DOI: 10.53660/CLM-3590-24M28

Compliance combined with LGPD as a tool to combat corruption

O Compliance aliada a LGPD como ferramenta de combate a corrupção

Received: 18-05-2024 | Accepted: 21-06-2024 | Published: 24-06-2024

Timoteo David Marcelino de Oliveira
ORCID: https://orcid.org/0000-0002-6931-9939
Universidade de Rio Verde, Brasil
E-mail: vvtnc@yahoo.com.br
Bacus de Oliveira Nahime
ORCID: https://orcid.org/0000-0002-7292-7919
Unirversidade de Rio Verde, Brasil
E-mail:bacus@unirv.edu.br
Fabrício Muraro Novais
ORCID: https://orcid.org/0000-0002-6367-530X
Universidade de Rio Verde, Brasil
E-mail: fabriciomuraro@uol.com.br

ABSTRACT

This is research on Compliance acting as a risk prevention model in the management of organizations, addressing the reduction of fraud and corruption risks. Due to this entire scenario, the following problem arises: What is the significance of Compliance in relation to the management of organizations? The objective of this study is to present the importance of companies adopting and following the Compliance program, taking into account this mechanism for preventing risks of an illicit nature. The specific objectives aim to identify and conceptualize corruption and organizational fraud; the importance of Digital Compliance in business management has been demonstrated; understand Digital Compliance as a Compliance mechanism, analyzing how its application can directly affect organizations; research good practices such as Compliance strategies. The test work will be developed through the analysis of the importance of implementing Digital Compliance in the organizational environment with the aim of prevention, in addition to indicating and reducing issues related to the risks of fraud and corruption.
Keywords: Prevention; Management of organizations; General Data Protection Law.

RESUMO

Trata-se de pesquisa sobre o *Compliance* atuando como modelo de prevenção nos riscos na gestão das organizações, abordando a diminuição de riscos de fraude e corrupção. Mercê a todo este cenário, surge a seguinte problemática: Qual a significância do *Compliance* frente a gestão das organizações? O objetivo do presente estudo é apresentar a importância das empresas em adotarem e seguirem o programa de *Compliance* levando em conta esse mecanismo de prevenção aos riscos de natureza ilícita. Os objetivos específicos pretendem identificar e conceituar corrupção e fraude organizacional; restar demonstrado a importância do *Compliance* Digital na gestão empresarial; entender *o Compliance* Digital como mecanismo de *Compliance*, analisando como sua aplicação pode incidir diretamente as organizações; pesquisar boas práticas como estratégias de *Compliance*. O trabalho em testilha será desenvolvido através da análise da importância da implantação do *Compliance* Digital no meio organizacional com o fito de prevenção, além de indicar e diminuir questões relacionadas aos riscos de fraude e corrupção.
Palavras-chave: Prevenção; Gestão das organizações; Lei Geral de Proteção de Dados.

INTRODUÇÃO

Na atualidade o tema "*Compliance* como modelo de prevenção aos riscos na gestão das organizações", que por sua vez procura diminuir os riscos de fraude e corrupção, esse termo tem origem no verbo inglês to comply, cujo significado é agir de acordo com uma regra, uma instrução interna, um comando ou pedido. Conforme Assi (2013, p. 152), *Compliance* significa estar em *Compliance* com leis e regulamentos externos e internos. Assim, entende-se por atender aos normativos dos órgãos reguladores como manter a empresa em *Compliance*.

Nos moldes dos documentos elaborado pelas associações de bancos ABBI (Associação Bancos Internacionais) e FEBRABAN (Federação Brasileira de Bancos), o *Compliance* é o dever de cumprir, cumprir e aplicar regras, restrições internas e externas impostas às atividades da organização. Ainda nessa margem e, conforme a FEBRABAN (2003), além de estar ligado a investimento em pessoas, processos e conscientização, assim é necessário que as pessoas estejam cientes do quão importante é estar de acordo com leis, regulamentos internos e externos das diferentes organizações e paises (FEBRABAN, 2003, s/p).

Segundo Coimbra e Manzi (2010, p.123), o estruturar e o colocar em funcionamento um programa de *Compliance* podem não ser suficientes para fazer com que a empresa ou uma entidade sem fins lucrativos ou até mesmo um órgão público seja posto à prova de desvio de conduta e de outras mazelas decorrentes. Destarte, poderá ser utilizada com o fito de proteger à integridade, com a diminuição de riscos e aperfeiçoamento do sistema de controles internos e combate a fraudes e corrupção.

A importância em se estudar sobre o tema recai no fato de que, hodiernamente, no mundo globalizado, nota-se constantemente nas mídias com organizações públicas e privadas o envolvimento em escândalos de fraude e corrupção, malgrado existirem leis, normas, códigos de conduta que sinalizam e orientam na prevenção de crimes tais, se faz mister a compreensão quanto ao uso do *Compliance* como instrumento, para fazer cumprir os regulamentos.

