WESLEY VICENTE DA SILVA

A IMPORTÂNCIA DO COMPLIANCE EMPRESARIAL NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA

SALVADOR
2023

WESLEY VICENTE DA SILVA

A IMPORTÂNCIA DO COMPLIANCE EMPRESARIAL NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA

Artigo apresentado como requisito parcial para obtenção do título de Bacharel em Direito pela Universidade Católica do Salvador.

Orientador: Prof. Darlã Conceição Santos.

SALVADOR
2023

A IMPORTÂNCIA DO COMPLIANCE EMPRESARIAL NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA

Wesley Vicente da Silva[1]
Darlã Conceição Santos[2]

RESUMO: No cenário de exploração das informações como mercadoria econômica, os dados pessoais coletados por empresas privadas tornaram-se fator de tutela legislativa. Assim, surgiu a necessidade de organizar os setores privados para adequar aos moldes da Lei Geral de Proteção de Dados Pessoais – LGPD, com o intuito de proteger a privacidade, como direito autônomo e fundamental para a tutela da pessoa humana, destacando os programas de compliance aliados as boas práticas e governança de dados. Nesse contexto, a fim de consolidar os mecanismos técnicos de segurança para a efetividade da legislação com a finalidade de mitigar os casos de vazamento de dados pessoais, a LGPD implementou medidas administrativas para inibir incidentes decorrentes das condutas infratoras a legislação. Desse modo, este trabalho tem como objetivo demonstrar a importância dos programas de compliance para a proteção aos direitos dos titulares dos dados, visando o cumprimento do ordenamento jurídico. Valendo-se do método hipotético-dedutivo, com abordagem qualitativa, utilizando da revisão bibliográfica de livros, legislação, artigos, dissertações e teses concernente à tutela de dados pessoais no Brasil para o desenvolvimento do presente artigo.

PALAVRAS-CHAVES: Compliance Empresarial. Governança corporativa. LGPD. Vazamento de dados.

ABSTRACT: In the scenario of exploitation of information as an economic commodity, personal data collected by private companies have become a factor of legislative protection. Thus, the need arose to organize the private sectors to conform to the General Law for the Protection of Personal Data - LGPD, in order to protect privacy, as an autonomous and fundamental right for the protection of the human person, highlighting compliance programs allied with good practices and data governance. In this context, in order to consolidate the technical security mechanisms for the effectiveness of the legislation with the purpose of mitigating cases of leakage of personal data, the LGPD implemented administrative measures to inhibit incidents arising from conducts that violate the legislation. Thus, this work aims to demonstrate the importance of compliance programs to protect the rights of data subjects, aiming at compliance with the legal system. Taking advantage of the hypothetical-deductive method, with a qualitative approach, using the bibliographic review of books, legislation, articles, dissertations and theses concerning the protection of personal data in Brazil for the development of this article.

KEYWORDS: Corporate Compliance. Corporate governance. LGPD. Data leak.

[1] Discente do curso de Direito da Universidade Católica do Salvador.
[2] Mestre em Direito, Docente na Universidade Católica do Salvador.

1 INTRODUÇÃO

A nova moeda de troca não é apenas aquela que podemos ver, quantificar ou converter. Os moldes do mercado financeiro mudaram, sendo em questão material ou ao produto que eles precificam, postulando um novo aparato ao objeto contratual: os dados.

Muito embora, os dados pessoais, ainda para muitos, são apenas informações deslocadas acerca de fatores específicos, atualmente, podem ser conceituados como um conjunto de indicadores, regrados por um complexo condensado de informações em um fluxo crescente tangencial.

Os dados da grande massa acabam gerando indicadores que podem ser balizados e influenciados de acordo com os detentores dessa informação, apenas apartado em blocos de informações não são considerados como vetores orçamentários. Porém, direcionados para uma finalidade ordenada tem o condão de influenciar o interesse social.

Dito isso, os mecanismos postos pelo Reino Unido para possibilitar uma estruturação normativa para organizar e gerir os dados dos indivíduos, foi crucial para a criação em outros países, como no Brasil, onde instituiu-se a Lei Geral de Proteção de Dados Pessoais (LGPD). Muito embora, a lei brasileira trouxe um arcabouço de normas reguladoras e sanções aos casos de tratamento de dados, que não foram abarcados com o marco da internet, os dados em uma visão macro constitucional já eram de forma genérica tutelados pela Constituição Federal de 1988.

Todavia, apenas a sanção da LGPD não seria, isoladamente, capaz de coibir as violações ao tratamento de dados na esfera privada, mas sim a necessidade de uma regulamentação do ciclo de vida das informações, que além de estipular os dados que podem ser utilizados ou até quando podem ser armazenados, estabelecer expressamente no bojo da norma como deve ser a proteção na operação do tratamento de dados.

De forma efêmera, conclui-se que a legislação pode delimitar os alicerces capazes de ensejar uma fiscalização, sendo estas através de mecanismo de gerenciamento de atividades, políticas de condutas e implementação de governança de dados, pois os dados hackeados ou vazados de forma isoladas, não seria possível identificar dados sensíveis, muitos menos individualizar o sujeito.

Portanto, o gerenciamento dos dados em provedores de armazenamento pode ter os riscos reduzidos de acordo com a realização de medidas de compliance para dirimir os impactos na

atividade empresarial, como também para tutelar os dados, cada vez mais acentuado como um produto orçamentário.

2 COMPLIANCE EMPRESARIAL

A criação do compliance está entrelaçado sob o cenário econômico-social, assim, sua implementação como sistema de organização foi instaurado e aprimorado a partir dos problemas práticos estruturais para gerir uma boa governança, com intuito de assegurar a proteção e o controle que garante a qualidade do negócio.

A utilização do termo foi inicializada no mercado financeiro, especialmente após a criação do Banco Central em 1913 nos Estados Unidos da América, com a necessidade de um sistema econômico ajustável e estável. Só após 1960, com a regularização da *Securities and Exchange Commission (SEC*), que houve a necessidade de implementação do compliance como um programa para a integração dos procedimento, controle e monitoramento de operação interna. (CARVALHO, 2021)

Em 1977, com a Convenção Relativa à Obrigação de Diligência dos Bancos Suíços, estabeleceu os modelos auto regulatórios, com adequação de condutas e processos internos, na qual a infração tem como consequência à aplicação de sanções. (CARVALHO, 2021)

Só após esse processo de amadurecimento histórico, que o Brasil teve a necessidade de competir em escala global, implementado novos processos de segurança no sistema financeiro brasileiro.

Pode-se concluir que, após a globalização com o fenômeno da criação dos dados estruturais, houve a potencialização das informações adquiridas por meio de provedores, classificadas, atualmente, como fonte econômica de um produto quantificativo e qualitativo, ao qual possibilita uma utilização como um produto do sistema financeiro.

Nesse sentido, em decorrência de ataques cibernéticos em provedores de informações massificadas conduziram a sociedade na aplicação de institutos de melhoramento, como o compliance e suas interfaces para proteger no ambiente corporativo os dados massificados recebidos em seus provedores.

2.1 O CONCEITO DE COMPLIANCE

Antes de enveredar sob o conceito de compliance na esfera privada, é oportuno compreender o seu significado. Nesse contexto, a palavra compliance advém do verbo inglês, *to comply*, que pode ser definida como conformidade. O instituto deve ser aplicado como plano principal de uma diretriz pré-estabelecida para ser dirigida a todos capazes de enfrentar a finalidade destinada. (BERTOCCELLI, 2019)

Nesse parâmetro, pode ser traduzida como:

> *Comply*, em inglês, significa "agir em sintonia com as regras", o que já explica um pouquinho do termo. Compliance, em termos didáticos, significa estar absolutamente em linha com normas, controles internos e externos, além de todas as políticas e diretrizes estabelecidas para o seu negócio. (ENDEAVOR DO BRASIL, 2022, n.p)

O compliance pode-se ser definido de forma técnica como um conjunto de normas padronizadas, sob um viés ético e legal, na qual após estruturação será a matriz orientadora para o comportamento organizacional da instituição ao qual atuará no mercado, como também irá reger as atividades dos colaboradores. Dessa forma, sendo um instrumento hábil a controlar o risco de imagem, a normatização legal, chamados de riscos de compliance, as que recaem nas instituições no decorrer da sua atividade laboral. (CANDELORO, 2012).

Superada a barreira terminológica, a finalidade do compliance tem como escopo o gerenciamento adequado do risco de atividades, verificar adequadamente as normas éticas e legais, e estudar os possíveis danos tangenciais. Dessa forma, esses elementos visam a redução de perdas e danos, como também amplifica a cultura e fortalecimento corporativo nos moldes aos padrões exigidos, seja esse por lei ou na tentativa de dirimir o risco do serviço prestado.

Portanto, segundo a doutrinadora Frazão (2007, p. 42), destina-se em sua obra que o compliance é como:

> (...) conjunto de ações a serem adotadas no ambiente corporativo para que se reforce anuência da empresa à legislação vigente, de modo a prevenir a ocorrência de infrações ou, já tendo ocorrido o ilícito, propiciar o imediato retorno ao contexto de normalidade e legalidade.

Nessa mesma linha de pensamento, de acordo com os autores da obra Compliance 360° (2012, n.p), referem-se o compliance a:

> Um conjunto de regras, padrões, procedimentos éticos e legais que, uma vez definido e implantado, será a linha mestra que orientará o comportamento da instituição no mercado em que atua, bem como as atitudes de seus funcionários; um instrumento capaz de controlar o risco de imagem e o risco legal, os chamados 'riscos de compliance', a que se sujeitam as instituições no curso de suas atividades.

Pode-se concluir que o conceito de compliance, em uma esfera macro, é um aglomerado de regras pré-estabelecidas através de um instrumento perpetuado por técnica de desenvolvimento, capaz de dirimir riscos e danos das atividades devolvidas pelo plano diretor.

Muito embora, o instituto "compliance" tem uma definição extensiva e não tem como fim apenas o cumprimento da legislação e de condutas éticas, pode ser compreendida também como um instrumento de diminuição de riscos, desenvolvimento corporativo sustentável e subsequentes segmentos empresariais de negócio. (ROQUE, 2019)

O compliance além de estar associado tradicionalmente a uma perspectiva organizacional aos comandos administrativos, pode ser vinculada também a uma visão de uma sociedade digital 4.0, devendo não só apresentar o compliance empresarial na esfera de redução de risco à imagem, mas sim, em uma abordagem de pré-orientação e implementação de desenvolvimento aos moldes legislativo de proteção aos dados, como objeto principal de estudos.

Portanto, é necessário a elaboração do projeto de compliance em uma visão lógica, a modo de compreender os objetivos e os componentes da aplicação do programa. Posteriormente, superado os obstáculos, aplica-se os estudos de riscos a boa governança corporativa com a implementação de programas de governança de dados objetivando auxiliar o controle de informações em conformidade aos padrões da corporação, e mitigar os danos da empresa.

2.1.1 AS GOVERNANÇAS CORPORATIVAS E A IMPLEMENTAÇÃO DOS PROGRAMAS DE COMPLIANCE

Em linhas gerais, o Instituto Brasileiro de Governança Corporativa – IBGC (2015, n.p) discrimina o conceito de Governança Corporativa, como: “Sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas. ”

O sistema da governança corporativa está associado ao desenvolvimento interno de uma empresa, seja ele entre a administração, sócios e funcionários, capaz de criar elos para uma estruturação de direção racional e acima de tudo nos moldes da ética e legislação.

Muito embora, a governança corporativa e o compliance sejam institutos que se assemelham em uma visão macro, os mesmos, diferenciam na aplicação prática, mas se complementam no objetivo final, sendo um instrumento para aplicação do outro.

A prática da governança corporativa, além de estimular o valor empresarial, pode-se concluir que estrutura de forma adequada a medida necessária para organizar a atividade empresarial, assim, não há que se falar em condutas prejudiciais. Por exemplo: empresários compreendem que para realizar uma instrumentalização segura aos seus sócios e administradores tendem a prejudicar o negócio empresarial, assim o autor Eggon João da Silva (2005, p.259) retrata que: "A governança corporativa assegura tratamento equânime a todos os acionistas, inclusive minoritários, preferencialistas, nacionais e estrangeiros. Todos devem ter oportunidade de reparação caso venham a sofrer violação de seus diretores. "

Nesse passo, as críticas ao sistema não são viáveis, tendo em vista a utilização de instrumento capaz de integralizar ao plano empresarial. Sendo assim, o programa de compliance visa amplificar a utilização de um sistema para garantir que todos possam participar de forma justa sob o aspecto legal, seja sócio ou administrador.

Em uma tangente geral, a implementação da governança corporativa ressoa em uma perspectiva segura, tanto internamente, seja auxiliando as avaliações das atividades executadas pelos sócios/administradores, quanto externamente, em relação à imagem da empresa, sendo este um fator primordial a empresas estruturadas no mercado.

A implementação da governança corporativa deve ser estruturada de acordo com as necessidades da empresa, devendo verificar o histórico de desenvolvimento do estabelecimento, pois, só a partir do status da empresa pode-se delimitar a estratégia possível para uma implementação segura e adequada. Sendo assim, um regramento mais rigoroso pode gerar consequências negativas e ineficazes, especificamente em estágios primários, pois em atividades inicias, as tomadas de decisões e a execução da atividade empresarial é primordial, sendo necessário, um aspecto negocial informal para realizar os objetivos da empresa, o que não se verifica quando existe prática de boa governança devidamente estruturadas no negócio. (KLEINDIENST, 2019)

Ao desenvolver da atividade da empresa, além da atenção a organização interna, sendo está um fator primordial da governança, ainda que no fim acabe tendo um aspecto externo por vislumbrar no mercado financeiro uma maior complexidade da entidade. O desenvolvimento da empresa, seja no faturamento, importação comercial, quantidade de funcionários, além dos controles a observância da legislação e regras internas, tendem à serem complexos, e, que necessita

de ações maiores que a própria instituição empresarial, restando necessária a implementação de sistema organizacionais aos fluxos de informações. (KLEINDIENST, 2019)

Ultrapassado a esfera conceitual e instrumentalização da política de boas práticas de governança, cabe pontuar que as empresas que possuem fluxos de informações sensíveis, conforme estipula o artigo 50 da Lei Geral de Proteção de Dados Pessoais, os controladores e operadores são responsáveis pelo tratamento de dados, devendo criar planos de adequação a legislação.

Assim, ao confeccionar as regras de boas práticas, os controladores adjuntos com a administração devem estipular através da análise da natureza dos dados coletados, a probabilidade, a finalidade e o potencial de riscos das vantagens advindas dos tratamentos dos dados verificados. (NASCIMENTO, 2020)

É necessário pontuar que, os agentes de tratamento, após a autenticação da gravidade e sensibilidade dos dados aos riscos de operação, poderão estabelecer programa de governança em privacidade, sendo este, um instrumento amplo com normas de compliance, além dos aspectos operacionais.

Em relação ao programa de governança de privacidade, pode-se estabelecer como um aglomerado de normas-regras de boas práticas de governança, com a finalidade de executar ordens de natureza legal. (NASCIMENTO, 2020)

Portanto, os instrumentos do compliance em conjunto com a boa prática de governança, se consagram na identificação dos riscos e estruturação de medidas para a empresa, sendo respondida de forma adequada e proporcional ao suporte da tomada de decisão.

O Programa de compliance na esfera privada para análise de dados pessoais, com a finalidade de promover a segurança, deve ser constantemente monitorado e atualizado, com a implementação de “salva vidas” em decorrência de avaliação de riscos à privacidade e o acometimento de vazamentos. (NASCIMENTO, 2020)

Portanto, os instrumentos e objetos referenciados demonstram a determinação de regras de governança no ambiente de operação de tratamento de dados pessoais, a modo que seja realizado uma estruturação nas empresas para que possibilitem a implementação de mecanismos de segurança, com a finalidade de dirimir os riscos da atividade empresarial na sociedade digital.

3 GOVERNANÇA DE DADOS

O mercado digital tem como principal ativo financeiro os dados, este considerado como "matéria prima" de uma economia baseada no conjunto de informações, sendo que nos últimos anos, houve um aumento exponencial na coleta de dados por cooperativas, startups e novos nichos empresariais, tendo a finalidade de quantificar e gerencias os dados.

Dados, informações, conhecimento e sabedoria são os quatros estágios evolutivos da cadeia de informação, pode-se assim, compreender os dados como fatos ou registros em seu formato primário. (BEAL, 2014). Já a informação é entendida como os conjuntos processados de dados em um contexto aplicado (RÊGO, 2013). Muito embora, na sociedade da informação "os dados são o novo petróleo", apenas os dados isoladamente não são capazes de transformar em ativo financeiro, sendo necessário administrá-lo de forma eficaz, para que assim, as empresas adquiram vantagem competitiva.

Dessa forma, a governança de dados tem como principal objetivo atender as necessidades das empresas, ou seja, solucionar problemas, diminuir custos da administração, para que os dados transformem em saldo positivo para os negócios (TERRA, 2017).

O *Data Governance Institute -DGI* (2017, n.p) definiu governança de dados como "um sistema de direitos de decisão e responsabilidades para processos relacionados à informação, executado de acordo com modelos acordados que descrevem quem pode realizar quais ações com quais informações e quando. " Portanto, a utilização da governança de dados orienta quais os métodos deverão ser aplicados no ciclo de vida dos dados.

Uma das atribuições da governança é o acompanhamento da operação dos dados com a finalidade de gerir que as informações estejam alinhadas com os objetivos pré-determinados na coleta primária, além disso, é necessário assegurar que as informações estejam disponíveis para acesso, quando consultadas, gozar de qualidade, consistência, auditabilidade e segurança dos dados (ESPÍNDOLA, 2018).

No âmago da cadeia evolutiva da informação uma das preocupações dentro das organizações corporativas é o receio com a proteção das informações, ou seja, a capacidade das empresas no protagonismo da segurança com os provedores internos, tendo em vista a necessidade de conformidade com a legislação pátria.

A boa governança tem como objetivo aplicável à prática do controle dos processos de operação dos dados: a prevenção de situações adversas que podem gerar o comprometimento da

integralidade dos dados adquiridos pelas organizações empresariais, que por sua vez, devem ter o condão de reforçar a confidencialidade das informações. (ESPÍNDOLA, 2018).

A integração do programa de governança de dados nas corporativas empresariais, tem como o esforço principal a organização de dados, que deve ser observado por um prisma basilar, ou seja, a aplicação dos princípios como limite legal e ético no ciclo de vida dos dados.

Para Rêgo (2013), os princípios são regulamentações para compreender aplicação da governança dos dados como linha direta para os negócios, sendo: (i) A gestão de dados estratégicos, tem o dever de vislumbrar as tomadas decisões por um coeficiente tático e operacional. (ii) A governança como instituição, ou seja, a governança de dados pode ser comparada como sistema governamental, na qual dispõe de legislação, execução e jurisdição; (iii) A governança de dados como um programa, devendo ser implementado como fator permanente, não apenas um projeto temporário. Ainda, pontua-se que os princípios da Governança de dados não são limitados, tendo uma orientação basilar a cada implementação de um sistema organizacional que deve ser observado pelo prisma ético e legal.

Assim, os princípios devem incumbir os papéis que a serem preenchidos pela gestão moldar os comportamentos das empresas para a aquisição, reserva e utilização dos dados conforme as normas e políticas da corporação (TERRA, 2017).

Coleta, armazenamento, recuperação e descartes, são as quatro etapas do ciclo de vida dos dados (SANTANA, 2013), ou seja, para a aquisição de dados pelas empresas, deverão observar a vida útil do dado para não incorrer na (in) responsabilidade da utilização indevida de informações dos seus provedores.

As fases do ciclo de vida dos dados devem ser observadas pela ótica de seis objetivos, sendo eles: a qualidade, a privacidade, os direitos autorais, a integração, compartilhamento e preservação dos dados (ESPÍNDOLA, 2018). Muito embora, a lei geral de proteção de dados implementou e traçou novos objetivos para a coleta de dados pessoais, cabe destacar que os objetivos vislumbrados na Governança de dados têm como parâmetro preliminar a tomada de decisão, na qual deve ser os negócios pautados nos moldes legais e éticos vigentes.

Nesse contexto, o controle de informações é necessário, tendo em vista que na sociedade da informação, cada vez mais o volume de dados é crescente, acarretando mais vazão e protesto por políticas públicas para a preservação dos institutos, órgãos e empresas que detenham a

informação, sendo assim, necessário sistema de organização, softwares e hardwares capazes de processar as informações, criptografar e armazenar. (MARTIGNAGO, 2019)

Assim, para otimizar o ciclo de vida dos dados e garantir que os objetivos sejam preenchidos na estruturação do gerenciamento de dados, faz-se necessário a implementação de frameworks com o intuito de garantir que o procedimento seja cumprido com maior qualidade de informação e aproveitamento financeiro para a empresa, auxiliando a tomada de decisão para redução de risco para utilização de dados. (MARTIGNAGO, 2019)

Um Framework, segundo Johnson (1991), pode ser definida como um aglomerado de objetos que colabora entre si para que atinja um conjunto de obrigações para aplicação de um domínio especifico. Já para Pinto (2000), um framework é conceituado como um software incompleto criado para ser um objeto cujo estado e comportamento são definidos pela classe. Assim, o framework é uma concepção de uma arquitetura para um edifício de subsistemas e oferece o alicerce básico para criá-los.

Muito embora, os autores defendem uma conceituação distintas acerca da concepção de frameworks, pode-se verificar que ambas se complementam, tendo em vista que o framework é um sistema pré moldado, ou seja, é um programa com intuito de ser complementado através da finalidade a ser cumprida pela gestão empresarial, sendo instanciado por classes para categorizar os dados e ser alojado em hotspot, provedores físicos, capazes de armazenar as informações coletadas pelas empresas.

Portanto, para gerenciar os ativos de dados de forma complexa, ordenada e objetiva é necessário para proteção do procedimento do ciclo de vida dos dados, determinar os modelos de frameworks para o gerenciamento dos dados. Assim, para Carvalho (2021), podem ser apresentados três domínios CobiT, DAMA DMBOK e DGI Framework, sendo apenas dois destes observados para fomento deste artigo: (i) A DAMA (DAMA DMBOK), e (ii) CobiT.

A DAMA (*Data Management Association*) é uma associação sem fins lucrativos, com o intuito de promover boas práticas de gestão de dados, e em 2009 fundou o DAMA-DMBoK (Data Management Body of Knowledge), sendo um corpo de conhecimento que tem como ponto fundamental esclarecer como as corporativas devem aplicar a operação otimizada dos dados. (CARVALHO, 2021)

Em sua versão 2.0, acrescenta não só uma visão macro do gerenciamento de dados, definindo padrões, terminologias e práticas, mas a integração de dados, para definir táticas,

armazenamentos e sistemas, bem como implementação da ética na operação do tratamento de dados, a definição de big data e ciência de dados e amadurecimento das informações. (LIMA, 2019).

O DAMA-DMBOK V2 é formado por 11 (onze) funções de gestão de organização de dados, sendo incorporado como cerne principal: a governança de dados, tendo em vista que os dados percorrem por toda sistemática das onzes funções ordenadas, assim segundo Honório (2021):

A primeira função é a governa de dados, sendo o pilar do framework, tem o condão de orientar e supervisionar a operação do ciclo de vida dos dados, na qual deve estabelecer um sistema de apoio a decisão dos gestores sobre os dados, sob o prisma do negócio.

A arquitetura de dados, a segunda função, pode ser conceituada como um planejamento para administrar os dados, aquisição de ativos da empresa, com o intuito de definir a finalidade das informações adquiridas com os requisitos necessário para o gerenciamento dos dados.

Por sua vez, a modelagem de dados e design, tem a função de demonstrar de forma nítida os dados, sendo o processo da descoberta, análise e representação da etapa primária da informação.

O armazenamento, uma das etapas da operação do ciclo de vida dos dados, na qual vai incluir o design, o suporte dos dados armazenados para quantificar o coeficiente valorativo das informações, até o seu descarte, devendo respeitar todo o procedimento de segurança legal vigente.

Um dos alicerces para o gerenciamento de informação é a segurança, que deve garantir a proteção dos dados, a execução de políticas e procedimento de segurança, no intuito de moderar o acesso de forma consciente e controlado, não devendo ser infringido ou acessado de forma inadequada, afim de garantir autenticação e auditoria de dados informações.

A Integração e Interoperabilidade de dados, é a função responsável pela movimentação e a concretização dos dados na interligação do armazenamento e outras plataformas.

O gerenciamento de documentos, pode ser compreendida como o gerenciamento e inclusão da vida útil dos dados e informações, encontrados em programas não estruturados, em ênfase ao conteúdo de apoio de conformidade a legislação vigente e os termos éticos formalizados para o negócio.

Dados mestre e de referência, tem como condão a manutenção dos dados compartilhados para coexistir a integralidade dos sistemas internos de gerenciamento dos dados.

Em razão da interligação entre uma linha direta com os negócios, uma das funções do DAMA-DMBOK é a *Data warehousing* e *Business intelligence*, ou seja, a implementação de

planner para o *contoler* da administração dos dados e suporte a decisão com o intuito de conceder aos gestores de informação emitam relatórios de equalização de valores.

Segundo Barata (2015), os metadados, na qual consiste a décima função, é promover a facilitação do acesso dos dados interligados nas multifontes do sistema integrado, como também garantir a qualidade de dados.

Por fim, o gerenciamento de qualidade de dados é a implicação das técnicas para garantir a possibilidade de aferição, melhoramento e adequação da utilidade dos dados, com o intuito de monitorar a integridade da informação primária no ciclo de vida dos dados.

Já o COBIT (*Control Objectives for Information and related Technology*), é um framework de suporte fundado em 1994 administrado pela ISACA (*Information Systems Audit and Control Association*), estruturado como um arcabouço de informação direcionadas para governança de dados e gerenciamento de informação, tem como objetivo auxiliar os profissionais de gestão na conexão entre os problemas técnicos e os riscos do negócio. (BARATA, 2015).

Para Lima (2019), o COBIT é um framework que possui duas vertentes basilares: a gestão, que possui quatro áreas de domínios: planejamento, constituição, execução e monitoramento, e a governança que é a tomada de decisão de acordo com a gestão de dados, possuindo 37 (trinte e sete) processos integrados.

Na versão 5.0, o sistema é utilizado baseado em 05 princípio, conforme elucida Casaes (2019), Barata (2015) e Lima (2019), sendo: (i) atender às necessidades das partes interessadas; (ii) cobrir o negócio como um todo; (iii) aplicar um framework único e integrado; (iv) habilitar uma visão holística; e (v) distinção entre governança de gestão.

Um dos princípios é atender às necessidades das partes interessadas, sendo a necessidade das corporativas é satisfazer as expectativas dos seus *stakeholders*, proporcionando um equilíbrio na tripartite: benefícios, redução do risco e recurso disponíveis.

O segundo princípio é baseado na cobertura do negócio como um todo, ou seja, abranger a integralidade da empresa no processo, procedimento, pessoas e as relações com os habilitadores.

A aplicação do framework único e integrado, assim, o COBIT é capaz de promover uma relação completa com a Governança de dados, corroborando ao alinhamento com padrões externos e adaptabilidade dos modelos usuais de negócios.

O COBIT permite habilitar uma visão holística, ou seja, uma visão macro dos componentes que oferecem suporte para atingir as finalidades da governança de dados, na qual define como catalogadores: as políticas, processos, estruturas organizacionais, informação e ética.

Por derradeiro, o princípio da distinção entre governança de gestão, tendo em vista que ambos possuem estruturas organizacionais distintas, assim, governança tem como esforço principal que os objetivos corporativos sejam cumpridos, estabelecendo prioridades pela tomada de decisão, compliance e progresso das organizações. Por sua vez, a gestão é o planejamento, construção, execução e monitoramento das funções ornamentada com o direcionamento da governança.

Desse modo, com escalonamento dos cinco princípios é capaz de proporcionar o funcionamento otimizado do framework, destacando os seguintes processos:

O APO01: Gerenciar o framework de TI, tem como condição a otimização das atividades relacionadas ao TI, com a função principal de incluir os procedimentos e regulamentos para promover a integralidade das informações nos bancos de dados. (BARATA, 2015)

Já o APO03: Gerenciar a arquitetura corporativa, tem função primordial agrupar as informações para auxiliar as atividades e tomadas de decisões, conceituando e compartilhando as informações dos elementos dos dados, e por fim catalogar a empresa, com base na modulação e sensibilidade dos dados. (BARATA, 2015)

Nesse ínterim, a governança de dados como um sistema integrado com o programa de compliance, tem o condão de otimizar a operação de controle interno relacionado aos dados coletados pelas empresas, capaz de gerenciar as bases para o apoio de decisão ao tratamento das informações, com segurança e qualidade, garantido o ciclo da vida útil dos dados.

4 A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

As estruturas políticas, econômicas e sociais com desenvolvimento de novas tecnologias e mecanismo para a coleta de dados e informações, fez necessário modulações legislativas para a proteção da privacidade, além dos aspectos físicos, patrimoniais e morais.

A proteção à privacidade de dados foi dividida em quatros gerações: a primeira, oriunda do estado moderno, com o advento dos bancos de dados; a segunda, datada em 1980, com a expansão legislativa para a proteção à privacidade aos setores privados; a terceira geração em 1990, com o processo de tratamento de dados e o consentimento dos cidadãos; Por fim, a última dimensão, é

destinada ao protagonismo da permissão para coleta e uso dos dados pessoais, quando a lei estabeleceu a importância da titularidade das informações. (MENDES, 2014)

Nesse aspecto, é perceptível a evolução do direito aos fatores reais da sociedade e as transformações dos meios tecnológico, computacionais, genéticos e comunicativos, que por sua vez possibilitou a integração da comunicação global, e consequentemente, o rastreio dos dados através do armazenamento de informação. (SAAD, 2021).

Os legisladores ao considerar os dados pessoais como extensão ao direito à privacidade, preocuparam em tutelar constitucionalmente a proteção da população, em especial os países europeus, como: Espanha, Portugal, Hungria, Eslovênia e Rússia. (VIEIRA, 2007) Porém, só tornou-se fator primordial após o regulamento geral do Parlamento Europeu sobre a proteção de dados, n.º 2016/679, sendo necessário a adequação das empresas prestadoras de serviço na Europa ao regulamento, influenciado diretamente o Brasil para elaboração da Lei Geral de Proteção de Dados brasileira. (SAAD, 2021).

Muito embora, a Lei Geral de Proteção de Dados Pessoais - LGPD, em sua promulgação, não abarcou de forma expressa a proteção de dados como direito fundamental, a doutrina, em especial Nascimento (2020), por sua vez, já argumentava a proteção de dados e informações pessoais como direito autônomo, derivado do direito fundamental à privacidade, explicitamente no artigo 5°, X, da CRFB de 1988.

Após reiterados julgamento sobre a tutela dos dados pessoais como extensão da personalidade do indivíduo, o Supremo Tribunal Federal -STF reconheceu no Julgamento da Ação Direta de Inconstitucionalidade - ADI 6387, a existência dos dados como direito autônomo, derivada do direito fundamental a dignidade da pessoa humana, na proteção à intimidade e a centralidade do Habeas Data como autodeterminação informativa. (NASCIMENTO, 2020).

Ao compreender a necessidade da proteção aos dados pessoais, os legisladores brasileiros em votação de ⅗ das casas legislativas (câmara e Senado Federal) em dois turnos, aprovaram a Emenda Constitucional 115 de fevereiro de 2022, alterando o artigo 5° da Constituição Federal de 1988, incluindo o inciso LXXIX, tutelando constitucionalmente a proteção aos dados pessoais, inclusive nos meios digitais.

Ressalta-se, ainda, que os dados pessoais estão interligados com o direto fundamental à privacidade, na qual representa a capacidade de a pessoa administrar sua vida, seus pertences e

propriedades materiais e imateriais, permitindo ou não a utilização dos seus dados (bens imateriais) por terceiro. (NASCIMENTO, 2020).

A privacidade, por sua vez, segundo Mendes (2008), é o direito à proteção aos comportamentos pessoais e acontecimentos de caráter íntimo, bem como as informações prestadas aos profissionais e comerciantes, em que a pessoa não deseja que se compartilhe com o público.

Para o professor William Prosser, pode-se qualificar a lesão a privacidade em quatro graus: i) o intrometimento na reclusão ou solidão na vida privada, ii) a divulgação pública de fatos privados constrangedores sobre o indivíduo; iii) a publicidade sobre o indivíduo apresentada de forma equivocada; e iv) a apropriação, para obtenção de vantagem, do nome ou da imagem do demandante (PROSSER, 1960).

A doutrina, por sua vez, defende mais uma violação à privacidade: a privacidade informacional, interligada com os fatores tecnológicos de informação. (SAAD, 2021). Assim, quando a lei ao realizar o tratamento da privacidade, refere-se como um direito líquido, ao qual será tutelado para garantir que o indivíduo tenha um local reservado, que não tenha, se desejar, a interferência de outros sujeitos, seja pessoa física ou jurídica.

Com a proteção dos dados pessoais dos titulares, através da LGPD, possibilitou ao cidadão o acesso a informações ao ciclo de vida útil dos dados pelas empresas, e a certeza de fiscalização pela Autoridade Nacional de Proteção de Dados, com a finalidade de atingir os objetivos traçados pela legislação, na qual a lei traz conceitos e delimita princípios, que devem ser mencionados.

A LGPD tem como objetivo principal: “o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado”, com a destinação de assegurar os direitos fundamentais a liberdade e privacidade dos titulares dos dados, bem como tutelar a dignidade e a personalidade da pessoa natural. (LGPD).

A legislação está ordenada diretamente com o meio empresarial, sobretudo no que se refere aplicação aos seus destinatários que são pessoas físicas ou jurídicas que realizam a coleta e tratamento de dados no Brasil, conforme preceitua o artigo 1° da lei 13.709, de 14 de agosto de 2018.

Para compreender a LGPD, faz-se necessário elucidar os conceitos de dados pessoais: (art. 5º, I) é toda informação relacionada a pessoa natural, identificada ou identificável, sendo o dado aplicado no contexto que possibilite o reconhecimento do indivíduo. Bem como refere-se aos dados sensíveis (art. 5º, II), são todas as informações que se relaciona com pensamentos políticos, crenças,

identidade biológica e física. Portanto, a legislação tem como ponto a proteção e o cuidado para a não violação dos dados pessoais e sensíveis.

Os doutrinadores, Laura Schertel e Danilo Doneda, ainda aponta cinco pilares para compreender a LGPD, sendo: i) a unidade e generalidade da aplicação da Lei; ii) a legitimação para o tratamento de dados (hipóteses autorizativas); iii) os princípios e direitos do titular; iv) as obrigações dos agentes de tratamento de dados e v) a responsabilização dos agentes.

O primeiro pilar é considerado com aplicabilidade material da legislação, ou seja, aplica-se a qualquer operação realizada por pessoa natural ou jurídica de direito público ou privado, independentemente do meio, da sua sede ou do país onde estejam localizados os dados (Art. 3°). Considerado, assim, como uma aplicação uniforme para todos os setores público ou privados que realizam tratamento de dados.

O segundo pilar é a legitimação para o tratamento de dados, tendo em vista que a lei especificou critérios e requisitos para o reconhecimento da legitimidade, não podendo ser tratados os dados, sem que exista uma base normativa que autorize, prevista no artigo 7°, 11° ou 23° da LGPD, abordando 11 (onze) hipóteses, incluído o consentimento ou a previsão legislativa.

Destaca-se que a autorização por consentimento para ser considerado válido, deve observar os requisitos previsto no artigo 5°, XII, sendo considerado que a vontade deve ser livre, informada, inequívoca e com a finalidade determinada, consagrando os princípios norteadores da legislação.

O terceiro pilar é o conjunto de princípios e direitos que assegura o destinatário da lei a controlar a utilização do seu dado pessoal, sendo importante elencar dez princípios que estruturam a LGPD: a finalidade, a adequação, a necessidade, o livre acesso, a qualidade dos dados, a transparência, a segurança, a prevenção, a não discriminação e a responsabilização. (MENDES, DONEDA, 2018)

No que concerne, aos direitos dos titulares são expressos no artigo 18° da referida lei, que permite o titular dos dados adquirir através do controler, independentemente do momento, as informações relacionadas ao indivíduo, prevendo: acesso, confirmação, correção, anonimização, bloqueou ou eliminação e a portabilidade.

Para adentrar no cerne dos problemas enfrentados pela legislação, em especial, sobre o vazamento de dados, os dois últimos pilares serão abordados sob a perspectiva da violação e responsabilização acerca da proteção de dados nos casos incidentes de vazamento.

Assim, o quarto pilar, destina-se às obrigações dos agentes de tratamento dos dados, na qual estabeleceu limites que devem ser observados nas operações realizadas para reforçar a segurança e prevenir os problemas da atividade no tratamento de dados.

Uma das obrigações fundamentais, consiste na intitulação do encarregado pelo tratamento dos dados indicados pelo controlador, conforme artigo 41 da LGPD, que possui a função de aceitar as reclamações e comunicações dos sujeitos dos dados, receber informações da Autoridade Nacional, como deve orientar os funcionários a respeito das práticas a serem adotadas em relação à proteção de dados pessoais.

Assim, as informações devem ser fornecidas ao proprietário dos dados, quando os dados forem coletados, como: os meios de segurança aderidos ao tratamento de dados, quais são os riscos da atividade que podem gerar lesão ao titular, pois pode gerar a mitigação dos prejuízos. (SAAD, 2021)

A lei Geral de Proteção de Dados Pessoais tem como objetivo a proteção do dados pessoais dos titulares dos dados, sendo assim, uma das obrigações principais é adoção de medidas de segurança, técnicas e administrativas hábeis a proteger os dados pessoais de acessos não autorizados, como promover a integralidade dos dados, não permitindo, assim, a alteração das informações, a prevenção de situações ilícitas ou acidentais, ou qualquer forma de tratamento inadequado, consoante se desprende do artigo 46 da lei.

Tornou-se corriqueiro manchetes acerca do vazamento de dados por corporativas, uma das violações mais graves incidentes abarcados pela LGPD, o que ocasiona a vulnerabilidade do titular dos dados, e dos sistemas internos que são responsáveis pelo ciclo de vida útil dos dados. (SAAD,2021)

A seção de segurança de informação tem como condão as obrigações inerentes aos agentes de tratamento, devendo ser adotado pela integralidade das pessoas que realizam o tratamento de dados, garantido que os dados sejam confidenciais, bem como disponíveis nas operações de tratamento. (Art.48). Nos casos incidentais de vazamento de dados, insurge a necessidade ao controlador de informar a autoridade de proteção de dados, que podem definir as medidas para mitigação dos danos.

No entanto, com a utilização da internet, compras online, transferência virtuais e outros meios tecnológicos, criou-se uma dificuldade para atuar na segurança de dados, tendo em vista a abrangência e os domínios de redes globais, que combinados com fatores não perceptível, forma

um perfil não rastreavel capaz de ocasionar violação às diretrizes básicas da legislação, que mesmo com ações posteriores não conseguem excluir os inúmeros registros de pessoas e organizações que coletaram os dados, lesionando a confidencialidade das informações (SAAD, 2021)

Destaca-se que as obrigações aos controladores e operadores, devem ser observados desde a coleta dos dados até seu descarte, assim o artigo 46 da LGPD, introduziu o conceito de *privacy by design*, sendo a incorporação pelas empresas nos serviços e produtos, na qual dispõe a proteção da privacidade no centro de todo o desenvolvimento corporativo.

Embora, a legislação tenta dirimir os riscos da atividade, os prejuízos causados pelo vazamento de informações são altos, e perpassam pela inadequação do sistema de proteção, perda de credibilidade e de clientes, ocasionado uma ruptura na imagem da empresa, impossibilitando, muitas vezes de concorrer no mercado corporativo. (SAAD,2021)

Portanto, a LGPD concebeu obrigações aos agentes de tratamento de dados, para que se delimite a finalidade da utilização dos dados desde o início da concepção, devendo o controlador confeccionar relatório de impacto a privacidade, utilizando de métodos para a captação da operação do ciclo de vida dos dados, observando as mediadas adotada para aumentar a segurança e mitigar o risco do tratamento das informações, conforme artigo 3 da LGPD.

O último pilar, considerado como a responsabilidade dos agentes na incidência de ocorrência de danos derivados do tratamento de dados. A LGPD consagrou a natureza do tratamento, limitando os parâmetros ao artigo 7° da lei, nas 10 hipóteses dos incisos, vinculados a finalidade da captação dos dados, consoante prevê o artigo 6°, inciso I, II, da LGPD.

A legislação tem como regra o descarte (eliminação) dos dados ao fim do tratamento da operação (art. 16), com o intuito de mitigar os riscos presente no tratamento de dados, principalmente, no que concerne à limitação das hipóteses de tratamentos para não lesionar os direitos dos titulares.

Nos casos, em que mesmo após o término de vida útil dos dados, as empresas podem, quando permitido, armazenar dados que em situação incidentais serem objetos de violação, principalmente nos casos de vazamento, que podem ocorrer, quando não autorizados pelo titular ou controladores, serem acessados, captados, compartilhados pela internet, para outros sujeitos ou empresas.

Assim, a Lei Geral de Proteção de dados Pessoais, em especial em seu artigo 42, dispõe que o controlador ou operador, quando realizar o exercício do tratamento de dados pessoais, vem

a ocasionar dano patrimonial, moral, individual ou coletivo em detrimento a aplicação da legislação, é obrigado a repará-lo, definindo a responsabilidade de forma objetiva.

Embora, a responsabilização objetiva não é necessária a demonstração de culpa do controlador ou operador. Faz mister esclarecer que o operador, só será responsabilizado quando os atos praticados forem contrário à legislação, ou às instruções que foram fornecidas pelo controlador. (MENDES, DONEDA, 2018)

Ainda, a legislação prevê exceções a responsabilidade objetiva (art. 43), sendo: quando o agente demonstrar que não realizou o tratamento de dados pessoais que foi atribuído, ou quando não houve violação da segurança ou a legislação, e por fim, quando for por culpa exclusiva do titular ou de terceiros.

Porém, o cenário que é vislumbrado no Brasil nos casos de vazamento de dados, é que as violações pelas instituições vêm ocorrendo, majoritariamente, sob ataques deliberados de hacker, ou falha de segurança dos controladores dos dados. (SAAD, 2021)

Dessa forma, é necessário adotar medidas para dirimir os riscos da atividade, e possibilitar o discernimento das informações acerca dos perigos de vazamento de dados, tendo em vista que a tendência é aumento significativo das violações vinculados com a crescente tecnológica. Assim, as empresas devem implementar mecanismos para a segurança das informações.

5 O COMPLIANCE EMPRESARIAL COMO INSTRUMENTO DE PROTEÇÃO DE DADOS NA ESFERA EMPRESARIAL

Em decorrência das constantes violações aos dados armazenados em provedores privados, a tutela ao direito à privacidade nos meios tecnológicos, já era pauta de debate na legislação brasileira, e já existiam mecanismos para a proteção, como: a proibição de direcionamento dos provedores em relação ao compartilhamento de dados, bem como a inibição ao monitoramento nos navegadores de internet.

Vinte e seis bilhões de dados foram vazados no Brasil em 2019, de acordo com pesquisas realizadas pelo Massachusetts Institute of Tecnology – MIT, possibilitando a utilização de números telefônicos, score de crédito, endereço eletrônico, fotos, números de identificações e outros dados pessoais, para o cometimento de crimes cibernéticos, e a violação aos direitos dos titulares.

A utilização e uso dos dados pessoais por pessoa física ou jurídica, com sede no Brasil ou não, devem se atentar as normas gerais de proteção aos dados brasileiro, segundo Frazão, Oliva e

Abilio (2020), é a necessidade de conferir a efetividade aos direitos e prevenir a violação aos dados, através da implementação de mecanismo de compliance, como uma ferramenta capaz de promover a adequação das atividades aportadas pelas empresas.

Assim, os controladores e operadores poderão formular regras de boas práticas e governança (Art. 50), que contenha as disposições de organização interna, o regime de funcionamento, as operações, o canal de comunicação entre os encarregados e os titulares dos dados, e o procedimento de segurança.

Nessa perspectiva, considerando que a maioria das tratativas de dados perpassam por meios digitais, deve-se adotar sistema para mapear os riscos, e implementar mecanismos para minorar as vulnerabilidades apontadas pelos programas, através da alta administração, do código de ética, para proteger os dados pessoais dos titulares. (PESSOA, 2021)

Existem inúmeras formas de ocorrer o vazamento de dados, sendo através de ataques cibernéticos, sequestro de conta, furtos de dados, compartilhamento de dados por agentes ou ex-agentes da empresa, erro ou negligência, entre outros, que podem ser para adquirir dados de nomes, CPF, celulares, endereços, dados financeiros, senhas, registro de saúde ou credenciais de acesso. (SAAD, 2021)

Desse modo, para realizar o mapeamento dos problemas que as corporativas podem enfrentar, é necessário identificar os fluxos e processos de informação que percorrem os sistemas, que irão auxiliar na tomada de decisão pelas empresas. (NASCIMENTO, 2020)

A alta administração deverá colaborar ativamente no programa de compliance, seja monitorando as investigações e intervenções em situação para estabelecer controles internos em conformidade com a legislação, bem como possibilitar a interdependência dos setores para realizar as atividades designadas para o tratamento de dados (PESSOA, 2021).

Com a elaboração do código de ética pela organização possibilitará o treinamento regular das equipes, responsáveis pela tecnologia da informação, para enraizar a cultura corporativa da boa governança, com a finalidade de assegurar o respeito ao programa de compliance (NASCIMENTO, 2020)

Nesse contexto, para manter uma boa relação com seus clientes, as organizações devem instalar canais de comunicação, para que os titulares dos dados possam contatar os encarregados responsáveis pelos armazenamentos dos seus dados, e exerçam seus direitos sobre as informações contidas nos provedores. (PESSOA, 2021).

Desse modo, quando se trata de concretização a alteração cultural coportariva é preciso realizar o alinhamento dos funcionários com o código de ética, com política de privacidade, para fins de efetividade do programa de compliance de dados. (PESSOA, 2021).

5.1 A IMPLEMENTAÇÃO DE MECANISMOS DE GOVERNANÇA DE DADOS PESSOAIS

Para a efetividade da legislação em relação ao tratamento de dados, a LGPD direciona um capítulo para implementar o programa de governança em privacidade, com a finalidade das empresas adotarem medidas técnicas, para fins de proteção e segurança dos dados pessoais. (PESSOA, 2021)

A governança em privacidade, pode ser conceituada como um conjunto de regras e práticas positivas a serem implementadas pelos agentes de tratamento, e encontra-se em conformidade com as políticas de compliance empresarial, com o objetivo de gerir os dados das empresas para estabelecer um diferencial competitivo aos negócios. (KOEPSEL,2020)

O programa integra o aperfeiçoamento do procedimento de utilização dos dados, com os requisitos pré-estabelecidos na implementação dos softwares, com a finalidade de gerir de forma otimizada os dados para preencher as diretrizes da legislação. (SAAD, 2021)

A Lei Geral de Proteção de Dados Pessoais dispôs que os controladores e operadores poderão adotar programas de governança em privacidade, que devem ser implementados com o mínimo, (art. 50, § 2°, I): a) o comprometimento dos agentes de tratamento com as políticas internas que devem garantir o cumprimento das normas e regras de boas práticas; b) que aplicação seja de forma uniforme para todo a operação de tratamento de dados; c) que a governança seja adaptativa as estruturas da empresas, sendo compatível com a densidade dos dados e operação; d) como implementar políticas de salvaguardas em relação aos titulares dos dados; e) tenha como objetivo estabelecer uma relação de confiança com sujeitos dos dados, estabelecendo situações de transparência e que possibilite a atuação do titular; g) que conte com planos de respostas a incidentes e remediações; h) seja continuamente atualizado sua base.

Nesse aspecto, devem ser adotadas medidas administrativas para que as instituições, em conformidade com a legislação, apliquem estímulos para assegurar as informações armazenadas pelas empresas, com a adoção de orientações internas que respeitem as diretrizes que inclua o uso

minimizado ou a anonimização das informações, desde a coleta dos dados, conforme artigo 46 da LGPD.

Com o mapeamento das atividades, é importante verificar: O que são esses dados?; de que forma foram coletados ?; quem são os coletores ?; existe relação entre os dados e atividade realizada ?; O que pode ocorrer com esses dados ao serem coletados? E, como são descartados da gestão organizacional da empresa? (NASCIMENTO, 2020). Dessa forma, para adotar medidas compatíveis com os riscos alertados pelos sistemas para a proteção de dados nas organizações privadas, é necessário possuir conhecimento do caminho realizado inerentes ao ciclo de vida útil dos dados.

Embora, a legislação já estabeleça diretriz mínima para o tratamento de informação, a Autoridade Nacional de Proteção de Dados - ANPD, poderá, ainda, determinar padrões técnicos para serem implementados pelo programa de governança em privacidade, devendo ser observado a qualidade de dados, as especificações do tratamento e status tecnológico, em especial a proteção aos dados sensíveis disposto na legislação. (NASCIMENTO, 2020)

Muito embora, a lei geral de proteção de dados, apenas delimita as características e os requisitos mínimos que os operadores deverão tomar para desenvolver um compliance na organização das empresas privadas em consonância com a legislação, porém não impõe um modelo específico para integração de um programa nas corporativas. (PESSOA, 2021)

Assim, para Saad (2021), as medidas técnicas que podem ser adotadas pelos agentes de tratamento de dados, são: i) o uso de firewalls, sendo um mecanismo de segurança que coleta os dados em conformidade com as regras pré estabelecido para análise de tráfego de rede, delimitando as operações de compartilhamento e captação de informações a serem cumpridas; ii) a utilização de antimalware, que consiste na proteção contra vírus que é capaz de fragilizar o sistema, apagar dados e infectar outros arquivos; iii) a utilização de criptografia dos dados, que possibilite quando ocorrer situações incidentais a não identificação do titular do direito.

Já para Fernandes e Abreu, (2014) defendem a implementação de frameworks como a DAMABOK e COBIT, para o gerenciamento de dados, pois tem como meta principal a delimitação do escopo das atividades, as funções envolvidas no tratamento e as interações a serem executadas pelo software, com a finalidade de proteger a privacidade em ambientes corporativos que gerenciam o armazenamento de informações aplicados na prevenção à fraude.

Segundo Carvalho (2021), a integração do software, através das boas práticas estabelecidas pela legislação, poderá aprimorar os aspectos de proteção à privacidade e prevenção a fraude do tratamento de coleta de dados. Tendo em vista, que os frameworks, podem balizar as métricas de qualidade dos dados que indicam uma utilização adequada e otimizada, e aponta a melhor proteção da privacidade.

Com a melhoria de processo de governança para o tratamento de dados, estabelece uma divisão entres as operações que possibilita uma automatização do ciclo de vida dos dados (coleta, utilização, armazenamento e exclusão), capaz de gerar relatório de risco, para o auxílio da tomada de decisão com o intuito de gerir de forma adequada o tratamento de dados. (CARVALHO, 2021)

Neste parâmetro, os programas de compliance com a implementação de frameworks, podem responder questionamento acerca do procedimento de tratamento de informação, dispondo de quais práticas relacionadas à governança, privacidade e segurança de dados, apresentam melhor benefício para o tratamento de dados pessoais. (CARVALHO, 2021)

Ademais, os controladores e operadores deverão adotar medidas, como o Relatório de Impacto – DPIA), que corresponde a avaliação dos riscos e impactos relacionados com o tratamento de dados pessoais, além da anonimização, da transparência e do sigilo, deverão delimitar prazos para retenção de dados e aderir políticas seguras de informação acerca da operação de tratamento. (SILVA, 2022)

Após realizar a implementação e observância das estruturas mínimas estabelecidas pela LGPD, é necessário adotar um programa de gerenciamento de vulnerabilidades, com atualizações constantes e autocorreções alinhados com as boas práticas de atividades cotidianas, com a finalidade de proteger os dados pessoais, e promover um ambiente corporativo adequado para realizar o tratamento de dados. (SAAD, 2021)

No entanto, ao verificar que houve vazamento de dados, seja pelo recebimento de notificação ou pela veiculação na mídia, os agentes de tratamentos deverão identificar quais dados vazaram e realizar o procedimento estabelecido no programa de compliance de segurança, além de notificar as instituições. (Art. 48, caput).

De acordo com MIT, o prazo entre a comunicação à autoridade competente e a ocorrência do fato ilícito ultrapassa 200 (duzentos) dias em média, sendo umas das preocupações para a efetividade da legislação, e a redução dos danos causados aos titulares dos bens imateriais.

A Lei Geral de Proteção de Dados, dispõe que nas situações que ocorrer a probabilidade de riscos ou violação aos direitos dos titulares, tem como obrigação do encarregado a comunicação à autoridade nacional e ao titular do dado (art. 48, caput). Sendo que o contato deve ser em período razoável (art. 48, § 1º), contendo a natureza dos dados dos titulares atingindo (art. 48, § 1º, I).

Em decorrência dos possíveis incidentes, a LGPD determinou critério para aplicação de sanções, em casos de vazamento de dados, observando as situações específicas de cada caso, disposto no art. 52, § 1º. Assim, deve ser considerada a avaliação da gravidade, a natureza das informações e do dano ocorrido (incisos I e VI), sendo necessário para este caso, tendo em vista que o compartilhamento indesejado de dados sensíveis pode ocasionar danos irremediáveis para os titulares.

Portanto, existe a necessidade da adesão aos mecanismos e técnicas para promover a efetividade dos programas internos com a finalidade de mitigar os danos, assim, a implementação de boas práticas e governança têm como fator o cumprimento da legislação, por meio de medidas de segurança. Entende-se, que a proteção integral contra falhas que possibilitam a ocorrência de ilícitos não é possível, porém essas diretrizes reduzem as possibilidades de existir desvios de condutas e criar salvaguardas para identificação dos incidentes, de forma eficaz, rápida e adequada.

6 CONSIDERAÇÕES FINAIS

A partir da permissão ao acesso dos dados pessoais, as informações coletadas passaram a integralizar as redes de tratamento de dados, tornando-se alvo de ataques cibernéticos, contribuindo para o aumento da intercorrência no ambiente corporativo, tornando-se o gerenciamento de informação um dos diferenciais no desenvolvimento do negócio.

Nesse contexto, foi imperativo o surgimento de leis que protejam os dados dos cidadãos, e que limitem a gestão das entidades públicas e privadas em relação as informações coletadas, transformando o sistema organizacionais, como compliance, em ferramentas de efetivação das normas éticas e legais. Assim, a implementação do programa alinhado com a governança corporativa é capaz de integralizar o corpo de normas internas com o intuito de adequar a legislação brasileira e criar uma cultura corporativa.

Dentro do programa de compliance, a administração em conjunto com a gestão da empresa, poderá implementar ao plano diretor, a utilização de software, sendo este capaz de possibilitar a

automatização do ciclo de vida útil dos dados para realizar o auxílio da tomada de decisão, com o intuito de mitigar os possíveis danos decorrentes da violação aos dispositivos da Lei Geral de Proteção de Dados Pessoais.

Nesse sentido, para realizar uma proteção extensiva aos direitos dos titulares dos dados, a LGPD integrou ao seu corpo de normas-condutas a serem adotadas pelos operadores do tratamento de dados, com escopo de preservar a integralidade, a qualidade e o sigilos dos dados, tendo como consequência da violação, a majoração de sanções pecuniárias.

Embora, o vazamento de dados ocorra de forma ordenada, a implementação de sistema de segurança nas corporações implica na diminuição de situações incidentais por erro humano, ou inadequação dos programas empresarias, assim, devendo a gestão ensejar esforços para que a proteção dos dados seja preservada, desde a concepção do serviço.

Para a efetivação da Lei Geral de Proteção de Dados Pessoais, as empresas devem realizar a adequação de medidas de boas práticas e governança em privacidade para mitigar os possíveis danos decorrente da violação aos dados em provedores privados. Mesmo que a proteção aos dados de forma concreta não seja possível, as adoções de mecanismo de segurança podem atenuar as sanções e as perdas aos titulares dos dados.

REFERÊNCIAS

BARATA, André Mantola. Governança de dados em organizações brasileira: uma avaliação comparativa entre os benefícios previstos na literatura e os obtidos pelas organizações. 2015. Dissertação (Mestrado em Sistema de Informação) - Universidade de São Paulo, São Paulo, 2015.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, [2022]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 15 abr. 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidente da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 abr. 2023.

BERTOCCELLI, Rodrigo de Pinho. Compliance. In: CARVALHO, André Castro et. al. Manual de compliance. Rio de Janeiro: Forense, 2019. p. 35.

CANDELORO, Ana Paula; RIZZO, Maria Balbina Martins De; PINHO, Vinícius (Coord). Compliance 360: riscos, estratégias, conflitos e vaidades no mundo corporativo. São Paulo: Trevisan, 2012.

CARVALHO, A. P. Proposta de um framework de compliance à Lei Geral de Proteção a Dados Pessoais (LGPD): um estudo de caso para prevenção a fraude no contexto de big data. 2021. Dissertação (Mestrado em Engenharia Elétrica) - Universidade de Brasília, Brasília, 2021.

CARVALHO, Andre Castro. Manual de compliance. 3. ed. Rio de Janeiro: Forense, 2021.

CASAES, Júlio César Costa. Governança de dados abertos governamentais: frameworks conceitual para as Universidades Federais, baseada em uma visão sistemática, 2019. Tese (Doutorado em Engenharia e Gestão do Conhecimento). Universidade Federal de Santa Catarina, Florinaóplis, 2019.

