CENTRO UNIVERSITÁRIO DO ESTADO DO PARÁ
CURSO DE BACHARELADO EM DIREITO

RAYANE CORRÊA DA SILVA

COMPLIANCE, CULTURA CORPORATIVA ÉTICA: uma análise sobre a Aplicação da Lei Geral de Proteção de Dados 13.709/18

BELÉM
2020

RAYANE CORRÊA DA SILVA

COMPLIANCE, CULTURA CORPORATIVA ÉTICA: uma análise sobre a Aplicação da Lei Geral de Proteção de Dados 13.709/18

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção de grau em Bacharel em Direito, pelo Centro Universitário do Estado do Pará.

Orientadora: Profa. Me. Amanda Maia Ramalho

BELÉM
2020

Dados Internacionais de Catalogação na Publicação (CIP)
Biblioteca do CESUPA, Belém – PA

S568n Silva, Rayane Corrêa da.

Compliance, cultura corporativa ética: uma análise sobre a aplicação da lei geral de proteção de dados 13.709/18 / Rayane Corrêa da Silva. – Belém, 2020.

22 p.

Trabalho de Conclusão de Curso (Graduação) – Centro Universitário do Estado do Pará, Bacharelado em Direito, Belém, 2020.
Orientador: Profa. Ma. Amanda Maia Ramalho

1. Proteção de dados. 2. Direito à privacidade. I. Ramalho, Amanda Maia (orient.). II. Título.

CDD 341.2738

Regina Coeli Araújo Ribeiro CRB-2/739

RAYANE CORRÊA DA SILVA

COMPLIANCE, CULTURA CORPORATIVA ÉTICA: uma análise sobre a Aplicação da Lei Geral de Proteção de Dados 13.709/18

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção de grau em Bacharel em Direito, pelo Centro Universitário do Estado do Pará.

Orientadora: Profa. Me. Amanda Maia Ramalho

Data de aprovação: _____/_____/_____

Conceito:

Banca Examinadora:

_____
Profa. Me. Amanda Maia Ramalho - Orientadora
Centro Universitário do Estado do Pará (CESUPA)

_____
Nome com titulação
Instituição a que pertence

_____
Nome com titulação
Instituição a que pertence

COMPLIANCE, CULTURA CORPORATIVA ÉTICA:

Uma análise sobre a Aplicação da Lei Geral de Proteção de Dados 13.709/18.

COMPLIANCE, ETHICAL CORPORATE CULTURE:

An analysis of the Application of the General Data Protection Law 13.709 / 18.

Rayane Corrêa da Silva[1]

Amanda Maia Ramalho[2]

Resumo: A recente aplicabilidade da Lei Geral de Proteção de Dados – LGPD, 13.709/2018, enseja regras quanto ao interesse legítimo na coleta, manipulação e tratamento de dados pessoais, por empresas e órgãos públicos. Justificando assim, a permissividade de uma Organização detentora dos dados, em acessá-los, utilizá-los e o compartilhá-los desde que protegidos direitos fundamentais tal como, a privacidade dos seus titulares. Nesse sentido, o objetivo deste trabalho é demonstrar a importância dos pilares de um programa de *Compliance* na promoção de uma Cultura Corporativa direcionada à ética e a integridade, cooperando com que Organizações que possuírem esse controle interno de conformidade adequem-se às diretrizes da Lei Geral de Proteção de Dados – LGPD. A metodologia utilizada baseou-se em uma abordagem qualitativa por meio de pesquisa revisão bibliográfica, com a utilização do método dedutivo-dialético em observância às legislações vigentes ligadas à tecnologia da informação e a políticas de privacidade como o Marco Civil da Internet e o Regulamento Europeu de Proteção de Dados, tendo ainda, por base a Pesquisa Maturidade do *Compliance* no Brasil – KPMG. Diante o exposto, conclui-se a importância do *Compliance* para além do cumprimento das barreiras legais e regulamentares, incorporando um modelo estratégico-sustentável às Organizações, o que respalda seus códigos de conduta, orienta as atividades dos seus membros e traz uma Governança Corporativa voltada à eficiência, a gestão de riscos e a segurança dos negócios.

Palavras- chave: Proteção de dados; *Compliance*, Cultura Corporativa, Ética.

Abstract: The recent applicability of the General Data Protection Law - LGPD, 13,709 / 2018, creates rules regarding the legitimate interest in the collection, manipulation and treatment of personal data, by companies and public agencies. Justifying, thus, the permissiveness of an Organization that owns the data, in accessing, using and sharing it, provided that fundamental rights such as the privacy of its owners are protected. In this sense, the objective of this work is to demonstrate the importance of the pillars of a Compliance program in the promotion of a Corporate Culture directed to ethics and integrity, cooperating with Organizations that have this internal compliance control to conform to the guidelines of the General Law Data Protection Act - LGPD. The methodology used was based on a qualitative approach through research bibliographic review, using the deductive-dialectical method in compliance with the current legislation related to information technology and privacy policies such as the Marco Civil da Internet and the European Data Protection Regulation, also based on the Compliance Maturity Survey in Brazil - KPMG. In view of the above, it is concluded the importance of Compliance beyond the fulfillment of legal and regulatory barriers, incorporating a strategic-sustainable model to Organizations, which supports their codes of conduct, guides the activities of its members and brings a Corporate Governance focused efficiency, risk management and business security.

[1] Graduanda em Direito no Centro Universitário do Estado do Pará. Cursando o 10º semestre.

[2] Graduada em Direito pelo Centro Universitário do Estado do Pará, Mestre em Direito pela UNAMA

Keyword: Data protection; *Compliance,* Corporate Culture, Ethics

INTRODUÇÃO

Diante os avanços da tecnologia da informação experimentado pela sociedade nos últimos anos e os novos espaços para a difusão de dados como a internet, fez-se necessário o surgimento de regulamentos específicos, que visam proteger a privacidade dos usuários.

As informações e dados podem individualizar pessoas, configurar suas opções, selecionar suas preferências e servir de capital para práticas de comercialização e prestação de serviços no meio digital. Com isso, fora inevitável que os diplomas normativos e o sistema jurídico se adequassem para atender e solucionar conflitos, essencialmente os que versam sobre a violação de dados pessoais.

A construção da esfera privada no mundo digital deve ser compreendida na possibilidade de o indivíduo controlar o acesso e o uso dos dados que constituem a sua identidade pessoal e permitem o livre desenvolvimento de sua personalidade. Diante essa sistemática surgiu a Lei Geral de Proteção de Dados (LGPD) Lei nº 13.709/2018, que busca regulamentar o acesso, tratamento e compartilhamento de dados pessoais dos usuários brasileiros.

Mas para tratar da implementação da referida Lei faz-se necessário observá-la em conjunto ao *Compliance*. Derivada do verbo em inglês, *"to comply"*, remete a ideia de agir em conformidade ao ordenado, por meio de atos, normas, leis e padrões éticos, capazes de instituir, de um ponto de vista estratégico, um padrão de conduta e seu efetivo cumprimento. Com isso, as práticas e os pilares do *Compliance* na tentativa de promover uma Cultura Corporativa direcionada à ética e a integridade nas Organizações buscam utilizar e adequar-se aos controles internos das diretrizes impostas pela Lei Geral de Proteção de Dados – LGPD.

Assim, o presente trabalho pretende abordar em como se dará a aplicação da Lei Geral de Proteção de Dados diante aos programas de *Compliance* e mediante a Cultura Corporativa ética instituídas pelas organizações empresariais. Nesse sentido, o artigo está estruturado em quatro tópicos, o primeiro abordará a era do direito digital e as implicações que exsurge da necessidade do novo Direito em criar regulamentações específicas para solucionar conflitos ligados ao uso de dados no meio digital. O segundo, tratará da Lei Geral de Proteção de Dados e sua evolução, dispondo sobre a competência de agir em acordo ao interesse legítimo na coleta, manipulação e tratamento dos dados pessoais.

O terceiro, versará acerca dos desafios das Organizações Corporativas quanto a aplicabilidade da Lei Geral de Proteção de Dados e o *Compliance* no acesso, utilização e compartilhamento dos dados pessoais de forma legal. Por fim, o quarto tópico demonstrará a

importância dos programas de *Compliance* junto a aplicabilidade da Lei Geral de Proteção de Dados tratando-os como parte estratégica de uma governança corporativa, minimamente sujeitos a falhas de gestão interpessoal, nos seus processos e operações alinhados aos códigos internos de conduta e aos requisitos emanados pela LGPD.

1. A ERA DO DIREITO DIGITAL

O Direito Digital ao longo dos últimos anos, tem como ponto central a solução de impasses ligados ao uso da tecnologia da informação no meio digital por seus usuários quanto indivíduos e provedores. Representando uma nova vertente jurídica, onde há incidência de normas aplicadas ao chamado *ciberespaço,* reconhecendo na prática que a legislação e a jurisprudência tradicional já não são suficientes para regular tais relações.

Cabe ainda, explanar o conceito de Direito Digital que, apesar de ser um ramo novo do Direito e possuir poucas normas jurídicas e regulamentos positivados, tem sido um assunto pertinente dentre os legisladores na atualidade. Peck (2007) refere-se ao Direito Digital como sendo um avanço do Direito, visto que contempla princípios atuais que ainda são aplicados, bem como possibilita a inserção de novos elementos para as outras áreas do mesmo.

De acordo com Paiva (2019) o Direito Digital se constitui de regulamentos que determinam as interações decorrentes no meio digital, para que se deem de forma harmônica. Esta disciplina em completo desenvolvimento alerta o senso comum para as implicações no manuseio, a exemplo dos dados pessoais, se tratando de um desafio para os operadores do Direito assegurar as garantias constitucionais e o direito à privacidade dos indivíduos, aqui selecionados como usuários e consumidores em potencial.

