GRADUAÇÃO EM MOVIMENTO
CIÊNCIAS JURÍDICAS
www.periodicos.uniftc.edu.br
Volume. 1 n. 2 - 2022

COMPLIANCE DIGITAL: FERRAMENTA ESTRATÉGICA NA GESTÃO DE UMA GOVERNANÇA POSITIVA

DIGITAL COMPLIANCE: A STRATEGIC TOOL IN MANAGING A POSITIVE GOVERNANCE

Cibele Guimarães de Brito[1]
Orlando Alves Lopes de Jesus[2]
Laine Reis[3]

RESUMO

O presente trabalho pretende responder a seguinte questão: Qual a importância do compliance 4 digital nas organizações? O objetivo geral deste trabalho é o de identificar fatores relacionados a necessidade de implementação de um programa de integridade, bem como da atuação do profissional de compliance nas empresas. O Compliance Digital, além dos outros elementos a ele conectados, incluindo o da necessidade de se estabelecer uma Governança em Privacidade de Dados, de forma positiva e preventiva no que tange a LGPD e demais regras aplicáveis às tecnologias da informação, serão também temas a serem abordados neste artigo; Ademais, a pesquisa também tem o intuito de agregar relevância e fazer perceber que o compliance age de acordo com uma regra, um comando, e um dever ser que é o de estar em conformidade com a ética, relações, leis e regulamentos internos e externos das organizações.

PALAVRAS-CHAVE

Compliance; Stakeholders; Digital; Ética; Governança.

[1] Empresária, Pós-graduada em Administração com ênfase em Gestão de Negócios pela FGV - Fundação Getúlio Vargas, Pós-graduada em Compliance e Governança pela Brasil Jurídico em parceria com a UniFTC, Turismóloga pela Faculdade Visconde de Cairu, e Graduanda em Direito pela UniFTC - Campus Paralela. cibelegbrito@gmail.com
[2] Orlando Alves Lopes de Jesus. Estudante do Curso de Direito UniFTC – Campus Paralela. orlandoalves3@icloud.com
[3] Laine Reis Dos Santos Araújo. Doutoranda em Direito Civil. Mestra. Professora Universitária do Curso de Direito UniFTC – Campus Comércio. laine_reis@yahoo.com.

ABSTRACT

The present study aims to answer the following question: What is the importance of digital compliance for organizations? The general objective of this work is to identify factors related to the need for this área to be implemented, as well as to know the compliance professional duties. Digital Compliance, as well as all other elements connected to it, including the need to establish a Data Privacy Governance, in a positive and preventive way with regard to LGPD and other rules applicable to information technologies, will also be topics to be addressed in this article; The research also aims to add relevance and make people realize that compliance acts according to a rule, a command, and a duty that must be in compliance with ethics, relashions, law, internal and external regulations of organizations.

KEYWORDS

Compliance; Stakeholders; Digital; Ethics; Governance.

1 INTRODUÇÃO

O compliance surgiu nos Estados Unidos, no início do século 20, com a criação do Banco Central dos Estados Unidos, buscando tornar o ambiente financeiro mais seguro e estável. O termo compliance deriva-se da palavra “to comply with” e significa estar em conformidade, de forma íntegra e no caminho da ética.

No Brasil, o compliance ganhou notoriedade em 1922, quando o mercado nacional abriu as portas para as empresas estrangeiras. Em 2013, ocorreu a promulgação da Lei anticorrupção (nº 12.846), da qual definiu a responsabilidade da pessoa jurídica em atos contra a administração pública. Ocorre, entretanto, uma revolução no cenário brasileiro em termos de programas de compliance, em 2014, pois surgira inúmeros escândalos de corrupção, cujo exemplo mais notório é a Operação Lava Jato.

O compliance tem como uma das principais funções, tornar mais segura as relações entre empresas e instituições, tornando possível assim menores os riscos dessas organizações se envolverem em atos ilícitos, o que consequentemente otimiza as relações internas e externas.

A tecnologia possibilita soluções para que esse processo seja mais ágil, seguro e efetivo, sendo assim, a tecnologia possui grande importância para que o compliance funcione com maior celeridade e eficácia.

