FUNDAÇÃO EDUCACIONAL DE ITUVERAVA
FACULDADE DR. FRANCISCO MAEDA

Hernandes Vicente Torres

COMPLIANCE NAS EMPRESAS E AS NOVAS DIRETRIZES TRAÇADAS PELA LGPD

ITUVERAVA
2022

HERNANDES VICENTE TORRES

COMPLIANCE NAS EMPRESAS E AS NOVAS DIRETRIZES TRAÇADAS PELA LGPD.

Trabalho de Conclusão de Curso apresentado à Faculdade Dr. Francisco Maeda. Fundação Educacional de Ituverava para a obtenção do título de Bacharel em Direito.

Orientador: Prof. Me. Cristina Elena Bernardi Iaroszeski.

ITUVERAVA
2022

HERNANDES VICENTE TORRES

COMPLIANCE NAS EMPRESAS E AS NOVAS DIRETRIZES TRAÇADAS PELA LGPD.

Trabalho de Conclusão de Curso apresentado à Faculdade Dr. Francisco Maeda. Fundação Educacional de Ituverava para a obtenção do título de Bacharel em Direito.

Ituverava, _____de _____de _____.

Orientador (a): _____
Prof. Me. Cristina Elena Bernardi Iaroszeski

Examinador (a): _____
Nome do Examinador (a)

Examinador (a): _____
Nome do Examinador (a)

AGRADECIMENTOS

Em primeiro lugar, a Deus, por ter permitido que eu tivesse saúde e determinação, para superar todos os obstáculos durante todos os meus anos de estudos.

Aos familiares, Silvia, Lucas e Alcides por todo o apoio e pela ajuda, que muito contribuiu para a realização deste trabalho, sempre incentivando nos momentos difíceis e compreendendo a minha ausência enquanto eu me dedicava à realização deste trabalho.

Aos professores, pelos ensinamentos que me permitiram apresentar um melhor desempenho no meu processo de formação profissional ao longo do curso.

DEDICATÓRIA

Dedico esta monografia inteiramente à minha professora orientadora Cristina Iaroszeski, que sempre me manteve focado e na trilha certa para a conclusão satisfatória deste projeto. Grato pela sua orientação preciosa.

COMPLIANCE NAS EMPRESAS E AS NOVAS DIRETRIZES TRAÇADAS PELA LGPD

Hernandes Torres[1]
Cristina Bernardi Iaroszeski[2]

RESUMO: Os programas de *compliance* consistem na reestruturação do ambiente corporativo através de normas de conduta que estabelecem a autorregulação e sua autorresponsabilidade, buscando promover o combate à corrupção. Assim, esta pesquisa objetiva exibir a importância dos programas de *compliance* como ferramenta de autorregulação para as organizações livrarem-se de quaisquer ilícitos corporativos. Para tanto, este trabalho tem o intuito específico de apresentar os conceitos e a relevância dos sistemas de *compliance* e governança corporativa, exibindo os fundamentos da Lei Geral de Proteção de Dados, relacionando e correlacionando as responsabilidades civil, penal e administrativa das organizações que introduzem o sistema de *compliance* em suas empresas. Sendo assim, esta pesquisa se justifica devido à importância de se verificar a conexão entre o direito empresarial e o sistema de *compliance* na apresentação de uma governança corporativa transparente. Para a concretização deste trabalho, realizou-se uma pesquisa bibliográfica crítica através de doutrina, artigos científicos, legislação vigente.

Palavras-chave: Regulação, Procedimentos, Fraudes, Corrupção.

COMPLIANCE IN COMPANIES AND THE NEW GUIDELINES DRAWN BY LGPD

SUMMARY: *Compliance* programs consist of restructuring the corporate environment through rules of conduct that establish self-regulation and self-responsibility, seeking to promote the fight against corruption. Thus, this research aims to show the importance of *compliance* programs as a self-regulation tool for organizations to get rid of any corporate wrongdoing. Therefore, this work has the specific purpose of presenting the concepts and relevance of *compliance* and corporate governance systems; showing the fundamentals of the General Data Protection Law relating and correlating the civil, criminal, and administrative responsibilities of organizations that introduce the *compliance* system in their companies. Therefore, this research is justified due to the importance of verifying the connection between business law and the *compliance* system in the presentation of transparent corporate governance. For the accomplishment of this work, critical bibliographic research was carried out through doctrine, scientific articles, current legislation.

Keywords: Regulation, Procedures, Fraud, Corruption.

1. INTRODUÇÃO

O Brasil tem, ao longo de sua história, desde sua colonização, apresentado inúmeros escândalos de corrupção tanto na política quanto em sua economia nacional. Entretanto, a

[1] Graduando em Direito pela Faculdade Dr. Francisco Maeda – FAFRAM. E-mail: hernandestorres@hotmail.com
[2] Professora de Bacharelado em Direito pela Faculdade Dr. Francisco Maeda – FAFRAM. E-mail: cristina.iaroszeski@fafram.com.br.

corrupção não acontece somente neste país, ela é um problema mundial ocasionado pela intensificação das transações econômicas entre os países e pela busca por resultados positivos e lucratividades sempre maiores.

Diante de tais circunstâncias, o Brasil promulgou em 2013 a Lei nº 12.846, denominada Lei Anticorrupção, que tem como intuito responsabilizar civil e administrativamente as organizações e seus gestores assegurando que seus negócios e parceiros comerciais passem a adotar normas que reduzam o risco de corrupção. Dentre as ferramentas existentes no ambiente empresarial, têm-se a adoção de prestação de contas e o sistema de *compliance.*

No âmbito empresarial, os bens mais valorizados pelas organizações são seu nome, sua marca e sua imagem. Com a globalização, esses três bens passaram a sobrepor todo o ativo tangível de uma empresa. O impacto de uma exposição negativa no mercado ou perante um agente regular é capaz de comprometer diretamente a reputação da organização, trazendo consequências como perda de clientes, novos negócios, redução de seus resultados e lucros. Diante da evolução tecnológica da comunicação, as organizações podem ter sua reputação comprometida mundialmente em questão de minutos.

Para manter seu valor no mercado, as organizações estão aderindo ao emprego de ferramentas que sejam capazes de assegurar a ética em seus negócios, garantindo sua reputação e integridade. Visto que a governança corporativa transparente é um requisito básico para a sobrevivência e perenidade das organizações, estas estão aderindo aos sistemas de *compliance.*

O *compliance,* ou programas de integridade, consiste em fazer cumprir as leis, diretrizes, normas internas e externas de uma organização, com o intuito de reduzir os riscos associados ao negócio da empresa procurando prevalecer a ética e cumprimento dos regulamentos e procedimentos organizacionais.

Além do atendimento da Lei Anticorrupção, os programas de *compliance* são tidos como uma ferramenta importantíssima para que as organizações se estruturem e cumpram a normas estabelecidas pela 13.709/18, LGPD Lei Geral de Proteção de Dados Pessoais em vigor desde agosto de 2020. A LGPD busca proteger os direitos fundamentais de liberdade e privacidade, bem como o desenvolvimento da personalidade da pessoa natural diante dos serviços ofertados atualmente, que têm por característica uma constante coleta de dados de seus usuários. Assim, a LGPD obriga as empresas a gerenciarem e registrarem os tratamentos de dados pessoais de seus clientes e funcionários, disponibilizando uma maior segurança jurídica.