Cabe detalhar que apesar de deter uma hermenêutica diferenciada o Direito Digital ao coibir a prática de condutas lesivas, que geram a responsabilização dos agentes autorais, conecta-se de forma consultiva aos demais Direitos como Consumidor e Civil.

Nessa sequência, ao analisar a contextualização e evolução do Direito Digital, temos o Marco Civil da Internet, Lei nº 12.965/14, que será melhor abordada posteriormente, como pioneira na regulamentação do uso da Internet no Brasil, estabelecendo princípios, garantias, direitos e deveres aos envolvidos. Adiante, a Lei Geral de Proteção de Dados, visando tutelar direitos envolvendo o uso indevido dos dados pessoais. Logo, torna-se imprescindível que o Direito Digital venha regular situações conflitantes, já que a rápida circulação de informações poderá ocasionar falta de razoabilidade e proporção dentre as relações sociais. Portanto, ao se ter a informação como ativo básico do Direito Digital surge-se um dilema quanto aos limites

da circulação destes dados, uma vez que as práticas virtuais devem ser concebidas de forma transparente.

Vaz (2004) relata que a problematização entre ética e técnica sobre o que se gera nas redes se dá pela linha tênue entre liberdade e demasia, visto que a internet se torna atrativa justamente pela liberdade de experienciar o mundo em seus diversos aspectos através de interações com um simples toque dos dedos. Assim a delimitação se fará justamente para o que for excedente.

Tendo-se o Direito Digital como um componente estratégico no auxílio de um ambiente virtual seguro, de forma a regular, proteger, limitar e abster excessos nas relações oriundas da internet, haja vista, que promove segurança jurídica e responsabiliza aqueles os que atuarem de forma contrária e danosa.

1.1 O MARCO CIVIL DA INTERNET NO BRASIL

O Marco Civil da Internet no Brasil é a primeira norma regulada pelo Direito Digital atendendo a expansão do uso da Internet no país e estabelece diretrizes no intuito de inibir crimes cometidos no ambiente eletrônico, sendo maioria intermediados por canais provedores invasivos, publicações não autorizadas, que expõem informações confidenciais dos usuários.

No sentido de corrigir os conflitos existentes, foi criada em 23 de abril de 2014, a Lei Federal nº 12.965, conhecida como “Marco Civil da Internet”, trazendo para o ordenamento jurídico brasileiro a proteção de direitos e deveres para a utilização da internet, seja através do computador, celular, smartphone, ou qualquer outro meio de comunicação. (LEWENSTEIN, 2014, p.10)

Para tanto, Art. 3°, do Marco Civil da Internet o legislador preocupou-se em descrever os princípios da proteção à privacidade, intimidade e dos dados pessoais, aliando-os ao princípio da liberdade de expressão e traz como principal objetivo o acesso a todos à informação, de forma igualitária e participativa no exercício da sua cidadania, promovendo o uso de novas tecnologias de forma segura por usuários e provedores.

Cumpre ainda destacar que, a Constituição Federal de 1988, no seu artigo 5º e dispositivos, já protege amplamente os direitos individuais e coletivos, que versam sobre a liberdade de expressão, informação, privacidade, intimidade, honra e a imagem das pessoas.

No entanto, a constante evolução da sociedade em receptividade aos avanços tecnológicos, sobretudo os da informação finda-se por gerar relações virtuais diversificadas, criando-se a necessidade de leis específicas para regulá-las, bem como a tutela destes direitos, tidos como bens imateriais.

Prosseguindo com o raciocínio, vejamos o julgado:

> 1. A compensação por danos morais se impõe quando o direito à informação extrapola dolosamente os limites impostos no artigo 5.º, inciso V da Constituição Federal, causando prejuízos a outrem.
> 2. Há de se fazer um juízo de ponderação, a fim de se saber acerca da matéria e se houver críticas feitas com leviandade e o manifesto propósito de denegrir a honra do autor a ponto de caracterizar desvio ou abuso de direito, ou se ficou limitada narração ou crítica dirigida a assuntos do interesse do público em geral.
> 3. Não se desincumbindo a parte ré do ônus probatório que lhe cabia, nos termos do art. 373, inciso II, do CPC, impõe-se a condenação por veicular matéria acerca da personalidade, da conduta ou do caráter do autor, extrapolando o mero exercício do direito de imprensa dos réus." (Acórdão 1097811, unânime, Relator: CARLOS RODRIGUES, 6ª Turma Cível, data de julgamento: 2/5/2018) (RODRIGUES, 2018, p. 15)

Percebe-se que o Ministro da decisão acima, interpõe uma linha de ponderação e aduz que a compensação por danos morais se impõe quando o direito à informação extrapola dolosamente os limites impostos no artigo 5.º, inciso V da Constituição Federal, causando prejuízos a outrem.

De acordo Lewenstein (2014), quando usuários se conectam à internet e acessam as mais diversas plataformas estão passíveis a ceder informações, sejam pessoais ou de outras pessoas, o que pode fomentar a prática de crimes cometidos através dos dados disponibilizados e trazer insegurança jurídica no uso da rede.

Nesse ponto, vejamos o que dispõe o artigo décimo, *caput*, da referida lei:

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

Compreende-se sublimar, que o Marco Civil da Internet permeia três fundamentos essenciais são eles: neutralidade da rede, privacidade e liberdade de expressão.

Nesse tocante, Lewenstein (2014), define o primeiro baseado no tráfego de dados de forma idêntica por toda rede, independente da fonte, conteúdo ou destino, sem discriminação entre os usuários. Já o segundo, enfatiza à proteção dos dados pessoais e informações que podem identificar o usuário comumente utilizadas pelos provedores de acesso à internet. Enquanto, o terceiro garante igual direito aos usuários em difundir informações e opiniões na rede, responsabilizando-os quanto o conteúdo, retirados pelos provedores apenas em desacordo a políticas de privacidade, disposições legais ou mediante ordem judicial.

Diante do mencionado, vê-se que, as mudanças trazidas pelo Marco Civil da Internet impactam diretamente provedores e usuários da internet, bem como os procedimentos de

transferência dos dados na rede, resultando em uma maior segurança jurídica, visto a defesa de direitos e o emprego dos deveres nos ditames da Lei, seja de forma individual ou coletiva.

1.2 A PRIVACIDADE COMO UM DIREITO FUNDAMENTAL

De acordo com o art. 5°, inciso X da Constituição Federal, tem-se a privacidade como um direito individual inviolável.

Ocorre que em virtude das relações no âmbito digital e o rápido compartilhamento de informações, este direito acaba por ser infringido em certas práticas lesivas sem o consentimento, da agora, parte prejudicada assegurando a esta indenizações pelo dano material ou moral ocasionado.

Assim, dispõe Kildare Gonçalves Carvalho:

> (...) o direito de estar só e o direito à própria imagem, às vezes tão impiedo-samente exposta pelos meios de comunicação de massa, ganham eminência constitucional, protegendo-se o homem na sua intimidade e privacidade. O dano moral decorrente da violação desses direitos, além do dano material, será indenizado, encerrando assim a Constituição a polêmica até então existente no Direito brasileiro sobre a indenização do dano moral. (CARVALHO,2009, p. 752)

Nessa perspectiva, a privacidade está diretamente ligada a um conjunto de dados pessoais de cada indivíduo, onde caberá exclusivamente a este a titularidade de tais informações, estando estas de acordo com sua vontade, disponíveis ou sob sigilo.

Vale ressaltar que, o direito à privacidade consolidou-se anterior ao ordenamento brasileiro com a Convenção Europeia de Direitos Humanos de 1950 ao dispor em seu art. 8° acerca do direito ao respeito à vida privada e familiar.

Notemos o que diz o art. 8º da referida Convenção:

> 1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infracções penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros. (Convenção Europeia de Direitos Humanos, 1950, p. 10)

Tendo o Tribunal Europeu de Direitos Humanos, possibilitado diversas interpretações deste artigo em suas jurisprudências, levando-se a Diretiva 95/46/CE do Parlamento e Conselho Europeu, que relativiza à de proteção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e a livre circulação de destes na União Europeia.

Assim, o processamento de dados só poderá ser considerado legítimo se estiverem de acordo com o art. 7° da Diretiva 95/46 CE, que dispõe da seguinte maneira:

> Os Estados-membros estabelecerão que o tratamento de dados pessoais só poderá ser efetuado se: a) A pessoa em causa tiver dado de forma inequívoca o seu consentimento; ou b) O tratamento for necessário para a execução de um contrato no qual a pessoa em causa é parte ou de diligências prévias à formação do contrato decididas a pedido da pessoa em causa; ou c) O tratamento for necessário para cumprir uma obrigação legal à qual o responsável pelo tratamento esteja sujeito; ou d) O tratamento for necessário para a proteção de interesses vitais da pessoa em causa; ou e) O tratamento for necessário para a execução de uma missão de interesse público ou o exercício da autoridade pública de que é investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados; ou f) O tratamento for necessário para prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais da pessoa em causa, protegidos ao abrigo do nº 1 do art. 1º". (CE, 95/46, online)

Na prática com o avanço das plataformas digitais, as relações sociais estão se desenvolvendo cada vez mais digitalmente, expondo os indivíduos e os tornando vulneráveis quanto sua privacidade. Tal direito, no entanto, continua sendo debatido mundialmente e produzindo novas interpretações.