Nas palavras de Assi (2013), Compliance pode ser definida como um sistema de controle que permite esclarecer e proporcionar maior segurança àqueles que utilizam a contabilidade e suas demonstrações financeiras para análise econômico-financeira.

Neste sentido, podemos definir ainda o Compliance como um sistema de controle de padrões voltados para dirimir e prevenir danos/conflitos, além de proporcionar maior transparência para as empresas, mantendo padrões éticos.

Este trabalho é fundamentado em pesquisa bibliográfica qualitativa e propõe uma observação atenta, dos valores e das relações humanas profissionais. Propõe também um parecer acerca do Compliance Digital e das ferramentas estratégicas que favorecem ações de governanças positivas. Dessa forma, este trabalho pretende identificar, os principais fatores relacionados a

importância desta área no direito digital e do profissional de compliance nas organizações.

Parte-se da premissa, que o profissional de compliance possui uma função determinante para a prevenção de prejuízos, buscando sempre a melhor opção de governança. Portanto, justifica-se a realização deste estudo por meio de pesquisa sobre a importância do compliance digital, para a promoção de discussões e debates não apenas no campo organizacional, mas também acadêmico, além de contribuir com estudos posteriores com objetivos de avanços significativos, que elevem aprendizagens cognitivas pontuais cada vez mais técnica e eficaz no mundo corporativo.

O objetivo Geral é analisar os impactos da LGPD e a necessidade de implantação de um compliance digital nas empresas brasileiras, quais ações devem ser tomadas além das atitudes éticas e transparentes esperadas pelo profissional de compliance. Os Objetivos Específicos, induz a perceber a importância do compliance digital para o desenvolvimento dos negócios e as ações de governança positiva nas empresas, propõe verificar o atual cenário corporativo e a adequação da empresa frente a LGPD, expõe a ética como premissa básica a ser trabalhada no fomento de uma cultura de integridade a qual atua em prol da longevidade e perpetuidade de uma empresa.

2 REFERENCIAL TEÓRICO – COMPLIANCE DIGITAL

2.1 A Lei Geral de Proteção de Dados (LGPD)

A Lei Geral de Proteção de Dados (LGPD), n° 13.709/2018, entrou em vigor em setembro de 2020, e tem como finalidade padronizar as normas e práticas de coletas, armazenamento, tratamento e compartilhamento de dados pessoais, inclusive nos meios digitais por pessoa jurídica de direito privado.

O objetivo principal da LGPD é o de proteger direitos fundamentais de liberdade e privacidade, conforme previsto na Constituição, além de garantir ao cidadão o controle sobre os seus dados pessoais. Esses dados, identificados como pessoais, podem ser ou não sensíveis, nesse caso, requerer-se-á diferentes formas de tratamento, conforme especificado na legislação.

Assim, de igual modo, a LGPD prevê sobre o acesso do titular de dados, a informação sobre os dados pessoais:

> O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso [...] (BRASIL, 2018, Art.9)

Ressalta-se que é necessário o consentimento expresso do titular para a realização de tratamento de dados por outrem, como é bem-disposto no Art. 7, I da LGPD, tanto que existe a possibilidade de arrependimento do titular e/ou consumidor sendo capaz de restringir, recusar, cancelar e excluir seus dados pessoais fornecidos.

Ademais, existem sanções previstas no art. 52 da LGPD que poderão ser aplicadas pela ANPD - Autoridade Nacional de Proteção de Dados. Dentre as sanções elencadas, existem as advertências, com indicação de prazo para adoção de medidas corretivas, até multa simples, de até 2% do faturamento,

limitada a R$ 50.000.000,00, além da proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.
A ANPD, entretanto, tem o papel de mensurar esforços de prevenção existentes na organização, como um setor de compliance, programa de integridade efetivo e ações mitigadoras, para a partir daí estabelecer o grau de gravidade e sanção a ser adotada.
Faz-se, portanto, necessária a compreensão da LGPD e suas consequências a partir da sua vigência, incluindo o que tange a implementação de uma governança de privacidade positiva nas empresas e organizações.