Este estudo visa demonstrar a importância do programa de Compliance digital para as empresas, e o que essa ferramenta traduz como prevenção aos riscos de natureza ilícita. De modo específico visa além de identificações de falhas, outrossim conceituar fraude organizacional e corrupção, também entender o *Compliance* como mecanismo de

transparência, observando como sua inserção atinge as organizações e demonstrar boas práticas como estratégias de gestão.

A seguir, será desenvolvido por meio da análise da importância da implantação do *Compliance* Digital no meio organizacional com a finalidade de precaver, mostrar e mitigar questões que dizem respeito aos riscos de fraude e corrupção nas diferentes organizações. O procedimento metodológico aplicado será a pesquisa bibliográfica, a partir da busca das diversas contribuições científicas sobre o tema abordado.

REVISÃO DA LITERATURA

A ideia de programas de *Compliance* originou-se nos Estados Unidos no século XX, ocasião em que as agências reguladoras começaram a surgir. Em 1906, com a promulgação do Food and Drug Act e a criação do FDA, o governo norte-americano criou um modelo centralizado de fiscalização com o intuito de regulamentar certar atividades que diziam respeito a saúde alimentar e a comercialização de medicamentos. Contudo, foi por causa das instituições financeiras que o *Compliance* seguiu adiante. No ano de 1913, criou-se o *Federal Reserve System* (Banco Central dos EUA), tendo ele o escopo de criar um sistema financeiro mais estável, seguro e adequado às Leis (Assi, 2013, p.18).

Já em 1977, fora promulgada o FCPA (*Foreign Corrupt Practices Act*)[1], a lei anticorrupção transnacional norte-americana, que forçava as empresas a (I) manter registros e livros que refletiam exatamente as suas operações e (II) criar um sistema eficaz interno de controles. Na década seguinte, depois do escândalo que envolveu a indústria de defesa, as empresas desse setor resolveram criar espontaneamente a DII (Iniciativa da Indústria de Defesa), que montou um conjunto de princípios de ética e de boa conduta empresarial.

Entrando no ano de 1991, a Comissão de Penas dos EUA editou e fez publicar um documento Diretrizes Federais para a Condenação de Organizações[2], que visava articular os elementos próprios de um programa de *Compliance* e ética eficaz. Segundo esse documento, aquelas empresas que mostrassem os mencionados programas teriam penas mais brandas caso incorressem em algum deslize. Aqui no Brasil, em junho de 2009, a CGU e o Instituto Ethos publicaram o seguinte documento: "A Responsabilidade Social das Empresas no Combate à Corrupção", seria o primeiro guia brasileiro para orientação

[1] Retirado de: https://www.sec.gov/enforcement/foreign-corrupt-practices-act.
[2] UNITED STATES SENTENCING GUIDELINES. **Federal Sentencing Guidelines Manual**.1991.

de ações das empresas que se preocupassem em dar a sua contribuição para o surgimento um lugar íntegro e de combate à corrupção (Ethos, 2018, p.2).

Em se tratando de matéria legislativa, temos como a primeira lei a regular um programa de *Compliance* a Lei nº 12.846/2013 (Lei da Empresa Limpa), a qual disciplinou a responsabilidade objetiva das pessoas jurídicas que incorressem na prática de atos contra a Administração Pública Direta ou Indireta, com a aplicação de multas de até 20% de seu faturamento bruto anual. O decreto nº 8.420/2015, por sua vez, leciona no sentido de que as pessoas jurídicas que terem e aplicarem um programa de integridade, irão receber até 20% de desconto no valor da multa (Brasil, 2013).

Abril de 2015, a CGU, via Portaria nº 909/2015, estabeleceu critérios de análise dos programas de integridade das empresas como requisito para concessão de redução no valor da multa, onde estabeleceu três faces de análise no cumprimento dos requisitos. *In limine*, a empresa terá que provar que o programa de integridade foi estabelecido nos moldes do seu tamanho, posicionamento e perfil de mercado, bem como, outrossim, restará comprovado o histórico de aplicabilidade desse programa e resultados atingidos anteriormente na prevenção de atos lesivos. Outra vertente será a demonstração no sentido de que o programa fora aplicado no próprio ato lesivo em tela, tendo sito positivo como prevenção contra um dano maior ou na reparação do prejuízo causado (Brasil, 2015)

A necessidade crescente de uma regulação e surgimento de critérios de transparência ficou mais evidente na década de 1970. Contudo, foi na década de 1940 que apareceu o primeiro modelo sistêmico de regramento, procedimentos e instituições para uma regulagem da política econômica internacional, a qual ficou conhecida como Acordo de *Bretton Woods*. Foi aqui que se criou o BIRD (Banco Internacional para a Reconstrução e Desenvolvimento), que posteriormente deu origem ao Banco Mundial, e ao FMI (Fundo Monetário Internacional).