Conforme preceitua Fortes:

> Em perspectiva histórica mais recente, Tapper (1973) identifica duas maneiras de violação da privacidade. A primeira consiste na coleta de informações pessoais a segunda concentra-se no seu uso. O primeiro modo de violação da privacidade pode ser realizado de dois modos: ilícito, quando clandestinamente, alguém coleta informações pessoais, a fim de descobrir aquelas que ainda não se tornam públicas, lícito quando voluntariamente um indivíduo fornece informações pessoais para uma finalidade e, sem seu consentimento, tais informações são disponibilizadas para finalidade diversa. (FORTES, 2016)

Diante disso, interpõe-se que à proteção à privacidade mantém-se inerente a todo indivíduo não cabendo ser mitigada ou contida pelos avanços tecnológicos e as vantagens econômicas obtidas pelo enfraquecimento dos direitos da personalidade. Pois, não se pode lucrar de modo indevido sem o consentimento primário do indivíduo ou utilizar como matéria-prima seus dados privados.

2. A LEI GERAL DE PROTEÇÃO DE DADOS N° 13.709/2018 E SUA EVOLUÇÃO

Após o avanço temporal da tecnologia da informação, surgiu a necessidade econômico-social da proteção dos dados pessoais, neste enfoque, impondo limites éticos para sua coleta, tratamento, utilização e distribuição.

Com o fluxo de informações nas bases eletrônicas e a atual configuração tecnológica resultou-se na expansão significativa e aderência por parte dos consumidores, usuários, operadores e fornecedores às plataformas digitais precisando o ordenamento jurídico estabelecer novos mecanismos de regulamentação.

A LGPD surgiu nesse sentido com fundamentos à inviolabilidade da privacidade, intimidade, da honra e da imagem; visando com que um indivíduo tenha maior controle sobre seus dados pessoais, estabelecendo práticas transparentes para o recolhimento e uso dos dados por pessoa natural, ou jurídica, de direito público ou privado. De modo que, além de proteger a privacidade dos cidadãos, a Lei Geral de Proteção de Dados busca fomentar a inovação tecnológica gerando caminhos para que as Organizações em seus negócios possam oferecer segurança jurídica. (SOBRINHO, 2019).

Nesse sentido, trata Doneda:

> A proteção de dados pessoais é uma maneira indireta de atingir um objetivo último, que é a proteção da pessoa. Ao estabelecer um regime de obrigações para os responsáveis pelo tratamento de dados, bem como de direitos para os titulares destes, não se está meramente regulando um objeto externo à pessoa, porém uma representação da própria pessoa. Os dados pessoais, por definição, representam algum atributo de uma pessoa identificada ou identificável e, portanto, mantém uma ligação concreta e viva com a pessoa titular destes dados. (DONEDA,2010, p. 52)

Seguindo o mesmo raciocínio Cavalcanti e Santos (2018), visionam que é necessário adotar uma concepção de serviços, produtos e modelos de negócio que garantam direitos de proteção à privacidade e aos dados pessoais. Ainda nessa perspectiva, Demócrito (2002) relata que a propagação da utilização de computadores na atualidade resultou na ampliação dos centros de coleta e processamento de dados e informações pessoais, saindo da esfera restrita de agências governamentais, e levando as empresas privadas a possuírem meios para tal de maneira mais simples e relativamente menos custosa.

Reconhecendo a Lei Geral de Proteção de Dados, as limitações do indivíduo no controle das suas informações, tendo seus dados pessoais compreendidos como fatores integrais da sua personalidade. Apresentando um aporte de princípios no intuito de incumbir transparência e responsabilidade, àqueles que os manipulam.

Seguinte esta contextualização importa-se traçar um paradigma histórico da proteção de dados, sendo a matéria dividida pela doutrina, em quatro gerações, que serão brevemente citadas para melhor exposição deste trabalho.

De acordo com Doneda (2011), a primeira geração ligou-se à criação de uma ferramenta chamada banco de dados, que possibilitou a sistematização de volumes grandes de informações estruturados de acordo com uma determinada lógica. A verdadeira preocupação da geração era expandir a tecnologia de processar dados, contudo a proteção dos dados não era importante para o legislador.

Sobre o uso do banco de dados:

> A base de dados sendo um conjunto de informações referentes a um determinado setor do conhecimento humano, está organizada por meio de programas de computador

> especialmente desenvolvidos para esta finalidade, e é suscetível de ser utilizada em várias aplicações. WACHOWICZ (2005, p.13)

Ainda, para Doneda (2011), a segunda geração estava voltada para a informação e os dados pessoais, preocupando-se em proteger informações estritamente pessoais para que não fossem acessadas por terceiros sem a devida permissão.

Afirma, Pierre Catala:

> Mesmo que a pessoa em questão não seja a "autora" da informação, no sentido de sua concepção, ela é a titular legítima de seus elementos. Seu vínculo com o indivíduo é por demais estreito para que pudesse ser de outra forma. Quando o objeto dos dados é um sujeito de direito, a informação é um atributo da personalidade. (CATALA, 1983, p. 20)

Logo após, Doneda (2011), demonstra que na terceira geração começou-se a serem desenvolvidas leis de proteção de dados, com a ideia de que os cidadãos deveriam controle sobre essas informações pessoais e quais dados seus iriam ser coletados. Por fim, apontando a existência uma quarta geração, voltada para efetivação da proteção de dados garantindo os direitos fundamentais dos indivíduos.

Cumpre enfatizar que na Europa, a proteção de dados pessoais se desenvolveu desde os anos 70/80, compreendendo atenção especial ao princípio da dignidade humana, onde na consolidação europeia outros princípios estão interligados, como a proteção das pessoas singulares relativamente ao tratamento de dados pessoais como um direito fundamental.

Ainda se faz necessário explicar o importante marco da proteção dos dados pessoais ocorrido na União Europeia, ao ser aprovado o *General Data Protection Regulation* (Regulamento Geral sobre a Proteção de Dados Europeia) n° 679/2016, elencando seus Estados-membros, todos os indivíduos da União Europeia e presentes no Espaço Econômico Europeu criando assim, uma influência internacional, para que outros países como o Brasil pudesse normatizar o tema.

O Brasil já havia ratificado alguns acordos internacionais que tratavam da proteção de dados pessoais, como por exemplo, a Convenção de Berna de 1886 e estipulado algumas Leis internas, como no Código de Defesa do Consumidor, mas todas citadas, tratam brevemente a temática.

Sabe-se que o país é uma das nações interessadas em entrar na Organização de Cooperação e Desenvolvimento Econômico (OCDE), que tem como principal missão incentivar o progresso econômico e comercial a nível mundial. Sendo um dos requisitos de entrada na Organização Internacional, possuir uma legislação exclusiva voltada à proteção de dados pessoais. Nesse cenário, a Lei Geral de Proteção de Dados foi apresentada semelhante a

visão europeia quanto os princípios e fundamentos que baseiam o tratamento dos dados pessoais coletados e armazenados em território nacional, seja por Organizações Privadas ou Órgãos Públicos.

Cabendo ressaltar uma dualidade, como um dos desafios da sua implementação, onde as Organizações Corporativas que possuírem filiais nos países membros da União Europeia, devem estar atentas por intermédio dos seus setores de *Compliance* as duas legislações, LGPD e GDPR. Já que, nas políticas de dados, a lei brasileira trata a implementação de um programa de governança e privacidade como faculdade dos controladores de dados e o regulamento europeu atribui aos controladores de dados a obrigação de adotar medidas técnicas e administrativas adequadas para assegurar o cumprimento da legislação.

Deste modo, destaca-se que a referida Lei n° 13.709/2018, previu sua vigência para dezembro/2018, no tocante aos dispostos sobre as funções e a estrutura da Autoridade Nacional de Proteção de Dados (ANPD) e vinte e quatro meses após a data da publicação da Lei, ou seja, agosto/20 para os demais dispositivos.

Por conseguinte, em uma visão geral, os dispositivos de aplicabilidade da LGPD, observam o consentimento do titular dos dados pessoais. Porém, isto não significa dizer que ao consentir, a coleta dos dados estes poderão ser migrados por tempo indeterminado, devendo-se haver um tempo estipulado para o término do tratamento, que poderá ocorrer apenas nas hipóteses previstas em lei, independentemente do consentimento deste. Sendo uma lei que vale tanto para o setor público, quanto para o setor privado.

Inclusive a Lei Geral de Proteção de Dados não vem regular somente dados como nome, endereço de residência, número de RG, CPF, ou outros documentos, regula também a coleta e o tratamento dos dados capazes de individualizar uma pessoa como em respeito à sua origem, raça, etnia, sexo, religião, posicionamento político, biometria, dados bancários, os denominados dados sensíveis (COSTA, 2019).

Nesse sentido, Leme (2019), aduz que a LGPD estabelece o princípio da necessidade, em que as empresas só poderão fazer a coleta desses dados pessoais quando forem indispensáveis para execução de suas finalidades. Apenas devendo haver o compartilhamento de dados sensíveis entre empresas, nos casos de legitimidade dos controladores, quando os titulares dos dados pessoais forem obrigatoriamente informados sobre o feito, indicando quem será o receptor desses dados.

Conforme dispõe o art. 7°, inciso I da Lei 13.709/18 tem-se o consentimento do titular no manuseio dos dados como um de seus principais pilares, uma vez que, em muitos casos a concessão dos direitos sobre os dados pessoais não estão claros, de modo que o usuário acaba

por prejudicar-se ao anuir tacitamente uma cláusula, em botões pré-selecionados, de “ok”, “aceito”, “sim” e consentir acesso aos controladores sem possuir antes conhecimento adequado. Fazendo-se necessário esclarecer em que consistem esses dados pessoais e suas características, tendo em vista o crescimento exponencial da sua produção e a realidade causada pela *big data* com o aumento significativo e o vazamento de informações trocadas na realidade digital ou não sem fins específicos.

Assim, a LGPD determina o indivíduo como detentor das informações que o personalizam, tendo o domínio de modificá-las, transportá-las e excluí-las. Exigindo das Organizações transparência na captura dos dados e seu tratamento.

