APLICAÇÃO DO PROGRAMA DE COMPLIANCE NAS EMPRESAS BRASILEIRAS À LUZ DO MARCO CIVIL DA INTERNET E DA LEI GERAL DE PROTEÇÃO DE DADOS[1]

THE APPLICATION OF COMPLIANCE PROGRAMS IN THE BRAZILIANS COMPANIES IN THE LIGHT OF THE BRAZILIAN CIVIL FRAMEWORK OF THE INTERNET AND DATA PROTECTION LAW

Isabeli Cintra COUTO[2]

RESUMO

O objetivo do presente trabalho foi analisar a implementação do programa de compliance digital no âmbito da Lei Geral de Proteção de Dados e do Marco Civil da Internet. Destarte, foi necessário abordar a historicidade do programa com o surgimento de leis anticorrupção e posterior regulamentação do programa de compliance no Brasil e no exterior. Por fim, para estudar a aplicação dos programas de compliance digital foi pesquisado sobre Marco Civil da Internet, Lei Geral de Proteção de Dados e como o programa de integridade digital deve ser implementado, no tocante à proteção de dados, evitando possíveis vazamentos de dados.

Palavras-chave: Programa de compliance. Programa de Integridade. Boa governança corporativa. Tratamento de dados. Compliance digital.

ABSTRACT

[1] O presente artigo sintetiza a monografia de conclusão da pesquisa, realizada para o Programa Interno de Bolsas de Iniciação Científica (PIBIC 2021-2022) da Faculdade de Direito de Franca (FDF), Franca/SP.

[2]Graduanda em direito pela Faculdade de Direito de Franca, aluna pesquisadora PIBIC 2020-2021/2021-2022, trabalhou como diretora da Pasta Representatividade no ano de 2021 e membro no ano 2022 pelo Diretório Acadêmico "28 de Março". Fundadora e trabalhou como coordenadora de materiais do Cursinho Popular "Dra. Jurema Gomes Xavier". Foi estagiária na Delegacia de Defesa da Mulher e atualmente é estagiária no Núcleo de Assistência Judiciária da Faculdade de Direito de Franca. Celular: (16) 99358-5200, e-mail: isabeliccouto@gmail.com.

The aim of this paper was to analyzed the implementation of digital compliance under the scope of the Brazilian General Data Protection Law and the Brazilian Civil Framework of the Internet. Therefore, it was necessary to approach the historicity of the compliance program with the promulgation of anti-corruption laws and subsequent regulation of the compliance program in Brazil and abroad. At last, to study the application of digital compliance programs, it was researched about the Brazilian Civil Framework of the Internet, the Brazilian General Data Protection law and how the Digital Integrity Program should be implemented concerning data protection avoiding possible data leakage.
Keywords: Compliance program. Integrity program. Good corporate governance. Processing of data. Digital Compliance.

1 INTRODUÇÃO

A escolha da presente pesquisa justifica-se pela necessidade de adequar as empresas com o *compliance* digital, desse modo, a incorporação deve estar em conformidade com a Lei nº 12.965/2014 (Marco Civil da Internet) e a Lei nº 13.709/2018 (Lei Geral de Proteção de dados).

O tema em discussão é bastante debatido na conjuntura atual, visto que os dados são armazenados e processados pelas empresas e muitas vezes de modo indevido. Ademais, o enfoque da pesquisa é a adequação das empresas para que estas não sofram sanções pela não aplicação das leis ou por aplicá-las de maneira incorreta.

Com isso, iniciando o estudo do *compliance*, pode-se constatar que ele foi criado nos Estados Unidos, com a promulgação da *Foreing Corrupt Practices Act* e após isso o governo americano editou normativas para implementar o programa de *compliance* nas empresas americanas. Destarte, seguindo exemplo desse país, o Brasil e a União Europeia passaram a redigir regulamentos de anticorrupção e a implementar os programas de integridade nos seus ordenamentos jurídicos.

Outrossim, o Brasil implementou a Lei Anticorrupção, Lei nº 12.846/13, a qual responsabiliza as empresas por práticas de corrupção. Além disso, essa lei prevê atenuação de sanções para as instituições que aplicam o programa de *compliance* de maneira efetiva. Desse modo, devem aplicar os pilares necessários de acordo com as suas necessidades.

