inspirada em legislações internacionais, como o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, a LGPD estabelece diretrizes claras para o tratamento de dados pessoais, garantindo maior segurança e privacidade para os indivíduos.

A LGPD traz um marco regulatório robusto que impacta diversas áreas do direito brasileiro. No direito civil, a lei impõe que os contratos envolvendo tratamento de dados pessoais sejam revisados para assegurar conformidade com os novos requisitos legais, incluindo cláusulas sobre consentimento, finalidade e segurança dos dados.

No âmbito do direito do consumidor, a LGPD fortalece os direitos dos consumidores, impondo às empresas a obrigação de informar claramente como os dados serão utilizados e garantindo aos consumidores o direito ao acesso, correção e exclusão dos dados pessoais.

Além disso, a LGPD influencia o direito penal ao introduzir sanções administrativas para o tratamento inadequado de dados pessoais e potencialmente afetar a tipificação de crimes relacionados à privacidade e proteção de dados.

No direito do trabalho, a LGPD impõe novas regras sobre a coleta e armazenamento de dados pessoais de funcionários, exigindo que empregadores justifiquem a coleta de dados sensíveis e adotem medidas adequadas para proteger esses dados.

A LGPD promove uma cultura de privacidade e aumenta a confiança dos cidadãos nas instituições. Ao garantir que os dados pessoais sejam protegidos, a lei fortalece a confiança nas interações digitais e no compartilhamento de informações. Este aumento da confiança é essencial em uma era onde a digitalização é onipresente e os dados pessoais são coletados e processados constantemente.

A conscientização pública sobre a importância da proteção de dados também é elevada. Indivíduos tornam-se mais cientes de seus direitos e mais críticos em relação às práticas de coleta e uso de dados pelas empresas e outras entidades. Isso

resulta em uma sociedade mais informada e exigente quanto à transparência e responsabilidade no tratamento de dados pessoais.

Para as empresas, a LGPD exige a implementação de políticas de compliance e governança de dados. Isso inclui a criação de programas de treinamento, a nomeação de um encarregado de proteção de dados (DPO) e a adoção de medidas técnicas e organizacionais adequadas. As empresas devem revisar e, muitas vezes, reformular seus processos e procedimentos internos relacionados ao tratamento de dados pessoais, desde a coleta de consentimentos explícitos até a realização de avaliações de impacto à proteção de dados (DPIA).

A conformidade com a LGPD também representa um diferencial competitivo no mercado. Empresas que demonstram um compromisso sério com a proteção de dados podem ganhar a confiança de consumidores e parceiros de negócios, o que pode se traduzir em vantagens comerciais significativas.

No mercado de trabalho, a demanda por profissionais especializados em proteção de dados e cibersegurança cresce exponencialmente. A necessidade de compliance com a LGPD cria novas oportunidades de emprego e valoriza profissionais com conhecimentos específicos em regulamentações de privacidade.

Apesar dos avanços, a implementação da LGPD enfrenta desafios significativos. Muitas empresas ainda estão em processo de adaptação e precisam investir em tecnologias, treinamento e processos para garantir a conformidade. A Autoridade Nacional de Proteção de Dados (ANPD) desempenha um papel crucial na orientação e fiscalização do cumprimento da lei.

Além disso, a LGPD deve ser continuamente atualizada para acompanhar as rápidas evoluções tecnológicas e as novas formas de coleta e processamento de dados. O diálogo constante entre legisladores, autoridades reguladoras, empresas e a sociedade civil é fundamental para garantir que a legislação continue relevante e eficaz na proteção dos dados pessoais.

Assim, entende-se que a LGPD marca uma era de maior proteção e responsabilidade no tratamento de dados pessoais no Brasil. Seus impactos são profundos e abrangentes, afetando o direito brasileiro, as relações sociais e profissionais de maneira significativa. A lei fortalece a proteção dos direitos fundamentais de privacidade, liberdade e o livre desenvolvimento da personalidade,

ao mesmo tempo em que promove uma cultura de respeito e responsabilidade no tratamento de dados pessoais. A implementação eficaz da LGPD é essencial para garantir que o Brasil esteja alinhado com as melhores práticas globais de proteção de dados e privacidade, proporcionando um ambiente mais seguro e confiável para todos.