DATA GOVERNANCE INSTITUTE (DGI). Definitions of data governance. 2017. Disponível em: http://www.datagovernance.com/adg_data_governance_definition. Acesso em: 01 mai. 2023.

ENDEAVOR DO BRASIL. Prevenindo com o Compliance para não remediar com o caixa. In: ENDEAVOR. [S. l.], 26 abr. 2017. Disponível em: https://endeavor.org.br/pessoas/compliance/. Acesso em: 15 mar. 2023.

ESPÍNDOLA, P. L.; SALM JUNIOR, J. F.; ROSA, F.; JULIANI, J. P. Governança de dados aplicada à ciência da informação: análise de um sistema de dados científicos para a área da saúde. Revista Digital de Biblioteconomia & Ciência da Informação, Campinas, v. 16, n. 3, p. 274-298, 2018.

FERNANDES, Aguinaldo Aragon; DE ABREU, Vladimir Ferraz. Implantando a governança de TI: da estratégia à gestão de processos e serviços. 4. Ed. Rio de Janeiro: Brasport, 2014.

FRAZÃO, Ana. Programas de compliance e critérios de responsabilização de pessoas jurídicas por ilícitos administrativos. In: ROSSETTI, Maristela Abla; PITTA, Andre Grunspun. Governança corporativa: avanços e retrocessos. São Paulo: Quartier Latin, 2007. p. 42

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. A Lei Geral de proteção de Dados Pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

HONÓRIO, Roseli. Modelo conceitual de governança de dados como suporte à governança do conhecimento organizacional. 2022. Dissertação (Mestrado em Engenharia e Gestão do Conhecimento) - Universidade Federal de Santa Catarina, Florianópolis, 2022.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC). Guia das melhores práticas de governança para cooperativas. São Paulo, 2015. Disponível em http://www.ibgc.org.br/ userfiles/files/2014/files/CMPGPT.pdf

JOHNSON, Ralph E.; RUSSO, Vincent. Reusing object-oriented designs. Relatório Técnico da Universidade de Illinois, UIUCDCS 91-1696, 1991.

KLEINDIENST, Ana Cristina. Grandes temas do direito brasileiro: compliance. São Paulo: Almedina Brasil, 2019

KOEPSEL, Alice de Medeiros. Adoção e efeitos dos programas de compliance à luz da Lei Geral de Proteção de Dados Pessoais. 2020. Monografia (Graduação em Direito) -Universidade do Sul de Santa Catarina, Florianópolis, 2020.

LIMA, C., BASTOS, R. C. A criação de conhecimento apoiada pela governança de dados. *In*: CONGRESSO INTERNACIONAL DE CONHECIMENTO E INOVAÇÃO, 2019, Santa Catarina. Anais eletrônicos [...]. Santa Catarina Disponível em: https://proceeding.ciki.ufsc.br/index.php/ciki/article/view/647. Acesso em 10 Mar. 2023.

MARTIGNAGO, Deisi *et al.* Governança de dados aplicado no processo de catalogação. Revista Brasileira de Biblioteconomia e Documentação, São Paulo, V.15, n. 2, 2019.

MENDES, Gilmar Ferreira. Curso de direito constitucional. 2. ed. São Paulo: Saraiva, 2008.

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. São Paulo: Revista de Direito do Consumidor, 2018.

NASCIMENTO, Suellen Lima do. A lei Geral de Dados Pessoais e a Adoção dos Programas de compliance na sociedade da Informação. 2020. Monografia (Graduação em Direito) - Centro Universitário de Brasília, Brasília, 2020.

PESSOA, Larissa Rocha de Paula. Os desafios da Governança de dados e a realidade cultural brasileira. 2021. Dissertação (Mestrado em Direito) – Universidade Federal do Ceará, Fortaleza, 2021.

PINTO, S. C. C. S.. Composição em Web Frameworks, 2000. Tese (Doutorado em Informática) Pontifícia Universidade Católica do Rio de Janeiro, Rio Janeiro, 2000.

PROSSER, William L. Privacy. California Law Review. California, v. 48, n. 3. p. 383 – 423, agosto, 1960.

RÊGO, Bergson Lopes. Gestão e governança de dados: promovendo dados como ativo de valor nas empresas. 1. ed. Rio de Janeiro: Brasport, 2013,

ROQUE, Pamela Romeu. Estudos aplicados de direito empresarial: LL.C. em direito empresarial. São Paulo: Almedina, 2019.

SAAD, Carolina de Oliveira. A lei geral de proteção de dados pessoais e incidentes de segurança: regulação e prática de vazamento de dados, 2021. Monografia (Graduação em Direito). Fundação Getúlio Vargas. Rio de Janeiro, 2021.

SANTANA, Ricardo Cesar Gonçalves. Ciclo de vida dos dados e o papel da ciência da informação. *In*: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO. 14., 2013. Florianópolis. […]. Florianópolis: UFSC, 2013. Disponível em: http://enancib2013.ufsc.br/index.php/enancib2013/%20XIVenancib/paper/viewFile/284/319. Acesso em: 13 mar. 2023.

SILVA, Ana Laura Fonseca. O papel das Soft Skills na implementação efetiva dos programas de compliance com foco na adequação à Lei Geral de Proteção de Dados – Lei N° 13.709/18. 2022. Monografia (Graduação em Direito) - Universidade Federal de Ouro Preto, Ouro Preto. 2022

SILVA, Eggon João da. A defesa da ética e transparência. *In*: VENTURA, Luciano Carvalho. Governança corporativa. São Paulo: Saint Paul Editora, 2005, página 259.

TERRA, Priscila de Mello. A influência da governança de dados na gestão estratégica, 2017. Monografia (Bacharelado em Sistema de Informação) - Universidade Federal Fluminense, Niterói, 2017.

VAZAMENTO de dados aumentaram 493% no Brasil, segundo pesquisa do MIT.VEJA, São Paulo, 24 fev. 2021. Sociedade. Disponível em: https://vocesa.abril.com.br/sociedade/vazamentos-de-dados-aumentaram-493-no-brasil-segundo-pesquisa-do-mit. Acesso em: 15 mar. 2023.

VIEIRA, Tatiana Malta. O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante da tecnologia da informação. Porto Alegre: Sergio Antonio Fabris Editor, 2007.

Relatório do Software Anti-plágio CopySpider
Para mais detalhes sobre o CopySpider, acesse: https://copyspider.com.br

Instruções
Este relatório apresenta na próxima página uma tabela na qual cada linha associa o conteúdo do arquivo de entrada com um documento encontrado na internet (para "Busca em arquivos da internet") ou do arquivo de entrada com outro arquivo em seu computador (para "Pesquisa em arquivos locais"). A quantidade de termos comuns representa um fator utilizado no cálculo de Similaridade dos arquivos sendo comparados. Quanto maior a quantidade de termos comuns, maior a similaridade entre os arquivos. É importante destacar que o limite de 3% representa uma estatística de semelhança e não um "índice de plágio". Por exemplo, documentos que citam de forma direta (transcrição) outros documentos, podem ter uma similaridade maior do que 3% e ainda assim não podem ser caracterizados como plágio. Há sempre a necessidade do avaliador fazer uma análise para decidir se as semelhanças encontradas caracterizam ou não o problema de plágio ou mesmo de erro de formatação ou adequação às normas de referências bibliográficas. Para cada par de arquivos, apresenta-se uma comparação dos termos semelhantes, os quais aparecem em vermelho.
Veja também:
Analisando o resultado do CopySpider
Qual o percentual aceitável para ser considerado plágio?

Versão do CopySpider: 2.2.0
Relatório gerado por: wesvicentes@gmail.com
Modo: web / normal

Arquivos	Termos comuns	Similaridade
TCC - A IMPORTÂNCIA DO COMPLIANCE NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA - WESLEY VICENTE.pdf X https://www.euax.com.br/2021/04/implantacao-de-sistema	42	0,36
TCC - A IMPORTÂNCIA DO COMPLIANCE NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA - WESLEY VICENTE.pdf X https://www.upguard.com/blog/lgpd	19	0,16
TCC - A IMPORTÂNCIA DO COMPLIANCE NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA - WESLEY VICENTE.pdf X https://www.linguee.com.br/ingles-portugues/traducao/this+work+aims.html	15	0,13
TCC - A IMPORTÂNCIA DO COMPLIANCE NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA - WESLEY VICENTE.pdf X https://www.sciencedirect.com/science/article/pii/S0148296321003155	6	0,04
TCC - A IMPORTÂNCIA DO COMPLIANCE NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA - WESLEY VICENTE.pdf X https://textranch.com/376824/this-work-aims-to/or/this-work-is-aimed-to	4	0,03
TCC - A IMPORTÂNCIA DO COMPLIANCE NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA - WESLEY VICENTE.pdf X https://ludwig.guru/s/this+work+aims+to	2	0,02
TCC - A IMPORTÂNCIA DO COMPLIANCE NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA - WESLEY VICENTE.pdf X https://english.stackexchange.com/questions/314716/is-this-project-aims-to-logically-correct	2	0,01
TCC - A IMPORTÂNCIA DO COMPLIANCE NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA - WESLEY VICENTE.pdf X https://legaldictionary.net/mitigating-circumstances	0	0,00
TCC - A IMPORTÂNCIA DO COMPLIANCE NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA - WESLEY VICENTE.pdf X https://investorplace.com/stock-quotes/www-stock-quote	0	0,00
TCC - A IMPORTÂNCIA DO COMPLIANCE NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA - WESLEY VICENTE.pdf X https://www.questionsanswered.net/article/inspiring-quotes-history?utm_content=params%3Ao%3D740012%26ad%3DdirN%26qo%3DserpIndex&ueid=7071288f-9e02-4d51-a234-80c758412ac5	0	0,00
Arquivos com problema de download		

https://www.ibgc.org.br/conhecimento/governanca-corporativa	Não foi possível baixar o arquivo. É recomendável baixar o arquivo manualmente e realizar a análise em conluio (Um contra todos). - Erro: Parece que o documento não existe ou não pode ser acessado. HTTP response code: 403 - Server returned HTTP response code: 403 for URL: https://www.ibgc.org.br/conhecimento/governanca-corporativa

==========

Arquivo 1: TCC - A IMPORTÂNCIA DO COMPLIANCE NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA - WESLEY VICENTE.pdf (8805 termos)
Arquivo 2: https://www.euax.com.br/2021/04/implantacao-de-sistema (2716 termos)
Termos comuns: 42
Similaridade: 0,36%
O texto abaixo é o conteúdo do documento TCC - A IMPORTÂNCIA DO COMPLIANCE NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA - WESLEY VICENTE.pdf (8805 termos)
Os termos em vermelho foram encontrados no documento
https://www.euax.com.br/2021/04/implantacao-de-sistema (2716 termos)

==========

WESLEY VICENTE DA SILVA

A IMPORTÂNCIA DO COMPLIANCE EMPRESARIAL NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA

SALVADOR
2023

WESLEY VICENTE DA SILVA

A IMPORTÂNCIA DO COMPLIANCE EMPRESARIAL NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA

Artigo apresentado como requisito parcial para obtenção do título de Bacharel em Direito pela Universidade Católica do Salvador.

Orientador: Prof. Darlã Conceição Santos.

SALVADOR
2023

A IMPORTÂNCIA DO COMPLIANCE EMPRESARIAL NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA

Wesley Vicente da Silva1
Darlã Conceição Santos2

RESUMO: No cenário de exploração das informações como mercadoria econômica, os dados pessoais coletados por empresas privadas tornaram-se fator de tutela legislativa. Assim, surgiu a necessidade de organizar os setores privados para adequar aos moldes da Lei Geral de Proteção de Dados Pessoais ? LGPD, com o intuito de proteger a privacidade, como direito autônomo e fundamental para a tutela da pessoa humana, destacando os programas de compliance aliados as boas práticas e governança de dados. Nesse contexto, a fim de consolidar os mecanismos técnicos de segurança para a efetividade da legislação com a finalidade de mitigar os casos de vazamento de dados pessoais, a LGPD implementou medidas administrativas para inibir incidentes decorrentes das condutas infratoras a legislação. Desse modo, este trabalho tem como objetivo demonstrar a importância dos programas de compliance para a proteção aos direitos dos titulares dos dados, visando o cumprimento do ordenamento jurídico. Valendo-se do método hipotético-dedutivo, com abordagem qualitativa, utilizando da revisão bibliográfica de livros, legislação, artigos, dissertações e teses concernente à tutela de dados pessoais no Brasil para o desenvolvimento do presente artigo.

PALAVRAS-CHAVES: Compliance Empresarial. Governança corporativa. LGPD. Vazamento

de dados.

ABSTRACT: In the scenario of exploitation of information as an economic commodity, personal data collected by private companies have become a factor of legislative protection. Thus, the need arose to organize the private sectors to conform to the General Law for the Protection of Personal Data - LGPD, in order to protect privacy, as an autonomous and fundamental right for the protection of the human person, highlighting compliance programs allied with good practices and data governance. In this context, in order to consolidate the technical security mechanisms for the effectiveness of the legislation with the purpose of mitigating cases of leakage of personal data, the LGPD implemented administrative measures to inhibit incidents arising from conducts that violate the legislation. Thus, this work aims to demonstrate the importance of compliance programs to protect the rights of data subjects, aiming at compliance with the legal system. Taking advantage of the hypothetical-deductive method, with a qualitative approach, using the bibliographic review of books, legislation, articles, dissertations and theses concerning the protection of personal data in Brazil for the development of this article.

KEYWORDS: Corporate Compliance. Corporate governance. LGPD. Data leak.

1
Discente do curso de Direito da Universidade Católica do Salvador.
2
Mestre em Direito, Docente na Universidade Católica do Salvador.

1 INTRODUÇÃO

A nova moeda de troca não é apenas aquela que podemos ver, quantificar ou converter. Os moldes do mercado financeiro mudaram, sendo em questão material ou ao produto que eles precificam, postulando um novo aparato ao objeto contratual: os dados.
Muito embora, os dados pessoais, ainda para muitos, são apenas informações deslocadas acerca de fatores específicos, atualmente, podem ser conceituados como um conjunto de indicadores, regrados por um complexo condensado de informações em um fluxo crescente tangencial.
Os dados da grande massa acabam gerando indicadores que podem ser balizados e influenciados de acordo com os detentores dessa informação, apenas apartado em blocos de informações não são considerados como vetores orçamentários. Porém, direcionados para uma finalidade ordenada tem o condão de influenciar o interesse social.
Dito isso, os mecanismos postos pelo Reino Unido para possibilitar uma estruturação normativa para organizar e gerir os dados dos indivíduos, foi crucial para a criação em outros países, como no Brasil, onde instituiu-se a Lei Geral de Proteção de Dados Pessoais (LGPD). Muito

embora, a lei brasileira trouxe um arcabouço de normas reguladoras e sanções aos casos de tratamento de dados, que não foram abarcados com o marco da internet, os dados em uma visão macro constitucional já eram de forma genérica tutelados pela Constituição Federal de 1988.
Todavia, apenas a sanção da LGPD não seria, isoladamente, capaz de coibir as violações ao tratamento de dados na esfera privada, mas sim a necessidade de uma regulamentação do ciclo de vida das informações, que além de estipular os dados que podem ser utilizados ou até quando podem ser armazenados, estabelecer expressamente no bojo da norma como deve ser a proteção na operação do tratamento de dados.
De forma efêmera, conclui-se que a legislação pode delimitar os alicerces capazes de ensejar uma fiscalização, sendo estas através de mecanismo de gerenciamento de atividades, políticas de condutas e implementação de governança de dados, pois os dados hackeados ou vazados de forma isoladas, não seria possível identificar dados sensíveis, muitos menos individualizar o sujeito.
Portanto, o gerenciamento dos dados em provedores de armazenamento pode ter os riscos reduzidos de acordo com a realização de medidas de compliance para dirimir os impactos na

atividade empresarial, como também para tutelar os dados, cada vez mais acentuado como um produto orçamentário.

2 COMPLIANCE EMPRESARIAL

A criação do compliance está entrelaçado sob o cenário econômico-social, assim, sua implementação como sistema de organização foi instaurado e aprimorado a partir dos problemas práticos estruturais para gerir uma boa governança, com intuito de assegurar a proteção e o controle que garante a qualidade do negócio.
A utilização do termo foi inicializada no mercado financeiro, especialmente após a criação do Banco Central em 1913 nos Estados Unidos da América, com a necessidade de um sistema econômico ajustável e estável. Só após 1960, com a regularização da Securities and Exchange Commission (SEC), que houve a necessidade de implementação do compliance como um programa para a integração dos procedimento, controle e monitoramento de operação interna. (CARVALHO, 2021)
Em 1977, com a Convenção Relativa à Obrigação de Diligência dos Bancos Suíços, estabeleceu os modelos auto regulatórios, com adequação de condutas e processos internos, na qual a infração tem como consequência à aplicação de sanções. (CARVALHO, 2021)
Só após esse processo de amadurecimento histórico, que o Brasil teve a necessidade de competir em escala global, implementado novos processos de segurança no sistema financeiro brasileiro.
Pode-se concluir que, após a globalização com o fenômeno da criação dos dados estruturais, houve a potencialização das informações adquiridas por meio de provedores, classificadas, atualmente, como fonte econômica de um produto quantificativo e qualitativo, ao qual possibilita uma utilização como um produto do sistema financeiro.
Nesse sentido, em decorrência de ataques cibernéticos em provedores de informações

massificadas conduziram a sociedade na aplicação de institutos de melhoramento, como o compliance e suas interfaces para proteger no ambiente corporativo os dados massificados recebidos em seus provedores.

2.1 O CONCEITO DE COMPLIANCE

Antes de enveredar sob o conceito de compliance na esfera privada, é oportuno compreender o seu significado. Nesse contexto, a palavra compliance advém do verbo inglês, to comply, que pode ser definida como conformidade. O instituto deve ser aplicado como plano principal de uma diretriz pré-estabelecida para ser dirigida a todos capazes de enfrentar a finalidade destinada. (BERTOCCELLI, 2019)
Nesse parâmetro, pode ser traduzida como:

Comply, em inglês, significa ?agir em sintonia com as regras?, o que já explica um pouquinho do termo. Compliance, em termos didáticos, significa estar absolutamente em linha com normas, controles internos e externos, além de todas as políticas e diretrizes estabelecidas para o seu negócio. (ENDEAVOR DO BRASIL, 2022, n.p)

O compliance pode-se ser definido de forma técnica como um conjunto de normas padronizadas, sob um viés ético e legal, na qual após estruturação será a matriz orientadora para o comportamento organizacional da instituição ao qual atuará no mercado, como também irá reger as atividades dos colaboradores. Dessa forma, sendo um instrumento hábil a controlar o risco de imagem, a normatização legal, chamados de riscos de compliance, as que recaem nas instituições no decorrer da sua atividade laboral. (CANDELORO, 2012).
Superada a barreira terminológica, a finalidade do compliance tem como escopo o gerenciamento adequado do risco de atividades, verificar adequadamente as normas éticas e legais, e estudar os possíveis danos tangenciais. Dessa forma, esses elementos visam a redução de perdas e danos, como também amplifica a cultura e fortalecimento corporativo nos moldes aos padrões exigidos, seja esse por lei ou na tentativa de dirimir o risco do serviço prestado.
Portanto, segundo a doutrinadora Frazão (2007, p. 42), destina-se em sua obra que o compliance é como:
(...) conjunto de ações a serem adotadas no ambiente corporativo para que se reforce anuência da empresa à legislação vigente, de modo a prevenir a ocorrência de infrações ou, já tendo ocorrido o ilícito, propiciar o imediato retorno ao contexto de normalidade e legalidade.

Nessa mesma linha de pensamento, de acordo com os autores da obra Compliance 360° (2012, n.p), referem-se o compliance a:

Um conjunto de regras, padrões, procedimentos éticos e legais que, uma vez definido e

implantado, será a linha mestra que orientará o comportamento da instituição no mercado em que atua, bem como as atitudes de seus funcionários; um instrumento capaz de controlar o risco de imagem e o risco legal, os chamados ?riscos de compliance?, a que se sujeitam as instituições no curso de suas atividades.

Pode-se concluir que o conceito de compliance, em uma esfera macro, é um aglomerado de regras pré-estabelecidas através de um instrumento perpetuado por técnica de desenvolvimento, capaz de dirimir riscos e danos das atividades devolvidas pelo plano diretor.
Muito embora, o instituto "compliance" tem uma definição extensiva e não tem como fim apenas o cumprimento da legislação e de condutas éticas, pode ser compreendida também como um instrumento de diminuição de riscos, desenvolvimento corporativo sustentável e subsequentes segmentos empresariais de negócio. (ROQUE, 2019)
O compliance além de estar associado tradicionalmente a uma perspectiva organizacional aos comandos administrativos, pode ser vinculada também a uma visão de uma sociedade digital 4.0, devendo não só apresentar o compliance empresarial na esfera de redução de risco à imagem, mas sim, em uma abordagem de pré-orientação e implementação de desenvolvimento aos moldes legislativo de proteção aos dados, como objeto principal de estudos.
Portanto, é necessário a elaboração do projeto de compliance em uma visão lógica, a modo de compreender os objetivos e os componentes da aplicação do programa. Posteriormente, superado os obstáculos, aplica-se os estudos de riscos a boa governança corporativa com a implementação de programas de governança de dados objetivando auxiliar o controle de informações em conformidade aos padrões da corporação, e mitigar os danos da empresa.

2.1.1 AS GOVERNANÇAS CORPORATIVAS E A IMPLEMENTAÇÃO DOS PROGRAMAS DE COMPLIANCE

Em linhas gerais, o Instituto Brasileiro de Governança Corporativa ? IBGC (2015, n.p) discrimina o conceito de Governança Corporativa, como: ?Sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas. ?
O sistema da governança corporativa está associado ao desenvolvimento interno de uma empresa, seja ele entre a administração, sócios e funcionários, capaz de criar elos para uma estruturação de direção racional e acima de tudo nos moldes da ética e legislação.
Muito embora, a governança corporativa e o compliance sejam institutos que se assemelham em uma visão macro, os mesmos, diferenciam na aplicação prática, mas se complementam no objetivo final, sendo um instrumento para aplicação do outro.

A prática da governança corporativa, além de estimular o valor empresarial, pode-se concluir que estrutura de forma adequada a medida necessária para organizar a atividade empresarial, assim, não há que se falar em condutas prejudiciais. Por exemplo: empresários compreendem que para realizar uma instrumentalização segura aos seus sócios e administradores tendem a prejudicar o negócio empresarial, assim o autor Eggon João da Silva (2005, p.259) retrata que: ?A governança corporativa assegura tratamento equânime a todos os acionistas, inclusive minoritários, preferencialistas, nacionais e estrangeiros. Todos devem ter oportunidade de reparação caso venham a sofrer violação de seus diretores. ?

Nesse passo, as críticas ao sistema não são viáveis, tendo em vista a utilização de instrumento capaz de integralizar ao plano empresarial. Sendo assim, o programa de compliance visa amplificar a utilização de um sistema para garantir que todos possam participar de forma justa sob o aspecto legal, seja sócio ou administrador.

Em uma tangente geral, a implementação da governança corporativa ressoa em uma perspectiva segura, tanto internamente, seja auxiliando as avaliações das atividades executadas pelos sócios/administradores, quanto externamente, em relação à imagem da empresa, sendo este um fator primordial a empresas estruturadas no mercado.

A implementação da governança corporativa deve ser estruturada de acordo com as necessidades da empresa, devendo verificar o histórico de desenvolvimento do estabelecimento, pois, só a partir do status da empresa pode-se delimitar a estratégia possível para uma implementação segura e adequada. Sendo assim, um regramento mais rigoroso pode gerar consequências negativas e ineficazes, especificamente em estágios primários, pois em atividades inicias, as tomadas de decisões e a execução da atividade empresarial é primordial, sendo necessário, um aspecto negocial informal para realizar os objetivos da empresa, o que não se verifica quando existe prática de boa governança devidamente estruturadas no negócio. (KLEINDIENST, 2019)

Ao desenvolver da atividade da empresa, além da atenção a organização interna, sendo está um fator primordial da governança, ainda que no fim acabe tendo um aspecto externo por vislumbrar no mercado financeiro uma maior complexidade da entidade. O desenvolvimento da empresa, seja no faturamento, importação comercial, quantidade de funcionários, além dos controles a observância da legislação e regras internas, tendem à serem complexos, e, que necessita

de ações maiores que a própria instituição empresarial, restando necessária a implementação de sistema organizacionais aos fluxos de informações. (KLEINDIENST, 2019)

Ultrapassado a esfera conceitual e instrumentalização da política de boas práticas de governança, cabe pontuar que as empresas que possuem fluxos de informações sensíveis, conforme estipula o artigo 50 da Lei Geral de Proteção de Dados Pessoais, os controladores e operadores são responsáveis pelo tratamento de dados, devendo criar planos de adequação a legislação.

Assim, ao confeccionar as regras de boas práticas, os controladores adjuntos com a administração devem estipular através da análise da natureza dos dados coletados, a probabilidade, a finalidade e o potencial de riscos das vantagens advindas dos tratamentos dos dados verificados. (NASCIMENTO, 2020)

É necessário pontuar que, os agentes de tratamento, após a autenticação da gravidade e sensibilidade dos dados aos riscos de operação, poderão estabelecer programa de governança em privacidade, sendo este, um instrumento amplo com normas de compliance, além dos aspectos operacionais.
Em relação ao programa de governança de privacidade, pode-se estabelecer como um aglomerado de normas-regras de boas práticas de governança, com a finalidade de executar ordens de natureza legal. (NASCIMENTO, 2020)
Portanto, os instrumentos do compliance em conjunto com a boa prática de governança, se consagram na identificação dos riscos e estruturação de medidas para a empresa, sendo respondida de forma adequada e proporcional ao suporte da tomada de decisão.
O Programa de compliance na esfera privada para análise de dados pessoais, com a finalidade de promover a segurança, deve ser constantemente monitorado e atualizado, com a implementação de ?salva vidas? em decorrência de avaliação de riscos à privacidade e o acometimento de vazamentos. (NASCIMENTO, 2020)
Portanto, os instrumentos e objetos referenciados demonstram a determinação de regras de governança no ambiente de operação de tratamento de dados pessoais, a modo que seja realizado uma estruturação nas empresas para que possibilitem a implementação de mecanismos de segurança, com a finalidade de dirimir os riscos da atividade empresarial na sociedade digital.

3 GOVERNANÇA DE DADOS

O mercado digital tem como principal ativo financeiro os dados, este considerado como ?matéria prima? de uma economia baseada no conjunto de informações, sendo que nos últimos anos, houve um aumento exponencial na coleta de dados por cooperativas, startups e novos nichos empresariais, tendo a finalidade de quantificar e gerencias os dados.
Dados, informações, conhecimento e sabedoria são os quatros estágios evolutivos da cadeia de informação, pode-se assim, compreender os dados como fatos ou registros em seu formato primário. (BEAL, 2014). Já a informação é entendida como os conjuntos processados de dados em um contexto aplicado (RÊGO, 2013). Muito embora, na sociedade da informação ?os dados são o novo petróleo?, apenas os dados isoladamente não são capazes de transformar em ativo financeiro, sendo necessário administrá-lo de forma eficaz, para que assim, as empresas adquiram vantagem competitiva.
Dessa forma, a governança de dados tem como principal objetivo atender as necessidades das empresas, ou seja, solucionar problemas, diminuir custos da administração, para que os dados transformem em saldo positivo para os negócios (TERRA, 2017).
O Data Governance Institute -DGI (2017, n.p) definiu governança de dados como ?um sistema de direitos de decisão e responsabilidades para processos relacionados à informação, executado de acordo com modelos acordados que descrevem quem pode realizar quais ações com quais informações e quando. ? Portanto, a utilização da governança de dados orienta quais os métodos deverão ser aplicados no ciclo de vida dos dados.

Uma das atribuições da governança é o acompanhamento da operação dos dados com a finalidade de gerir que as informações estejam alinhadas com os objetivos pré-determinados na coleta primária, além disso, é necessário assegurar que as informações estejam disponíveis para acesso, quando consultadas, gozar de qualidade, consistência, auditabilidade e segurança dos dados (ESPÍNDOLA, 2018).

No âmago da cadeia evolutiva da informação uma das preocupações dentro das organizações corporativas é o receio com a proteção das informações, ou seja, a capacidade das empresas no protagonismo da segurança com os provedores internos, tendo em vista a necessidade de conformidade com a legislação pátria.

A boa governança tem como objetivo aplicável à prática do controle dos processos de operação dos dados: a prevenção de situações adversas que podem gerar o comprometimento da integralidade dos dados adquiridos pelas organizações empresariais, que por sua vez, devem ter o condão de reforçar a confidencialidade das informações. (ESPÍNDOLA, 2018).

A integração do programa de governança de dados nas corporativas empresariais, tem como o esforço principal a organização de dados, que deve ser observado por um prisma basilar, ou seja, a aplicação dos princípios como limite legal e ético no ciclo de vida dos dados.

Para Rêgo (2013), os princípios são regulamentações para compreender aplicação da governança dos dados como linha direta para os negócios, sendo: (i) A gestão de dados estratégicos, tem o dever de vislumbrar as tomadas decisões por um coeficiente tático e operacional. (ii) A governança como instituição, ou seja, a governança de dados pode ser comparada como sistema governamental, na qual dispõe de legislação, execução e jurisdição; (iii) A governança de dados como um programa, devendo ser implementado como fator permanente, não apenas um projeto temporário. Ainda, pontua-se que os princípios da Governança de dados não são limitados, tendo uma orientação basilar a cada implementação de um sistema organizacional que deve ser observado pelo prisma ético e legal.

Assim, os princípios devem incumbir os papéis que a serem preenchidos pela gestão moldar os comportamentos das empresas para a aquisição, reserva e utilização dos dados conforme as normas e políticas da corporação (TERRA, 2017).

Coleta, armazenamento, recuperação e descartes, são as quatro etapas do ciclo de vida dos dados (SANTANA, 2013), ou seja, para a aquisição de dados pelas empresas, deverão observar a vida útil do dado para não incorrer na (in) responsabilidade da utilização indevida de informações dos seus provedores.

As fases do ciclo de vida dos dados devem ser observadas pela ótica de seis objetivos, sendo eles: a qualidade, a privacidade, os direitos autorais, a integração, compartilhamento e preservação dos dados (ESPÍNDOLA, 2018). Muito embora, a lei geral de proteção de dados implementou e traçou novos objetivos para a coleta de dados pessoais, cabe destacar que os objetivos vislumbrados na Governança de dados têm como parâmetro preliminar a tomada de decisão, na qual deve ser os negócios pautados nos moldes legais e éticos vigentes.

Nesse contexto, o controle de informações é necessário, tendo em vista que na sociedade da informação, cada vez mais o volume de dados é crescente, acarretando mais vazão e protesto

por políticas públicas para a preservação dos institutos, órgãos e empresas que detenham a

informação, sendo assim, necessário sistema de organização, softwares e hardwares capazes de processar as informações, criptografar e armazenar. (MARTIGNAGO, 2019)
Assim, para otimizar o ciclo de vida dos dados e garantir que os objetivos sejam preenchidos na estruturação do gerenciamento de dados, faz-se necessário a implementação de frameworks com o intuito de garantir que o procedimento seja cumprido com maior qualidade de informação e aproveitamento financeiro para a empresa, auxiliando a tomada de decisão para redução de risco para utilização de dados. (MARTIGNAGO, 2019)
Um Framework, segundo Johnson (1991), pode ser definida como um aglomerado de objetos que colabora entre si para que atinja um conjunto de obrigações para aplicação de um domínio especifico. Já para Pinto (2000), um framework é conceituado como um software incompleto criado para ser um objeto cujo estado e comportamento são definidos pela classe. Assim, o framework é uma concepção de uma arquitetura para um edifício de subsistemas e oferece o alicerce básico para criá-los.
Muito embora, os autores defendem uma conceituação distintas acerca da concepção de frameworks, pode-se verificar que ambas se complementam, tendo em vista que o framework é um sistema pré moldado, ou seja, é um programa com intuito de ser complementado através da finalidade a ser cumprida pela gestão empresarial, sendo instanciado por classes para categorizar os dados e ser alojado em hotspot, provedores físicos, capazes de armazenar as informações coletadas pelas empresas.
Portanto, para gerenciar os ativos de dados de forma complexa, ordenada e objetiva é necessário para proteção do procedimento do ciclo de vida dos dados, determinar os modelos de frameworks para o gerenciamento dos dados. Assim, para Carvalho (2021), podem ser apresentados três domínios CobiT, DAMA DMBOK e DGI Framework, sendo apenas dois destes observados para fomento deste artigo: (i) A DAMA (DAMA DMBOK), e (ii) CobiT.
A DAMA (Data Management Association) é uma associação sem fins lucrativos, com o intuito de promover boas práticas de gestão de dados, e em 2009 fundou o DAMA-DMBoK (Data Management Body of Knowledge), sendo um corpo de conhecimento que tem como ponto fundamental esclarecer como as corporativas devem aplicar a operação otimizada dos dados. (CARVALHO, 2021)
Em sua versão 2.0, acrescenta não só uma visão macro do gerenciamento de dados, definindo padrões, terminologias e práticas, mas a integração de dados, para definir táticas,

armazenamentos e sistemas, bem como implementação da ética na operação do tratamento de dados, a definição de big data e ciência de dados e amadurecimento das informações. (LIMA, 2019).
O DAMA-DMBOK V2 é formado por 11 (onze) funções de gestão de organização de

dados, sendo incorporado como cerne principal: a governança de dados, tendo em vista que os dados percorrem por toda sistemática das onzes funções ordenadas, assim segundo Honório (2021):
A primeira função é a governa de dados, sendo o pilar do framework, tem o condão de orientar e supervisionar a operação do ciclo de vida dos dados, na qual deve estabelecer um sistema de apoio a decisão dos gestores sobre os dados, sob o prisma do negócio.
A arquitetura de dados, a segunda função, pode ser conceituada como um planejamento para administrar os dados, aquisição de ativos da empresa, com o intuito de definir a finalidade das informações adquiridas com os requisitos necessário para o gerenciamento dos dados.
Por sua vez, a modelagem de dados e design, tem a função de demonstrar de forma nítida os dados, sendo o processo da descoberta, análise e representação da etapa primária da informação.
O armazenamento, uma das etapas da operação do ciclo de vida dos dados, na qual vai incluir o design, o suporte dos dados armazenados para quantificar o coeficiente valorativo das informações, até o seu descarte, devendo respeitar todo o procedimento de segurança legal vigente.
Um dos alicerces para o gerenciamento de informação é a segurança, que deve garantir a proteção dos dados, a execução de políticas e procedimento de segurança, no intuito de moderar o acesso de forma consciente e controlado, não devendo ser infringido ou acessado de forma inadequada, afim de garantir autenticação e auditoria de dados informações.
A Integração e Interoperabilidade de dados, é a função responsável pela movimentação e a concretização dos dados na interligação do armazenamento e outras plataformas.
O gerenciamento de documentos, pode ser compreendida como o gerenciamento e inclusão da vida útil dos dados e informações, encontrados em programas não estruturados, em ênfase ao conteúdo de apoio de conformidade a legislação vigente e os termos éticos formalizados para o negócio.
Dados mestre e de referência, tem como condão a manutenção dos dados compartilhados para coexistir a integralidade dos sistemas internos de gerenciamento dos dados.
Em razão da interligação entre uma linha direta com os negócios, uma das funções do DAMA-DMBOK é a Data warehousing e Business intelligence, ou seja, a implementação de

planner para o contoler da administração dos dados e suporte a decisão com o intuito de conceder aos gestores de informação emitam relatórios de equalização de valores.
Segundo Barata (2015), os metadados, na qual consiste a décima função, é promover a facilitação do acesso dos dados interligados nas multifontes do sistema integrado, como também garantir a qualidade de dados.
Por fim, o gerenciamento de qualidade de dados é a implicação das técnicas para garantir a possibilidade de aferição, melhoramento e adequação da utilidade dos dados, com o intuito de monitorar a integridade da informação primária no ciclo de vida dos dados.
Já o COBIT (Control Objectives for Information and related Technology), é um framework de suporte fundado em 1994 administrado pela ISACA (Information Systems Audit and Control Association), estruturado como um arcabouço de informação direcionadas para governança de dados e gerenciamento de informação, tem como objetivo auxiliar os profissionais de gestão na conexão entre os problemas técnicos e os riscos do negócio. (BARATA, 2015).

Para Lima (2019), o COBIT é um framework que possui duas vertentes basilares: a gestão, que possui quatro áreas de domínios: planejamento, constituição, execução e monitoramento, e a governança que é a tomada de decisão de acordo com a gestão de dados, possuindo 37 (trinte e sete) processos integrados.
Na versão 5.0, o sistema é utilizado baseado em 05 princípio, conforme elucida Casaes (2019), Barata (2015) e Lima (2019), sendo: (i) atender às necessidades das partes interessadas; (ii) cobrir o negócio como um todo; (iii) aplicar um framework único e integrado; (iv) habilitar uma visão holística; e (v) distinção entre governança de gestão.
Um dos princípios é atender às necessidades das partes interessadas, sendo a necessidade das corporativas é satisfazer as expectativas dos seus stakeholders, proporcionando um equilíbrio na tripartite: benefícios, redução do risco e recurso disponíveis.
O segundo princípio é baseado na cobertura do negócio como um todo, ou seja, abranger a integralidade da empresa no processo, procedimento, pessoas e as relações com os habilitadores.
A aplicação do framework único e integrado, assim, o COBIT é capaz de promover uma relação completa com a Governança de dados, corroborando ao alinhamento com padrões externos e adaptabilidade dos modelos usuais de negócios.

O COBIT permite habilitar uma visão holística, ou seja, uma visão macro dos componentes que oferecem suporte para atingir as finalidades da governança de dados, na qual define como catalogadores: as políticas, processos, estruturas organizacionais, informação e ética.
Por derradeiro, o princípio da distinção entre governança de gestão, tendo em vista que ambos possuem estruturas organizacionais distintas, assim, governança tem como esforço principal que os objetivos corporativos sejam cumpridos, estabelecendo prioridades pela tomada de decisão, compliance e progresso das organizações. Por sua vez, a gestão é o planejamento, construção, execução e monitoramento das funções ornamentada com o direcionamento da governança.
Desse modo, com escalonamento dos cinco princípios é capaz de proporcionar o funcionamento otimizado do framework, destacando os seguintes processos:
O APO01: Gerenciar o framework de TI, tem como condição a otimização das atividades relacionadas ao TI, com a função principal de incluir os procedimentos e regulamentos para promover a integralidade das informações nos bancos de dados. (BARATA, 2015)
Já o APO03: Gerenciar a arquitetura corporativa, tem função primordial agrupar as informações para auxiliar as atividades e tomadas de decisões, conceituando e compartilhando as informações dos elementos dos dados, e por fim catalogar a empresa, com base na modulação e sensibilidade dos dados. (BARATA, 2015)
Nesse ínterim, a governança de dados como um sistema integrado com o programa de compliance, tem o condão de otimizar a operação de controle interno relacionado aos dados coletados pelas empresas, capaz de gerenciar as bases para o apoio de decisão ao tratamento das informações, com segurança e qualidade, garantido o ciclo da vida útil dos dados.

4 A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

As estruturas políticas, econômicas e sociais com desenvolvimento de novas tecnologias e mecanismo para a coleta de dados e informações, fez necessário modulações legislativas para a proteção da privacidade, além dos aspectos físicos, patrimoniais e morais.
A proteção à privacidade de dados foi dividida em quatros gerações: a primeira, oriunda do estado moderno, com o advento dos bancos de dados; a segunda, datada em 1980, com a expansão legislativa para a proteção à privacidade aos setores privados; a terceira geração em 1990, com o processo de tratamento de dados e o consentimento dos cidadãos; Por fim, a última dimensão, é

destinada ao protagonismo da permissão para coleta e uso dos dados pessoais, quando a lei estabeleceu a importância da titularidade das informações. (MENDES, 2014)
Nesse aspecto, é perceptível a evolução do direito aos fatores reais da sociedade e as transformações dos meios tecnológico, computacionais, genéticos e comunicativos, que por sua vez possibilitou a integração da comunicação global, e consequentemente, o rastreio dos dados através do armazenamento de informação. (SAAD, 2021).
Os legisladores ao considerar os dados pessoais como extensão ao direito à privacidade, preocuparam em tutelar constitucionalmente a proteção da população, em especial os países europeus, como: Espanha, Portugal, Hungria, Eslovênia e Rússia. (VIEIRA, 2007) Porém, só tornou-se fator primordial após o regulamento geral do Parlamento Europeu sobre a proteção de dados, n.º 2016/679, sendo necessário a adequação das empresas prestadoras de serviço na Europa ao regulamento, influenciado diretamente o Brasil para elaboração da Lei Geral de Proteção de Dados brasileira. (SAAD, 2021).
Muito embora, a Lei Geral de Proteção de Dados Pessoais - LGPD, em sua promulgação, não abarcou de forma expressa a proteção de dados como direito fundamental, a doutrina, em especial Nascimento (2020), por sua vez, já argumentava a proteção de dados e informações pessoais como direito autônomo, derivado do direito fundamental à privacidade, explicitamente no artigo 5°, X, da CRFB de 1988.
Após reiterados julgamento sobre a tutela dos dados pessoais como extensão da personalidade do indivíduo, o Supremo Tribunal Federal -STF reconheceu no Julgamento da Ação Direta de Inconstitucionalidade - ADI 6387, a existência dos dados como direito autônomo, derivada do direito fundamental a dignidade da pessoa humana, na proteção à intimidade e a centralidade do Habeas Data como autodeterminação informativa. (NASCIMENTO, 2020).
Ao compreender a necessidade da proteção aos dados pessoais, os legisladores brasileiros em votação de ? das casas legislativas (câmara e Senado Federal) em dois turnos, aprovaram a Emenda Constitucional 115 de fevereiro de 2022, alterando o artigo 5° da Constituição Federal de 1988, incluindo o inciso LXXIX, tutelando constitucionalmente a proteção aos dados pessoais, inclusive nos meios digitais.
Ressalta-se, ainda, que os dados pessoais estão interligados com o direto fundamental à privacidade, na qual representa a capacidade de a pessoa administrar sua vida, seus pertences e

propriedades materiais e imateriais, permitindo ou não a utilização dos seus dados (bens imateriais) por terceiro. (NASCIMENTO, 2020).

A privacidade, por sua vez, segundo Mendes (2008), é o direito à proteção aos comportamentos pessoais e acontecimentos de caráter íntimo, bem como as informações prestadas aos profissionais e comerciantes, em que a pessoa não deseja que se compartilhe com o público.

Para o professor William Prosser, pode-se qualificar a lesão a privacidade em quatro graus: i) o intrometimento na reclusão ou solidão na vida privada, ii) a divulgação pública de fatos privados constrangedores sobre o indivíduo; iii) a publicidade sobre o indivíduo apresentada de forma equivocada; e iv) a apropriação, para obtenção de vantagem, do nome ou da imagem do demandante (PROSSER, 1960).

A doutrina, por sua vez, defende mais uma violação à privacidade: a privacidade informacional, interligada com os fatores tecnológicos de informação. (SAAD, 2021). Assim, quando a lei ao realizar o tratamento da privacidade, refere-se como um direito líquido, ao qual será tutelado para garantir que o indivíduo tenha um local reservado, que não tenha, se desejar, a interferência de outros sujeitos, seja pessoa física ou jurídica.

Com a proteção dos dados pessoais dos titulares, através da LGPD, possibilitou ao cidadão o acesso a informações ao ciclo de vida útil dos dados pelas empresas, e a certeza de fiscalização pela Autoridade Nacional de Proteção de Dados, com a finalidade de atingir os objetivos traçados pela legislação, na qual a lei traz conceitos e delimita princípios, que devem ser mencionados.

A LGPD tem como objetivo principal: ?o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado?, com a destinação de assegurar os direitos fundamentais a liberdade e privacidade dos titulares dos dados, bem como tutelar a dignidade e a personalidade da pessoa natural. (LGPD).

A legislação está ordenada diretamente com o meio empresarial, sobretudo no que se refere aplicação aos seus destinatários que são pessoas físicas ou jurídicas que realizam a coleta e tratamento de dados no Brasil, conforme preceitua o artigo 1° da lei 13.709, de 14 de agosto de 2018.

Para compreender a LGPD, faz-se necessário elucidar os conceitos de dados pessoais: (art. 5º, I) é toda informação relacionada a pessoa natural, identificada ou identificável, sendo o dado aplicado no contexto que possibilite o reconhecimento do indivíduo. Bem como refere-se aos dados sensíveis (art. 5º, II), são todas as informações que se relaciona com pensamentos políticos, crenças, identidade biológica e física. Portanto, a legislação tem como ponto a proteção e o cuidado para a não violação dos dados pessoais e sensíveis.

Os doutrinadores, Laura Schertel e Danilo Doneda, ainda aponta cinco pilares para compreender a LGPD, sendo: i) a unidade e generalidade da aplicação da Lei; ii) a legitimação para o tratamento de dados (hipóteses autorizativas); iii) os princípios e direitos do titular; iv) as obrigações dos agentes de tratamento de dados e v) a responsabilização dos agentes.

O primeiro pilar é considerado com aplicabilidade material da legislação, ou seja, aplica-se a qualquer operação realizada por pessoa natural ou jurídica de direito público ou privado,

independentemente do meio, da sua sede ou do país onde estejam localizados os dados (Art. 3°). Considerado, assim, como uma aplicação uniforme para todos os setores público ou privados que realizam tratamento de dados.

O segundo pilar é a legitimação para o tratamento de dados, tendo em vista que a lei especificou critérios e requisitos para o reconhecimento da legitimidade, não podendo ser tratados os dados, sem que exista uma base normativa que autorize, prevista no artigo 7°, 11° ou 23° da LGPD, abordando 11 (onze) hipóteses, incluído o consentimento ou a previsão legislativa.

Destaca-se que a autorização por consentimento para ser considerado válido, deve observar os requisitos previsto no artigo 5°, XII, sendo considerado que a vontade deve ser livre, informada, inequívoca e com a finalidade determinada, consagrando os princípios norteadores da legislação.

O terceiro pilar é o conjunto de princípios e direitos que assegura o destinatário da lei a controlar a utilização do seu dado pessoal, sendo importante elencar dez princípios que estruturam a LGPD: a finalidade, a adequação, a necessidade, o livre acesso, a qualidade dos dados, a transparência, a segurança, a prevenção, a não discriminação e a responsabilização. (MENDES, DONEDA, 2018)

No que concerne, aos direitos dos titulares são expressos no artigo 18° da referida lei, que permite o titular dos dados adquirir através do controler, independentemente do momento, as informações relacionadas ao indivíduo, prevendo: acesso, confirmação, correção, anonimização, bloqueou ou eliminação e a portabilidade.

Para adentrar no cerne dos problemas enfrentados pela legislação, em especial, sobre o vazamento de dados, os dois últimos pilares serão abordados sob a perspectiva da violação e responsabilização acerca da proteção de dados nos casos incidentes de vazamento.

Assim, o quarto pilar, destina-se às obrigações dos agentes de tratamento dos dados, na qual estabeleceu limites que devem ser observados nas operações realizadas para reforçar a segurança e prevenir os problemas da atividade no tratamento de dados.

Uma das obrigações fundamentais, consiste na intitulação do encarregado pelo tratamento dos dados indicados pelo controlador, conforme artigo 41 da LGPD, que possui a função de aceitar as reclamações e comunicações dos sujeitos dos dados, receber informações da Autoridade Nacional, como deve orientar os funcionários a respeito das práticas a serem adotadas em relação à proteção de dados pessoais.

Assim, as informações devem ser fornecidas ao proprietário dos dados, quando os dados forem coletados, como: os meios de segurança aderidos ao tratamento de dados, quais são os riscos da atividade que podem gerar lesão ao titular, pois pode gerar a mitigação dos prejuízos. (SAAD, 2021)

A lei Geral de Proteção de Dados Pessoais tem como objetivo a proteção do dados pessoais dos titulares dos dados, sendo assim, uma das obrigações principais é adoção de medidas de segurança, técnicas e administrativas hábeis a proteger os dados pessoais de acessos não autorizados, como promover a integralidade dos dados, não permitindo, assim, a alteração das informações, a prevenção de situações ilícitas ou acidentais, ou qualquer forma de tratamento inadequado, consoante se desprende do artigo 46 da lei.

Tornou-se corriqueiro manchetes acerca do vazamento de dados por corporativas, uma das violações mais graves incidentes abarcados pela LGPD, o que ocasiona a vulnerabilidade do titular dos dados, e dos sistemas internos que são responsáveis pelo ciclo de vida útil dos dados. (SAAD,2021)

A seção de segurança de informação tem como condão as obrigações inerentes aos agentes de tratamento, devendo ser adotado pela integralidade das pessoas que realizam o tratamento de dados, garantido que os dados sejam confidenciais, bem como disponíveis nas operações de tratamento. (Art.48). Nos casos incidentais de vazamento de dados, insurge a necessidade ao controlador de informar a autoridade de proteção de dados, que podem definir as medidas para mitigação dos danos.

No entanto, com a utilização da internet, compras online, transferência virtuais e outros meios tecnológicos, criou-se uma dificuldade para atuar na segurança de dados, tendo em vista a abrangência e os domínios de redes globais, que combinados com fatores não perceptível, forma

um perfil não rastreavel capaz de ocasionar violação às diretrizes básicas da legislação, que mesmo com ações posteriores não conseguem excluir os inúmeros registros de pessoas e organizações que coletaram os dados, lesionando a confidencialidade das informações (SAAD, 2021)

Destaca-se que as obrigações aos controladores e operadores, devem ser observados desde a coleta dos dados até seu descarte, assim o artigo 46 da LGPD, introduziu o conceito de privacy by design, sendo a incorporação pelas empresas nos serviços e produtos, na qual dispõe a proteção da privacidade no centro de todo o desenvolvimento corporativo.

Embora, a legislação tenta dirimir os riscos da atividade, os prejuízos causados pelo vazamento de informações são altos, e perpassam pela inadequação do sistema de proteção, perda de credibilidade e de clientes, ocasionado uma ruptura na imagem da empresa, impossibilitando, muitas vezes de concorrer no mercado corporativo. (SAAD,2021)

Portanto, a LGPD concebeu obrigações aos agentes de tratamento de dados, para que se delimite a finalidade da utilização dos dados desde o início da concepção, devendo o controlador confeccionar relatório de impacto a privacidade, utilizando de métodos para a captação da operação do ciclo de vida dos dados, observando as mediadas adotada para aumentar a segurança e mitigar o risco do tratamento das informações, conforme artigo 3 da LGPD.

O último pilar, considerado como a responsabilidade dos agentes na incidência de ocorrência de danos derivados do tratamento de dados. A LGPD consagrou a natureza do tratamento, limitando os parâmetros ao artigo 7° da lei, nas 10 hipóteses dos incisos, vinculados a finalidade da captação dos dados, consoante prevê o artigo 6°, inciso I, II, da LGPD.

A legislação tem como regra o descarte (eliminação) dos dados ao fim do tratamento da operação (art. 16), com o intuito de mitigar os riscos presente no tratamento de dados, principalmente, no que concerne à limitação das hipóteses de tratamentos para não lesionar os direitos dos titulares.

Nos casos, em que mesmo após o término de vida útil dos dados, as empresas podem, quando permitido, armazenar dados que em situação incidentais serem objetos de violação, principalmente nos casos de vazamento, que podem ocorrer, quando não autorizados pelo titular

ou controladores, serem acessados, captados, compartilhados pela internet, para outros sujeitos ou empresas.
Assim, a Lei Geral de Proteção de dados Pessoais, em especial em seu artigo 42, dispõe que o controlador ou operador, quando realizar o exercício do tratamento de dados pessoais, vem

a ocasionar dano patrimonial, moral, individual ou coletivo em detrimento a aplicação da legislação, é obrigado a repará-lo, definindo a responsabilidade de forma objetiva.
Embora, a responsabilização objetiva não é necessária a demonstração de culpa do controlador ou operador. Faz mister esclarecer que o operador, só será responsabilizado quando os atos praticados forem contrário à legislação, ou às instruções que foram fornecidas pelo controlador. (MENDES, DONEDA, 2018)
Ainda, a legislação prevê exceções a responsabilidade objetiva (art. 43), sendo: quando o agente demonstrar que não realizou o tratamento de dados pessoais que foi atribuído, ou quando não houve violação da segurança ou a legislação, e por fim, quando for por culpa exclusiva do titular ou de terceiros.
Porém, o cenário que é vislumbrado no Brasil nos casos de vazamento de dados, é que as violações pelas instituições vêm ocorrendo, majoritariamente, sob ataques deliberados de hacker, ou falha de segurança dos controladores dos dados. (SAAD, 2021)
Dessa forma, é necessário adotar medidas para dirimir os riscos da atividade, e possibilitar o discernimento das informações acerca dos perigos de vazamento de dados, tendo em vista que a tendência é aumento significativo das violações vinculados com a crescente tecnológica. Assim, as empresas devem implementar mecanismos para a segurança das informações.

5 O COMPLIANCE EMPRESARIAL COMO INSTRUMENTO DE PROTEÇÃO DE DADOS NA ESFERA EMPRESARIAL

Em decorrência das constantes violações aos dados armazenados em provedores privados, a tutela ao direito à privacidade nos meios tecnológicos, já era pauta de debate na legislação brasileira, e já existiam mecanismos para a proteção, como: a proibição de direcionamento dos provedores em relação ao compartilhamento de dados, bem como a inibição ao monitoramento nos navegadores de internet.
Vinte e seis bilhões de dados foram vazados no Brasil em 2019, de acordo com pesquisas realizadas pelo Massachusetts Institute of Tecnology ? MIT, possibilitando a utilização de números telefônicos, score de crédito, endereço eletrônico, fotos, números de identificações e outros dados pessoais, para o cometimento de crimes cibernéticos, e a violação aos direitos dos titulares.
A utilização e uso dos dados pessoais por pessoa física ou jurídica, com sede no Brasil ou não, devem se atentar as normas gerais de proteção aos dados brasileiro, segundo Frazão, Oliva e

Abilio (2020), é a necessidade de conferir a efetividade aos direitos e prevenir a violação aos dados, através da implementação de mecanismo de compliance, como uma ferramenta capaz de promover a adequação das atividades aportadas pelas empresas.
Assim, os controladores e operadores poderão formular regras de boas práticas e governança (Art. 50), que contenha as disposições de organização interna, o regime de funcionamento, as operações, o canal de comunicação entre os encarregados e os titulares dos dados, e o procedimento de segurança.
Nessa perspectiva, considerando que a maioria das tratativas de dados perpassam por meios digitais, deve-se adotar sistema para mapear os riscos, e implementar mecanismos para minorar as vulnerabilidades apontadas pelos programas, através da alta administração, do código de ética, para proteger os dados pessoais dos titulares. (PESSOA, 2021)
Existem inúmeras formas de ocorrer o vazamento de dados, sendo através de ataques cibernéticos, sequestro de conta, furtos de dados, compartilhamento de dados por agentes ou ex-agentes da empresa, erro ou negligência, entre outros, que podem ser para adquirir dados de nomes, CPF, celulares, endereços, dados financeiros, senhas, registro de saúde ou credenciais de acesso. (SAAD, 2021)
Desse modo, para realizar o mapeamento dos problemas que as corporativas podem enfrentar, é necessário identificar os fluxos e processos de informação que percorrem os sistemas, que irão auxiliar na tomada de decisão pelas empresas. (NASCIMENTO, 2020)
A alta administração deverá colaborar ativamente no programa de compliance, seja monitorando as investigações e intervenções em situação para estabelecer controles internos em conformidade com a legislação, bem como possibilitar a interdependência dos setores para realizar as atividades designadas para o tratamento de dados (PESSOA, 2021).
Com a elaboração do código de ética pela organização possibilitará o treinamento regular das equipes, responsáveis pela tecnologia da informação, para enraizar a cultura corporativa da boa governança, com a finalidade de assegurar o respeito ao programa de compliance (NASCIMENTO, 2020)
Nesse contexto, para manter uma boa relação com seus clientes, as organizações devem instalar canais de comunicação, para que os titulares dos dados possam contatar os encarregados responsáveis pelos armazenamentos dos seus dados, e exerçam seus direitos sobre as informações contidas nos provedores. (PESSOA, 2021).

Desse modo, quando se trata de concretização a alteração cultural coportariva é preciso realizar o alinhamento dos funcionários com o código de ética, com política de privacidade, para fins de efetividade do programa de compliance de dados. (PESSOA, 2021).

5.1 A IMPLEMENTAÇÃO DE MECANISMOS DE GOVERNANÇA DE DADOS PESSOAIS

Para a efetividade da legislação em relação ao tratamento de dados, a LGPD direciona um capítulo para implementar o programa de governança em privacidade, com a finalidade das empresas adotarem medidas técnicas, para fins de proteção e segurança dos dados pessoais.