O *compliance* digital é aquele que visa a aplicação de forma eficaz da Lei Geral de Proteção de Dados e do Marco Civil da Internet nas empresas para que elas saibam como os dados devem ser tratados, dado que, a infringência da Lei Geral de Proteção de Dados gera sanções a essas corporações por meio da Autoridade Nacional de Proteção de Dados (ANPD).

Destarte, a implementação do programa de integridade previsto na LGPD traz impactos na empresa, as quais podem ter as suas sanções atenuadas em caso da execução do programa.

Por fim, neste trabalho foram utilizados meios de pesquisas doutrinários, jurisprudenciais, documental, entre outros. Quanto à metodologia recorreu a uma pesquisa dedutiva e descritiva, optando-se por abordagem qualitativa com técnica de revisão bibliográfica e documental, consultas em artigos científicos, monografias e doutrinas.

2 CONCEITO E HISTORICIDADE DO *COMPLIANCE* NO MUNDO E NO BRASIL

2.1 CONCEITO DE *COMPLIANCE*

O termo *compliance* advém do termo em inglês *to comply*¸ o qual tem como significado no âmbito jurídico estar em conformidade com as leis e regulamentos. Nesse sentido, Soltes evidencia em sua obra *Evaluating the effectiveness of corporate compliance programs: Establishing a model for prosecutors, courts, and firms*

> Compliance programs are internal firm structures and processes designed to support firms' efforts to achieve this concurrence. Compliance programs are expected to achieve three objectives. First, and most fundamentally, compliance programs seek to prevent misconduct from occurring. Recognizing that firms cannot design programs to prevent all misconduct from occurring (e.g., the conduct of a rogue employee), the second element of programs is a mechanism to detect deviant behavior if it does arise. Finally, programs need policies that align corporate behavior with applicable laws and regulations. Policies should not only describe the conduct that ought to be detected and prevented, but also outline

> the procedures for appropriate action if misconduct arises.[3-4]

Como foi exposto, os programas de governança corporativa têm três estruturas, a prevenção da infração econômica da empresa, não é possível prever todas as infrações; a detecção de diversos riscos que possam surgir e, por fim, possuir uma política regulatória.

2.2 HISTÓRIA DO *COMPLIANCE*

O *compliance* surgiu em um cenário de altos índices de corrupção e fraudes nas empresas em diversos países. Por conta desse cenário, os países elaboraram leis contra corrupção e, posteriormente, efetivaram programas de *compliance*.

Em 1972, os Estados Unidos tiveram escancarado o escândalo político, *Watergate* e, posteriormente, a renúncia do Presidente Nixon. Após investigações sobre o caso descobriram que essa fraude estava ligada ao Comitê do Presidente Richard Nixon. Por conta desse caso, passaram a investigar casos de corrupção nas empresas norte-americanas e depararam com financiamentos de campanhas políticas tanto dentro do país como no exterior.

Nesse cenário, o Congresso americano sancionou a *Foreign Corrupt Practices Act* em 1977, a qual visa combater a corrupção nas empresas. Dessarte, o governo americano fez guias explicativos, como o *Resource guide to the U.S. Foreign Corrupt Pratices Act*. Em síntese, essa é uma lei pioneira no combate a corrupção e é uma das mais importantes do mundo. Após a implementação da lei, os Estados Unidos foi o primeiro país a regulamentar o programa de integridade para as empresas e o próprio governo seguirem.

[3] SOLTES, Eugene. Evaluating the effectiveness of corporate compliance programs: establishing a model for prosecutors, courts, and firms. NYU Jornal of Law & Business, 2018. p. 978.

[4]Os programas de compliance são uma estrutura interna da empresa e um processo destinado a suportar os esforços da empresa para manter a concorrência. Os programas de compliance são previstos de ter três objetivos. O primeiro, e o mais fundamental, programa de compliance busca prevenir más condutas de acontecer. Distinguindo das empresas que não podem desenvolver programas para prevenir todas más condutas de acontecer (ex.: a conduta de um empregado desonesto), o segundo elemento do programa é o mecanismo de detectar comportamentos desviantes se vier a ocorrer. Por fim, programas precisam de medidas para alinhar os comportamentos corporativos com a aplicabilidade de leis e regulamentos. Medidas não deveriam apenas descrever as condutas que deveriam ser detectadas e prevenidas, mas também o resumo dos procedimentos apropriados de intervenção caso a má conduta aconteça.