2.1.1 LGPD e Compliance

Em um ambiente corporativo, onde existem inúmeras interações on-line, evidenciou-se não apenas a necessidade da criação de meios de segurança dos dados pessoais por força da LGPD, mas também a necessidade de se criar ferramentas internas onde a cultura da ética e da integridade possa ser fomentada.

Além da LGPD, existe também a necessidade de adequação no que diz respeito a lei n°12.846/2013 (Lei Anticorrupção), da qual dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira.

Um dos objetivos do programa de compliance, está o de criar meios de prevenção para o combate a fraudes, desvios de condutas éticas, atos ilícitos, conflitos de interesses, corrupção e lavagem de dinheiro. É através de ações voltadas para a prevenção que a organização, por meio do programa de integridade, consegue proteger a sua imagem e reputação não apenas para os seus integrantes, mas também para os seus clientes e fornecedores.

Para (CADE, 2016, p.09) uma definição para o programa de conformidade, seria a de que “compliance é um conjunto de medidas internas que permite prevenir ou minimizar os riscos de violação às leis decorrentes de atividade praticada por um agente econômico e de qualquer um de seus sócios ou colaboradores.”

Com a promulgação da LGPD, as empresas passaram a integrar no seu programa de compliance, políticas e procedimentos de segurança de dados e informação, além de treinamentos, matriz de risco e regras no seio digital e territorial, a fim de garantir a proteção e adequação da organização conforme o estabelecido pelas leis acima citadas.

2.1.2 DPO – Data Protection Office ou Encarregado de dados

Entre as exigências da LGPD está a criação do cargo DPO (sigla em inglês para Data Protection Officer), ou encarregado pelo tratamento de dados pessoais. O DPO é o profissional que deve ficar inteiramente responsável pela segurança de dados de uma organização, incluindo seus funcionários, fornecedores e clientes. Poderá ser uma pessoa física ou jurídica, sendo seu papel principal, ser o elo de contato entre a organização, titulares de dados e a ANPD.

Por conta de tamanha responsabilidade na sua função e existência, é que o art. 41, § 1º da LGPD, estabeleceu que:

> O controlador deverá indicar encarregado pelo tratamento de dados pessoais.
> § 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

É desejável que o profissional tenha habilidades jurídicas, gestão de processos, tecnologia e Sistemas da informação, além de noções gerais administrativas responsivas e formação multidisciplinar, conhecendo as principais tendências de tecnologia e o impacto das mudanças na lei e nas empresas.

O art. 5, VIII, da LGPD, define o DPO ou encarregado de dados, como "pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)", ademais, faz parte de suas funções o elencado no art. 41, § 2º da LGPD:

> I- Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
> II- Receber comunicações da autoridade nacional e adotar providências;
> III - Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
> IV- Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Refletiremos ainda também acerca da função do profissional de compliance e suas características. E de que forma, esses profissionais atuam quando a mitigação de riscos, proteção da integridade e aprimoramento do sistema de controle interno para o combate da corrupção e fraudes nas organizações.

3 COMPLIANCE

3.1 Surgimento do Compliance

Desde os primórdios das relações comerciais o compliance sempre esteve presente, percebemos que cada empresa tem adotado o seu próprio código de conduta, de ética, com o intuito de evitar danos à imagem e reputação. Em meado do século XX cresceu a preocupação e a regulamentação surgiu das necessidades de as empresas respaldarem-se no seguimento da lei. Diante da urgência da complexidade da regulação moderna as empresas requeriam de uma maneira mais formal e organizada para assim, suster as ações éticas de sua governança.

De acordo com Bielgelman (2008), preços altos, manipulação geral, envolvendo fabricantes de equipamentos elétricos, como a tão conhecida General Eletric e a Westinghouse, teve como resultado várias pessoas físicas e jurídicas condenadas por violação antitruste. O caso repercutiu de tal forma que a primeira prisão e condenação na história em 1970 de Sherman Antritrust Act estimulou a criação de códigos de conduta para o fomento da ética e integridade. Inicia-se, portanto, uma mobilização por parte das empresas para a implantação de programas de compliance, visto que existia uma demanda externa da qual

pressionava a necessidade de adoção de medidas e políticas para frear tamanhos escândalos da qual levara a sociedade a indignar-se.