O respectivo acordo criou obrigação que ligou os países signatários forçando-os a adotarem e a manterem uma política monetária com a finalidade de preservar suas moedas dentro de uma determinada taxa de câmbio. O sistema, no entanto, foi suspenso em 1971 por Richard Nixon e, em contrapartida às cenas de inúmeras incertezas geradas, é que surgiu o Comitê da Basiléia cujo objetivo era proteger o sistema financeiro, atrelado ao estabelecimento de balizas de boas práticas e procedimentos financeiros (Manzi, 2008, p. 109).

Ainda na década de 1970, devido aos escândalos de Watergate, aprovou-se, pelo congresso note americano a FCPA (Foreign Corrupt Practice Act), principal ou uma das

principais referências americanas no que tange a anticorrupção. É a partir daí, que o governo americano intensificou a fiscalização frente as atividades das empresas não apenas interna, mas outrossim daquelas ao redor do mundo. Poderia ser qualquer companhia que entrasse em negociata com ações em bolsas americanas ou empresas locais com operações fora do País eram alvos potenciais de investigações e, destarte, punidas pela FCPA.

De outra banda, aqui no Brasil, no ano de 1990, o mercado começava sua abertura comercial e, dessarte, as pressões para alinhamento aos padrões de competitividade e transparência face ao mundo lá fora só aumentavam, principalmente no quesito a regulagem por aqueles órgãos internacionais, a saber: BIS (Bank for International Settlements) e SEC (Securities and Exchange Comission) (Coimbra; Manzi, 2010, p.193).

Já em 1997, o Comitê da Basiléia começou a dizer as orientações aos bancos centrais no que se referia a garantia de rigidez em seus sistemas financeiros, delineando escopo e responsabilidades. No Século XXI, o mundo foi pego de surpresa com os ataques terroristas do 11 de setembro nos USA, tendo enorme impacto não apenas na política como esperado, mas também no mercado financeiro, o qual foi bastante abalado por essa tragédia e escândalos a seguir (Coimbra; Manzi, 2010, p.194).

Esse arcabouço edificado na época, forçou uma nova reflexão sobre o sistema de controle e regulação e pontuou, ainda mais, a necessidade de criação de regras mais rígidas. Foi então, nesse contexto, que se editou a Lei Sarbanes-Oxley, também conhecida como SarBox ou SOX. Seu objetivo foi a criação de mecanismos de auditoria e segurança confiáveis, além de criação de regramento alinhavado e comitês responsáveis pela supervisão dessas operações, procurando reduzir os riscos do negócio, daí se evitaria fraudes e criaria meios de identificação de irregularidades, na busca de total transparência nos negócios (Manzi, 2008, p.96).

No Brasil, regras análogas estavam sendo aceitas pelo Conselho Monetário Nacional, como por exemplo a Resolução n. 2.554 de 1998, porém, até as empresas brasileiras poderiam estar sujeitas à SOX, desde que tivessem ações negociadas no mercado americano. Além disso, em 2011, a legislação anticoncorrencial pátria foi renovada com a Lei 12.529, ficando estruturado, desta forma, o Sistema Brasileiro de Defesa da Concorrência, restando fortalecido ainda mais o CADE (Conselho Administrativo de Defesa Econômica), sendo impreterível e necessária a sua análise em atos de concentração. *Alfim*, em 2013, talvez mercê das pressões sociais sofridas, o que acelerou o processo de aprovação de uma lei que regulasse as práticas de corrupção no

país, foi então que passou, finalmente, a viger em janeiro de 2014 a Lei 12.846/13, chamada de Lei Anticorrupção ou LAC.

RESULTADOS E DISCUSSÃO

Malgrado ter características inerentes a cada empresa, dependendo essencialmente da cultura organizacional, os programas de *Compliance* conservam em si elementos que podem ser definidos como requisitos essenciais a todas as empresas, pouco importando sua cultura, campo de atuação, tamanho e estrutura. Destarte, existem diversos exemplos, podendo citar o da OCDE, que em 2010 estabeleceu o Guia de Boas Práticas em Controles Internos, Ética e *Compliance*.

Na linha de Debbie Troklus e Sheryl Vacca, (2013, p.227), é apontado sete elementos essenciais para que um programa de Compliance seja classificado eficiente. Estabelecer padrões de conduta, políticas e procedimentos internos. Essas ferramentas serão primordiais para o alicerce de um bom programa de *Compliance*. Precisam, portanto, ser desenvolvidas levando em conta a cultura organizacional, o ramo em que a empresa atua e o perfil dos seus colaboradores.

Primordialmente, contudo, essas normas internas mister serem anunciadas a todos os fornecedores e colaboradores de todos os níveis da companhia e, com o intento de garantir que a comunicação seja feita de maneira eficiente, é salutar que os documentos estejam transcritos de forma legível e inteligível, a fim de que haja fácil absorção por parte daqueles que irão participar o mencionado programa. Desta forma, as empresas multinacionais que atuam em vários Países devem ter a cautela de utilizar a tradução de maior compreensão por parte dos seus usuários (Coimbra; Manzi, 2010, p.209).