Outrossim, com o objetivo de combater fraudes, o Bloco da União Europeia formou o Organismo Europeu de Luta Antifraude o qual investiga casos de corrupção que abrange fundos europeus. Em vista disso, editaram o Relatório Anticorrupção da União Europeia, o qual apresenta alguns pilares do programa de *compliance* como a necessidade de se ter uma gestão de risco, pilar da transparência e a proteção ao denunciante.

Em 2018 o bloco econômico da União Europeia implementou o *General Data Protection Regulation* (GDPR), o qual exige que as corporações europeias ou as estrangeiras que processem algum dado de cidadãos europeus estejam em conformidade com as legislações europeias, principalmente com o regulamento do GDPR. Por conta dessas exigências é de suma importância que as companhias tenham o programa implementado de maneira efetiva.

Desse modo, o Brasil instituiu no seu ordenamento jurídico a Lei n° 12.846/2013 que traz disposições de responsabilizar civil e administrativamente pessoas jurídicas pela prática de atos lesivos contra a Administração Pública nacional ou estrangeira. Ademais, a responsabilidade objetiva é conceituada com a que não precisa da aferição de culpa para configurar o ato ilícito, precisando apenas da comprovação do dano ou do nexo causal.

O programa de *compliance* é uma novidade na Lei Anticorrupção. Desse modo, o artigo 7º da Lei expressa diversas ações que podem ser levadas em consideração para a aplicação de uma sanção à empresa infratora. No inciso VIII[5] do artigo citado evidencia o programa de integridade como uma forma atenuação de sanção.

Diante desses fatos, a Lei n°12.846/2013 atenua as sanções para as corporações que possuírem um programa de integridade implementado de maneira efetiva, sendo um atrativo para que as instituições apliquem o programa. É importante ressaltar que a aplicação do programa de maneira efetiva não exime a responsabilização da empresa.

Desse modo, o Poder Executivo Federal editou o Decreto nº 8.420/15, o qual regulamentou as responsabilizações da pessoa jurídica pelos atos praticados contra a Administração Pública na lei anticorrupção, entre esses atos está o programa de *compliance*.

Assim sendo, o Decreto nº 8.420/15 é constituído por seis capítulos, no seu quarto capítulo regulamenta a forma que o programa de

[5] Art. 7º Serão levados em consideração na aplicação das sanções: VIII – a existência de mecanismos e procedimentos internos de integridade, auditoria e incentivo à denúncia de irregularidades e a aplicação efetiva de códigos de ética e de conduta no âmbito da pessoa jurídica;

integridade deve ser aplicado nas empresas, explana também como será feita a avaliação do programa para poder aplicar uma atenuação de sanção e como o programa deve ser aplicado em microempresas ou empresas de pequeno porte.

Por fim, os programas de *compliance* originaram em razão do aumento de casos de corrupção e fraudes nos países, por isso eles passaram sancionar as leis anticorrupção e regulamentaram os programas de integridade.

3 PROGRAMAS DE *COMPLIANCE* NO BRASIL

3.1 *COMPLIANCE* EMPRESARIAL

As grandes companhias possuem os programas de *compliance* aplicados e normalmente possuem exigências que para negociar com outra empresa é necessário que essa última possua também o programa de integridade implementado, pois a incorporação sabe que essa empresa é ética, transparente e íntegra.

O programa de *compliance* pode ser aplicado também em pequenas e médias empresas, de acordo a Portaria nº 2.279 da Controladoria Geral da União que regulamenta o *compliance* em microempresas e empresas de pequeno porte.

Dessarte, para o programa de integridade ser considerado efetivo é necessário adequá-lo de acordo com a necessidade de cada instituição. Para isso ocorrer é importante que a empresa implemente os pilares do *compliance* que serão tratados nesse artigo.

O programa de integridade é muito importante para todos, não só para a empresa, mas também para o meio social e para a administração pública. Pois os níveis de infrações diminuirão, o meio social estará em um ambiente mais ético, para o meio corporativo terão uma concorrência legal. Contudo, vale lembrar que para o programa de integridade ter uma eficácia é importante que modifique os valores antigos de práticas ilegais.

Corroborando com esse pensamento, o julgado do Tribunal de Justiça do Estado de São Paulo, pelo Relator Alexandre Lazzarini, “[...] demonstrar que de nada adiante criar “padrões de governança”, sem que se

modifique os valores das próprias pessoas envolvidas."[6] Por fim, conforme entendimento jurisprudencial é necessário que seja feito treinamentos corporativos para que os colaboradores entendam a importância de aplicar e executar o programa de forma efetiva.