Partindo destas uma responsabilidade objetiva em agir com plausibilidade durante a utilização dos dados pessoais e sensíveis. Ainda, em manter o direito de acesso à informação aos titulares dos dados, que poderão a qualquer momento solicitar correções, atualizações e sua remoção. Algumas das adequações da Lei que tendem constituir procedimentos padrões internos dentro das Organizações Corporativas evitando perdas e penalidades pelo seu descumprimento.

2.1 OS DADOS PESSOAIS - CONCEITOS E ASPECTOS GERAIS

A menção que aqui se faz de “dados pessoais”, refere-se a peculiaridades termológicas. Para Doneda (2011), o termo “dado”, já faz referência a uma determinada informação, mesmo antes que esta seja processada ou interpretada. Podem ser vistos como “fatos brutos” que necessitam de um processamento adequado e organizado antes de serem repassados. (BIONI, 2019).

Ao fazermos a junção do termo “dado” com o termo “pessoal”, surgirá um vínculo objetivo, que está relacionado a uma pessoa, já que essas informações passarão a apresentar dados sobre ações e manifestações desta determinada pessoa.

Na visão de Doneda:

> Uma determinada informação pode possuir um vínculo objetivo com uma pessoa, revelando algo sobre ela. Este vínculo significa que a informação refere-se às características ou ações desta pessoa, que podem ser a ela atribuídas em conformidade com a lei, como no caso do nome civil ou do domicílio, ou então, às informações provenientes de seus atos, como os dados referentes ao seu consumo, informações provenientes de suas manifestações, como as opiniões que manifesta, e tantas outras. (DONEDA, 2006, p. 156)

É possível dizer que, apesar de já existirem leis anteriores que definem essa expressão, o conceito mais relevante de dados pessoais surgiu em 2016 com o *General Data Protection Regulation* – GDPR, onde para uma definição doutrinária das diretrizes dos dados pessoais,

surgiram duas correntes com amplitudes conceituais distintas, são elas a expansionista e a reducionista. A primeira corrente afirma que a pessoa titular dos dados pessoais é uma pessoa identificável e indeterminada e o vínculo desta pessoa com seus dados é mediata, indireta, imprecisa ou inexata.

Já para a outra corrente chamada reducionista, o titular do dado é uma pessoa específica, identificada e o vínculo entre eles se dará de forma imediata, direta, precisa (BIONI, 2018). Com base nisso, as diretrizes estabelecidas na GRPR se baseiam na corrente expansionista e através do seu art. 4°, n. 1 do Regulamento dispõe que:

> Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular (Regulamento Geral de Proteção de Dados, 2018, p. 39)

Nesta senda conceitual do regulamento europeu, corroborando para o Brasil, a Lei Geral de Proteção de Dados conceitua em seu art. 5, inciso I, que o dado pessoal pode ser caracterizado como uma informação pessoal que está relacionada a uma pessoa natural que pode ser identificável ou não, dessa forma observa-se que, a lei brasileira também aderiu à corrente expansionista.

Logo, de forma clara, segundo (LIMA, 2014), os dados pessoais caracterizam-se por uma série de informações inerentes a uma determinada pessoa, sendo possível ser dados cadastrais ou dados de maior relevância, como identidade, CPF, raça, política etc.

Nesse viés, considerando-se o disposto n° 51 do *General Data Protection Regulation* – GDPR estabelece-se que os dados serão classificados devido à sua natureza e por estarem ligados à direitos e liberdades fundamentais, merecem uma proteção especial e tratamento adequado.

Com isso, a Lei 13.709/18 se encarrega de elaborar uma seção exclusiva que visa tratar hipóteses específicas para o uso e manipulação desses dados, fazendo uma ressalva para aqueles dados denominados anônimos ou que passam por um processo de anonimização, já que não é possível identificar quem são seus titulares, disposto no art. 5°, inciso XI.

Ainda sobre a importância da proteção desses dados, em brilhante decisão o Ministro Ruy Rosado de Aguiar, dissertou acerca do correto tratamento de dados pessoais:

> A inserção de dados pessoais do cidadão em bancos de informações tem se constituído em uma das preocupações do Estado moderno, onde o uso da informática e a possibilidade de controle unificado das diversas atividades da pessoa, nas múltiplas situações de vida, permitem o conhecimento de sua conduta pública e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que

> deveria ficar restrita à sua intimidade; ao mesmo tempo, o cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo. E assim como o conjunto dessas informações, pode ser usado para fins lícitos, públicos e privados, na prevenção ou repressão de delitos, ou habilitando o particular a celebrar contratos com pleno conhecimento de causa, também pode servir, ao Estado ou ao particular, para alcançar fins contrários à moral ou ao Direito, como instrumento de perseguição política ou opressão econômica. STJ, Recurso Especial n. 22.337/RS, rel. Ministro Ruy Rosado de Aguiar, DJ 20/03/1995.

O Ministro pauta sua decisão na importância de um correto tratamento e proteção dos dados pessoais, alegando que com a evolução da tecnologia, os cidadãos passaram a utilizar de forma mais intensa os meios eletrônicos para resolver seus problemas.

Vejamos uma decisão nesse sentido:

> APELAÇÃO CÍVEL. OBRIGAÇÃO DE FAZER CUMULADA COM INDENIZAÇÃO POR DANOS MORAIS. RESPONSABILIDADE CIVIL. DANOS À IMAGEM E À HONRA. SÍTIO DE BUSCA GOOGLE SEARCH. DISPONIBILIZAÇÃO DE INFORMAÇÕES QUE VINCULAM O NOME DOS AUTORES A PREDICATIVOS QUE DEPRECIAM A SUA HONRA. SENTENÇA DE PROCEDÊNCIA. PREVENÇÃO DA CÂMARA. RÉU QUE É PARTE LEGÍTIMA PARA FIGURAR EM AÇÃO QUE VISA A REMOÇÃO DE CONTEÚDO OFENSIVO, VEICULADO NA INTERNET. NULIDADES, ARGUIDAS SOB O FUNDAMENTO DE INOBSERVÂNCIA DA LEI 12.965/2014, REJEITADAS. MARCO CIVIL DA INTERNET (LEI 12.965 /2014). INAPLICABILIDADE AOS CASOS ANTERIORES A SUA VIGÊNCIA. NOTIFICAÇÃO EXTRAJUDICIAL PARA EXCLUSÃO DO CONTEÚDO DIFAMATÓRIO, NÃO ATENDIDA. DEFERIMENTO DA TUTELA DE URGÊNCIA ANTECIPADA PARA DETERMINAR AO RÉU QUE RETIRE A MENSAGEM OFENSIVA. VIOLAÇÃO DO DIREITO DA PERSONALIDADE QUE ENSEJA A REPARAÇÃO POR DANO MORAL. DIREITO AO ESQUECIMENTO. DESNECESSIDADE DE INDICAÇÃO DA URL. AUTORES QUE APRESENTARAM INFORMAÇÕES SUFICIENTES PARA A LOCALIZAÇÃO DO CONTEÚDO OFENSIVO. PROVEDOR QUE POSSUI MEIOS PARA DESVINCULAR A PESQUISA DO NOME DOS AUTORES DAS PÁGINAS, INDICADAS. PRECEDENTES DO STJ. DANO MORAL, CONFIGURADO. MAJORAÇÃO DA VERBA INDENIZATÓRIA. HONORÁRIOS ADVOCATÍCIOS, FIXADOS EM VALOR PROPORCIONAL AO TRABALHO EXERCIDO E COMPLEXIDADE DA CAUSA. MAJORAÇÃO DOS HONORÁRIOS ADVOCATÍCIOS EM SEDE RECURSAL, NA FORMA DO ARTIGO 85, § 11 DO NCPC. MANUTENÇÃO DO VALOR DAS ASTREINTES. ERRO MATERIAL NO PRONUNCIAMENTO DO TERMO INICIAL DA MULTA PELO DESCUMPRIMENTO DA OBRIGAÇÃO DE FAZER. TERMO A QUO QUE SE DÁ A PARTIR DA INTIMAÇÃO PESSOAL DO DEVEDOR PARA CUMPRIMENTO DA OBRIGAÇÃO. PRECEDENTES DO STJ. MULTA, APLICADA POR ATO ATENTATÓRIO À DIGNIDADE DA JUSTIÇA, NO PERCENTUAL DE 20% POR CENTO. DESPROVIMENTO DO RECURSO DO RÉU. PARCIAL PROVIMENTO DO RECURSO DOS CASOS AUTORES. CÂMARA CÍVEL – APELAÇÃO CÍVEL Nº 0363103-46.2013.8.19.0001 – ESTADO DO RIO DE JANEIRO

Podendo-se concluir que as atividades no tratamento dos dados pessoais devem respeitar a boa-fé e os princípios da finalidade, da adequação, da necessidade e do livre acesso a qualidade de dados, da transparência, da responsabilização e da prestação de contas. Ou seja,

os dados pessoais precisam estar de acordo com o teor dos artigos 7° ao 10°, da Lei de Proteção de Dados, além de que aqueles dados considerados sensíveis devem passar por uma espécie de tratamento especial e respeitar os arts.11 ao 13° da mesma Lei.

O fato é que, as Organizações precisaram fazer uma revisão completa de todas as formas pelas quais se realizam a coleta e armazenamento dos dados pessoais, mesmo que encontrem dificuldades para implementar a LGPD.

2.2 OS DESAFIOS DE ADEQUAÇÃO DA LGPD PELAS ORGANIZAÇÕES CORPORATIVAS

Com a entrada em vigor da Lei de Proteção de Dados, as Organizações Corporativas precisam adequar-se ao cumprimento das regras impostas pela Lei. O primeiro passo será o mapeamento criterioso das atividades que cada departamento exercerá no que tange à coleta, tratamento e finalidade de dados pessoais. Neste ponto, a Organização especificará as funções de cada departamento e membros envolvidos no cumprimento dos requisitos da Lei.