A notícia dessas normas, quando possível, deve ser feita presencialmente, com treinamentos e abrindo a possibilidade para questionamentos e esclarecimento de eventuais dúvidas. Em se tratando de versões online, é aconselhável haver avaliações de absorção de conhecimento, quando houver treinamentos presenciais, principalmente quando houver um número maior de participantes. Tais procedimentos podem ser bastante úteis quando houver a necessidade de demonstrar a eficiência do programa junto às autoridades, sem dizer que é mister e curial que as políticas e procedimentos sejam de fato cumpridos e não fiquem apenas no papel ou executadas por uma camada de colaboradores.

É necessário ficar bem claro a todos que elas são aplicáveis a toda a empresa e isso independe do cargo ocupado, desde o simples faxineiro até o seu gestor mais elevado. Isso pode ser garantido pelo envolvimento do Presidente, CEO ou autoridade

correspondente. Para assegurar uma abordagem ampla e eficiente, as políticas e procedimentos considerados estruturais, *i. e.*, aqueles que criam os alicerces para o funcionamento do programa de *Compliance*, devem, antes de mais nada, conter os seguintes elementos (Assi, 2013, p.160):

- Diretivas/missão do programa de *Compliance*;
- Regras para revisão constante e criação de novas políticas e procedimentos;
- Papel bem acentuado do *Compliance* Officer, Gerente de *Compliance* ou cargo análogo;
- Existência de um Comitê de *Compliance* com papel bem especificado;
- Metodologia para denúncia anônima (melhores práticas) ou pelo menos com credibilidade e confiabilidade e garantia de não retaliação e não retribuição, que deve ficar clara para todos os colaboradores;
- Estabelecimento de processos de auditoria e monitoramento de tempos em tempos;
- Metodologia de resolução de denúncias de possíveis mal condutas.
- Ações disciplinares bem definidas e em harmonia com as políticas da área de Recursos Humanos;
- Procedimentos de destruição de arquivos.

No entanto, as políticas e procedimentos que recebem o nome de substantivos, que são aqueles que efetivamente definem a aplicação das regulações, necessário conter os seguintes pontos:

- Processos de prevenção para ações inapropriadas em áreas de risco específico em que ainda não haja políticas definidas;
- Delimitar áreas de risco chave nas quais ainda não existam políticas e procedimentos específicos;
- Requisitos para documentação.

Afim de que se garanta uma abordagem ampla e eficaz, as políticas e procedimentos ditos estruturais, explico, aqueles que criam as bases para o funcionamento do programa de *Compliance*, devem, preferencialmente, conter os seguintes elementos:

- As diretivas ou missão do programa de *Compliance*;
- Regras para revisão constante e criação de novas políticas e procedimentos;
- Um papel bem definido do *Compliance* Officer, Gerente de *Compliance* ou cargo similar;

- Existência de um Comitê de *Compliance* com papel bem definido;
- Metodologia para denúncia anônima (melhores práticas) ou pelo menos que seja confiável no que tange ao sigilo, a fim de que não ocorra uma retaliação e não retribuição, que deve ficar clara para todos os colaboradores;
- Estabelecimento de processos de auditoria e monitoramento periódicos;
- Metodologia de resolução de denúncias de possíveis mal condutas.
- Ações disciplinares bem claras e em harmonia com as políticas da área de Recursos Humanos;
- Procedimentos de destruição de arquivos.

No que se refere as políticas e procedimentos chamados de substantivos, devem conter os pontos abaixo:

- Processos de prevenção para ações impróprias em áreas de risco especificado em que ainda não haja políticas definidas;
- Definir áreas de risco chave nas quais ainda não existam políticas e procedimentos específicos;
- Requisitos para documentação.
- Assegurar que a gerência atue de forma correta para solucionar problemas identificados.

As boas práticas de mercado vêm considerando que o profissional de *Compliance* não é capaz suficiente a fim de garantir um ambiente totalmente aderente às normas, políticas e procedimentos estabelecidos. Necessário a existência de um comitê de *Compliance*, sendo um diferencial de suma importância e que torna as atividades de *Compliance* ainda mais consistentes. Dentre suas funções, podem ser destacadas (Assi, 2013, p.159):

- Análise de requisitos legais e áreas de risco especificadas;
- Revisão regular e avaliação de aderência das políticas e procedimentos;
- Assessoria no desenvolvimento de padrões de conduta, políticas e procedimentos;
- Monitoramento de sistemas internos relacionados aos padrões, políticas e procedimentos;
- Revisão de diretrizes e normas do setor em que a empresa atua;
- Determinação da estratégia mais apropriada para promover o Compliance na companhia.