3.2 PILARES DO PROGRAMA DE INTEGRIDADE

O programa de integridade possui alguns pilares, os quais formam a base do programa. Há uma divergência doutrinária sobre quais e quantos são os pilares do *compliance*.

Os escritores Daniel Sibille e Alexandre Serpa demonstram em sua obra "Os pilares do programa de *compliance"* que o programa de integridade possui nove pilares. São eles: *suporte da alta administração,* o qual é a base para o programa ser eficaz; *avaliação de risco*; *código de conduta e políticas de compliance,* os quais mostrará a conduta que a instituição espera de seus funcionários, devendo todos da empresa submeter as suas normas; *controles internos, treinamentos e comunicação*, é necessário implementar esse pilar para o desenvolvimento do programa na empresa; *canais de denúncias*, é o meio para demonstrar a empresa que há uma potencial violação à legislação; *investigações internas*, é realizado após a identificação de um fato suspeito na denúncia, com o implemento da LGPD, será necessária uma autorização da Autoridade Nacional de Proteção de Dados para realizar a investigação; *due diligence,* é necessário avaliar as condutas das empresas que serão contratadas; e *monitoramento e auditoria*, finalidade averiguar se o programa está sendo executado da maneira que deve ser.[7]

Nessa mesma linha, o doutrinador Eduardo Saad-Diniz apresenta quais são os pilares na doutrina "Ética Negocial e *Compliance*: Entre a educação executiva e a interpretação judicial". Para Eduardo Saad-Diniz o programa de integridade possui seis pilares, alguns já foi explicado acima, *códigos de conduta corporativos e manual de compliance, liderança e tone at the top¸ o departamento de compliance e compliance officer,* ele que vai coordenar as diretrizes do programa de integridade, se está sendo aplicado de maneira correta, *canais de comunicação e whistleblowing, treinamento,*

[6] SÃO PAULO. Tribunal de Justiça de São Paulo. Apelação Cível. 1086219-29.2019.8.26.0100. 1ª Câmara Reservada de Direito Empresarial. Relator Cesar Ciampolini. Julgamento 28 de jul. de 2021. Publicação 15 de set. 2021.

[7] SIBILLE, Daniel, SERPA, Alexandre. Os pilares do programa de compliance. LEC, 2017.

*monitoramento e revisão e gestão de cris*e, como toda empresa é suscetível a correr riscos, por isso é necessário ela tenha a capacidade de aprender com os riscos, assim que detectada os riscos da empresa é feita a *due diligence*.[8]

Esses pilares também estão expressos no Decreto nº 8.420/15, em seus incisos do artigo 42, tal como no inciso I encontra-se a liderança e *tone at the top*, nos incisos II e III o pilar do código de conduta, inciso IV o treinamento corporativo, inciso V o pilar de gestão de risco, inciso VII controles internos, inciso IX o departamento de *compliance* e o *compliance officer*, inciso X o pilar do canal de denúncia, inciso XIII o pilar do *due diligence*, por último, no inciso XV temos o pilar do monitoramento.

É importante ressaltar que cada empresa deve aplicar os pilares de acordo com a necessidade que ela tiver, portanto deve-se fazer uma análise para ver quais pilares é relevante aplicar naquela empresa.

4 APLICAÇÃO DOS PROGRAMAS DE *COMPLIANCE* DIGITAL À LUZ DO MARCO CIVIL DA INTERNET E DA LGPD

Com o surgimento das novas tecnologias, foram aparecendo também os problemas, desse modo, fez-se necessário regulamentar essas inovações, surgindo o Direito Digital. Com essas novas legislações sendo normatizadas foi primordial adequar as empresas para que elas não corram riscos de infringir essas leis.

Outrossim, a Emenda Constitucional nº 115/2022, a qual alterou a Magna Carta para incluir a proteção de dados pessoais como direitos e garantias constitucionais no artigo 5º, inciso LXXIX[9]. Além disso, essa Emenda Constitucional fixou a competência privativa da União para legislar sobre a proteção e tratamentos dos dados pessoais, desse modo, acrescentando o inciso XXVI no artigo 21[10] e o inciso XXX no artigo 22[11] da Constituição Federal.

[8] SAAD-DINIZ, Eduardo. Ética Negocial e Compliance: Entre a educação executiva e a interpretação judicial. São Paulo. Thomson Reuters Brasil – Revista dos Tribunais, 2019. p. 164 – 191.