Dentre os vários desafios encontrados na adequação das empresas à Lei, um deles será o reforço da conscientização da sociedade e do corporativismo ético de que os dados pessoais são bens a serem tutelados. Além do mais, as empresas precisam criar mecanismos internos efetivos de conformidade aos objetivos principais de proteção da Lei.

Nesse sentido, leciona Heliezer Viana:

> O assunto é complexo, pois envolve toda a estrutura da empresa, a cultura, os seus hábitos, processos, procedimentos de manuais, as políticas internas, o mapeamento e enquadramento de informações; ou seja, é um projeto que pode levar de quatro a seis meses, dependendo do tamanho da companhia. (VIANA, 2020, p. 01)

Outro desafio que será enfrentado pelos Organismos Corporativos na adequação ao regulamento, de acordo com Viana:

> Para quem vende produtos no e-commerce, por exemplo, quando for buscar as informações do cliente, é preciso passar o termo de consentimento, explicar qual é a sua política de segurança da informação e, permitir que ele depois de cadastrado possa visualizar os dados. Além disso, terá que explicar qual é a finalidade do uso da informação e quem terá acesso. Por fim, a área jurídica também deve ter a adequação de todas as políticas e contratos com um enquadramento de tratamento de dados de acordo com cada artigo e dispositivo da lei. (VIANA, 2020, p. 01)

Para isso, o fomento de uma Cultura e Governança Corporativa Ética torna-se imprescindível na adoção de boas práticas e efetiva proteção dos dados pessoais vinculados. Pois, ao avaliar os riscos, benefícios surgem desta correlação gerando uma margem competitiva

da Organização frente a concorrência no mercado onde atuam, já que falhas operacionais serão evitadas, até mesmo pressentidas por todo corpo organizacional.

O que por consequência dará credibilidade, lisura e uma imagem de confiança à Organização. Além de que, no mesmo cerne, toda área jurídica deverá fazer suas atualizações e ajustar-se, como por exemplo, aos contratos de confidencialidade, com cláusulas de privacidade ligadas ao manuseio de dados pessoais.

Diante o mencionado, se faz necessário um hábil gerenciamento do fluxo dos dados pessoais e sensíveis, fora os que envolvem crianças e adolescentes, já que se requerem cuidados diferenciados, bem como controles e proteção condizentes evitando riscos e casos de violação, vazamento de informações ou de uso indevido. Sem este entendimento torna-se impossível à empresa uma Governança Corporativa ética como anseia a LGPD.

3. *COMPLIANCE* E SEUS ASPECTOS GERAIS

O *Compliance* pode ser traduzido como um ato de conformidade, ou seja, é estar agindo de acordo com as leis, regras, os regulamentos externos e internos como uma forma de evitar descumprimentos legais.

Nas Organizações Corporativas o *Compliance* vem estruturando suas atividades com legitimidade em atenção à legalidade dos atos normativos determinados pelos órgãos reguladores e as legislações operantes, sendo na prática um conjunto de regras estabelecidas para o prosseguimento por parte dos seus funcionários, colaboradores e fornecedores visando um comportamento ético ao estarem cumprindo as disposições legais impostas, independente da esfera hierárquica onde atuam.

Ao analisar os conceitos de ética e moral que fazem parte do convívio em sociedade, entende-se que estes são indissociáveis da Cultura Corporativa, servindo de base para uma Governança consistente. Logo, atendidos os preceitos estipulados pelo *Compliance,* que versam sobre toda a atividade profissional realizada, as Organizações terão seus atos cada vez menos sujeitos a questionamentos subjetivos, sobre integridade e moralidade.

Nesse tocante, tem-se o *Compliance* como um instrumento que aproxima e estrutura a relação entre a Organização Corporativa, os membros envolvidos e o Estado. A citar, por exemplo, os atos de fiscalização onde verificam-se se as obrigações da Organização estão sendo exercidas perante o determinável em Lei.

André Cabete Fábio conceitua o *Compliance* da seguinte maneira:

> O *Compliance* é uma prática corporativa que pode ser tocada por um departamento interno da empresa ou de forma terceirizada. Seu objetivo é analisar o funcionamento da companhia e assegurar que suas condutas estejam de acordo com as regras

> administrativas e legais, sejam essas regras externas (do país, Estado e cidade onde ela atua) ou internas (da própria empresa). (FÁBIO, 2017, p.01)

Em meio deste conceito, os programas de Compliance acabam por difundir-se cada vez mais dentro das Organizações Corporativas, para além das práticas anticorrupção, desviadas do contexto legal, pois a ferramenta também auxilia uma Governança Corporativa Ética. Uma vez que, convertem-se princípios, valores e uma missão específica as ações concretas da Organização, alinhando-se interesses para uma organização estratégica, motivada na transparência das condutas que garantem melhorias e o crescimento sustentável da Organização.

Ainda sobre o *Compliance*, Abbi e Febraban dispõe da seguinte forma:

> Assegurar, em conjunto com as demais áreas, a adequação, fortalecimento e o funcionamento do Sistema de Controles Internos da Instituição, procurando mitigar os Riscos de acordo com a complexidade de seus negócios, bem como disseminar a cultura de controles para assegurar o cumprimento de leis e regulamentos existentes. Além de atuar na orientação e conscientização à prevenção de atividades e condutas que possam ocasionar riscos à imagem da instituição. (ABBI E FEBRABAN, 2009, p.07)

Entende-se que, o *Compliance* sustenta mecanismos relevantes para que as empresas andem em conformidade com os dispositivos legais, pois o Estado por si só não consegue realizar um controle absoluto de todas as entidades econômicas necessitando de auxílio.

Antonietto Rios dissertou sobre o tema:

> Modelos extremos se mostraram falhos, primeiro porque o Estado com suas limitações estruturais não consegue regular e controlar as especificidades de cada empresa e o incremento do risco gerado no âmbito de suas atividades, segundo porque as empresas possuem outros interesses econômicos que se sobressaem ao da autorregulação, não conferindo a atenção demandada pelos mecanismos de prevenção dos perigos provenientes de sua atividade. (RIOS, 2015, p. 346)

Sendo os mecanismos de *Compliance,* independentes, possuindo um caráter preventivo e fiscalizador do setor privado e auxiliador do setor público. Pois, como mencionado, o Estado possui limitações, estando o *Compliance,* colaborando de forma positiva e suprindo as necessidades de autofiscalização.

Nesta conjuntura, o *Compliance* vem se tornando essencial durante a necessidade de buscar-se um cenário econômico seguro, transparente, justo e ético, principalmente quando o assunto é a confiança entre as relações do negócio e segurança dos dados fornecidos. (COLARES, 2014)

Menciona Colares:

> Garantir a aderência e cumprimento de leis; desenvolver e fomentar princípios éticos e normas de conduta; implementar normas e regulamentos de conduta; criar sistemas de informação; desenvolver planos de contingência; monitorar e eliminar conflitos de interesses; realizar avaliações de risco periódicas; desenvolver treinamentos constantes e estabelecer relacionamento com os órgãos fiscalizadores, auditores

> internos e externos e associações relacionadas ao setor da companhia. (COLARES 2014, p. 64)

Insurge-se que, o *Compliance,* é a ligação dos preceitos éticos e o mundo jurídico, nas suas diversas esferas, podendo atuar dentre as Organizações em outras áreas, não somente, a corporativa.

No Brasil, o *Compliance* ganhou visibilidade a partir da Lei 12.846/2013, conhecida como Lei Anticorrupção, que trata da responsabilização objetiva administrativa e civil de empresas pela prática de atos contra a Administração Pública nacional ou estrangeira. Aqui, ao contextualizar o *Compliance*, observamos sua aplicação atuando em duas linhas de frente, a primeira versando sobre a criação de políticas públicas e mecanismos internos que possam ser eficazes na observância das Leis e a segunda assegurando que esses mecanismos serão cumpridos.

Para Santos, a implementação do *Compliance* no Brasil:

> A preocupação era apenas com a burocracia dos regulamentos e procedimentos, ou seja, foi inserido apenas no âmbito jurídico. Posteriormente percebeu-se que a notória complexidade das pessoas jurídicas inseridas no mercado era de grande medida. Dessa forma, foi concluído que o *Compliance* não se restringia apenas ao mundo jurídico, estava inserido na implementação, aceitação e treinamento, também na gestão da pessoa jurídica e no clima organizacional. Isto é, o mecanismo de conformidade fazia parte da organização desde sua implementação pela alta direção, a aceitação por parte de todos que exercessem seus devidos labores na empresa e no treinamento de todos para que passassem a aderir a um novo clima baseado em um código de ética específico munido de medidas íntegras e de transparência interna e externa à organização.(SANTOS, 2011, p. 05)

Nesse contexto, conforme Saavedre (2011) a implementação dos mecanismos de conformidade no Brasil, é encarado como um intermediador e conciliador nas relações negociais entre as Organizações Corporativas, o mercado e o Estado sendo os programas de *Compliance* uma espécie de "mandamento ético".