(PESSOA, 2021)
A governança em privacidade, pode ser conceituada como um conjunto de regras e práticas positivas a serem implementadas pelos agentes de tratamento, e encontra-se em conformidade com as políticas de compliance empresarial, com o objetivo de gerir os dados das empresas para estabelecer um diferencial competitivo aos negócios. (KOEPSEL,2020)
O programa integra o aperfeiçoamento do procedimento de utilização dos dados, com os requisitos pré-estabelecidos na implementação dos softwares, com a finalidade de gerir de forma otimizada os dados para preencher as diretrizes da legislação. (SAAD, 2021)
A Lei Geral de Proteção de Dados Pessoais dispôs que os controladores e operadores poderão adotar programas de governança em privacidade, que devem ser implementados com o mínimo, (art. 50, § 2°, I): a) o comprometimento dos agentes de tratamento com as políticas internas que devem garantir o cumprimento das normas e regras de boas práticas; b) que aplicação seja de forma uniforme para todo a operação de tratamento de dados; c) que a governança seja adaptativa as estruturas da empresas, sendo compatível com a densidade dos dados e operação; d) como implementar políticas de salvaguardas em relação aos titulares dos dados; e) tenha como objetivo estabelecer uma relação de confiança com sujeitos dos dados, estabelecendo situações de transparência e que possibilite a atuação do titular; g) que conte com planos de respostas a incidentes e remediações; h) seja continuamente atualizado sua base.
Nesse aspecto, devem ser adotadas medidas administrativas para que as instituições, em conformidade com a legislação, apliquem estímulos para assegurar as informações armazenadas pelas empresas, com a adoção de orientações internas que respeitem as diretrizes que inclua o uso

minimizado ou a anonimização das informações, desde a coleta dos dados, conforme artigo 46 da LGPD.
Com o mapeamento das atividades, é importante verificar: O que são esses dados?; de que forma foram coletados ?; quem são os coletores ?; existe relação entre os dados e atividade realizada ?; O que pode ocorrer com esses dados ao serem coletados? E, como são descartados da gestão organizacional da empresa? (NASCIMENTO, 2020). Dessa forma, para adotar medidas compatíveis com os riscos alertados pelos sistemas para a proteção de dados nas organizações privadas, é necessário possuir conhecimento do caminho realizado inerentes ao ciclo de vida útil dos dados.
Embora, a legislação já estabeleça diretriz mínima para o tratamento de informação, a Autoridade Nacional de Proteção de Dados - ANPD, poderá, ainda, determinar padrões técnicos para serem implementados pelo programa de governança em privacidade, devendo ser observado a qualidade de dados, as especificações do tratamento e status tecnológico, em especial a proteção aos dados sensíveis disposto na legislação. (NASCIMENTO, 2020)
Muito embora, a lei geral de proteção de dados, apenas delimita as características e os requisitos mínimos que os operadores deverão tomar para desenvolver um compliance na organização das empresas privadas em consonância com a legislação, porém não impõe um modelo específico para integração de um programa nas corporativas. (PESSOA, 2021)
Assim, para Saad (2021), as medidas técnicas que podem ser adotadas pelos agentes de

tratamento de dados, são: i) o uso de firewalls, sendo um mecanismo de segurança que coleta os dados em conformidade com as regras pré estabelecido para análise de tráfego de rede, delimitando as operações de compartilhamento e captação de informações a serem cumpridas; ii) a utilização de antimalware, que consiste na proteção contra vírus que é capaz de fragilizar o sistema, apagar dados e infectar outros arquivos; iii) a utilização de criptografia dos dados, que possibilite quando ocorrer situações incidentais a não identificação do titular do direito.
Já para Fernandes e Abreu, (2014) defendem a implementação de frameworks como a DAMABOK e COBIT, para o gerenciamento de dados, pois tem como meta principal a delimitação do escopo das atividades, as funções envolvidas no tratamento e as interações a serem executadas pelo software, com a finalidade de proteger a privacidade em ambientes corporativos que gerenciam o armazenamento de informações aplicados na prevenção à fraude.

Segundo Carvalho (2021), a integração do software, através das boas práticas estabelecidas pela legislação, poderá aprimorar os aspectos de proteção à privacidade e prevenção a fraude do tratamento de coleta de dados. Tendo em vista, que os frameworks, podem balizar as métricas de qualidade dos dados que indicam uma utilização adequada e otimizada, e aponta a melhor proteção da privacidade.
Com a melhoria de processo de governança para o tratamento de dados, estabelece uma divisão entres as operações que possibilita uma automatização do ciclo de vida dos dados (coleta, utilização, armazenamento e exclusão), capaz de gerar relatório de risco, para o auxílio da tomada de decisão com o intuito de gerir de forma adequada o tratamento de dados. (CARVALHO, 2021)
Neste parâmetro, os programas de compliance com a implementação de frameworks, podem responder questionamento acerca do procedimento de tratamento de informação, dispondo de quais práticas relacionadas à governança, privacidade e segurança de dados, apresentam melhor benefício para o tratamento de dados pessoais. (CARVALHO, 2021)
Ademais, os controladores e operadores deverão adotar medidas, como o Relatório de Impacto ? DPIA), que corresponde a avaliação dos riscos e impactos relacionados com o tratamento de dados pessoais, além da anonimização, da transparência e do sigilo, deverão delimitar prazos para retenção de dados e aderir políticas seguras de informação acerca da operação de tratamento. (SILVA, 2022)
Após realizar a implementação e observância das estruturas mínimas estabelecidas pela LGPD, é necessário adotar um programa de gerenciamento de vulnerabilidades, com atualizações constantes e autocorreções alinhados com as boas práticas de atividades cotidianas, com a finalidade de proteger os dados pessoais, e promover um ambiente corporativo adequado para realizar o tratamento de dados. (SAAD, 2021)
No entanto, ao verificar que houve vazamento de dados, seja pelo recebimento de notificação ou pela veiculação na mídia, os agentes de tratamentos deverão identificar quais dados vazaram e realizar o procedimento estabelecido no programa de compliance de segurança, além de notificar as instituições. (Art. 48, caput).
De acordo com MIT, o prazo entre a comunicação à autoridade competente e a ocorrência do fato ilícito ultrapassa 200 (duzentos) dias em média, sendo umas das preocupações para a

efetividade da legislação, e a redução dos danos causados aos titulares dos bens imateriais.

A Lei Geral de Proteção de Dados, dispõe que nas situações que ocorrer a probabilidade de riscos ou violação aos direitos dos titulares, tem como obrigação do encarregado a comunicação à autoridade nacional e ao titular do dado (art. 48, caput). Sendo que o contato deve ser em período razoável (art. 48, § 1º), contendo a natureza dos dados dos titulares atingindo (art. 48, § 1º, I).
Em decorrência dos possíveis incidentes, a LGPD determinou critério para aplicação de sanções, em casos de vazamento de dados, observando as situações específicas de cada caso, disposto no art. 52, § 1º. Assim, deve ser considerada a avaliação da gravidade, a natureza das informações e do dano ocorrido (incisos I e VI), sendo necessário para este caso, tendo em vista que o compartilhamento indesejado de dados sensíveis pode ocasionar danos irremediáveis para os titulares.
Portanto, existe a necessidade da adesão aos mecanismos e técnicas para promover a efetividade dos programas internos com a finalidade de mitigar os danos, assim, a implementação de boas práticas e governança têm como fator o cumprimento da legislação, por meio de medidas de segurança. Entende-se, que a proteção integral contra falhas que possibilitam a ocorrência de ilícitos não é possível, porém essas diretrizes reduzem as possibilidades de existir desvios de condutas e criar salvaguardas para identificação dos incidentes, de forma eficaz, rápida e adequada.

6 CONSIDERAÇÕES FINAIS

A partir da permissão ao acesso dos dados pessoais, as informações coletadas passaram a integralizar as redes de tratamento de dados, tornando-se alvo de ataques cibernéticos, contribuindo para o aumento da intercorrência no ambiente corporativo, tornando-se o gerenciamento de informação um dos diferenciais no desenvolvimento do negócio.
Nesse contexto, foi imperativo o surgimento de leis que protejam os dados dos cidadãos, e que limitem a gestão das entidades públicas e privadas em relação as informações coletadas, transformando o sistema organizacionais, como compliance, em ferramentas de efetivação das normas éticas e legais. Assim, a implementação do programa alinhado com a governança corporativa é capaz de integralizar o corpo de normas internas com o intuito de adequar a legislação brasileira e criar uma cultura corporativa.
Dentro do programa de compliance, a administração em conjunto com a gestão da empresa, poderá implementar ao plano diretor, a utilização de software, sendo este capaz de possibilitar a automatização do ciclo de vida útil dos dados para realizar o auxílio da tomada de decisão, com o intuito de mitigar os possíveis danos decorrentes da violação aos dispositivos da Lei Geral de Proteção de Dados Pessoais.
Nesse sentido, para realizar uma proteção extensiva aos direitos dos titulares dos dados, a

LGPD integrou ao seu corpo de normas-condutas a serem adotadas pelos operadores do tratamento de dados, com escopo de preservar a integralidade, a qualidade e o sigilos dos dados, tendo como consequência da violação, a majoração de sanções pecuniárias.
Embora, o vazamento de dados ocorra de forma ordenada, a implementação de sistema de segurança nas corporações implica na diminuição de situações incidentais por erro humano, ou inadequação dos programas empresarias, assim, devendo a gestão ensejar esforços para que a proteção dos dados seja preservada, desde a concepção do serviço.
Para a efetivação da Lei Geral de Proteção de Dados Pessoais, as empresas devem realizar a adequação de medidas de boas práticas e governança em privacidade para mitigar os possíveis danos decorrente da violação aos dados em provedores privados. Mesmo que a proteção aos dados de forma concreta não seja possível, as adoções de mecanismo de segurança podem atenuar as sanções e as perdas aos titulares dos dados.

REFERÊNCIAS

BARATA, André Mantola. Governança de dados em organizações brasileira: uma avaliação comparativa entre os benefícios previstos na literatura e os obtidos pelas organizações. 2015. Dissertação (Mestrado em Sistema de Informação) - Universidade de São Paulo, São Paulo, 2015.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, [2022]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 15 abr. 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidente da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 abr. 2023.

BERTOCCELLI, Rodrigo de Pinho. Compliance. In: CARVALHO, André Castro et. al. Manual de compliance. Rio de Janeiro: Forense, 2019. p. 35.

CANDELORO, Ana Paula; RIZZO, Maria Balbina Martins De; PINHO, Vinícius (Coord). Compliance 360: riscos, estratégias, conflitos e vaidades no mundo corporativo. São Paulo: Trevisan, 2012.

CARVALHO, A. P. Proposta de um framework de compliance à Lei Geral de Proteção a Dados Pessoais (LGPD): um estudo de caso para prevenção a fraude no contexto de big data. 2021. Dissertação (Mestrado em Engenharia Elétrica) - Universidade de Brasília, Brasília, 2021.

CARVALHO, Andre Castro. Manual de compliance. 3. ed. Rio de Janeiro: Forense, 2021.

CASAES, Júlio César Costa. Governança de dados abertos governamentais: frameworks conceitual para as Universidades Federais, baseada em uma visão sistemática, 2019. Tese (Doutorado em Engenharia e Gestão do Conhecimento). Universidade Federal de Santa Catarina, Florinaóplis, 2019.

DATA GOVERNANCE INSTITUTE (DGI). Definitions of data governance. 2017. Disponível em: http://www.datagovernance.com/adg_data_governance_definition. Acesso em: 01 mai. 2023.

ENDEAVOR DO BRASIL. Prevenindo com o Compliance para não remediar com o caixa. In: ENDEAVOR. [S. l.], 26 abr. 2017. Disponível em: https://endeavor.org.br/pessoas/compliance/. Acesso em: 15 mar. 2023.

ESPÍNDOLA, P. L.; SALM JUNIOR, J. F.; ROSA, F.; JULIANI, J. P. Governança de dados aplicada à ciência da informação: análise de um sistema de dados científicos para a área da saúde. Revista Digital de Biblioteconomia & Ciência da Informação, Campinas, v. 16, n. 3, p. 274-298, 2018.

FERNANDES, Aguinaldo Aragon; DE ABREU, Vladimir Ferraz. Implantando a governança de TI: da estratégia à gestão de processos e serviços. 4. Ed. Rio de Janeiro: Brasport, 2014.

FRAZÃO, Ana. Programas de compliance e critérios de responsabilização de pessoas jurídicas por ilícitos administrativos. In: ROSSETTI, Maristela Abla; PITTA, Andre Grunspun. Governança corporativa: avanços e retrocessos. São Paulo: Quartier Latin, 2007. p. 42

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. A Lei Geral de proteção de Dados Pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

HONÓRIO, Roseli. Modelo conceitual de governança de dados como suporte à governança do conhecimento organizacional. 2022. Dissertação (Mestrado em Engenharia e Gestão do Conhecimento) - Universidade Federal de Santa Catarina, Florianópolis, 2022.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC). Guia das melhores práticas de governança para cooperativas. São Paulo, 2015. Disponível em http://www.ibgc.org.br/ userfiles/files/2014/files/CMPGPT.pdf

JOHNSON, Ralph E.; RUSSO, Vincent. Reusing object-oriented designs. Relatório Técnico da Universidade de Illinois, UIUCDCS 91-1696, 1991.

KLEINDIENST, Ana Cristina. Grandes temas do direito brasileiro: compliance. São Paulo: Almedina Brasil, 2019

KOEPSEL, Alice de Medeiros. Adoção e efeitos dos programas de compliance à luz da Lei Geral de Proteção de Dados Pessoais. 2020. Monografia (Graduação em Direito) -Universidade do Sul de Santa Catarina, Florianópolis, 2020.

LIMA, C., BASTOS, R. C. A criação de conhecimento apoiada pela governança de dados. In: CONGRESSO INTERNACIONAL DE CONHECIMENTO E INOVAÇÃO, 2019, Santa Catarina. Anais eletrônicos [...]. Santa Catarina Disponível em: https://proceeding.ciki.ufsc.br/index.php/ciki/article/view/647. Acesso em 10 Mar. 2023.

MARTIGNAGO, Deisi et al. Governança de dados aplicado no processo de catalogação. Revista Brasileira de Biblioteconomia e Documentação, São Paulo, V.15, n. 2, 2019.

MENDES, Gilmar Ferreira. Curso de direito constitucional. 2. ed. São Paulo: Saraiva, 2008.

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. São Paulo: Revista de Direito do Consumidor, 2018.

NASCIMENTO, Suellen Lima do. A lei Geral de Dados Pessoais e a Adoção dos Programas de compliance na sociedade da Informação. 2020. Monografia (Graduação em Direito) - Centro Universitário de Brasília, Brasília, 2020.

PESSOA, Larissa Rocha de Paula. Os desafios da Governança de dados e a realidade cultural brasileira. 2021. Dissertação (Mestrado em Direito) ? Universidade Federal do Ceará, Fortaleza, 2021.

PINTO, S. C. C. S.. Composição em Web Frameworks, 2000. Tese (Doutorado em Informática) Pontifícia Universidade Católica do Rio de Janeiro, Rio Janeiro, 2000.

PROSSER, William L. Privacy. California Law Review. California, v. 48, n. 3. p. 383 ? 423, agosto, 1960.

RÊGO, Bergson Lopes. Gestão e governança de dados: promovendo dados como ativo de valor nas empresas. 1. ed. Rio de Janeiro: Brasport, 2013,

ROQUE, Pamela Romeu. Estudos aplicados de direito empresarial: LL.C. em direito empresarial. São Paulo: Almedina, 2019.

SAAD, Carolina de Oliveira. A lei geral de proteção de dados pessoais e incidentes de segurança: regulação e prática de vazamento de dados, 2021. Monografia (Graduação em Direito). Fundação Getúlio Vargas. Rio de Janeiro, 2021.

SANTANA, Ricardo Cesar Gonçalves. Ciclo de vida dos dados e o papel da ciência da informação. In: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO. 14., 2013. Florianópolis. [?]. Florianópolis: UFSC, 2013. Disponível em: http://enancib2013.ufsc.br/index.php/enancib2013/%20XIVenancib/paper/viewFile/284/319. Acesso em: 13 mar. 2023.

SILVA, Ana Laura Fonseca. O papel das Soft Skills na implementação efetiva dos programas de compliance com foco na adequação à Lei Geral de Proteção de Dados ? Lei N° 13.709/18. 2022. Monografia (Graduação em Direito) - Universidade Federal de Ouro Preto, Ouro Preto. 2022

SILVA, Eggon João da. A defesa da ética e transparência. In: VENTURA, Luciano Carvalho. Governança corporativa. São Paulo: Saint Paul Editora, 2005, página 259.

TERRA, Priscila de Mello. A influência da governança de dados na gestão estratégica, 2017. Monografia (Bacharelado em Sistema de Informação) - Universidade Federal Fluminense, Niterói, 2017.

VAZAMENTO de dados aumentaram 493% no Brasil, segundo pesquisa do MIT.VEJA, São Paulo, 24 fev. 2021. Sociedade. Disponível em: https://vocesa.abril.com.br/sociedade/vazamentos-de-dados-aumentaram-493-no-brasil-segundo-pesquisa-do-mit. Acesso em: 15 mar. 2023.

VIEIRA, Tatiana Malta. O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante da tecnologia da informação. Porto Alegre: Sergio Antonio Fabris Editor, 2007.

==========

Arquivo 1: TCC - A IMPORTÂNCIA DO COMPLIANCE NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA - WESLEY VICENTE.pdf (8805 termos)
Arquivo 2: https://www.upguard.com/blog/lgpd (2535 termos)
Termos comuns: 19
Similaridade: 0,16%
O texto abaixo é o conteúdo do documento TCC - A IMPORTÂNCIA DO COMPLIANCE NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA - WESLEY VICENTE.pdf (8805 termos)
Os termos em vermelho foram encontrados no documento https://www.upguard.com/blog/lgpd (2535 termos)

==========

WESLEY VICENTE DA SILVA

A IMPORTÂNCIA DO COMPLIANCE EMPRESARIAL NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA

SALVADOR
2023

WESLEY VICENTE DA SILVA

A IMPORTÂNCIA DO COMPLIANCE EMPRESARIAL NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA

Artigo apresentado como requisito parcial para obtenção do título de Bacharel em Direito pela Universidade Católica do Salvador.

Orientador: Prof. Darlã Conceição Santos.

SALVADOR
2023

A IMPORTÂNCIA DO COMPLIANCE EMPRESARIAL NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA

Wesley Vicente da Silva1
Darlã Conceição Santos2

RESUMO: No cenário de exploração das informações como mercadoria econômica, os dados pessoais coletados por empresas privadas tornaram-se fator de tutela legislativa. Assim, surgiu a necessidade de organizar os setores privados para adequar aos moldes da Lei Geral de Proteção de Dados Pessoais ? LGPD, com o intuito de proteger a privacidade, como direito autônomo e fundamental para a tutela da pessoa humana, destacando os programas de compliance aliados as boas práticas e governança de dados. Nesse contexto, a fim de consolidar os mecanismos técnicos de segurança para a efetividade da legislação com a finalidade de mitigar os casos de vazamento de dados pessoais, a LGPD implementou medidas administrativas para inibir incidentes decorrentes das condutas infratoras a legislação. Desse modo, este trabalho tem como objetivo demonstrar a importância dos programas de compliance para a proteção aos direitos dos titulares dos dados, visando o cumprimento do ordenamento jurídico. Valendo-se do método hipotético-dedutivo, com abordagem qualitativa, utilizando da revisão bibliográfica de livros, legislação, artigos, dissertações e teses concernente à tutela de dados pessoais no Brasil para o desenvolvimento do presente artigo.

PALAVRAS-CHAVES: Compliance Empresarial. Governança corporativa. LGPD. Vazamento

de dados.

ABSTRACT: In the scenario of exploitation of information as an economic commodity, personal data collected by private companies have become a factor of legislative protection. Thus, the need arose to organize the private sectors to conform to the General Law for the Protection of Personal Data - LGPD, in order to protect privacy, as an autonomous and fundamental right for the protection of the human person, highlighting compliance programs allied with good practices and data governance. In this context, in order to consolidate the technical security mechanisms for the effectiveness of the legislation with the purpose of mitigating cases of leakage of personal data, the LGPD implemented administrative measures to inhibit incidents arising from conducts that violate the legislation. Thus, this work aims to demonstrate the importance of compliance programs to protect the rights of data subjects, aiming at compliance with the legal system. Taking advantage of the hypothetical-deductive method, with a qualitative approach, using the bibliographic review of books, legislation, articles, dissertations and theses concerning the protection of personal data in Brazil for the development of this article.

KEYWORDS: Corporate Compliance. Corporate governance. LGPD. Data leak.

1
Discente do curso de Direito da Universidade Católica do Salvador.
2
Mestre em Direito, Docente na Universidade Católica do Salvador.

1 INTRODUÇÃO

A nova moeda de troca não é apenas aquela que podemos ver, quantificar ou converter. Os moldes do mercado financeiro mudaram, sendo em questão material ou ao produto que eles precificam, postulando um novo aparato ao objeto contratual: os dados.
Muito embora, os dados pessoais, ainda para muitos, são apenas informações deslocadas acerca de fatores específicos, atualmente, podem ser conceituados como um conjunto de indicadores, regrados por um complexo condensado de informações em um fluxo crescente tangencial.
Os dados da grande massa acabam gerando indicadores que podem ser balizados e influenciados de acordo com os detentores dessa informação, apenas apartado em blocos de informações não são considerados como vetores orçamentários. Porém, direcionados para uma finalidade ordenada tem o condão de influenciar o interesse social.
Dito isso, os mecanismos postos pelo Reino Unido para possibilitar uma estruturação normativa para organizar e gerir os dados dos indivíduos, foi crucial para a criação em outros países, como no Brasil, onde instituiu-se a Lei Geral de Proteção de Dados Pessoais (LGPD). Muito

embora, a lei brasileira trouxe um arcabouço de normas reguladoras e sanções aos casos de tratamento de dados, que não foram abarcados com o marco da internet, os dados em uma visão macro constitucional já eram de forma genérica tutelados pela Constituição Federal de 1988.
Todavia, apenas a sanção da LGPD não seria, isoladamente, capaz de coibir as violações ao tratamento de dados na esfera privada, mas sim a necessidade de uma regulamentação do ciclo de vida das informações, que além de estipular os dados que podem ser utilizados ou até quando podem ser armazenados, estabelecer expressamente no bojo da norma como deve ser a proteção na operação do tratamento de dados.
De forma efêmera, conclui-se que a legislação pode delimitar os alicerces capazes de ensejar uma fiscalização, sendo estas através de mecanismo de gerenciamento de atividades, políticas de condutas e implementação de governança de dados, pois os dados hackeados ou vazados de forma isoladas, não seria possível identificar dados sensíveis, muitos menos individualizar o sujeito.
Portanto, o gerenciamento dos dados em provedores de armazenamento pode ter os riscos reduzidos de acordo com a realização de medidas de compliance para dirimir os impactos na

atividade empresarial, como também para tutelar os dados, cada vez mais acentuado como um produto orçamentário.

2 COMPLIANCE EMPRESARIAL

A criação do compliance está entrelaçado sob o cenário econômico-social, assim, sua implementação como sistema de organização foi instaurado e aprimorado a partir dos problemas práticos estruturais para gerir uma boa governança, com intuito de assegurar a proteção e o controle que garante a qualidade do negócio.
A utilização do termo foi inicializada no mercado financeiro, especialmente após a criação do Banco Central em 1913 nos Estados Unidos da América, com a necessidade de um sistema econômico ajustável e estável. Só após 1960, com a regularização da Securities and Exchange Commission (SEC), que houve a necessidade de implementação do compliance como um programa para a integração dos procedimento, controle e monitoramento de operação interna. (CARVALHO, 2021)
Em 1977, com a Convenção Relativa à Obrigação de Diligência dos Bancos Suíços, estabeleceu os modelos auto regulatórios, com adequação de condutas e processos internos, na qual a infração tem como consequência à aplicação de sanções. (CARVALHO, 2021)
Só após esse processo de amadurecimento histórico, que o Brasil teve a necessidade de competir em escala global, implementado novos processos de segurança no sistema financeiro brasileiro.
Pode-se concluir que, após a globalização com o fenômeno da criação dos dados estruturais, houve a potencialização das informações adquiridas por meio de provedores, classificadas, atualmente, como fonte econômica de um produto quantificativo e qualitativo, ao qual possibilita uma utilização como um produto do sistema financeiro.
Nesse sentido, em decorrência de ataques cibernéticos em provedores de informações

massificadas conduziram a sociedade na aplicação de institutos de melhoramento, como o compliance e suas interfaces para proteger no ambiente corporativo os dados massificados recebidos em seus provedores.

2.1 O CONCEITO DE COMPLIANCE

Antes de enveredar sob o conceito de compliance na esfera privada, é oportuno compreender o seu significado. Nesse contexto, a palavra compliance advém do verbo inglês, to comply, que pode ser definida como conformidade. O instituto deve ser aplicado como plano principal de uma diretriz pré-estabelecida para ser dirigida a todos capazes de enfrentar a finalidade destinada. (BERTOCCELLI, 2019)
Nesse parâmetro, pode ser traduzida como:

Comply, em inglês, significa ?agir em sintonia com as regras?, o que já explica um pouquinho do termo. Compliance, em termos didáticos, significa estar absolutamente em linha com normas, controles internos e externos, além de todas as políticas e diretrizes estabelecidas para o seu negócio. (ENDEAVOR DO BRASIL, 2022, n.p)

O compliance pode-se ser definido de forma técnica como um conjunto de normas padronizadas, sob um viés ético e legal, na qual após estruturação será a matriz orientadora para o comportamento organizacional da instituição ao qual atuará no mercado, como também irá reger as atividades dos colaboradores. Dessa forma, sendo um instrumento hábil a controlar o risco de imagem, a normatização legal, chamados de riscos de compliance, as que recaem nas instituições no decorrer da sua atividade laboral. (CANDELORO, 2012).
Superada a barreira terminológica, a finalidade do compliance tem como escopo o gerenciamento adequado do risco de atividades, verificar adequadamente as normas éticas e legais, e estudar os possíveis danos tangenciais. Dessa forma, esses elementos visam a redução de perdas e danos, como também amplifica a cultura e fortalecimento corporativo nos moldes aos padrões exigidos, seja esse por lei ou na tentativa de dirimir o risco do serviço prestado.
Portanto, segundo a doutrinadora Frazão (2007, p. 42), destina-se em sua obra que o compliance é como:
(...) conjunto de ações a serem adotadas no ambiente corporativo para que se reforce anuência da empresa à legislação vigente, de modo a prevenir a ocorrência de infrações ou, já tendo ocorrido o ilícito, propiciar o imediato retorno ao contexto de normalidade e legalidade.

Nessa mesma linha de pensamento, de acordo com os autores da obra Compliance 360° (2012, n.p), referem-se o compliance a:

Um conjunto de regras, padrões, procedimentos éticos e legais que, uma vez definido e

implantado, será a linha mestra que orientará o comportamento da instituição no mercado em que atua, bem como as atitudes de seus funcionários; um instrumento capaz de controlar o risco de imagem e o risco legal, os chamados ?riscos de compliance?, a que se sujeitam as instituições no curso de suas atividades.

Pode-se concluir que o conceito de compliance, em uma esfera macro, é um aglomerado de regras pré-estabelecidas através de um instrumento perpetuado por técnica de desenvolvimento, capaz de dirimir riscos e danos das atividades devolvidas pelo plano diretor.
Muito embora, o instituto "compliance" tem uma definição extensiva e não tem como fim apenas o cumprimento da legislação e de condutas éticas, pode ser compreendida também como um instrumento de diminuição de riscos, desenvolvimento corporativo sustentável e subsequentes segmentos empresariais de negócio. (ROQUE, 2019)
O compliance além de estar associado tradicionalmente a uma perspectiva organizacional aos comandos administrativos, pode ser vinculada também a uma visão de uma sociedade digital 4.0, devendo não só apresentar o compliance empresarial na esfera de redução de risco à imagem, mas sim, em uma abordagem de pré-orientação e implementação de desenvolvimento aos moldes legislativo de proteção aos dados, como objeto principal de estudos.
Portanto, é necessário a elaboração do projeto de compliance em uma visão lógica, a modo de compreender os objetivos e os componentes da aplicação do programa. Posteriormente, superado os obstáculos, aplica-se os estudos de riscos a boa governança corporativa com a implementação de programas de governança de dados objetivando auxiliar o controle de informações em conformidade aos padrões da corporação, e mitigar os danos da empresa.

2.1.1 AS GOVERNANÇAS CORPORATIVAS E A IMPLEMENTAÇÃO DOS PROGRAMAS DE COMPLIANCE

Em linhas gerais, o Instituto Brasileiro de Governança Corporativa ? IBGC (2015, n.p) discrimina o conceito de Governança Corporativa, como: ?Sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas. ?
O sistema da governança corporativa está associado ao desenvolvimento interno de uma empresa, seja ele entre a administração, sócios e funcionários, capaz de criar elos para uma estruturação de direção racional e acima de tudo nos moldes da ética e legislação.
Muito embora, a governança corporativa e o compliance sejam institutos que se assemelham em uma visão macro, os mesmos, diferenciam na aplicação prática, mas se complementam no objetivo final, sendo um instrumento para aplicação do outro.

A prática da governança corporativa, além de estimular o valor empresarial, pode-se concluir que estrutura de forma adequada a medida necessária para organizar a atividade empresarial, assim, não há que se falar em condutas prejudiciais. Por exemplo: empresários compreendem que para realizar uma instrumentalização segura aos seus sócios e administradores tendem a prejudicar o negócio empresarial, assim o autor Eggon João da Silva (2005, p.259) retrata que: ?A governança corporativa assegura tratamento equânime a todos os acionistas, inclusive minoritários, preferencialistas, nacionais e estrangeiros. Todos devem ter oportunidade de reparação caso venham a sofrer violação de seus diretores. ?

Nesse passo, as críticas ao sistema não são viáveis, tendo em vista a utilização de instrumento capaz de integralizar ao plano empresarial. Sendo assim, o programa de compliance visa amplificar a utilização de um sistema para garantir que todos possam participar de forma justa sob o aspecto legal, seja sócio ou administrador.

Em uma tangente geral, a implementação da governança corporativa ressoa em uma perspectiva segura, tanto internamente, seja auxiliando as avaliações das atividades executadas pelos sócios/administradores, quanto externamente, em relação à imagem da empresa, sendo este um fator primordial a empresas estruturadas no mercado.

A implementação da governança corporativa deve ser estruturada de acordo com as necessidades da empresa, devendo verificar o histórico de desenvolvimento do estabelecimento, pois, só a partir do status da empresa pode-se delimitar a estratégia possível para uma implementação segura e adequada. Sendo assim, um regramento mais rigoroso pode gerar consequências negativas e ineficazes, especificamente em estágios primários, pois em atividades inicias, as tomadas de decisões e a execução da atividade empresarial é primordial, sendo necessário, um aspecto negocial informal para realizar os objetivos da empresa, o que não se verifica quando existe prática de boa governança devidamente estruturadas no negócio. (KLEINDIENST, 2019)

Ao desenvolver da atividade da empresa, além da atenção a organização interna, sendo está um fator primordial da governança, ainda que no fim acabe tendo um aspecto externo por vislumbrar no mercado financeiro uma maior complexidade da entidade. O desenvolvimento da empresa, seja no faturamento, importação comercial, quantidade de funcionários, além dos controles a observância da legislação e regras internas, tendem à serem complexos, e, que necessita

de ações maiores que a própria instituição empresarial, restando necessária a implementação de sistema organizacionais aos fluxos de informações. (KLEINDIENST, 2019)

Ultrapassado a esfera conceitual e instrumentalização da política de boas práticas de governança, cabe pontuar que as empresas que possuem fluxos de informações sensíveis, conforme estipula o artigo 50 da Lei Geral de Proteção de Dados Pessoais, os controladores e operadores são responsáveis pelo tratamento de dados, devendo criar planos de adequação a legislação.

Assim, ao confeccionar as regras de boas práticas, os controladores adjuntos com a administração devem estipular através da análise da natureza dos dados coletados, a probabilidade, a finalidade e o potencial de riscos das vantagens advindas dos tratamentos dos dados verificados. (NASCIMENTO, 2020)

É necessário pontuar que, os agentes de tratamento, após a autenticação da gravidade e sensibilidade dos dados aos riscos de operação, poderão estabelecer programa de governança em privacidade, sendo este, um instrumento amplo com normas de compliance, além dos aspectos operacionais.
Em relação ao programa de governança de privacidade, pode-se estabelecer como um aglomerado de normas-regras de boas práticas de governança, com a finalidade de executar ordens de natureza legal. (NASCIMENTO, 2020)
Portanto, os instrumentos do compliance em conjunto com a boa prática de governança, se consagram na identificação dos riscos e estruturação de medidas para a empresa, sendo respondida de forma adequada e proporcional ao suporte da tomada de decisão.
O Programa de compliance na esfera privada para análise de dados pessoais, com a finalidade de promover a segurança, deve ser constantemente monitorado e atualizado, com a implementação de ?salva vidas? em decorrência de avaliação de riscos à privacidade e o acometimento de vazamentos. (NASCIMENTO, 2020)
Portanto, os instrumentos e objetos referenciados demonstram a determinação de regras de governança no ambiente de operação de tratamento de dados pessoais, a modo que seja realizado uma estruturação nas empresas para que possibilitem a implementação de mecanismos de segurança, com a finalidade de dirimir os riscos da atividade empresarial na sociedade digital.

3 GOVERNANÇA DE DADOS

O mercado digital tem como principal ativo financeiro os dados, este considerado como ?matéria prima? de uma economia baseada no conjunto de informações, sendo que nos últimos anos, houve um aumento exponencial na coleta de dados por cooperativas, startups e novos nichos empresariais, tendo a finalidade de quantificar e gerencias os dados.
Dados, informações, conhecimento e sabedoria são os quatros estágios evolutivos da cadeia de informação, pode-se assim, compreender os dados como fatos ou registros em seu formato primário. (BEAL, 2014). Já a informação é entendida como os conjuntos processados de dados em um contexto aplicado (RÊGO, 2013). Muito embora, na sociedade da informação ?os dados são o novo petróleo?, apenas os dados isoladamente não são capazes de transformar em ativo financeiro, sendo necessário administrá-lo de forma eficaz, para que assim, as empresas adquiram vantagem competitiva.
Dessa forma, a governança de dados tem como principal objetivo atender as necessidades das empresas, ou seja, solucionar problemas, diminuir custos da administração, para que os dados transformem em saldo positivo para os negócios (TERRA, 2017).
O Data Governance Institute -DGI (2017, n.p) definiu governança de dados como ?um sistema de direitos de decisão e responsabilidades para processos relacionados à informação, executado de acordo com modelos acordados que descrevem quem pode realizar quais ações com quais informações e quando. ? Portanto, a utilização da governança de dados orienta quais os métodos deverão ser aplicados no ciclo de vida dos dados.

Uma das atribuições da governança é o acompanhamento da operação dos dados com a finalidade de gerir que as informações estejam alinhadas com os objetivos pré-determinados na coleta primária, além disso, é necessário assegurar que as informações estejam disponíveis para acesso, quando consultadas, gozar de qualidade, consistência, auditabilidade e segurança dos dados (ESPÍNDOLA, 2018).

No âmago da cadeia evolutiva da informação uma das preocupações dentro das organizações corporativas é o receio com a proteção das informações, ou seja, a capacidade das empresas no protagonismo da segurança com os provedores internos, tendo em vista a necessidade de conformidade com a legislação pátria.

A boa governança tem como objetivo aplicável à prática do controle dos processos de operação dos dados: a prevenção de situações adversas que podem gerar o comprometimento da integralidade dos dados adquiridos pelas organizações empresariais, que por sua vez, devem ter o condão de reforçar a confidencialidade das informações. (ESPÍNDOLA, 2018).

A integração do programa de governança de dados nas corporativas empresariais, tem como o esforço principal a organização de dados, que deve ser observado por um prisma basilar, ou seja, a aplicação dos princípios como limite legal e ético no ciclo de vida dos dados.

Para Rêgo (2013), os princípios são regulamentações para compreender aplicação da governança dos dados como linha direta para os negócios, sendo: (i) A gestão de dados estratégicos, tem o dever de vislumbrar as tomadas decisões por um coeficiente tático e operacional. (ii) A governança como instituição, ou seja, a governança de dados pode ser comparada como sistema governamental, na qual dispõe de legislação, execução e jurisdição; (iii) A governança de dados como um programa, devendo ser implementado como fator permanente, não apenas um projeto temporário. Ainda, pontua-se que os princípios da Governança de dados não são limitados, tendo uma orientação basilar a cada implementação de um sistema organizacional que deve ser observado pelo prisma ético e legal.

Assim, os princípios devem incumbir os papéis que a serem preenchidos pela gestão moldar os comportamentos das empresas para a aquisição, reserva e utilização dos dados conforme as normas e políticas da corporação (TERRA, 2017).

Coleta, armazenamento, recuperação e descartes, são as quatro etapas do ciclo de vida dos dados (SANTANA, 2013), ou seja, para a aquisição de dados pelas empresas, deverão observar a vida útil do dado para não incorrer na (in) responsabilidade da utilização indevida de informações dos seus provedores.

As fases do ciclo de vida dos dados devem ser observadas pela ótica de seis objetivos, sendo eles: a qualidade, a privacidade, os direitos autorais, a integração, compartilhamento e preservação dos dados (ESPÍNDOLA, 2018). Muito embora, a lei geral de proteção de dados implementou e traçou novos objetivos para a coleta de dados pessoais, cabe destacar que os objetivos vislumbrados na Governança de dados têm como parâmetro preliminar a tomada de decisão, na qual deve ser os negócios pautados nos moldes legais e éticos vigentes.

Nesse contexto, o controle de informações é necessário, tendo em vista que na sociedade da informação, cada vez mais o volume de dados é crescente, acarretando mais vazão e protesto

por políticas públicas para a preservação dos institutos, órgãos e empresas que detenham a

informação, sendo assim, necessário sistema de organização, softwares e hardwares capazes de processar as informações, criptografar e armazenar. (MARTIGNAGO, 2019)
Assim, para otimizar o ciclo de vida dos dados e garantir que os objetivos sejam preenchidos na estruturação do gerenciamento de dados, faz-se necessário a implementação de frameworks com o intuito de garantir que o procedimento seja cumprido com maior qualidade de informação e aproveitamento financeiro para a empresa, auxiliando a tomada de decisão para redução de risco para utilização de dados. (MARTIGNAGO, 2019)
Um Framework, segundo Johnson (1991), pode ser definida como um aglomerado de objetos que colabora entre si para que atinja um conjunto de obrigações para aplicação de um domínio especifico. Já para Pinto (2000), um framework é conceituado como um software incompleto criado para ser um objeto cujo estado e comportamento são definidos pela classe. Assim, o framework é uma concepção de uma arquitetura para um edifício de subsistemas e oferece o alicerce básico para criá-los.
Muito embora, os autores defendem uma conceituação distintas acerca da concepção de frameworks, pode-se verificar que ambas se complementam, tendo em vista que o framework é um sistema pré moldado, ou seja, é um programa com intuito de ser complementado através da finalidade a ser cumprida pela gestão empresarial, sendo instanciado por classes para categorizar os dados e ser alojado em hotspot, provedores físicos, capazes de armazenar as informações coletadas pelas empresas.
Portanto, para gerenciar os ativos de dados de forma complexa, ordenada e objetiva é necessário para proteção do procedimento do ciclo de vida dos dados, determinar os modelos de frameworks para o gerenciamento dos dados. Assim, para Carvalho (2021), podem ser apresentados três domínios CobiT, DAMA DMBOK e DGI Framework, sendo apenas dois destes observados para fomento deste artigo: (i) A DAMA (DAMA DMBOK), e (ii) CobiT.
A DAMA (Data Management Association) é uma associação sem fins lucrativos, com o intuito de promover boas práticas de gestão de dados, e em 2009 fundou o DAMA-DMBoK (Data Management Body of Knowledge), sendo um corpo de conhecimento que tem como ponto fundamental esclarecer como as corporativas devem aplicar a operação otimizada dos dados. (CARVALHO, 2021)
Em sua versão 2.0, acrescenta não só uma visão macro do gerenciamento de dados, definindo padrões, terminologias e práticas, mas a integração de dados, para definir táticas,

armazenamentos e sistemas, bem como implementação da ética na operação do tratamento de dados, a definição de big data e ciência de dados e amadurecimento das informações. (LIMA, 2019).
O DAMA-DMBOK V2 é formado por 11 (onze) funções de gestão de organização de

dados, sendo incorporado como cerne principal: a governança de dados, tendo em vista que os dados percorrem por toda sistemática das onzes funções ordenadas, assim segundo Honório (2021):
A primeira função é a governa de dados, sendo o pilar do framework, tem o condão de orientar e supervisionar a operação do ciclo de vida dos dados, na qual deve estabelecer um sistema de apoio a decisão dos gestores sobre os dados, sob o prisma do negócio.
A arquitetura de dados, a segunda função, pode ser conceituada como um planejamento para administrar os dados, aquisição de ativos da empresa, com o intuito de definir a finalidade das informações adquiridas com os requisitos necessário para o gerenciamento dos dados.
Por sua vez, a modelagem de dados e design, tem a função de demonstrar de forma nítida os dados, sendo o processo da descoberta, análise e representação da etapa primária da informação.
O armazenamento, uma das etapas da operação do ciclo de vida dos dados, na qual vai incluir o design, o suporte dos dados armazenados para quantificar o coeficiente valorativo das informações, até o seu descarte, devendo respeitar todo o procedimento de segurança legal vigente.
Um dos alicerces para o gerenciamento de informação é a segurança, que deve garantir a proteção dos dados, a execução de políticas e procedimento de segurança, no intuito de moderar o acesso de forma consciente e controlado, não devendo ser infringido ou acessado de forma inadequada, afim de garantir autenticação e auditoria de dados informações.
A Integração e Interoperabilidade de dados, é a função responsável pela movimentação e a concretização dos dados na interligação do armazenamento e outras plataformas.
O gerenciamento de documentos, pode ser compreendida como o gerenciamento e inclusão da vida útil dos dados e informações, encontrados em programas não estruturados, em ênfase ao conteúdo de apoio de conformidade a legislação vigente e os termos éticos formalizados para o negócio.
Dados mestre e de referência, tem como condão a manutenção dos dados compartilhados para coexistir a integralidade dos sistemas internos de gerenciamento dos dados.
Em razão da interligação entre uma linha direta com os negócios, uma das funções do DAMA-DMBOK é a Data warehousing e Business intelligence, ou seja, a implementação de

planner para o contoler da administração dos dados e suporte a decisão com o intuito de conceder aos gestores de informação emitam relatórios de equalização de valores.
Segundo Barata (2015), os metadados, na qual consiste a décima função, é promover a facilitação do acesso dos dados interligados nas multifontes do sistema integrado, como também garantir a qualidade de dados.
Por fim, o gerenciamento de qualidade de dados é a implicação das técnicas para garantir a possibilidade de aferição, melhoramento e adequação da utilidade dos dados, com o intuito de monitorar a integridade da informação primária no ciclo de vida dos dados.
Já o COBIT (Control Objectives for Information and related Technology), é um framework de suporte fundado em 1994 administrado pela ISACA (Information Systems Audit and Control Association), estruturado como um arcabouço de informação direcionadas para governança de dados e gerenciamento de informação, tem como objetivo auxiliar os profissionais de gestão na conexão entre os problemas técnicos e os riscos do negócio. (BARATA, 2015).

Para Lima (2019), o COBIT é um framework que possui duas vertentes basilares: a gestão, que possui quatro áreas de domínios: planejamento, constituição, execução e monitoramento, e a governança que é a tomada de decisão de acordo com a gestão de dados, possuindo 37 (trinte e sete) processos integrados.
Na versão 5.0, o sistema é utilizado baseado em 05 princípio, conforme elucida Casaes (2019), Barata (2015) e Lima (2019), sendo: (i) atender às necessidades das partes interessadas; (ii) cobrir o negócio como um todo; (iii) aplicar um framework único e integrado; (iv) habilitar uma visão holística; e (v) distinção entre governança de gestão.
Um dos princípios é atender às necessidades das partes interessadas, sendo a necessidade das corporativas é satisfazer as expectativas dos seus stakeholders, proporcionando um equilíbrio na tripartite: benefícios, redução do risco e recurso disponíveis.
O segundo princípio é baseado na cobertura do negócio como um todo, ou seja, abranger a integralidade da empresa no processo, procedimento, pessoas e as relações com os habilitadores.
A aplicação do framework único e integrado, assim, o COBIT é capaz de promover uma relação completa com a Governança de dados, corroborando ao alinhamento com padrões externos e adaptabilidade dos modelos usuais de negócios.

O COBIT permite habilitar uma visão holística, ou seja, uma visão macro dos componentes que oferecem suporte para atingir as finalidades da governança de dados, na qual define como catalogadores: as políticas, processos, estruturas organizacionais, informação e ética.
Por derradeiro, o princípio da distinção entre governança de gestão, tendo em vista que ambos possuem estruturas organizacionais distintas, assim, governança tem como esforço principal que os objetivos corporativos sejam cumpridos, estabelecendo prioridades pela tomada de decisão, compliance e progresso das organizações. Por sua vez, a gestão é o planejamento, construção, execução e monitoramento das funções ornamentada com o direcionamento da governança.
Desse modo, com escalonamento dos cinco princípios é capaz de proporcionar o funcionamento otimizado do framework, destacando os seguintes processos:
O APO01: Gerenciar o framework de TI, tem como condição a otimização das atividades relacionadas ao TI, com a função principal de incluir os procedimentos e regulamentos para promover a integralidade das informações nos bancos de dados. (BARATA, 2015)
Já o APO03: Gerenciar a arquitetura corporativa, tem função primordial agrupar as informações para auxiliar as atividades e tomadas de decisões, conceituando e compartilhando as informações dos elementos dos dados, e por fim catalogar a empresa, com base na modulação e sensibilidade dos dados. (BARATA, 2015)
Nesse ínterim, a governança de dados como um sistema integrado com o programa de compliance, tem o condão de otimizar a operação de controle interno relacionado aos dados coletados pelas empresas, capaz de gerenciar as bases para o apoio de decisão ao tratamento das informações, com segurança e qualidade, garantido o ciclo da vida útil dos dados.

4 A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

As estruturas políticas, econômicas e sociais com desenvolvimento de novas tecnologias e mecanismo para a coleta de dados e informações, fez necessário modulações legislativas para a proteção da privacidade, além dos aspectos físicos, patrimoniais e morais.
A proteção à privacidade de dados foi dividida em quatros gerações: a primeira, oriunda do estado moderno, com o advento dos bancos de dados; a segunda, datada em 1980, com a expansão legislativa para a proteção à privacidade aos setores privados; a terceira geração em 1990, com o processo de tratamento de dados e o consentimento dos cidadãos; Por fim, a última dimensão, é

destinada ao protagonismo da permissão para coleta e uso dos dados pessoais, quando a lei estabeleceu a importância da titularidade das informações. (MENDES, 2014)
Nesse aspecto, é perceptível a evolução do direito aos fatores reais da sociedade e as transformações dos meios tecnológico, computacionais, genéticos e comunicativos, que por sua vez possibilitou a integração da comunicação global, e consequentemente, o rastreio dos dados através do armazenamento de informação. (SAAD, 2021).
Os legisladores ao considerar os dados pessoais como extensão ao direito à privacidade, preocuparam em tutelar constitucionalmente a proteção da população, em especial os países europeus, como: Espanha, Portugal, Hungria, Eslovênia e Rússia. (VIEIRA, 2007) Porém, só tornou-se fator primordial após o regulamento geral do Parlamento Europeu sobre a proteção de dados, n.º 2016/679, sendo necessário a adequação das empresas prestadoras de serviço na Europa ao regulamento, influenciado diretamente o Brasil para elaboração da Lei Geral de Proteção de Dados brasileira. (SAAD, 2021).
Muito embora, a Lei Geral de Proteção de Dados Pessoais - LGPD, em sua promulgação, não abarcou de forma expressa a proteção de dados como direito fundamental, a doutrina, em especial Nascimento (2020), por sua vez, já argumentava a proteção de dados e informações pessoais como direito autônomo, derivado do direito fundamental à privacidade, explicitamente no artigo 5°, X, da CRFB de 1988.
Após reiterados julgamento sobre a tutela dos dados pessoais como extensão da personalidade do indivíduo, o Supremo Tribunal Federal -STF reconheceu no Julgamento da Ação Direta de Inconstitucionalidade - ADI 6387, a existência dos dados como direito autônomo, derivada do direito fundamental a dignidade da pessoa humana, na proteção à intimidade e a centralidade do Habeas Data como autodeterminação informativa. (NASCIMENTO, 2020).
Ao compreender a necessidade da proteção aos dados pessoais, os legisladores brasileiros em votação de ? das casas legislativas (câmara e Senado Federal) em dois turnos, aprovaram a Emenda Constitucional 115 de fevereiro de 2022, alterando o artigo 5° da Constituição Federal de 1988, incluindo o inciso LXXIX, tutelando constitucionalmente a proteção aos dados pessoais, inclusive nos meios digitais.
Ressalta-se, ainda, que os dados pessoais estão interligados com o direto fundamental à privacidade, na qual representa a capacidade de a pessoa administrar sua vida, seus pertences e

propriedades materiais e imateriais, permitindo ou não a utilização dos seus dados (bens imateriais) por terceiro. (NASCIMENTO, 2020).

A privacidade, por sua vez, segundo Mendes (2008), é o direito à proteção aos comportamentos pessoais e acontecimentos de caráter íntimo, bem como as informações prestadas aos profissionais e comerciantes, em que a pessoa não deseja que se compartilhe com o público.

Para o professor William Prosser, pode-se qualificar a lesão a privacidade em quatro graus: i) o intrometimento na reclusão ou solidão na vida privada, ii) a divulgação pública de fatos privados constrangedores sobre o indivíduo; iii) a publicidade sobre o indivíduo apresentada de forma equivocada; e iv) a apropriação, para obtenção de vantagem, do nome ou da imagem do demandante (PROSSER, 1960).

A doutrina, por sua vez, defende mais uma violação à privacidade: a privacidade informacional, interligada com os fatores tecnológicos de informação. (SAAD, 2021). Assim, quando a lei ao realizar o tratamento da privacidade, refere-se como um direito líquido, ao qual será tutelado para garantir que o indivíduo tenha um local reservado, que não tenha, se desejar, a interferência de outros sujeitos, seja pessoa física ou jurídica.

Com a proteção dos dados pessoais dos titulares, através da LGPD, possibilitou ao cidadão o acesso a informações ao ciclo de vida útil dos dados pelas empresas, e a certeza de fiscalização pela Autoridade Nacional de Proteção de Dados, com a finalidade de atingir os objetivos traçados pela legislação, na qual a lei traz conceitos e delimita princípios, que devem ser mencionados.

A LGPD tem como objetivo principal: ?o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado?, com a destinação de assegurar os direitos fundamentais a liberdade e privacidade dos titulares dos dados, bem como tutelar a dignidade e a personalidade da pessoa natural. (LGPD).

A legislação está ordenada diretamente com o meio empresarial, sobretudo no que se refere aplicação aos seus destinatários que são pessoas físicas ou jurídicas que realizam a coleta e tratamento de dados no Brasil, conforme preceitua o artigo 1° da lei 13.709, de 14 de agosto de 2018.

Para compreender a LGPD, faz-se necessário elucidar os conceitos de dados pessoais: (art. 5º, I) é toda informação relacionada a pessoa natural, identificada ou identificável, sendo o dado aplicado no contexto que possibilite o reconhecimento do indivíduo. Bem como refere-se aos dados sensíveis (art. 5º, II), são todas as informações que se relaciona com pensamentos políticos, crenças, identidade biológica e física. Portanto, a legislação tem como ponto a proteção e o cuidado para a não violação dos dados pessoais e sensíveis.

Os doutrinadores, Laura Schertel e Danilo Doneda, ainda aponta cinco pilares para compreender a LGPD, sendo: i) a unidade e generalidade da aplicação da Lei; ii) a legitimação para o tratamento de dados (hipóteses autorizativas); iii) os princípios e direitos do titular; iv) as obrigações dos agentes de tratamento de dados e v) a responsabilização dos agentes.

O primeiro pilar é considerado com aplicabilidade material da legislação, ou seja, aplica-se a qualquer operação realizada por pessoa natural ou jurídica de direito público ou privado,

independentemente do meio, da sua sede ou do país onde estejam localizados os dados (Art. 3°). Considerado, assim, como uma aplicação uniforme para todos os setores público ou privados que realizam tratamento de dados.

O segundo pilar é a legitimação para o tratamento de dados, tendo em vista que a lei especificou critérios e requisitos para o reconhecimento da legitimidade, não podendo ser tratados os dados, sem que exista uma base normativa que autorize, prevista no artigo 7°, 11° ou 23° da LGPD, abordando 11 (onze) hipóteses, incluído o consentimento ou a previsão legislativa.

Destaca-se que a autorização por consentimento para ser considerado válido, deve observar os requisitos previsto no artigo 5°, XII, sendo considerado que a vontade deve ser livre, informada, inequívoca e com a finalidade determinada, consagrando os princípios norteadores da legislação.

O terceiro pilar é o conjunto de princípios e direitos que assegura o destinatário da lei a controlar a utilização do seu dado pessoal, sendo importante elencar dez princípios que estruturam a LGPD: a finalidade, a adequação, a necessidade, o livre acesso, a qualidade dos dados, a transparência, a segurança, a prevenção, a não discriminação e a responsabilização. (MENDES, DONEDA, 2018)

No que concerne, aos direitos dos titulares são expressos no artigo 18° da referida lei, que permite o titular dos dados adquirir através do controler, independentemente do momento, as informações relacionadas ao indivíduo, prevendo: acesso, confirmação, correção, anonimização, bloqueou ou eliminação e a portabilidade.

Para adentrar no cerne dos problemas enfrentados pela legislação, em especial, sobre o vazamento de dados, os dois últimos pilares serão abordados sob a perspectiva da violação e responsabilização acerca da proteção de dados nos casos incidentes de vazamento.

Assim, o quarto pilar, destina-se às obrigações dos agentes de tratamento dos dados, na qual estabeleceu limites que devem ser observados nas operações realizadas para reforçar a segurança e prevenir os problemas da atividade no tratamento de dados.

Uma das obrigações fundamentais, consiste na intitulação do encarregado pelo tratamento dos dados indicados pelo controlador, conforme artigo 41 da LGPD, que possui a função de aceitar as reclamações e comunicações dos sujeitos dos dados, receber informações da Autoridade Nacional, como deve orientar os funcionários a respeito das práticas a serem adotadas em relação à proteção de dados pessoais.

Assim, as informações devem ser fornecidas ao proprietário dos dados, quando os dados forem coletados, como: os meios de segurança aderidos ao tratamento de dados, quais são os riscos da atividade que podem gerar lesão ao titular, pois pode gerar a mitigação dos prejuízos. (SAAD, 2021)

A lei Geral de Proteção de Dados Pessoais tem como objetivo a proteção do dados pessoais dos titulares dos dados, sendo assim, uma das obrigações principais é adoção de medidas de segurança, técnicas e administrativas hábeis a proteger os dados pessoais de acessos não autorizados, como promover a integralidade dos dados, não permitindo, assim, a alteração das informações, a prevenção de situações ilícitas ou acidentais, ou qualquer forma de tratamento inadequado, consoante se desprende do artigo 46 da lei.

Tornou-se corriqueiro manchetes acerca do vazamento de dados por corporativas, uma das violações mais graves incidentes abarcados pela LGPD, o que ocasiona a vulnerabilidade do titular dos dados, e dos sistemas internos que são responsáveis pelo ciclo de vida útil dos dados. (SAAD,2021)

A seção de segurança de informação tem como condão as obrigações inerentes aos agentes de tratamento, devendo ser adotado pela integralidade das pessoas que realizam o tratamento de dados, garantido que os dados sejam confidenciais, bem como disponíveis nas operações de tratamento. (Art.48). Nos casos incidentais de vazamento de dados, insurge a necessidade ao controlador de informar a autoridade de proteção de dados, que podem definir as medidas para mitigação dos danos.

No entanto, com a utilização da internet, compras online, transferência virtuais e outros meios tecnológicos, criou-se uma dificuldade para atuar na segurança de dados, tendo em vista a abrangência e os domínios de redes globais, que combinados com fatores não perceptível, forma

um perfil não rastreavel capaz de ocasionar violação às diretrizes básicas da legislação, que mesmo com ações posteriores não conseguem excluir os inúmeros registros de pessoas e organizações que coletaram os dados, lesionando a confidencialidade das informações (SAAD, 2021)

Destaca-se que as obrigações aos controladores e operadores, devem ser observados desde a coleta dos dados até seu descarte, assim o artigo 46 da LGPD, introduziu o conceito de privacy by design, sendo a incorporação pelas empresas nos serviços e produtos, na qual dispõe a proteção da privacidade no centro de todo o desenvolvimento corporativo.

Embora, a legislação tenta dirimir os riscos da atividade, os prejuízos causados pelo vazamento de informações são altos, e perpassam pela inadequação do sistema de proteção, perda de credibilidade e de clientes, ocasionado uma ruptura na imagem da empresa, impossibilitando, muitas vezes de concorrer no mercado corporativo. (SAAD,2021)

Portanto, a LGPD concebeu obrigações aos agentes de tratamento de dados, para que se delimite a finalidade da utilização dos dados desde o início da concepção, devendo o controlador confeccionar relatório de impacto a privacidade, utilizando de métodos para a captação da operação do ciclo de vida dos dados, observando as mediadas adotada para aumentar a segurança e mitigar o risco do tratamento das informações, conforme artigo 3 da LGPD.