Supõem-se que para manter seu valor no mercado, as organizações buscam através da *compliance* em seus negócios assegurar sua reputação e integridade.

Dessa forma, esta pesquisa se justifica devido à importância de se verificar a conexão entre o direito empresarial e o sistema de *compliance* na apresentação de uma governança corporativa transparente, atualmente um requisito básico para a sobrevivência e perenidade das organizações.

A presente pesquisa possui por objetivo geral apresentar a importância dos programas de *compliance* como ferramenta de autorregulação para as organizações se precaverem de ilícitos corporativos. Já os objetivos específicos consistem em exibir os conceitos e a importância do sistema de *compliance* e governança corporativa, apresentar os fundamentos da LGPD e correlacionar as responsabilidades civil, penal e administrativa das organizações que aderem ao sistema de *compliance*.

Para a concretização deste trabalho, foi realizada uma pesquisa bibliográfica crítica através do emprego de doutrina, artigos científicos, leis e jurisprudências.

Assim, este artigo apresenta a introdução do trabalho, no tópico dois serão expostos os conceitos de *compliance* e sua importância como ferramenta de governança corporativa. Na terceira seção, serão exibidos os fundamentos da Lei LGPD e será correlacionada a LGPD com a responsabilidades civil, penal e administrativa das organizações que aderem ao sistema de *compliance*. O último tópico apresenta as considerações finais do artigo.

2. *COMPLIANCE* NAS EMPRESAS

A *compliance* refere-se a um conjunto de mecanismos que exigem que uma organização previna, identifique e corrija os riscos de praticar atos ilegais ou irregulares, sejam eles ocorridos dentro da empresa ou fora dela. O sistema de *compliance* vai além da mera formalidade, é por meio dessa ferramenta que as empresas buscam preservar seus negócios e interesses.

O impacto ocasionado pelos escândalos de corrupção vivenciados no Brasil especialmente com o Petrolão e a Lava-Jato, fez com que as empresas públicas e privadas buscassem por maior transparência em suas gestões e prestação de contas através da adoção de programas de *compliance.* A implementação dessa ferramenta está associada à conformidade e à busca pela excelência na execução de todos os processos da empresa, assim, a instituição que adere a esse programa apresenta maior transparência em suas prestações de contas, bem como não mede esforços para manter a imagem da empresa livre de ligações com

fraudes e esquemas de corrupção, atuando no mercado com responsabilidade fiscal e social, respeitando as leis vigentes (SOUZA; ALVES, 2021).

Assim, pode-se afirmar que ao se aderir a um programa de *compliance*, as empresas estão reduzindo risco da ocorrência de condutas ilícitas por parte de seus administradores e colaboradores, além do mais, o efetivo programa diante de uma violação às normas é capaz de identificar o ato, buscando investigar e remediar. É por meio da *compliance* que as empresas asseguram a qualidade de sua imagem e de sua atuação no mercado bem, como reduzem gastos com multas, punições e cobranças judiciais.

Assim a *compliance* é tida como um conjunto de normas legais, regras disciplinares e diretrizes estabelecidas para as operações e atividades de uma empresa, com o objetivo de prevenir, detectar e tratar desvios ou inconsistências. Com origem nos Estados Unidos, em 1913, nas instituições financeiras que buscavam a formação de um sistema financeiro mais flexível, seguro e estável, os programas de *compliance* se baseiam, fundamentalmente, em mecanismos e procedimentos internos, auditorias e estímulo à denúncia de desvios e na aplicação eficaz de códigos de ética (CLAMER, 2018).

Roberto Clamer (2018) ressalta em seu estudo que a ferramenta de *compliance* não se apresenta apenas como uma medida preventiva baseada no estabelecimento de controles internos e medidas que podem ajudar a corporação a evitar processos criminais. É tida também, como um sistema investigativo, podendo ampliar seus efeitos no âmbito civil, penal e trabalhista. Como resultado, a *compliance* é utilizada pelas organizações para prevenir e detectar comportamentos criminosos, ilegais e fraudulentos, bem como para promover uma cultura que incentive a conformidade legal e o comportamento ético. Após sua implementação, as empresas necessitam ter estruturas disciplinares para a ocorrência de infrações à legislação anticorrupção e ao próprio programa, como a adoção de canais de denúncias sobre suspeitas de condutas inadequadas.

O programa de *compliance* considera as características únicas de cada empresa, levando em consideração seu setor de atuação e localidade. Como resultado, assegura que a empresa explore todo o seu potencial, respeitando a legislação. Exige uma fiscalização das atividades realizadas pelos colaboradores dentro da empresa, estabelece atenuantes previstos na lei, que são acatados nas penalidades a serem aplicadas, até mesmo nos acordos de leniências. Se uma organização puder demonstrar que tomou todas as precauções para evitar o suposto ato de corrupção, a qual está sendo acusada, estará sujeita poderá ser isenta ou reduzida sua penalidade (ANDRADE; RODRIGUES, 2019).

Jacqueline Vasconcelos Leoni e Viviane Coêlho Séllos-Knoerr (2020), enfatizam a importância da *compliance* como uma ferramenta de defesa para uma gestão corporativa eficaz. Esse sistema age especialmente monitorando e prevendo riscos associados a: quebras legais e regulatórias; impactos negativos da imagem e reputação; atos ilícitos associados à corrupção, lavagem de dinheiro e suborno; falhas no cumprimento da legislação do ramo que atua entre outros riscos. A *compliance* e a governança corporativa são intimamente interligadas, visto que optar pela implementação de um programa de *compliance* eficaz faz parte de uma decisão de gestão, determinando, assim, a forma com que as empresas serão administradas e como as decisões de gestão são tomadas.

A *compliance* deve ser estruturada e implementada de forma adequada, observando o tamanho e o ramo de cada empresa e operação, bem como cinco pilares específicos:

> I. Comprometimento e apoio da Alta Administração: condição essencial para garantir a efetividade do programa;
> II. Instância responsável pelo programa de integridade: deve possuir autonomia, independência, recursos e garantia de imparcialidade;
> III. Análise de perfil e riscos: a empresa deve ter pleno conhecimento do setor em que atua;
> IV. Estrutura de regras e instrumentos: devem ser elaborados instrumentos normativos para dar suporte ao programa, como o código de ética, políticas de risco e de controle interno, por exemplo;
> V. Estratégias de monitoramento contínuo: com a finalidade de garantir a efetividade do programa. (LIMA, 2019, p. 16)

Assim, todos os pilares apresentados são essenciais para a excelência da implantação da *compliance* em uma empresa, devendo ser adotadas estratégias de monitoramento contínuo e medidas disciplinares caso ocorram infrações à legislação, e ao próprio programa.