REFERENCIAS

AGÊNCIA BRASIL. Entenda o Marco Civil da Internet. Disponível em <http://www.em.com.br/app/noticia/politica/2014/04/26/interna_politica,522910/entenda-o-marco-civil-da-internet.shtml. acesso em jun. 2024.

ANPD. Hipóteses legais aplicáveis ao tratamento de dados pessoais de crianças e adolescentes. 2022. Disponivel em https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/estudo-preliminar-tratamento-de-dados-crianca-e-adolescente.pdf acesso em jun. 2024.

BARROS, Augusto Paes de. Gestão de risco. In: CABRAL, Carlos; CAPRINO, Willian (org.). Trilhas em segurança da informação, caminhos e ideias para a proteção de dados. Rio de Janeiro: Brasport, 2015.

BRASIL. LEI Nº 12.965, DE 23 DE ABRIL DE 2014 Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponivel em https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm acessoem jun. 2024.

BRASIL. CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988. Disponivel em https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm acesso em jun. 2024.

BRASIL. LEI Nº 13.709, DE 14 DE AGOSTO DE 2018 Lei Geral de Proteção de Dados Pessoais (LGPD). Disponivel em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm acesso em jun. 2024.

CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. Cadernos Jurídicos, São Paulo, ano 21, nº 53, p. 163-170, Janeiro-Março/2020

CARVALHO, Gisele Primo; PEDRINI, Tainá Fernanda. Direito à privacidade na Lei Geral de Proteção de Dados Pessoais. Revista da Esmesc, v.26, n.32, p. 363-382 , 2019

CAVALCANTI, Natália Peppi; SANTOS, Luiza Mendonça da Silva Belo. A Lei Geral de Proteção de Dados do Brasil na era do Big Data. In: Tecnologia Jurídica & Direito Digital - II Congresso Internacional de Direito, Governo e Tecnologia. 2018.

COMISSÃO Nacional de Proteção de Dados (CNPD). Rede Ibero-Americana. Disponivel em https://www.cnpd.pt/internacional/rede-ibero-americana/ acesso em jun. 2024.

ESTEVÃO, Luciana Costa; LIMA, Stephane Kelly da Silva; SILVA, Luanjir Luna da. A Lei Geral de Proteção de Dados (LGPD) no âmbito das relações trabalhistas: conceitos, impactos e suas implicações. Revista Brasileira de Direito Social - RBDS, v. 5, n. 2, p. 63-74, 2022.

FRAZÃO, Ana. A nova lei geral de proteção de dados pessoais. 2018. Disponivel em http://www.professoraanafrazao.com.br/files/publicacoes/2018-11-07-A_nova_Lei_Geral_de_Protecao_de_Dados_Pessoais_Principais_repercussoes_para_a_atividade_empresarial_direito_a_portabilidade_Parte_XI.pdf acesso em jun. 2024.

GIUNTINI, Adriana et al. LGPD nas relações de trabalho. 1.ed. Salvador, BA: Motres, 2021. PDF. 1.ed. Vários autores. Bibliografia.

GOVERNO DIGITAL. Guia de boas práticas Lei Geral de Proteção de Dados (LGPD). Agosto, 2020. Disponivel em https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias/guia_lgpd.pdf acesso em jun. 2024.

JURISPRUDENCIA. TRT-8 - IRDR: 0000613-07.2022.5.08.0000, Relator: CARLOS RODRIGUES ZAHLOUTH JUNIOR, Pleno, Data de Publicação: 11/12/2023. Disponivel em https://www.jusbrasil.com.br/jurisprudencia/trt-8/2099932545 acesso em jun. 2024.

JURISPRUDENCIA TRT-13 - MSCiv: 00004508620225130000, Relator: WOLNEY DE MACEDO CORDEIRO, Tribunal Pleno - Gabinete do Desembargador Wolney de Macedo Cordeiro. Disponivel em https://www.jusbrasil.com.br/jurisprudencia/trt-13/1854186169 acesso em jun. 2024.

JURISPRUDENCIA STF - ARE: 1391865 MG, Relator: Min. EDSON FACHIN, Data de Julgamento: 14/02/2024, Segunda Turma, Data de Publicação: PROCESSO ELETRÔNICO DJe-s/n DIVULG 20-02-2024 PUBLIC 21-02-2024. Disponivel em https://www.jusbrasil.com.br/jurisprudencia/stf/2174949707 acesso em jun. 2024.