O último pilar, considerado como a responsabilidade dos agentes na incidência de ocorrência de danos derivados do tratamento de dados. A LGPD consagrou a natureza do tratamento, limitando os parâmetros ao artigo 7° da lei, nas 10 hipóteses dos incisos, vinculados a finalidade da captação dos dados, consoante prevê o artigo 6°, inciso I, II, da LGPD.

A legislação tem como regra o descarte (eliminação) dos dados ao fim do tratamento da operação (art. 16), com o intuito de mitigar os riscos presente no tratamento de dados, principalmente, no que concerne à limitação das hipóteses de tratamentos para não lesionar os direitos dos titulares.

Nos casos, em que mesmo após o término de vida útil dos dados, as empresas podem, quando permitido, armazenar dados que em situação incidentais serem objetos de violação, principalmente nos casos de vazamento, que podem ocorrer, quando não autorizados pelo titular

ou controladores, serem acessados, captados, compartilhados pela internet, para outros sujeitos ou empresas.
Assim, a Lei Geral de Proteção de dados Pessoais, em especial em seu artigo 42, dispõe que o controlador ou operador, quando realizar o exercício do tratamento de dados pessoais, vem

a ocasionar dano patrimonial, moral, individual ou coletivo em detrimento a aplicação da legislação, é obrigado a repará-lo, definindo a responsabilidade de forma objetiva.
Embora, a responsabilização objetiva não é necessária a demonstração de culpa do controlador ou operador. Faz mister esclarecer que o operador, só será responsabilizado quando os atos praticados forem contrário à legislação, ou às instruções que foram fornecidas pelo controlador. (MENDES, DONEDA, 2018)
Ainda, a legislação prevê exceções a responsabilidade objetiva (art. 43), sendo: quando o agente demonstrar que não realizou o tratamento de dados pessoais que foi atribuído, ou quando não houve violação da segurança ou a legislação, e por fim, quando for por culpa exclusiva do titular ou de terceiros.
Porém, o cenário que é vislumbrado no Brasil nos casos de vazamento de dados, é que as violações pelas instituições vêm ocorrendo, majoritariamente, sob ataques deliberados de hacker, ou falha de segurança dos controladores dos dados. (SAAD, 2021)
Dessa forma, é necessário adotar medidas para dirimir os riscos da atividade, e possibilitar o discernimento das informações acerca dos perigos de vazamento de dados, tendo em vista que a tendência é aumento significativo das violações vinculados com a crescente tecnológica. Assim, as empresas devem implementar mecanismos para a segurança das informações.

5 O COMPLIANCE EMPRESARIAL COMO INSTRUMENTO DE PROTEÇÃO DE DADOS NA ESFERA EMPRESARIAL

Em decorrência das constantes violações aos dados armazenados em provedores privados, a tutela ao direito à privacidade nos meios tecnológicos, já era pauta de debate na legislação brasileira, e já existiam mecanismos para a proteção, como: a proibição de direcionamento dos provedores em relação ao compartilhamento de dados, bem como a inibição ao monitoramento nos navegadores de internet.
Vinte e seis bilhões de dados foram vazados no Brasil em 2019, de acordo com pesquisas realizadas pelo Massachusetts Institute of Tecnology ? MIT, possibilitando a utilização de números telefônicos, score de crédito, endereço eletrônico, fotos, números de identificações e outros dados pessoais, para o cometimento de crimes cibernéticos, e a violação aos direitos dos titulares.
A utilização e uso dos dados pessoais por pessoa física ou jurídica, com sede no Brasil ou não, devem se atentar as normas gerais de proteção aos dados brasileiro, segundo Frazão, Oliva e

Abilio (2020), é a necessidade de conferir a efetividade aos direitos e prevenir a violação aos dados, através da implementação de mecanismo de compliance, como uma ferramenta capaz de promover a adequação das atividades aportadas pelas empresas.
Assim, os controladores e operadores poderão formular regras de boas práticas e governança (Art. 50), que contenha as disposições de organização interna, o regime de funcionamento, as operações, o canal de comunicação entre os encarregados e os titulares dos dados, e o procedimento de segurança.
Nessa perspectiva, considerando que a maioria das tratativas de dados perpassam por meios digitais, deve-se adotar sistema para mapear os riscos, e implementar mecanismos para minorar as vulnerabilidades apontadas pelos programas, através da alta administração, do código de ética, para proteger os dados pessoais dos titulares. (PESSOA, 2021)
Existem inúmeras formas de ocorrer o vazamento de dados, sendo através de ataques cibernéticos, sequestro de conta, furtos de dados, compartilhamento de dados por agentes ou ex-agentes da empresa, erro ou negligência, entre outros, que podem ser para adquirir dados de nomes, CPF, celulares, endereços, dados financeiros, senhas, registro de saúde ou credenciais de acesso. (SAAD, 2021)
Desse modo, para realizar o mapeamento dos problemas que as corporativas podem enfrentar, é necessário identificar os fluxos e processos de informação que percorrem os sistemas, que irão auxiliar na tomada de decisão pelas empresas. (NASCIMENTO, 2020)
A alta administração deverá colaborar ativamente no programa de compliance, seja monitorando as investigações e intervenções em situação para estabelecer controles internos em conformidade com a legislação, bem como possibilitar a interdependência dos setores para realizar as atividades designadas para o tratamento de dados (PESSOA, 2021).
Com a elaboração do código de ética pela organização possibilitará o treinamento regular das equipes, responsáveis pela tecnologia da informação, para enraizar a cultura corporativa da boa governança, com a finalidade de assegurar o respeito ao programa de compliance (NASCIMENTO, 2020)
Nesse contexto, para manter uma boa relação com seus clientes, as organizações devem instalar canais de comunicação, para que os titulares dos dados possam contatar os encarregados responsáveis pelos armazenamentos dos seus dados, e exerçam seus direitos sobre as informações contidas nos provedores. (PESSOA, 2021).

Desse modo, quando se trata de concretização a alteração cultural coportariva é preciso realizar o alinhamento dos funcionários com o código de ética, com política de privacidade, para fins de efetividade do programa de compliance de dados. (PESSOA, 2021).

5.1 A IMPLEMENTAÇÃO DE MECANISMOS DE GOVERNANÇA DE DADOS PESSOAIS

Para a efetividade da legislação em relação ao tratamento de dados, a LGPD direciona um capítulo para implementar o programa de governança em privacidade, com a finalidade das empresas adotarem medidas técnicas, para fins de proteção e segurança dos dados pessoais.

(PESSOA, 2021)
A governança em privacidade, pode ser conceituada como um conjunto de regras e práticas positivas a serem implementadas pelos agentes de tratamento, e encontra-se em conformidade com as políticas de compliance empresarial, com o objetivo de gerir os dados das empresas para estabelecer um diferencial competitivo aos negócios. (KOEPSEL,2020)
O programa integra o aperfeiçoamento do procedimento de utilização dos dados, com os requisitos pré-estabelecidos na implementação dos softwares, com a finalidade de gerir de forma otimizada os dados para preencher as diretrizes da legislação. (SAAD, 2021)
A Lei Geral de Proteção de Dados Pessoais dispôs que os controladores e operadores poderão adotar programas de governança em privacidade, que devem ser implementados com o mínimo, (art. 50, § 2°, I): a) o comprometimento dos agentes de tratamento com as políticas internas que devem garantir o cumprimento das normas e regras de boas práticas; b) que aplicação seja de forma uniforme para todo a operação de tratamento de dados; c) que a governança seja adaptativa as estruturas da empresas, sendo compatível com a densidade dos dados e operação; d) como implementar políticas de salvaguardas em relação aos titulares dos dados; e) tenha como objetivo estabelecer uma relação de confiança com sujeitos dos dados, estabelecendo situações de transparência e que possibilite a atuação do titular; g) que conte com planos de respostas a incidentes e remediações; h) seja continuamente atualizado sua base.
Nesse aspecto, devem ser adotadas medidas administrativas para que as instituições, em conformidade com a legislação, apliquem estímulos para assegurar as informações armazenadas pelas empresas, com a adoção de orientações internas que respeitem as diretrizes que inclua o uso

minimizado ou a anonimização das informações, desde a coleta dos dados, conforme artigo 46 da LGPD.
Com o mapeamento das atividades, é importante verificar: O que são esses dados?; de que forma foram coletados ?; quem são os coletores ?; existe relação entre os dados e atividade realizada ?; O que pode ocorrer com esses dados ao serem coletados? E, como são descartados da gestão organizacional da empresa? (NASCIMENTO, 2020). Dessa forma, para adotar medidas compatíveis com os riscos alertados pelos sistemas para a proteção de dados nas organizações privadas, é necessário possuir conhecimento do caminho realizado inerentes ao ciclo de vida útil dos dados.
Embora, a legislação já estabeleça diretriz mínima para o tratamento de informação, a Autoridade Nacional de Proteção de Dados - ANPD, poderá, ainda, determinar padrões técnicos para serem implementados pelo programa de governança em privacidade, devendo ser observado a qualidade de dados, as especificações do tratamento e status tecnológico, em especial a proteção aos dados sensíveis disposto na legislação. (NASCIMENTO, 2020)
Muito embora, a lei geral de proteção de dados, apenas delimita as características e os requisitos mínimos que os operadores deverão tomar para desenvolver um compliance na organização das empresas privadas em consonância com a legislação, porém não impõe um modelo específico para integração de um programa nas corporativas. (PESSOA, 2021)
Assim, para Saad (2021), as medidas técnicas que podem ser adotadas pelos agentes de

tratamento de dados, são: i) o uso de firewalls, sendo um mecanismo de segurança que coleta os dados em conformidade com as regras pré estabelecido para análise de tráfego de rede, delimitando as operações de compartilhamento e captação de informações a serem cumpridas; ii) a utilização de antimalware, que consiste na proteção contra vírus que é capaz de fragilizar o sistema, apagar dados e infectar outros arquivos; iii) a utilização de criptografia dos dados, que possibilite quando ocorrer situações incidentais a não identificação do titular do direito.
Já para Fernandes e Abreu, (2014) defendem a implementação de frameworks como a DAMABOK e COBIT, para o gerenciamento de dados, pois tem como meta principal a delimitação do escopo das atividades, as funções envolvidas no tratamento e as interações a serem executadas pelo software, com a finalidade de proteger a privacidade em ambientes corporativos que gerenciam o armazenamento de informações aplicados na prevenção à fraude.

Segundo Carvalho (2021), a integração do software, através das boas práticas estabelecidas pela legislação, poderá aprimorar os aspectos de proteção à privacidade e prevenção a fraude do tratamento de coleta de dados. Tendo em vista, que os frameworks, podem balizar as métricas de qualidade dos dados que indicam uma utilização adequada e otimizada, e aponta a melhor proteção da privacidade.
Com a melhoria de processo de governança para o tratamento de dados, estabelece uma divisão entres as operações que possibilita uma automatização do ciclo de vida dos dados (coleta, utilização, armazenamento e exclusão), capaz de gerar relatório de risco, para o auxílio da tomada de decisão com o intuito de gerir de forma adequada o tratamento de dados. (CARVALHO, 2021)
Neste parâmetro, os programas de compliance com a implementação de frameworks, podem responder questionamento acerca do procedimento de tratamento de informação, dispondo de quais práticas relacionadas à governança, privacidade e segurança de dados, apresentam melhor benefício para o tratamento de dados pessoais. (CARVALHO, 2021)
Ademais, os controladores e operadores deverão adotar medidas, como o Relatório de Impacto ? DPIA), que corresponde a avaliação dos riscos e impactos relacionados com o tratamento de dados pessoais, além da anonimização, da transparência e do sigilo, deverão delimitar prazos para retenção de dados e aderir políticas seguras de informação acerca da operação de tratamento. (SILVA, 2022)
Após realizar a implementação e observância das estruturas mínimas estabelecidas pela LGPD, é necessário adotar um programa de gerenciamento de vulnerabilidades, com atualizações constantes e autocorreções alinhados com as boas práticas de atividades cotidianas, com a finalidade de proteger os dados pessoais, e promover um ambiente corporativo adequado para realizar o tratamento de dados. (SAAD, 2021)
No entanto, ao verificar que houve vazamento de dados, seja pelo recebimento de notificação ou pela veiculação na mídia, os agentes de tratamentos deverão identificar quais dados vazaram e realizar o procedimento estabelecido no programa de compliance de segurança, além de notificar as instituições. (Art. 48, caput).
De acordo com MIT, o prazo entre a comunicação à autoridade competente e a ocorrência do fato ilícito ultrapassa 200 (duzentos) dias em média, sendo umas das preocupações para a

efetividade da legislação, e a redução dos danos causados aos titulares dos bens imateriais.

A Lei Geral de Proteção de Dados, dispõe que nas situações que ocorrer a probabilidade de riscos ou violação aos direitos dos titulares, tem como obrigação do encarregado a comunicação à autoridade nacional e ao titular do dado (art. 48, caput). Sendo que o contato deve ser em período razoável (art. 48, § 1º), contendo a natureza dos dados dos titulares atingindo (art. 48, § 1º, I).
Em decorrência dos possíveis incidentes, a LGPD determinou critério para aplicação de sanções, em casos de vazamento de dados, observando as situações específicas de cada caso, disposto no art. 52, § 1º. Assim, deve ser considerada a avaliação da gravidade, a natureza das informações e do dano ocorrido (incisos I e VI), sendo necessário para este caso, tendo em vista que o compartilhamento indesejado de dados sensíveis pode ocasionar danos irremediáveis para os titulares.
Portanto, existe a necessidade da adesão aos mecanismos e técnicas para promover a efetividade dos programas internos com a finalidade de mitigar os danos, assim, a implementação de boas práticas e governança têm como fator o cumprimento da legislação, por meio de medidas de segurança. Entende-se, que a proteção integral contra falhas que possibilitam a ocorrência de ilícitos não é possível, porém essas diretrizes reduzem as possibilidades de existir desvios de condutas e criar salvaguardas para identificação dos incidentes, de forma eficaz, rápida e adequada.

6 CONSIDERAÇÕES FINAIS

A partir da permissão ao acesso dos dados pessoais, as informações coletadas passaram a integralizar as redes de tratamento de dados, tornando-se alvo de ataques cibernéticos, contribuindo para o aumento da intercorrência no ambiente corporativo, tornando-se o gerenciamento de informação um dos diferenciais no desenvolvimento do negócio.
Nesse contexto, foi imperativo o surgimento de leis que protejam os dados dos cidadãos, e que limitem a gestão das entidades públicas e privadas em relação as informações coletadas, transformando o sistema organizacionais, como compliance, em ferramentas de efetivação das normas éticas e legais. Assim, a implementação do programa alinhado com a governança corporativa é capaz de integralizar o corpo de normas internas com o intuito de adequar a legislação brasileira e criar uma cultura corporativa.
Dentro do programa de compliance, a administração em conjunto com a gestão da empresa, poderá implementar ao plano diretor, a utilização de software, sendo este capaz de possibilitar a automatização do ciclo de vida útil dos dados para realizar o auxílio da tomada de decisão, com o intuito de mitigar os possíveis danos decorrentes da violação aos dispositivos da Lei Geral de Proteção de Dados Pessoais.
Nesse sentido, para realizar uma proteção extensiva aos direitos dos titulares dos dados, a

LGPD integrou ao seu corpo de normas-condutas a serem adotadas pelos operadores do tratamento de dados, com escopo de preservar a integralidade, a qualidade e o sigilos dos dados, tendo como consequência da violação, a majoração de sanções pecuniárias.
Embora, o vazamento de dados ocorra de forma ordenada, a implementação de sistema de segurança nas corporações implica na diminuição de situações incidentais por erro humano, ou inadequação dos programas empresarias, assim, devendo a gestão ensejar esforços para que a proteção dos dados seja preservada, desde a concepção do serviço.
Para a efetivação da Lei Geral de Proteção de Dados Pessoais, as empresas devem realizar a adequação de medidas de boas práticas e governança em privacidade para mitigar os possíveis danos decorrente da violação aos dados em provedores privados. Mesmo que a proteção aos dados de forma concreta não seja possível, as adoções de mecanismo de segurança podem atenuar as sanções e as perdas aos titulares dos dados.

REFERÊNCIAS

BARATA, André Mantola. Governança de dados em organizações brasileira: uma avaliação comparativa entre os benefícios previstos na literatura e os obtidos pelas organizações. 2015. Dissertação (Mestrado em Sistema de Informação) - Universidade de São Paulo, São Paulo, 2015.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, [2022]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 15 abr. 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidente da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 abr. 2023.

BERTOCCELLI, Rodrigo de Pinho. Compliance. In: CARVALHO, André Castro et. al. Manual de compliance. Rio de Janeiro: Forense, 2019. p. 35.

CANDELORO, Ana Paula; RIZZO, Maria Balbina Martins De; PINHO, Vinícius (Coord). Compliance 360: riscos, estratégias, conflitos e vaidades no mundo corporativo. São Paulo: Trevisan, 2012.

CARVALHO, A. P. Proposta de um framework de compliance à Lei Geral de Proteção a Dados Pessoais (LGPD): um estudo de caso para prevenção a fraude no contexto de big data. 2021. Dissertação (Mestrado em Engenharia Elétrica) - Universidade de Brasília, Brasília, 2021.

CARVALHO, Andre Castro. Manual de compliance. 3. ed. Rio de Janeiro: Forense, 2021.

CASAES, Júlio César Costa. Governança de dados abertos governamentais: frameworks conceitual para as Universidades Federais, baseada em uma visão sistemática, 2019. Tese (Doutorado em Engenharia e Gestão do Conhecimento). Universidade Federal de Santa Catarina, Florinaóplis, 2019.

DATA GOVERNANCE INSTITUTE (DGI). Definitions of data governance. 2017. Disponível em: http://www.datagovernance.com/adg_data_governance_definition. Acesso em: 01 mai. 2023.

ENDEAVOR DO BRASIL. Prevenindo com o Compliance para não remediar com o caixa. In: ENDEAVOR. [S. l.], 26 abr. 2017. Disponível em: https://endeavor.org.br/pessoas/compliance/. Acesso em: 15 mar. 2023.

ESPÍNDOLA, P. L.; SALM JUNIOR, J. F.; ROSA, F.; JULIANI, J. P. Governança de dados aplicada à ciência da informação: análise de um sistema de dados científicos para a área da saúde. Revista Digital de Biblioteconomia & Ciência da Informação, Campinas, v. 16, n. 3, p. 274-298, 2018.

FERNANDES, Aguinaldo Aragon; DE ABREU, Vladimir Ferraz. Implantando a governança de TI: da estratégia à gestão de processos e serviços. 4. Ed. Rio de Janeiro: Brasport, 2014.

FRAZÃO, Ana. Programas de compliance e critérios de responsabilização de pessoas jurídicas por ilícitos administrativos. In: ROSSETTI, Maristela Abla; PITTA, Andre Grunspun. Governança corporativa: avanços e retrocessos. São Paulo: Quartier Latin, 2007. p. 42

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. A Lei Geral de proteção de Dados Pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

HONÓRIO, Roseli. Modelo conceitual de governança de dados como suporte à governança do conhecimento organizacional. 2022. Dissertação (Mestrado em Engenharia e Gestão do Conhecimento) - Universidade Federal de Santa Catarina, Florianópolis, 2022.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC). Guia das melhores práticas de governança para cooperativas. São Paulo, 2015. Disponível em http://www.ibgc.org.br/ userfiles/files/2014/files/CMPGPT.pdf

JOHNSON, Ralph E.; RUSSO, Vincent. Reusing object-oriented designs. Relatório Técnico da Universidade de Illinois, UIUCDCS 91-1696, 1991.

KLEINDIENST, Ana Cristina. Grandes temas do direito brasileiro: compliance. São Paulo: Almedina Brasil, 2019

KOEPSEL, Alice de Medeiros. Adoção e efeitos dos programas de compliance à luz da Lei Geral de Proteção de Dados Pessoais. 2020. Monografia (Graduação em Direito) -Universidade do Sul de Santa Catarina, Florianópolis, 2020.

LIMA, C., BASTOS, R. C. A criação de conhecimento apoiada pela governança de dados. In: CONGRESSO INTERNACIONAL DE CONHECIMENTO E INOVAÇÃO, 2019, Santa Catarina. Anais eletrônicos [...]. Santa Catarina Disponível em: https://proceeding.ciki.ufsc.br/index.php/ciki/article/view/647. Acesso em 10 Mar. 2023.

MARTIGNAGO, Deisi et al. Governança de dados aplicado no processo de catalogação. Revista Brasileira de Biblioteconomia e Documentação, São Paulo, V.15, n. 2, 2019.

MENDES, Gilmar Ferreira. Curso de direito constitucional. 2. ed. São Paulo: Saraiva, 2008.

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. São Paulo: Revista de Direito do Consumidor, 2018.

NASCIMENTO, Suellen Lima do. A lei Geral de Dados Pessoais e a Adoção dos Programas de compliance na sociedade da Informação. 2020. Monografia (Graduação em Direito) - Centro Universitário de Brasília, Brasília, 2020.

PESSOA, Larissa Rocha de Paula. Os desafios da Governança de dados e a realidade cultural brasileira. 2021. Dissertação (Mestrado em Direito) ? Universidade Federal do Ceará, Fortaleza, 2021.

PINTO, S. C. C. S.. Composição em Web Frameworks, 2000. Tese (Doutorado em Informática) Pontifícia Universidade Católica do Rio de Janeiro, Rio Janeiro, 2000.

PROSSER, William L. Privacy. California Law Review. California, v. 48, n. 3. p. 383 ? 423, agosto, 1960.

RÊGO, Bergson Lopes. Gestão e governança de dados: promovendo dados como ativo de valor nas empresas. 1. ed. Rio de Janeiro: Brasport, 2013,

ROQUE, Pamela Romeu. Estudos aplicados de direito empresarial: LL.C. em direito empresarial. São Paulo: Almedina, 2019.

SAAD, Carolina de Oliveira. A lei geral de proteção de dados pessoais e incidentes de segurança: regulação e prática de vazamento de dados, 2021. Monografia (Graduação em Direito). Fundação Getúlio Vargas. Rio de Janeiro, 2021.

SANTANA, Ricardo Cesar Gonçalves. Ciclo de vida dos dados e o papel da ciência da informação. In: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO. 14., 2013. Florianópolis. [?]. Florianópolis: UFSC, 2013. Disponível em: http://enancib2013.ufsc.br/index.php/enancib2013/%20XIVenancib/paper/viewFile/284/319. Acesso em: 13 mar. 2023.

SILVA, Ana Laura Fonseca. O papel das Soft Skills na implementação efetiva dos programas de compliance com foco na adequação à Lei Geral de Proteção de Dados ? Lei N° 13.709/18. 2022. Monografia (Graduação em Direito) - Universidade Federal de Ouro Preto, Ouro Preto. 2022

SILVA, Eggon João da. A defesa da ética e transparência. In: VENTURA, Luciano Carvalho. Governança corporativa. São Paulo: Saint Paul Editora, 2005, página 259.

TERRA, Priscila de Mello. A influência da governança de dados na gestão estratégica, 2017. Monografia (Bacharelado em Sistema de Informação) - Universidade Federal Fluminense, Niterói, 2017.

VAZAMENTO de dados aumentaram 493% no Brasil, segundo pesquisa do MIT.VEJA, São Paulo, 24 fev. 2021. Sociedade. Disponível em: https://vocesa.abril.com.br/sociedade/vazamentos-de-dados-aumentaram-493-no-brasil-segundo-pesquisa-do-mit. Acesso em: 15 mar. 2023.

VIEIRA, Tatiana Malta. O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante da tecnologia da informação. Porto Alegre: Sergio Antonio Fabris Editor, 2007.

==========

Arquivo 1: TCC - A IMPORTÂNCIA DO COMPLIANCE NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA - WESLEY VICENTE.pdf (8805 termos)
Arquivo 2: https://www.linguee.com.br/ingles-portugues/traducao/this+work+aims.html (2706 termos)
Termos comuns: 15
Similaridade: 0,13%
O texto abaixo é o conteúdo do documento TCC - A IMPORTÂNCIA DO COMPLIANCE NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA - WESLEY VICENTE.pdf (8805 termos)
Os termos em vermelho foram encontrados no documento https://www.linguee.com.br/ingles-portugues/traducao/this+work+aims.html (2706 termos)

==========

WESLEY VICENTE DA SILVA

A IMPORTÂNCIA DO COMPLIANCE EMPRESARIAL NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA

SALVADOR
2023

WESLEY VICENTE DA SILVA

A IMPORTÂNCIA DO COMPLIANCE EMPRESARIAL NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA

Artigo apresentado como requisito parcial para obtenção do título de Bacharel em Direito pela Universidade Católica do Salvador.

Orientador: Prof. Darlã Conceição Santos.

SALVADOR
2023

A IMPORTÂNCIA DO COMPLIANCE EMPRESARIAL NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA

Wesley Vicente da Silva1
Darlã Conceição Santos2

RESUMO: No cenário de exploração das informações como mercadoria econômica, os dados pessoais coletados por empresas privadas tornaram-se fator de tutela legislativa. Assim, surgiu a necessidade de organizar os setores privados para adequar aos moldes da Lei Geral de Proteção de Dados Pessoais ? LGPD, com o intuito de proteger a privacidade, como direito autônomo e fundamental para a tutela da pessoa humana, destacando os programas de compliance aliados as boas práticas e governança de dados. Nesse contexto, a fim de consolidar os mecanismos técnicos de segurança para a efetividade da legislação com a finalidade de mitigar os casos de vazamento de dados pessoais, a LGPD implementou medidas administrativas para inibir incidentes decorrentes das condutas infratoras a legislação. Desse modo, este trabalho tem como objetivo demonstrar a importância dos programas de compliance para a proteção aos direitos dos titulares dos dados, visando o cumprimento do ordenamento jurídico. Valendo-se do método hipotético-dedutivo, com abordagem qualitativa, utilizando da revisão bibliográfica de livros, legislação, artigos, dissertações e teses concernente à tutela de dados pessoais no Brasil para o desenvolvimento do presente artigo.

PALAVRAS-CHAVES: Compliance Empresarial. Governança corporativa. LGPD. Vazamento

de dados.

ABSTRACT: In the scenario of exploitation of information as an economic commodity, personal data collected by private companies have become a factor of legislative protection. Thus, the need arose to organize the private sectors to conform to the General Law for the Protection of Personal Data - LGPD, in order to protect privacy, as an autonomous and fundamental right for the protection of the human person, highlighting compliance programs allied with good practices and data governance. In this context, in order to consolidate the technical security mechanisms for the effectiveness of the legislation with the purpose of mitigating cases of leakage of personal data, the LGPD implemented administrative measures to inhibit incidents arising from conducts that violate the legislation. Thus, this work aims to demonstrate the importance of compliance programs to protect the rights of data subjects, aiming at compliance with the legal system. Taking advantage of the hypothetical-deductive method, with a qualitative approach, using the bibliographic review of books, legislation, articles, dissertations and theses concerning the protection of personal data in Brazil for the development of this article.

KEYWORDS: Corporate Compliance. Corporate governance. LGPD. Data leak.

1
Discente do curso de Direito da Universidade Católica do Salvador.
2
Mestre em Direito, Docente na Universidade Católica do Salvador.

1 INTRODUÇÃO

A nova moeda de troca não é apenas aquela que podemos ver, quantificar ou converter. Os moldes do mercado financeiro mudaram, sendo em questão material ou ao produto que eles precificam, postulando um novo aparato ao objeto contratual: os dados.
Muito embora, os dados pessoais, ainda para muitos, são apenas informações deslocadas acerca de fatores específicos, atualmente, podem ser conceituados como um conjunto de indicadores, regrados por um complexo condensado de informações em um fluxo crescente tangencial.
Os dados da grande massa acabam gerando indicadores que podem ser balizados e influenciados de acordo com os detentores dessa informação, apenas apartado em blocos de informações não são considerados como vetores orçamentários. Porém, direcionados para uma finalidade ordenada tem o condão de influenciar o interesse social.
Dito isso, os mecanismos postos pelo Reino Unido para possibilitar uma estruturação normativa para organizar e gerir os dados dos indivíduos, foi crucial para a criação em outros países, como no Brasil, onde instituiu-se a Lei Geral de Proteção de Dados Pessoais (LGPD). Muito

embora, a lei brasileira trouxe um arcabouço de normas reguladoras e sanções aos casos de tratamento de dados, que não foram abarcados com o marco da internet, os dados em uma visão macro constitucional já eram de forma genérica tutelados pela Constituição Federal de 1988.
Todavia, apenas a sanção da LGPD não seria, isoladamente, capaz de coibir as violações ao tratamento de dados na esfera privada, mas sim a necessidade de uma regulamentação do ciclo de vida das informações, que além de estipular os dados que podem ser utilizados ou até quando podem ser armazenados, estabelecer expressamente no bojo da norma como deve ser a proteção na operação do tratamento de dados.
De forma efêmera, conclui-se que a legislação pode delimitar os alicerces capazes de ensejar uma fiscalização, sendo estas através de mecanismo de gerenciamento de atividades, políticas de condutas e implementação de governança de dados, pois os dados hackeados ou vazados de forma isoladas, não seria possível identificar dados sensíveis, muitos menos individualizar o sujeito.
Portanto, o gerenciamento dos dados em provedores de armazenamento pode ter os riscos reduzidos de acordo com a realização de medidas de compliance para dirimir os impactos na

atividade empresarial, como também para tutelar os dados, cada vez mais acentuado como um produto orçamentário.

2 COMPLIANCE EMPRESARIAL

A criação do compliance está entrelaçado sob o cenário econômico-social, assim, sua implementação como sistema de organização foi instaurado e aprimorado a partir dos problemas práticos estruturais para gerir uma boa governança, com intuito de assegurar a proteção e o controle que garante a qualidade do negócio.
A utilização do termo foi inicializada no mercado financeiro, especialmente após a criação do Banco Central em 1913 nos Estados Unidos da América, com a necessidade de um sistema econômico ajustável e estável. Só após 1960, com a regularização da Securities and Exchange Commission (SEC), que houve a necessidade de implementação do compliance como um programa para a integração dos procedimento, controle e monitoramento de operação interna. (CARVALHO, 2021)
Em 1977, com a Convenção Relativa à Obrigação de Diligência dos Bancos Suíços, estabeleceu os modelos auto regulatórios, com adequação de condutas e processos internos, na qual a infração tem como consequência à aplicação de sanções. (CARVALHO, 2021)
Só após esse processo de amadurecimento histórico, que o Brasil teve a necessidade de competir em escala global, implementado novos processos de segurança no sistema financeiro brasileiro.
Pode-se concluir que, após a globalização com o fenômeno da criação dos dados estruturais, houve a potencialização das informações adquiridas por meio de provedores, classificadas, atualmente, como fonte econômica de um produto quantificativo e qualitativo, ao qual possibilita uma utilização como um produto do sistema financeiro.
Nesse sentido, em decorrência de ataques cibernéticos em provedores de informações

massificadas conduziram a sociedade na aplicação de institutos de melhoramento, como o compliance e suas interfaces para proteger no ambiente corporativo os dados massificados recebidos em seus provedores.

2.1 O CONCEITO DE COMPLIANCE

Antes de enveredar sob o conceito de compliance na esfera privada, é oportuno compreender o seu significado. Nesse contexto, a palavra compliance advém do verbo inglês, to comply, que pode ser definida como conformidade. O instituto deve ser aplicado como plano principal de uma diretriz pré-estabelecida para ser dirigida a todos capazes de enfrentar a finalidade destinada. (BERTOCCELLI, 2019)
Nesse parâmetro, pode ser traduzida como:

Comply, em inglês, significa ?agir em sintonia com as regras?, o que já explica um pouquinho do termo. Compliance, em termos didáticos, significa estar absolutamente em linha com normas, controles internos e externos, além de todas as políticas e diretrizes estabelecidas para o seu negócio. (ENDEAVOR DO BRASIL, 2022, n.p)

O compliance pode-se ser definido de forma técnica como um conjunto de normas padronizadas, sob um viés ético e legal, na qual após estruturação será a matriz orientadora para o comportamento organizacional da instituição ao qual atuará no mercado, como também irá reger as atividades dos colaboradores. Dessa forma, sendo um instrumento hábil a controlar o risco de imagem, a normatização legal, chamados de riscos de compliance, as que recaem nas instituições no decorrer da sua atividade laboral. (CANDELORO, 2012).
Superada a barreira terminológica, a finalidade do compliance tem como escopo o gerenciamento adequado do risco de atividades, verificar adequadamente as normas éticas e legais, e estudar os possíveis danos tangenciais. Dessa forma, esses elementos visam a redução de perdas e danos, como também amplifica a cultura e fortalecimento corporativo nos moldes aos padrões exigidos, seja esse por lei ou na tentativa de dirimir o risco do serviço prestado.
Portanto, segundo a doutrinadora Frazão (2007, p. 42), destina-se em sua obra que o compliance é como:
(...) conjunto de ações a serem adotadas no ambiente corporativo para que se reforce anuência da empresa à legislação vigente, de modo a prevenir a ocorrência de infrações ou, já tendo ocorrido o ilícito, propiciar o imediato retorno ao contexto de normalidade e legalidade.

Nessa mesma linha de pensamento, de acordo com os autores da obra Compliance 360° (2012, n.p), referem-se o compliance a:

Um conjunto de regras, padrões, procedimentos éticos e legais que, uma vez definido e

implantado, será a linha mestra que orientará o comportamento da instituição no mercado em que atua, bem como as atitudes de seus funcionários; um instrumento capaz de controlar o risco de imagem e o risco legal, os chamados ?riscos de compliance?, a que se sujeitam as instituições no curso de suas atividades.

Pode-se concluir que o conceito de compliance, em uma esfera macro, é um aglomerado de regras pré-estabelecidas através de um instrumento perpetuado por técnica de desenvolvimento, capaz de dirimir riscos e danos das atividades devolvidas pelo plano diretor.
Muito embora, o instituto "compliance" tem uma definição extensiva e não tem como fim apenas o cumprimento da legislação e de condutas éticas, pode ser compreendida também como um instrumento de diminuição de riscos, desenvolvimento corporativo sustentável e subsequentes segmentos empresariais de negócio. (ROQUE, 2019)
O compliance além de estar associado tradicionalmente a uma perspectiva organizacional aos comandos administrativos, pode ser vinculada também a uma visão de uma sociedade digital 4.0, devendo não só apresentar o compliance empresarial na esfera de redução de risco à imagem, mas sim, em uma abordagem de pré-orientação e implementação de desenvolvimento aos moldes legislativo de proteção aos dados, como objeto principal de estudos.
Portanto, é necessário a elaboração do projeto de compliance em uma visão lógica, a modo de compreender os objetivos e os componentes da aplicação do programa. Posteriormente, superado os obstáculos, aplica-se os estudos de riscos a boa governança corporativa com a implementação de programas de governança de dados objetivando auxiliar o controle de informações em conformidade aos padrões da corporação, e mitigar os danos da empresa.

2.1.1 AS GOVERNANÇAS CORPORATIVAS E A IMPLEMENTAÇÃO DOS PROGRAMAS DE COMPLIANCE

Em linhas gerais, o Instituto Brasileiro de Governança Corporativa ? IBGC (2015, n.p) discrimina o conceito de Governança Corporativa, como: ?Sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas. ?
O sistema da governança corporativa está associado ao desenvolvimento interno de uma empresa, seja ele entre a administração, sócios e funcionários, capaz de criar elos para uma estruturação de direção racional e acima de tudo nos moldes da ética e legislação.
Muito embora, a governança corporativa e o compliance sejam institutos que se assemelham em uma visão macro, os mesmos, diferenciam na aplicação prática, mas se complementam no objetivo final, sendo um instrumento para aplicação do outro.

A prática da governança corporativa, além de estimular o valor empresarial, pode-se concluir que estrutura de forma adequada a medida necessária para organizar a atividade empresarial, assim, não há que se falar em condutas prejudiciais. Por exemplo: empresários compreendem que para realizar uma instrumentalização segura aos seus sócios e administradores tendem a prejudicar o negócio empresarial, assim o autor Eggon João da Silva (2005, p.259) retrata que: ?A governança corporativa assegura tratamento equânime a todos os acionistas, inclusive minoritários, preferencialistas, nacionais e estrangeiros. Todos devem ter oportunidade de reparação caso venham a sofrer violação de seus diretores. ?

Nesse passo, as críticas ao sistema não são viáveis, tendo em vista a utilização de instrumento capaz de integralizar ao plano empresarial. Sendo assim, o programa de compliance visa amplificar a utilização de um sistema para garantir que todos possam participar de forma justa sob o aspecto legal, seja sócio ou administrador.

Em uma tangente geral, a implementação da governança corporativa ressoa em uma perspectiva segura, tanto internamente, seja auxiliando as avaliações das atividades executadas pelos sócios/administradores, quanto externamente, em relação à imagem da empresa, sendo este um fator primordial a empresas estruturadas no mercado.

A implementação da governança corporativa deve ser estruturada de acordo com as necessidades da empresa, devendo verificar o histórico de desenvolvimento do estabelecimento, pois, só a partir do status da empresa pode-se delimitar a estratégia possível para uma implementação segura e adequada. Sendo assim, um regramento mais rigoroso pode gerar consequências negativas e ineficazes, especificamente em estágios primários, pois em atividades inicias, as tomadas de decisões e a execução da atividade empresarial é primordial, sendo necessário, um aspecto negocial informal para realizar os objetivos da empresa, o que não se verifica quando existe prática de boa governança devidamente estruturadas no negócio. (KLEINDIENST, 2019)

Ao desenvolver da atividade da empresa, além da atenção a organização interna, sendo está um fator primordial da governança, ainda que no fim acabe tendo um aspecto externo por vislumbrar no mercado financeiro uma maior complexidade da entidade. O desenvolvimento da empresa, seja no faturamento, importação comercial, quantidade de funcionários, além dos controles a observância da legislação e regras internas, tendem à serem complexos, e, que necessita de ações maiores que a própria instituição empresarial, restando necessária a implementação de sistema organizacionais aos fluxos de informações. (KLEINDIENST, 2019)

Ultrapassado a esfera conceitual e instrumentalização da política de boas práticas de governança, cabe pontuar que as empresas que possuem fluxos de informações sensíveis, conforme estipula o artigo 50 da Lei Geral de Proteção de Dados Pessoais, os controladores e operadores são responsáveis pelo tratamento de dados, devendo criar planos de adequação a legislação.

Assim, ao confeccionar as regras de boas práticas, os controladores adjuntos com a administração devem estipular através da análise da natureza dos dados coletados, a probabilidade, a finalidade e o potencial de riscos das vantagens advindas dos tratamentos dos dados verificados. (NASCIMENTO, 2020)

É necessário pontuar que, os agentes de tratamento, após a autenticação da gravidade e sensibilidade dos dados aos riscos de operação, poderão estabelecer programa de governança em privacidade, sendo este, um instrumento amplo com normas de compliance, além dos aspectos operacionais.
Em relação ao programa de governança de privacidade, pode-se estabelecer como um aglomerado de normas-regras de boas práticas de governança, com a finalidade de executar ordens de natureza legal. (NASCIMENTO, 2020)
Portanto, os instrumentos do compliance em conjunto com a boa prática de governança, se consagram na identificação dos riscos e estruturação de medidas para a empresa, sendo respondida de forma adequada e proporcional ao suporte da tomada de decisão.
O Programa de compliance na esfera privada para análise de dados pessoais, com a finalidade de promover a segurança, deve ser constantemente monitorado e atualizado, com a implementação de ?salva vidas? em decorrência de avaliação de riscos à privacidade e o acometimento de vazamentos. (NASCIMENTO, 2020)
Portanto, os instrumentos e objetos referenciados demonstram a determinação de regras de governança no ambiente de operação de tratamento de dados pessoais, a modo que seja realizado uma estruturação nas empresas para que possibilitem a implementação de mecanismos de segurança, com a finalidade de dirimir os riscos da atividade empresarial na sociedade digital.

3 GOVERNANÇA DE DADOS

O mercado digital tem como principal ativo financeiro os dados, este considerado como ?matéria prima? de uma economia baseada no conjunto de informações, sendo que nos últimos anos, houve um aumento exponencial na coleta de dados por cooperativas, startups e novos nichos empresariais, tendo a finalidade de quantificar e gerencias os dados.
Dados, informações, conhecimento e sabedoria são os quatros estágios evolutivos da cadeia de informação, pode-se assim, compreender os dados como fatos ou registros em seu formato primário. (BEAL, 2014). Já a informação é entendida como os conjuntos processados de dados em um contexto aplicado (RÊGO, 2013). Muito embora, na sociedade da informação ?os dados são o novo petróleo?, apenas os dados isoladamente não são capazes de transformar em ativo financeiro, sendo necessário administrá-lo de forma eficaz, para que assim, as empresas adquiram vantagem competitiva.
Dessa forma, a governança de dados tem como principal objetivo atender as necessidades das empresas, ou seja, solucionar problemas, diminuir custos da administração, para que os dados transformem em saldo positivo para os negócios (TERRA, 2017).
O Data Governance Institute -DGI (2017, n.p) definiu governança de dados como ?um sistema de direitos de decisão e responsabilidades para processos relacionados à informação, executado de acordo com modelos acordados que descrevem quem pode realizar quais ações com quais informações e quando. ? Portanto, a utilização da governança de dados orienta quais os métodos deverão ser aplicados no ciclo de vida dos dados.

Uma das atribuições da governança é o acompanhamento da operação dos dados com a finalidade de gerir que as informações estejam alinhadas com os objetivos pré-determinados na coleta primária, além disso, é necessário assegurar que as informações estejam disponíveis para acesso, quando consultadas, gozar de qualidade, consistência, auditabilidade e segurança dos dados (ESPÍNDOLA, 2018).

No âmago da cadeia evolutiva da informação uma das preocupações dentro das organizações corporativas é o receio com a proteção das informações, ou seja, a capacidade das empresas no protagonismo da segurança com os provedores internos, tendo em vista a necessidade de conformidade com a legislação pátria.

A boa governança tem como objetivo aplicável à prática do controle dos processos de operação dos dados: a prevenção de situações adversas que podem gerar o comprometimento da integralidade dos dados adquiridos pelas organizações empresariais, que por sua vez, devem ter o condão de reforçar a confidencialidade das informações. (ESPÍNDOLA, 2018).

A integração do programa de governança de dados nas corporativas empresariais, tem como o esforço principal a organização de dados, que deve ser observado por um prisma basilar, ou seja, a aplicação dos princípios como limite legal e ético no ciclo de vida dos dados.

Para Rêgo (2013), os princípios são regulamentações para compreender aplicação da governança dos dados como linha direta para os negócios, sendo: (i) A gestão de dados estratégicos, tem o dever de vislumbrar as tomadas decisões por um coeficiente tático e operacional. (ii) A governança como instituição, ou seja, a governança de dados pode ser comparada como sistema governamental, na qual dispõe de legislação, execução e jurisdição; (iii) A governança de dados como um programa, devendo ser implementado como fator permanente, não apenas um projeto temporário. Ainda, pontua-se que os princípios da Governança de dados não são limitados, tendo uma orientação basilar a cada implementação de um sistema organizacional que deve ser observado pelo prisma ético e legal.

Assim, os princípios devem incumbir os papéis que a serem preenchidos pela gestão moldar os comportamentos das empresas para a aquisição, reserva e utilização dos dados conforme as normas e políticas da corporação (TERRA, 2017).

Coleta, armazenamento, recuperação e descartes, são as quatro etapas do ciclo de vida dos dados (SANTANA, 2013), ou seja, para a aquisição de dados pelas empresas, deverão observar a vida útil do dado para não incorrer na (in) responsabilidade da utilização indevida de informações dos seus provedores.

As fases do ciclo de vida dos dados devem ser observadas pela ótica de seis objetivos, sendo eles: a qualidade, a privacidade, os direitos autorais, a integração, compartilhamento e preservação dos dados (ESPÍNDOLA, 2018). Muito embora, a lei geral de proteção de dados implementou e traçou novos objetivos para a coleta de dados pessoais, cabe destacar que os objetivos vislumbrados na Governança de dados têm como parâmetro preliminar a tomada de decisão, na qual deve ser os negócios pautados nos moldes legais e éticos vigentes.

Nesse contexto, o controle de informações é necessário, tendo em vista que na sociedade da informação, cada vez mais o volume de dados é crescente, acarretando mais vazão e protesto

por políticas públicas para a preservação dos institutos, órgãos e empresas que detenham a

informação, sendo assim, necessário sistema de organização, softwares e hardwares capazes de processar as informações, criptografar e armazenar. (MARTIGNAGO, 2019)
Assim, para otimizar o ciclo de vida dos dados e garantir que os objetivos sejam preenchidos na estruturação do gerenciamento de dados, faz-se necessário a implementação de frameworks com o intuito de garantir que o procedimento seja cumprido com maior qualidade de informação e aproveitamento financeiro para a empresa, auxiliando a tomada de decisão para redução de risco para utilização de dados. (MARTIGNAGO, 2019)
Um Framework, segundo Johnson (1991), pode ser definida como um aglomerado de objetos que colabora entre si para que atinja um conjunto de obrigações para aplicação de um domínio especifico. Já para Pinto (2000), um framework é conceituado como um software incompleto criado para ser um objeto cujo estado e comportamento são definidos pela classe. Assim, o framework é uma concepção de uma arquitetura para um edifício de subsistemas e oferece o alicerce básico para criá-los.
Muito embora, os autores defendem uma conceituação distintas acerca da concepção de frameworks, pode-se verificar que ambas se complementam, tendo em vista que o framework é um sistema pré moldado, ou seja, é um programa com intuito de ser complementado através da finalidade a ser cumprida pela gestão empresarial, sendo instanciado por classes para categorizar os dados e ser alojado em hotspot, provedores físicos, capazes de armazenar as informações coletadas pelas empresas.
Portanto, para gerenciar os ativos de dados de forma complexa, ordenada e objetiva é necessário para proteção do procedimento do ciclo de vida dos dados, determinar os modelos de frameworks para o gerenciamento dos dados. Assim, para Carvalho (2021), podem ser apresentados três domínios CobiT, DAMA DMBOK e DGI Framework, sendo apenas dois destes observados para fomento deste artigo: (i) A DAMA (DAMA DMBOK), e (ii) CobiT.
A DAMA (Data Management Association) é uma associação sem fins lucrativos, com o intuito de promover boas práticas de gestão de dados, e em 2009 fundou o DAMA-DMBoK (Data Management Body of Knowledge), sendo um corpo de conhecimento que tem como ponto fundamental esclarecer como as corporativas devem aplicar a operação otimizada dos dados. (CARVALHO, 2021)
Em sua versão 2.0, acrescenta não só uma visão macro do gerenciamento de dados, definindo padrões, terminologias e práticas, mas a integração de dados, para definir táticas,

armazenamentos e sistemas, bem como implementação da ética na operação do tratamento de dados, a definição de big data e ciência de dados e amadurecimento das informações. (LIMA, 2019).
O DAMA-DMBOK V2 é formado por 11 (onze) funções de gestão de organização de

dados, sendo incorporado como cerne principal: a governança de dados, tendo em vista que os dados percorrem por toda sistemática das onzes funções ordenadas, assim segundo Honório (2021):
A primeira função é a governa de dados, sendo o pilar do framework, tem o condão de orientar e supervisionar a operação do ciclo de vida dos dados, na qual deve estabelecer um sistema de apoio a decisão dos gestores sobre os dados, sob o prisma do negócio.
A arquitetura de dados, a segunda função, pode ser conceituada como um planejamento para administrar os dados, aquisição de ativos da empresa, com o intuito de definir a finalidade das informações adquiridas com os requisitos necessário para o gerenciamento dos dados.
Por sua vez, a modelagem de dados e design, tem a função de demonstrar de forma nítida os dados, sendo o processo da descoberta, análise e representação da etapa primária da informação.
O armazenamento, uma das etapas da operação do ciclo de vida dos dados, na qual vai incluir o design, o suporte dos dados armazenados para quantificar o coeficiente valorativo das informações, até o seu descarte, devendo respeitar todo o procedimento de segurança legal vigente.
Um dos alicerces para o gerenciamento de informação é a segurança, que deve garantir a proteção dos dados, a execução de políticas e procedimento de segurança, no intuito de moderar o acesso de forma consciente e controlado, não devendo ser infringido ou acessado de forma inadequada, afim de garantir autenticação e auditoria de dados informações.
A Integração e Interoperabilidade de dados, é a função responsável pela movimentação e a concretização dos dados na interligação do armazenamento e outras plataformas.
O gerenciamento de documentos, pode ser compreendida como o gerenciamento e inclusão da vida útil dos dados e informações, encontrados em programas não estruturados, em ênfase ao conteúdo de apoio de conformidade a legislação vigente e os termos éticos formalizados para o negócio.
Dados mestre e de referência, tem como condão a manutenção dos dados compartilhados para coexistir a integralidade dos sistemas internos de gerenciamento dos dados.
Em razão da interligação entre uma linha direta com os negócios, uma das funções do DAMA-DMBOK é a Data warehousing e Business intelligence, ou seja, a implementação de

planner para o contoler da administração dos dados e suporte a decisão com o intuito de conceder aos gestores de informação emitam relatórios de equalização de valores.
Segundo Barata (2015), os metadados, na qual consiste a décima função, é promover a facilitação do acesso dos dados interligados nas multifontes do sistema integrado, como também garantir a qualidade de dados.
Por fim, o gerenciamento de qualidade de dados é a implicação das técnicas para garantir a possibilidade de aferição, melhoramento e adequação da utilidade dos dados, com o intuito de monitorar a integridade da informação primária no ciclo de vida dos dados.
Já o COBIT (Control Objectives for Information and related Technology), é um framework de suporte fundado em 1994 administrado pela ISACA (Information Systems Audit and Control Association), estruturado como um arcabouço de informação direcionadas para governança de dados e gerenciamento de informação, tem como objetivo auxiliar os profissionais de gestão na conexão entre os problemas técnicos e os riscos do negócio. (BARATA, 2015).

Para Lima (2019), o COBIT é um framework que possui duas vertentes basilares: a gestão, que possui quatro áreas de domínios: planejamento, constituição, execução e monitoramento, e a governança que é a tomada de decisão de acordo com a gestão de dados, possuindo 37 (trinte e sete) processos integrados.
Na versão 5.0, o sistema é utilizado baseado em 05 princípio, conforme elucida Casaes (2019), Barata (2015) e Lima (2019), sendo: (i) atender às necessidades das partes interessadas; (ii) cobrir o negócio como um todo; (iii) aplicar um framework único e integrado; (iv) habilitar uma visão holística; e (v) distinção entre governança de gestão.
Um dos princípios é atender às necessidades das partes interessadas, sendo a necessidade das corporativas é satisfazer as expectativas dos seus stakeholders, proporcionando um equilíbrio na tripartite: benefícios, redução do risco e recurso disponíveis.
O segundo princípio é baseado na cobertura do negócio como um todo, ou seja, abranger a integralidade da empresa no processo, procedimento, pessoas e as relações com os habilitadores.
A aplicação do framework único e integrado, assim, o COBIT é capaz de promover uma relação completa com a Governança de dados, corroborando ao alinhamento com padrões externos e adaptabilidade dos modelos usuais de negócios.

O COBIT permite habilitar uma visão holística, ou seja, uma visão macro dos componentes que oferecem suporte para atingir as finalidades da governança de dados, na qual define como catalogadores: as políticas, processos, estruturas organizacionais, informação e ética.
Por derradeiro, o princípio da distinção entre governança de gestão, tendo em vista que ambos possuem estruturas organizacionais distintas, assim, governança tem como esforço principal que os objetivos corporativos sejam cumpridos, estabelecendo prioridades pela tomada de decisão, compliance e progresso das organizações. Por sua vez, a gestão é o planejamento, construção, execução e monitoramento das funções ornamentada com o direcionamento da governança.
Desse modo, com escalonamento dos cinco princípios é capaz de proporcionar o funcionamento otimizado do framework, destacando os seguintes processos:
O APO01: Gerenciar o framework de TI, tem como condição a otimização das atividades relacionadas ao TI, com a função principal de incluir os procedimentos e regulamentos para promover a integralidade das informações nos bancos de dados. (BARATA, 2015)
Já o APO03: Gerenciar a arquitetura corporativa, tem função primordial agrupar as informações para auxiliar as atividades e tomadas de decisões, conceituando e compartilhando as informações dos elementos dos dados, e por fim catalogar a empresa, com base na modulação e sensibilidade dos dados. (BARATA, 2015)
Nesse ínterim, a governança de dados como um sistema integrado com o programa de compliance, tem o condão de otimizar a operação de controle interno relacionado aos dados coletados pelas empresas, capaz de gerenciar as bases para o apoio de decisão ao tratamento das informações, com segurança e qualidade, garantido o ciclo da vida útil dos dados.

4 A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

As estruturas políticas, econômicas e sociais com desenvolvimento de novas tecnologias e mecanismo para a coleta de dados e informações, fez necessário modulações legislativas para a proteção da privacidade, além dos aspectos físicos, patrimoniais e morais.
A proteção à privacidade de dados foi dividida em quatros gerações: a primeira, oriunda do estado moderno, com o advento dos bancos de dados; a segunda, datada em 1980, com a expansão legislativa para a proteção à privacidade aos setores privados; a terceira geração em 1990, com o processo de tratamento de dados e o consentimento dos cidadãos; Por fim, a última dimensão, é

destinada ao protagonismo da permissão para coleta e uso dos dados pessoais, quando a lei estabeleceu a importância da titularidade das informações. (MENDES, 2014)
Nesse aspecto, é perceptível a evolução do direito aos fatores reais da sociedade e as transformações dos meios tecnológico, computacionais, genéticos e comunicativos, que por sua vez possibilitou a integração da comunicação global, e consequentemente, o rastreio dos dados através do armazenamento de informação. (SAAD, 2021).
Os legisladores ao considerar os dados pessoais como extensão ao direito à privacidade, preocuparam em tutelar constitucionalmente a proteção da população, em especial os países europeus, como: Espanha, Portugal, Hungria, Eslovênia e Rússia. (VIEIRA, 2007) Porém, só tornou-se fator primordial após o regulamento geral do Parlamento Europeu sobre a proteção de dados, n.º 2016/679, sendo necessário a adequação das empresas prestadoras de serviço na Europa ao regulamento, influenciado diretamente o Brasil para elaboração da Lei Geral de Proteção de Dados brasileira. (SAAD, 2021).
Muito embora, a Lei Geral de Proteção de Dados Pessoais - LGPD, em sua promulgação, não abarcou de forma expressa a proteção de dados como direito fundamental, a doutrina, em especial Nascimento (2020), por sua vez, já argumentava a proteção de dados e informações pessoais como direito autônomo, derivado do direito fundamental à privacidade, explicitamente no artigo 5°, X, da CRFB de 1988.
Após reiterados julgamento sobre a tutela dos dados pessoais como extensão da personalidade do indivíduo, o Supremo Tribunal Federal -STF reconheceu no Julgamento da Ação Direta de Inconstitucionalidade - ADI 6387, a existência dos dados como direito autônomo, derivada do direito fundamental a dignidade da pessoa humana, na proteção à intimidade e a centralidade do Habeas Data como autodeterminação informativa. (NASCIMENTO, 2020).
Ao compreender a necessidade da proteção aos dados pessoais, os legisladores brasileiros em votação de ? das casas legislativas (câmara e Senado Federal) em dois turnos, aprovaram a Emenda Constitucional 115 de fevereiro de 2022, alterando o artigo 5° da Constituição Federal de 1988, incluindo o inciso LXXIX, tutelando constitucionalmente a proteção aos dados pessoais, inclusive nos meios digitais.
Ressalta-se, ainda, que os dados pessoais estão interligados com o direto fundamental à privacidade, na qual representa a capacidade de a pessoa administrar sua vida, seus pertences e

propriedades materiais e imateriais, permitindo ou não a utilização dos seus dados (bens imateriais) por terceiro. (NASCIMENTO, 2020).

A privacidade, por sua vez, segundo Mendes (2008), é o direito à proteção aos comportamentos pessoais e acontecimentos de caráter íntimo, bem como as informações prestadas aos profissionais e comerciantes, em que a pessoa não deseja que se compartilhe com o público.

Para o professor William Prosser, pode-se qualificar a lesão a privacidade em quatro graus: i) o intrometimento na reclusão ou solidão na vida privada, ii) a divulgação pública de fatos privados constrangedores sobre o indivíduo; iii) a publicidade sobre o indivíduo apresentada de forma equivocada; e iv) a apropriação, para obtenção de vantagem, do nome ou da imagem do demandante (PROSSER, 1960).

A doutrina, por sua vez, defende mais uma violação à privacidade: a privacidade informacional, interligada com os fatores tecnológicos de informação. (SAAD, 2021). Assim, quando a lei ao realizar o tratamento da privacidade, refere-se como um direito líquido, ao qual será tutelado para garantir que o indivíduo tenha um local reservado, que não tenha, se desejar, a interferência de outros sujeitos, seja pessoa física ou jurídica.

Com a proteção dos dados pessoais dos titulares, através da LGPD, possibilitou ao cidadão o acesso a informações ao ciclo de vida útil dos dados pelas empresas, e a certeza de fiscalização pela Autoridade Nacional de Proteção de Dados, com a finalidade de atingir os objetivos traçados pela legislação, na qual a lei traz conceitos e delimita princípios, que devem ser mencionados.

A LGPD tem como objetivo principal: ?o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado?, com a destinação de assegurar os direitos fundamentais a liberdade e privacidade dos titulares dos dados, bem como tutelar a dignidade e a personalidade da pessoa natural. (LGPD).