[9] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

[10] Art. 21. Compete à União: XXVI - organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei.

[11] Art. 22. Compete privativamente à União legislar sobre: XXX - proteção e tratamento de dados pessoais.

4.1 DESDOBRAMENTOS DO MARCO CIVIL DA INTERNET (LEI Nº 12.965/14) E DA LEI GERAL DE PROTEÇÃO DE DADOS (LEI Nº 13.709/18)

O Marco Civil da Internet, Lei nº 12.065, foi promulgado em 2014, regulamentando os princípios, garantias, direitos e deveres para o uso da internet no Brasil. Ademais, entre os princípios que a lei dispõe a respeito da disciplina do uso da internet está a proteção dos dados pessoais, em seu art. 3º-A, III "Art. 3º A - disciplina do uso da internet no Brasil tem os seguintes princípios: III - proteção dos dados pessoais, na forma da lei.". A lei nº 12.065/17 garante que o acesso à internet é essencial para o exercício da cidadania, de acordo com o seu artigo 7º.

O Marco Civil da Internet dispõe sobre a proteção aos registros, aos dados pessoais e as comunicações privadas, os quais devem estar de acordo com à preservação da intimidade, da vida privada, da honra e da imagem das partes. Caso um dos terminais que coleta, armazena, guarda e trata os registros, dados pessoais ou comunicações por provedores de conexão e de aplicações da internet estiver em território nacional deverá ser aplicada a legislação brasileira.

Caso ocorra infrações a essas normas poderão ser aplicadas sanções, conforme art. 12 da Lei 12.965/14. Essas sanções podem ser executadas cumulativa ou isoladamente e poderão ser efetuadas também às sanções cíveis, criminais ou administrativas, são elas a advertência, multa, suspensão temporária das atividades e proibição de exercício das atividades.

Em suma, a lei 12.965/14 introduziu a regulamentação do direito digital no Brasil, sendo primordial, e posteriormente a Lei Geral de Proteção de Dados, Lei nº 13.709/18, a qual fez algumas alterações no Marco Civil da Internet (Lei nº 12.965/14).

Por conseguinte, a Lei Geral de Proteção de Dados (LGPD), Lei 13.709/18, foi inspirada no GDPR (*General Data Protection Regulation*). Posteriormente, foi modificada pela Lei nº 13.853/19, a qual fez algumas alterações e criou a Autoridade Nacional de Proteção de Dados, e pela Lei 14.010/2020, alterando a data de vigência no tocante às sanções administrativas.

Desse modo, para entender a regulamentação da lei é necessário saber alguns conceitos que são apresentados pela própria lei no seu artigo 5º.

Dessarte, dado pessoal é aquele que traz uma informação que possam gerar uma identificação da pessoa natural com base na associação dos dados. Ademais, dado pessoal sensível "estão relacionados com aspectos da personalidade do indivíduo, como, por exemplo, orientação sexual, opinião política, convicção religiosa, origem racial, estado de saúde, dado genético, filiação sindical, entre outros". [12] Nesse mesmo sentido, o dado anonimizado, é aquele é incapaz de identificar o titular do dado.

Além disso, é necessário saber como foi feito o tratamento do dado que está armazenado em um banco de dados, o qual é o local onde o conjunto de dados ficam armazenados.

Dessa forma, o titular dos dados é a pessoa natural que se referem as informações que estão sendo tratadas. Esse titular deve dar um consentimento de forma livre e com a finalidade específica para o tratamento do dado, não podendo ser concedido com finalidades genéricas.

Quanto aos agentes de tratamento dos dados são o controlador, aquele que possui o poder decisório, e o operador, apenas executa as ordens oferecidas pelo controlador e possui contato direto com o titular do dado, ambos podem ser pessoa natural ou jurídica de direito público ou privado. Há também o encarregado, é a pessoa indicada pelo controlador para ser o canal de comunicação entre o controlador, o titular do dado e Autoridade Nacional de Proteção de Dados. As atribuições do encarregado estão elencadas no §2º do artigo 41 da Lei nº 13.709/18[13].

A Autoridade Nacional de Proteção de Dados (ANPD) é um órgão "responsável por cuidar, orientar, implementar e fiscalizar o cumprimento da LGPD"[14]. Em vista disso, foi promulgada um Medida Provisório nº 1.124/2022 que transformou a ANPD em autarquia de natureza especial (artigo 55-A da Lei 13.709/18[15]). Essas autarquias não

[12] KOEPSEL, Alice de Medeiros. ADOÇÃO E EFEITOS DOS PROGRAMAS DE COMPLIANCE À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS. 2020. Trabalho de Conclusão de Curso (Bacharelado em Direito) p. 30.