O comitê deve ser composto, preferencialmente, por indivíduos de diversos departamentos, com perfil condizente a essa função, que consigam transmitir o espírito do programa para toda a companhia. Preferencialmente, o Compliance officer é escolhido pelo comitê e pode inclusive fazer parte dele. Vale ressaltar também um outro elemento essencial que é a educação, a formação dada aos colaboradores por meio de treinamentos. É por meio deles e, em especial, os presenciais, que realmente se consegue atingir o público desejado e conquistar a colaboração da grande maioria no desenrolar de um *Compliance* eficaz.

World Trade Council for Sustainable Development em 1998, bem conceitua responsabilidade social, afirmando que "trata-se do compromisso constante dos empresários em adotar um comportamento ético e contribuir para o desenvolvimento econômico, melhorando a qualidade de vida de seus colaboradores".

Colaboradores e suas famílias, juntos, extraindo a seriedade da ética e da transparência nas relações com todos os seus públicos, bem como conservando o meio ambiente, e respeitando à diversidade e a promoção da redução das desigualdades sociais (Costa; Carvalho, 2005, p.47).

Existem uma vasta gama de itens que podem motivar as empresas a agirem de forma socialmente responsável. Talvez isso se dê devido as pressões externas, à forma instrumental ou devido a princípios. Essas pressões externas estão relacionadas à legislação ambiental, movimentos de consumidores, ações sindicais visando aumentar os padrões de trabalho, ações de consumidores e demandas de comunidades afetadas por atividades industriais (Costa; Carvalho, 2005, p.49).

Essa argumentação diz respeito à sociedade pós-industrial, onde os valores são representados pela melhora da qualidade de vida da sociedade e não apenas pelo êxito econômico. Trazendo à baila um outro argumento externo, a globalização está pressionando a prática da responsabilidade social corporativa. Já os organismos internacionais como a Organização Mundial do Comércio (OMC) e a própria Organização das Nações Unidas (ONU), através do programa Pacto Global, estimulam empresas de todo globo terrestre a adotarem códigos de conduta e princípios basilares com o fito de preservar o meio ambiente equilibrado no trabalho e condições de respeito aos direitos humanos (Tenório, 2006, p.33).

Vale salientar que a responsabilidade social exsurge do comprometimento de uma empresa com a sociedade, onde a sua participação vai para além do pagamento de impostos, geração de empregos e renda, sendo levando muito em conta o interesse

empresarial pela sua atuação social, além do reconhecimento e importância da empresa responsável pelo negócio, juntando ainda mais valores sociais às suas atividades (Breitbarth; Harris, 2008, p.12).

Inúmeros fatores contribuíram para que isso acontecesse, onde sito a globalização, consumidores, legislação ambiental e por aí a fora vai. Porém, a Responsabilidade Social de uma empresa reside no fato de sua decisão em participar mais diretamente de todas as ações comunitárias onde está presente, mitigando os danos ao meio ambiente devido ao tipo de atividade que desenvolve (Tenório, 2006, p.54).

A Responsabilidade Social Corporativa constantemente envolve a procura de novas oportunidades como forma de atender às demandas ambientais, sociais e econômicas do mercado. Nesse conceito de Responsabilidade Social Corporativa foi incorporado pelas empresas, o público-alvo deixando de ser apenas o consumidor, passando a abarcar u maior número de pessoas e empresas, esse é chamado de "stakeholders". O termo "partes interessadas" foi cunhado para indicar todas as pessoas ou empresas que são, de certa maneira, afetadas pelas ações de uma organização (Breitbarth; Harris, 2008, p. 55).

Segundo Mattar (2001, p. 33), tanto a renda quanto a informação e o conhecimento estão totalmente firmados nas mãos de uma minoria. E ele afirma, ainda, que a concentração de informações acaba por produzir o aumento na concentração de renda, criando, destarte, um ciclo vicioso, ilegítimo e de difícil superação.

Aquelas empresas se transformaram em atores-chave na retificação e implementação de mudanças bem-sucedidas na sociedade e colaborando no alinhar das distorções que o Estado não conseguiu atingir e que jamais perceberia se outras pessoas, inserindo a própria sociedade civil, não se apegassem e buscassem um mundo econômico, social e ambientalmente sustentável (Mattar, 2001, p.33).

A visão do Instituto Ethos (2018), entidade empresarial criada em 1998, é no sentido de que as empresas são agentes influenciadores na promoção do desenvolvimento econômico e do avanço tecnológico que estão mudando de forma rápida o planeta em uma aldeia global. Dessarte, é de suma importância que haja uma consciência global que entronize todos num processo de desenvolvimento voltado para o cuidado e preservação do meio ambiente e do patrimônio cultural, o acesso aos direitos humanos e o estabelecimento de uma sociedade economicamente próspera e socialmente justa.