Cabe ressaltar, que a *compliance* contribui para a organização interna das empresas, concretizando sua missão, visão e valores. Entretanto, a implementação desse programa apresenta dificuldades, visto a vasta abrangência de normas reguladoras: civil, trabalhista, tributária, penal, ambiental entre outras esferas, a fim de evitar atos ilícitos. A *compliance* não deve ser confundida com a simples observância de regras formais e informativas, pois seu objetivo é muito mais amplo, ou seja, consiste em um conjunto de normas, modelos, procedimentos éticos e legais, que, ao ser implementado, torna-se a linha de orientação da conduta da empresa e de seus colaboradores, no mercado em que atua (LIMA, 2019).

Sendo assim, a *compliance* é tida como um programa de integridade, que promove a implantação de mecanismos de controle interno nos negócios por meio da gestão de riscos e da utilização de instrumentos que garantam o cumprimento de leis e regulamentos,

promovendo, através dos princípios éticos, uma melhor visibilidade da empresa que adota esse programa no segmento em que atua.

Atualmente, a *compliance* é o principal programa empregado pelas empresas brasileiras para se adequarem às especificidades da Lei Geral de Proteção de Dados, Lei nº 13.709 de 2018, a qual busca definir parâmetros de processamento de dados mais seguros e confiáveis, além de garantir mais transparência e privacidade para os indivíduos, responsabilizando as empresas que vierem a expor os dados, sejam de seus clientes, de fornecedores ou de seus próprios colaboradores.

3. TRANSPARÊNCIA SOBRE VAZAMENTO DE DADOS POR PARTE DAS EMPRESAS

3.1 A LGPD

Os avanços tecnológicos e a globalização resultaram em um grande fluxo de negócios, um aumento na troca de informações e o surgimento de negócios digitais. Os negócios digitais, por sua vez, garantiram que a informação se tornasse cada vez mais crucial para a tomada de decisões, para isso, passaram a armazená-las em bancos de dados.

Assim, deter a informação na era do Big Data (área da Tecnologia da Informação TI responsável por realizar o tratamento, processamento e armazenamento de grandes conjuntos de dados) representa deter poder. Todas as pessoas são influenciadas diretamente pela produção, armazenamento e tratamento de dados. Nos últimos anos, a indústria do banco de dados é responsável por direcionar a tomada de decisões do segmento empresarial ao político. Entretanto, a circulação de dados privados pode colocar em risco a pessoa natural ou jurídica que está associada a esses dados, se considerar a forma que são manipulados esses dados (GARCEL *et al*., 2020).

Santos (2019) apresenta em seu estudo os principais conceitos abordados pela LGPD. A autora conceitua dados, no sentido desta pesquisa, como todas as informações que detêm o poder de identificar um indivíduo, podendo ser fatos, conceitos, sinais, números entre outros, desde que possam ser ordenadas, transmitidas, analisadas e processadas. Segundo a autora, dados pessoais são informações sobre uma pessoa que foi ou pode vir a ser identificada através de dados de identificação, sobre sua localidade, sua genética, entre outros. Já dados pessoais sensíveis, referem-se à etnia, religião, posicionamento sobre política, filosofia, opção sexual, entre outros.

É importante ressaltar que dados incorretos, ou mentiras sobre uma pessoa, também são considerados dados pessoais, e o meio em que a informação é veiculada não é importante, ou seja, a informação na forma de texto, foto, vídeo, áudio ou qualquer outro meio é permitida pela nova lei.

Um dado pessoal pode deixar de ser protegido pela lei caso seja anonimizado, com a "utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação direta ou indireta a um indivíduo" (BRASIL, 2018, Art. 5º, III e XI).

Já o processamento, ou tratamento, de dados possui o conceito mais abrangente de toda a lei: consiste no processamento significativo de qualquer operação ou conjunto de operações automatizadas ou não, assim, todos os processamentos que envolvam dados de terceiros são abrangidos pela lei (GOMES, 2019).

Portanto, temos uma personalização do conceito, o que o leva a estar vinculado a questões jurídicas como a privacidade e o direito ao esquecimento, por exemplo. Entretanto, o Brasil não possuía uma definição para dados até a promulgação da Lei nº 13.709, Lei Geral de Proteção de Dados, fundamentada com base na Diretiva nº 9/46/CE da União Europeia, de 24 de outubro de 1995, e o Regulamento Geral de sobre a Proteção de Dados (RGPD) 2016/679, promulgado em 2018, que regulamenta a questão da privacidade e a proteção de dados pessoais, em toda União Europeia e Espaço Econômico Europeu (SANTOS, 2019).

Diante da relevância dos dados pessoais para um indivíduo, é razoável que a LGPD se sinta compelida a protegê-los com rigor, baseada nos princípios constitucionais, tutelando o direito à privacidade, resguardando também o direito de informação previstos na Constituição Federal da República Federativa do Brasil de 1988 (CF/88), em seu artigo 5º, incisos X e XIV:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: […]
> X - São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; […]
> XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional; […].

A interpretação do dispositivo constitucional revela que não há razão para retirar a proteção à intimidação nas situações em que a pessoa é mais vulnerável. Essa vulnerabilidade

é destacada pelo entendimento de que os bancos de dados fornecem um risco constante e diário para todas as cidades (SANTOS, 2019).

A LGPD reflete a estrutura das regulamentações de proteção de dados existentes, incluindo o assunto em uma legislação específica para tratar das questões mais importantes para a organização. No âmbito da proteção de dados pessoais, os fundamentos e objetivos da LGPD encontram-se em seus artigos 1º e 2º, indica seu objetivo e seus fundamentos:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I - O respeito à privacidade;
> II - A autodeterminação informativa;
> III - A liberdade de expressão, de informação, de comunicação e de opinião;
> IV - A inviolabilidade da intimidade, da honra e da imagem;
> V - O desenvolvimento econômico e tecnológico e a inovação;
> VI - A livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII - Os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Os fundamentos apresentados no art. 2º, apresenta o objetivo central da LGPD, o qual consiste em assegurar que o titular dos dados tenha o conhecimento que seus dados que estão sendo acessados e armazenados, possibilitando a todos a segurança do tratamento de suas informações, bem como ao acesso a elas, se for requisitado.

Murari, Schiavon e Barretos (2021), em seu artigo, fazem uma síntese sobre os princípios fundamentais da LGPD. De acordo com as autoras, o princípio da finalidade na LGPD refere-se ao tratamento para fins explícitos, específicos e legais, informando o titular e proibindo tratamento posterior incompatível com esses fins, a fim de garantir a equidade no tratamento dos dados pessoais de cada titular. O princípio da necessidade, por outro lado, busca restringir o tratamento ao mínimo necessário para atingir as metas de forma proporcional e não excessiva. De acordo com a LGPD, o princípio da adequação trata da compatibilidade entre o tratamento e os objetivos para os quais o indivíduo foi informado.

Os tratamentos de dados devem ser pautados obedecendo os princípios da adequação e da necessidade, buscando estabelecer os limites do seu tratamento para o atendimento da finalidade proposta.