A legislação está ordenada diretamente com o meio empresarial, sobretudo no que se refere aplicação aos seus destinatários que são pessoas físicas ou jurídicas que realizam a coleta e tratamento de dados no Brasil, conforme preceitua o artigo 1° da lei 13.709, de 14 de agosto de 2018.

Para compreender a LGPD, faz-se necessário elucidar os conceitos de dados pessoais: (art. 5º, I) é toda informação relacionada a pessoa natural, identificada ou identificável, sendo o dado aplicado no contexto que possibilite o reconhecimento do indivíduo. Bem como refere-se aos dados sensíveis (art. 5º, II), são todas as informações que se relaciona com pensamentos políticos, crenças, identidade biológica e física. Portanto, a legislação tem como ponto a proteção e o cuidado para a não violação dos dados pessoais e sensíveis.

Os doutrinadores, Laura Schertel e Danilo Doneda, ainda aponta cinco pilares para compreender a LGPD, sendo: i) a unidade e generalidade da aplicação da Lei; ii) a legitimação para o tratamento de dados (hipóteses autorizativas); iii) os princípios e direitos do titular; iv) as obrigações dos agentes de tratamento de dados e v) a responsabilização dos agentes.

O primeiro pilar é considerado com aplicabilidade material da legislação, ou seja, aplica-se a qualquer operação realizada por pessoa natural ou jurídica de direito público ou privado,

independentemente do meio, da sua sede ou do país onde estejam localizados os dados (Art. 3°). Considerado, assim, como uma aplicação uniforme para todos os setores público ou privados que realizam tratamento de dados.

O segundo pilar é a legitimação para o tratamento de dados, tendo em vista que a lei especificou critérios e requisitos para o reconhecimento da legitimidade, não podendo ser tratados os dados, sem que exista uma base normativa que autorize, prevista no artigo 7°, 11° ou 23° da LGPD, abordando 11 (onze) hipóteses, incluído o consentimento ou a previsão legislativa.

Destaca-se que a autorização por consentimento para ser considerado válido, deve observar os requisitos previsto no artigo 5°, XII, sendo considerado que a vontade deve ser livre, informada, inequívoca e com a finalidade determinada, consagrando os princípios norteadores da legislação.

O terceiro pilar é o conjunto de princípios e direitos que assegura o destinatário da lei a controlar a utilização do seu dado pessoal, sendo importante elencar dez princípios que estruturam a LGPD: a finalidade, a adequação, a necessidade, o livre acesso, a qualidade dos dados, a transparência, a segurança, a prevenção, a não discriminação e a responsabilização. (MENDES, DONEDA, 2018)

No que concerne, aos direitos dos titulares são expressos no artigo 18° da referida lei, que permite o titular dos dados adquirir através do controler, independentemente do momento, as informações relacionadas ao indivíduo, prevendo: acesso, confirmação, correção, anonimização, bloqueou ou eliminação e a portabilidade.

Para adentrar no cerne dos problemas enfrentados pela legislação, em especial, sobre o vazamento de dados, os dois últimos pilares serão abordados sob a perspectiva da violação e responsabilização acerca da proteção de dados nos casos incidentes de vazamento.

Assim, o quarto pilar, destina-se às obrigações dos agentes de tratamento dos dados, na qual estabeleceu limites que devem ser observados nas operações realizadas para reforçar a segurança e prevenir os problemas da atividade no tratamento de dados.

Uma das obrigações fundamentais, consiste na intitulação do encarregado pelo tratamento dos dados indicados pelo controlador, conforme artigo 41 da LGPD, que possui a função de aceitar as reclamações e comunicações dos sujeitos dos dados, receber informações da Autoridade Nacional, como deve orientar os funcionários a respeito das práticas a serem adotadas em relação à proteção de dados pessoais.

Assim, as informações devem ser fornecidas ao proprietário dos dados, quando os dados forem coletados, como: os meios de segurança aderidos ao tratamento de dados, quais são os riscos da atividade que podem gerar lesão ao titular, pois pode gerar a mitigação dos prejuízos. (SAAD, 2021)

A lei Geral de Proteção de Dados Pessoais tem como objetivo a proteção do dados pessoais dos titulares dos dados, sendo assim, uma das obrigações principais é adoção de medidas de segurança, técnicas e administrativas hábeis a proteger os dados pessoais de acessos não autorizados, como promover a integralidade dos dados, não permitindo, assim, a alteração das informações, a prevenção de situações ilícitas ou acidentais, ou qualquer forma de tratamento inadequado, consoante se desprende do artigo 46 da lei.

Tornou-se corriqueiro manchetes acerca do vazamento de dados por corporativas, uma das violações mais graves incidentes abarcados pela LGPD, o que ocasiona a vulnerabilidade do titular dos dados, e dos sistemas internos que são responsáveis pelo ciclo de vida útil dos dados. (SAAD,2021)

A seção de segurança de informação tem como condão as obrigações inerentes aos agentes de tratamento, devendo ser adotado pela integralidade das pessoas que realizam o tratamento de dados, garantido que os dados sejam confidenciais, bem como disponíveis nas operações de tratamento. (Art.48). Nos casos incidentais de vazamento de dados, insurge a necessidade ao controlador de informar a autoridade de proteção de dados, que podem definir as medidas para mitigação dos danos.

No entanto, com a utilização da internet, compras online, transferência virtuais e outros meios tecnológicos, criou-se uma dificuldade para atuar na segurança de dados, tendo em vista a abrangência e os domínios de redes globais, que combinados com fatores não perceptível, forma

um perfil não rastreavel capaz de ocasionar violação às diretrizes básicas da legislação, que mesmo com ações posteriores não conseguem excluir os inúmeros registros de pessoas e organizações que coletaram os dados, lesionando a confidencialidade das informações (SAAD, 2021)

Destaca-se que as obrigações aos controladores e operadores, devem ser observados desde a coleta dos dados até seu descarte, assim o artigo 46 da LGPD, introduziu o conceito de privacy by design, sendo a incorporação pelas empresas nos serviços e produtos, na qual dispõe a proteção da privacidade no centro de todo o desenvolvimento corporativo.

Embora, a legislação tenta dirimir os riscos da atividade, os prejuízos causados pelo vazamento de informações são altos, e perpassam pela inadequação do sistema de proteção, perda de credibilidade e de clientes, ocasionado uma ruptura na imagem da empresa, impossibilitando, muitas vezes de concorrer no mercado corporativo. (SAAD,2021)

Portanto, a LGPD concebeu obrigações aos agentes de tratamento de dados, para que se delimite a finalidade da utilização dos dados desde o início da concepção, devendo o controlador confeccionar relatório de impacto a privacidade, utilizando de métodos para a captação da operação do ciclo de vida dos dados, observando as mediadas adotada para aumentar a segurança e mitigar o risco do tratamento das informações, conforme artigo 3 da LGPD.

O último pilar, considerado como a responsabilidade dos agentes na incidência de ocorrência de danos derivados do tratamento de dados. A LGPD consagrou a natureza do tratamento, limitando os parâmetros ao artigo 7° da lei, nas 10 hipóteses dos incisos, vinculados a finalidade da captação dos dados, consoante prevê o artigo 6°, inciso I, II, da LGPD.

A legislação tem como regra o descarte (eliminação) dos dados ao fim do tratamento da operação (art. 16), com o intuito de mitigar os riscos presente no tratamento de dados, principalmente, no que concerne à limitação das hipóteses de tratamentos para não lesionar os direitos dos titulares.

Nos casos, em que mesmo após o término de vida útil dos dados, as empresas podem, quando permitido, armazenar dados que em situação incidentais serem objetos de violação, principalmente nos casos de vazamento, que podem ocorrer, quando não autorizados pelo titular

ou controladores, serem acessados, captados, compartilhados pela internet, para outros sujeitos ou empresas.
Assim, a Lei Geral de Proteção de dados Pessoais, em especial em seu artigo 42, dispõe que o controlador ou operador, quando realizar o exercício do tratamento de dados pessoais, vem

a ocasionar dano patrimonial, moral, individual ou coletivo em detrimento a aplicação da legislação, é obrigado a repará-lo, definindo a responsabilidade de forma objetiva.
Embora, a responsabilização objetiva não é necessária a demonstração de culpa do controlador ou operador. Faz mister esclarecer que o operador, só será responsabilizado quando os atos praticados forem contrário à legislação, ou às instruções que foram fornecidas pelo controlador. (MENDES, DONEDA, 2018)
Ainda, a legislação prevê exceções a responsabilidade objetiva (art. 43), sendo: quando o agente demonstrar que não realizou o tratamento de dados pessoais que foi atribuído, ou quando não houve violação da segurança ou a legislação, e por fim, quando for por culpa exclusiva do titular ou de terceiros.
Porém, o cenário que é vislumbrado no Brasil nos casos de vazamento de dados, é que as violações pelas instituições vêm ocorrendo, majoritariamente, sob ataques deliberados de hacker, ou falha de segurança dos controladores dos dados. (SAAD, 2021)
Dessa forma, é necessário adotar medidas para dirimir os riscos da atividade, e possibilitar o discernimento das informações acerca dos perigos de vazamento de dados, tendo em vista que a tendência é aumento significativo das violações vinculados com a crescente tecnológica. Assim, as empresas devem implementar mecanismos para a segurança das informações.

5 O COMPLIANCE EMPRESARIAL COMO INSTRUMENTO DE PROTEÇÃO DE DADOS NA ESFERA EMPRESARIAL

Em decorrência das constantes violações aos dados armazenados em provedores privados, a tutela ao direito à privacidade nos meios tecnológicos, já era pauta de debate na legislação brasileira, e já existiam mecanismos para a proteção, como: a proibição de direcionamento dos provedores em relação ao compartilhamento de dados, bem como a inibição ao monitoramento nos navegadores de internet.
Vinte e seis bilhões de dados foram vazados no Brasil em 2019, de acordo com pesquisas realizadas pelo Massachusetts Institute of Tecnology ? MIT, possibilitando a utilização de números telefônicos, score de crédito, endereço eletrônico, fotos, números de identificações e outros dados pessoais, para o cometimento de crimes cibernéticos, e a violação aos direitos dos titulares.
A utilização e uso dos dados pessoais por pessoa física ou jurídica, com sede no Brasil ou não, devem se atentar as normas gerais de proteção aos dados brasileiro, segundo Frazão, Oliva e

Abilio (2020), é a necessidade de conferir a efetividade aos direitos e prevenir a violação aos dados, através da implementação de mecanismo de compliance, como uma ferramenta capaz de promover a adequação das atividades aportadas pelas empresas.
Assim, os controladores e operadores poderão formular regras de boas práticas e governança (Art. 50), que contenha as disposições de organização interna, o regime de funcionamento, as operações, o canal de comunicação entre os encarregados e os titulares dos dados, e o procedimento de segurança.
Nessa perspectiva, considerando que a maioria das tratativas de dados perpassam por meios digitais, deve-se adotar sistema para mapear os riscos, e implementar mecanismos para minorar as vulnerabilidades apontadas pelos programas, através da alta administração, do código de ética, para proteger os dados pessoais dos titulares. (PESSOA, 2021)
Existem inúmeras formas de ocorrer o vazamento de dados, sendo através de ataques cibernéticos, sequestro de conta, furtos de dados, compartilhamento de dados por agentes ou ex-agentes da empresa, erro ou negligência, entre outros, que podem ser para adquirir dados de nomes, CPF, celulares, endereços, dados financeiros, senhas, registro de saúde ou credenciais de acesso. (SAAD, 2021)
Desse modo, para realizar o mapeamento dos problemas que as corporativas podem enfrentar, é necessário identificar os fluxos e processos de informação que percorrem os sistemas, que irão auxiliar na tomada de decisão pelas empresas. (NASCIMENTO, 2020)
A alta administração deverá colaborar ativamente no programa de compliance, seja monitorando as investigações e intervenções em situação para estabelecer controles internos em conformidade com a legislação, bem como possibilitar a interdependência dos setores para realizar as atividades designadas para o tratamento de dados (PESSOA, 2021).
Com a elaboração do código de ética pela organização possibilitará o treinamento regular das equipes, responsáveis pela tecnologia da informação, para enraizar a cultura corporativa da boa governança, com a finalidade de assegurar o respeito ao programa de compliance (NASCIMENTO, 2020)
Nesse contexto, para manter uma boa relação com seus clientes, as organizações devem instalar canais de comunicação, para que os titulares dos dados possam contatar os encarregados responsáveis pelos armazenamentos dos seus dados, e exerçam seus direitos sobre as informações contidas nos provedores. (PESSOA, 2021).

Desse modo, quando se trata de concretização a alteração cultural coportariva é preciso realizar o alinhamento dos funcionários com o código de ética, com política de privacidade, para fins de efetividade do programa de compliance de dados. (PESSOA, 2021).

5.1 A IMPLEMENTAÇÃO DE MECANISMOS DE GOVERNANÇA DE DADOS PESSOAIS

Para a efetividade da legislação em relação ao tratamento de dados, a LGPD direciona um capítulo para implementar o programa de governança em privacidade, com a finalidade das empresas adotarem medidas técnicas, para fins de proteção e segurança dos dados pessoais.

(PESSOA, 2021)
A governança em privacidade, pode ser conceituada como um conjunto de regras e práticas positivas a serem implementadas pelos agentes de tratamento, e encontra-se em conformidade com as políticas de compliance empresarial, com o objetivo de gerir os dados das empresas para estabelecer um diferencial competitivo aos negócios. (KOEPSEL,2020)
O programa integra o aperfeiçoamento do procedimento de utilização dos dados, com os requisitos pré-estabelecidos na implementação dos softwares, com a finalidade de gerir de forma otimizada os dados para preencher as diretrizes da legislação. (SAAD, 2021)
A Lei Geral de Proteção de Dados Pessoais dispôs que os controladores e operadores poderão adotar programas de governança em privacidade, que devem ser implementados com o mínimo, (art. 50, § 2°, I): a) o comprometimento dos agentes de tratamento com as políticas internas que devem garantir o cumprimento das normas e regras de boas práticas; b) que aplicação seja de forma uniforme para todo a operação de tratamento de dados; c) que a governança seja adaptativa as estruturas da empresas, sendo compatível com a densidade dos dados e operação; d) como implementar políticas de salvaguardas em relação aos titulares dos dados; e) tenha como objetivo estabelecer uma relação de confiança com sujeitos dos dados, estabelecendo situações de transparência e que possibilite a atuação do titular; g) que conte com planos de respostas a incidentes e remediações; h) seja continuamente atualizado sua base.
Nesse aspecto, devem ser adotadas medidas administrativas para que as instituições, em conformidade com a legislação, apliquem estímulos para assegurar as informações armazenadas pelas empresas, com a adoção de orientações internas que respeitem as diretrizes que inclua o uso

minimizado ou a anonimização das informações, desde a coleta dos dados, conforme artigo 46 da LGPD.
Com o mapeamento das atividades, é importante verificar: O que são esses dados?; de que forma foram coletados ?; quem são os coletores ?; existe relação entre os dados e atividade realizada ?; O que pode ocorrer com esses dados ao serem coletados? E, como são descartados da gestão organizacional da empresa? (NASCIMENTO, 2020). Dessa forma, para adotar medidas compatíveis com os riscos alertados pelos sistemas para a proteção de dados nas organizações privadas, é necessário possuir conhecimento do caminho realizado inerentes ao ciclo de vida útil dos dados.
Embora, a legislação já estabeleça diretriz mínima para o tratamento de informação, a Autoridade Nacional de Proteção de Dados - ANPD, poderá, ainda, determinar padrões técnicos para serem implementados pelo programa de governança em privacidade, devendo ser observado a qualidade de dados, as especificações do tratamento e status tecnológico, em especial a proteção aos dados sensíveis disposto na legislação. (NASCIMENTO, 2020)
Muito embora, a lei geral de proteção de dados, apenas delimita as características e os requisitos mínimos que os operadores deverão tomar para desenvolver um compliance na organização das empresas privadas em consonância com a legislação, porém não impõe um modelo específico para integração de um programa nas corporativas. (PESSOA, 2021)
Assim, para Saad (2021), as medidas técnicas que podem ser adotadas pelos agentes de

tratamento de dados, são: i) o uso de firewalls, sendo um mecanismo de segurança que coleta os dados em conformidade com as regras pré estabelecido para análise de tráfego de rede, delimitando as operações de compartilhamento e captação de informações a serem cumpridas; ii) a utilização de antimalware, que consiste na proteção contra vírus que é capaz de fragilizar o sistema, apagar dados e infectar outros arquivos; iii) a utilização de criptografia dos dados, que possibilite quando ocorrer situações incidentais a não identificação do titular do direito.
Já para Fernandes e Abreu, (2014) defendem a implementação de frameworks como a DAMABOK e COBIT, para o gerenciamento de dados, pois tem como meta principal a delimitação do escopo das atividades, as funções envolvidas no tratamento e as interações a serem executadas pelo software, com a finalidade de proteger a privacidade em ambientes corporativos que gerenciam o armazenamento de informações aplicados na prevenção à fraude.

Segundo Carvalho (2021), a integração do software, através das boas práticas estabelecidas pela legislação, poderá aprimorar os aspectos de proteção à privacidade e prevenção a fraude do tratamento de coleta de dados. Tendo em vista, que os frameworks, podem balizar as métricas de qualidade dos dados que indicam uma utilização adequada e otimizada, e aponta a melhor proteção da privacidade.
Com a melhoria de processo de governança para o tratamento de dados, estabelece uma divisão entres as operações que possibilita uma automatização do ciclo de vida dos dados (coleta, utilização, armazenamento e exclusão), capaz de gerar relatório de risco, para o auxílio da tomada de decisão com o intuito de gerir de forma adequada o tratamento de dados. (CARVALHO, 2021)
Neste parâmetro, os programas de compliance com a implementação de frameworks, podem responder questionamento acerca do procedimento de tratamento de informação, dispondo de quais práticas relacionadas à governança, privacidade e segurança de dados, apresentam melhor benefício para o tratamento de dados pessoais. (CARVALHO, 2021)
Ademais, os controladores e operadores deverão adotar medidas, como o Relatório de Impacto ? DPIA), que corresponde a avaliação dos riscos e impactos relacionados com o tratamento de dados pessoais, além da anonimização, da transparência e do sigilo, deverão delimitar prazos para retenção de dados e aderir políticas seguras de informação acerca da operação de tratamento. (SILVA, 2022)
Após realizar a implementação e observância das estruturas mínimas estabelecidas pela LGPD, é necessário adotar um programa de gerenciamento de vulnerabilidades, com atualizações constantes e autocorreções alinhados com as boas práticas de atividades cotidianas, com a finalidade de proteger os dados pessoais, e promover um ambiente corporativo adequado para realizar o tratamento de dados. (SAAD, 2021)
No entanto, ao verificar que houve vazamento de dados, seja pelo recebimento de notificação ou pela veiculação na mídia, os agentes de tratamentos deverão identificar quais dados vazaram e realizar o procedimento estabelecido no programa de compliance de segurança, além de notificar as instituições. (Art. 48, caput).
De acordo com MIT, o prazo entre a comunicação à autoridade competente e a ocorrência do fato ilícito ultrapassa 200 (duzentos) dias em média, sendo umas das preocupações para a

efetividade da legislação, e a redução dos danos causados aos titulares dos bens imateriais.

A Lei Geral de Proteção de Dados, dispõe que nas situações que ocorrer a probabilidade de riscos ou violação aos direitos dos titulares, tem como obrigação do encarregado a comunicação à autoridade nacional e ao titular do dado (art. 48, caput). Sendo que o contato deve ser em período razoável (art. 48, § 1º), contendo a natureza dos dados dos titulares atingindo (art. 48, § 1º, I).
Em decorrência dos possíveis incidentes, a LGPD determinou critério para aplicação de sanções, em casos de vazamento de dados, observando as situações específicas de cada caso, disposto no art. 52, § 1º. Assim, deve ser considerada a avaliação da gravidade, a natureza das informações e do dano ocorrido (incisos I e VI), sendo necessário para este caso, tendo em vista que o compartilhamento indesejado de dados sensíveis pode ocasionar danos irremediáveis para os titulares.
Portanto, existe a necessidade da adesão aos mecanismos e técnicas para promover a efetividade dos programas internos com a finalidade de mitigar os danos, assim, a implementação de boas práticas e governança têm como fator o cumprimento da legislação, por meio de medidas de segurança. Entende-se, que a proteção integral contra falhas que possibilitam a ocorrência de ilícitos não é possível, porém essas diretrizes reduzem as possibilidades de existir desvios de condutas e criar salvaguardas para identificação dos incidentes, de forma eficaz, rápida e adequada.

6 CONSIDERAÇÕES FINAIS

A partir da permissão ao acesso dos dados pessoais, as informações coletadas passaram a integralizar as redes de tratamento de dados, tornando-se alvo de ataques cibernéticos, contribuindo para o aumento da intercorrência no ambiente corporativo, tornando-se o gerenciamento de informação um dos diferenciais no desenvolvimento do negócio.
Nesse contexto, foi imperativo o surgimento de leis que protejam os dados dos cidadãos, e que limitem a gestão das entidades públicas e privadas em relação as informações coletadas, transformando o sistema organizacionais, como compliance, em ferramentas de efetivação das normas éticas e legais. Assim, a implementação do programa alinhado com a governança corporativa é capaz de integralizar o corpo de normas internas com o intuito de adequar a legislação brasileira e criar uma cultura corporativa.
Dentro do programa de compliance, a administração em conjunto com a gestão da empresa, poderá implementar ao plano diretor, a utilização de software, sendo este capaz de possibilitar a automatização do ciclo de vida útil dos dados para realizar o auxílio da tomada de decisão, com o intuito de mitigar os possíveis danos decorrentes da violação aos dispositivos da Lei Geral de Proteção de Dados Pessoais.
Nesse sentido, para realizar uma proteção extensiva aos direitos dos titulares dos dados, a

LGPD integrou ao seu corpo de normas-condutas a serem adotadas pelos operadores do tratamento de dados, com escopo de preservar a integralidade, a qualidade e o sigilos dos dados, tendo como consequência da violação, a majoração de sanções pecuniárias.
Embora, o vazamento de dados ocorra de forma ordenada, a implementação de sistema de segurança nas corporações implica na diminuição de situações incidentais por erro humano, ou inadequação dos programas empresarias, assim, devendo a gestão ensejar esforços para que a proteção dos dados seja preservada, desde a concepção do serviço.
Para a efetivação da Lei Geral de Proteção de Dados Pessoais, as empresas devem realizar a adequação de medidas de boas práticas e governança em privacidade para mitigar os possíveis danos decorrente da violação aos dados em provedores privados. Mesmo que a proteção aos dados de forma concreta não seja possível, as adoções de mecanismo de segurança podem atenuar as sanções e as perdas aos titulares dos dados.

REFERÊNCIAS

BARATA, André Mantola. Governança de dados em organizações brasileira: uma avaliação comparativa entre os benefícios previstos na literatura e os obtidos pelas organizações. 2015. Dissertação (Mestrado em Sistema de Informação) - Universidade de São Paulo, São Paulo, 2015.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, [2022]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 15 abr. 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidente da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 abr. 2023.

BERTOCCELLI, Rodrigo de Pinho. Compliance. In: CARVALHO, André Castro et. al. Manual de compliance. Rio de Janeiro: Forense, 2019. p. 35.

CANDELORO, Ana Paula; RIZZO, Maria Balbina Martins De; PINHO, Vinícius (Coord). Compliance 360: riscos, estratégias, conflitos e vaidades no mundo corporativo. São Paulo: Trevisan, 2012.

CARVALHO, A. P. Proposta de um framework de compliance à Lei Geral de Proteção a Dados Pessoais (LGPD): um estudo de caso para prevenção a fraude no contexto de big data. 2021. Dissertação (Mestrado em Engenharia Elétrica) - Universidade de Brasília, Brasília, 2021.

CARVALHO, Andre Castro. Manual de compliance. 3. ed. Rio de Janeiro: Forense, 2021.

CASAES, Júlio César Costa. Governança de dados abertos governamentais: frameworks conceitual para as Universidades Federais, baseada em uma visão sistemática, 2019. Tese (Doutorado em Engenharia e Gestão do Conhecimento). Universidade Federal de Santa Catarina, Florinaóplis, 2019.

DATA GOVERNANCE INSTITUTE (DGI). Definitions of data governance. 2017. Disponível em: http://www.datagovernance.com/adg_data_governance_definition. Acesso em: 01 mai. 2023.

ENDEAVOR DO BRASIL. Prevenindo com o Compliance para não remediar com o caixa. In: ENDEAVOR. [S. l.], 26 abr. 2017. Disponível em: https://endeavor.org.br/pessoas/compliance/. Acesso em: 15 mar. 2023.

ESPÍNDOLA, P. L.; SALM JUNIOR, J. F.; ROSA, F.; JULIANI, J. P. Governança de dados aplicada à ciência da informação: análise de um sistema de dados científicos para a área da saúde. Revista Digital de Biblioteconomia & Ciência da Informação, Campinas, v. 16, n. 3, p. 274-298, 2018.

FERNANDES, Aguinaldo Aragon; DE ABREU, Vladimir Ferraz. Implantando a governança de TI: da estratégia à gestão de processos e serviços. 4. Ed. Rio de Janeiro: Brasport, 2014.

FRAZÃO, Ana. Programas de compliance e critérios de responsabilização de pessoas jurídicas por ilícitos administrativos. In: ROSSETTI, Maristela Abla; PITTA, Andre Grunspun. Governança corporativa: avanços e retrocessos. São Paulo: Quartier Latin, 2007. p. 42

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. A Lei Geral de proteção de Dados Pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

HONÓRIO, Roseli. Modelo conceitual de governança de dados como suporte à governança do conhecimento organizacional. 2022. Dissertação (Mestrado em Engenharia e Gestão do Conhecimento) - Universidade Federal de Santa Catarina, Florianópolis, 2022.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC). Guia das melhores práticas de governança para cooperativas. São Paulo, 2015. Disponível em http://www.ibgc.org.br/ userfiles/files/2014/files/CMPGPT.pdf

JOHNSON, Ralph E.; RUSSO, Vincent. Reusing object-oriented designs. Relatório Técnico da Universidade de Illinois, UIUCDCS 91-1696, 1991.

KLEINDIENST, Ana Cristina. Grandes temas do direito brasileiro: compliance. São Paulo: Almedina Brasil, 2019

KOEPSEL, Alice de Medeiros. Adoção e efeitos dos programas de compliance à luz da Lei Geral de Proteção de Dados Pessoais. 2020. Monografia (Graduação em Direito) -Universidade do Sul de Santa Catarina, Florianópolis, 2020.

LIMA, C., BASTOS, R. C. A criação de conhecimento apoiada pela governança de dados. In: CONGRESSO INTERNACIONAL DE CONHECIMENTO E INOVAÇÃO, 2019, Santa Catarina. Anais eletrônicos [...]. Santa Catarina Disponível em: https://proceeding.ciki.ufsc.br/index.php/ciki/article/view/647. Acesso em 10 Mar. 2023.

MARTIGNAGO, Deisi et al. Governança de dados aplicado no processo de catalogação. Revista Brasileira de Biblioteconomia e Documentação, São Paulo, V.15, n. 2, 2019.

MENDES, Gilmar Ferreira. Curso de direito constitucional. 2. ed. São Paulo: Saraiva, 2008.

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. São Paulo: Revista de Direito do Consumidor, 2018.

NASCIMENTO, Suellen Lima do. A lei Geral de Dados Pessoais e a Adoção dos Programas de compliance na sociedade da Informação. 2020. Monografia (Graduação em Direito) - Centro Universitário de Brasília, Brasília, 2020.

PESSOA, Larissa Rocha de Paula. Os desafios da Governança de dados e a realidade cultural brasileira. 2021. Dissertação (Mestrado em Direito) ? Universidade Federal do Ceará, Fortaleza, 2021.

PINTO, S. C. C. S.. Composição em Web Frameworks, 2000. Tese (Doutorado em Informática) Pontifícia Universidade Católica do Rio de Janeiro, Rio Janeiro, 2000.

PROSSER, William L. Privacy. California Law Review. California, v. 48, n. 3. p. 383 ? 423, agosto, 1960.

RÊGO, Bergson Lopes. Gestão e governança de dados: promovendo dados como ativo de valor nas empresas. 1. ed. Rio de Janeiro: Brasport, 2013,

ROQUE, Pamela Romeu. Estudos aplicados de direito empresarial: LL.C. em direito empresarial. São Paulo: Almedina, 2019.

SAAD, Carolina de Oliveira. A lei geral de proteção de dados pessoais e incidentes de segurança: regulação e prática de vazamento de dados, 2021. Monografia (Graduação em Direito). Fundação Getúlio Vargas. Rio de Janeiro, 2021.

SANTANA, Ricardo Cesar Gonçalves. Ciclo de vida dos dados e o papel da ciência da informação. In: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO. 14., 2013. Florianópolis. [?]. Florianópolis: UFSC, 2013. Disponível em: http://enancib2013.ufsc.br/index.php/enancib2013/%20XIVenancib/paper/viewFile/284/319. Acesso em: 13 mar. 2023.

SILVA, Ana Laura Fonseca. O papel das Soft Skills na implementação efetiva dos programas de compliance com foco na adequação à Lei Geral de Proteção de Dados ? Lei N° 13.709/18. 2022. Monografia (Graduação em Direito) - Universidade Federal de Ouro Preto, Ouro Preto. 2022

SILVA, Eggon João da. A defesa da ética e transparência. In: VENTURA, Luciano Carvalho. Governança corporativa. São Paulo: Saint Paul Editora, 2005, página 259.

TERRA, Priscila de Mello. A influência da governança de dados na gestão estratégica, 2017. Monografia (Bacharelado em Sistema de Informação) - Universidade Federal Fluminense, Niterói, 2017.

VAZAMENTO de dados aumentaram 493% no Brasil, segundo pesquisa do MIT.VEJA, São Paulo, 24 fev. 2021. Sociedade. Disponível em: https://vocesa.abril.com.br/sociedade/vazamentos-de-dados-aumentaram-493-no-brasil-segundo-pesquisa-do-mit. Acesso em: 15 mar. 2023.

VIEIRA, Tatiana Malta. O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante da tecnologia da informação. Porto Alegre: Sergio Antonio Fabris Editor, 2007.

==========

Arquivo 1: TCC - A IMPORTÂNCIA DO COMPLIANCE NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA - WESLEY VICENTE.pdf (8805 termos)
Arquivo 2: https://www.sciencedirect.com/science/article/pii/S0148296321003155 (3869 termos)
Termos comuns: 6
Similaridade: 0,04%
O texto abaixo é o conteúdo do documento TCC - A IMPORTÂNCIA DO COMPLIANCE NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA - WESLEY VICENTE.pdf (8805 termos)
Os termos em vermelho foram encontrados no documento
https://www.sciencedirect.com/science/article/pii/S0148296321003155 (3869 termos)

==========

WESLEY VICENTE DA SILVA

A IMPORTÂNCIA DO COMPLIANCE EMPRESARIAL NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA

SALVADOR
2023

WESLEY VICENTE DA SILVA

A IMPORTÂNCIA DO COMPLIANCE EMPRESARIAL NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA

Artigo apresentado como requisito parcial para obtenção do título de Bacharel em Direito pela Universidade Católica do Salvador.

Orientador: Prof. Darlã Conceição Santos.

SALVADOR
2023

A IMPORTÂNCIA DO COMPLIANCE EMPRESARIAL NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA

Wesley Vicente da Silva1
Darlã Conceição Santos2

RESUMO: No cenário de exploração das informações como mercadoria econômica, os dados pessoais coletados por empresas privadas tornaram-se fator de tutela legislativa. Assim, surgiu a necessidade de organizar os setores privados para adequar aos moldes da Lei Geral de Proteção de Dados Pessoais ? LGPD, com o intuito de proteger a privacidade, como direito autônomo e fundamental para a tutela da pessoa humana, destacando os programas de compliance aliados as boas práticas e governança de dados. Nesse contexto, a fim de consolidar os mecanismos técnicos de segurança para a efetividade da legislação com a finalidade de mitigar os casos de vazamento de dados pessoais, a LGPD implementou medidas administrativas para inibir incidentes decorrentes das condutas infratoras a legislação. Desse modo, este trabalho tem como objetivo demonstrar a importância dos programas de compliance para a proteção aos direitos dos titulares dos dados, visando o cumprimento do ordenamento jurídico. Valendo-se do método hipotético-dedutivo, com abordagem qualitativa, utilizando da revisão bibliográfica de livros, legislação, artigos, dissertações e teses concernente à tutela de dados pessoais no Brasil para o desenvolvimento do presente artigo.

PALAVRAS-CHAVES: Compliance Empresarial. Governança corporativa. LGPD. Vazamento

de dados.

ABSTRACT: In the scenario of exploitation of information as an economic commodity, personal data collected by private companies have become a factor of legislative protection. Thus, the need arose to organize the private sectors to conform to the General Law for the Protection of Personal Data - LGPD, in order to protect privacy, as an autonomous and fundamental right for the protection of the human person, highlighting compliance programs allied with good practices and data governance. In this context, in order to consolidate the technical security mechanisms for the effectiveness of the legislation with the purpose of mitigating cases of leakage of personal data, the LGPD implemented administrative measures to inhibit incidents arising from conducts that violate the legislation. Thus, this work aims to demonstrate the importance of compliance programs to protect the rights of data subjects, aiming at compliance with the legal system. Taking advantage of the hypothetical-deductive method, with a qualitative approach, using the bibliographic review of books, legislation, articles, dissertations and theses concerning the protection of personal data in Brazil for the development of this article.

KEYWORDS: Corporate Compliance. Corporate governance. LGPD. Data leak.

1
Discente do curso de Direito da Universidade Católica do Salvador.
2
Mestre em Direito, Docente na Universidade Católica do Salvador.

1 INTRODUÇÃO

A nova moeda de troca não é apenas aquela que podemos ver, quantificar ou converter. Os moldes do mercado financeiro mudaram, sendo em questão material ou ao produto que eles precificam, postulando um novo aparato ao objeto contratual: os dados.
Muito embora, os dados pessoais, ainda para muitos, são apenas informações deslocadas acerca de fatores específicos, atualmente, podem ser conceituados como um conjunto de indicadores, regrados por um complexo condensado de informações em um fluxo crescente tangencial.
Os dados da grande massa acabam gerando indicadores que podem ser balizados e influenciados de acordo com os detentores dessa informação, apenas apartado em blocos de informações não são considerados como vetores orçamentários. Porém, direcionados para uma finalidade ordenada tem o condão de influenciar o interesse social.
Dito isso, os mecanismos postos pelo Reino Unido para possibilitar uma estruturação normativa para organizar e gerir os dados dos indivíduos, foi crucial para a criação em outros países, como no Brasil, onde instituiu-se a Lei Geral de Proteção de Dados Pessoais (LGPD). Muito

embora, a lei brasileira trouxe um arcabouço de normas reguladoras e sanções aos casos de tratamento de dados, que não foram abarcados com o marco da internet, os dados em uma visão macro constitucional já eram de forma genérica tutelados pela Constituição Federal de 1988.
Todavia, apenas a sanção da LGPD não seria, isoladamente, capaz de coibir as violações ao tratamento de dados na esfera privada, mas sim a necessidade de uma regulamentação do ciclo de vida das informações, que além de estipular os dados que podem ser utilizados ou até quando podem ser armazenados, estabelecer expressamente no bojo da norma como deve ser a proteção na operação do tratamento de dados.
De forma efêmera, conclui-se que a legislação pode delimitar os alicerces capazes de ensejar uma fiscalização, sendo estas através de mecanismo de gerenciamento de atividades, políticas de condutas e implementação de governança de dados, pois os dados hackeados ou vazados de forma isoladas, não seria possível identificar dados sensíveis, muitos menos individualizar o sujeito.
Portanto, o gerenciamento dos dados em provedores de armazenamento pode ter os riscos reduzidos de acordo com a realização de medidas de compliance para dirimir os impactos na

atividade empresarial, como também para tutelar os dados, cada vez mais acentuado como um produto orçamentário.

2 COMPLIANCE EMPRESARIAL

A criação do compliance está entrelaçado sob o cenário econômico-social, assim, sua implementação como sistema de organização foi instaurado e aprimorado a partir dos problemas práticos estruturais para gerir uma boa governança, com intuito de assegurar a proteção e o controle que garante a qualidade do negócio.
A utilização do termo foi inicializada no mercado financeiro, especialmente após a criação do Banco Central em 1913 nos Estados Unidos da América, com a necessidade de um sistema econômico ajustável e estável. Só após 1960, com a regularização da Securities and Exchange Commission (SEC), que houve a necessidade de implementação do compliance como um programa para a integração dos procedimento, controle e monitoramento de operação interna. (CARVALHO, 2021)
Em 1977, com a Convenção Relativa à Obrigação de Diligência dos Bancos Suíços, estabeleceu os modelos auto regulatórios, com adequação de condutas e processos internos, na qual a infração tem como consequência à aplicação de sanções. (CARVALHO, 2021)
Só após esse processo de amadurecimento histórico, que o Brasil teve a necessidade de competir em escala global, implementado novos processos de segurança no sistema financeiro brasileiro.
Pode-se concluir que, após a globalização com o fenômeno da criação dos dados estruturais, houve a potencialização das informações adquiridas por meio de provedores, classificadas, atualmente, como fonte econômica de um produto quantificativo e qualitativo, ao qual possibilita uma utilização como um produto do sistema financeiro.
Nesse sentido, em decorrência de ataques cibernéticos em provedores de informações

massificadas conduziram a sociedade na aplicação de institutos de melhoramento, como o compliance e suas interfaces para proteger no ambiente corporativo os dados massificados recebidos em seus provedores.

2.1 O CONCEITO DE COMPLIANCE

Antes de enveredar sob o conceito de compliance na esfera privada, é oportuno compreender o seu significado. Nesse contexto, a palavra compliance advém do verbo inglês, to comply, que pode ser definida como conformidade. O instituto deve ser aplicado como plano principal de uma diretriz pré-estabelecida para ser dirigida a todos capazes de enfrentar a finalidade destinada. (BERTOCCELLI, 2019)
Nesse parâmetro, pode ser traduzida como:

Comply, em inglês, significa ?agir em sintonia com as regras?, o que já explica um pouquinho do termo. Compliance, em termos didáticos, significa estar absolutamente em linha com normas, controles internos e externos, além de todas as políticas e diretrizes estabelecidas para o seu negócio. (ENDEAVOR DO BRASIL, 2022, n.p)

O compliance pode-se ser definido de forma técnica como um conjunto de normas padronizadas, sob um viés ético e legal, na qual após estruturação será a matriz orientadora para o comportamento organizacional da instituição ao qual atuará no mercado, como também irá reger as atividades dos colaboradores. Dessa forma, sendo um instrumento hábil a controlar o risco de imagem, a normatização legal, chamados de riscos de compliance, as que recaem nas instituições no decorrer da sua atividade laboral. (CANDELORO, 2012).
Superada a barreira terminológica, a finalidade do compliance tem como escopo o gerenciamento adequado do risco de atividades, verificar adequadamente as normas éticas e legais, e estudar os possíveis danos tangenciais. Dessa forma, esses elementos visam a redução de perdas e danos, como também amplifica a cultura e fortalecimento corporativo nos moldes aos padrões exigidos, seja esse por lei ou na tentativa de dirimir o risco do serviço prestado.
Portanto, segundo a doutrinadora Frazão (2007, p. 42), destina-se em sua obra que o compliance é como:
(...) conjunto de ações a serem adotadas no ambiente corporativo para que se reforce anuência da empresa à legislação vigente, de modo a prevenir a ocorrência de infrações ou, já tendo ocorrido o ilícito, propiciar o imediato retorno ao contexto de normalidade e legalidade.

Nessa mesma linha de pensamento, de acordo com os autores da obra Compliance 360° (2012, n.p), referem-se o compliance a:

Um conjunto de regras, padrões, procedimentos éticos e legais que, uma vez definido e

implantado, será a linha mestra que orientará o comportamento da instituição no mercado em que atua, bem como as atitudes de seus funcionários; um instrumento capaz de controlar o risco de imagem e o risco legal, os chamados ?riscos de compliance?, a que se sujeitam as instituições no curso de suas atividades.

Pode-se concluir que o conceito de compliance, em uma esfera macro, é um aglomerado de regras pré-estabelecidas através de um instrumento perpetuado por técnica de desenvolvimento, capaz de dirimir riscos e danos das atividades devolvidas pelo plano diretor.
Muito embora, o instituto "compliance" tem uma definição extensiva e não tem como fim apenas o cumprimento da legislação e de condutas éticas, pode ser compreendida também como um instrumento de diminuição de riscos, desenvolvimento corporativo sustentável e subsequentes segmentos empresariais de negócio. (ROQUE, 2019)
O compliance além de estar associado tradicionalmente a uma perspectiva organizacional aos comandos administrativos, pode ser vinculada também a uma visão de uma sociedade digital 4.0, devendo não só apresentar o compliance empresarial na esfera de redução de risco à imagem, mas sim, em uma abordagem de pré-orientação e implementação de desenvolvimento aos moldes legislativo de proteção aos dados, como objeto principal de estudos.
Portanto, é necessário a elaboração do projeto de compliance em uma visão lógica, a modo de compreender os objetivos e os componentes da aplicação do programa. Posteriormente, superado os obstáculos, aplica-se os estudos de riscos a boa governança corporativa com a implementação de programas de governança de dados objetivando auxiliar o controle de informações em conformidade aos padrões da corporação, e mitigar os danos da empresa.

2.1.1 AS GOVERNANÇAS CORPORATIVAS E A IMPLEMENTAÇÃO DOS PROGRAMAS DE COMPLIANCE

Em linhas gerais, o Instituto Brasileiro de Governança Corporativa ? IBGC (2015, n.p) discrimina o conceito de Governança Corporativa, como: ?Sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas. ?
O sistema da governança corporativa está associado ao desenvolvimento interno de uma empresa, seja ele entre a administração, sócios e funcionários, capaz de criar elos para uma estruturação de direção racional e acima de tudo nos moldes da ética e legislação.
Muito embora, a governança corporativa e o compliance sejam institutos que se assemelham em uma visão macro, os mesmos, diferenciam na aplicação prática, mas se complementam no objetivo final, sendo um instrumento para aplicação do outro.

A prática da governança corporativa, além de estimular o valor empresarial, pode-se concluir que estrutura de forma adequada a medida necessária para organizar a atividade empresarial, assim, não há que se falar em condutas prejudiciais. Por exemplo: empresários compreendem que para realizar uma instrumentalização segura aos seus sócios e administradores tendem a prejudicar o negócio empresarial, assim o autor Eggon João da Silva (2005, p.259) retrata que: ?A governança corporativa assegura tratamento equânime a todos os acionistas, inclusive minoritários, preferencialistas, nacionais e estrangeiros. Todos devem ter oportunidade de reparação caso venham a sofrer violação de seus diretores. ?

Nesse passo, as críticas ao sistema não são viáveis, tendo em vista a utilização de instrumento capaz de integralizar ao plano empresarial. Sendo assim, o programa de compliance visa amplificar a utilização de um sistema para garantir que todos possam participar de forma justa sob o aspecto legal, seja sócio ou administrador.

Em uma tangente geral, a implementação da governança corporativa ressoa em uma perspectiva segura, tanto internamente, seja auxiliando as avaliações das atividades executadas pelos sócios/administradores, quanto externamente, em relação à imagem da empresa, sendo este um fator primordial a empresas estruturadas no mercado.

A implementação da governança corporativa deve ser estruturada de acordo com as necessidades da empresa, devendo verificar o histórico de desenvolvimento do estabelecimento, pois, só a partir do status da empresa pode-se delimitar a estratégia possível para uma implementação segura e adequada. Sendo assim, um regramento mais rigoroso pode gerar consequências negativas e ineficazes, especificamente em estágios primários, pois em atividades inicias, as tomadas de decisões e a execução da atividade empresarial é primordial, sendo necessário, um aspecto negocial informal para realizar os objetivos da empresa, o que não se verifica quando existe prática de boa governança devidamente estruturadas no negócio. (KLEINDIENST, 2019)

Ao desenvolver da atividade da empresa, além da atenção a organização interna, sendo está um fator primordial da governança, ainda que no fim acabe tendo um aspecto externo por vislumbrar no mercado financeiro uma maior complexidade da entidade. O desenvolvimento da empresa, seja no faturamento, importação comercial, quantidade de funcionários, além dos controles a observância da legislação e regras internas, tendem à serem complexos, e, que necessita

de ações maiores que a própria instituição empresarial, restando necessária a implementação de sistema organizacionais aos fluxos de informações. (KLEINDIENST, 2019)

Ultrapassado a esfera conceitual e instrumentalização da política de boas práticas de governança, cabe pontuar que as empresas que possuem fluxos de informações sensíveis, conforme estipula o artigo 50 da Lei Geral de Proteção de Dados Pessoais, os controladores e operadores são responsáveis pelo tratamento de dados, devendo criar planos de adequação a legislação.

Assim, ao confeccionar as regras de boas práticas, os controladores adjuntos com a administração devem estipular através da análise da natureza dos dados coletados, a probabilidade, a finalidade e o potencial de riscos das vantagens advindas dos tratamentos dos dados verificados. (NASCIMENTO, 2020)

É necessário pontuar que, os agentes de tratamento, após a autenticação da gravidade e sensibilidade dos dados aos riscos de operação, poderão estabelecer programa de governança em privacidade, sendo este, um instrumento amplo com normas de compliance, além dos aspectos operacionais.
Em relação ao programa de governança de privacidade, pode-se estabelecer como um aglomerado de normas-regras de boas práticas de governança, com a finalidade de executar ordens de natureza legal. (NASCIMENTO, 2020)
Portanto, os instrumentos do compliance em conjunto com a boa prática de governança, se consagram na identificação dos riscos e estruturação de medidas para a empresa, sendo respondida de forma adequada e proporcional ao suporte da tomada de decisão.
O Programa de compliance na esfera privada para análise de dados pessoais, com a finalidade de promover a segurança, deve ser constantemente monitorado e atualizado, com a implementação de ?salva vidas? em decorrência de avaliação de riscos à privacidade e o acometimento de vazamentos. (NASCIMENTO, 2020)
Portanto, os instrumentos e objetos referenciados demonstram a determinação de regras de governança no ambiente de operação de tratamento de dados pessoais, a modo que seja realizado uma estruturação nas empresas para que possibilitem a implementação de mecanismos de segurança, com a finalidade de dirimir os riscos da atividade empresarial na sociedade digital.

3 GOVERNANÇA DE DADOS

O mercado digital tem como principal ativo financeiro os dados, este considerado como ?matéria prima? de uma economia baseada no conjunto de informações, sendo que nos últimos anos, houve um aumento exponencial na coleta de dados por cooperativas, startups e novos nichos empresariais, tendo a finalidade de quantificar e gerencias os dados.
Dados, informações, conhecimento e sabedoria são os quatros estágios evolutivos da cadeia de informação, pode-se assim, compreender os dados como fatos ou registros em seu formato primário. (BEAL, 2014). Já a informação é entendida como os conjuntos processados de dados em um contexto aplicado (RÊGO, 2013). Muito embora, na sociedade da informação ?os dados são o novo petróleo?, apenas os dados isoladamente não são capazes de transformar em ativo financeiro, sendo necessário administrá-lo de forma eficaz, para que assim, as empresas adquiram vantagem competitiva.
Dessa forma, a governança de dados tem como principal objetivo atender as necessidades das empresas, ou seja, solucionar problemas, diminuir custos da administração, para que os dados transformem em saldo positivo para os negócios (TERRA, 2017).
O Data Governance Institute -DGI (2017, n.p) definiu governança de dados como ?um sistema de direitos de decisão e responsabilidades para processos relacionados à informação, executado de acordo com modelos acordados que descrevem quem pode realizar quais ações com quais informações e quando. ? Portanto, a utilização da governança de dados orienta quais os métodos deverão ser aplicados no ciclo de vida dos dados.

Uma das atribuições da governança é o acompanhamento da operação dos dados com a finalidade de gerir que as informações estejam alinhadas com os objetivos pré-determinados na coleta primária, além disso, é necessário assegurar que as informações estejam disponíveis para acesso, quando consultadas, gozar de qualidade, consistência, auditabilidade e segurança dos dados (ESPÍNDOLA, 2018).

No âmago da cadeia evolutiva da informação uma das preocupações dentro das organizações corporativas é o receio com a proteção das informações, ou seja, a capacidade das empresas no protagonismo da segurança com os provedores internos, tendo em vista a necessidade de conformidade com a legislação pátria.

A boa governança tem como objetivo aplicável à prática do controle dos processos de operação dos dados: a prevenção de situações adversas que podem gerar o comprometimento da integralidade dos dados adquiridos pelas organizações empresariais, que por sua vez, devem ter o condão de reforçar a confidencialidade das informações. (ESPÍNDOLA, 2018).

A integração do programa de governança de dados nas corporativas empresariais, tem como o esforço principal a organização de dados, que deve ser observado por um prisma basilar, ou seja, a aplicação dos princípios como limite legal e ético no ciclo de vida dos dados.

Para Rêgo (2013), os princípios são regulamentações para compreender aplicação da governança dos dados como linha direta para os negócios, sendo: (i) A gestão de dados estratégicos, tem o dever de vislumbrar as tomadas decisões por um coeficiente tático e operacional. (ii) A governança como instituição, ou seja, a governança de dados pode ser comparada como sistema governamental, na qual dispõe de legislação, execução e jurisdição; (iii) A governança de dados como um programa, devendo ser implementado como fator permanente, não apenas um projeto temporário. Ainda, pontua-se que os princípios da Governança de dados não são limitados, tendo uma orientação basilar a cada implementação de um sistema organizacional que deve ser observado pelo prisma ético e legal.

Assim, os princípios devem incumbir os papéis que a serem preenchidos pela gestão moldar os comportamentos das empresas para a aquisição, reserva e utilização dos dados conforme as normas e políticas da corporação (TERRA, 2017).

Coleta, armazenamento, recuperação e descartes, são as quatro etapas do ciclo de vida dos dados (SANTANA, 2013), ou seja, para a aquisição de dados pelas empresas, deverão observar a vida útil do dado para não incorrer na (in) responsabilidade da utilização indevida de informações dos seus provedores.

As fases do ciclo de vida dos dados devem ser observadas pela ótica de seis objetivos, sendo eles: a qualidade, a privacidade, os direitos autorais, a integração, compartilhamento e preservação dos dados (ESPÍNDOLA, 2018). Muito embora, a lei geral de proteção de dados implementou e traçou novos objetivos para a coleta de dados pessoais, cabe destacar que os objetivos vislumbrados na Governança de dados têm como parâmetro preliminar a tomada de decisão, na qual deve ser os negócios pautados nos moldes legais e éticos vigentes.

Nesse contexto, o controle de informações é necessário, tendo em vista que na sociedade da informação, cada vez mais o volume de dados é crescente, acarretando mais vazão e protesto

por políticas públicas para a preservação dos institutos, órgãos e empresas que detenham a

informação, sendo assim, necessário sistema de organização, softwares e hardwares capazes de processar as informações, criptografar e armazenar. (MARTIGNAGO, 2019)
Assim, para otimizar o ciclo de vida dos dados e garantir que os objetivos sejam preenchidos na estruturação do gerenciamento de dados, faz-se necessário a implementação de frameworks com o intuito de garantir que o procedimento seja cumprido com maior qualidade de informação e aproveitamento financeiro para a empresa, auxiliando a tomada de decisão para redução de risco para utilização de dados. (MARTIGNAGO, 2019)
Um Framework, segundo Johnson (1991), pode ser definida como um aglomerado de objetos que colabora entre si para que atinja um conjunto de obrigações para aplicação de um domínio especifico. Já para Pinto (2000), um framework é conceituado como um software incompleto criado para ser um objeto cujo estado e comportamento são definidos pela classe. Assim, o framework é uma concepção de uma arquitetura para um edifício de subsistemas e oferece o alicerce básico para criá-los.
Muito embora, os autores defendem uma conceituação distintas acerca da concepção de frameworks, pode-se verificar que ambas se complementam, tendo em vista que o framework é um sistema pré moldado, ou seja, é um programa com intuito de ser complementado através da finalidade a ser cumprida pela gestão empresarial, sendo instanciado por classes para categorizar os dados e ser alojado em hotspot, provedores físicos, capazes de armazenar as informações coletadas pelas empresas.
Portanto, para gerenciar os ativos de dados de forma complexa, ordenada e objetiva é necessário para proteção do procedimento do ciclo de vida dos dados, determinar os modelos de frameworks para o gerenciamento dos dados. Assim, para Carvalho (2021), podem ser apresentados três domínios CobiT, DAMA DMBOK e DGI Framework, sendo apenas dois destes observados para fomento deste artigo: (i) A DAMA (DAMA DMBOK), e (ii) CobiT.
A DAMA (Data Management Association) é uma associação sem fins lucrativos, com o intuito de promover boas práticas de gestão de dados, e em 2009 fundou o DAMA-DMBoK (Data Management Body of Knowledge), sendo um corpo de conhecimento que tem como ponto fundamental esclarecer como as corporativas devem aplicar a operação otimizada dos dados. (CARVALHO, 2021)
Em sua versão 2.0, acrescenta não só uma visão macro do gerenciamento de dados, definindo padrões, terminologias e práticas, mas a integração de dados, para definir táticas,

armazenamentos e sistemas, bem como implementação da ética na operação do tratamento de dados, a definição de big data e ciência de dados e amadurecimento das informações. (LIMA, 2019).
O DAMA-DMBOK V2 é formado por 11 (onze) funções de gestão de organização de

dados, sendo incorporado como cerne principal: a governança de dados, tendo em vista que os dados percorrem por toda sistemática das onzes funções ordenadas, assim segundo Honório (2021):
A primeira função é a governa de dados, sendo o pilar do framework, tem o condão de orientar e supervisionar a operação do ciclo de vida dos dados, na qual deve estabelecer um sistema de apoio a decisão dos gestores sobre os dados, sob o prisma do negócio.
A arquitetura de dados, a segunda função, pode ser conceituada como um planejamento para administrar os dados, aquisição de ativos da empresa, com o intuito de definir a finalidade das informações adquiridas com os requisitos necessário para o gerenciamento dos dados.
Por sua vez, a modelagem de dados e design, tem a função de demonstrar de forma nítida os dados, sendo o processo da descoberta, análise e representação da etapa primária da informação.
O armazenamento, uma das etapas da operação do ciclo de vida dos dados, na qual vai incluir o design, o suporte dos dados armazenados para quantificar o coeficiente valorativo das informações, até o seu descarte, devendo respeitar todo o procedimento de segurança legal vigente.
Um dos alicerces para o gerenciamento de informação é a segurança, que deve garantir a proteção dos dados, a execução de políticas e procedimento de segurança, no intuito de moderar o acesso de forma consciente e controlado, não devendo ser infringido ou acessado de forma inadequada, afim de garantir autenticação e auditoria de dados informações.
A Integração e Interoperabilidade de dados, é a função responsável pela movimentação e a concretização dos dados na interligação do armazenamento e outras plataformas.
O gerenciamento de documentos, pode ser compreendida como o gerenciamento e inclusão da vida útil dos dados e informações, encontrados em programas não estruturados, em ênfase ao conteúdo de apoio de conformidade a legislação vigente e os termos éticos formalizados para o negócio.
Dados mestre e de referência, tem como condão a manutenção dos dados compartilhados para coexistir a integralidade dos sistemas internos de gerenciamento dos dados.
Em razão da interligação entre uma linha direta com os negócios, uma das funções do DAMA-DMBOK é a Data warehousing e Business intelligence, ou seja, a implementação de

planner para o contoler da administração dos dados e suporte a decisão com o intuito de conceder aos gestores de informação emitam relatórios de equalização de valores.
Segundo Barata (2015), os metadados, na qual consiste a décima função, é promover a facilitação do acesso dos dados interligados nas multifontes do sistema integrado, como também garantir a qualidade de dados.
Por fim, o gerenciamento de qualidade de dados é a implicação das técnicas para garantir a possibilidade de aferição, melhoramento e adequação da utilidade dos dados, com o intuito de monitorar a integridade da informação primária no ciclo de vida dos dados.
Já o COBIT (Control Objectives for Information and related Technology), é um framework de suporte fundado em 1994 administrado pela ISACA (Information Systems Audit and Control Association), estruturado como um arcabouço de informação direcionadas para governança de dados e gerenciamento de informação, tem como objetivo auxiliar os profissionais de gestão na conexão entre os problemas técnicos e os riscos do negócio. (BARATA, 2015).

Para Lima (2019), o COBIT é um framework que possui duas vertentes basilares: a gestão, que possui quatro áreas de domínios: planejamento, constituição, execução e monitoramento, e a governança que é a tomada de decisão de acordo com a gestão de dados, possuindo 37 (trinte e sete) processos integrados.
Na versão 5.0, o sistema é utilizado baseado em 05 princípio, conforme elucida Casaes (2019), Barata (2015) e Lima (2019), sendo: (i) atender às necessidades das partes interessadas; (ii) cobrir o negócio como um todo; (iii) aplicar um framework único e integrado; (iv) habilitar uma visão holística; e (v) distinção entre governança de gestão.
Um dos princípios é atender às necessidades das partes interessadas, sendo a necessidade das corporativas é satisfazer as expectativas dos seus stakeholders, proporcionando um equilíbrio na tripartite: benefícios, redução do risco e recurso disponíveis.
O segundo princípio é baseado na cobertura do negócio como um todo, ou seja, abranger a integralidade da empresa no processo, procedimento, pessoas e as relações com os habilitadores.
A aplicação do framework único e integrado, assim, o COBIT é capaz de promover uma relação completa com a Governança de dados, corroborando ao alinhamento com padrões externos e adaptabilidade dos modelos usuais de negócios.