O cuidado do legislador em relação a questão da privacidade e proteção dos dados dos utilizadores, passa a ser a proteção da privacidade daqueles, levando em conta o

crescente e significativo atores envolvidos neste cenário, nomeadamente, as empresas de tecnologia. Diante desse preconceito, onde por inúmeras vezes representa um obstáculo à inovação e às novas tecnologias, a proteção de dados e a privacidade ocupam agora a condição de direito muito pessoal com regulagem europeia, que acabou por traçar o direito do Brasil e de outros Países (Bioni, 2019, p.93).

Desta forma, com arrimo nas notas fornecidas tanto pelo GDPR quanto pela LGPD sobre a regulamentação da responsabilidade pelo processamento, uso, coleta, armazenamento e transferência de dados, é criterioso observar uma sequência de comportamentos a serem admitidos pelas organizações a fim de que possam estar em *Compliance* com os padrões. Nessa margem, o Digital *Compliance* ganhará a máxima atenção, já que a obrigação proteger e salvaguardar os dados envolve, nos moldes padronizado atual do Brasil, não apenas os dados digitais, mas outrossim os dados em meio físico. Daí, o *Compliance* não pode se contentar a bancos de dados e meros arquivos digitais, sendo criterioso observar também que deve estar atento aos arquivos físicos, em papel ou não (Bonatti, 2020, p.116).

As responsabilidades devem restar claras e bastante definidas a fim de que cada área responsável pela gestão e direção de controle de riscos siba seus limites e atribuições na organização da estrutura da empresa, porque as pessoas estão acostumadas a agir da mesma forma e obter resultados diferentes. Neste diapasão, os processos de gestão necessitam estar mais alinhavados a fim de que se possam completar o labor uns dos outros (Bonatti, 2020, p.117).

Ao cabo de tais considerações, vale mencionar a promulgação, no ano de 2014, da Lei nº 12.965, chamada de Marco Civil da Internet, a qual foi responsável por estabelecer princípios, garantias, direitos e deveres para o uso da internet no Brasil, contudo, por outro lado, não avançou no quesito da proteção de dados, fazendo, destarte, uma abordagem superficial do tema. Nesse contexto, surge a Lei 13.709/2018, denominada Lei Geral de Proteção de Dados, LGPD, complementada e alterada, em parte, pela MP 869/2018.

A LGPD é a contrapartida brasileira ao Regulamento 2016/679 (RGPD), da Comunidade Europeia, a qual é aplicada a qualquer pessoa (natural ou jurídica, de direito público ou privado) que venha a usar de forma direta ou indireta, de dados pessoais, incluindo-se os meios digitais. Cumpre ressaltar, nesse ponto, de que até mesmo empresas que não tenham sede no país serão alvo da LGPD, desde que estas companhias firmem relações de alguma natureza (mercantil, jurídica, financeira, etc) com empresas outras

empresas estabelecidas no cenário nacional, e que haja o tratamento de dados por meio desta.

O instituto do *compliance* teve sua aparição com a legislação norte-americana, a qual criou a *Prudential Securities*, na década de 1950, e ainda com a regulação da *Securities and Exchange Commission* (SEC), de 1960, onde se começou a notar a necessidade de se formar um programa de *compliance* com o escopo de instrumentalizar certos procedimentos internos de controle, e também realizar o monitoramento de certas operações. Na década seguinte e mais precisamente no ano de 1977, foi criada a Convenção Relativa à Obrigação de Diligência dos Bancos, no Marco da Associação de Bancos Suíços, a qual criou o sistema interno entre as instituições financeiras, onde regulou as condutas e as vinculou às multas e outras penalidades caso houvesse descumprimento das regras.

A LGPD não se destina, *in limine*, às relações de trabalho. O escopo da norma é resguardar os direitos fundamentais da liberdade e privacidade, bem como do livre desenvolvimento da personalidade da pessoa natural. Desta forma, toda e qualquer relação jurídica que tenha como fim precípuo natural o manejo de dados e informações, entre pessoas naturais e/ou jurídicas, serão atingidas pela LGPD.

Esta Lei se aplica a qualquer operação de tratamento a ser realizada por pessoa natural ou por pessoa jurídica quer seja de direito público ou de direito privado, independentemente do meio, do País de sua sede ou do País onde estejam localizados os dados, desde que: I - a operação de tratamento seja realizada no território nacional; II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou (Redação dada pela Lei nº 13.853, de 2019):

> III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.
> § 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.
> § 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei agir de acordo com um Compliance seguro para buscar a adequação à Lei.

Na legislação pátria se observa, especialmente, a redação dos artigos 2º e 3º da CLT, restando claro que, naquelas relações de trabalho, o empregado passará a figurar como titular dos dados, haja vista que, em virtude do contrato de trabalho, é comum que se forneça informações pessoais ao empregador, como nome completo, número da

carteira de identidade, cadastro de pessoa física, endereço completo, dados bancários, dentre outros.