[13] § 2º As atividades do encarregado consistem em: I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; II - receber comunicações da autoridade nacional e adotar providências;

III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

[14] KOEPSEL, Alice de Medeiros. ADOÇÃO E EFEITOS DOS PROGRAMAS DE COMPLIANCE À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS. 2020. Trabalho de Conclusão de Curso (Bacharelado em Direito) p. 33.

[15] Art. 55-A. Fica criada a Autoridade Nacional de Proteção de Dados - ANPD, autarquia de natureza especial, dotada de autonomia técnica e decisória, com patrimônio próprio e com sede e foro no Distrito Federal.

são subordinadas hierarquicamente a ministérios e à Presidência, elas possuem autonomia técnica e decisória.

Por fim, o artigo 5º da Lei 13.709/18 dispõe sobre o relatório de impactos à proteção de dados pessoais no inciso XVII, que é a documentação elaborada pelo controlador com descrição dos procedimentos do tratamento dos dados e riscos envolvidos, além das medidas que foram realizadas para a mitigação desses riscos. Por conseguinte, essa lei abrange todas as empresas que fazem o tratamento de dados e não apenas aquelas que trabalham com tecnologias.

4.2 PROGRAMA DE *COMPLIANCE* DIGITAL

O *compliance* digital visa a aplicação, de forma correta, das legislações, principalmente da Lei Geral de Proteção de Dados e o Marco Civil da Internet, normas e regulamentos que visem a proteção dos dados, para que, desse modo, as empresas que implementam esses programas tenham as sanções atenuadas em caso de descumprimento das normas.

A Lei nº 13.709/18 abrange no artigo 50 que as empresas apliquem o programa de integridade. Será implementado o programa e delimitá-lo para a proteção de dados, formulando as regras do programa de integridade, regime de funcionamento, procedimentos, normas de segurança e como será feito o tratamento dos dados, ações educativas de como devem ser tratados, para que se evite vazamento dos mesmos e demonstre a mitigação de riscos.

Outrossim, para implementar o programa de integridade, deve-se levar em consideração a natureza, escopo, finalidade, gravidade dos riscos e os benefícios decorrentes de tratamento dos dados. Desse modo, de acordo com o §2º do artigo supracitado, o controlador pode formular programa de governança corporativa em privacidade, devendo respeitar a estrutura, escala e volume das operações de dados, bem como se o dado é sensível, a possibilidade deles vazarem e a gravidade desse dano aos titulares dos dados.

O *compliance* digital é uma espécie de programa de integridade, desse modo, deve também possuir o pilar de revisão e atualização do programa. De acordo com o §3º do artigo citado é importante que seus regulamentos e normas sejam públicas e atualizadas periodicamente, visto que um programa que não está atualizado não é passível de atenuar as

responsabilidades da corporação em caso de alguma infração à Lei Geral de Proteção de Dados.

Há uma necessidade de ter implementado nas instituições um código de conduta e ética demonstrando as condutas que devem ser feitas no tratamento dos dados, uma relação de como verificar se os dados podem ser tratados por aquela empresa, se há o consentimento do titular do dado, a finalidade para o tratamento e o período que o dado será armazenado pela instituição.

Além desse Código, outro pilar que é importante aplicar no *compliance* digital, é o treinamento corporativo. Além desse, é fundamental o comprometimento da Alta gestão na implementação corretamente das normas.

Por fim, a empresa, representada pela Alta Gestão, deve implementar os pilares do programa de *compliance* de acordo com as necessidades da empresa, para que, dessa forma, ele seja efetivo.

4.2.1 MEDIDAS DE SEGURANÇA

O artigo 46 da lei 13.709/18 dispõe a respeito das medidas de segurança, as quais se relacionam com o princípio da segurança para proteger o dado de ameaças, diminuindo os riscos de vazamentos dos mesmos.

Os doutrinadores Rita Blum e Hélio Moraes argumentam que a empresa deve sempre manter a segurança dos dados, desse modo deve verificar como foi realizado o tratamento do dado pessoal, para isso é pega-se o resultado e os riscos que se esperam para que se elaborem técnicas aptas para proteger os dados de possíveis tratamentos inadequados ou ilícitos.[16]

Destarte, a Autoridade Nacional de Proteção de Dados que vai dispor sobre os padrões técnicos mínimos para que essas medidas sejam aplicadas.