O COBIT permite habilitar uma visão holística, ou seja, uma visão macro dos componentes que oferecem suporte para atingir as finalidades da governança de dados, na qual define como catalogadores: as políticas, processos, estruturas organizacionais, informação e ética.
Por derradeiro, o princípio da distinção entre governança de gestão, tendo em vista que ambos possuem estruturas organizacionais distintas, assim, governança tem como esforço principal que os objetivos corporativos sejam cumpridos, estabelecendo prioridades pela tomada de decisão, compliance e progresso das organizações. Por sua vez, a gestão é o planejamento, construção, execução e monitoramento das funções ornamentada com o direcionamento da governança.
Desse modo, com escalonamento dos cinco princípios é capaz de proporcionar o funcionamento otimizado do framework, destacando os seguintes processos:
O APO01: Gerenciar o framework de TI, tem como condição a otimização das atividades relacionadas ao TI, com a função principal de incluir os procedimentos e regulamentos para promover a integralidade das informações nos bancos de dados. (BARATA, 2015)
Já o APO03: Gerenciar a arquitetura corporativa, tem função primordial agrupar as informações para auxiliar as atividades e tomadas de decisões, conceituando e compartilhando as informações dos elementos dos dados, e por fim catalogar a empresa, com base na modulação e sensibilidade dos dados. (BARATA, 2015)
Nesse ínterim, a governança de dados como um sistema integrado com o programa de compliance, tem o condão de otimizar a operação de controle interno relacionado aos dados coletados pelas empresas, capaz de gerenciar as bases para o apoio de decisão ao tratamento das informações, com segurança e qualidade, garantido o ciclo da vida útil dos dados.

4 A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

As estruturas políticas, econômicas e sociais com desenvolvimento de novas tecnologias e mecanismo para a coleta de dados e informações, fez necessário modulações legislativas para a proteção da privacidade, além dos aspectos físicos, patrimoniais e morais.
A proteção à privacidade de dados foi dividida em quatros gerações: a primeira, oriunda do estado moderno, com o advento dos bancos de dados; a segunda, datada em 1980, com a expansão legislativa para a proteção à privacidade aos setores privados; a terceira geração em 1990, com o processo de tratamento de dados e o consentimento dos cidadãos; Por fim, a última dimensão, é

destinada ao protagonismo da permissão para coleta e uso dos dados pessoais, quando a lei estabeleceu a importância da titularidade das informações. (MENDES, 2014)
Nesse aspecto, é perceptível a evolução do direito aos fatores reais da sociedade e as transformações dos meios tecnológico, computacionais, genéticos e comunicativos, que por sua vez possibilitou a integração da comunicação global, e consequentemente, o rastreio dos dados através do armazenamento de informação. (SAAD, 2021).
Os legisladores ao considerar os dados pessoais como extensão ao direito à privacidade, preocuparam em tutelar constitucionalmente a proteção da população, em especial os países europeus, como: Espanha, Portugal, Hungria, Eslovênia e Rússia. (VIEIRA, 2007) Porém, só tornou-se fator primordial após o regulamento geral do Parlamento Europeu sobre a proteção de dados, n.º 2016/679, sendo necessário a adequação das empresas prestadoras de serviço na Europa ao regulamento, influenciado diretamente o Brasil para elaboração da Lei Geral de Proteção de Dados brasileira. (SAAD, 2021).
Muito embora, a Lei Geral de Proteção de Dados Pessoais - LGPD, em sua promulgação, não abarcou de forma expressa a proteção de dados como direito fundamental, a doutrina, em especial Nascimento (2020), por sua vez, já argumentava a proteção de dados e informações pessoais como direito autônomo, derivado do direito fundamental à privacidade, explicitamente no artigo 5°, X, da CRFB de 1988.
Após reiterados julgamento sobre a tutela dos dados pessoais como extensão da personalidade do indivíduo, o Supremo Tribunal Federal -STF reconheceu no Julgamento da Ação Direta de Inconstitucionalidade - ADI 6387, a existência dos dados como direito autônomo, derivada do direito fundamental a dignidade da pessoa humana, na proteção à intimidade e a centralidade do Habeas Data como autodeterminação informativa. (NASCIMENTO, 2020).
Ao compreender a necessidade da proteção aos dados pessoais, os legisladores brasileiros em votação de ? das casas legislativas (câmara e Senado Federal) em dois turnos, aprovaram a Emenda Constitucional 115 de fevereiro de 2022, alterando o artigo 5° da Constituição Federal de 1988, incluindo o inciso LXXIX, tutelando constitucionalmente a proteção aos dados pessoais, inclusive nos meios digitais.
Ressalta-se, ainda, que os dados pessoais estão interligados com o direto fundamental à privacidade, na qual representa a capacidade de a pessoa administrar sua vida, seus pertences e

propriedades materiais e imateriais, permitindo ou não a utilização dos seus dados (bens imateriais) por terceiro. (NASCIMENTO, 2020).

A privacidade, por sua vez, segundo Mendes (2008), é o direito à proteção aos comportamentos pessoais e acontecimentos de caráter íntimo, bem como as informações prestadas aos profissionais e comerciantes, em que a pessoa não deseja que se compartilhe com o público.

Para o professor William Prosser, pode-se qualificar a lesão a privacidade em quatro graus: i) o intrometimento na reclusão ou solidão na vida privada, ii) a divulgação pública de fatos privados constrangedores sobre o indivíduo; iii) a publicidade sobre o indivíduo apresentada de forma equivocada; e iv) a apropriação, para obtenção de vantagem, do nome ou da imagem do demandante (PROSSER, 1960).

A doutrina, por sua vez, defende mais uma violação à privacidade: a privacidade informacional, interligada com os fatores tecnológicos de informação. (SAAD, 2021). Assim, quando a lei ao realizar o tratamento da privacidade, refere-se como um direito líquido, ao qual será tutelado para garantir que o indivíduo tenha um local reservado, que não tenha, se desejar, a interferência de outros sujeitos, seja pessoa física ou jurídica.

Com a proteção dos dados pessoais dos titulares, através da LGPD, possibilitou ao cidadão o acesso a informações ao ciclo de vida útil dos dados pelas empresas, e a certeza de fiscalização pela Autoridade Nacional de Proteção de Dados, com a finalidade de atingir os objetivos traçados pela legislação, na qual a lei traz conceitos e delimita princípios, que devem ser mencionados.

A LGPD tem como objetivo principal: ?o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado?, com a destinação de assegurar os direitos fundamentais a liberdade e privacidade dos titulares dos dados, bem como tutelar a dignidade e a personalidade da pessoa natural. (LGPD).

A legislação está ordenada diretamente com o meio empresarial, sobretudo no que se refere aplicação aos seus destinatários que são pessoas físicas ou jurídicas que realizam a coleta e tratamento de dados no Brasil, conforme preceitua o artigo 1° da lei 13.709, de 14 de agosto de 2018.

Para compreender a LGPD, faz-se necessário elucidar os conceitos de dados pessoais: (art. 5º, I) é toda informação relacionada a pessoa natural, identificada ou identificável, sendo o dado aplicado no contexto que possibilite o reconhecimento do indivíduo. Bem como refere-se aos dados sensíveis (art. 5º, II), são todas as informações que se relaciona com pensamentos políticos, crenças,

identidade biológica e física. Portanto, a legislação tem como ponto a proteção e o cuidado para a não violação dos dados pessoais e sensíveis.

Os doutrinadores, Laura Schertel e Danilo Doneda, ainda aponta cinco pilares para compreender a LGPD, sendo: i) a unidade e generalidade da aplicação da Lei; ii) a legitimação para o tratamento de dados (hipóteses autorizativas); iii) os princípios e direitos do titular; iv) as obrigações dos agentes de tratamento de dados e v) a responsabilização dos agentes.

O primeiro pilar é considerado com aplicabilidade material da legislação, ou seja, aplica-se a qualquer operação realizada por pessoa natural ou jurídica de direito público ou privado,

independentemente do meio, da sua sede ou do país onde estejam localizados os dados (Art. 3°). Considerado, assim, como uma aplicação uniforme para todos os setores público ou privados que realizam tratamento de dados.

O segundo pilar é a legitimação para o tratamento de dados, tendo em vista que a lei especificou critérios e requisitos para o reconhecimento da legitimidade, não podendo ser tratados os dados, sem que exista uma base normativa que autorize, prevista no artigo 7°, 11° ou 23° da LGPD, abordando 11 (onze) hipóteses, incluído o consentimento ou a previsão legislativa.

Destaca-se que a autorização por consentimento para ser considerado válido, deve observar os requisitos previsto no artigo 5°, XII, sendo considerado que a vontade deve ser livre, informada, inequívoca e com a finalidade determinada, consagrando os princípios norteadores da legislação.

O terceiro pilar é o conjunto de princípios e direitos que assegura o destinatário da lei a controlar a utilização do seu dado pessoal, sendo importante elencar dez princípios que estruturam a LGPD: a finalidade, a adequação, a necessidade, o livre acesso, a qualidade dos dados, a transparência, a segurança, a prevenção, a não discriminação e a responsabilização. (MENDES, DONEDA, 2018)

No que concerne, aos direitos dos titulares são expressos no artigo 18° da referida lei, que permite o titular dos dados adquirir através do controler, independentemente do momento, as informações relacionadas ao indivíduo, prevendo: acesso, confirmação, correção, anonimização, bloqueou ou eliminação e a portabilidade.

Para adentrar no cerne dos problemas enfrentados pela legislação, em especial, sobre o vazamento de dados, os dois últimos pilares serão abordados sob a perspectiva da violação e responsabilização acerca da proteção de dados nos casos incidentes de vazamento.

Assim, o quarto pilar, destina-se às obrigações dos agentes de tratamento dos dados, na qual estabeleceu limites que devem ser observados nas operações realizadas para reforçar a segurança e prevenir os problemas da atividade no tratamento de dados.

Uma das obrigações fundamentais, consiste na intitulação do encarregado pelo tratamento dos dados indicados pelo controlador, conforme artigo 41 da LGPD, que possui a função de aceitar as reclamações e comunicações dos sujeitos dos dados, receber informações da Autoridade Nacional, como deve orientar os funcionários a respeito das práticas a serem adotadas em relação à proteção de dados pessoais.

Assim, as informações devem ser fornecidas ao proprietário dos dados, quando os dados forem coletados, como: os meios de segurança aderidos ao tratamento de dados, quais são os riscos da atividade que podem gerar lesão ao titular, pois pode gerar a mitigação dos prejuízos. (SAAD, 2021)

A lei Geral de Proteção de Dados Pessoais tem como objetivo a proteção do dados pessoais dos titulares dos dados, sendo assim, uma das obrigações principais é adoção de medidas de segurança, técnicas e administrativas hábeis a proteger os dados pessoais de acessos não autorizados, como promover a integralidade dos dados, não permitindo, assim, a alteração das informações, a prevenção de situações ilícitas ou acidentais, ou qualquer forma de tratamento inadequado, consoante se desprende do artigo 46 da lei.

Tornou-se corriqueiro manchetes acerca do vazamento de dados por corporativas, uma das violações mais graves incidentes abarcados pela LGPD, o que ocasiona a vulnerabilidade do titular dos dados, e dos sistemas internos que são responsáveis pelo ciclo de vida útil dos dados. (SAAD,2021)

A seção de segurança de informação tem como condão as obrigações inerentes aos agentes de tratamento, devendo ser adotado pela integralidade das pessoas que realizam o tratamento de dados, garantido que os dados sejam confidenciais, bem como disponíveis nas operações de tratamento. (Art.48). Nos casos incidentais de vazamento de dados, insurge a necessidade ao controlador de informar a autoridade de proteção de dados, que podem definir as medidas para mitigação dos danos.

No entanto, com a utilização da internet, compras online, transferência virtuais e outros meios tecnológicos, criou-se uma dificuldade para atuar na segurança de dados, tendo em vista a abrangência e os domínios de redes globais, que combinados com fatores não perceptível, forma

um perfil não rastreavel capaz de ocasionar violação às diretrizes básicas da legislação, que mesmo com ações posteriores não conseguem excluir os inúmeros registros de pessoas e organizações que coletaram os dados, lesionando a confidencialidade das informações (SAAD, 2021)

Destaca-se que as obrigações aos controladores e operadores, devem ser observados desde a coleta dos dados até seu descarte, assim o artigo 46 da LGPD, introduziu o conceito de privacy by design, sendo a incorporação pelas empresas nos serviços e produtos, na qual dispõe a proteção da privacidade no centro de todo o desenvolvimento corporativo.

Embora, a legislação tenta dirimir os riscos da atividade, os prejuízos causados pelo vazamento de informações são altos, e perpassam pela inadequação do sistema de proteção, perda de credibilidade e de clientes, ocasionado uma ruptura na imagem da empresa, impossibilitando, muitas vezes de concorrer no mercado corporativo. (SAAD,2021)

Portanto, a LGPD concebeu obrigações aos agentes de tratamento de dados, para que se delimite a finalidade da utilização dos dados desde o início da concepção, devendo o controlador confeccionar relatório de impacto a privacidade, utilizando de métodos para a captação da operação do ciclo de vida dos dados, observando as mediadas adotada para aumentar a segurança e mitigar o risco do tratamento das informações, conforme artigo 3 da LGPD.

O último pilar, considerado como a responsabilidade dos agentes na incidência de ocorrência de danos derivados do tratamento de dados. A LGPD consagrou a natureza do tratamento, limitando os parâmetros ao artigo 7° da lei, nas 10 hipóteses dos incisos, vinculados a finalidade da captação dos dados, consoante prevê o artigo 6°, inciso I, II, da LGPD.

A legislação tem como regra o descarte (eliminação) dos dados ao fim do tratamento da operação (art. 16), com o intuito de mitigar os riscos presente no tratamento de dados, principalmente, no que concerne à limitação das hipóteses de tratamentos para não lesionar os direitos dos titulares.

Nos casos, em que mesmo após o término de vida útil dos dados, as empresas podem, quando permitido, armazenar dados que em situação incidentais serem objetos de violação, principalmente nos casos de vazamento, que podem ocorrer, quando não autorizados pelo titular

ou controladores, serem acessados, captados, compartilhados pela internet, para outros sujeitos ou empresas.
Assim, a Lei Geral de Proteção de dados Pessoais, em especial em seu artigo 42, dispõe que o controlador ou operador, quando realizar o exercício do tratamento de dados pessoais, vem

a ocasionar dano patrimonial, moral, individual ou coletivo em detrimento a aplicação da legislação, é obrigado a repará-lo, definindo a responsabilidade de forma objetiva.
Embora, a responsabilização objetiva não é necessária a demonstração de culpa do controlador ou operador. Faz mister esclarecer que o operador, só será responsabilizado quando os atos praticados forem contrário à legislação, ou às instruções que foram fornecidas pelo controlador. (MENDES, DONEDA, 2018)
Ainda, a legislação prevê exceções a responsabilidade objetiva (art. 43), sendo: quando o agente demonstrar que não realizou o tratamento de dados pessoais que foi atribuído, ou quando não houve violação da segurança ou a legislação, e por fim, quando for por culpa exclusiva do titular ou de terceiros.
Porém, o cenário que é vislumbrado no Brasil nos casos de vazamento de dados, é que as violações pelas instituições vêm ocorrendo, majoritariamente, sob ataques deliberados de hacker, ou falha de segurança dos controladores dos dados. (SAAD, 2021)
Dessa forma, é necessário adotar medidas para dirimir os riscos da atividade, e possibilitar o discernimento das informações acerca dos perigos de vazamento de dados, tendo em vista que a tendência é aumento significativo das violações vinculados com a crescente tecnológica. Assim, as empresas devem implementar mecanismos para a segurança das informações.

5 O COMPLIANCE EMPRESARIAL COMO INSTRUMENTO DE PROTEÇÃO DE DADOS NA ESFERA EMPRESARIAL

Em decorrência das constantes violações aos dados armazenados em provedores privados, a tutela ao direito à privacidade nos meios tecnológicos, já era pauta de debate na legislação brasileira, e já existiam mecanismos para a proteção, como: a proibição de direcionamento dos provedores em relação ao compartilhamento de dados, bem como a inibição ao monitoramento nos navegadores de internet.
Vinte e seis bilhões de dados foram vazados no Brasil em 2019, de acordo com pesquisas realizadas pelo Massachusetts Institute of Tecnology ? MIT, possibilitando a utilização de números telefônicos, score de crédito, endereço eletrônico, fotos, números de identificações e outros dados pessoais, para o cometimento de crimes cibernéticos, e a violação aos direitos dos titulares.
A utilização e uso dos dados pessoais por pessoa física ou jurídica, com sede no Brasil ou não, devem se atentar as normas gerais de proteção aos dados brasileiro, segundo Frazão, Oliva e

Abilio (2020), é a necessidade de conferir a efetividade aos direitos e prevenir a violação aos dados, através da implementação de mecanismo de compliance, como uma ferramenta capaz de promover a adequação das atividades aportadas pelas empresas.

Assim, os controladores e operadores poderão formular regras de boas práticas e governança (Art. 50), que contenha as disposições de organização interna, o regime de funcionamento, as operações, o canal de comunicação entre os encarregados e os titulares dos dados, e o procedimento de segurança.

Nessa perspectiva, considerando que a maioria das tratativas de dados perpassam por meios digitais, deve-se adotar sistema para mapear os riscos, e implementar mecanismos para minorar as vulnerabilidades apontadas pelos programas, através da alta administração, do código de ética, para proteger os dados pessoais dos titulares. (PESSOA, 2021)

Existem inúmeras formas de ocorrer o vazamento de dados, sendo através de ataques cibernéticos, sequestro de conta, furtos de dados, compartilhamento de dados por agentes ou ex-agentes da empresa, erro ou negligência, entre outros, que podem ser para adquirir dados de nomes, CPF, celulares, endereços, dados financeiros, senhas, registro de saúde ou credenciais de acesso. (SAAD, 2021)

Desse modo, para realizar o mapeamento dos problemas que as corporativas podem enfrentar, é necessário identificar os fluxos e processos de informação que percorrem os sistemas, que irão auxiliar na tomada de decisão pelas empresas. (NASCIMENTO, 2020)

A alta administração deverá colaborar ativamente no programa de compliance, seja monitorando as investigações e intervenções em situação para estabelecer controles internos em conformidade com a legislação, bem como possibilitar a interdependência dos setores para realizar as atividades designadas para o tratamento de dados (PESSOA, 2021).

Com a elaboração do código de ética pela organização possibilitará o treinamento regular das equipes, responsáveis pela tecnologia da informação, para enraizar a cultura corporativa da boa governança, com a finalidade de assegurar o respeito ao programa de compliance (NASCIMENTO, 2020)

Nesse contexto, para manter uma boa relação com seus clientes, as organizações devem instalar canais de comunicação, para que os titulares dos dados possam contatar os encarregados responsáveis pelos armazenamentos dos seus dados, e exerçam seus direitos sobre as informações contidas nos provedores. (PESSOA, 2021).

Desse modo, quando se trata de concretização a alteração cultural coportariva é preciso realizar o alinhamento dos funcionários com o código de ética, com política de privacidade, para fins de efetividade do programa de compliance de dados. (PESSOA, 2021).

5.1 A IMPLEMENTAÇÃO DE MECANISMOS DE GOVERNANÇA DE DADOS PESSOAIS

Para a efetividade da legislação em relação ao tratamento de dados, a LGPD direciona um capítulo para implementar o programa de governança em privacidade, com a finalidade das empresas adotarem medidas técnicas, para fins de proteção e segurança dos dados pessoais.

(PESSOA, 2021)
A governança em privacidade, pode ser conceituada como um conjunto de regras e práticas positivas a serem implementadas pelos agentes de tratamento, e encontra-se em conformidade com as políticas de compliance empresarial, com o objetivo de gerir os dados das empresas para estabelecer um diferencial competitivo aos negócios. (KOEPSEL,2020)
O programa integra o aperfeiçoamento do procedimento de utilização dos dados, com os requisitos pré-estabelecidos na implementação dos softwares, com a finalidade de gerir de forma otimizada os dados para preencher as diretrizes da legislação. (SAAD, 2021)
A Lei Geral de Proteção de Dados Pessoais dispôs que os controladores e operadores poderão adotar programas de governança em privacidade, que devem ser implementados com o mínimo, (art. 50, § 2°, I): a) o comprometimento dos agentes de tratamento com as políticas internas que devem garantir o cumprimento das normas e regras de boas práticas; b) que aplicação seja de forma uniforme para todo a operação de tratamento de dados; c) que a governança seja adaptativa as estruturas da empresas, sendo compatível com a densidade dos dados e operação; d) como implementar políticas de salvaguardas em relação aos titulares dos dados; e) tenha como objetivo estabelecer uma relação de confiança com sujeitos dos dados, estabelecendo situações de transparência e que possibilite a atuação do titular; g) que conte com planos de respostas a incidentes e remediações; h) seja continuamente atualizado sua base.
Nesse aspecto, devem ser adotadas medidas administrativas para que as instituições, em conformidade com a legislação, apliquem estímulos para assegurar as informações armazenadas pelas empresas, com a adoção de orientações internas que respeitem as diretrizes que inclua o uso

minimizado ou a anonimização das informações, desde a coleta dos dados, conforme artigo 46 da LGPD.
Com o mapeamento das atividades, é importante verificar: O que são esses dados?; de que forma foram coletados ?; quem são os coletores ?; existe relação entre os dados e atividade realizada ?; O que pode ocorrer com esses dados ao serem coletados? E, como são descartados da gestão organizacional da empresa? (NASCIMENTO, 2020). Dessa forma, para adotar medidas compatíveis com os riscos alertados pelos sistemas para a proteção de dados nas organizações privadas, é necessário possuir conhecimento do caminho realizado inerentes ao ciclo de vida útil dos dados.
Embora, a legislação já estabeleça diretriz mínima para o tratamento de informação, a Autoridade Nacional de Proteção de Dados - ANPD, poderá, ainda, determinar padrões técnicos para serem implementados pelo programa de governança em privacidade, devendo ser observado a qualidade de dados, as especificações do tratamento e status tecnológico, em especial a proteção aos dados sensíveis disposto na legislação. (NASCIMENTO, 2020)
Muito embora, a lei geral de proteção de dados, apenas delimita as características e os requisitos mínimos que os operadores deverão tomar para desenvolver um compliance na organização das empresas privadas em consonância com a legislação, porém não impõe um modelo específico para integração de um programa nas corporativas. (PESSOA, 2021)
Assim, para Saad (2021), as medidas técnicas que podem ser adotadas pelos agentes de

tratamento de dados, são: i) o uso de firewalls, sendo um mecanismo de segurança que coleta os dados em conformidade com as regras pré estabelecido para análise de tráfego de rede, delimitando as operações de compartilhamento e captação de informações a serem cumpridas; ii) a utilização de antimalware, que consiste na proteção contra vírus que é capaz de fragilizar o sistema, apagar dados e infectar outros arquivos; iii) a utilização de criptografia dos dados, que possibilite quando ocorrer situações incidentais a não identificação do titular do direito.
Já para Fernandes e Abreu, (2014) defendem a implementação de frameworks como a DAMABOK e COBIT, para o gerenciamento de dados, pois tem como meta principal a delimitação do escopo das atividades, as funções envolvidas no tratamento e as interações a serem executadas pelo software, com a finalidade de proteger a privacidade em ambientes corporativos que gerenciam o armazenamento de informações aplicados na prevenção à fraude.

Segundo Carvalho (2021), a integração do software, através das boas práticas estabelecidas pela legislação, poderá aprimorar os aspectos de proteção à privacidade e prevenção a fraude do tratamento de coleta de dados. Tendo em vista, que os frameworks, podem balizar as métricas de qualidade dos dados que indicam uma utilização adequada e otimizada, e aponta a melhor proteção da privacidade.
Com a melhoria de processo de governança para o tratamento de dados, estabelece uma divisão entres as operações que possibilita uma automatização do ciclo de vida dos dados (coleta, utilização, armazenamento e exclusão), capaz de gerar relatório de risco, para o auxílio da tomada de decisão com o intuito de gerir de forma adequada o tratamento de dados. (CARVALHO, 2021)
Neste parâmetro, os programas de compliance com a implementação de frameworks, podem responder questionamento acerca do procedimento de tratamento de informação, dispondo de quais práticas relacionadas à governança, privacidade e segurança de dados, apresentam melhor benefício para o tratamento de dados pessoais. (CARVALHO, 2021)
Ademais, os controladores e operadores deverão adotar medidas, como o Relatório de Impacto ? DPIA), que corresponde a avaliação dos riscos e impactos relacionados com o tratamento de dados pessoais, além da anonimização, da transparência e do sigilo, deverão delimitar prazos para retenção de dados e aderir políticas seguras de informação acerca da operação de tratamento. (SILVA, 2022)
Após realizar a implementação e observância das estruturas mínimas estabelecidas pela LGPD, é necessário adotar um programa de gerenciamento de vulnerabilidades, com atualizações constantes e autocorreções alinhados com as boas práticas de atividades cotidianas, com a finalidade de proteger os dados pessoais, e promover um ambiente corporativo adequado para realizar o tratamento de dados. (SAAD, 2021)
No entanto, ao verificar que houve vazamento de dados, seja pelo recebimento de notificação ou pela veiculação na mídia, os agentes de tratamentos deverão identificar quais dados vazaram e realizar o procedimento estabelecido no programa de compliance de segurança, além de notificar as instituições. (Art. 48, caput).
De acordo com MIT, o prazo entre a comunicação à autoridade competente e a ocorrência do fato ilícito ultrapassa 200 (duzentos) dias em média, sendo umas das preocupações para a

efetividade da legislação, e a redução dos danos causados aos titulares dos bens imateriais.

A Lei Geral de Proteção de Dados, dispõe que nas situações que ocorrer a probabilidade de riscos ou violação aos direitos dos titulares, tem como obrigação do encarregado a comunicação à autoridade nacional e ao titular do dado (art. 48, caput). Sendo que o contato deve ser em período razoável (art. 48, § 1º), contendo a natureza dos dados dos titulares atingindo (art. 48, § 1º, I).
Em decorrência dos possíveis incidentes, a LGPD determinou critério para aplicação de sanções, em casos de vazamento de dados, observando as situações específicas de cada caso, disposto no art. 52, § 1º. Assim, deve ser considerada a avaliação da gravidade, a natureza das informações e do dano ocorrido (incisos I e VI), sendo necessário para este caso, tendo em vista que o compartilhamento indesejado de dados sensíveis pode ocasionar danos irremediáveis para os titulares.
Portanto, existe a necessidade da adesão aos mecanismos e técnicas para promover a efetividade dos programas internos com a finalidade de mitigar os danos, assim, a implementação de boas práticas e governança têm como fator o cumprimento da legislação, por meio de medidas de segurança. Entende-se, que a proteção integral contra falhas que possibilitam a ocorrência de ilícitos não é possível, porém essas diretrizes reduzem as possibilidades de existir desvios de condutas e criar salvaguardas para identificação dos incidentes, de forma eficaz, rápida e adequada.

6 CONSIDERAÇÕES FINAIS

A partir da permissão ao acesso dos dados pessoais, as informações coletadas passaram a integralizar as redes de tratamento de dados, tornando-se alvo de ataques cibernéticos, contribuindo para o aumento da intercorrência no ambiente corporativo, tornando-se o gerenciamento de informação um dos diferenciais no desenvolvimento do negócio.
Nesse contexto, foi imperativo o surgimento de leis que protejam os dados dos cidadãos, e que limitem a gestão das entidades públicas e privadas em relação as informações coletadas, transformando o sistema organizacionais, como compliance, em ferramentas de efetivação das normas éticas e legais. Assim, a implementação do programa alinhado com a governança corporativa é capaz de integralizar o corpo de normas internas com o intuito de adequar a legislação brasileira e criar uma cultura corporativa.
Dentro do programa de compliance, a administração em conjunto com a gestão da empresa, poderá implementar ao plano diretor, a utilização de software, sendo este capaz de possibilitar a automatização do ciclo de vida útil dos dados para realizar o auxílio da tomada de decisão, com o intuito de mitigar os possíveis danos decorrentes da violação aos dispositivos da Lei Geral de Proteção de Dados Pessoais.
Nesse sentido, para realizar uma proteção extensiva aos direitos dos titulares dos dados, a

LGPD integrou ao seu corpo de normas-condutas a serem adotadas pelos operadores do tratamento de dados, com escopo de preservar a integralidade, a qualidade e o sigilos dos dados, tendo como consequência da violação, a majoração de sanções pecuniárias.
Embora, o vazamento de dados ocorra de forma ordenada, a implementação de sistema de segurança nas corporações implica na diminuição de situações incidentais por erro humano, ou inadequação dos programas empresarias, assim, devendo a gestão ensejar esforços para que a proteção dos dados seja preservada, desde a concepção do serviço.
Para a efetivação da Lei Geral de Proteção de Dados Pessoais, as empresas devem realizar a adequação de medidas de boas práticas e governança em privacidade para mitigar os possíveis danos decorrente da violação aos dados em provedores privados. Mesmo que a proteção aos dados de forma concreta não seja possível, as adoções de mecanismo de segurança podem atenuar as sanções e as perdas aos titulares dos dados.

REFERÊNCIAS

BARATA, André Mantola. Governança de dados em organizações brasileira: uma avaliação comparativa entre os benefícios previstos na literatura e os obtidos pelas organizações. 2015. Dissertação (Mestrado em Sistema de Informação) - Universidade de São Paulo, São Paulo, 2015.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, [2022]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 15 abr. 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidente da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 abr. 2023.

BERTOCCELLI, Rodrigo de Pinho. Compliance. In: CARVALHO, André Castro et. al. Manual de compliance. Rio de Janeiro: Forense, 2019. p. 35.

CANDELORO, Ana Paula; RIZZO, Maria Balbina Martins De; PINHO, Vinícius (Coord). Compliance 360: riscos, estratégias, conflitos e vaidades no mundo corporativo. São Paulo: Trevisan, 2012.

CARVALHO, A. P. Proposta de um framework de compliance à Lei Geral de Proteção a Dados Pessoais (LGPD): um estudo de caso para prevenção a fraude no contexto de big data. 2021. Dissertação (Mestrado em Engenharia Elétrica) - Universidade de Brasília, Brasília, 2021.

CARVALHO, Andre Castro. Manual de compliance. 3. ed. Rio de Janeiro: Forense, 2021.

CASAES, Júlio César Costa. Governança de dados abertos governamentais: frameworks conceitual para as Universidades Federais, baseada em uma visão sistemática, 2019. Tese (Doutorado em Engenharia e Gestão do Conhecimento). Universidade Federal de Santa Catarina, Florinaóplis, 2019.

DATA GOVERNANCE INSTITUTE (DGI). Definitions of data governance. 2017. Disponível em: http://www.datagovernance.com/adg_data_governance_definition. Acesso em: 01 mai. 2023.

ENDEAVOR DO BRASIL. Prevenindo com o Compliance para não remediar com o caixa. In: ENDEAVOR. [S. l.], 26 abr. 2017. Disponível em: https://endeavor.org.br/pessoas/compliance/. Acesso em: 15 mar. 2023.

ESPÍNDOLA, P. L.; SALM JUNIOR, J. F.; ROSA, F.; JULIANI, J. P. Governança de dados aplicada à ciência da informação: análise de um sistema de dados científicos para a área da saúde. Revista Digital de Biblioteconomia & Ciência da Informação, Campinas, v. 16, n. 3, p. 274-298, 2018.

FERNANDES, Aguinaldo Aragon; DE ABREU, Vladimir Ferraz. Implantando a governança de TI: da estratégia à gestão de processos e serviços. 4. Ed. Rio de Janeiro: Brasport, 2014.

FRAZÃO, Ana. Programas de compliance e critérios de responsabilização de pessoas jurídicas por ilícitos administrativos. In: ROSSETTI, Maristela Abla; PITTA, Andre Grunspun. Governança corporativa: avanços e retrocessos. São Paulo: Quartier Latin, 2007. p. 42

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. A Lei Geral de proteção de Dados Pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

HONÓRIO, Roseli. Modelo conceitual de governança de dados como suporte à governança do conhecimento organizacional. 2022. Dissertação (Mestrado em Engenharia e Gestão do Conhecimento) - Universidade Federal de Santa Catarina, Florianópolis, 2022.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC). Guia das melhores práticas de governança para cooperativas. São Paulo, 2015. Disponível em http://www.ibgc.org.br/ userfiles/files/2014/files/CMPGPT.pdf

JOHNSON, Ralph E.; RUSSO, Vincent. Reusing object-oriented designs. Relatório Técnico da Universidade de Illinois, UIUCDCS 91-1696, 1991.

KLEINDIENST, Ana Cristina. Grandes temas do direito brasileiro: compliance. São Paulo: Almedina Brasil, 2019

KOEPSEL, Alice de Medeiros. Adoção e efeitos dos programas de compliance à luz da Lei Geral de Proteção de Dados Pessoais. 2020. Monografia (Graduação em Direito) -Universidade do Sul de Santa Catarina, Florianópolis, 2020.

LIMA, C., BASTOS, R. C. A criação de conhecimento apoiada pela governança de dados. In: CONGRESSO INTERNACIONAL DE CONHECIMENTO E INOVAÇÃO, 2019, Santa Catarina. Anais eletrônicos [...]. Santa Catarina Disponível em: https://proceeding.ciki.ufsc.br/index.php/ciki/article/view/647. Acesso em 10 Mar. 2023.

MARTIGNAGO, Deisi et al. Governança de dados aplicado no processo de catalogação. Revista Brasileira de Biblioteconomia e Documentação, São Paulo, V.15, n. 2, 2019.

MENDES, Gilmar Ferreira. Curso de direito constitucional. 2. ed. São Paulo: Saraiva, 2008.

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. São Paulo: Revista de Direito do Consumidor, 2018.

NASCIMENTO, Suellen Lima do. A lei Geral de Dados Pessoais e a Adoção dos Programas de compliance na sociedade da Informação. 2020. Monografia (Graduação em Direito) - Centro Universitário de Brasília, Brasília, 2020.

PESSOA, Larissa Rocha de Paula. Os desafios da Governança de dados e a realidade cultural brasileira. 2021. Dissertação (Mestrado em Direito) ? Universidade Federal do Ceará, Fortaleza, 2021.

PINTO, S. C. C. S.. Composição em Web Frameworks, 2000. Tese (Doutorado em Informática) Pontifícia Universidade Católica do Rio de Janeiro, Rio Janeiro, 2000.

PROSSER, William L. Privacy. California Law Review. California, v. 48, n. 3. p. 383 ? 423, agosto, 1960.

RÊGO, Bergson Lopes. Gestão e governança de dados: promovendo dados como ativo de valor nas empresas. 1. ed. Rio de Janeiro: Brasport, 2013,

ROQUE, Pamela Romeu. Estudos aplicados de direito empresarial: LL.C. em direito empresarial. São Paulo: Almedina, 2019.

SAAD, Carolina de Oliveira. A lei geral de proteção de dados pessoais e incidentes de segurança: regulação e prática de vazamento de dados, 2021. Monografia (Graduação em Direito). Fundação Getúlio Vargas. Rio de Janeiro, 2021.

SANTANA, Ricardo Cesar Gonçalves. Ciclo de vida dos dados e o papel da ciência da informação. In: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO. 14., 2013. Florianópolis. [?]. Florianópolis: UFSC, 2013. Disponível em: http://enancib2013.ufsc.br/index.php/enancib2013/%20XIVenancib/paper/viewFile/284/319. Acesso em: 13 mar. 2023.

SILVA, Ana Laura Fonseca. O papel das Soft Skills na implementação efetiva dos programas de compliance com foco na adequação à Lei Geral de Proteção de Dados ? Lei N° 13.709/18. 2022. Monografia (Graduação em Direito) - Universidade Federal de Ouro Preto, Ouro Preto. 2022

SILVA, Eggon João da. A defesa da ética e transparência. In: VENTURA, Luciano Carvalho. Governança corporativa. São Paulo: Saint Paul Editora, 2005, página 259.

TERRA, Priscila de Mello. A influência da governança de dados na gestão estratégica, 2017. Monografia (Bacharelado em Sistema de Informação) - Universidade Federal Fluminense, Niterói, 2017.

VAZAMENTO de dados aumentaram 493% no Brasil, segundo pesquisa do MIT.VEJA, São Paulo, 24 fev. 2021. Sociedade. Disponível em: https://vocesa.abril.com.br/sociedade/vazamentos-de-dados-aumentaram-493-no-brasil-segundo-pesquisa-do-mit. Acesso em: 15 mar. 2023.

VIEIRA, Tatiana Malta. O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante da tecnologia da informação. Porto Alegre: Sergio Antonio Fabris Editor, 2007.

==========

Arquivo 1: TCC - A IMPORTÂNCIA DO COMPLIANCE NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA - WESLEY VICENTE.pdf (8805 termos)
Arquivo 2: https://textranch.com/376824/this-work-aims-to/or/this-work-is-aimed-to (2316 termos)
Termos comuns: 4
Similaridade: 0,03%
O texto abaixo é o conteúdo do documento TCC - A IMPORTÂNCIA DO COMPLIANCE NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA - WESLEY VICENTE.pdf (8805 termos)
Os termos em vermelho foram encontrados no documento https://textranch.com/376824/this-work-aims-to/or/this-work-is-aimed-to (2316 termos)

==========

WESLEY VICENTE DA SILVA

A IMPORTÂNCIA DO COMPLIANCE EMPRESARIAL NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA

SALVADOR
2023

WESLEY VICENTE DA SILVA

A IMPORTÂNCIA DO COMPLIANCE EMPRESARIAL NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA

Artigo apresentado como requisito parcial para obtenção do título de Bacharel em Direito pela Universidade Católica do Salvador.

Orientador: Prof. Darlã Conceição Santos.

SALVADOR
2023

A IMPORTÂNCIA DO COMPLIANCE EMPRESARIAL NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA

Wesley Vicente da Silva1
Darlã Conceição Santos2

RESUMO: No cenário de exploração das informações como mercadoria econômica, os dados pessoais coletados por empresas privadas tornaram-se fator de tutela legislativa. Assim, surgiu a necessidade de organizar os setores privados para adequar aos moldes da Lei Geral de Proteção de Dados Pessoais ? LGPD, com o intuito de proteger a privacidade, como direito autônomo e fundamental para a tutela da pessoa humana, destacando os programas de compliance aliados as boas práticas e governança de dados. Nesse contexto, a fim de consolidar os mecanismos técnicos de segurança para a efetividade da legislação com a finalidade de mitigar os casos de vazamento de dados pessoais, a LGPD implementou medidas administrativas para inibir incidentes decorrentes das condutas infratoras a legislação. Desse modo, este trabalho tem como objetivo demonstrar a importância dos programas de compliance para a proteção aos direitos dos titulares dos dados, visando o cumprimento do ordenamento jurídico. Valendo-se do método hipotético-dedutivo, com abordagem qualitativa, utilizando da revisão bibliográfica de livros, legislação, artigos, dissertações e teses concernente à tutela de dados pessoais no Brasil para o desenvolvimento do presente artigo.

PALAVRAS-CHAVES: Compliance Empresarial. Governança corporativa. LGPD. Vazamento

de dados.

ABSTRACT: In the scenario of exploitation of information as an economic commodity, personal data collected by private companies have become a factor of legislative protection. Thus, the need arose to organize the private sectors to conform to the General Law for the Protection of Personal Data - LGPD, in order to protect privacy, as an autonomous and fundamental right for the protection of the human person, highlighting compliance programs allied with good practices and data governance. In this context, in order to consolidate the technical security mechanisms for the effectiveness of the legislation with the purpose of mitigating cases of leakage of personal data, the LGPD implemented administrative measures to inhibit incidents arising from conducts that violate the legislation. Thus, this work aims to demonstrate the importance of compliance programs to protect the rights of data subjects, aiming at compliance with the legal system. Taking advantage of the hypothetical-deductive method, with a qualitative approach, using the bibliographic review of books, legislation, articles, dissertations and theses concerning the protection of personal data in Brazil for the development of this article.

KEYWORDS: Corporate Compliance. Corporate governance. LGPD. Data leak.

1
Discente do curso de Direito da Universidade Católica do Salvador.
2
Mestre em Direito, Docente na Universidade Católica do Salvador.

1 INTRODUÇÃO

A nova moeda de troca não é apenas aquela que podemos ver, quantificar ou converter. Os moldes do mercado financeiro mudaram, sendo em questão material ou ao produto que eles precificam, postulando um novo aparato ao objeto contratual: os dados.
Muito embora, os dados pessoais, ainda para muitos, são apenas informações deslocadas acerca de fatores específicos, atualmente, podem ser conceituados como um conjunto de indicadores, regrados por um complexo condensado de informações em um fluxo crescente tangencial.
Os dados da grande massa acabam gerando indicadores que podem ser balizados e influenciados de acordo com os detentores dessa informação, apenas apartado em blocos de informações não são considerados como vetores orçamentários. Porém, direcionados para uma finalidade ordenada tem o condão de influenciar o interesse social.
Dito isso, os mecanismos postos pelo Reino Unido para possibilitar uma estruturação normativa para organizar e gerir os dados dos indivíduos, foi crucial para a criação em outros países, como no Brasil, onde instituiu-se a Lei Geral de Proteção de Dados Pessoais (LGPD). Muito

embora, a lei brasileira trouxe um arcabouço de normas reguladoras e sanções aos casos de tratamento de dados, que não foram abarcados com o marco da internet, os dados em uma visão macro constitucional já eram de forma genérica tutelados pela Constituição Federal de 1988.
Todavia, apenas a sanção da LGPD não seria, isoladamente, capaz de coibir as violações ao tratamento de dados na esfera privada, mas sim a necessidade de uma regulamentação do ciclo de vida das informações, que além de estipular os dados que podem ser utilizados ou até quando podem ser armazenados, estabelecer expressamente no bojo da norma como deve ser a proteção na operação do tratamento de dados.
De forma efêmera, conclui-se que a legislação pode delimitar os alicerces capazes de ensejar uma fiscalização, sendo estas através de mecanismo de gerenciamento de atividades, políticas de condutas e implementação de governança de dados, pois os dados hackeados ou vazados de forma isoladas, não seria possível identificar dados sensíveis, muitos menos individualizar o sujeito.
Portanto, o gerenciamento dos dados em provedores de armazenamento pode ter os riscos reduzidos de acordo com a realização de medidas de compliance para dirimir os impactos na

atividade empresarial, como também para tutelar os dados, cada vez mais acentuado como um produto orçamentário.

2 COMPLIANCE EMPRESARIAL

A criação do compliance está entrelaçado sob o cenário econômico-social, assim, sua implementação como sistema de organização foi instaurado e aprimorado a partir dos problemas práticos estruturais para gerir uma boa governança, com intuito de assegurar a proteção e o controle que garante a qualidade do negócio.
A utilização do termo foi inicializada no mercado financeiro, especialmente após a criação do Banco Central em 1913 nos Estados Unidos da América, com a necessidade de um sistema econômico ajustável e estável. Só após 1960, com a regularização da Securities and Exchange Commission (SEC), que houve a necessidade de implementação do compliance como um programa para a integração dos procedimento, controle e monitoramento de operação interna. (CARVALHO, 2021)
Em 1977, com a Convenção Relativa à Obrigação de Diligência dos Bancos Suíços, estabeleceu os modelos auto regulatórios, com adequação de condutas e processos internos, na qual a infração tem como consequência à aplicação de sanções. (CARVALHO, 2021)
Só após esse processo de amadurecimento histórico, que o Brasil teve a necessidade de competir em escala global, implementado novos processos de segurança no sistema financeiro brasileiro.
Pode-se concluir que, após a globalização com o fenômeno da criação dos dados estruturais, houve a potencialização das informações adquiridas por meio de provedores, classificadas, atualmente, como fonte econômica de um produto quantificativo e qualitativo, ao qual possibilita uma utilização como um produto do sistema financeiro.
Nesse sentido, em decorrência de ataques cibernéticos em provedores de informações

massificadas conduziram a sociedade na aplicação de institutos de melhoramento, como o compliance e suas interfaces para proteger no ambiente corporativo os dados massificados recebidos em seus provedores.

2.1 O CONCEITO DE COMPLIANCE

Antes de enveredar sob o conceito de compliance na esfera privada, é oportuno compreender o seu significado. Nesse contexto, a palavra compliance advém do verbo inglês, to comply, que pode ser definida como conformidade. O instituto deve ser aplicado como plano principal de uma diretriz pré-estabelecida para ser dirigida a todos capazes de enfrentar a finalidade destinada. (BERTOCCELLI, 2019)
Nesse parâmetro, pode ser traduzida como:

Comply, em inglês, significa ?agir em sintonia com as regras?, o que já explica um pouquinho do termo. Compliance, em termos didáticos, significa estar absolutamente em linha com normas, controles internos e externos, além de todas as políticas e diretrizes estabelecidas para o seu negócio. (ENDEAVOR DO BRASIL, 2022, n.p)

O compliance pode-se ser definido de forma técnica como um conjunto de normas padronizadas, sob um viés ético e legal, na qual após estruturação será a matriz orientadora para o comportamento organizacional da instituição ao qual atuará no mercado, como também irá reger as atividades dos colaboradores. Dessa forma, sendo um instrumento hábil a controlar o risco de imagem, a normatização legal, chamados de riscos de compliance, as que recaem nas instituições no decorrer da sua atividade laboral. (CANDELORO, 2012).
Superada a barreira terminológica, a finalidade do compliance tem como escopo o gerenciamento adequado do risco de atividades, verificar adequadamente as normas éticas e legais, e estudar os possíveis danos tangenciais. Dessa forma, esses elementos visam a redução de perdas e danos, como também amplifica a cultura e fortalecimento corporativo nos moldes aos padrões exigidos, seja esse por lei ou na tentativa de dirimir o risco do serviço prestado.
Portanto, segundo a doutrinadora Frazão (2007, p. 42), destina-se em sua obra que o compliance é como:
(...) conjunto de ações a serem adotadas no ambiente corporativo para que se reforce anuência da empresa à legislação vigente, de modo a prevenir a ocorrência de infrações ou, já tendo ocorrido o ilícito, propiciar o imediato retorno ao contexto de normalidade e legalidade.

Nessa mesma linha de pensamento, de acordo com os autores da obra Compliance 360° (2012, n.p), referem-se o compliance a:

Um conjunto de regras, padrões, procedimentos éticos e legais que, uma vez definido e

implantado, será a linha mestra que orientará o comportamento da instituição no mercado em que atua, bem como as atitudes de seus funcionários; um instrumento capaz de controlar o risco de imagem e o risco legal, os chamados ?riscos de compliance?, a que se sujeitam as instituições no curso de suas atividades.

Pode-se concluir que o conceito de compliance, em uma esfera macro, é um aglomerado de regras pré-estabelecidas através de um instrumento perpetuado por técnica de desenvolvimento, capaz de dirimir riscos e danos das atividades devolvidas pelo plano diretor.
Muito embora, o instituto "compliance" tem uma definição extensiva e não tem como fim apenas o cumprimento da legislação e de condutas éticas, pode ser compreendida também como um instrumento de diminuição de riscos, desenvolvimento corporativo sustentável e subsequentes segmentos empresariais de negócio. (ROQUE, 2019)
O compliance além de estar associado tradicionalmente a uma perspectiva organizacional aos comandos administrativos, pode ser vinculada também a uma visão de uma sociedade digital 4.0, devendo não só apresentar o compliance empresarial na esfera de redução de risco à imagem, mas sim, em uma abordagem de pré-orientação e implementação de desenvolvimento aos moldes legislativo de proteção aos dados, como objeto principal de estudos.
Portanto, é necessário a elaboração do projeto de compliance em uma visão lógica, a modo de compreender os objetivos e os componentes da aplicação do programa. Posteriormente, superado os obstáculos, aplica-se os estudos de riscos a boa governança corporativa com a implementação de programas de governança de dados objetivando auxiliar o controle de informações em conformidade aos padrões da corporação, e mitigar os danos da empresa.

2.1.1 AS GOVERNANÇAS CORPORATIVAS E A IMPLEMENTAÇÃO DOS PROGRAMAS DE COMPLIANCE

Em linhas gerais, o Instituto Brasileiro de Governança Corporativa ? IBGC (2015, n.p) discrimina o conceito de Governança Corporativa, como: ?Sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas. ?
O sistema da governança corporativa está associado ao desenvolvimento interno de uma empresa, seja ele entre a administração, sócios e funcionários, capaz de criar elos para uma estruturação de direção racional e acima de tudo nos moldes da ética e legislação.
Muito embora, a governança corporativa e o compliance sejam institutos que se assemelham em uma visão macro, os mesmos, diferenciam na aplicação prática, mas se complementam no objetivo final, sendo um instrumento para aplicação do outro.

A prática da governança corporativa, além de estimular o valor empresarial, pode-se concluir que estrutura de forma adequada a medida necessária para organizar a atividade empresarial, assim, não há que se falar em condutas prejudiciais. Por exemplo: empresários compreendem que para realizar uma instrumentalização segura aos seus sócios e administradores tendem a prejudicar o negócio empresarial, assim o autor Eggon João da Silva (2005, p.259) retrata que: ?A governança corporativa assegura tratamento equânime a todos os acionistas, inclusive minoritários, preferencialistas, nacionais e estrangeiros. Todos devem ter oportunidade de reparação caso venham a sofrer violação de seus diretores. ?

Nesse passo, as críticas ao sistema não são viáveis, tendo em vista a utilização de instrumento capaz de integralizar ao plano empresarial. Sendo assim, o programa de compliance visa amplificar a utilização de um sistema para garantir que todos possam participar de forma justa sob o aspecto legal, seja sócio ou administrador.

Em uma tangente geral, a implementação da governança corporativa ressoa em uma perspectiva segura, tanto internamente, seja auxiliando as avaliações das atividades executadas pelos sócios/administradores, quanto externamente, em relação à imagem da empresa, sendo este um fator primordial a empresas estruturadas no mercado.

A implementação da governança corporativa deve ser estruturada de acordo com as necessidades da empresa, devendo verificar o histórico de desenvolvimento do estabelecimento, pois, só a partir do status da empresa pode-se delimitar a estratégia possível para uma implementação segura e adequada. Sendo assim, um regramento mais rigoroso pode gerar consequências negativas e ineficazes, especificamente em estágios primários, pois em atividades inicias, as tomadas de decisões e a execução da atividade empresarial é primordial, sendo necessário, um aspecto negocial informal para realizar os objetivos da empresa, o que não se verifica quando existe prática de boa governança devidamente estruturadas no negócio. (KLEINDIENST, 2019)

Ao desenvolver da atividade da empresa, além da atenção a organização interna, sendo está um fator primordial da governança, ainda que no fim acabe tendo um aspecto externo por vislumbrar no mercado financeiro uma maior complexidade da entidade. O desenvolvimento da empresa, seja no faturamento, importação comercial, quantidade de funcionários, além dos controles a observância da legislação e regras internas, tendem à serem complexos, e, que necessita

de ações maiores que a própria instituição empresarial, restando necessária a implementação de sistema organizacionais aos fluxos de informações. (KLEINDIENST, 2019)

Ultrapassado a esfera conceitual e instrumentalização da política de boas práticas de governança, cabe pontuar que as empresas que possuem fluxos de informações sensíveis, conforme estipula o artigo 50 da Lei Geral de Proteção de Dados Pessoais, os controladores e operadores são responsáveis pelo tratamento de dados, devendo criar planos de adequação a legislação.

Assim, ao confeccionar as regras de boas práticas, os controladores adjuntos com a administração devem estipular através da análise da natureza dos dados coletados, a probabilidade, a finalidade e o potencial de riscos das vantagens advindas dos tratamentos dos dados verificados. (NASCIMENTO, 2020)

É necessário pontuar que, os agentes de tratamento, após a autenticação da gravidade e sensibilidade dos dados aos riscos de operação, poderão estabelecer programa de governança em privacidade, sendo este, um instrumento amplo com normas de compliance, além dos aspectos operacionais.
Em relação ao programa de governança de privacidade, pode-se estabelecer como um aglomerado de normas-regras de boas práticas de governança, com a finalidade de executar ordens de natureza legal. (NASCIMENTO, 2020)
Portanto, os instrumentos do compliance em conjunto com a boa prática de governança, se consagram na identificação dos riscos e estruturação de medidas para a empresa, sendo respondida de forma adequada e proporcional ao suporte da tomada de decisão.
O Programa de compliance na esfera privada para análise de dados pessoais, com a finalidade de promover a segurança, deve ser constantemente monitorado e atualizado, com a implementação de ?salva vidas? em decorrência de avaliação de riscos à privacidade e o acometimento de vazamentos. (NASCIMENTO, 2020)
Portanto, os instrumentos e objetos referenciados demonstram a determinação de regras de governança no ambiente de operação de tratamento de dados pessoais, a modo que seja realizado uma estruturação nas empresas para que possibilitem a implementação de mecanismos de segurança, com a finalidade de dirimir os riscos da atividade empresarial na sociedade digital.

3 GOVERNANÇA DE DADOS

O mercado digital tem como principal ativo financeiro os dados, este considerado como ?matéria prima? de uma economia baseada no conjunto de informações, sendo que nos últimos anos, houve um aumento exponencial na coleta de dados por cooperativas, startups e novos nichos empresariais, tendo a finalidade de quantificar e gerencias os dados.
Dados, informações, conhecimento e sabedoria são os quatros estágios evolutivos da cadeia de informação, pode-se assim, compreender os dados como fatos ou registros em seu formato primário. (BEAL, 2014). Já a informação é entendida como os conjuntos processados de dados em um contexto aplicado (RÊGO, 2013). Muito embora, na sociedade da informação ?os dados são o novo petróleo?, apenas os dados isoladamente não são capazes de transformar em ativo financeiro, sendo necessário administrá-lo de forma eficaz, para que assim, as empresas adquiram vantagem competitiva.
Dessa forma, a governança de dados tem como principal objetivo atender as necessidades das empresas, ou seja, solucionar problemas, diminuir custos da administração, para que os dados transformem em saldo positivo para os negócios (TERRA, 2017).
O Data Governance Institute -DGI (2017, n.p) definiu governança de dados como ?um sistema de direitos de decisão e responsabilidades para processos relacionados à informação, executado de acordo com modelos acordados que descrevem quem pode realizar quais ações com quais informações e quando. ? Portanto, a utilização da governança de dados orienta quais os métodos deverão ser aplicados no ciclo de vida dos dados.

Uma das atribuições da governança é o acompanhamento da operação dos dados com a finalidade de gerir que as informações estejam alinhadas com os objetivos pré-determinados na coleta primária, além disso, é necessário assegurar que as informações estejam disponíveis para acesso, quando consultadas, gozar de qualidade, consistência, auditabilidade e segurança dos dados (ESPÍNDOLA, 2018).

No âmago da cadeia evolutiva da informação uma das preocupações dentro das organizações corporativas é o receio com a proteção das informações, ou seja, a capacidade das empresas no protagonismo da segurança com os provedores internos, tendo em vista a necessidade de conformidade com a legislação pátria.

A boa governança tem como objetivo aplicável à prática do controle dos processos de operação dos dados: a prevenção de situações adversas que podem gerar o comprometimento da integralidade dos dados adquiridos pelas organizações empresariais, que por sua vez, devem ter o condão de reforçar a confidencialidade das informações. (ESPÍNDOLA, 2018).

A integração do programa de governança de dados nas corporativas empresariais, tem como o esforço principal a organização de dados, que deve ser observado por um prisma basilar, ou seja, a aplicação dos princípios como limite legal e ético no ciclo de vida dos dados.

Para Rêgo (2013), os princípios são regulamentações para compreender aplicação da governança dos dados como linha direta para os negócios, sendo: (i) A gestão de dados estratégicos, tem o dever de vislumbrar as tomadas decisões por um coeficiente tático e operacional. (ii) A governança como instituição, ou seja, a governança de dados pode ser comparada como sistema governamental, na qual dispõe de legislação, execução e jurisdição; (iii) A governança de dados como um programa, devendo ser implementado como fator permanente, não apenas um projeto temporário. Ainda, pontua-se que os princípios da Governança de dados não são limitados, tendo uma orientação basilar a cada implementação de um sistema organizacional que deve ser observado pelo prisma ético e legal.

Assim, os princípios devem incumbir os papéis que a serem preenchidos pela gestão moldar os comportamentos das empresas para a aquisição, reserva e utilização dos dados conforme as normas e políticas da corporação (TERRA, 2017).

Coleta, armazenamento, recuperação e descartes, são as quatro etapas do ciclo de vida dos dados (SANTANA, 2013), ou seja, para a aquisição de dados pelas empresas, deverão observar a vida útil do dado para não incorrer na (in) responsabilidade da utilização indevida de informações dos seus provedores.

As fases do ciclo de vida dos dados devem ser observadas pela ótica de seis objetivos, sendo eles: a qualidade, a privacidade, os direitos autorais, a integração, compartilhamento e preservação dos dados (ESPÍNDOLA, 2018). Muito embora, a lei geral de proteção de dados implementou e traçou novos objetivos para a coleta de dados pessoais, cabe destacar que os objetivos vislumbrados na Governança de dados têm como parâmetro preliminar a tomada de decisão, na qual deve ser os negócios pautados nos moldes legais e éticos vigentes.