É possível dizer que, ao adotar os programas de *Compliance*, as empresas estejam resguardadas de lides judiciais, sendo possível evitá-las com a adesão de um monitoramento interno. Por este motivo que, preza-se por uma interação entre todos os setores da empresa criando um ambiente de trabalho onde todos convivam harmonicamente, tendo seus comportamentos padronizados, que respeitem acima de tudo o ordenamento jurídico, evitando por exemplo, atitudes racistas, abusos psicológicos, assédios em geral, atitudes de cunho preconceituoso, quanto religião, opção sexual, dentre outros. (NOVELLI, 2016)

O Conselho Administrativo de Defesa Econômica – CADE, aduz que:

> Por meio dos programas de *Compliance*, os agentes reforçam seu compromisso com os valores e objetivos ali explicitados, primordialmente com o cumprimento da legislação. Esse objetivo é bastante ambicioso e por isso mesmo ele requer não apenas

> a elaboração de uma série de procedimentos, mas também (e principalmente) uma mudança na cultura corporativa. O programa de *Compliance* terá resultados positivos quando conseguir incutir nos colaboradores a importância em fazer a coisa certa. (CADE, 2016, p. 9)

Assim, analisa-se o *Compliance* não apenas, como um diferencial, mas sim, um pré-requisito de sustentabilidade para uma Cultura Corporativa baseada na ética e integridade, respondendo a convergência global acerca do assunto e as mudanças regulatórias impulsionadas pelo rápido avanço tecnológico, necessidades estas, que redefinem as políticas internas e diretrizes corporativas.

3.1 ÉTICA CORPORATIVA

É possível dizer que, os Programas de *Compliance* estão diretamente atrelados ao conceito de Ética Corporativa que reúne os valores que orientam a forma e a conduta que uma entidade organizacional deve seguir.

A ética tem como fundamento, a construção dos valores que devem ser respeitados, principalmente na tomada de decisões e influencia diretamente nas estratégias e de uma Governança Corporativa.

Assim dispõe o Instituto Brasileiro de Ética nos negócios:

> Uma declaração do conjunto de direitos, deveres e responsabilidades empresariais para com todos os stakeholders e refletindo os princípios e os valores da empresa; a gestão social e ambiental; e o conjunto das normas de conduta para dirigentes, executivos e colaboradores, como também para os integrantes da cadeia produtiva, mediante os quais atuam as premissas que enriquecem os processos decisórios da empresa e orientam o seu comportamento. Além disso, deve ser o principal instrumento de governo e da gestão estratégica das empresas. (IBEN 2009, p. 53)

É por meio da Ética Corporativa que serão estabelecidos os princípios norteadores das condutas dos gestores, membros e colaboradores de uma Organização Empresarial determinando também como será o relacionamento com seu público-alvo. Tal estrutura recebe o nome de Ética Empresarial ou, de forma mais ampla, Ética Organizacional e é por meio deste conhecimento (*know-how*) que as empresas e organizações públicas e do terceiro setor incorporam, em suas atividades, contratos e operações baseadas em seus códigos morais (ética ou conduta).

O Código de Ética tem como objetivo trazer harmonia, ordem, transparência e tranquilidade para uma empresa, em razão dos referenciais que foram criados, embasando o cumprimento da sua missão e de seus compromissos.

Chalita aduz que:

> É absolutamente imprescindível que haja consistência e coerência entre o que está disposto no código de ética e o que se vive na organização. Caso contrário, ficaria patente uma falsidade que desfaz toda a imagem que a empresa pretende transmitir ao seu público. Essa é a grande desvantagem do código de ética. Há, ainda, aqueles que, considerando que a consciência ética dos integrantes de uma organização, desde os mais altos executivos até o mais simples funcionário, é um patrimônio do indivíduo, defendem a desnecessidade de se implantar códigos de ética, já que a atuação de cada um propiciará, por via de consequência, um ambiente. (CHALITA 2003, p. 67)

Nesse sentido, a postura ética de uma empresa reflete-se diretamente na conduta de seus profissionais. Não limitando-se ao mero cumprimento da legislação, sendo necessário uma soma de princípios éticos e morais operados por cada integrante. Em síntese, a Ética empresarial ou Organizacional é composta pelo conjunto de valores, princípios e fins que orientam o comportamento dentro da Organização e compõem sua cultura corporativa, influenciando estratégias, decisões, procedimentos e operações.

3.2 A VISÃO DO *COMPLIANCE* COMO UM NOVO MODELO DE NEGÓCIO

Com a evolução tecnológica digital, a difusão rápida de informações e novas perspectivas dos comportamentos sociais, as empresas na atualidade já não são avaliadas somente por sua substancialidade lucrativa, mas também por sua atuação frente o mercado que representam, como se comportam perante a concorrência e o ordenamento jurídico, por exemplo.

Durante muito tempo, grandes empresas foram envolvidas negativamente pelo descumprimento das normas legais, tendo suas penalidades expostas e credibilidade questionada no mercado e entorno social. Mediante essa situação, o *Compliance* passou a ser considerado um modelo de negócio, uma vez que dita a forma correta das execuções dentro de uma empresa.

De acordo com Stahler (2001), o *Compliance* intervém em três elementos fundamentais para constituição de um negócio, sendo estes, a proposição de valores, a arquitetura de uma cadeia de valores e um modelo de receita eficaz. Tornando assim o *Compliance* um plano de negócio para uma Organização Corporativa ganhando dentre os vários objetivos empregados, benefícios na competitividade concorrencial, quanto a produtividade, estruturação e manutenção da credibilidade corporativa, pois seu caráter preventivo evita demandas judiciais e autuações.

Nesse nível, observamos empresas sendo avaliadas positivamente por possuírem setores de *Compliance*, pois subentende-se que estas prezam pelo bom relacionamento entre seus agentes, funcionários, colaboradores e estão em observância às leis vigentes.

3.3 OS PILARES DO *COMPLIANCE*

Para entender sobre o *Compliance* na prática, se faz necessário uma breve explicação sobre os pilares que regem esse instrumento.

O primeiro pilar é denominado suporte da alta administração. Este princípio segue o entendimento de que os níveis mais elevados hierarquicamente da empresa devam ser os primeiros a seguirem as regras estabelecidas, servindo de exemplo para que os demais colaboradores no impacto e cumprimento das normas impostas. Ou seja, não basta que os líderes da organização apoiem as comunicações de *Compliance*, precisam ser os primeiros a segui-las.

O segundo pilar se dará na avaliação de riscos, também chamada de Mapeamento de Riscos de *Compliance*, sendo uma das etapas mais importantes da implementação de um programa de integridade, aqui é de suma relevância que, a empresa possa conhecer, dirimir ou mitigar todos os riscos do seu negócio, sendo fundamental manter-se tecnicamente sustentável, além de conseguir mapear possíveis riscos e corrigi-los, identificando falhas, a fim de evitar que haja um contencioso, seja judicial ou administrativo.

O terceiro pilar é o Código de Conduta e Políticas de *Compliance*, onde entende-se que o código de ética de uma empresa tem por dever ser ajustado de acordo com suas necessidades. O conjunto de regras e valores que estarão presentes neste código, deverão estar de acordo com os valores da empresa, para garantir uma cultura de integridade e valorização de comportamentos éticos.

Ademais, o quarto pilar aduz sobre os controles internos da empresa. Nos programas de *Compliance* registrar e arquivar documentos tem grande importância, todas as decisões tomadas pela empresa devem ser devidamente armazenadas, para que seja possível medir o desempenho de todos os processos, tendo uma visão adequada dos resultados obtidos.

O quinto pilar é o de treinamento e comunicação, devendo fazer parte da Cultura Corporativa de toda empresa nos programas de *Compliance*, uma vez que é através deste a eficácia do programa torna-se possível. Esses treinamentos e comunicação interna precisam ser realizados para que cada colaborador tenha a capacidade de efetivar os objetivos e regras comuns previstas no Código de conduta da empresa.

Há ainda o canal de denúncias, tido como o sexto pilar dos programas de *Compliance*, é através dessa ferramenta que a empresa poderá ser notificada de possíveis fraudes ou irregularidades que possam estar ocorrendo de forma anônima. Adiante como o sétimo pilar, temos a investigação interna, que vem logo após a denúncia. A empresa deverá fazer uma minuciosa investigação de forma sigilosa para averiguar a veracidade da denúncia.

O oitavo pilar se chama *Due Diligence*, ou em sede de tradução "diligência devida." Significa dizer que o *Compliance* não pode estar restrito ao comportamento apenas da Organização, fornecedores, representantes, distribuidores e outros parceiros também devem ser submetidos a análise antes de estabelecer-se uma relação contratual.

O penúltimo pilar é o da auditoria e monitoramento, observado que em programa de *Compliance,* é essencial o acompanhamento da sua manutenção, avaliando sua continuidade, execuções e se todas as esferas estão comprometidas com as normas e se todos os pilares estão cooperando como o esperado.

Por último, como décimo pilar teremos o de diversidade e inclusão como forma de prestigiar a temática e transformar o ambiente corporativo pautado no respeito e igualdade. Evidencia-se nesse tocante, a necessidade das Organizações Corporativas se adequarem à nova realidade, reconhecendo o auxílio prestado pelos programas de *Compliance* e seus pilares de sustentação.

4. A LEI GERAL DE PROTEÇÃO DE DADOS E O *COMPLIANCE*

A Lei Geral de Proteção de Dados irá instituir a figura do que denominamos de *Data Protection Officer* (DPO) de acordo com a tradução, o encarregado na proteção dos dados, que terá a responsabilidade de interligar a comunicação entre empresa, o titular dos dados pessoais e a Agência Nacional de Proteção de Dados. Este encarregado (DPO) deverá ser um profissional com conhecimentos na área de *Compliance*.

Assim, o *Compliance* poderá ser associado à LGPD, com o objetivo de proteger a sociedade contra o uso indevido e disfuncional dos dados ou informações pessoais. Essas informações nem sempre tem um caráter sigiloso, porém não podem ser utilizadas sem a expressa permissão do titular, uma vez que se estaria configurando invasão à privacidade. Ao tempo que tem de se exigir que se haja um consentimento explícito, consciente e inequívoco manifestação de anuência do indivíduo, para coleta e uso desses dados, além de ser opcional para os usuários a autorização, modificação, exclusão e qualquer dado que esteja inserido nas plataformas.