4.2.2 SANÇÕES A EMPRESAS INFRATORAS

[16] BLUM, Rita Peixoto Ferreira; MORAES, Hélio Ferreira. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS – LGPD. In: op. cit. p. 557.

Em caso de não cumprimento das normas aplicadas pela lei estará sujeitas às penalidades previstas na lei. O artigo 42 da lei dispõe a respeito da responsabilidade civil do colaborador e operador, os quais podem responder solidariamente. Assim, o encarregado não responde civilmente, mas poderá responder por suas próprias ações se comprovar dolo e má-fé.

Os agentes de tratamento são o controlador e o operador, o encarregado não é responsável pela sanção. Há diversas penalidades administrativas como advertências com indicação de prazos para a correção, multa de até 2% do faturamento do último exercício, excluindo os tributos, e limitando a R$50.000.000,00 por infração, publicização da infração, suspensão parcial do funcionamento do banco de dados, suspensão do exercício da atividade de tratamento dos dados por seis meses e prorrogáveis por igual período e proibição natural ou total das atividades relacionadas a tratamento de dados.

A Autoridade Nacional de Proteção de Dados é competente para aplicar as sanções administrativas por meio de processos administrativos, garantindo o contraditório, ampla defesa e o direito de recurso. Após definir a penalidade, analisa se a empresa possui medidas para fiscalizar e evitar os atos ilícitos e vazamentos de dados, como os programas de integridade.

O artigo 43 explicita a forma de isenção de responsabilidade pelo descumprimento da LGPD. Em vista disso, o controlador e o operador não serão responsabilizados civilmente se comprovarem que não fizeram o tratamento do dado quando não há descumprimento à legislação de proteção de dados e quando o titular der causa do dano, por culpa sua ou de terceiros, não havendo culpa dos agentes de tratamento dos dados.

4.2.3 IMPACTOS DA IMPLEMENTAÇÃO DO PROGRAMA DE *COMPLIANCE* DIGITAL

A implementação do programa efetivo traz algumas vantagens para a empresa que aplica o programa. Como foi demonstrado neste capítulo as empresas que descumprem a lei ficam sujeitas às penalidades que são aplicáveis pela autoridade nacional, podendo ser uma sanção administrativa. Essas sanções impostas a empresas infratoras devem

garantir o contraditório e a ampla defesa, além disso, deve-se analisar parâmetros, que dependerá do caso concreto.

Desse modo, Rita Blum e Hélio Moraes demonstram os parâmetros, os quais são "a boa-fé do infrator, adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados"[17], além desses parâmetros tem também a adoção de programas de integridade.

Corroborando com o exposto acima, a escritora Alice Koepsel evidencia,

> Dessa forma, o *compliance* de dados pessoais tente a auxiliar os agentes de tratamento a aplicar normas de proteção de dados eficazes e, por causa disso, conduzirá a entidade a manter toda sua atividade de acordo com a legislação, utilizando a segurança da informação para diminuir incidentes que resultem na responsabilidade empresarial.[18]

Portanto, possuir programas de integridade implementados em suas empresas, de forma efetiva, pode ter a redução das penalidades impostas pela ANPD.

5 CONSIDERAÇÕES FINAIS

Os programas de *compliance* foram desenvolvidos no contexto de corrupções ao redor do mundo e após foram elaborados programas de integridade. Países como Estados Unidos, Brasil e União Europeia implementaram esse programa. No Brasil, a lei anticorrupção e a partir dessa lei foi promulgada decretos que implementam o programa de integridade, como o Decreto nº 8.420/15 e a Portaria nº 2.279/15 da Controladoria Geral da União.

A pesquisa demonstra a imprescindibilidade de aplicar esse programa nas empresas, visto que se aplicado de maneira correta pode

[17]BLUM, Rita Peixoto Ferreira; MORAES, Hélio Ferreira. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS – LGPD. In: op. cit. p. 559.
[18]KOEPSEL, Alice de Medeiros. ADOÇÃO E EFEITOS DOS PROGRAMAS DE COMPLIANCE À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS. 2020. Trabalho de Conclusão de Curso (Bacharelado em Direito), p. 67

aumentar a produtividade da instituição, trazer uma conscientização dos colaboradores para que estes ajam de maneira íntegras e éticas.