O empregador, por sua vez, aqui, estará a funcionar como controlador desses dados, já que competirá a ele decidir quais atitudes deverão ser tomadas a partir dessas informações. Nota-se que aqui deve-se diferenciar duas figuras previstas na legislação: o controlador e o operador de dados. O controlador encontra-se guarida no art. 5º, VI. Já a figura do operador, está tipificada no mesmo artigo, no inciso VII. Tanto o controlador quanto o operador, ambos possuem papeis de extrema relevância no que concerne ao trato dos dados colhidos e em seu poder, malgrado desempenharem funções diametralmente opostas, uma vez que a um cabe decidir e ao outro executar.

Nesse percurso, a LGPD determina que o controlador é a pessoa natural ou jurídica, de direito público ou privado, e a quem compete as decisões relacionadas ao tratamento de dados pessoais. Qualifica, assim, o operador sendo a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Relatado isso, fica esclarecido de que o papel do operador pode ser desenvolvido pelo próprio empregador ou por aquele a seu mando.

No entanto, pode ainda ser desempenhado por um dado setor da companhia, pré-existente ou criado exclusivamente para esta finalidade. Ao final, pode ser desempenhado, inclusive, por terceiros estranhos à relação, como empresas terceirizadas que prestam serviços atuando em substituição ao setor de recursos humanos.

É possível extrair que a execução de um programa de *compliance* direcionado às disposições da Lei Geral de Proteção de Dados exige, *a priori*, uma equipe multidisciplinar, fora os investimentos na área, a fim de viabilizar a privacidade dos dados armazenados fisicamente ou digitalmente. A desobediência frente a essas normas, pode trazer consequências às empresas que não implementarem, na prática, as normas trazidas com o advento da Lei. O artigo 52 da LGPD é claro ao enumerar as sanções aplicáveis aos agentes de tratamento de dados que não observarem suas disposições (Coelho, 2019, p.223).

Vale lembrar que por agente de tratamento de dados, entende-se todo e qualquer que manuseie dados (informações identificáveis de terceiros), com o escopo de auferir lucro. O dispositivo em comento enumera a possibilidade de aplicação de simples advertências, com indicação de prazo para correção dos vícios encontrados pela autoridade nacional, em processo administrativo, conforme se extrai do § 1º do mesmo artigo, a ser instaurado após a lavratura de auto de infração pelo ente responsável, a

Autoridade Nacional de Proteção de Dados (ANPD), criada tão somente para acompanhar o cumprimento das normas protetivas de dados e executar as sanções cabíveis.

O artigo 52 ainda prevê a possibilidade de aplicação de multa simples no percentual de até 2% (dois por cento) relacionado ao faturamento do último exercício da pessoa jurídica de direito privado ou conglomerado no Brasil, ficando fora o valor referente aos tributos, e limitando-se a quantia de até R$ 50.000.000,00 (cinquenta milhões de reais). O inciso III do artigo reza, outrossim, sobre a aplicação de multa diária por descumprimento da lei, limitada ao valor previsto no inciso anterior.

Por outro turno, há a possibilidade de ser ver a questão de forma contrária, analisando a partir do instrumento legal que tem como arrimo a relação jurídica, sendo que nesse sentido bem já decidiu outrora o STF no RE 586.453, ao apreciar sobre a competência da Justiça do Trabalho para julgar pedidos de complementação de aposentadoria. No Recurso Extraordinário em pauta, entendeu o STF que aquela relação jurídica se pautava nos regulamentos das entidades e não no contrato de trabalho. Destarte, nessa linha de interpretação, a relação titular-controlador dos dados, existente a partir da LGPD, embora ocorra no âmbito de um contrato de trabalho, não haveria falar em coincidência, em sua natureza, com a relação trabalhista típica, entre empregado x empregador, já que os direitos previstos na LGPD transcenderiam o contrato de trabalho.

No entanto, existem outros pontos omissos e controversos na legislação e que são passíveis de discussões. Ou seja, poderia o controlador-empregador lançar mão e utilizar desse conceito para efeito da dispensa de consentimento, nos termos do art. 7º, inciso IX, e art. 10 da LGPD.

Pode-se destacar o mapeamento de informações-dados que circulam nos diferentes setores da empresa, e que se referem às pessoas físicas, como empregados, autônomos e terceirizados, e também pessoas jurídicas prestadoras de serviços. Não se podendo esquecer é essencial realizar um mapeamento referente a natureza e do tipo dessas informações-dados, com o intuito que sejam analisados se esses dados têm natureza pessoal ou sensível, além de qual é o tratamento que deve ser dado a eles.

Alfim, questiona-se a necessidade de realização de estudos de simplificação das rotinas dos tratamentos de dados, além da análise referente as medidas mais eficazes para a verificação dos dados já obtidos, seu armazenamento e sua exclusão dos bancos de dados, tudo em regime de *compliance* com a legislação. Destarte, os programas de *compliance* devem se adequar à LGPD, revendo os procedimentos a serem adotados e,

acima de tudo, buscar democratizar as informações e o acesso aos dados por parte dos seus titulares.