No ano de 1977, o Congresso Estadunidense aprova o Foreign Corrupt Practices (FCPA), lei que torna crime para empresas americanas, bem como indivíduos e organizações que atuem em seu nome, que subornem um funcionário do governo estrangeiro em troca da assistência na obtenção, manutenção ou direcionamento dos negócios.

Com a criação do FCPA, houve um desenvolvimento generalizado de empresas com códigos de ética e conduta, o que foi um marco muito importante para novas reflexões nas empresas de uma maneira geral. Bielgelman (2008) diz que:

> Muitas empresas não tinham freios efetivos e contrapesos para regular seu comportamento e os consultores jurídicos internos eram incapazes ou não queriam dar conselhos legais claros e pertinentes. A gestão agiu com superproteção e assumiu grandes riscos, assim como preocupações de curto prazo dominaram as tomadas de decisões corporativas. Isso coincidiu com uma maior atenção do público acadêmico sobre atos ilegais e lesivos das corporações, que levaram à regulamentação posterior. (BIEIGELMAN, 2008, p.107).

O desenvolvimento contínuo de programas de compliance foi marcado pela criação das Diretrizes Federais de Condenação para o Crime Organizacional nos Estados Unidos, em 1991, que apoiavam as organizações responsáveis aplicando “pena justa” para ações criminosas e incentivos dissuasivos para detectar e prevenir o crime. Estas diretrizes para Crime Organizacional foram uma nova adição às Diretrizes de Penas Globais, já que as diretrizes originais não abordaram as organizações. A Comissão de Sentença Americana (United States Sentence Commission – USSC) e muitos outros comentaristas acreditavam que devido às características inerentes de uma organização, ela precisava ser tratada de forma diferente de um criminoso comum. O USSC recomendou sete requisitos mínimos para um programa eficaz, capaz de prevenir e reprimir as violações da lei. As Diretrizes da Condenação para as Organizações, deram às empresas um forte incentivo para ter um programa efetivo de cumprimento de normas, seja para receber uma sentença menor ou imposta como parte da proibição. (BIELGELMAN, 2008).

3.2 Compliance Officer

3.2.1 Perfil do CCO – Chief Compliance Officer

O “Chief Compliance Officer” (CCO), hoje tornou-se um dos mais importantes profissionais que compõe o quadro organizacional de uma empresa. Ter um CCO no seu quadro de integrantes já é visto como fundamental e indispensável no mundo coorporativo.

Para que seja efetivado de fato o compliance nas organizações e para que as ações planejadas sejam alcançadas, faz-se necessário a figura do CCO. É preciso compreender que ele não atuará como fiscal ou policial na organização, mas como agente que promove a integralidade na organização, conhecedor de leis e da ética no setor corporativo.

3.2.2 Atribuições do CCO

De acordo com (CADE, 2016, p.19), “programas bem estruturados são normalmente precedidos e acompanhados da realização de uma análise aprofundada dos riscos, aos quais a entidade está exposta em suas atividades.”

O CCO estrutura, supervisiona o canal de denúncias, acompanha processos investigativos, elabora relatórios, e é a pessoa responsável pela gestão do programa de compliance e por sua efetivação em todos os setores da empresa, pode executar sua função de maneira individual como também coletiva, mas será alguém capacitado a gerir o programa. As demandas por estes profissionais vêm crescendo dia após dia, ele é o responsável pelo treinamento, investigação isso pede um profissional com capacidades múltiplas.

4 COMPLIANCE DIGITAL E STAKEHOLDERS

4.1 Stakeholders

Os stakeholders são os colaboradores, clientes, fornecedores e acionistas. Ou seja, partes interessadas de uma empresa ou organização, portanto, são peças fundamentais envolvidas.

É papel dos líderes, decidir sobre o propósito, missão, visão, valores e princípios, além de compreender que os seus comportamentos diários impactam de maneira direta no modelo de governança a ser adotado. Para tanto, é também dever do compliance, se preocupar quanto a participação dos líderes na disseminação de uma governança positiva, estratégica e preventiva, a fim de tranquilizar e preservar valor do negócio aos stakeholders envolvidos.