Segundo Murari, Schiavon e Barretos (2021), o princípio do livre acesso tem como objetivo a prestação de uma consulta cômoda e gratuita ao titular em matéria de tratamento e integridade dos seus dados pessoais. Da mesma forma, o princípio da qualidade dos dados

busca garantir ao titular a exatidão, clareza e relevância dos dados, de acordo com a necessidade e finalidade do tratamento. Além disso, o princípio da transparência tem como escopo assegurar que o indivíduo receba informações claras, acessíveis e necessárias sobre o tratamento, observadas as salvaguardas comerciais e industriais. O princípio da segurança utiliza medidas técnicas e administrativas para proteger os dados pessoais, impedindo o acesso não autorizado e situações que comprometam o processamento de dados.

Já o princípio da prevenção visa prevenir a ocorrência de danos causados pelo tratamento de dados pessoais, enquanto o princípio da não discriminação proíbe o uso do tratamento para fins discriminatórios, abusivos ou ilegais. Além disso, o princípio da prestação de contas e da contabilidade visa demonstrar a utilização de medidas eficazes para garantir a observância e o cumprimento das normas de proteção de dados (MURARI; SCHIAVON; BARRETOS, 2021).

Dessa forma, os indivíduos além de terem seus direitos reconhecidos em suas relações pessoais, também estarão amparados em suas relações virtuais, isso porque a inviolabilidade da intimidade, da honra e imagem é um desdobramento da proteção à privacidade e visa prevenir danos ocasionados por tratamentos de dados indevidos.

A proteção de dados pessoais, a fim de se evitar danos à personalidade de seu titular, ocorre de dois modos: a proteção da identidade pessoal do consumidor contra os riscos que o ameaçam como resultado da coleta, processamento, uso e divulgação de dados pessoais; e assegurar ao consumidor o controle do fluxo de seus dados em toda a sociedade (BRASIL, 2018).

Com a promulgação da LGPD, é possível controlar o fluxo de dados de um indivíduo através de consentimento do titular conforme o artigo 7º, inciso I, a proteção de dados só será efetiva quando houver a pressuposição de que a pessoa tem controle sobre suas informações. Nesse mesmo sentido, o artigo 11º, inciso I, da LGPD, requer o aceite titular para o tratamento de dados sensíveis. O artigo 14, §1º da mesma lei, estabelece que, quando os dados pertencerem a crianças e adolescentes, os pais ou responsáveis legais devem consentir no processamento desses dados. Entretanto, cabe ressaltar que haverá casos em que o titular não será obrigado a manifestar concordância com o tratamento. O legislador reconheceu que os controladores que processam os dados necessitarão também de certa liberdade para a execução de suas atividades (SANTOS, 2019).

O objetivo da Lei Geral de Proteção de Dados é garantir que o titular dos dados esteja ciente dos dados que estão sendo acessados e armazenados, a fim de proporcionar segurança e

acessibilidade a todos. A LGPD, em seu artigo 6°, dispõe sobre os princípios que guiam o tratamento de dados (BRASIL, 2018).

De acordo com André Ramiro *et al.* (2019), em primeiro lugar, é crucial notar que muitos dos princípios são autoexplicativos, apresentados nos incisos I, II, III e IV do Artigo 6º versando sobre a finalidade, adequação, necessidade e livre acesso referente ao tratamento de dados. Já os incisos V, VI, IX e X, estabelecem uma conexão. O inciso V, que trata sobre a qualidade dos dados, estabelece que os dados devem ser precisos, claros e atualizáveis para que a sua finalidade especificada e consentida possa ser alcançada. Já o inciso VI, que versa sobre a transparência, auxilia os titulares na busca de informações sobre seus dados, que devem ser claras e de fácil acesso. Dessa forma, é possível solicitar os dados, corrigi-los e até mesmo requerer sua exclusão de forma rápida e simples. O inciso IX discorre sobre a importância da não discriminação, assim os dados coletados não podem ser classificados por cor, raça, religião ou crenças políticas que tenham tendência a discriminar. E, por fim, o inciso X apresenta a responsabilização e prestação de contas, assim quando solicitado, a empresa ou organização deve prestar contas de conformidade com a LGPD, e caso algum ponto da lei seja descumprido, a empresa ou organização será responsabilizada.

Toda interação entre o proprietário e o responsável pelo tratamento dos dados deve ser moderada pelo princípio da vulnerabilidade. Não apenas em termos de disparidades de poder econômico entre as partes, mas também em termos de projeção social do dano em relação ao conhecimento e capacidade técnica para mitigar ou gerenciar tais consequências.

É inevitável que a pessoa física esteja sempre em situação de vulnerabilidade em relação à pessoa jurídica. É precisamente por esse motivo que a Lei Geral de Proteção de Dados especifica as diretrizes e os fundamentos sobre os quais os relacionamentos de transferência de dados devem se basear. A LGPD traz um rol de diretrizes quanto à Agência Nacional de Proteção de Dados, na qual os objetivos são determinados, no artigo 55-J da Lei, incluído pela Lei nº. 13.853/2019. Podem ser relacionados como exemplo das diretrizes, a fiscalização, sanções e penalidades que devem ser aplicadas quando o tratamento inadequado é fornecido; as políticas de proteção de dados que devem ser desenvolvidas; o incentivo à cooperação com autoridades internacionais de proteção de dados; e a prática de auditorias quanto à fiscalização, implementação de sistemas que promova a interatividade do titular com o controlador quanto ao tratamento de dados (SANTOS, 2019).

A promulgação da Lei Geral de Proteção de Dados, e sua vigência a partir de agosto de 2020, fez com que as empresas passassem por mudanças culturais, em seus procedimentos

internos, adequação de normas de segurança para o atendimento a essa normativa. Uma ferramenta de grande importância nesse processo é a *compliance*.

3.2 *COMPLIANCE* E A LGPD

Após o rápido crescimento da tecnologia e das comunicações, um dos desafios mais difíceis na sociedade da informação ou sociedade digital é a segurança jurídica. Um marco legal para responsabilizar agentes públicos e privados por danos causados pelo manuseio indevido de dados pessoais em face de violações de direitos à privacidade e intimidade (NUNES, 2021).

A Lei Geral de Proteção de Dados foi um passo indispensável para proteger os direitos fundamentais dos titulares de dados. Em vez de obstruir o uso de dados que são tão críticos no mundo de hoje, a lei estabelece o que se tornará a base para o manuseio adequado de dados, incluindo a proteção da autonomia do usuário, abordando interesses legítimos e mantendo padrões de transparência, verificação e responsabilidade (GARCEL *et al*., 2020).

De acordo com Silva, Laureano e Violin (2021), as implicações da LGPD são significativas tanto em termos de proteção de dados pessoais quanto na atividade empresarial porque têm influência direta no relacionamento e na comunicação com o cliente, na coleta e análise de dados, nos horários dos funcionários da empresa e nos custos. Como resultado, é fundamental desenvolver políticas de segurança de dados claras e concisas para garantir a compreensão e a confiança do cliente, além dos investimentos em um banco de dados seguro, imune a qualquer violação. É fundamental disseminar princípios jurídicos básicos e manter sua equipe atualizada sobre o que a lei exige, escolher custos adequados à lei de proteção de dados acima de multas e penalidades por descumprimento da lei.