LEARN.MICROSOFT. Lei de Proteção de Dados Pessoais da Argentina (PDPA). 2024. Disponivel em https://learn.microsoft.com/pt-br/compliance/regulatory/offering-pdpa-argentina acesso em jun. 2024.

LIGATI, Lys Nunes; ALMEIDA, Juliana Evangelista de. Da evolução das legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa. Revista de Direito, v. 12, n. 02, pp. 1-33, 2020.

MACÁRIO, Lincoln; FERRICHE, Elisabel. Marco civil da internet: relator mantém parecer e quer votação na semana que vem. (2014). Disponível em <http://www2.camara.leg.br/camaranoticias/radio/materias/COM-A-

PALAVRA/461437-MARCO-CIVIL-DA-INTERNET-RELATOR-MANTEM-PARECER-E-QUER-VOTACAO-NA-SEMANA-QUE-VEM.html. acesso em jun. 2024.

MATTIA, Elaine Renata Sabi. Os Desafios da Adequação à LGPD nas Relações de Trabalho. (2021). Disponível em <https://www.sabi.adv.br/blog/www-sabi-adv-br. acesso em jun. 2024.

MELO, M. M. D. de. Divulgação de práticas de compliance anticorrupção e fases da vantagem competitiva transitória: um estudo em companhias abertas brasileiras. (Tese de Doutorado). Universidade Federal do Rio Grande do Norte, Natal, RN, Brasil. 2019. Disponivel em https://repositorio.ufrn.br/jspui/handle/123456789/27566. acesso em jun. 2024.

MONTEIRO, Renato Leite; GOMES, Maria Cecília Oliveira; NOVAES, Adriane Loureiro; MORIBE, Gabriela; CAMARA, Eduardo Gonsales et al. Lei Geral de Proteção de Dados e GDPR. Disponivel emhttps://baptistaluz.com.br/wp-content/uploads/2019/01/RD-DataProtection-ProvF.pdf acesso em jun. 2024.

OLIVEIRA, Patrícia de Lima de. Impactos da lei geral de proteção de dados nas relações do trabalho. 68 fl. 2021. Monografia (Bacharel em Direito). FSG Centro Universitário. Caxias do Sul/RS, 2021.

PINHEIRO, Patricia Peck. Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018: LGPD. São Paulo: Saraiva, 2018

PONTE, Amanda Leite de Farias. Da necessidade de limites ao tratamento e compartilhamento de dados por órgãos de inteligência do estado à luz da lei geral de proteção de dados em matéria penal. Disponivel em https://www.portaldeperiodicos.idp.edu.br/cadernovirtual/article/download/6481/2718 acesso em jun. 2024.

SANTOS, Viviane Bezerra de Menezes. Lei Geral de Proteção de Dados: fundamentos e compliance. (2019). Disponível em <https://repositorio.ufc.br/bitstream/riufc/49370/1/2019_tcc_vbmsantos.pdf. acesso em jun. 2024.

SILVA, Jefferson Lucas Rodrigues da. Proteção de Dados no Brasil e no Japão. 2023. Disponivel em https://www.jusbrasil.com.br/artigos/protecao-de-dados-no-brasil-e-no-japao/1778739928 acesso em jun. 2024.

SOARES, Igor Raphael Guimarães; SILVA, Cláudio R. M. da. Breve Análise Comparativa das Principais Normas Internacionais sobre Proteção de Dados Pessoais. Natal, 2021. Disponivel em https://repositorio.ufrn.br/bitstream/123456789/48207/1/BreveAnaliseProtecaoDados Pessoais_Soares_2021.pdf acesso em jun. 2024.

SOUSA, Nadya Rodrigues Gomes de. Guia Rápido da LGPD. 2021 Disponivel em https://escola.mpu.mp.br/transparencia/lei-geral-de-protecao-de-dados/guiarapidolgpd.pdf acesso em jun. 2024.

VERÍSSIMO, Carla. Compliance: incentivo à adoção de medidas anticorrupção. São Paulo: Saraiva, 2017.

WIRELESS BRASIL. Marco Civil da Internet: o que muda na sua vida. (2012). Disponível em <http://www.wirelessbrasil.org/bloco/websites_tecnologia/crimes_digitais_marco_civil/artigos_noticias/2012/nov_21e.html. acesso em jun. 2024.