Vale ressaltar que os stakeholders por serem pessoas que podem ser diretamente afetadas pelas decisões que vierem a ser tomadas pela organização, é um interessado direto e tende a ser também a favor da implementação do compliance. Pois, é sabido que, nas organizações, é função do compliance, a criação de normas, preservação de valor dos negócios, atuando na mitigação de riscos, sanções legais dentre outros prejuízos existentes.

Afinal, são os princípios da governança corporativa que proporcionam segurança à implementação do propósito organizacional e orientam o processo de adaptação aos novos cenários.

4.2 Relação entre Steakeholders e compliance

A ampliação excessiva do âmbito do programa de compliance para todos os stakeholders da organização, chegando a ponto de fiscalizar a conduta nas relações com terceiros, pode gerar um dispêndio de recursos desproporcional aos seus riscos e ganhos.

Por esse motivo, recomenda-se a definição da abrangência do programa de compliance, a partir do conceito de gestão de stakeholders, com a seleção e identificação daqueles que são mais prioritários.

Para tanto, também deve ser considerado o grau de risco atribuído a cada um deles. É, portanto, uma via de mão dupla na percepção de ganhos e perdas. Importante se faz entender que o termo stakeholders é bem atual e sua concepção está agregada a vários contextos como comunicação, administração e tecnologia da informação.

Seu propósito é direcionar a gestão da empresa, o conselho de administração, funcionários, ou seja, quem faz parte do projeto um planejamento estratégico ou do plano de negócios. São os stakeholders que dão legitimidade as atitudes de uma organização e isso influencia diretamente nos seus resultados.

4.3 Integridade também no meio Digital

É necessário que as empresas se preocupem e invistam hoje no desenvolvimento e disseminação de uma cultura ética e íntegra no âmbito digital?

Sim. O Compliance tem a proposta de através de uma cultura de integridade, traçar um caminho onde condutas íntegras e lícitas sejam consideradas pelos stakeholders quando na tomada de decisões. O zelo pela boa imagem, reputação e ética, deve nortear a conduta da organização e de seus colaboradores, até mesmo quando se refere ao desenvolvimento de novas tecnologias. Pois, aspectos relacionados à responsabilidade, direito à privacidade, autodeterminação informativa e às liberdades individuais, incluindo a dignidade da pessoa humana e a diversidade cultural, precisam ser considerados.

Portanto é importante que empresas, ONGs e organizações invistam cada vez mais em Compliance Digital, que é onde deverá ser estruturado o cuidado quanto ao tratamento de dados pessoais, infraestrutura tecnológica, análise de riscos e adoção de medidas preventivas para adequar a organização às regras aplicáveis às tecnologias da informação, de acordo com as leis específicas.

5 A PANDEMIA E O COMPLIANCE DIGITAL

Compliance digital é um tema bem relevante na atualidade. Nas grandes empresas, nos últimos anos tornou-se uma questão em evidência, principalmente nos países onde ocorre o combate a corrupção como é o caso do Brasil. Diante do cenário atual de pandemia por conta do Covid.19, vivemos uma situação de mudança no cenário econômico profissional, avanço na esfera corporativa e na economia, e um crescimento assombroso nas áreas de tecnologia e digital. A crise impactou de forma negativa vários setores, por outro lado a LGPD trouxe a necessidade de fazer com que as empresas acelerassem na busca de melhorias dos seus processos internos relacionados a governança, para além de olhar as lacunas e brechas da qual porventura ficaram expostas, protegendo os negócios e garantindo a perpetuidade da organização. Conforme leciona Maldonado:

> Ao contrário, trata-se de compreender que, para permanecer no mercado, é obrigatória a consideração desses fatores. Na ausência de níveis adequados de proteção, às empresas, em um momento ou outro, não se sustentarão, seja porque serão alvos mais fáceis de incidentes criminosos, seja porque não ofertarão, desde logo o melhor produto entre os seus concorrentes. (MALDONADO, 2019, p. 31).