Com a aprovação da LGPD, entende-se que o verdadeiro dono dos dados é o cidadão, e que, para cumprir a lei, as empresas devem alterar todas as suas práticas de processamento, coleta e uso de dados. Como todos os aspectos do processamento de dados mudaram, agora é necessário adotar transparência e responsabilidade.

Sendo assim, todo procedimento de processamento de dados deve ser documentado e justificado, garantindo um maior nível de atendimento da conta da empresa. A empresa será responsável por informar os clientes sobre os procedimentos e medidas de segurança em vigor, bem como garantir que as informações coletadas são preciso ser condizente com a realidade, preservando o patrimônio da empresa (NUNES, 2019). É o que busca a normativa: as empresas necessitam estabelecer o modo como tratam e armazenam os dados, assegurando a finalidade de seu uso.

Com a introdução da LGPD, o objetivo é oferecer maior segurança não só para os proprietários de dados, mas também para as empresas. Ao estabelecer limites para a coleta de dados e a forma como ela será conduzida, o objetivo é criar um ambiente estável e seguro para todas as partes (NUNES, 2019). Todo o processo de armazenamento e tratamento de dados deve ser estruturado de acordo com os princípios elencados no art. 2º da LGPD.

Sendo assim, conforme Nascimento (2020), os princípios de finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção e não discriminação deve ser ressaltados ao longo desse tratamento de dados e em sua condução.

Dessa maneira, a LGPD prevê um sistema de governança de privacidade, o qual consiste em um conjunto de condutas e diretrizes de governança, semelhantes a um programa de *compliance*, em que o intuito está em assegurar que as leis e o regimento interno sejam cumpridos, além de coordenar a gestão de riscos. Para que esse programa seja eficaz, ele deve ter um código de ética, suporte administrativo de alto nível, treinamento frequente e canais de adoção. Como resultado, a adoção de programas de *compliance* de dados pessoais é imprescindível para assegurar as conformidades instituídas pela LGPD (NASCIMENTO, 2020).

Com isso, a *compliance* pode ser usada como mecanismo de conformidade em qualquer contexto, seja ele legal, administrativo ou tecnológico, ou seja, associada a qualquer segmento que busque a eficiência de seus processos.

É o que enfatizam Adriane Garcel *et al.* (2020), quando afirmam que as mudanças provocadas pela nova legislação incluem a adoção de novas ferramentas de transparência, controle e *compliance*, bem como a contratação de profissionais especializados e a adequação dos já existentes no mercado. Outra opção seria contratar uma empresa terceirizada para realizar a transição. Todas as possibilidades para que as empresas brasileiras se adequem à LGPD implicam em gastos expressivos. Nesse caso, toda cultura e estrutura baseada nos produtos, serviços e modelos de negócios devem ser repensados, proporcionando maior segurança aos consumidores e empresas por meio de um processamento de dados mais transparente.

Com a possibilidade de penalidades severas, é razoável concluir que uma das principais preocupações das empresas é como proteger os dados coletados. Nesse processo de conformidade, é fundamental que esses indivíduos compreendam os agentes e sua importância no ciclo de vida da informação em seu meio.

Entende-se que as informações devem ser esclarecidas para os proprietários e tratadas pela ferramenta do operador de forma que somente aqueles que necessitem de acesso possam

obtê-las; em termos técnicos, esses dados devem ser criptografados e protegidos de possíveis invasores (SILVA, LAUREANO, VIOLIN, 2021).

O trabalho remoto é muito mais vulnerável a incidentes envolvendo dados pessoais e informações estratégicas corporativas, ao ser comparado à execução das atividades dentro do ambiente da empresa, onde há uma infraestrutura de rede segura que bloqueia sites e domínios considerados ameaças aos sistemas e rede da instituição. Para adotar medidas de prevenção realmente eficazes, é necessário mapear o fluxo de dados da empresa, identificando as ameaças relacionadas à LGPD e ao trabalho remoto em todas as fases operacionais.

Dessa forma, somente através da participação ativa das empresas no desenvolvimento de programas e boas práticas a lei pode ser efetivada, pois esses são os principais agentes responsáveis por sua implementação. Para garantir que o programa de *compliance* seja eficaz, é necessário identificar os principais riscos aos quais a empresa está exposta ao realizar o processamento de dados. Essa é uma etapa crítica no desenvolvimento de um programa que atenda às necessidades operacionais da empresa, permitindo a identificação dos principais riscos e a implementação de contramedidas para mitigar esses riscos (NUNES, 2019).

O desenvolvimento de um código de ética é uma das etapas capazes de auxiliar e embasar a criação de uma matriz de riscos (riscos internos e externos), bem como o adequado envolvimento de todos os níveis da hierarquia da empresa.

De acordo com Nunes (2019), as empresas necessitam elaborar um código de conduta conhecido como Boas Práticas e Governança na LGPD, ter a participação ativa da alta administração no estabelecimento e implementação dessas práticas bem como na sua avaliação.

Os princípios de Boas Práticas e Governança estão previstos no art. 50, que estabelece os padrões mínimos a serem seguidos pelos agentes de processamento de dados no estabelecimento de um programa de *compliance*.

Assim, conforme Mattos *et al.* (2019), a Lei de Proteção de Dados Pessoais exige uma estrutura com mecanismos dedicados apenas a garantir o cumprimento das leis que regem o tratamento de dados pessoais. Dentre as diversas responsabilidades e responsabilidades do agente de tratamento descritas na LGPD, é preciso atentar-se para:

> 1 – O cumprimento dos princípios gerais e assegurar os direitos do titular dos dados (art.7º, §6º);
> 2 - Obtenção de permissão quando preciso (art.7°, §5°; art. 8°, §6°);
> 3 – Esclarecer e prestar contas do modo em que são tratados os dados;
> 4 – Assegurar a portabilidade dos dados quando requisitado (art.9°; art.18; art.20);

> 5 - Assegurar a transparência no processamento de dados com base em interesses legítimos (art. 10, §2°);
> 6 - Acompanhar e manter as operações de processamento de dados pessoais, principalmente quando baseadas em interesses legítimos (art.37);
> 7- Criação de um relatório sobre a influência da proteção de dados pessoais, incluindo dados sensíveis, em suas operações de processamento de dados, respeitando as normas de segurança comercial e industrial (art. 10; §3°; art. 38);
> 8 – Determinar quem é encarregado, ou seja, o responsável pelo tratamento dos dados (art. 41);
> 9 - Reparação de prejuízos patrimoniais, monetários, individuais ou coletivos causados por violação da legislação de proteção de dados pessoais (art. 42 e 44, parágrafo único);
> 10 – Definir procedimentos de segurança, técnicas e administrativas (art.46);
> 11 – Assegurar a segurança das informações perante os dados pessoais, mesmo após a sua cessação (art. 47);
> 12 - Notificar a autoridade nacional e o proprietário de uma ocorrência de segurança que possa representar um risco ou causar danos aos proprietários (art.48);
> 13 - Proteger os direitos dos titulares por meio da adoção de disposições como, por exemplo, a divulgação da ocorrência por meio de canais de comunicação e ações capazes de solucionar ou minimizar os efeitos do incidente (art. 48, §2°);
> 14 – Elaborar normas de boas práticas e de governança (art. 50). (MATTOS, *et al.*, 2019, p. 80).