Para isso, faz-se essencial a satisfação de preceitos basilares de uma Governança Corporativa eficaz, como a necessária transparência na aferição do desejo efetivo das partes interessadas em disponibilizar suas informações, o tratamento isonômico de todas as partes interessadas levando em consideração direitos e deveres de cada uma, a prestação de contas da atuação dos agentes de governança, sempre de modo claro, compreensível e tempestivo e o a

responsabilidade corporativa no zelo para com a viabilidade econômico-financeira das organizações, visando diminuir os efeitos negativos dos negócios positivando-os.

Portanto, é através do seguimento destes preceitos que se formatará uma Governança Corporativa aliada ao *Compliance*, reforçando a identidade corporativa de uma Organização, além de proteger sua reputação e promover um crescimento sustentável para o negócio. Tão logo, com a vigência da LGPD, Organizações Corporativas e Instituições passaram a atualizar seus códigos de conduta, para que seus procedimentos internos estejam efetivamente voltados às normas de segurança da informação, de acordo com a nova Lei. Aderindo a uma abordagem estratégica capaz de gerenciar o compartilhamento e divulgação dos dados pessoais.

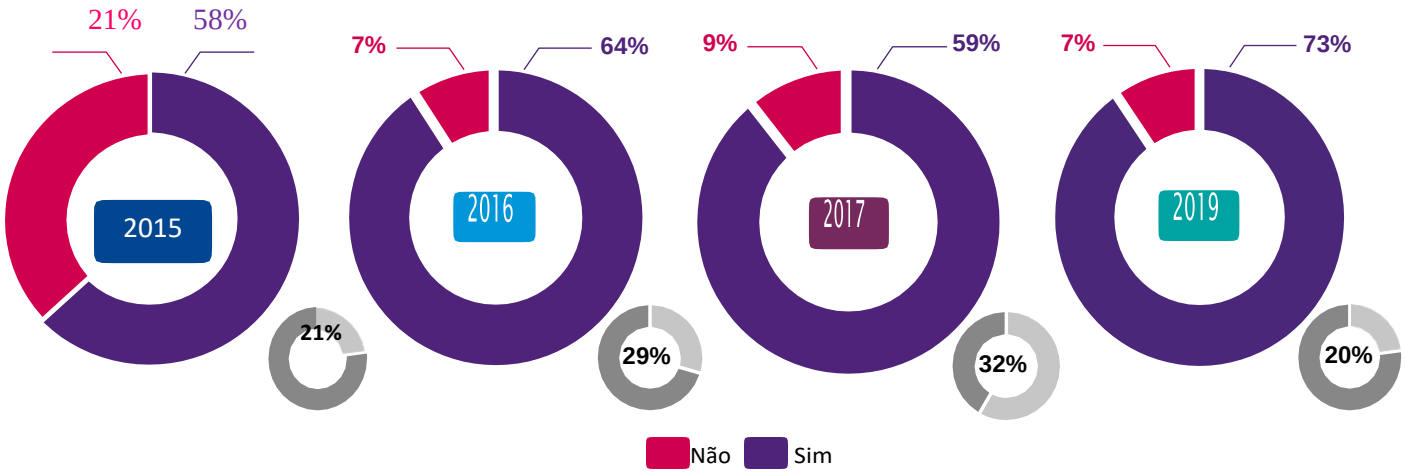
Além da adequação normativa, é preciso que em conjunto subsista uma estratégia de proteção a esses dados pessoais enquanto durar o ciclo de vida dos arquivos. Devendo os programas de *Compliance* incluírem regras que evitem invasões a infraestrutura da rede de controle do uso de dados de forma ilegal.

Assim, como primeiro passo para implementação da LGPD nas empresas, é necessário um estudo aprofundado do preceito normativo, compreendendo os principais objetivos contidos, identificando os agentes que estão envolvidos nas relações como titular, controlador, operador ou encarregado, e ainda selecionando quais os dados pessoais são essenciais, verificando como estão sendo coletados, se há ou não o consentimento do titular e para quais finalidades estão sendo destinados.

Há exemplo, em uma pesquisa realizada pela KPMG (2019), a cultura de ética e *Compliance* se mostrou fundamental para que a empresa tivesse sucesso, construindo um ecossistema sustentável que forneça base para relações saudáveis, éticas e transparentes entre seus colaboradores. Assim, a pesquisa buscou analisar o nível de maturidade dos setores relacionados à gestão de boas práticas, como a governança corporativa, comunicação e treinamento, pessoas e competências.

A seguir os resultados colhidos pela pesquisa com relação a Governança e a Cultura das empresas que demonstram os efeitos do reforço a cultura e governança de *Compliance*:

Gráfico de círculos – Os executivos seniores reforçam, periodicamente, que a governança e a cultura de *Compliance* são essenciais para o sucesso da estratégia da empresa (tone at the top and/or middle)?



Fonte: KPMG, 2019

De acordo com os dados obtidos na pesquisa, a governança e a cultura são essenciais para uma abordagem voltada ao gerenciamento de riscos de conformidade, além disso, as empresas necessitam de uma maior integração em seus esforços de governança e cultura, para que assim possam ter acesso às informações da companhia, principalmente dos riscos, identificando as causas-raiz do problema, de modo que se governança e cultura de *Compliance* forem sólidos, estará feito o suporte necessário para o sucesso das estratégias e das prioridades das empresas (KPMG,2019) .

Portanto, para que uma empresa consiga fazer a correta adaptação a LGPD é essencial que implemente uma boa Governança e cultura de *Compliance.* Alguns dos motivos pelos quais a Lei de Proteção de Dados aplica multas e sanções são apresentadas pela empresa Protiviti em seu manual de *Compliance* e LGPD (2019):

Vazamento de dados tais como: e-mails, nomes de usuários e senha. No total, mais de 800 mil dados foram vazados.

→

Insuficiência de informações disponibilizadas ao titular do dado sobre o tratamento de seus dados pessoais.

→

Inadequação de perfis em sistemas, tais como perfis de pessoas demitidas no banco de dados da empresa, com acesso a dados pessoais.

Fonte: Protiviti, 2019.

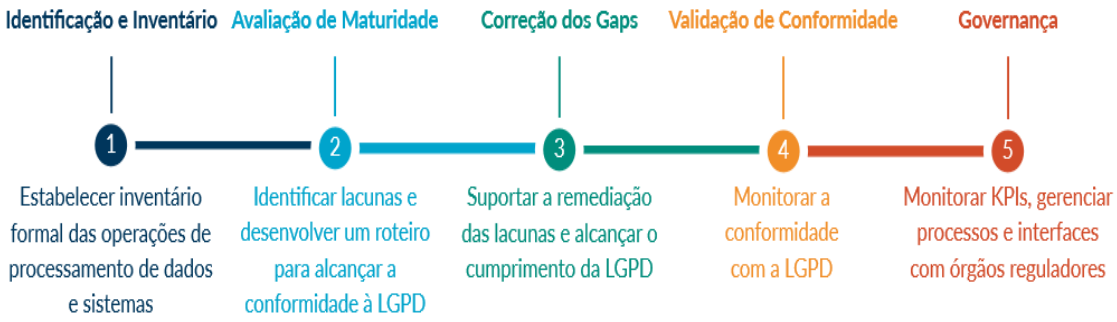
Demonstra-se, que a LGPD foi criada com base na Legislação Europeia, a *General Data Protection Regulation* e com base nisso foi que a empresa Protiviti (2019) elaborou alguns questionamentos necessários para aferir a capacidade de adequação aos códigos de conduta normativo interno e externo.

Questões acerca da ciência de colaboradores e funcionários quanto a importância da segurança da informação e da proteção de dados pessoais, se as empresas possuem processos definidos para lidar com incidentes de segurança da informação e se preexistem planos de remediação e notificação ao titular e à Autoridade Nacional de Proteção de Dados, se há pessoas responsáveis por atender às necessidades dos titulares dos dados e por fazer os devidos reportes à Autoridade Nacional de Proteção de Dados.

Além disso, elenca a necessidade de uma base legal identificada para cada tratamento de dados pessoais realizado, a imprescindibilidade de relatórios estruturados para reportar à Autoridade Nacional de Proteção de Dados e ainda se as empresas tem pleno conhecimento de onde estão todos os dados pessoais que possuem, sejam eles estruturados ou não estruturados (vídeos, arquivos de texto) (Protiviti, 2019).

Portanto, uma empresa que traga consigo um programa de *Compliance* com mecanismos de gestão de dados, e que estes estejam em concordância com o que estabelece a LGPD, eventos danosos futuros são evitados e se caso ainda ocorram, o programa de *Compliance* poderá ser usado como um elemento atenuante na dosimetria da punição que será aplicada pela autoridade fiscalizadora.

Ademais, vejamos um Fluxograma que representa as etapas de um programa de *Compliance* da empresa Protiviti:



Fonte: Protiviti, 2019.

Ante o exposto, os programas de *Compliance* tem como objetivo garantir que os regulamentos e políticas internas de proteção de dados sejam cumpridas pelos colaboradores preservando a capacidade institucional de exercer sua função sem que haja violação das diretrizes estabelecidas pela LGPD.

5. CONSIDERAÇÕES FINAIS

Constata-se que o *Compliance* sendo um instituto relativamente novo dentro do ordenamento jurídico brasileiro, porém, em potencialidade dentro das Organizações Corporativas, primordialmente compreendido como parte estratégica a implementação de boas práticas institucionais e de uma Governança Corporativa Ética.

Observando-se na visão do órgão regulador, como propósito da área citada, assistir os gestores das Organizações no gerenciamento dos riscos causados pela não conformidade às legislações e regulamentos operantes, evitando-se perdas legais, que resultam em empecilhos jurídicos ou mesmo prejuízos à reputação da Organização.