A partir desse novo contexto de sobrevivência que surge de forma acelerada também o compliance digital, como meio de barrar essas ameaças, com o intuito de mitigar os riscos de infração, e adotar de forma preventiva,

medidas baseadas na lei para melhor transparecer nos seus negócios, ações pela empresa projetadas.

E neste momento de pandemia o profissional de compliance digital vem para agregar valores éticos e controlar a rede corporativa, garantindo através da lei que que nenhuma irregularidade ou ação ilícita venha a afetará os dados e atividade fim da empresa, isso mantém a credibilidade da empresa perante os seus clientes, o mercado e colaboradores.

5.1 Adaptação das empresas diante do novo cenário na esfera digital

Houve uma nova realidade no cenário das empresas e a mudança para novos espaços também estavam incluídas nestas mudanças. Entre elas, destaca-se o crescimento do trabalho na modalidade home office, além da extensão do trabalho remoto, que cresceu de maneira veloz. No início, houveram várias dificuldades relacionadas a equipamentos e acessos em geral, pois as pessoas precisavam adequar-se a novas formas de trabalho exigidas pelo modelo remoto. Além disso, também foi necessário pensar em cuidar da exposição a riscos cibernéticos, que podem gerar prejuízos relacionados a roubo ou até mesmo destruição de dados empresariais.

Dentre alguns riscos, existe o Eavesdropping onde o agente cibercriminoso invade e-mails, mensagem, telefonia para quebrar a confidencialidade, o Decoy onde se cria um programa falso similar ao legítimo onde o usuário faz o login e compartilha informações. Isso acontece em app de bancos, com intuito de obtenção de informação bancária, além do Keylogger e o Pishing e vários outros que atacam senhas e são utilizados por hackers de maneira não autorizadas.

Por outro lado, existem também ferramentas variadas que em contrapartida colaboram de forma significativa na proteção de dados e contra esses crimes cibernéticos. Destacamos o Google Vault que é um serviço da Google Workspace que atende muito bem a gestão e aos princípios de governança de uma organização pertinentes à coleta, tratamento, guarda e descarte de informações digital, ele atende as prerrogativas da nova LGDP dentro de suas normas e leis, sendo bastante atualizado. O Google Cloud oferece as empresas e governos do mundo inteiro segurança integrada a nuvem, existem seguros cibernéticos e muitas outras ferramentas que auxiliam na gestão da confidencialidade do espaço corporativo.

Vale salientar que a pandemia fez com que as empresas se adaptassem ao mundo digital e ao home office, sendo o home office possível graças ao avanço da tecnologia. Com esse novo modelo de trabalho, foi possível atenuar certos prejuízos que as empresas tiveram durante o ápice da pandemia, fazendo-se necessário a ligeira adequação à nova realidade do mundo digital. As empresas e pessoas, passaram a ver a tecnologia como uma aliada e não mais como um investimento extra e desnecessário.

Segundo Andrade (2020), líder da área de estratégia de talentos da Mercer no Brasil, “o que as empresas não fizeram em cinco anos, fizeram nas últimas cinco semanas”, fazendo uma referência direta a corrida pela modernização vivenciada na pandemia, pelas empresas que negligenciaram a tecnologia e que com a pandemia tiveram que ir em busca de algo que já deviam ter buscado e inserido no seu cotidiano.

5.2 O Profissional de Direito e o Compliance Digital

O profissional de direito atua como orientador efetivo das leis, sempre em busca de um maior entendimento das normas e consequentemente da sua aplicação. Posto isso, um profissional com esse know-how, tende a destacar-se, quando na função de compliance officer, DPO ou gestor de uma governança positiva onde o mundo digital é levado em consideração, assim como os riscos a ele atrelados. Além disso, aquele que decidir se especializar no direito digital poderá atuar com crimes digitais – como violação de privacidade, roubo de dados, divulgação de notícias falsas (fake news e deep fakes) e muitos outros.

Diante dos avanços tecnológicos e das características do ciberespaço, se faz necessário ter uma ciência jurídica capaz não só de evoluir de forma intuitiva, rápida e dinâmica, mas, assegurar também a aplicação das normas e eficiência legislativa dentro deste âmbito.