Diante do exposto, os profissionais que desejam ocupar a vaga de agente de tratamento de dados devem ter conhecimento técnico e jurídico, além de habilidades interpessoais e o princípio da boa-fé, bem como outros atributos que irão oscilar de acordo com as necessidades da empresa.

Nunes (2019) enfatiza que a LGPD confere aos agentes de tratamento, em especial ao controlador, a responsabilidade pela implementação do programa de governança de privacidade e pela demonstração do devido compromisso da empresa com as normas de proteção de dados.

Com base nessas definições legais, é fácil concluir que o controlador é o principal tomador de decisões quando se trata de coleta de dados pessoais. Ele determina a necessidade de coleta de dados, controla como os dados são coletados e, em seguida, seleciona quais dados são coletados, bem como quem tem acesso aos dados. Além disso, ele é o principal responsável pela proteção dos dados dos proprietários e, como resultado direto, a maioria das responsabilidades descritas na LGPD recai diretamente sobre seus ombros.

Também é sua responsabilidade estabelecer políticas de segurança e monitoramento de dados, permitindo o diálogo entre a empresa e o titular dos dados e, portanto, garantindo mais transparência no processo de processamento de dados. Levando em conta a realidade da LGPD para que um dado seja recolhido, ele deve ter uma finalidade específica, bem como um período específico de uso. Expirada a finalidade do dado, a empresa deve descartá-lo de acordo com as normas de segurança previstas na legislação (NUNES, 2019). É fundamental

que o programa de *compliance* atenda às necessidades exclusivas da organização, sendo o papel do controlador estabelecer um Código de Conduta adaptado às necessidades da organização e aos tipos de dados coletados e usados (NUNES, 2019).

Nesse sentido, a *compliance*, que surge com o objetivo de criar controle interno e monitoramento das operações em resposta à crescente preocupação com a aplicação de um código de ética interno, é tido como um mecanismo eficaz em termos de adequação dos negócios às referida Lei Geral de Proteção de Dados.

É o que considera Scatolin (2022), ao afirmar que a Lei de Proteção de Dados Pessoais agora exige uma estrutura com mecanismos dedicados apenas a garantir o cumprimento das leis que regem o tratamento de dados pessoais. Por exemplo, o art. 37, que exige a manutenção de um registro de todas as atividades de tratamento, o art. 38, que exige a apresentação de um relatório sobre o impacto na proteção de dados pessoais, o art. 46, que exige a observância das normas de tratamento, que, em caso de descumprimento, automaticamente acarreta responsabilidade, e o art. 50, que obriga a comprovação dos padrões de tratamento.

Assim, empresas que possuem operações orientadas por dados devem se preocupar mais em investir em medidas para garantir a segurança dos dados e o tratamento adequado dos dados.

Para estabelecer um programa de *compliance* que atenda a todos os requisitos e princípios da LGPD, é necessário conhecer todos os fluxos de dados existentes na organização. Todo ciclo de dados deve ser mapeado, assim como as características de cada tipo de dado. Os riscos do tratamento de dados pessoais são contínuos, e um desses riscos é garantir que o sistema utilizado no tratamento permita o pleno exercício dos direitos dos titulares. Em resultado da identificação do risco, as entidades podem proceder à segunda etapa, que é a elaboração de um código de conduta, com o objetivo de definir os processos utilizados pela pessoa coletiva no tratamento dos dados. Além disso, a LGPD determina que os dados coletados possam ser revogados alterando o acordo do titular para o tratamento de seus dados (SCATOLIM, 2022).

A adoção de práticas de *compliance* é sempre personalizada para as necessidades específicas de cada empresa e muda conforme as necessidades de cada contexto mudam. No entanto, alguns deles são fundamentais, o que significa que estão presentes em todos os casos. Se a matriz de risco for alterada, as consequências serão diretas. Como dito anteriormente, o desenvolvimento da matriz de risco é uma etapa crítica na prática de *compliance*, o que significa que ela será apresentada em todos os modelos. Como resultado, é um passo

necessário no desenvolvimento da empresa, cabe à teoria da gestão de riscos filtrar e priorizar as informações para que metas e planos de ação possam ser desenvolvidos.

Para assegurar que isso ocorra, a Sociedade Brasileira de Informática em Sade (SBIS) certifica instituições operadoras em diversos aspectos como segurança e confiabilidade, classificando os sistemas de informação em hardware, software, bancos de dados, redes, procedimentos e pessoas. Referência em certificações de ERP no setor de segurança, a SBIS orienta e capacita profissionais do setor de tecnologia sobre as normas e atualizações do mercado de segurança, área que está em constante adaptação às mudanças e exigências da legislação n°. 13.709/18 (SILVA, LAUREANO, VIOLIN, 2021).

A capacitação e a adoção de sistemas inovadores em segurança de informação beneficiam tanto as empresas ao terem a coleta e o gerenciamento de seus dados; quanto os proprietários de dados que passam a ter a garantia de que seus dados serão tratados com respeito e de maneira adequada. É óbvio que nesse novo cenário, apenas um lado tem o incentivo de dedicar tempo e recursos financeiros na compra de tecnologia e contratação de pessoas para se manter dentro da lei. Assim, empresas que possuem operações orientadas por dados devem se preocupar mais em investir em medidas para garantir a segurança dos dados e o tratamento adequado dos dados.

Silva, Laureano e Violin (2021) ressaltam ainda que políticas operacionais internas para ferramentas de processamento de dados, bem como padrões tecnológicos, devem ser seguidas pela Instituição para evitar consequências não intencionais. A formação de um comitê interno de gestão de tecnologia é um passo necessário para começar a entender a relação entre o dono da informação e as etapas subsequentes de interação com a Instituição.

Sendo assim, é preciso que requisitos mínimos sejam definidos para garantir a eficácia do programa de *compliance*, como análise de risco, suporte administrativo de alto nível, formulação de código ético e treinamento frequente, cultura corporativa, processos e canais de controle, monitoramento de processos, investigação do programa e sanções.

Além do mais, o treinamento periódico dos funcionários é tido também fundamental para estabelecer essas novas práticas de proteção de dados. Como resultado dessas mudanças significativas, será necessário estabelecer uma cultura de proteção de dados, que atualmente falta em muitas de nossas organizações, e que só pode ser alcançada por meio de treinamentos regulares que preparem os funcionários para as novas práticas e atitudes que a empresa adotará. Essa relação é fundamental, mesmo no estabelecimento de um bom programa de *compliance* (NUNES, 2019).