Assim, mister que seja desenvolvida uma cultura de respeito e proteção dos dados, pessoais ou empresariais, no sentido a preservar o direito à privacidade dessas pessoas e garantir o livre desenvolvimento da personalidade da pessoa natural e acesso a livre concorrência na esfera corporativa, de acordo com o que preconiza o texto constitucional.

CONSIDERAÇÕES FINAIS

Por fim, este artigo procurou identificar os principais fatores relacionados à importância da existência do *compliance* digital nas organizações, já que, sua função precípua é a análise de riscos, bem como a adoção de medidas preventivas com o fim de adequar as organizações à legislação aplicável à tecnologia da informação, segurança da informação e proteção de dados, cumprindo, dessarte, seu propósito geral.

Observou-se, que antes da LGPD, o Brasil não dispunha de um regramento específico sobre o tema. Observa-se que a definição de dado pessoal na LGPD é mais ampla que o conceito adotado pelo Marco Civil da Internet, não encontrando barreiras em dados de subscrição ou nome, endereço, CPF, englobando, inclusive dados sensíveis, como orientação sexual e preferências políticas, bem como em dados biométricos.

A LGPD, no que tange à sua abrangência, tem aplicabilidade ampliada, ou seja, mais que o Marco Civil da internet. É que ela traz regramento sobre dados pessoais, online e/ou offline, por pessoa natural ou por pessoa jurídica de direito público ou de direito privado, com o fito de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, firmando, destarte, regras e limites para empresas a respeito da coleta, armazenamento, tratamento e compartilhamento de dados.

Obtemperou, *alfim*, que existe sim privacidade quanto ao tratamento de dados virtuais, tendo a LGPD garantido, quase de forma integral, a proteção do seu titular. Diga-se que tal proteção será efetiva com a criação da Autoridade Nacional, pelos motivos supracitados.

REFERÊNCIAS

ASSI, M. **Gestão de Compliance e Seus Desafios**. São Paulo: Saint Paul Editora, 2013

BIONI, B. R. **Proteção de dados pessoais:** a função e o limite do consentimento.Rio de Janeiro: Forense, 2019.

BONATTI, A. **Os Sistemas e as novas aplicabilidades da LGPD**. São Paulo. 2020.

BRASIL. Controladoria-Geral da União (CGU). **Portaria n. 909, de 7 de abril de 2015**. Dispõe sobre a avaliação de programas de integridade de pessoas jurídicas. Diário Oficial da União n. 66, Seção 1, p. 3, 2015.

BRASIL. **Lei nº 12.846, de 1 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. Brasília, 2013.

BRASIL. **Lei nº 12.965, de 23 de abril de 2013.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, 2014.

BRASIL. **Lei nº 13.853, de 8 de julho de 2019.** Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, 2019.

BREITBARTH, T.; HARRIS, P. The role of corporate social responsibility in the football business: toward the development of a conceptual model. **European Sport Marketing Quarterly**, v. 8, p. 179-206, 2008.

COELHO, A. C. B. **A Lei Geral de Proteção de Dados Pessoais Brasileira como meio de efetivação dos direitos da personalidade**. João Pessoa: [s.n.], 2019.

COIMBRA, M. D.A; MANZI, V. A. **Manual de *Compliance***. São Paulo: Atlas, 2010.

COSTA, A. M.; CARVALHO, J. L. F. Legitimando Papéis ou Conciliando Interesses? A Reprodução Discursiva da Responsabilidade Social Empresarial. **Anais Eletrônicos do XXIX Encontro Anual da ANPAD**, 2005.

INSTITUTO ETHOS. Indicadores Ethos para Negócios Sustentáveis e Responsáveis. 2018. Disponível em: <http://www.ethos.org.br>. Acesso em: 01 fev. 2024.

FEDERAÇÃO BRASILEIRA DE BANCOS - FEBRABAN. Função de Compliance. 2003. Disponível em: http://www.febraban.org.br/. Acesso em: 01 fev. 2024.

MANZI, V. A. **Compliance no Brasil**: consolidação e perspectivas. São Paulo: Ed. Saint Paul, 2008.

MATTAR, F. N. **Pesquisa de marketing.** 3.ed. São Paulo: Atlas, 2001.

NASH, L. L. **Ética nas empresas:** boas intenções à parte. São Paulo: Makron Books, 1993.

TENÓRIO, F. G. (Org.) **Responsabilidade Social Empresarial**: Teoria e Prática. 2. ed. Rio de Janeiro: Editora FGV, 2006. 259 p.

TROKLUS, D.; VACCA, S. **International Compliance**. How to build and maintain an effective Compliance and ethics program. Minneapolis: SCCE, 2013.