O profissional de direito de hoje lida com uma realidade diferente do profissional de direito de 10 (dez) anos atrás. A digitalização do judiciário, transformação dos processos manuais em eletrônicos, atos, sessões de julgamento e despachos virtuais, são alguns dos exemplos do porquê é imprescindível que esses profissionais também estejam atentos às tendências com relação a regulações normativas que deverão surgir em um futuro próximo, pois, sem dúvida, o Marco Civil da Internet (12.965/2014), Regulação do Comércio Eletrônico (Decreto 7.962/13), e a LGPD, são apenas leis iniciais a compor a abrangente pauta do compliance digital.

A implementação de um programa de compliance digital nas esferas jurídicas é uma necessidade presente para as organizações que buscam a sobrevivência e estabilidade no mercado. Ademais, a presença de um profissional do ramo do direito é inquestionável, vez que “(...) as mudanças pelas quais o Direito passa, inevitavelmente trarão outras preocupações para organizações de todos os portes quando se fala de conformidade com normas” (PALHARES; PRADO; VIDIGAL,2021, p. 330).

6 CONSIDERAÇÕES FINAIS

Este artigo de conclusão do curso de direito da faculdade UNIFTC, atende a proposta sobre a explanação acerca da necessidade de adequação que as empresas precisam atingir em ambiente digital, considerando, sobretudo hábitos e padrões de conduta éticos e íntegros, no que tange a privacidade e proteção de dados pessoais.

Ademais, é perceptível que o tema aqui abordado, assume relevância não apenas para advogados ou especialista, mas também profissionais ligados a tecnologia, gestão, dentre outras que tenham como área de atuação o ambiente digital e a necessidade de estar em um caminho ético e em conformidade com as leis vigentes.

O artigo atende ao objetivo geral e específico identificados na pesquisa além de responder com relação da importância do profissional de compliance nas organizações. Percebe-se a importância desses profissionais e a entrega de valor para as empresas como um agente de aprimoramento. Pois, são eles que fazem com que haja o cumprimento de normas legais, de certificação e de regulamentos internos previstos no ambiente digital corporativo.

O artigo favorece, avanços para pesquisas e discussões posteriores em espaços diversos, pois aborda tema atual e de grande relevância na esfera profissional, educacional, social, pessoal e corporativo.

Por utilizar de pesquisa bibliográfica qualitativa, o presente artigo proporciona também a ampliação do conhecimento cognitivo, além de ter proporcionado diálogos relevantes entre os seus autores, partilha de experiência e resposta quanto aos caminhos que podem e devem ser percorridos na capacitação de profissionais para atuar no mundo profissional de maneira concisa.

A experiência foi positiva, agregando de forma pessoal novos conhecimentos, e fortalecendo o desejo de atuar como um profissional preparado para atender as demandas corporativas de maneira ética e dentro da lei, objetivando sempre o avanço e crescimento da organização e ao mesmo tempo pessoal, contribuindo assim para uma cultura social de crescimento e evolução empresarial e social.

REFERÊNCIAS

ABNT. Disponível em: Referencias bibliograficas - exemplos (livros, e-books, blogs, internet) (normasabnt.org). Acesso em 14 de abril 2022.

ASSI, Marcos. **Gestão de Compliance e seus desafios**. Vol. 1. Saint Paul Institute of Finance, 2013.

BIELGELMAN, Martin T. **Building a world-class compliance program**, Hoboken,NJ:John Wiley, 2008.
BRASIL, Constituição: **República Federativa do Brasil de 1988**. Brasília, DF: Senado Federal,1988, ed. 57°, ano 2021.

BRASIL. **Lei n° 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Disponível: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 01 de out. de 2022

BRASIL, (LGPD). **Redação dada pela Lei no 13.853, de 2019**. Brasília, DF: Senado Federal, 2018, Lei 13853/19 | Lei nº 13.853, de 8 de julho de 2019, Presidência da Republica (jusbrasil.com.br), Acesso em: 10 de abril de 2022.