Dessa maneira, a alta administração deve participar ativamente das atividades, bem como dos planos de treinamento e monitoramento. Além disso, a formação regular proporcionada aos colaboradores permite-lhes compreender melhor as áreas onde não existem regras aplicáveis ou onde as regras não são claras, bem como o comportamento pretendido.

Todas as especificidades necessárias para a implantação de uma *compliance* eficaz estão associadas às penalidades que a empresa pode ter que enfrentar caso ocorra algum vazamento de dados. O art. 38 da LGPD expressa a possibilidade de a Agência Nacional de Proteção de Dados a ANPD órgão responsável por fiscalizar o cumprimento da Lei Geral de Proteção de Dados, solicitar a publicação de um relatório sobre o impacto da proteção de dados pessoais em relação às operações de processamento de dados da organização, resultando em maior transparência e segurança dos dados armazenados no sistema (SCATOLIM, 2022).

A ANPD é responsável por fiscalizar, investigar, avaliar denúncias e orientar a sociedade quanto ao tratamento de dados. Ela pode solicitar documentos, relatórios sobre riscos de exposição de dados, impor sanções administrativas às empresas e emitir recomendações. A lei deve ser aplicada independentemente do tamanho da empresa ou de sua receita. Todas as organizações devem cumprir a nova legislação.

Numes (2019) enfatiza, por fim, que a LGPD determina que o plano de governança da empresa inclua uma estratégia de resposta e remediação de incidentes (art. 50), tornando essa ação como uma garantia legal em que, em caso de furto ou prática ilegal, a empresa esteja preparada para lidar com a situação. Assim, a LGPD estabelece em seu art. 48 que diante de uma ocorrência, a organização deverá notificar a ANPD com a maior brevidade possível, com as seguintes informações:

> Art. 48, §1º, I - a descrição da natureza dos dados pessoais afetados; II - as informações sobre os titulares envolvidos; III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; IV - os riscos relacionados ao incidente; V - os motivos da demora, no caso de a comunicação não ter sido imediata; e VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo. (BRASIL, 2018, art. 48)

A ANPD determinará o prazo para essa comunicação em caso de incidente ou violação de segurança de dados, devendo a empresa apresentar um relatório incluindo, no mínimo, a natureza dos dados afetados, a informação dos respetivos proprietários, uma descrição detalhada das medidas de segurança usadas para proteger os dados, quaisquer riscos potenciais associados ao incidente e o que será feito para reduzir ou reverter as consequências.

Caso haja demora na comunicação, é preciso incluir também os motivos para o atraso. Cabendo à ANPD averiguar a situação e gravidade do ocorrido.

A LGPD causará ou já está causando impacto significativo em todos os setores da economia, trazendo mudanças tanto na esfera privada quanto na pública, inclusive extra territorialmente, quando especifica que todas as operações de coleta e/ou tratamento de dados pessoais realizadas no Brasil com a intenção de oferecer bens ou serviços em nosso território estarão sujeitas à lei. Como resultado, as empresas devem se adaptar aos novos padrões de segurança e privacidade, independentemente de gerenciarem as informações coletadas por meio de armazenamento físico de documentos ou sistemas digitais sob pena de, de acordo com o art. 52:

> a) Advertência, com indicação de prazo para adoção de medidas corretivas;
> b) Multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
> c) Multa diária, observado o limite total a que se refere o inciso II;
> d) Publicização da infração após devidamente apurada e confirmada a sua ocorrência;
> e) Bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
> f) Eliminação dos dados pessoais a que se refere a infração (SANTINI et al., 2019, p. 25).

É da responsabilidade das empresas promover o tratamento adequado dos dados, uma vez que as violações deles implicam por parte da empresa/controlador a obrigação ressarcir quem foi violado ou lesado. Também é possível que a empresa esteja sujeita a penalidades administrativas impostas pela ANPD.

As sanções são rígidas e precisam de atenção. No entanto, para que sejam eficazes, devem ser utilizados após o procedimento administrativo que possibilite a defesa integral de modo gradativo, isolado ou cumulativo. Tudo é feito de acordo com as especialidades do caso apresentado, bem como com base na observação de parâmetros e critérios como: gravidade, natureza da infração, reincidência, grau do dano, mecanismos internos instruídos para reduzir o dano, adoção de política de boas práticas e governança, entre outros. Com isso, as sanções da LGPD podem ser aplicadas corretamente, seguindo todos os procedimentos administrativos, permitindo ampla defesa, e de acordo com os parâmetros e critérios estabelecidos (SANTINI *et al*., 2019).

A LGPD, além de determinar as penalidades impostas a violação de dados, procurou dar um tratamento especial para aqueles que implementam programas eficazes de *compliance*. Além dos incentivos previstos em lei, a *compliance* traz benefícios econômicos e reputacionais significativos para quem a pratica, o legislador se preocupou em estabelecer

incentivos para quem a cumpre. No art. 52, incisos VIII e IX, é reconhecida a importância conferida por lei aos programas de *compliance* que, dependendo da observância dos demais fatores elencados no parágrafo, podem ser utilizados como atenuantes de sanções administrativas.

4. CONSIDERAÇÕES FINAIS

O objetivo desta pesquisa foi contemplado ao se identificar a importância da implementação de *compliance* nas empresas, visto que ao aderir a um programa de *compliance* as organizações estão reduzindo risco da ocorrência de condutas ilícitas por parte de seus administradores e colaboradores, além do mais, o efetivo programa diante de uma violação às normas é capaz de identificar o ato, buscando investigar, remediar.

Assim a *compliance* é tida como uma ferramenta de defesa para uma gestão corporativa eficaz, consiste em um programa de integridade, que promove a implantação de mecanismos de controle interno nos negócios por meio da gestão de riscos e da utilização de instrumentos que garantam o cumprimento de leis e regulamentos promovendo através dos princípios éticos uma melhor visibilidade da empresa que adota esse programa no segmento em que atua. A *compliance* e a governança corporativa são intimamente interligadas, visto que optar pela implementação dessa ferramenta faz parte de uma decisão de gestão, determinando, assim, a forma com que as empresas serão administradas e como as decisões de gestão são tomadas.

Foi possível verificar também a conexão entre sistema de *compliance* e o direito empresarial. No Brasil há uma vasta abrangência de normas reguladoras que comtempla o direito empresarial: civil, trabalhista, tributária, penal, ambiental entre outras esferas, a *compliance* possibilita não somente a adequação, ela promove mudanças culturais e no modelo de negócio da organização evitando o surgimento de demandas judiciais, bem como a corrupção e o uso indevido de dados.

Atualmente a *compliance* é o principal programa empregado pelas empresas brasileiras para se adequarem as especificidades da Lei Geral de Proteção de Dados nº. 13.709 de 2018, a qual busca definir parâmetros de processamento de dados mais seguros e confiáveis, além de garantir mais transparência e privacidade para os indivíduos.