O presente trabalho concluiu que é importante a aplicação do programa de maneira efetiva. Para que esse programa de integridade seja efetivo é essencial que aplique os pilares compatíveis com a demanda da empresa e sempre atualizá-los. Desse modo, essas empresas que mantem o programa em suas instituições possuem atenuação nas sanções se caso tiver alguma infração às normas dentro de suas empresas.

O objetivo principal da pesquisa é tratar do *compliance* digital que é a aplicação do programa de *compliance* especializado para o tratamento dos dados. O programa dessa modalidade de *compliance* é regido sob a Lei nº 12.965/14 e Lei nº 13.709/18. Destarte, são utilizados todos os elementos do programa de integridade, inclusive os pilares.

Por fim, como esse programa é específico para tratamento de dados, é necessário que esses pilares tenham um foco de como realizar o tratamento dos dados como dispõe a Lei Geral de Proteção de Dados para que não haja nenhum vazamento dos dados que estão sendo tratados pela empresa.

6 REFERÊNCIAS

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República. Disponível em: http://www.
http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm.

BRASIL. Controladoria Geral da União. **Portaria Conjunta nº 2.279, de 9 de setembro de 2015.** Dispõe sobre a avaliação de programas de integridade de microempresa e de empresa de pequeno porte. Brasília, DF. Disponível em: https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/30172275/do1-2015-09-10-portaria-conjunta-n-2-279-de-9-de-setembro-de-2015-30172271.

BRASIL. **Decreto nº 8.420, de 18 de março de 2015.** Regulamenta a Lei nº 12.846, de 1º de agosto de 2013, que dispõe sobre a responsabilização administrativa de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira e dá outras providências. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/decreto/d8420.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. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12846.htm.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

CARVALHO, André Castro *et. al*. (org)**. Manual de *Compliance*.** vol. 3. Rio de Janeiro, Forense, 2021.

CUNHA, Matheus; EL KALAY, Márcio (org.), PUNDER, Patrícia. **Manual de *compliance*:** *compliance mastermind* vol. 1. LEC Editora. São Paulo. 2019. Ebook.

DO NASCIMENTO. Suellen Lima. **A lei geral de proteção de dados pessoais e a adoção dos programas de *compliance* na sociedade da informação.** Brasília, 2020. Disponível em: https://repositorio.uniceub.br/jspui/handle/prefix/14877

KOEPSEL, Alice de Medeiros. **Adoção e efeitos dos programas de *compliance* à luz da lei geral de proteção de dados pessoais**. 2020. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade do Sul de Santa Catarina, Tubarão, 2020. Disponível em: https://repositorio.animaeducacao.com.br/handle/ANIMA/5452

SAAD-DINIZ, Eduardo. **Ética Negocial e *Compliance*:** Entre a educação executiva e a interpretação judicial. São Paulo. Thomson Reuters Brasil – Revista dos Tribunais, 2019.

SÃO PAULO. Tribunal de Justiça de São Paulo. Apelação Cível. 1086219-29.2019.8.26.0100. 1ª Câmara Reservada de Direito Empresarial. Relator Cesar Ciampolini. Julgamento 28 de jul. de 2021. Publicação 15 de set. 2021. Disponível em: https://tj-sp.jusbrasil.com.br/jurisprudencia/1282204829/apelacao-civel-ac-10862192920198260100-sp-1086219-2920198260100/inteiro-teor-1282204833

SECURITIES AND EXCHANGE COMMISSION; U.S. DEPARTAMENT OF JUSTICE; **FCPA**: A Resource Guide to the U.S. Foreign Corrupt Practices Act, Second Edition. EUA. 2020. Disponível em: https://www.justice.gov/criminal-fraud/fcpa-resource-guide.

SIBILLE, Daniel, SERPA, Alexandre. **Os pilares do programa de *compliance.*** LEC, 2017. Disponível em: https://lec.com.br/beta2021final/os-10-pilares-de-um-programa-de-compliance/.

SOLTES, Eugene. **Evaluating the effectiveness of corporate compliance programs:** establishing a model for prosecutors, courts, and firms. NYU Jornal of Law & Business, 2018. Disponível em: https://www.hbs.edu/faculty/Pages/item.aspx?num=55233

UNIÃO EUROPEIA. **Relatório Anticorrupção da UE.** Bruxelas, 2019. Disponível em: https://op.europa.eu/pt/publication-detail/-/publication/058aecf0-d9b7-11e3-8cd4-01aa75ed71a1.