CADE – Conselho Administrativo de Defesa Econômica – Guia Programas de Compliance, 2016. Disponivel em: http://antigo.cade.gov.br/acesso-a-informacao/publicacoes-institucionais/guias_do_Cade/guia-compliance-versao-oficial.pdf. Acesso em: 8 de abril 2022.

CASTELLS, M.; CARDOSO, G. (Org.). **A sociedade em rede: do conhecimento a acção política**. Lisboa: Imprensa Nacional: Casa da Moeda, 2006.

CASTELLS, Manuel. **A sociedade em rede**. Vol. 1. São Paulo: Paz e Terra, 1999.
CAVALCANTI, Leo, 2021.Disponível em https://www.linkana.com/blog/como-implantar-governanca-corporativa/. Acesso 8 de abril 2022.

CORRÊA, Gustavo Testa. **Aspectos jurídicos da internet**. São Paulo: Saraiva, 2000.
CUNHA, Mateus, 2021. Disponível em https://www.t4compliance.com/desafios-na-implementacao-e-gestao-de-um-programa-de-compliance-em-empresas-familiares/ Acesso em: 04 de abril 2022.

DONEDA, D. (1). **A proteção dos dados pessoais como um direito fundamental**. Espaço Jurídico Journal of Law [EJJL], 12(2), 91-108. A proteção dos dados pessoais como um direito fundamental | Espaço Jurídico Journal of Law [EJJL] (unoesc.edu.br). Acesso em: 12 de abril 2022.

GUERRA, Sidney Cesar Silva. **O direito à privacidade na internet: uma discussão da esfera privada no mundo globalizado**. Rio de Janeiro: América Jurídica, 2004.

IBEF-PR,2021. Disponível em: https://www.gazetadopovo.com.br/conteudo-publicitario/ibef-pr/compliance-digital-o-impacto-da-pandemia-na-digitalizacao-das-empresas/. Acesso em 14 de abril de 2022.

IBGC - Instituto Brasileiro de Governança Corporativa, 2021. Disponível em https://ancd.org.br/wp-content/uploads/2021/03/Agenda-Positiva.pdf. Acesso 8 de abril 2022.

LÔBO, Paulo. **Direito civil: parte geral**. 3 ed. São Paulo: Saraiva, 2012.
MALDONADO, Viviane Nobrega. LGPD – Lei Geral de Proteção de Dados Pessoais: manual de implementação. São Paulo: Thomson Reuters, 2019.

MARQUES, Cláudia **L; BEJAMIN, Antônio, H. V.; BESSA, Leonardo, R. Manual de Direito do Consumidor**. 6a ed. rev. atual. São Paulo: Editora Revista dos Tribunais, 2014.

MELO, Pedro, 2020. Disponível em https://acionista.com.br/wp-content/uploads/2020/12/RI-247-IBGC-COMUNICA-15-medidas-para-Governan%C3%A7a-por-Pedro-Melo-1.pdf.Acesso 11 de abril 2022.

MENDES, Gilmar F.; BRANCO, Paulo G. G. **Curso de Direito Constitucional**. 10a ed. ver atual. São Paulo: Saraiva, 2015.

MERCER do Brasil, 2020. **Empresas olham para o futuro do trabalho, a transformação das carreiras e a necessidade de requalificação de funcionários, aponta novo estudo da Mercer**. Disponível em: https://www .mercer.com.br/newsroom/tendencias-globais-de-talentos-2020.html Acesso em: 8 de abril 2022.

PALHARES, Felipe; PRADO, Luis Fernando; VIDIGAL, Paulo. **Compliance Dig ital e LGPD**. V volume. São Paulo: Editora Revista dos Tribunais, 2021.

SANTOS, Renato Almeida, 2011. Disponível em https://www.editoraroncarati.com.br/v2/phocadownload/compliance_ferramenta_mitigacao.pdf. Acesso 30 de março 2022.

ZANNE, Marcos, 2021. Disponível em: https://inova.globalweb.com.br/post/descubra-os-maiores-beneficios-que-o-compliance-traz-para-as-empresas. Acesso em: 8 de abril 2022.