As implicações da LGPD são significativas, tanto em termos de proteção de dados pessoais, quanto na atividade empresarial. Isso porque tem influência direta no relacionamento e na comunicação com o cliente, na coleta e análise de dados, nos horários

dos funcionários da empresa e nos custos. Como resultado, é fundamental desenvolver políticas de segurança de dados claras e concisas para garantir a compreensão e a confiança do cliente, além dos investimentos em um banco de dados seguro, imune a qualquer violação, é fundamental disseminar princípios jurídicos básicos e manter sua equipe atualizada sobre o que a lei exige. Escolher custos adequados à lei de proteção de dados acima de multas e penalidades por descumprimento da lei.

O descumprimento das normas da LGPD não é uma opção; pelo contrário, conforme mencionado, as penalidades impostas pelo descumprimento são severas e podem ter uma influência significativa na reputação da empresa. Como resultado, torna-se fundamental estabelecer programas de conformidade eficazes

Por fim, é importante enfatizar que a realidade brasileira em termos de proteção de dados ainda é muito nova, e ainda não se consolidou como algo a ser almejado por muitas empresas, principalmente as de pequeno e médio porte. Nesse contexto, a LGPD enfrentará um desafio maior do que as demais legislações contemporâneas no que diz respeito ao estabelecimento de uma cultura empresarial compatível com a lei. Os mecanismos de interpretação jurídica ainda estão sendo moldados como resultado de novas demandas que estão surgindo nos tribunais.

Com base nesse cenário, as empresas têm um papel inestimável na promoção dessa cultura de *compliance*, necessitando de diversos incentivos governamentais, além de uma fiscalização rigorosa, para garantir que essa nova realidade de *compliance* seja implementada.

REFERÊNCIAS

ANDRADE, Priscila de; RODRIGUES, Maria Rafaela Junqueira Bruno. O papel do advogado na governança corporativa através do *compliance* e da gestão de riscos. **Revista de Iniciação Científica e Extensão da Faculdade de Direito de Franca**, v. 4, n. 1, jun. 2019, p. 819-841.

BRASIL. **Lei nº 13.709, Lei Geral de Proteção de Dados**, Brasília, 14 de agosto de 2018. Diário oficial da União: seção 1, Brasília, DF, edição 157, p. 59, 15 set. 2018.

BRASIL. **Lei n. 12.846, de 1º de agosto de 2013**. Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências. **Diário Oficial da União**, Brasília, DF, 02 ago., 2013. Seção 1. p. 01.

BRASIL. **Constituição da República Federativa do Brasil**, de 5 de outubro de 1988.

CLAMER, Roberto. **Avaliação dos sistemas de *compliance* com a governança corporativa nas organizações da Serra Gaúcha:** uma análise nas empresas de capital aberto com ações na BM&F Bovespa. Dissertação (Mestrado em Administração). Universidade de Caxias do Sul. Caxias do Sul. 2018.

FREITAS, Yann Antônio Alves de; ZUIN, Débora Carneiro; MOREIRA, Nathalia Carvalho; SANTOS, Emili Barcellos Martins. Inovação em tempos de mudanças: o trabalho secretarial durante a pandemia da covid-19. **RCA – Revista Científica da AJES**, Juína/MT, v. 10, n. 20, jan/jun. 2021, p. 111-123.

GARCEL, Adriane; MORO, Sergio Fernando; SOUZA NETTO, José Laurindo de; HIPPERTT, Karen Paiva. Lei geral de proteção de dados: diretrizes e implicações para uma sociedade pandêmica. **Coletâneas de artigos jurídicos**: em homenagem ao Professor José Laurindo de Souza Netto. Curitiba: Clássica Editora, 2020.

GOMES, Heloísa dos Santos. **LGPD:** uma análise dos impactos da lei na cultura e tratamento de dados no Brasil. Monografia (Graduação em Análise e Desenvolvimento de Sistemas). Universidade do Sul de Santa Catarina. Florianópolis. UNISUL: 2019.

LEONI, Jacqueline Vasconcelos; SÉLLOS-KNOERR, Viviane Coêlho de. A importância do *compliance* na comunicação empresarial. In: **ANAIS DO IX CONBRADEC Congresso Brasileiro de Direito Empresarial e Cidadania**, Curitiba, v. 02, n. 33, 2020, p. 80-97.

LIMA, Alexandre da Silva. ***Compliance* e governança empresarial no direito pátrio - o caso Odebrecht.** Monografia (Graduação em Direito). Universidade Federal Fluminense, Instituto de Ciências da Sociedade. Macaé-RJ. UFF, 2019.

MATTOS, Bruna; Andrade, Genifer; BATISTA, Hélio; LUMAC, Leonardo. Dos agentes de tratamento de dados. **O que estão fazendo com os meus dados?** A importância da Lei Geral de Proteção de Dados. Saldanha, P.M. Recife: SerifaFina, 2019, p. 77-84.

MUNARI, Georgia Anastácia Campana; SCHIAVON, Isabela Nabas; BARRETOS, Ronaldo de Almeida. Dados pessoais: tratamento realizado pelo poder público à luz da

Lei Geral de Proteção de Dados, **Revista Judiciária do Paraná,** ano XVI, n. 22, novembro de 2021, p. 245-256.

NASCIMENTO, Suellen Lima do. **A lei geral de proteção de dados pessoais e a adoção dos programas de *compliance* na sociedade da informação.** Monografia (Graduação em Direito). Centro Universitário de Brasília. Brasília. UniCEUB, 2019.

NUNES, Gabriela Victória Miranda. **Governança e Boas Práticas na Lei Geral de Proteção de Dados Pessoais**: dos programas de *compliance*. Monografia (Graduação em Direito) Universidade de Brasília. Brasília: UNB, 2019, p.67.

RAMIRO, André; SANTIBI, Barbara; ANDRAD, GENIFER de; MARANHÃO, João Paulo Borba; LUCENA, Tatiana; AGUIAR, Thaís. Direito de Revisão: automatizada? **O que estão fazendo com os meus dados?** A importância da Lei Geral de Proteção de Dados. Saldanha, P.M. Recife. SerifaFina, 2019.

SANTOS, Viviane Bezerra de. **Lei Geral de Proteção de Dados:** fundamentos e *compliance*. Monografia. (Graduação em Direito). Universidade Federal do Ceará. Fortaleza. UFC, 2019.

SILVA, Fernanda Alves de Souza; Laureano, Guilherme; VIOLIN, Renato. Os impactos da LGPD e o *compliance* nas instituições controladoras de dados sensíveis In: **VIII Congresso de Trabalhos de Graduação Faculdade de Tecnologia de Mococa**, v.8, n.2, 2021.

SCATOLINE, Carolina Lanzini. Uso da tecnologia Blockchain no *compliance* de dados: uma análise da possibilidade e entraves a serem resolvidos. **Revista de Economia, Empresas e Empreendedores na CPLP***,* v. 8, n. 1, 31 de março de 2022.

SOUZA, Marlene de Fátima Campos; ALVES, Eric Matheus Ceccon Smaniotto. *Compliance* na governança corporativa para transparência e proteção fiscal das instituições privadas enquanto fomento de acesso à justiça. **Ciências Jurídicas: fundamentação, participação e efetividade**. Vasconcelos, A.W. S. Ponta Grossa-PR: Atena, 2021, p. 133-145.