Nesse contexto, o controle de informações é necessário, tendo em vista que na sociedade da informação, cada vez mais o volume de dados é crescente, acarretando mais vazão e protesto

por políticas públicas para a preservação dos institutos, órgãos e empresas que detenham a

informação, sendo assim, necessário sistema de organização, softwares e hardwares capazes de processar as informações, criptografar e armazenar. (MARTIGNAGO, 2019)
Assim, para otimizar o ciclo de vida dos dados e garantir que os objetivos sejam preenchidos na estruturação do gerenciamento de dados, faz-se necessário a implementação de frameworks com o intuito de garantir que o procedimento seja cumprido com maior qualidade de informação e aproveitamento financeiro para a empresa, auxiliando a tomada de decisão para redução de risco para utilização de dados. (MARTIGNAGO, 2019)
Um Framework, segundo Johnson (1991), pode ser definida como um aglomerado de objetos que colabora entre si para que atinja um conjunto de obrigações para aplicação de um domínio especifico. Já para Pinto (2000), um framework é conceituado como um software incompleto criado para ser um objeto cujo estado e comportamento são definidos pela classe. Assim, o framework é uma concepção de uma arquitetura para um edifício de subsistemas e oferece o alicerce básico para criá-los.
Muito embora, os autores defendem uma conceituação distintas acerca da concepção de frameworks, pode-se verificar que ambas se complementam, tendo em vista que o framework é um sistema pré moldado, ou seja, é um programa com intuito de ser complementado através da finalidade a ser cumprida pela gestão empresarial, sendo instanciado por classes para categorizar os dados e ser alojado em hotspot, provedores físicos, capazes de armazenar as informações coletadas pelas empresas.
Portanto, para gerenciar os ativos de dados de forma complexa, ordenada e objetiva é necessário para proteção do procedimento do ciclo de vida dos dados, determinar os modelos de frameworks para o gerenciamento dos dados. Assim, para Carvalho (2021), podem ser apresentados três domínios CobiT, DAMA DMBOK e DGI Framework, sendo apenas dois destes observados para fomento deste artigo: (i) A DAMA (DAMA DMBOK), e (ii) CobiT.
A DAMA (Data Management Association) é uma associação sem fins lucrativos, com o intuito de promover boas práticas de gestão de dados, e em 2009 fundou o DAMA-DMBoK (Data Management Body of Knowledge), sendo um corpo de conhecimento que tem como ponto fundamental esclarecer como as corporativas devem aplicar a operação otimizada dos dados. (CARVALHO, 2021)
Em sua versão 2.0, acrescenta não só uma visão macro do gerenciamento de dados, definindo padrões, terminologias e práticas, mas a integração de dados, para definir táticas,

armazenamentos e sistemas, bem como implementação da ética na operação do tratamento de dados, a definição de big data e ciência de dados e amadurecimento das informações. (LIMA, 2019).
O DAMA-DMBOK V2 é formado por 11 (onze) funções de gestão de organização de

dados, sendo incorporado como cerne principal: a governança de dados, tendo em vista que os dados percorrem por toda sistemática das onzes funções ordenadas, assim segundo Honório (2021):
A primeira função é a governa de dados, sendo o pilar do framework, tem o condão de orientar e supervisionar a operação do ciclo de vida dos dados, na qual deve estabelecer um sistema de apoio a decisão dos gestores sobre os dados, sob o prisma do negócio.
A arquitetura de dados, a segunda função, pode ser conceituada como um planejamento para administrar os dados, aquisição de ativos da empresa, com o intuito de definir a finalidade das informações adquiridas com os requisitos necessário para o gerenciamento dos dados.
Por sua vez, a modelagem de dados e design, tem a função de demonstrar de forma nítida os dados, sendo o processo da descoberta, análise e representação da etapa primária da informação.
O armazenamento, uma das etapas da operação do ciclo de vida dos dados, na qual vai incluir o design, o suporte dos dados armazenados para quantificar o coeficiente valorativo das informações, até o seu descarte, devendo respeitar todo o procedimento de segurança legal vigente.
Um dos alicerces para o gerenciamento de informação é a segurança, que deve garantir a proteção dos dados, a execução de políticas e procedimento de segurança, no intuito de moderar o acesso de forma consciente e controlado, não devendo ser infringido ou acessado de forma inadequada, afim de garantir autenticação e auditoria de dados informações.
A Integração e Interoperabilidade de dados, é a função responsável pela movimentação e a concretização dos dados na interligação do armazenamento e outras plataformas.
O gerenciamento de documentos, pode ser compreendida como o gerenciamento e inclusão da vida útil dos dados e informações, encontrados em programas não estruturados, em ênfase ao conteúdo de apoio de conformidade a legislação vigente e os termos éticos formalizados para o negócio.
Dados mestre e de referência, tem como condão a manutenção dos dados compartilhados para coexistir a integralidade dos sistemas internos de gerenciamento dos dados.
Em razão da interligação entre uma linha direta com os negócios, uma das funções do DAMA-DMBOK é a Data warehousing e Business intelligence, ou seja, a implementação de

planner para o contoler da administração dos dados e suporte a decisão com o intuito de conceder aos gestores de informação emitam relatórios de equalização de valores.
Segundo Barata (2015), os metadados, na qual consiste a décima função, é promover a facilitação do acesso dos dados interligados nas multifontes do sistema integrado, como também garantir a qualidade de dados.
Por fim, o gerenciamento de qualidade de dados é a implicação das técnicas para garantir a possibilidade de aferição, melhoramento e adequação da utilidade dos dados, com o intuito de monitorar a integridade da informação primária no ciclo de vida dos dados.
Já o COBIT (Control Objectives for Information and related Technology), é um framework de suporte fundado em 1994 administrado pela ISACA (Information Systems Audit and Control Association), estruturado como um arcabouço de informação direcionadas para governança de dados e gerenciamento de informação, tem como objetivo auxiliar os profissionais de gestão na conexão entre os problemas técnicos e os riscos do negócio. (BARATA, 2015).

Para Lima (2019), o COBIT é um framework que possui duas vertentes basilares: a gestão, que possui quatro áreas de domínios: planejamento, constituição, execução e monitoramento, e a governança que é a tomada de decisão de acordo com a gestão de dados, possuindo 37 (trinte e sete) processos integrados.
Na versão 5.0, o sistema é utilizado baseado em 05 princípio, conforme elucida Casaes (2019), Barata (2015) e Lima (2019), sendo: (i) atender às necessidades das partes interessadas; (ii) cobrir o negócio como um todo; (iii) aplicar um framework único e integrado; (iv) habilitar uma visão holística; e (v) distinção entre governança de gestão.
Um dos princípios é atender às necessidades das partes interessadas, sendo a necessidade das corporativas é satisfazer as expectativas dos seus stakeholders, proporcionando um equilíbrio na tripartite: benefícios, redução do risco e recurso disponíveis.
O segundo princípio é baseado na cobertura do negócio como um todo, ou seja, abranger a integralidade da empresa no processo, procedimento, pessoas e as relações com os habilitadores.
A aplicação do framework único e integrado, assim, o COBIT é capaz de promover uma relação completa com a Governança de dados, corroborando ao alinhamento com padrões externos e adaptabilidade dos modelos usuais de negócios.

O COBIT permite habilitar uma visão holística, ou seja, uma visão macro dos componentes que oferecem suporte para atingir as finalidades da governança de dados, na qual define como catalogadores: as políticas, processos, estruturas organizacionais, informação e ética.
Por derradeiro, o princípio da distinção entre governança de gestão, tendo em vista que ambos possuem estruturas organizacionais distintas, assim, governança tem como esforço principal que os objetivos corporativos sejam cumpridos, estabelecendo prioridades pela tomada de decisão, compliance e progresso das organizações. Por sua vez, a gestão é o planejamento, construção, execução e monitoramento das funções ornamentada com o direcionamento da governança.
Desse modo, com escalonamento dos cinco princípios é capaz de proporcionar o funcionamento otimizado do framework, destacando os seguintes processos:
O APO01: Gerenciar o framework de TI, tem como condição a otimização das atividades relacionadas ao TI, com a função principal de incluir os procedimentos e regulamentos para promover a integralidade das informações nos bancos de dados. (BARATA, 2015)
Já o APO03: Gerenciar a arquitetura corporativa, tem função primordial agrupar as informações para auxiliar as atividades e tomadas de decisões, conceituando e compartilhando as informações dos elementos dos dados, e por fim catalogar a empresa, com base na modulação e sensibilidade dos dados. (BARATA, 2015)
Nesse ínterim, a governança de dados como um sistema integrado com o programa de compliance, tem o condão de otimizar a operação de controle interno relacionado aos dados coletados pelas empresas, capaz de gerenciar as bases para o apoio de decisão ao tratamento das informações, com segurança e qualidade, garantido o ciclo da vida útil dos dados.

4 A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

As estruturas políticas, econômicas e sociais com desenvolvimento de novas tecnologias e mecanismo para a coleta de dados e informações, fez necessário modulações legislativas para a proteção da privacidade, além dos aspectos físicos, patrimoniais e morais.
A proteção à privacidade de dados foi dividida em quatros gerações: a primeira, oriunda do estado moderno, com o advento dos bancos de dados; a segunda, datada em 1980, com a expansão legislativa para a proteção à privacidade aos setores privados; a terceira geração em 1990, com o processo de tratamento de dados e o consentimento dos cidadãos; Por fim, a última dimensão, é

destinada ao protagonismo da permissão para coleta e uso dos dados pessoais, quando a lei estabeleceu a importância da titularidade das informações. (MENDES, 2014)
Nesse aspecto, é perceptível a evolução do direito aos fatores reais da sociedade e as transformações dos meios tecnológico, computacionais, genéticos e comunicativos, que por sua vez possibilitou a integração da comunicação global, e consequentemente, o rastreio dos dados através do armazenamento de informação. (SAAD, 2021).
Os legisladores ao considerar os dados pessoais como extensão ao direito à privacidade, preocuparam em tutelar constitucionalmente a proteção da população, em especial os países europeus, como: Espanha, Portugal, Hungria, Eslovênia e Rússia. (VIEIRA, 2007) Porém, só tornou-se fator primordial após o regulamento geral do Parlamento Europeu sobre a proteção de dados, n.º 2016/679, sendo necessário a adequação das empresas prestadoras de serviço na Europa ao regulamento, influenciado diretamente o Brasil para elaboração da Lei Geral de Proteção de Dados brasileira. (SAAD, 2021).
Muito embora, a Lei Geral de Proteção de Dados Pessoais - LGPD, em sua promulgação, não abarcou de forma expressa a proteção de dados como direito fundamental, a doutrina, em especial Nascimento (2020), por sua vez, já argumentava a proteção de dados e informações pessoais como direito autônomo, derivado do direito fundamental à privacidade, explicitamente no artigo 5°, X, da CRFB de 1988.
Após reiterados julgamento sobre a tutela dos dados pessoais como extensão da personalidade do indivíduo, o Supremo Tribunal Federal -STF reconheceu no Julgamento da Ação Direta de Inconstitucionalidade - ADI 6387, a existência dos dados como direito autônomo, derivada do direito fundamental a dignidade da pessoa humana, na proteção à intimidade e a centralidade do Habeas Data como autodeterminação informativa. (NASCIMENTO, 2020).
Ao compreender a necessidade da proteção aos dados pessoais, os legisladores brasileiros em votação de ? das casas legislativas (câmara e Senado Federal) em dois turnos, aprovaram a Emenda Constitucional 115 de fevereiro de 2022, alterando o artigo 5° da Constituição Federal de 1988, incluindo o inciso LXXIX, tutelando constitucionalmente a proteção aos dados pessoais, inclusive nos meios digitais.
Ressalta-se, ainda, que os dados pessoais estão interligados com o direto fundamental à privacidade, na qual representa a capacidade de a pessoa administrar sua vida, seus pertences e

propriedades materiais e imateriais, permitindo ou não a utilização dos seus dados (bens imateriais) por terceiro. (NASCIMENTO, 2020).

A privacidade, por sua vez, segundo Mendes (2008), é o direito à proteção aos comportamentos pessoais e acontecimentos de caráter íntimo, bem como as informações prestadas aos profissionais e comerciantes, em que a pessoa não deseja que se compartilhe com o público.

Para o professor William Prosser, pode-se qualificar a lesão a privacidade em quatro graus: i) o intrometimento na reclusão ou solidão na vida privada, ii) a divulgação pública de fatos privados constrangedores sobre o indivíduo; iii) a publicidade sobre o indivíduo apresentada de forma equivocada; e iv) a apropriação, para obtenção de vantagem, do nome ou da imagem do demandante (PROSSER, 1960).

A doutrina, por sua vez, defende mais uma violação à privacidade: a privacidade informacional, interligada com os fatores tecnológicos de informação. (SAAD, 2021). Assim, quando a lei ao realizar o tratamento da privacidade, refere-se como um direito líquido, ao qual será tutelado para garantir que o indivíduo tenha um local reservado, que não tenha, se desejar, a interferência de outros sujeitos, seja pessoa física ou jurídica.

Com a proteção dos dados pessoais dos titulares, através da LGPD, possibilitou ao cidadão o acesso a informações ao ciclo de vida útil dos dados pelas empresas, e a certeza de fiscalização pela Autoridade Nacional de Proteção de Dados, com a finalidade de atingir os objetivos traçados pela legislação, na qual a lei traz conceitos e delimita princípios, que devem ser mencionados.

A LGPD tem como objetivo principal: ?o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado?, com a destinação de assegurar os direitos fundamentais a liberdade e privacidade dos titulares dos dados, bem como tutelar a dignidade e a personalidade da pessoa natural. (LGPD).

A legislação está ordenada diretamente com o meio empresarial, sobretudo no que se refere aplicação aos seus destinatários que são pessoas físicas ou jurídicas que realizam a coleta e tratamento de dados no Brasil, conforme preceitua o artigo 1° da lei 13.709, de 14 de agosto de 2018.

Para compreender a LGPD, faz-se necessário elucidar os conceitos de dados pessoais: (art. 5º, I) é toda informação relacionada a pessoa natural, identificada ou identificável, sendo o dado aplicado no contexto que possibilite o reconhecimento do indivíduo. Bem como refere-se aos dados sensíveis (art. 5º, II), são todas as informações que se relaciona com pensamentos políticos, crenças, identidade biológica e física. Portanto, a legislação tem como ponto a proteção e o cuidado para a não violação dos dados pessoais e sensíveis.

Os doutrinadores, Laura Schertel e Danilo Doneda, ainda aponta cinco pilares para compreender a LGPD, sendo: i) a unidade e generalidade da aplicação da Lei; ii) a legitimação para o tratamento de dados (hipóteses autorizativas); iii) os princípios e direitos do titular; iv) as obrigações dos agentes de tratamento de dados e v) a responsabilização dos agentes.

O primeiro pilar é considerado com aplicabilidade material da legislação, ou seja, aplica-se a qualquer operação realizada por pessoa natural ou jurídica de direito público ou privado,

independentemente do meio, da sua sede ou do país onde estejam localizados os dados (Art. 3°). Considerado, assim, como uma aplicação uniforme para todos os setores público ou privados que realizam tratamento de dados.

O segundo pilar é a legitimação para o tratamento de dados, tendo em vista que a lei especificou critérios e requisitos para o reconhecimento da legitimidade, não podendo ser tratados os dados, sem que exista uma base normativa que autorize, prevista no artigo 7°, 11° ou 23° da LGPD, abordando 11 (onze) hipóteses, incluído o consentimento ou a previsão legislativa.

Destaca-se que a autorização por consentimento para ser considerado válido, deve observar os requisitos previsto no artigo 5°, XII, sendo considerado que a vontade deve ser livre, informada, inequívoca e com a finalidade determinada, consagrando os princípios norteadores da legislação.

O terceiro pilar é o conjunto de princípios e direitos que assegura o destinatário da lei a controlar a utilização do seu dado pessoal, sendo importante elencar dez princípios que estruturam a LGPD: a finalidade, a adequação, a necessidade, o livre acesso, a qualidade dos dados, a transparência, a segurança, a prevenção, a não discriminação e a responsabilização. (MENDES, DONEDA, 2018)

No que concerne, aos direitos dos titulares são expressos no artigo 18° da referida lei, que permite o titular dos dados adquirir através do controler, independentemente do momento, as informações relacionadas ao indivíduo, prevendo: acesso, confirmação, correção, anonimização, bloqueou ou eliminação e a portabilidade.

Para adentrar no cerne dos problemas enfrentados pela legislação, em especial, sobre o vazamento de dados, os dois últimos pilares serão abordados sob a perspectiva da violação e responsabilização acerca da proteção de dados nos casos incidentes de vazamento.

Assim, o quarto pilar, destina-se às obrigações dos agentes de tratamento dos dados, na qual estabeleceu limites que devem ser observados nas operações realizadas para reforçar a segurança e prevenir os problemas da atividade no tratamento de dados.

Uma das obrigações fundamentais, consiste na intitulação do encarregado pelo tratamento dos dados indicados pelo controlador, conforme artigo 41 da LGPD, que possui a função de aceitar as reclamações e comunicações dos sujeitos dos dados, receber informações da Autoridade Nacional, como deve orientar os funcionários a respeito das práticas a serem adotadas em relação à proteção de dados pessoais.

Assim, as informações devem ser fornecidas ao proprietário dos dados, quando os dados forem coletados, como: os meios de segurança aderidos ao tratamento de dados, quais são os riscos da atividade que podem gerar lesão ao titular, pois pode gerar a mitigação dos prejuízos. (SAAD, 2021)

A lei Geral de Proteção de Dados Pessoais tem como objetivo a proteção do dados pessoais dos titulares dos dados, sendo assim, uma das obrigações principais é adoção de medidas de segurança, técnicas e administrativas hábeis a proteger os dados pessoais de acessos não autorizados, como promover a integralidade dos dados, não permitindo, assim, a alteração das informações, a prevenção de situações ilícitas ou acidentais, ou qualquer forma de tratamento inadequado, consoante se desprende do artigo 46 da lei.

Tornou-se corriqueiro manchetes acerca do vazamento de dados por corporativas, uma das violações mais graves incidentes abarcados pela LGPD, o que ocasiona a vulnerabilidade do titular dos dados, e dos sistemas internos que são responsáveis pelo ciclo de vida útil dos dados. (SAAD,2021)

A seção de segurança de informação tem como condão as obrigações inerentes aos agentes de tratamento, devendo ser adotado pela integralidade das pessoas que realizam o tratamento de dados, garantido que os dados sejam confidenciais, bem como disponíveis nas operações de tratamento. (Art.48). Nos casos incidentais de vazamento de dados, insurge a necessidade ao controlador de informar a autoridade de proteção de dados, que podem definir as medidas para mitigação dos danos.

No entanto, com a utilização da internet, compras online, transferência virtuais e outros meios tecnológicos, criou-se uma dificuldade para atuar na segurança de dados, tendo em vista a abrangência e os domínios de redes globais, que combinados com fatores não perceptível, forma

um perfil não rastreavel capaz de ocasionar violação às diretrizes básicas da legislação, que mesmo com ações posteriores não conseguem excluir os inúmeros registros de pessoas e organizações que coletaram os dados, lesionando a confidencialidade das informações (SAAD, 2021)

Destaca-se que as obrigações aos controladores e operadores, devem ser observados desde a coleta dos dados até seu descarte, assim o artigo 46 da LGPD, introduziu o conceito de privacy by design, sendo a incorporação pelas empresas nos serviços e produtos, na qual dispõe a proteção da privacidade no centro de todo o desenvolvimento corporativo.

Embora, a legislação tenta dirimir os riscos da atividade, os prejuízos causados pelo vazamento de informações são altos, e perpassam pela inadequação do sistema de proteção, perda de credibilidade e de clientes, ocasionado uma ruptura na imagem da empresa, impossibilitando, muitas vezes de concorrer no mercado corporativo. (SAAD,2021)

Portanto, a LGPD concebeu obrigações aos agentes de tratamento de dados, para que se delimite a finalidade da utilização dos dados desde o início da concepção, devendo o controlador confeccionar relatório de impacto a privacidade, utilizando de métodos para a captação da operação do ciclo de vida dos dados, observando as mediadas adotada para aumentar a segurança e mitigar o risco do tratamento das informações, conforme artigo 3 da LGPD.

O último pilar, considerado como a responsabilidade dos agentes na incidência de ocorrência de danos derivados do tratamento de dados. A LGPD consagrou a natureza do tratamento, limitando os parâmetros ao artigo 7° da lei, nas 10 hipóteses dos incisos, vinculados a finalidade da captação dos dados, consoante prevê o artigo 6°, inciso I, II, da LGPD.

A legislação tem como regra o descarte (eliminação) dos dados ao fim do tratamento da operação (art. 16), com o intuito de mitigar os riscos presente no tratamento de dados, principalmente, no que concerne à limitação das hipóteses de tratamentos para não lesionar os direitos dos titulares.

Nos casos, em que mesmo após o término de vida útil dos dados, as empresas podem, quando permitido, armazenar dados que em situação incidentais serem objetos de violação, principalmente nos casos de vazamento, que podem ocorrer, quando não autorizados pelo titular

ou controladores, serem acessados, captados, compartilhados pela internet, para outros sujeitos ou empresas.
Assim, a Lei Geral de Proteção de dados Pessoais, em especial em seu artigo 42, dispõe que o controlador ou operador, quando realizar o exercício do tratamento de dados pessoais, vem

a ocasionar dano patrimonial, moral, individual ou coletivo em detrimento a aplicação da legislação, é obrigado a repará-lo, definindo a responsabilidade de forma objetiva.
Embora, a responsabilização objetiva não é necessária a demonstração de culpa do controlador ou operador. Faz mister esclarecer que o operador, só será responsabilizado quando os atos praticados forem contrário à legislação, ou às instruções que foram fornecidas pelo controlador. (MENDES, DONEDA, 2018)
Ainda, a legislação prevê exceções a responsabilidade objetiva (art. 43), sendo: quando o agente demonstrar que não realizou o tratamento de dados pessoais que foi atribuído, ou quando não houve violação da segurança ou a legislação, e por fim, quando for por culpa exclusiva do titular ou de terceiros.
Porém, o cenário que é vislumbrado no Brasil nos casos de vazamento de dados, é que as violações pelas instituições vêm ocorrendo, majoritariamente, sob ataques deliberados de hacker, ou falha de segurança dos controladores dos dados. (SAAD, 2021)
Dessa forma, é necessário adotar medidas para dirimir os riscos da atividade, e possibilitar o discernimento das informações acerca dos perigos de vazamento de dados, tendo em vista que a tendência é aumento significativo das violações vinculados com a crescente tecnológica. Assim, as empresas devem implementar mecanismos para a segurança das informações.

5 O COMPLIANCE EMPRESARIAL COMO INSTRUMENTO DE PROTEÇÃO DE DADOS NA ESFERA EMPRESARIAL

Em decorrência das constantes violações aos dados armazenados em provedores privados, a tutela ao direito à privacidade nos meios tecnológicos, já era pauta de debate na legislação brasileira, e já existiam mecanismos para a proteção, como: a proibição de direcionamento dos provedores em relação ao compartilhamento de dados, bem como a inibição ao monitoramento nos navegadores de internet.
Vinte e seis bilhões de dados foram vazados no Brasil em 2019, de acordo com pesquisas realizadas pelo Massachusetts Institute of Tecnology ? MIT, possibilitando a utilização de números telefônicos, score de crédito, endereço eletrônico, fotos, números de identificações e outros dados pessoais, para o cometimento de crimes cibernéticos, e a violação aos direitos dos titulares.
A utilização e uso dos dados pessoais por pessoa física ou jurídica, com sede no Brasil ou não, devem se atentar as normas gerais de proteção aos dados brasileiro, segundo Frazão, Oliva e

Abilio (2020), é a necessidade de conferir a efetividade aos direitos e prevenir a violação aos dados, através da implementação de mecanismo de compliance, como uma ferramenta capaz de promover a adequação das atividades aportadas pelas empresas.
Assim, os controladores e operadores poderão formular regras de boas práticas e governança (Art. 50), que contenha as disposições de organização interna, o regime de funcionamento, as operações, o canal de comunicação entre os encarregados e os titulares dos dados, e o procedimento de segurança.
Nessa perspectiva, considerando que a maioria das tratativas de dados perpassam por meios digitais, deve-se adotar sistema para mapear os riscos, e implementar mecanismos para minorar as vulnerabilidades apontadas pelos programas, através da alta administração, do código de ética, para proteger os dados pessoais dos titulares. (PESSOA, 2021)
Existem inúmeras formas de ocorrer o vazamento de dados, sendo através de ataques cibernéticos, sequestro de conta, furtos de dados, compartilhamento de dados por agentes ou ex-agentes da empresa, erro ou negligência, entre outros, que podem ser para adquirir dados de nomes, CPF, celulares, endereços, dados financeiros, senhas, registro de saúde ou credenciais de acesso. (SAAD, 2021)
Desse modo, para realizar o mapeamento dos problemas que as corporativas podem enfrentar, é necessário identificar os fluxos e processos de informação que percorrem os sistemas, que irão auxiliar na tomada de decisão pelas empresas. (NASCIMENTO, 2020)
A alta administração deverá colaborar ativamente no programa de compliance, seja monitorando as investigações e intervenções em situação para estabelecer controles internos em conformidade com a legislação, bem como possibilitar a interdependência dos setores para realizar as atividades designadas para o tratamento de dados (PESSOA, 2021).
Com a elaboração do código de ética pela organização possibilitará o treinamento regular das equipes, responsáveis pela tecnologia da informação, para enraizar a cultura corporativa da boa governança, com a finalidade de assegurar o respeito ao programa de compliance (NASCIMENTO, 2020)
Nesse contexto, para manter uma boa relação com seus clientes, as organizações devem instalar canais de comunicação, para que os titulares dos dados possam contatar os encarregados responsáveis pelos armazenamentos dos seus dados, e exerçam seus direitos sobre as informações contidas nos provedores. (PESSOA, 2021).

Desse modo, quando se trata de concretização a alteração cultural coportariva é preciso realizar o alinhamento dos funcionários com o código de ética, com política de privacidade, para fins de efetividade do programa de compliance de dados. (PESSOA, 2021).

5.1 A IMPLEMENTAÇÃO DE MECANISMOS DE GOVERNANÇA DE DADOS PESSOAIS

Para a efetividade da legislação em relação ao tratamento de dados, a LGPD direciona um capítulo para implementar o programa de governança em privacidade, com a finalidade das empresas adotarem medidas técnicas, para fins de proteção e segurança dos dados pessoais.

(PESSOA, 2021)
A governança em privacidade, pode ser conceituada como um conjunto de regras e práticas positivas a serem implementadas pelos agentes de tratamento, e encontra-se em conformidade com as políticas de compliance empresarial, com o objetivo de gerir os dados das empresas para estabelecer um diferencial competitivo aos negócios. (KOEPSEL,2020)
O programa integra o aperfeiçoamento do procedimento de utilização dos dados, com os requisitos pré-estabelecidos na implementação dos softwares, com a finalidade de gerir de forma otimizada os dados para preencher as diretrizes da legislação. (SAAD, 2021)
A Lei Geral de Proteção de Dados Pessoais dispôs que os controladores e operadores poderão adotar programas de governança em privacidade, que devem ser implementados com o mínimo, (art. 50, § 2°, I): a) o comprometimento dos agentes de tratamento com as políticas internas que devem garantir o cumprimento das normas e regras de boas práticas; b) que aplicação seja de forma uniforme para todo a operação de tratamento de dados; c) que a governança seja adaptativa as estruturas da empresas, sendo compatível com a densidade dos dados e operação; d) como implementar políticas de salvaguardas em relação aos titulares dos dados; e) tenha como objetivo estabelecer uma relação de confiança com sujeitos dos dados, estabelecendo situações de transparência e que possibilite a atuação do titular; g) que conte com planos de respostas a incidentes e remediações; h) seja continuamente atualizado sua base.
Nesse aspecto, devem ser adotadas medidas administrativas para que as instituições, em conformidade com a legislação, apliquem estímulos para assegurar as informações armazenadas pelas empresas, com a adoção de orientações internas que respeitem as diretrizes que inclua o uso

minimizado ou a anonimização das informações, desde a coleta dos dados, conforme artigo 46 da LGPD.
Com o mapeamento das atividades, é importante verificar: O que são esses dados?; de que forma foram coletados ?; quem são os coletores ?; existe relação entre os dados e atividade realizada ?; O que pode ocorrer com esses dados ao serem coletados? E, como são descartados da gestão organizacional da empresa? (NASCIMENTO, 2020). Dessa forma, para adotar medidas compatíveis com os riscos alertados pelos sistemas para a proteção de dados nas organizações privadas, é necessário possuir conhecimento do caminho realizado inerentes ao ciclo de vida útil dos dados.
Embora, a legislação já estabeleça diretriz mínima para o tratamento de informação, a Autoridade Nacional de Proteção de Dados - ANPD, poderá, ainda, determinar padrões técnicos para serem implementados pelo programa de governança em privacidade, devendo ser observado a qualidade de dados, as especificações do tratamento e status tecnológico, em especial a proteção aos dados sensíveis disposto na legislação. (NASCIMENTO, 2020)
Muito embora, a lei geral de proteção de dados, apenas delimita as características e os requisitos mínimos que os operadores deverão tomar para desenvolver um compliance na organização das empresas privadas em consonância com a legislação, porém não impõe um modelo específico para integração de um programa nas corporativas. (PESSOA, 2021)
Assim, para Saad (2021), as medidas técnicas que podem ser adotadas pelos agentes de

tratamento de dados, são: i) o uso de firewalls, sendo um mecanismo de segurança que coleta os dados em conformidade com as regras pré estabelecido para análise de tráfego de rede, delimitando as operações de compartilhamento e captação de informações a serem cumpridas; ii) a utilização de antimalware, que consiste na proteção contra vírus que é capaz de fragilizar o sistema, apagar dados e infectar outros arquivos; iii) a utilização de criptografia dos dados, que possibilite quando ocorrer situações incidentais a não identificação do titular do direito.
Já para Fernandes e Abreu, (2014) defendem a implementação de frameworks como a DAMABOK e COBIT, para o gerenciamento de dados, pois tem como meta principal a delimitação do escopo das atividades, as funções envolvidas no tratamento e as interações a serem executadas pelo software, com a finalidade de proteger a privacidade em ambientes corporativos que gerenciam o armazenamento de informações aplicados na prevenção à fraude.

Segundo Carvalho (2021), a integração do software, através das boas práticas estabelecidas pela legislação, poderá aprimorar os aspectos de proteção à privacidade e prevenção a fraude do tratamento de coleta de dados. Tendo em vista, que os frameworks, podem balizar as métricas de qualidade dos dados que indicam uma utilização adequada e otimizada, e aponta a melhor proteção da privacidade.
Com a melhoria de processo de governança para o tratamento de dados, estabelece uma divisão entres as operações que possibilita uma automatização do ciclo de vida dos dados (coleta, utilização, armazenamento e exclusão), capaz de gerar relatório de risco, para o auxílio da tomada de decisão com o intuito de gerir de forma adequada o tratamento de dados. (CARVALHO, 2021)
Neste parâmetro, os programas de compliance com a implementação de frameworks, podem responder questionamento acerca do procedimento de tratamento de informação, dispondo de quais práticas relacionadas à governança, privacidade e segurança de dados, apresentam melhor benefício para o tratamento de dados pessoais. (CARVALHO, 2021)
Ademais, os controladores e operadores deverão adotar medidas, como o Relatório de Impacto ? DPIA), que corresponde a avaliação dos riscos e impactos relacionados com o tratamento de dados pessoais, além da anonimização, da transparência e do sigilo, deverão delimitar prazos para retenção de dados e aderir políticas seguras de informação acerca da operação de tratamento. (SILVA, 2022)
Após realizar a implementação e observância das estruturas mínimas estabelecidas pela LGPD, é necessário adotar um programa de gerenciamento de vulnerabilidades, com atualizações constantes e autocorreções alinhados com as boas práticas de atividades cotidianas, com a finalidade de proteger os dados pessoais, e promover um ambiente corporativo adequado para realizar o tratamento de dados. (SAAD, 2021)
No entanto, ao verificar que houve vazamento de dados, seja pelo recebimento de notificação ou pela veiculação na mídia, os agentes de tratamentos deverão identificar quais dados vazaram e realizar o procedimento estabelecido no programa de compliance de segurança, além de notificar as instituições. (Art. 48, caput).
De acordo com MIT, o prazo entre a comunicação à autoridade competente e a ocorrência do fato ilícito ultrapassa 200 (duzentos) dias em média, sendo umas das preocupações para a

efetividade da legislação, e a redução dos danos causados aos titulares dos bens imateriais.

A Lei Geral de Proteção de Dados, dispõe que nas situações que ocorrer a probabilidade de riscos ou violação aos direitos dos titulares, tem como obrigação do encarregado a comunicação à autoridade nacional e ao titular do dado (art. 48, caput). Sendo que o contato deve ser em período razoável (art. 48, § 1º), contendo a natureza dos dados dos titulares atingindo (art. 48, § 1º, I).
Em decorrência dos possíveis incidentes, a LGPD determinou critério para aplicação de sanções, em casos de vazamento de dados, observando as situações específicas de cada caso, disposto no art. 52, § 1º. Assim, deve ser considerada a avaliação da gravidade, a natureza das informações e do dano ocorrido (incisos I e VI), sendo necessário para este caso, tendo em vista que o compartilhamento indesejado de dados sensíveis pode ocasionar danos irremediáveis para os titulares.
Portanto, existe a necessidade da adesão aos mecanismos e técnicas para promover a efetividade dos programas internos com a finalidade de mitigar os danos, assim, a implementação de boas práticas e governança têm como fator o cumprimento da legislação, por meio de medidas de segurança. Entende-se, que a proteção integral contra falhas que possibilitam a ocorrência de ilícitos não é possível, porém essas diretrizes reduzem as possibilidades de existir desvios de condutas e criar salvaguardas para identificação dos incidentes, de forma eficaz, rápida e adequada.

6 CONSIDERAÇÕES FINAIS

A partir da permissão ao acesso dos dados pessoais, as informações coletadas passaram a integralizar as redes de tratamento de dados, tornando-se alvo de ataques cibernéticos, contribuindo para o aumento da intercorrência no ambiente corporativo, tornando-se o gerenciamento de informação um dos diferenciais no desenvolvimento do negócio.
Nesse contexto, foi imperativo o surgimento de leis que protejam os dados dos cidadãos, e que limitem a gestão das entidades públicas e privadas em relação as informações coletadas, transformando o sistema organizacionais, como compliance, em ferramentas de efetivação das normas éticas e legais. Assim, a implementação do programa alinhado com a governança corporativa é capaz de integralizar o corpo de normas internas com o intuito de adequar a legislação brasileira e criar uma cultura corporativa.
Dentro do programa de compliance, a administração em conjunto com a gestão da empresa, poderá implementar ao plano diretor, a utilização de software, sendo este capaz de possibilitar a automatização do ciclo de vida útil dos dados para realizar o auxílio da tomada de decisão, com o intuito de mitigar os possíveis danos decorrentes da violação aos dispositivos da Lei Geral de Proteção de Dados Pessoais.
Nesse sentido, para realizar uma proteção extensiva aos direitos dos titulares dos dados, a

LGPD integrou ao seu corpo de normas-condutas a serem adotadas pelos operadores do tratamento de dados, com escopo de preservar a integralidade, a qualidade e o sigilos dos dados, tendo como consequência da violação, a majoração de sanções pecuniárias.
Embora, o vazamento de dados ocorra de forma ordenada, a implementação de sistema de segurança nas corporações implica na diminuição de situações incidentais por erro humano, ou inadequação dos programas empresarias, assim, devendo a gestão ensejar esforços para que a proteção dos dados seja preservada, desde a concepção do serviço.
Para a efetivação da Lei Geral de Proteção de Dados Pessoais, as empresas devem realizar a adequação de medidas de boas práticas e governança em privacidade para mitigar os possíveis danos decorrente da violação aos dados em provedores privados. Mesmo que a proteção aos dados de forma concreta não seja possível, as adoções de mecanismo de segurança podem atenuar as sanções e as perdas aos titulares dos dados.

REFERÊNCIAS

BARATA, André Mantola. Governança de dados em organizações brasileira: uma avaliação comparativa entre os benefícios previstos na literatura e os obtidos pelas organizações. 2015. Dissertação (Mestrado em Sistema de Informação) - Universidade de São Paulo, São Paulo, 2015.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, [2022]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 15 abr. 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidente da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 abr. 2023.

BERTOCCELLI, Rodrigo de Pinho. Compliance. In: CARVALHO, André Castro et. al. Manual de compliance. Rio de Janeiro: Forense, 2019. p. 35.

CANDELORO, Ana Paula; RIZZO, Maria Balbina Martins De; PINHO, Vinícius (Coord). Compliance 360: riscos, estratégias, conflitos e vaidades no mundo corporativo. São Paulo: Trevisan, 2012.

CARVALHO, A. P. Proposta de um framework de compliance à Lei Geral de Proteção a Dados Pessoais (LGPD): um estudo de caso para prevenção a fraude no contexto de big data. 2021. Dissertação (Mestrado em Engenharia Elétrica) - Universidade de Brasília, Brasília, 2021.

CARVALHO, Andre Castro. Manual de compliance. 3. ed. Rio de Janeiro: Forense, 2021.

CASAES, Júlio César Costa. Governança de dados abertos governamentais: frameworks conceitual para as Universidades Federais, baseada em uma visão sistemática, 2019. Tese (Doutorado em Engenharia e Gestão do Conhecimento). Universidade Federal de Santa Catarina, Florinaóplis, 2019.

DATA GOVERNANCE INSTITUTE (DGI). Definitions of data governance. 2017. Disponível em: http://www.datagovernance.com/adg_data_governance_definition. Acesso em: 01 mai. 2023.

ENDEAVOR DO BRASIL. Prevenindo com o Compliance para não remediar com o caixa. In: ENDEAVOR. [S. l.], 26 abr. 2017. Disponível em: https://endeavor.org.br/pessoas/compliance/. Acesso em: 15 mar. 2023.

ESPÍNDOLA, P. L.; SALM JUNIOR, J. F.; ROSA, F.; JULIANI, J. P. Governança de dados aplicada à ciência da informação: análise de um sistema de dados científicos para a área da saúde. Revista Digital de Biblioteconomia & Ciência da Informação, Campinas, v. 16, n. 3, p. 274-298, 2018.

FERNANDES, Aguinaldo Aragon; DE ABREU, Vladimir Ferraz. Implantando a governança de TI: da estratégia à gestão de processos e serviços. 4. Ed. Rio de Janeiro: Brasport, 2014.

FRAZÃO, Ana. Programas de compliance e critérios de responsabilização de pessoas jurídicas por ilícitos administrativos. In: ROSSETTI, Maristela Abla; PITTA, Andre Grunspun. Governança corporativa: avanços e retrocessos. São Paulo: Quartier Latin, 2007. p. 42

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. A Lei Geral de proteção de Dados Pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

HONÓRIO, Roseli. Modelo conceitual de governança de dados como suporte à governança do conhecimento organizacional. 2022. Dissertação (Mestrado em Engenharia e Gestão do Conhecimento) - Universidade Federal de Santa Catarina, Florianópolis, 2022.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC). Guia das melhores práticas de governança para cooperativas. São Paulo, 2015. Disponível em http://www.ibgc.org.br/ userfiles/files/2014/files/CMPGPT.pdf

JOHNSON, Ralph E.; RUSSO, Vincent. Reusing object-oriented designs. Relatório Técnico da Universidade de Illinois, UIUCDCS 91-1696, 1991.

KLEINDIENST, Ana Cristina. Grandes temas do direito brasileiro: compliance. São Paulo: Almedina Brasil, 2019

KOEPSEL, Alice de Medeiros. Adoção e efeitos dos programas de compliance à luz da Lei Geral de Proteção de Dados Pessoais. 2020. Monografia (Graduação em Direito) -Universidade do Sul de Santa Catarina, Florianópolis, 2020.

LIMA, C., BASTOS, R. C. A criação de conhecimento apoiada pela governança de dados. In: CONGRESSO INTERNACIONAL DE CONHECIMENTO E INOVAÇÃO, 2019, Santa Catarina. Anais eletrônicos [...]. Santa Catarina Disponível em: https://proceeding.ciki.ufsc.br/index.php/ciki/article/view/647. Acesso em 10 Mar. 2023.

MARTIGNAGO, Deisi et al. Governança de dados aplicado no processo de catalogação. Revista Brasileira de Biblioteconomia e Documentação, São Paulo, V.15, n. 2, 2019.

MENDES, Gilmar Ferreira. Curso de direito constitucional. 2. ed. São Paulo: Saraiva, 2008.

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. São Paulo: Revista de Direito do Consumidor, 2018.

NASCIMENTO, Suellen Lima do. A lei Geral de Dados Pessoais e a Adoção dos Programas de compliance na sociedade da Informação. 2020. Monografia (Graduação em Direito) - Centro Universitário de Brasília, Brasília, 2020.

PESSOA, Larissa Rocha de Paula. Os desafios da Governança de dados e a realidade cultural brasileira. 2021. Dissertação (Mestrado em Direito) ? Universidade Federal do Ceará, Fortaleza, 2021.

PINTO, S. C. C. S.. Composição em Web Frameworks, 2000. Tese (Doutorado em Informática) Pontifícia Universidade Católica do Rio de Janeiro, Rio Janeiro, 2000.

PROSSER, William L. Privacy. California Law Review. California, v. 48, n. 3. p. 383 ? 423, agosto, 1960.

RÊGO, Bergson Lopes. Gestão e governança de dados: promovendo dados como ativo de valor nas empresas. 1. ed. Rio de Janeiro: Brasport, 2013,

ROQUE, Pamela Romeu. Estudos aplicados de direito empresarial: LL.C. em direito empresarial. São Paulo: Almedina, 2019.

SAAD, Carolina de Oliveira. A lei geral de proteção de dados pessoais e incidentes de segurança: regulação e prática de vazamento de dados, 2021. Monografia (Graduação em Direito). Fundação Getúlio Vargas. Rio de Janeiro, 2021.

SANTANA, Ricardo Cesar Gonçalves. Ciclo de vida dos dados e o papel da ciência da informação. In: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO. 14., 2013. Florianópolis. [?]. Florianópolis: UFSC, 2013. Disponível em: http://enancib2013.ufsc.br/index.php/enancib2013/%20XIVenancib/paper/viewFile/284/319. Acesso em: 13 mar. 2023.

SILVA, Ana Laura Fonseca. O papel das Soft Skills na implementação efetiva dos programas de compliance com foco na adequação à Lei Geral de Proteção de Dados ? Lei N° 13.709/18. 2022. Monografia (Graduação em Direito) - Universidade Federal de Ouro Preto, Ouro Preto. 2022

SILVA, Eggon João da. A defesa da ética e transparência. In: VENTURA, Luciano Carvalho. Governança corporativa. São Paulo: Saint Paul Editora, 2005, página 259.

TERRA, Priscila de Mello. A influência da governança de dados na gestão estratégica, 2017. Monografia (Bacharelado em Sistema de Informação) - Universidade Federal Fluminense, Niterói, 2017.

VAZAMENTO de dados aumentaram 493% no Brasil, segundo pesquisa do MIT.VEJA, São Paulo, 24 fev. 2021. Sociedade. Disponível em: https://vocesa.abril.com.br/sociedade/vazamentos-de-dados-aumentaram-493-no-brasil-segundo-pesquisa-do-mit. Acesso em: 15 mar. 2023.

VIEIRA, Tatiana Malta. O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante da tecnologia da informação. Porto Alegre: Sergio Antonio Fabris Editor, 2007.

==========

Arquivo 1: TCC - A IMPORTÂNCIA DO COMPLIANCE NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA - WESLEY VICENTE.pdf (8805 termos)
Arquivo 2: https://ludwig.guru/s/this+work+aims+to (444 termos)
Termos comuns: 2
Similaridade: 0,02%
O texto abaixo é o conteúdo do documento TCC - A IMPORTÂNCIA DO COMPLIANCE NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA - WESLEY VICENTE.pdf (8805 termos)
Os termos em vermelho foram encontrados no documento https://ludwig.guru/s/this+work+aims+to (444 termos)

==========

WESLEY VICENTE DA SILVA

A IMPORTÂNCIA DO COMPLIANCE EMPRESARIAL NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA

SALVADOR
2023

WESLEY VICENTE DA SILVA

A IMPORTÂNCIA DO COMPLIANCE EMPRESARIAL NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA

Artigo apresentado como requisito parcial para obtenção do título de Bacharel em Direito pela Universidade Católica do Salvador.

Orientador: Prof. Darlã Conceição Santos.

SALVADOR
2023

A IMPORTÂNCIA DO COMPLIANCE EMPRESARIAL NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA

Wesley Vicente da Silva1
Darlã Conceição Santos2

RESUMO: No cenário de exploração das informações como mercadoria econômica, os dados pessoais coletados por empresas privadas tornaram-se fator de tutela legislativa. Assim, surgiu a necessidade de organizar os setores privados para adequar aos moldes da Lei Geral de Proteção de Dados Pessoais ? LGPD, com o intuito de proteger a privacidade, como direito autônomo e fundamental para a tutela da pessoa humana, destacando os programas de compliance aliados as boas práticas e governança de dados. Nesse contexto, a fim de consolidar os mecanismos técnicos de segurança para a efetividade da legislação com a finalidade de mitigar os casos de vazamento de dados pessoais, a LGPD implementou medidas administrativas para inibir incidentes decorrentes das condutas infratoras a legislação. Desse modo, este trabalho tem como objetivo demonstrar a importância dos programas de compliance para a proteção aos direitos dos titulares dos dados, visando o cumprimento do ordenamento jurídico. Valendo-se do método hipotético-dedutivo, com abordagem qualitativa, utilizando da revisão bibliográfica de livros, legislação, artigos, dissertações e teses concernente à tutela de dados pessoais no Brasil para o desenvolvimento do presente artigo.

PALAVRAS-CHAVES: Compliance Empresarial. Governança corporativa. LGPD. Vazamento

de dados.

ABSTRACT: In the scenario of exploitation of information as an economic commodity, personal data collected by private companies have become a factor of legislative protection. Thus, the need arose to organize the private sectors to conform to the General Law for the Protection of Personal Data - LGPD, in order to protect privacy, as an autonomous and fundamental right for the protection of the human person, highlighting compliance programs allied with good practices and data governance. In this context, in order to consolidate the technical security mechanisms for the effectiveness of the legislation with the purpose of mitigating cases of leakage of personal data, the LGPD implemented administrative measures to inhibit incidents arising from conducts that violate the legislation. Thus, this work aims to demonstrate the importance of compliance programs to protect the rights of data subjects, aiming at compliance with the legal system. Taking advantage of the hypothetical-deductive method, with a qualitative approach, using the bibliographic review of books, legislation, articles, dissertations and theses concerning the protection of personal data in Brazil for the development of this article.

KEYWORDS: Corporate Compliance. Corporate governance. LGPD. Data leak.

1
Discente do curso de Direito da Universidade Católica do Salvador.
2
Mestre em Direito, Docente na Universidade Católica do Salvador.

1 INTRODUÇÃO

A nova moeda de troca não é apenas aquela que podemos ver, quantificar ou converter. Os moldes do mercado financeiro mudaram, sendo em questão material ou ao produto que eles precificam, postulando um novo aparato ao objeto contratual: os dados.
Muito embora, os dados pessoais, ainda para muitos, são apenas informações deslocadas acerca de fatores específicos, atualmente, podem ser conceituados como um conjunto de indicadores, regrados por um complexo condensado de informações em um fluxo crescente tangencial.
Os dados da grande massa acabam gerando indicadores que podem ser balizados e influenciados de acordo com os detentores dessa informação, apenas apartado em blocos de informações não são considerados como vetores orçamentários. Porém, direcionados para uma finalidade ordenada tem o condão de influenciar o interesse social.
Dito isso, os mecanismos postos pelo Reino Unido para possibilitar uma estruturação normativa para organizar e gerir os dados dos indivíduos, foi crucial para a criação em outros países, como no Brasil, onde instituiu-se a Lei Geral de Proteção de Dados Pessoais (LGPD). Muito

embora, a lei brasileira trouxe um arcabouço de normas reguladoras e sanções aos casos de tratamento de dados, que não foram abarcados com o marco da internet, os dados em uma visão macro constitucional já eram de forma genérica tutelados pela Constituição Federal de 1988.
Todavia, apenas a sanção da LGPD não seria, isoladamente, capaz de coibir as violações ao tratamento de dados na esfera privada, mas sim a necessidade de uma regulamentação do ciclo de vida das informações, que além de estipular os dados que podem ser utilizados ou até quando podem ser armazenados, estabelecer expressamente no bojo da norma como deve ser a proteção na operação do tratamento de dados.
De forma efêmera, conclui-se que a legislação pode delimitar os alicerces capazes de ensejar uma fiscalização, sendo estas através de mecanismo de gerenciamento de atividades, políticas de condutas e implementação de governança de dados, pois os dados hackeados ou vazados de forma isoladas, não seria possível identificar dados sensíveis, muitos menos individualizar o sujeito.
Portanto, o gerenciamento dos dados em provedores de armazenamento pode ter os riscos reduzidos de acordo com a realização de medidas de compliance para dirimir os impactos na

atividade empresarial, como também para tutelar os dados, cada vez mais acentuado como um produto orçamentário.

2 COMPLIANCE EMPRESARIAL

A criação do compliance está entrelaçado sob o cenário econômico-social, assim, sua implementação como sistema de organização foi instaurado e aprimorado a partir dos problemas práticos estruturais para gerir uma boa governança, com intuito de assegurar a proteção e o controle que garante a qualidade do negócio.
A utilização do termo foi inicializada no mercado financeiro, especialmente após a criação do Banco Central em 1913 nos Estados Unidos da América, com a necessidade de um sistema econômico ajustável e estável. Só após 1960, com a regularização da Securities and Exchange Commission (SEC), que houve a necessidade de implementação do compliance como um programa para a integração dos procedimento, controle e monitoramento de operação interna. (CARVALHO, 2021)
Em 1977, com a Convenção Relativa à Obrigação de Diligência dos Bancos Suíços, estabeleceu os modelos auto regulatórios, com adequação de condutas e processos internos, na qual a infração tem como consequência à aplicação de sanções. (CARVALHO, 2021)
Só após esse processo de amadurecimento histórico, que o Brasil teve a necessidade de competir em escala global, implementado novos processos de segurança no sistema financeiro brasileiro.
Pode-se concluir que, após a globalização com o fenômeno da criação dos dados estruturais, houve a potencialização das informações adquiridas por meio de provedores, classificadas, atualmente, como fonte econômica de um produto quantificativo e qualitativo, ao qual possibilita uma utilização como um produto do sistema financeiro.
Nesse sentido, em decorrência de ataques cibernéticos em provedores de informações

massificadas conduziram a sociedade na aplicação de institutos de melhoramento, como o compliance e suas interfaces para proteger no ambiente corporativo os dados massificados recebidos em seus provedores.

2.1 O CONCEITO DE COMPLIANCE

Antes de enveredar sob o conceito de compliance na esfera privada, é oportuno compreender o seu significado. Nesse contexto, a palavra compliance advém do verbo inglês, to comply, que pode ser definida como conformidade. O instituto deve ser aplicado como plano principal de uma diretriz pré-estabelecida para ser dirigida a todos capazes de enfrentar a finalidade destinada. (BERTOCCELLI, 2019)
Nesse parâmetro, pode ser traduzida como:

Comply, em inglês, significa ?agir em sintonia com as regras?, o que já explica um pouquinho do termo. Compliance, em termos didáticos, significa estar absolutamente em linha com normas, controles internos e externos, além de todas as políticas e diretrizes estabelecidas para o seu negócio. (ENDEAVOR DO BRASIL, 2022, n.p)

O compliance pode-se ser definido de forma técnica como um conjunto de normas padronizadas, sob um viés ético e legal, na qual após estruturação será a matriz orientadora para o comportamento organizacional da instituição ao qual atuará no mercado, como também irá reger as atividades dos colaboradores. Dessa forma, sendo um instrumento hábil a controlar o risco de imagem, a normatização legal, chamados de riscos de compliance, as que recaem nas instituições no decorrer da sua atividade laboral. (CANDELORO, 2012).
Superada a barreira terminológica, a finalidade do compliance tem como escopo o gerenciamento adequado do risco de atividades, verificar adequadamente as normas éticas e legais, e estudar os possíveis danos tangenciais. Dessa forma, esses elementos visam a redução de perdas e danos, como também amplifica a cultura e fortalecimento corporativo nos moldes aos padrões exigidos, seja esse por lei ou na tentativa de dirimir o risco do serviço prestado.
Portanto, segundo a doutrinadora Frazão (2007, p. 42), destina-se em sua obra que o compliance é como:
(...) conjunto de ações a serem adotadas no ambiente corporativo para que se reforce anuência da empresa à legislação vigente, de modo a prevenir a ocorrência de infrações ou, já tendo ocorrido o ilícito, propiciar o imediato retorno ao contexto de normalidade e legalidade.

Nessa mesma linha de pensamento, de acordo com os autores da obra Compliance 360° (2012, n.p), referem-se o compliance a:

Um conjunto de regras, padrões, procedimentos éticos e legais que, uma vez definido e

implantado, será a linha mestra que orientará o comportamento da instituição no mercado em que atua, bem como as atitudes de seus funcionários; um instrumento capaz de controlar o risco de imagem e o risco legal, os chamados ?riscos de compliance?, a que se sujeitam as instituições no curso de suas atividades.

Pode-se concluir que o conceito de compliance, em uma esfera macro, é um aglomerado de regras pré-estabelecidas através de um instrumento perpetuado por técnica de desenvolvimento, capaz de dirimir riscos e danos das atividades devolvidas pelo plano diretor.
Muito embora, o instituto "compliance" tem uma definição extensiva e não tem como fim apenas o cumprimento da legislação e de condutas éticas, pode ser compreendida também como um instrumento de diminuição de riscos, desenvolvimento corporativo sustentável e subsequentes segmentos empresariais de negócio. (ROQUE, 2019)
O compliance além de estar associado tradicionalmente a uma perspectiva organizacional aos comandos administrativos, pode ser vinculada também a uma visão de uma sociedade digital 4.0, devendo não só apresentar o compliance empresarial na esfera de redução de risco à imagem, mas sim, em uma abordagem de pré-orientação e implementação de desenvolvimento aos moldes legislativo de proteção aos dados, como objeto principal de estudos.
Portanto, é necessário a elaboração do projeto de compliance em uma visão lógica, a modo de compreender os objetivos e os componentes da aplicação do programa. Posteriormente, superado os obstáculos, aplica-se os estudos de riscos a boa governança corporativa com a implementação de programas de governança de dados objetivando auxiliar o controle de informações em conformidade aos padrões da corporação, e mitigar os danos da empresa.

2.1.1 AS GOVERNANÇAS CORPORATIVAS E A IMPLEMENTAÇÃO DOS PROGRAMAS DE COMPLIANCE

Em linhas gerais, o Instituto Brasileiro de Governança Corporativa ? IBGC (2015, n.p) discrimina o conceito de Governança Corporativa, como: ?Sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas. ?
O sistema da governança corporativa está associado ao desenvolvimento interno de uma empresa, seja ele entre a administração, sócios e funcionários, capaz de criar elos para uma estruturação de direção racional e acima de tudo nos moldes da ética e legislação.
Muito embora, a governança corporativa e o compliance sejam institutos que se assemelham em uma visão macro, os mesmos, diferenciam na aplicação prática, mas se complementam no objetivo final, sendo um instrumento para aplicação do outro.

A prática da governança corporativa, além de estimular o valor empresarial, pode-se concluir que estrutura de forma adequada a medida necessária para organizar a atividade empresarial, assim, não há que se falar em condutas prejudiciais. Por exemplo: empresários compreendem que para realizar uma instrumentalização segura aos seus sócios e administradores tendem a prejudicar o negócio empresarial, assim o autor Eggon João da Silva (2005, p.259) retrata que: ?A governança corporativa assegura tratamento equânime a todos os acionistas, inclusive minoritários, preferencialistas, nacionais e estrangeiros. Todos devem ter oportunidade de reparação caso venham a sofrer violação de seus diretores. ?

Nesse passo, as críticas ao sistema não são viáveis, tendo em vista a utilização de instrumento capaz de integralizar ao plano empresarial. Sendo assim, o programa de compliance visa amplificar a utilização de um sistema para garantir que todos possam participar de forma justa sob o aspecto legal, seja sócio ou administrador.

Em uma tangente geral, a implementação da governança corporativa ressoa em uma perspectiva segura, tanto internamente, seja auxiliando as avaliações das atividades executadas pelos sócios/administradores, quanto externamente, em relação à imagem da empresa, sendo este um fator primordial a empresas estruturadas no mercado.