Evidentemente, que o movimento de promover a Cultura Corporativa Ética por meio das práticas de *Compliance* encontrará desafios na adequação e aplicabilidade da Lei Geral de Proteção de Dados. Entretanto, a novidade adequar-se-á cada vez mais, ao instrumento de *Compliance,* bem como a necessidade de tal estruturação, em consonância ao cenário atual voltado para a tecnologia de informação.

Desse modo, questões abordadas pela Lei Geral de Proteção de Dados, tais como a segurança da informação acerca do titular dos dados pessoais, seu direito inerente à privacidade, paralelo a responsabilização dos agentes controladores e operadores no tratamento dos dados pessoais, tendem ensejar controles de proteção, planos de ação aos mecanismos de implementação às exigências previstas em Lei.

Tal ideia é reforçada com a "Pesquisa Maturidade do *Compliance* no Brasil", que traz a Cultura Ética e o instituto do *Compliance* como determinantes para o sucesso, a perenidade das organizações e a construção de ecossistema sustentável corporativo entre seus membros.

Ao serem precedidos por um modelo de Governança eficaz, que elabora, revisa periodicamente, aprova, divulga procedimentos, inclui códigos de conduta, classifica exposições à riscos e realiza treinamentos operacionais.

Concluindo-se a importância do *Compliance* para além das barreiras legais e regulamentares, incorporando-o a um modelo de negócios estratégico e sustentável, a beneficiar as Organizações com princípios de integridade e conduta ética.

Dessa forma, deve-se ter em mente que, mesmo que nenhuma lei ou regulamento sejam descumpridos, ações que tragam impactos negativos geram automaticamente riscos à credibilidade, sanções e publicidade adversa, colocando em vulnerabilidade a continuidade de qualquer Organização Corporativa. Assim, torna-se vital para a nova realidade a compreensão do novo cenário político-econômico-jurídico mundial que se perfaz com a aplicação de leis de proteção de dados e sua adequação para com os setores de controle interno.

REFERÊNCIAS

ABBI; FEBRABAN. **Função de Compliance**. Disponível em: http://www.abbi.com.br/download/funcaodecompliance_09.pdf. Acesso em 22 ago. 2020;

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2018.

BIONI, B. R**. Xeque-Mate**: o tripé de proteção aos dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. GPoPAI/USP, 2015.

BRASIL. **Constituição (1988).** Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal: Centro Gráfico, 1988.

BRASIL, **LEI Nº 12.965, DE 23 DE ABRIL DE 2014**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011 2014/2014/lei/l12965.htm.

BRASIL. **Lei nº 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, 2 ago.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Redação dada pela Lei nº 13.853, de 2019. Brasília, DF: Senado Federal, 2018

CADE - **Conselho Administrativo de Defesa Econômica.** Guia programas de *Compliance*: orientações sobre a estruturação e benefícios da adoção de programas de *Compliance* concorrencial. Brasília, Distrito Federal, 2016.

CHALITA, Gabriel Benedito Issac. **Os dez mandamentos da ética. Rio de Janeiro:** Nova Fronteira, 2003.

CARVALHO, Kildare Gonçalves. Direito Constitucional. **Teoria do Estado e da Constituição. Direito Constitucional Positivo.** 12. ed. Belo Horizonte: Del Rey, 2006.

_____. Direito Constitucional. 15. ed., rev. atual. e ampl. Belo Horizonte: Del Rey, 2009.

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

CIDH – **COMISSÃO INTERAMERICANA DE DIREITOS HUMANOS.** Caso Trabalhadores da Fazenda Brasil Verde Vs. Brasil. Exceções Preliminares, Mérito, Reparações e Custas. Sentença de 20 de outubro de 2016.
Compilance e Lgpd. Protiviti,

Compliance e LGPG. Provitivi. 2019. Disponível em: https://www.protiviti.com/sites/default/files/brazil/insights/compliance_lgpd_-_protiviti_2019_0.pdf. Acesso em: 07 dez 2020.

COSTA, Juliana. **A importância da adequação da lei geral de proteção de dados aos programas de *Compliance.*** 2019. Disponível em: www.direitonet.com.br/artigos/exibir/10991/A-importancia-da-adequacao-dalei-geral-de-protecao-de-dados-aos-programas-de-compliancee. Acesso em: 02 jun. 2020

COLARES, Wilde. **Ética e Compliance nas empresas de outsourcing**. Monografia (Pósgraduação Lato Sensu em Direito – LLM). Insper Instituto de Ensino e Pesquisa, São Paulo, p. 21-192, 2014.

COMISSÃO EUROPEIA. **A Luta da União Europeia Contra a Fraude e a Corrupção**. No âmbito do Organismo Europeu de Luta Antifraude. Disponível em: Acesso em: 11 nov. 2020.

COMISSÃO EUROPEIA. Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (JO L 281 de 23.11.1995, p. 31).

DONEDA, D. (1). **A proteção dos dados pessoais como um direito fundamental**. Espaço Jurídico Journal of Law [EJJL], 12(2), 91-108.

DONEDA, Danilo. **A proteção de dados pessoais como direito fundamental**. Revista Espaço Jurídico 12/103. Joaçaba: Unoese, 2011.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

DONEDA, D. **A Proteção de dados pessoais nas relações de consumo:** para além da informação creditícia. Brasília: SDE/DPDC, 2010.

FÁBIO, André Cabbete. **O que é compliance**. E por que as empresas brasileiras têm aderido à prática. Disponível em: https://www.nexojornal.com.br/expresso/2017/07/24/O-que-%C3%A9-compliance.-E por-que-as-empresas-brasileiras-t%C3%AAm-aderido- %C3%A0-pr%C3%A1tica. Publicação em: 24 jul. 2017. Acesso em: 30 ago. 2020;

FORTES, V.B. (2016). **Os direitos de privacidade e proteção de dados pessoais na internet**. Rio de Janeiro: Lumen Juris.

INSTITUTO ÉTICA NOS NEGÓCIOS. **Pesquisa Código de Ética Corporativo no Brasil,** 2009. Disponível em: www.pesquisacodigodeetica.org.br. Acesso em: 20 de abril de 2020.

KPMG**. Pesquisa de maturidade do Compliance no Brasil**. 4ª edição. 2019. Disponível em: https://home.kpmg/br/pt/home/insights/2019/10/pesquisa-maturidade-compliance.html. Acesso em: 07 dez 2020.

LEME, Carolina. **Proteção e Tratamento de Dados sob o prisma da Legislação Vigente**. Interdisciplinary Boundaries of Law. v.1, n.1, p. 178-197. 2019.

LEWENSTEIN, Rafael Furtado. *Marco Civil da Internet: três princípios fundamentais ao uso da Internet no Brasil.* Artigo apresentado à Universidade Federal de Juiz de Fora: UFJF, 2014.

LIMA, Caio César Carvalho. **Marco Civil da Internet:** Garantia da privacidade e dados pessoais à luz do marco civil da internet. Organizadores: George Salomão e Ronaldo Lemos. São Paulo: Atlas, 2014.

NOVELLI, Breno. **Implementação de programa de compliance e seus impactos na área trabalhista.** Disponível em: https://www.direitonet.com.br/artigos/exibir/9732/Implementacao-de-programa decompliance-e-seus-impactos-na-area-trabalhista. Publicado em: 08 mai. 2016. Acesso em 09 nov. 2020;

PIERRE CATALA., "**Ebauche d'une théorie juridique de l'information**", *in*: Informatica e Diritto, ano IX, jan-apr. 1983, p. 20.

PINHEIRO, Patricia Peck. **Direito digital.** 6a. edição revisada, atualizada e ampliada – São Paulo: Saraiva, 2016

RIOS, Rodrigo; ANTONIETTO, Caio. **Prevenção e minimização de riscos na gestão da atividade empresarial.** Revista Brasileira de Ciências Criminais, São Paulo, v.23, n. 114, p.346, maio/jun. 2015

RODOTÁ, Stefano. **A vida na sociedade de vigilância: a privacidade hoje.** Rio de Janeiro: Renovar, 2008.p.24.

REGULAMENTO (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

RODRIGUES, edilma. D**úvidas e desafio para se adequarem à Lei Geral de Proteção de dados LGPD no Brasil**. Cantarino brasileiro.2020

SAAVEDRE, Giovani A. **Reflexões iniciais sobre criminal compliance.** Boletim IBCCRIM, São Paulo, ano 18, n. 218, p. 11, jan., 2011.

STJ. RECURSO ESPECIAL. 22.337/RS, rel. Ministro Ruy Rosado de Aguiar, DJ 20/03/1995, **JUSBRASIL**, 2018**.** Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/7204311/recurso-especial-resp-752135-rs-2005-0083236-3-stj/relatorio-e-voto-12952846.

SOBRINHO, Nayara. **A proteção de dados pessoais no e-commerce:** análise da aplicação da LGPD diante da vulnerabilidade do consumidor. 2019. Disponível em: http://pensaracademico.facig.edu.br/index.php/repositoriotcc/article/view/1745. Acesso em: 06 jun. 2020.

TRAPP, Hugo Leonardo do Amaral Ferreira. **Compliance na Lei Anticorrupção**: uma análise da aplicação prática do art. 7º, VIII, da Lei 12.846/2013. Boletim Jurídico, Uberaba/MG, a. 13, nº 1237, 3 mar. 2015.

WACHOWICZ, Marcos. **Cultura digital e marco civil da Internet**: contradições e impedimentos jurídicos no acesso à informação. In: DE LUCCA, Newton; SIMÃO, Adalberto; LIMA, Cíntia Rosa Pereira de (coords). Direito & Internet III – Tomo I: Marco Civil da Internet (Lei n. 12.965/2014). São Paulo: Quartier Latin, 2015.