A implementação da governança corporativa deve ser estruturada de acordo com as necessidades da empresa, devendo verificar o histórico de desenvolvimento do estabelecimento, pois, só a partir do status da empresa pode-se delimitar a estratégia possível para uma implementação segura e adequada. Sendo assim, um regramento mais rigoroso pode gerar consequências negativas e ineficazes, especificamente em estágios primários, pois em atividades inicias, as tomadas de decisões e a execução da atividade empresarial é primordial, sendo necessário, um aspecto negocial informal para realizar os objetivos da empresa, o que não se verifica quando existe prática de boa governança devidamente estruturadas no negócio. (KLEINDIENST, 2019)

Ao desenvolver da atividade da empresa, além da atenção a organização interna, sendo está um fator primordial da governança, ainda que no fim acabe tendo um aspecto externo por vislumbrar no mercado financeiro uma maior complexidade da entidade. O desenvolvimento da empresa, seja no faturamento, importação comercial, quantidade de funcionários, além dos controles a observância da legislação e regras internas, tendem à serem complexos, e, que necessita

de ações maiores que a própria instituição empresarial, restando necessária a implementação de sistema organizacionais aos fluxos de informações. (KLEINDIENST, 2019)

Ultrapassado a esfera conceitual e instrumentalização da política de boas práticas de governança, cabe pontuar que as empresas que possuem fluxos de informações sensíveis, conforme estipula o artigo 50 da Lei Geral de Proteção de Dados Pessoais, os controladores e operadores são responsáveis pelo tratamento de dados, devendo criar planos de adequação a legislação.

Assim, ao confeccionar as regras de boas práticas, os controladores adjuntos com a administração devem estipular através da análise da natureza dos dados coletados, a probabilidade, a finalidade e o potencial de riscos das vantagens advindas dos tratamentos dos dados verificados. (NASCIMENTO, 2020)

É necessário pontuar que, os agentes de tratamento, após a autenticação da gravidade e sensibilidade dos dados aos riscos de operação, poderão estabelecer programa de governança em privacidade, sendo este, um instrumento amplo com normas de compliance, além dos aspectos operacionais.
Em relação ao programa de governança de privacidade, pode-se estabelecer como um aglomerado de normas-regras de boas práticas de governança, com a finalidade de executar ordens de natureza legal. (NASCIMENTO, 2020)
Portanto, os instrumentos do compliance em conjunto com a boa prática de governança, se consagram na identificação dos riscos e estruturação de medidas para a empresa, sendo respondida de forma adequada e proporcional ao suporte da tomada de decisão.
O Programa de compliance na esfera privada para análise de dados pessoais, com a finalidade de promover a segurança, deve ser constantemente monitorado e atualizado, com a implementação de ?salva vidas? em decorrência de avaliação de riscos à privacidade e o acometimento de vazamentos. (NASCIMENTO, 2020)
Portanto, os instrumentos e objetos referenciados demonstram a determinação de regras de governança no ambiente de operação de tratamento de dados pessoais, a modo que seja realizado uma estruturação nas empresas para que possibilitem a implementação de mecanismos de segurança, com a finalidade de dirimir os riscos da atividade empresarial na sociedade digital.

3 GOVERNANÇA DE DADOS

O mercado digital tem como principal ativo financeiro os dados, este considerado como ?matéria prima? de uma economia baseada no conjunto de informações, sendo que nos últimos anos, houve um aumento exponencial na coleta de dados por cooperativas, startups e novos nichos empresariais, tendo a finalidade de quantificar e gerencias os dados.
Dados, informações, conhecimento e sabedoria são os quatros estágios evolutivos da cadeia de informação, pode-se assim, compreender os dados como fatos ou registros em seu formato primário. (BEAL, 2014). Já a informação é entendida como os conjuntos processados de dados em um contexto aplicado (RÊGO, 2013). Muito embora, na sociedade da informação ?os dados são o novo petróleo?, apenas os dados isoladamente não são capazes de transformar em ativo financeiro, sendo necessário administrá-lo de forma eficaz, para que assim, as empresas adquiram vantagem competitiva.
Dessa forma, a governança de dados tem como principal objetivo atender as necessidades das empresas, ou seja, solucionar problemas, diminuir custos da administração, para que os dados transformem em saldo positivo para os negócios (TERRA, 2017).
O Data Governance Institute -DGI (2017, n.p) definiu governança de dados como ?um sistema de direitos de decisão e responsabilidades para processos relacionados à informação, executado de acordo com modelos acordados que descrevem quem pode realizar quais ações com quais informações e quando. ? Portanto, a utilização da governança de dados orienta quais os métodos deverão ser aplicados no ciclo de vida dos dados.

Uma das atribuições da governança é o acompanhamento da operação dos dados com a finalidade de gerir que as informações estejam alinhadas com os objetivos pré-determinados na coleta primária, além disso, é necessário assegurar que as informações estejam disponíveis para acesso, quando consultadas, gozar de qualidade, consistência, auditabilidade e segurança dos dados (ESPÍNDOLA, 2018).

No âmago da cadeia evolutiva da informação uma das preocupações dentro das organizações corporativas é o receio com a proteção das informações, ou seja, a capacidade das empresas no protagonismo da segurança com os provedores internos, tendo em vista a necessidade de conformidade com a legislação pátria.

A boa governança tem como objetivo aplicável à prática do controle dos processos de operação dos dados: a prevenção de situações adversas que podem gerar o comprometimento da integralidade dos dados adquiridos pelas organizações empresariais, que por sua vez, devem ter o condão de reforçar a confidencialidade das informações. (ESPÍNDOLA, 2018).

A integração do programa de governança de dados nas corporativas empresariais, tem como o esforço principal a organização de dados, que deve ser observado por um prisma basilar, ou seja, a aplicação dos princípios como limite legal e ético no ciclo de vida dos dados.

Para Rêgo (2013), os princípios são regulamentações para compreender aplicação da governança dos dados como linha direta para os negócios, sendo: (i) A gestão de dados estratégicos, tem o dever de vislumbrar as tomadas decisões por um coeficiente tático e operacional. (ii) A governança como instituição, ou seja, a governança de dados pode ser comparada como sistema governamental, na qual dispõe de legislação, execução e jurisdição; (iii) A governança de dados como um programa, devendo ser implementado como fator permanente, não apenas um projeto temporário. Ainda, pontua-se que os princípios da Governança de dados não são limitados, tendo uma orientação basilar a cada implementação de um sistema organizacional que deve ser observado pelo prisma ético e legal.

Assim, os princípios devem incumbir os papéis que a serem preenchidos pela gestão moldar os comportamentos das empresas para a aquisição, reserva e utilização dos dados conforme as normas e políticas da corporação (TERRA, 2017).

Coleta, armazenamento, recuperação e descartes, são as quatro etapas do ciclo de vida dos dados (SANTANA, 2013), ou seja, para a aquisição de dados pelas empresas, deverão observar a vida útil do dado para não incorrer na (in) responsabilidade da utilização indevida de informações dos seus provedores.

As fases do ciclo de vida dos dados devem ser observadas pela ótica de seis objetivos, sendo eles: a qualidade, a privacidade, os direitos autorais, a integração, compartilhamento e preservação dos dados (ESPÍNDOLA, 2018). Muito embora, a lei geral de proteção de dados implementou e traçou novos objetivos para a coleta de dados pessoais, cabe destacar que os objetivos vislumbrados na Governança de dados têm como parâmetro preliminar a tomada de decisão, na qual deve ser os negócios pautados nos moldes legais e éticos vigentes.

Nesse contexto, o controle de informações é necessário, tendo em vista que na sociedade da informação, cada vez mais o volume de dados é crescente, acarretando mais vazão e protesto

por políticas públicas para a preservação dos institutos, órgãos e empresas que detenham a

informação, sendo assim, necessário sistema de organização, softwares e hardwares capazes de processar as informações, criptografar e armazenar. (MARTIGNAGO, 2019)
Assim, para otimizar o ciclo de vida dos dados e garantir que os objetivos sejam preenchidos na estruturação do gerenciamento de dados, faz-se necessário a implementação de frameworks com o intuito de garantir que o procedimento seja cumprido com maior qualidade de informação e aproveitamento financeiro para a empresa, auxiliando a tomada de decisão para redução de risco para utilização de dados. (MARTIGNAGO, 2019)
Um Framework, segundo Johnson (1991), pode ser definida como um aglomerado de objetos que colabora entre si para que atinja um conjunto de obrigações para aplicação de um domínio especifico. Já para Pinto (2000), um framework é conceituado como um software incompleto criado para ser um objeto cujo estado e comportamento são definidos pela classe. Assim, o framework é uma concepção de uma arquitetura para um edifício de subsistemas e oferece o alicerce básico para criá-los.
Muito embora, os autores defendem uma conceituação distintas acerca da concepção de frameworks, pode-se verificar que ambas se complementam, tendo em vista que o framework é um sistema pré moldado, ou seja, é um programa com intuito de ser complementado através da finalidade a ser cumprida pela gestão empresarial, sendo instanciado por classes para categorizar os dados e ser alojado em hotspot, provedores físicos, capazes de armazenar as informações coletadas pelas empresas.
Portanto, para gerenciar os ativos de dados de forma complexa, ordenada e objetiva é necessário para proteção do procedimento do ciclo de vida dos dados, determinar os modelos de frameworks para o gerenciamento dos dados. Assim, para Carvalho (2021), podem ser apresentados três domínios CobiT, DAMA DMBOK e DGI Framework, sendo apenas dois destes observados para fomento deste artigo: (i) A DAMA (DAMA DMBOK), e (ii) CobiT.
A DAMA (Data Management Association) é uma associação sem fins lucrativos, com o intuito de promover boas práticas de gestão de dados, e em 2009 fundou o DAMA-DMBoK (Data Management Body of Knowledge), sendo um corpo de conhecimento que tem como ponto fundamental esclarecer como as corporativas devem aplicar a operação otimizada dos dados. (CARVALHO, 2021)
Em sua versão 2.0, acrescenta não só uma visão macro do gerenciamento de dados, definindo padrões, terminologias e práticas, mas a integração de dados, para definir táticas,

armazenamentos e sistemas, bem como implementação da ética na operação do tratamento de dados, a definição de big data e ciência de dados e amadurecimento das informações. (LIMA, 2019).
O DAMA-DMBOK V2 é formado por 11 (onze) funções de gestão de organização de

dados, sendo incorporado como cerne principal: a governança de dados, tendo em vista que os dados percorrem por toda sistemática das onzes funções ordenadas, assim segundo Honório (2021):
A primeira função é a governa de dados, sendo o pilar do framework, tem o condão de orientar e supervisionar a operação do ciclo de vida dos dados, na qual deve estabelecer um sistema de apoio a decisão dos gestores sobre os dados, sob o prisma do negócio.
A arquitetura de dados, a segunda função, pode ser conceituada como um planejamento para administrar os dados, aquisição de ativos da empresa, com o intuito de definir a finalidade das informações adquiridas com os requisitos necessário para o gerenciamento dos dados.
Por sua vez, a modelagem de dados e design, tem a função de demonstrar de forma nítida os dados, sendo o processo da descoberta, análise e representação da etapa primária da informação.
O armazenamento, uma das etapas da operação do ciclo de vida dos dados, na qual vai incluir o design, o suporte dos dados armazenados para quantificar o coeficiente valorativo das informações, até o seu descarte, devendo respeitar todo o procedimento de segurança legal vigente.
Um dos alicerces para o gerenciamento de informação é a segurança, que deve garantir a proteção dos dados, a execução de políticas e procedimento de segurança, no intuito de moderar o acesso de forma consciente e controlado, não devendo ser infringido ou acessado de forma inadequada, afim de garantir autenticação e auditoria de dados informações.
A Integração e Interoperabilidade de dados, é a função responsável pela movimentação e a concretização dos dados na interligação do armazenamento e outras plataformas.
O gerenciamento de documentos, pode ser compreendida como o gerenciamento e inclusão da vida útil dos dados e informações, encontrados em programas não estruturados, em ênfase ao conteúdo de apoio de conformidade a legislação vigente e os termos éticos formalizados para o negócio.
Dados mestre e de referência, tem como condão a manutenção dos dados compartilhados para coexistir a integralidade dos sistemas internos de gerenciamento dos dados.
Em razão da interligação entre uma linha direta com os negócios, uma das funções do DAMA-DMBOK é a Data warehousing e Business intelligence, ou seja, a implementação de

planner para o contoler da administração dos dados e suporte a decisão com o intuito de conceder aos gestores de informação emitam relatórios de equalização de valores.
Segundo Barata (2015), os metadados, na qual consiste a décima função, é promover a facilitação do acesso dos dados interligados nas multifontes do sistema integrado, como também garantir a qualidade de dados.
Por fim, o gerenciamento de qualidade de dados é a implicação das técnicas para garantir a possibilidade de aferição, melhoramento e adequação da utilidade dos dados, com o intuito de monitorar a integridade da informação primária no ciclo de vida dos dados.
Já o COBIT (Control Objectives for Information and related Technology), é um framework de suporte fundado em 1994 administrado pela ISACA (Information Systems Audit and Control Association), estruturado como um arcabouço de informação direcionadas para governança de dados e gerenciamento de informação, tem como objetivo auxiliar os profissionais de gestão na conexão entre os problemas técnicos e os riscos do negócio. (BARATA, 2015).

Para Lima (2019), o COBIT é um framework que possui duas vertentes basilares: a gestão, que possui quatro áreas de domínios: planejamento, constituição, execução e monitoramento, e a governança que é a tomada de decisão de acordo com a gestão de dados, possuindo 37 (trinte e sete) processos integrados.
Na versão 5.0, o sistema é utilizado baseado em 05 princípio, conforme elucida Casaes (2019), Barata (2015) e Lima (2019), sendo: (i) atender às necessidades das partes interessadas; (ii) cobrir o negócio como um todo; (iii) aplicar um framework único e integrado; (iv) habilitar uma visão holística; e (v) distinção entre governança de gestão.
Um dos princípios é atender às necessidades das partes interessadas, sendo a necessidade das corporativas é satisfazer as expectativas dos seus stakeholders, proporcionando um equilíbrio na tripartite: benefícios, redução do risco e recurso disponíveis.
O segundo princípio é baseado na cobertura do negócio como um todo, ou seja, abranger a integralidade da empresa no processo, procedimento, pessoas e as relações com os habilitadores.
A aplicação do framework único e integrado, assim, o COBIT é capaz de promover uma relação completa com a Governança de dados, corroborando ao alinhamento com padrões externos e adaptabilidade dos modelos usuais de negócios.

O COBIT permite habilitar uma visão holística, ou seja, uma visão macro dos componentes que oferecem suporte para atingir as finalidades da governança de dados, na qual define como catalogadores: as políticas, processos, estruturas organizacionais, informação e ética.
Por derradeiro, o princípio da distinção entre governança de gestão, tendo em vista que ambos possuem estruturas organizacionais distintas, assim, governança tem como esforço principal que os objetivos corporativos sejam cumpridos, estabelecendo prioridades pela tomada de decisão, compliance e progresso das organizações. Por sua vez, a gestão é o planejamento, construção, execução e monitoramento das funções ornamentada com o direcionamento da governança.
Desse modo, com escalonamento dos cinco princípios é capaz de proporcionar o funcionamento otimizado do framework, destacando os seguintes processos:
O APO01: Gerenciar o framework de TI, tem como condição a otimização das atividades relacionadas ao TI, com a função principal de incluir os procedimentos e regulamentos para promover a integralidade das informações nos bancos de dados. (BARATA, 2015)
Já o APO03: Gerenciar a arquitetura corporativa, tem função primordial agrupar as informações para auxiliar as atividades e tomadas de decisões, conceituando e compartilhando as informações dos elementos dos dados, e por fim catalogar a empresa, com base na modulação e sensibilidade dos dados. (BARATA, 2015)
Nesse ínterim, a governança de dados como um sistema integrado com o programa de compliance, tem o condão de otimizar a operação de controle interno relacionado aos dados coletados pelas empresas, capaz de gerenciar as bases para o apoio de decisão ao tratamento das informações, com segurança e qualidade, garantido o ciclo da vida útil dos dados.

4 A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

As estruturas políticas, econômicas e sociais com desenvolvimento de novas tecnologias e mecanismo para a coleta de dados e informações, fez necessário modulações legislativas para a proteção da privacidade, além dos aspectos físicos, patrimoniais e morais.
A proteção à privacidade de dados foi dividida em quatros gerações: a primeira, oriunda do estado moderno, com o advento dos bancos de dados; a segunda, datada em 1980, com a expansão legislativa para a proteção à privacidade aos setores privados; a terceira geração em 1990, com o processo de tratamento de dados e o consentimento dos cidadãos; Por fim, a última dimensão, é

destinada ao protagonismo da permissão para coleta e uso dos dados pessoais, quando a lei estabeleceu a importância da titularidade das informações. (MENDES, 2014)
Nesse aspecto, é perceptível a evolução do direito aos fatores reais da sociedade e as transformações dos meios tecnológico, computacionais, genéticos e comunicativos, que por sua vez possibilitou a integração da comunicação global, e consequentemente, o rastreio dos dados através do armazenamento de informação. (SAAD, 2021).
Os legisladores ao considerar os dados pessoais como extensão ao direito à privacidade, preocuparam em tutelar constitucionalmente a proteção da população, em especial os países europeus, como: Espanha, Portugal, Hungria, Eslovênia e Rússia. (VIEIRA, 2007) Porém, só tornou-se fator primordial após o regulamento geral do Parlamento Europeu sobre a proteção de dados, n.º 2016/679, sendo necessário a adequação das empresas prestadoras de serviço na Europa ao regulamento, influenciado diretamente o Brasil para elaboração da Lei Geral de Proteção de Dados brasileira. (SAAD, 2021).
Muito embora, a Lei Geral de Proteção de Dados Pessoais - LGPD, em sua promulgação, não abarcou de forma expressa a proteção de dados como direito fundamental, a doutrina, em especial Nascimento (2020), por sua vez, já argumentava a proteção de dados e informações pessoais como direito autônomo, derivado do direito fundamental à privacidade, explicitamente no artigo 5°, X, da CRFB de 1988.
Após reiterados julgamento sobre a tutela dos dados pessoais como extensão da personalidade do indivíduo, o Supremo Tribunal Federal -STF reconheceu no Julgamento da Ação Direta de Inconstitucionalidade - ADI 6387, a existência dos dados como direito autônomo, derivada do direito fundamental a dignidade da pessoa humana, na proteção à intimidade e a centralidade do Habeas Data como autodeterminação informativa. (NASCIMENTO, 2020).
Ao compreender a necessidade da proteção aos dados pessoais, os legisladores brasileiros em votação de ? das casas legislativas (câmara e Senado Federal) em dois turnos, aprovaram a Emenda Constitucional 115 de fevereiro de 2022, alterando o artigo 5° da Constituição Federal de 1988, incluindo o inciso LXXIX, tutelando constitucionalmente a proteção aos dados pessoais, inclusive nos meios digitais.
Ressalta-se, ainda, que os dados pessoais estão interligados com o direto fundamental à privacidade, na qual representa a capacidade de a pessoa administrar sua vida, seus pertences e

propriedades materiais e imateriais, permitindo ou não a utilização dos seus dados (bens imateriais) por terceiro. (NASCIMENTO, 2020).

A privacidade, por sua vez, segundo Mendes (2008), é o direito à proteção aos comportamentos pessoais e acontecimentos de caráter íntimo, bem como as informações prestadas aos profissionais e comerciantes, em que a pessoa não deseja que se compartilhe com o público.

Para o professor William Prosser, pode-se qualificar a lesão a privacidade em quatro graus: i) o intrometimento na reclusão ou solidão na vida privada, ii) a divulgação pública de fatos privados constrangedores sobre o indivíduo; iii) a publicidade sobre o indivíduo apresentada de forma equivocada; e iv) a apropriação, para obtenção de vantagem, do nome ou da imagem do demandante (PROSSER, 1960).

A doutrina, por sua vez, defende mais uma violação à privacidade: a privacidade informacional, interligada com os fatores tecnológicos de informação. (SAAD, 2021). Assim, quando a lei ao realizar o tratamento da privacidade, refere-se como um direito líquido, ao qual será tutelado para garantir que o indivíduo tenha um local reservado, que não tenha, se desejar, a interferência de outros sujeitos, seja pessoa física ou jurídica.

Com a proteção dos dados pessoais dos titulares, através da LGPD, possibilitou ao cidadão o acesso a informações ao ciclo de vida útil dos dados pelas empresas, e a certeza de fiscalização pela Autoridade Nacional de Proteção de Dados, com a finalidade de atingir os objetivos traçados pela legislação, na qual a lei traz conceitos e delimita princípios, que devem ser mencionados.

A LGPD tem como objetivo principal: ?o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado?, com a destinação de assegurar os direitos fundamentais a liberdade e privacidade dos titulares dos dados, bem como tutelar a dignidade e a personalidade da pessoa natural. (LGPD).

A legislação está ordenada diretamente com o meio empresarial, sobretudo no que se refere aplicação aos seus destinatários que são pessoas físicas ou jurídicas que realizam a coleta e tratamento de dados no Brasil, conforme preceitua o artigo 1° da lei 13.709, de 14 de agosto de 2018.

Para compreender a LGPD, faz-se necessário elucidar os conceitos de dados pessoais: (art. 5º, I) é toda informação relacionada a pessoa natural, identificada ou identificável, sendo o dado aplicado no contexto que possibilite o reconhecimento do indivíduo. Bem como refere-se aos dados sensíveis (art. 5º, II), são todas as informações que se relaciona com pensamentos políticos, crenças,

identidade biológica e física. Portanto, a legislação tem como ponto a proteção e o cuidado para a não violação dos dados pessoais e sensíveis.

Os doutrinadores, Laura Schertel e Danilo Doneda, ainda aponta cinco pilares para compreender a LGPD, sendo: i) a unidade e generalidade da aplicação da Lei; ii) a legitimação para o tratamento de dados (hipóteses autorizativas); iii) os princípios e direitos do titular; iv) as obrigações dos agentes de tratamento de dados e v) a responsabilização dos agentes.

O primeiro pilar é considerado com aplicabilidade material da legislação, ou seja, aplica-se a qualquer operação realizada por pessoa natural ou jurídica de direito público ou privado,

independentemente do meio, da sua sede ou do país onde estejam localizados os dados (Art. 3°). Considerado, assim, como uma aplicação uniforme para todos os setores público ou privados que realizam tratamento de dados.

O segundo pilar é a legitimação para o tratamento de dados, tendo em vista que a lei especificou critérios e requisitos para o reconhecimento da legitimidade, não podendo ser tratados os dados, sem que exista uma base normativa que autorize, prevista no artigo 7°, 11° ou 23° da LGPD, abordando 11 (onze) hipóteses, incluído o consentimento ou a previsão legislativa.

Destaca-se que a autorização por consentimento para ser considerado válido, deve observar os requisitos previsto no artigo 5°, XII, sendo considerado que a vontade deve ser livre, informada, inequívoca e com a finalidade determinada, consagrando os princípios norteadores da legislação.

O terceiro pilar é o conjunto de princípios e direitos que assegura o destinatário da lei a controlar a utilização do seu dado pessoal, sendo importante elencar dez princípios que estruturam a LGPD: a finalidade, a adequação, a necessidade, o livre acesso, a qualidade dos dados, a transparência, a segurança, a prevenção, a não discriminação e a responsabilização. (MENDES, DONEDA, 2018)

No que concerne, aos direitos dos titulares são expressos no artigo 18° da referida lei, que permite o titular dos dados adquirir através do controler, independentemente do momento, as informações relacionadas ao indivíduo, prevendo: acesso, confirmação, correção, anonimização, bloqueou ou eliminação e a portabilidade.

Para adentrar no cerne dos problemas enfrentados pela legislação, em especial, sobre o vazamento de dados, os dois últimos pilares serão abordados sob a perspectiva da violação e responsabilização acerca da proteção de dados nos casos incidentes de vazamento.

Assim, o quarto pilar, destina-se às obrigações dos agentes de tratamento dos dados, na qual estabeleceu limites que devem ser observados nas operações realizadas para reforçar a segurança e prevenir os problemas da atividade no tratamento de dados.

Uma das obrigações fundamentais, consiste na intitulação do encarregado pelo tratamento dos dados indicados pelo controlador, conforme artigo 41 da LGPD, que possui a função de aceitar as reclamações e comunicações dos sujeitos dos dados, receber informações da Autoridade Nacional, como deve orientar os funcionários a respeito das práticas a serem adotadas em relação à proteção de dados pessoais.

Assim, as informações devem ser fornecidas ao proprietário dos dados, quando os dados forem coletados, como: os meios de segurança aderidos ao tratamento de dados, quais são os riscos da atividade que podem gerar lesão ao titular, pois pode gerar a mitigação dos prejuízos. (SAAD, 2021)

A lei Geral de Proteção de Dados Pessoais tem como objetivo a proteção do dados pessoais dos titulares dos dados, sendo assim, uma das obrigações principais é adoção de medidas de segurança, técnicas e administrativas hábeis a proteger os dados pessoais de acessos não autorizados, como promover a integralidade dos dados, não permitindo, assim, a alteração das informações, a prevenção de situações ilícitas ou acidentais, ou qualquer forma de tratamento inadequado, consoante se desprende do artigo 46 da lei.

Tornou-se corriqueiro manchetes acerca do vazamento de dados por corporativas, uma das violações mais graves incidentes abarcados pela LGPD, o que ocasiona a vulnerabilidade do titular dos dados, e dos sistemas internos que são responsáveis pelo ciclo de vida útil dos dados. (SAAD,2021)

A seção de segurança de informação tem como condão as obrigações inerentes aos agentes de tratamento, devendo ser adotado pela integralidade das pessoas que realizam o tratamento de dados, garantido que os dados sejam confidenciais, bem como disponíveis nas operações de tratamento. (Art.48). Nos casos incidentais de vazamento de dados, insurge a necessidade ao controlador de informar a autoridade de proteção de dados, que podem definir as medidas para mitigação dos danos.

No entanto, com a utilização da internet, compras online, transferência virtuais e outros meios tecnológicos, criou-se uma dificuldade para atuar na segurança de dados, tendo em vista a abrangência e os domínios de redes globais, que combinados com fatores não perceptível, forma

um perfil não rastreavel capaz de ocasionar violação às diretrizes básicas da legislação, que mesmo com ações posteriores não conseguem excluir os inúmeros registros de pessoas e organizações que coletaram os dados, lesionando a confidencialidade das informações (SAAD, 2021)

Destaca-se que as obrigações aos controladores e operadores, devem ser observados desde a coleta dos dados até seu descarte, assim o artigo 46 da LGPD, introduziu o conceito de privacy by design, sendo a incorporação pelas empresas nos serviços e produtos, na qual dispõe a proteção da privacidade no centro de todo o desenvolvimento corporativo.

Embora, a legislação tenta dirimir os riscos da atividade, os prejuízos causados pelo vazamento de informações são altos, e perpassam pela inadequação do sistema de proteção, perda de credibilidade e de clientes, ocasionado uma ruptura na imagem da empresa, impossibilitando, muitas vezes de concorrer no mercado corporativo. (SAAD,2021)

Portanto, a LGPD concebeu obrigações aos agentes de tratamento de dados, para que se delimite a finalidade da utilização dos dados desde o início da concepção, devendo o controlador confeccionar relatório de impacto a privacidade, utilizando de métodos para a captação da operação do ciclo de vida dos dados, observando as mediadas adotada para aumentar a segurança e mitigar o risco do tratamento das informações, conforme artigo 3 da LGPD.

O último pilar, considerado como a responsabilidade dos agentes na incidência de ocorrência de danos derivados do tratamento de dados. A LGPD consagrou a natureza do tratamento, limitando os parâmetros ao artigo 7° da lei, nas 10 hipóteses dos incisos, vinculados a finalidade da captação dos dados, consoante prevê o artigo 6°, inciso I, II, da LGPD.

A legislação tem como regra o descarte (eliminação) dos dados ao fim do tratamento da operação (art. 16), com o intuito de mitigar os riscos presente no tratamento de dados, principalmente, no que concerne à limitação das hipóteses de tratamentos para não lesionar os direitos dos titulares.

Nos casos, em que mesmo após o término de vida útil dos dados, as empresas podem, quando permitido, armazenar dados que em situação incidentais serem objetos de violação, principalmente nos casos de vazamento, que podem ocorrer, quando não autorizados pelo titular

ou controladores, serem acessados, captados, compartilhados pela internet, para outros sujeitos ou empresas.
Assim, a Lei Geral de Proteção de dados Pessoais, em especial em seu artigo 42, dispõe que o controlador ou operador, quando realizar o exercício do tratamento de dados pessoais, vem

a ocasionar dano patrimonial, moral, individual ou coletivo em detrimento a aplicação da legislação, é obrigado a repará-lo, definindo a responsabilidade de forma objetiva.
Embora, a responsabilização objetiva não é necessária a demonstração de culpa do controlador ou operador. Faz mister esclarecer que o operador, só será responsabilizado quando os atos praticados forem contrário à legislação, ou às instruções que foram fornecidas pelo controlador. (MENDES, DONEDA, 2018)
Ainda, a legislação prevê exceções a responsabilidade objetiva (art. 43), sendo: quando o agente demonstrar que não realizou o tratamento de dados pessoais que foi atribuído, ou quando não houve violação da segurança ou a legislação, e por fim, quando for por culpa exclusiva do titular ou de terceiros.
Porém, o cenário que é vislumbrado no Brasil nos casos de vazamento de dados, é que as violações pelas instituições vêm ocorrendo, majoritariamente, sob ataques deliberados de hacker, ou falha de segurança dos controladores dos dados. (SAAD, 2021)
Dessa forma, é necessário adotar medidas para dirimir os riscos da atividade, e possibilitar o discernimento das informações acerca dos perigos de vazamento de dados, tendo em vista que a tendência é aumento significativo das violações vinculados com a crescente tecnológica. Assim, as empresas devem implementar mecanismos para a segurança das informações.

5 O COMPLIANCE EMPRESARIAL COMO INSTRUMENTO DE PROTEÇÃO DE DADOS NA ESFERA EMPRESARIAL

Em decorrência das constantes violações aos dados armazenados em provedores privados, a tutela ao direito à privacidade nos meios tecnológicos, já era pauta de debate na legislação brasileira, e já existiam mecanismos para a proteção, como: a proibição de direcionamento dos provedores em relação ao compartilhamento de dados, bem como a inibição ao monitoramento nos navegadores de internet.
Vinte e seis bilhões de dados foram vazados no Brasil em 2019, de acordo com pesquisas realizadas pelo Massachusetts Institute of Tecnology ? MIT, possibilitando a utilização de números telefônicos, score de crédito, endereço eletrônico, fotos, números de identificações e outros dados pessoais, para o cometimento de crimes cibernéticos, e a violação aos direitos dos titulares.
A utilização e uso dos dados pessoais por pessoa física ou jurídica, com sede no Brasil ou não, devem se atentar as normas gerais de proteção aos dados brasileiro, segundo Frazão, Oliva e

Abilio (2020), é a necessidade de conferir a efetividade aos direitos e prevenir a violação aos dados, através da implementação de mecanismo de compliance, como uma ferramenta capaz de promover a adequação das atividades aportadas pelas empresas.
Assim, os controladores e operadores poderão formular regras de boas práticas e governança (Art. 50), que contenha as disposições de organização interna, o regime de funcionamento, as operações, o canal de comunicação entre os encarregados e os titulares dos dados, e o procedimento de segurança.
Nessa perspectiva, considerando que a maioria das tratativas de dados perpassam por meios digitais, deve-se adotar sistema para mapear os riscos, e implementar mecanismos para minorar as vulnerabilidades apontadas pelos programas, através da alta administração, do código de ética, para proteger os dados pessoais dos titulares. (PESSOA, 2021)
Existem inúmeras formas de ocorrer o vazamento de dados, sendo através de ataques cibernéticos, sequestro de conta, furtos de dados, compartilhamento de dados por agentes ou ex-agentes da empresa, erro ou negligência, entre outros, que podem ser para adquirir dados de nomes, CPF, celulares, endereços, dados financeiros, senhas, registro de saúde ou credenciais de acesso. (SAAD, 2021)
Desse modo, para realizar o mapeamento dos problemas que as corporativas podem enfrentar, é necessário identificar os fluxos e processos de informação que percorrem os sistemas, que irão auxiliar na tomada de decisão pelas empresas. (NASCIMENTO, 2020)
A alta administração deverá colaborar ativamente no programa de compliance, seja monitorando as investigações e intervenções em situação para estabelecer controles internos em conformidade com a legislação, bem como possibilitar a interdependência dos setores para realizar as atividades designadas para o tratamento de dados (PESSOA, 2021).
Com a elaboração do código de ética pela organização possibilitará o treinamento regular das equipes, responsáveis pela tecnologia da informação, para enraizar a cultura corporativa da boa governança, com a finalidade de assegurar o respeito ao programa de compliance (NASCIMENTO, 2020)
Nesse contexto, para manter uma boa relação com seus clientes, as organizações devem instalar canais de comunicação, para que os titulares dos dados possam contatar os encarregados responsáveis pelos armazenamentos dos seus dados, e exerçam seus direitos sobre as informações contidas nos provedores. (PESSOA, 2021).

Desse modo, quando se trata de concretização a alteração cultural coportariva é preciso realizar o alinhamento dos funcionários com o código de ética, com política de privacidade, para fins de efetividade do programa de compliance de dados. (PESSOA, 2021).

5.1 A IMPLEMENTAÇÃO DE MECANISMOS DE GOVERNANÇA DE DADOS PESSOAIS

Para a efetividade da legislação em relação ao tratamento de dados, a LGPD direciona um capítulo para implementar o programa de governança em privacidade, com a finalidade das empresas adotarem medidas técnicas, para fins de proteção e segurança dos dados pessoais.

(PESSOA, 2021)
A governança em privacidade, pode ser conceituada como um conjunto de regras e práticas positivas a serem implementadas pelos agentes de tratamento, e encontra-se em conformidade com as políticas de compliance empresarial, com o objetivo de gerir os dados das empresas para estabelecer um diferencial competitivo aos negócios. (KOEPSEL,2020)
O programa integra o aperfeiçoamento do procedimento de utilização dos dados, com os requisitos pré-estabelecidos na implementação dos softwares, com a finalidade de gerir de forma otimizada os dados para preencher as diretrizes da legislação. (SAAD, 2021)
A Lei Geral de Proteção de Dados Pessoais dispôs que os controladores e operadores poderão adotar programas de governança em privacidade, que devem ser implementados com o mínimo, (art. 50, § 2°, I): a) o comprometimento dos agentes de tratamento com as políticas internas que devem garantir o cumprimento das normas e regras de boas práticas; b) que aplicação seja de forma uniforme para todo a operação de tratamento de dados; c) que a governança seja adaptativa as estruturas da empresas, sendo compatível com a densidade dos dados e operação; d) como implementar políticas de salvaguardas em relação aos titulares dos dados; e) tenha como objetivo estabelecer uma relação de confiança com sujeitos dos dados, estabelecendo situações de transparência e que possibilite a atuação do titular; g) que conte com planos de respostas a incidentes e remediações; h) seja continuamente atualizado sua base.
Nesse aspecto, devem ser adotadas medidas administrativas para que as instituições, em conformidade com a legislação, apliquem estímulos para assegurar as informações armazenadas pelas empresas, com a adoção de orientações internas que respeitem as diretrizes que inclua o uso

minimizado ou a anonimização das informações, desde a coleta dos dados, conforme artigo 46 da LGPD.
Com o mapeamento das atividades, é importante verificar: O que são esses dados?; de que forma foram coletados ?; quem são os coletores ?; existe relação entre os dados e atividade realizada ?; O que pode ocorrer com esses dados ao serem coletados? E, como são descartados da gestão organizacional da empresa? (NASCIMENTO, 2020). Dessa forma, para adotar medidas compatíveis com os riscos alertados pelos sistemas para a proteção de dados nas organizações privadas, é necessário possuir conhecimento do caminho realizado inerentes ao ciclo de vida útil dos dados.
Embora, a legislação já estabeleça diretriz mínima para o tratamento de informação, a Autoridade Nacional de Proteção de Dados - ANPD, poderá, ainda, determinar padrões técnicos para serem implementados pelo programa de governança em privacidade, devendo ser observado a qualidade de dados, as especificações do tratamento e status tecnológico, em especial a proteção aos dados sensíveis disposto na legislação. (NASCIMENTO, 2020)
Muito embora, a lei geral de proteção de dados, apenas delimita as características e os requisitos mínimos que os operadores deverão tomar para desenvolver um compliance na organização das empresas privadas em consonância com a legislação, porém não impõe um modelo específico para integração de um programa nas corporativas. (PESSOA, 2021)
Assim, para Saad (2021), as medidas técnicas que podem ser adotadas pelos agentes de

tratamento de dados, são: i) o uso de firewalls, sendo um mecanismo de segurança que coleta os dados em conformidade com as regras pré estabelecido para análise de tráfego de rede, delimitando as operações de compartilhamento e captação de informações a serem cumpridas; ii) a utilização de antimalware, que consiste na proteção contra vírus que é capaz de fragilizar o sistema, apagar dados e infectar outros arquivos; iii) a utilização de criptografia dos dados, que possibilite quando ocorrer situações incidentais a não identificação do titular do direito.
Já para Fernandes e Abreu, (2014) defendem a implementação de frameworks como a DAMABOK e COBIT, para o gerenciamento de dados, pois tem como meta principal a delimitação do escopo das atividades, as funções envolvidas no tratamento e as interações a serem executadas pelo software, com a finalidade de proteger a privacidade em ambientes corporativos que gerenciam o armazenamento de informações aplicados na prevenção à fraude.

Segundo Carvalho (2021), a integração do software, através das boas práticas estabelecidas pela legislação, poderá aprimorar os aspectos de proteção à privacidade e prevenção a fraude do tratamento de coleta de dados. Tendo em vista, que os frameworks, podem balizar as métricas de qualidade dos dados que indicam uma utilização adequada e otimizada, e aponta a melhor proteção da privacidade.
Com a melhoria de processo de governança para o tratamento de dados, estabelece uma divisão entres as operações que possibilita uma automatização do ciclo de vida dos dados (coleta, utilização, armazenamento e exclusão), capaz de gerar relatório de risco, para o auxílio da tomada de decisão com o intuito de gerir de forma adequada o tratamento de dados. (CARVALHO, 2021)
Neste parâmetro, os programas de compliance com a implementação de frameworks, podem responder questionamento acerca do procedimento de tratamento de informação, dispondo de quais práticas relacionadas à governança, privacidade e segurança de dados, apresentam melhor benefício para o tratamento de dados pessoais. (CARVALHO, 2021)
Ademais, os controladores e operadores deverão adotar medidas, como o Relatório de Impacto ? DPIA), que corresponde a avaliação dos riscos e impactos relacionados com o tratamento de dados pessoais, além da anonimização, da transparência e do sigilo, deverão delimitar prazos para retenção de dados e aderir políticas seguras de informação acerca da operação de tratamento. (SILVA, 2022)
Após realizar a implementação e observância das estruturas mínimas estabelecidas pela LGPD, é necessário adotar um programa de gerenciamento de vulnerabilidades, com atualizações constantes e autocorreções alinhados com as boas práticas de atividades cotidianas, com a finalidade de proteger os dados pessoais, e promover um ambiente corporativo adequado para realizar o tratamento de dados. (SAAD, 2021)
No entanto, ao verificar que houve vazamento de dados, seja pelo recebimento de notificação ou pela veiculação na mídia, os agentes de tratamentos deverão identificar quais dados vazaram e realizar o procedimento estabelecido no programa de compliance de segurança, além de notificar as instituições. (Art. 48, caput).
De acordo com MIT, o prazo entre a comunicação à autoridade competente e a ocorrência do fato ilícito ultrapassa 200 (duzentos) dias em média, sendo umas das preocupações para a

efetividade da legislação, e a redução dos danos causados aos titulares dos bens imateriais.

A Lei Geral de Proteção de Dados, dispõe que nas situações que ocorrer a probabilidade de riscos ou violação aos direitos dos titulares, tem como obrigação do encarregado a comunicação à autoridade nacional e ao titular do dado (art. 48, caput). Sendo que o contato deve ser em período razoável (art. 48, § 1º), contendo a natureza dos dados dos titulares atingindo (art. 48, § 1º, I).
Em decorrência dos possíveis incidentes, a LGPD determinou critério para aplicação de sanções, em casos de vazamento de dados, observando as situações específicas de cada caso, disposto no art. 52, § 1º. Assim, deve ser considerada a avaliação da gravidade, a natureza das informações e do dano ocorrido (incisos I e VI), sendo necessário para este caso, tendo em vista que o compartilhamento indesejado de dados sensíveis pode ocasionar danos irremediáveis para os titulares.
Portanto, existe a necessidade da adesão aos mecanismos e técnicas para promover a efetividade dos programas internos com a finalidade de mitigar os danos, assim, a implementação de boas práticas e governança têm como fator o cumprimento da legislação, por meio de medidas de segurança. Entende-se, que a proteção integral contra falhas que possibilitam a ocorrência de ilícitos não é possível, porém essas diretrizes reduzem as possibilidades de existir desvios de condutas e criar salvaguardas para identificação dos incidentes, de forma eficaz, rápida e adequada.

6 CONSIDERAÇÕES FINAIS

A partir da permissão ao acesso dos dados pessoais, as informações coletadas passaram a integralizar as redes de tratamento de dados, tornando-se alvo de ataques cibernéticos, contribuindo para o aumento da intercorrência no ambiente corporativo, tornando-se o gerenciamento de informação um dos diferenciais no desenvolvimento do negócio.
Nesse contexto, foi imperativo o surgimento de leis que protejam os dados dos cidadãos, e que limitem a gestão das entidades públicas e privadas em relação as informações coletadas, transformando o sistema organizacionais, como compliance, em ferramentas de efetivação das normas éticas e legais. Assim, a implementação do programa alinhado com a governança corporativa é capaz de integralizar o corpo de normas internas com o intuito de adequar a legislação brasileira e criar uma cultura corporativa.
Dentro do programa de compliance, a administração em conjunto com a gestão da empresa, poderá implementar ao plano diretor, a utilização de software, sendo este capaz de possibilitar a automatização do ciclo de vida útil dos dados para realizar o auxílio da tomada de decisão, com o intuito de mitigar os possíveis danos decorrentes da violação aos dispositivos da Lei Geral de Proteção de Dados Pessoais.
Nesse sentido, para realizar uma proteção extensiva aos direitos dos titulares dos dados, a

LGPD integrou ao seu corpo de normas-condutas a serem adotadas pelos operadores do tratamento de dados, com escopo de preservar a integralidade, a qualidade e o sigilos dos dados, tendo como consequência da violação, a majoração de sanções pecuniárias.
Embora, o vazamento de dados ocorra de forma ordenada, a implementação de sistema de segurança nas corporações implica na diminuição de situações incidentais por erro humano, ou inadequação dos programas empresarias, assim, devendo a gestão ensejar esforços para que a proteção dos dados seja preservada, desde a concepção do serviço.
Para a efetivação da Lei Geral de Proteção de Dados Pessoais, as empresas devem realizar a adequação de medidas de boas práticas e governança em privacidade para mitigar os possíveis danos decorrente da violação aos dados em provedores privados. Mesmo que a proteção aos dados de forma concreta não seja possível, as adoções de mecanismo de segurança podem atenuar as sanções e as perdas aos titulares dos dados.

REFERÊNCIAS

BARATA, André Mantola. Governança de dados em organizações brasileira: uma avaliação comparativa entre os benefícios previstos na literatura e os obtidos pelas organizações. 2015. Dissertação (Mestrado em Sistema de Informação) - Universidade de São Paulo, São Paulo, 2015.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, [2022]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 15 abr. 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidente da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 abr. 2023.

BERTOCCELLI, Rodrigo de Pinho. Compliance. In: CARVALHO, André Castro et. al. Manual de compliance. Rio de Janeiro: Forense, 2019. p. 35.

CANDELORO, Ana Paula; RIZZO, Maria Balbina Martins De; PINHO, Vinícius (Coord). Compliance 360: riscos, estratégias, conflitos e vaidades no mundo corporativo. São Paulo: Trevisan, 2012.

CARVALHO, A. P. Proposta de um framework de compliance à Lei Geral de Proteção a Dados Pessoais (LGPD): um estudo de caso para prevenção a fraude no contexto de big data. 2021. Dissertação (Mestrado em Engenharia Elétrica) - Universidade de Brasília, Brasília, 2021.

CARVALHO, Andre Castro. Manual de compliance. 3. ed. Rio de Janeiro: Forense, 2021.

CASAES, Júlio César Costa. Governança de dados abertos governamentais: frameworks conceitual para as Universidades Federais, baseada em uma visão sistemática, 2019. Tese (Doutorado em Engenharia e Gestão do Conhecimento). Universidade Federal de Santa Catarina, Florinaóplis, 2019.

DATA GOVERNANCE INSTITUTE (DGI). Definitions of data governance. 2017. Disponível em: http://www.datagovernance.com/adg_data_governance_definition. Acesso em: 01 mai. 2023.

ENDEAVOR DO BRASIL. Prevenindo com o Compliance para não remediar com o caixa. In: ENDEAVOR. [S. l.], 26 abr. 2017. Disponível em: https://endeavor.org.br/pessoas/compliance/. Acesso em: 15 mar. 2023.

ESPÍNDOLA, P. L.; SALM JUNIOR, J. F.; ROSA, F.; JULIANI, J. P. Governança de dados aplicada à ciência da informação: análise de um sistema de dados científicos para a área da saúde. Revista Digital de Biblioteconomia & Ciência da Informação, Campinas, v. 16, n. 3, p. 274-298, 2018.

FERNANDES, Aguinaldo Aragon; DE ABREU, Vladimir Ferraz. Implantando a governança de TI: da estratégia à gestão de processos e serviços. 4. Ed. Rio de Janeiro: Brasport, 2014.

FRAZÃO, Ana. Programas de compliance e critérios de responsabilização de pessoas jurídicas por ilícitos administrativos. In: ROSSETTI, Maristela Abla; PITTA, Andre Grunspun. Governança corporativa: avanços e retrocessos. São Paulo: Quartier Latin, 2007. p. 42

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. A Lei Geral de proteção de Dados Pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

HONÓRIO, Roseli. Modelo conceitual de governança de dados como suporte à governança do conhecimento organizacional. 2022. Dissertação (Mestrado em Engenharia e Gestão do Conhecimento) - Universidade Federal de Santa Catarina, Florianópolis, 2022.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC). Guia das melhores práticas de governança para cooperativas. São Paulo, 2015. Disponível em http://www.ibgc.org.br/ userfiles/files/2014/files/CMPGPT.pdf

JOHNSON, Ralph E.; RUSSO, Vincent. Reusing object-oriented designs. Relatório Técnico da Universidade de Illinois, UIUCDCS 91-1696, 1991.

KLEINDIENST, Ana Cristina. Grandes temas do direito brasileiro: compliance. São Paulo: Almedina Brasil, 2019

KOEPSEL, Alice de Medeiros. Adoção e efeitos dos programas de compliance à luz da Lei Geral de Proteção de Dados Pessoais. 2020. Monografia (Graduação em Direito) -Universidade do Sul de Santa Catarina, Florianópolis, 2020.

LIMA, C., BASTOS, R. C. A criação de conhecimento apoiada pela governança de dados. In: CONGRESSO INTERNACIONAL DE CONHECIMENTO E INOVAÇÃO, 2019, Santa Catarina. Anais eletrônicos [...]. Santa Catarina Disponível em: https://proceeding.ciki.ufsc.br/index.php/ciki/article/view/647. Acesso em 10 Mar. 2023.

MARTIGNAGO, Deisi et al. Governança de dados aplicado no processo de catalogação. Revista Brasileira de Biblioteconomia e Documentação, São Paulo, V.15, n. 2, 2019.

MENDES, Gilmar Ferreira. Curso de direito constitucional. 2. ed. São Paulo: Saraiva, 2008.

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. São Paulo: Revista de Direito do Consumidor, 2018.

NASCIMENTO, Suellen Lima do. A lei Geral de Dados Pessoais e a Adoção dos Programas de compliance na sociedade da Informação. 2020. Monografia (Graduação em Direito) - Centro Universitário de Brasília, Brasília, 2020.

PESSOA, Larissa Rocha de Paula. Os desafios da Governança de dados e a realidade cultural brasileira. 2021. Dissertação (Mestrado em Direito) ? Universidade Federal do Ceará, Fortaleza, 2021.

PINTO, S. C. C. S.. Composição em Web Frameworks, 2000. Tese (Doutorado em Informática) Pontifícia Universidade Católica do Rio de Janeiro, Rio Janeiro, 2000.

PROSSER, William L. Privacy. California Law Review. California, v. 48, n. 3. p. 383 ? 423, agosto, 1960.

RÊGO, Bergson Lopes. Gestão e governança de dados: promovendo dados como ativo de valor nas empresas. 1. ed. Rio de Janeiro: Brasport, 2013,

ROQUE, Pamela Romeu. Estudos aplicados de direito empresarial: LL.C. em direito empresarial. São Paulo: Almedina, 2019.

SAAD, Carolina de Oliveira. A lei geral de proteção de dados pessoais e incidentes de segurança: regulação e prática de vazamento de dados, 2021. Monografia (Graduação em Direito). Fundação Getúlio Vargas. Rio de Janeiro, 2021.

SANTANA, Ricardo Cesar Gonçalves. Ciclo de vida dos dados e o papel da ciência da informação. In: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO. 14., 2013. Florianópolis. [?]. Florianópolis: UFSC, 2013. Disponível em: http://enancib2013.ufsc.br/index.php/enancib2013/%20XIVenancib/paper/viewFile/284/319. Acesso em: 13 mar. 2023.

SILVA, Ana Laura Fonseca. O papel das Soft Skills na implementação efetiva dos programas de compliance com foco na adequação à Lei Geral de Proteção de Dados ? Lei N° 13.709/18. 2022. Monografia (Graduação em Direito) - Universidade Federal de Ouro Preto, Ouro Preto. 2022

SILVA, Eggon João da. A defesa da ética e transparência. In: VENTURA, Luciano Carvalho. Governança corporativa. São Paulo: Saint Paul Editora, 2005, página 259.

TERRA, Priscila de Mello. A influência da governança de dados na gestão estratégica, 2017. Monografia (Bacharelado em Sistema de Informação) - Universidade Federal Fluminense, Niterói, 2017.

VAZAMENTO de dados aumentaram 493% no Brasil, segundo pesquisa do MIT.VEJA, São Paulo, 24 fev. 2021. Sociedade. Disponível em: https://vocesa.abril.com.br/sociedade/vazamentos-de-dados-aumentaram-493-no-brasil-segundo-pesquisa-do-mit. Acesso em: 15 mar. 2023.

VIEIRA, Tatiana Malta. O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante da tecnologia da informação. Porto Alegre: Sergio Antonio Fabris Editor, 2007.

==========

Arquivo 1: TCC - A IMPORTÂNCIA DO COMPLIANCE NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA - WESLEY VICENTE.pdf (8805 termos)
Arquivo 2: https://english.stackexchange.com/questions/314716/is-this-project-aims-to-logically-correct (1909 termos)
Termos comuns: 2
Similaridade: 0,01%
O texto abaixo é o conteúdo do documento TCC - A IMPORTÂNCIA DO COMPLIANCE NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA - WESLEY VICENTE.pdf (8805 termos)
Os termos em vermelho foram encontrados no documento
https://english.stackexchange.com/questions/314716/is-this-project-aims-to-logically-correct (1909 termos)

==========

WESLEY VICENTE DA SILVA

A IMPORTÂNCIA DO COMPLIANCE EMPRESARIAL NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA

SALVADOR
2023

WESLEY VICENTE DA SILVA

A IMPORTÂNCIA DO COMPLIANCE EMPRESARIAL NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA

Artigo apresentado como requisito parcial para obtenção do título de Bacharel em Direito pela Universidade Católica do Salvador.

Orientador: Prof. Darlã Conceição Santos.

SALVADOR
2023

A IMPORTÂNCIA DO COMPLIANCE EMPRESARIAL NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA

Wesley Vicente da Silva1
Darlã Conceição Santos2

RESUMO: No cenário de exploração das informações como mercadoria econômica, os dados pessoais coletados por empresas privadas tornaram-se fator de tutela legislativa. Assim, surgiu a necessidade de organizar os setores privados para adequar aos moldes da Lei Geral de Proteção de Dados Pessoais ? LGPD, com o intuito de proteger a privacidade, como direito autônomo e fundamental para a tutela da pessoa humana, destacando os programas de compliance aliados as boas práticas e governança de dados. Nesse contexto, a fim de consolidar os mecanismos técnicos de segurança para a efetividade da legislação com a finalidade de mitigar os casos de vazamento de dados pessoais, a LGPD implementou medidas administrativas para inibir incidentes decorrentes das condutas infratoras a legislação. Desse modo, este trabalho tem como objetivo demonstrar a importância dos programas de compliance para a proteção aos direitos dos titulares dos dados, visando o cumprimento do ordenamento jurídico. Valendo-se do método hipotético-dedutivo, com abordagem qualitativa, utilizando da revisão bibliográfica de livros, legislação, artigos, dissertações e teses concernente à tutela de dados pessoais no Brasil para o desenvolvimento do presente artigo.

PALAVRAS-CHAVES: Compliance Empresarial. Governança corporativa. LGPD. Vazamento de dados.

ABSTRACT: In the scenario of exploitation of information as an economic commodity, personal data collected by private companies have become a factor of legislative protection. Thus, the need arose to organize the private sectors to conform to the General Law for the Protection of Personal Data - LGPD, in order to protect privacy, as an autonomous and fundamental right for the protection of the human person, highlighting compliance programs allied with good practices and data governance. In this context, in order to consolidate the technical security mechanisms for the effectiveness of the legislation with the purpose of mitigating cases of leakage of personal data, the LGPD implemented administrative measures to inhibit incidents arising from conducts that violate the legislation. Thus, this work aims to demonstrate the importance of compliance programs to protect the rights of data subjects, aiming at compliance with the legal system. Taking advantage of the hypothetical-deductive method, with a qualitative approach, using the bibliographic review of books, legislation, articles, dissertations and theses concerning the protection of personal data in Brazil for the development of this article.

KEYWORDS: Corporate Compliance. Corporate governance. LGPD. Data leak.

1
Discente do curso de Direito da Universidade Católica do Salvador.
2
Mestre em Direito, Docente na Universidade Católica do Salvador.

1 INTRODUÇÃO

A nova moeda de troca não é apenas aquela que podemos ver, quantificar ou converter. Os moldes do mercado financeiro mudaram, sendo em questão material ou ao produto que eles precificam, postulando um novo aparato ao objeto contratual: os dados.
Muito embora, os dados pessoais, ainda para muitos, são apenas informações deslocadas acerca de fatores específicos, atualmente, podem ser conceituados como um conjunto de indicadores, regrados por um complexo condensado de informações em um fluxo crescente tangencial.
Os dados da grande massa acabam gerando indicadores que podem ser balizados e influenciados de acordo com os detentores dessa informação, apenas apartado em blocos de informações não são considerados como vetores orçamentários. Porém, direcionados para uma finalidade ordenada tem o condão de influenciar o interesse social.
Dito isso, os mecanismos postos pelo Reino Unido para possibilitar uma estruturação normativa para organizar e gerir os dados dos indivíduos, foi crucial para a criação em outros

países, como no Brasil, onde instituiu-se a Lei Geral de Proteção de Dados Pessoais (LGPD). Muito embora, a lei brasileira trouxe um arcabouço de normas reguladoras e sanções aos casos de tratamento de dados, que não foram abarcados com o marco da internet, os dados em uma visão macro constitucional já eram de forma genérica tutelados pela Constituição Federal de 1988.
Todavia, apenas a sanção da LGPD não seria, isoladamente, capaz de coibir as violações ao tratamento de dados na esfera privada, mas sim a necessidade de uma regulamentação do ciclo de vida das informações, que além de estipular os dados que podem ser utilizados ou até quando podem ser armazenados, estabelecer expressamente no bojo da norma como deve ser a proteção na operação do tratamento de dados.
De forma efêmera, conclui-se que a legislação pode delimitar os alicerces capazes de ensejar uma fiscalização, sendo estas através de mecanismo de gerenciamento de atividades, políticas de condutas e implementação de governança de dados, pois os dados hackeados ou vazados de forma isoladas, não seria possível identificar dados sensíveis, muitos menos individualizar o sujeito.
Portanto, o gerenciamento dos dados em provedores de armazenamento pode ter os riscos reduzidos de acordo com a realização de medidas de compliance para dirimir os impactos na

atividade empresarial, como também para tutelar os dados, cada vez mais acentuado como um produto orçamentário.

2 COMPLIANCE EMPRESARIAL

A criação do compliance está entrelaçado sob o cenário econômico-social, assim, sua implementação como sistema de organização foi instaurado e aprimorado a partir dos problemas práticos estruturais para gerir uma boa governança, com intuito de assegurar a proteção e o controle que garante a qualidade do negócio.
A utilização do termo foi inicializada no mercado financeiro, especialmente após a criação do Banco Central em 1913 nos Estados Unidos da América, com a necessidade de um sistema econômico ajustável e estável. Só após 1960, com a regularização da Securities and Exchange Commission (SEC), que houve a necessidade de implementação do compliance como um programa para a integração dos procedimento, controle e monitoramento de operação interna. (CARVALHO, 2021)
Em 1977, com a Convenção Relativa à Obrigação de Diligência dos Bancos Suíços, estabeleceu os modelos auto regulatórios, com adequação de condutas e processos internos, na qual a infração tem como consequência à aplicação de sanções. (CARVALHO, 2021)
Só após esse processo de amadurecimento histórico, que o Brasil teve a necessidade de competir em escala global, implementado novos processos de segurança no sistema financeiro brasileiro.
Pode-se concluir que, após a globalização com o fenômeno da criação dos dados estruturais, houve a potencialização das informações adquiridas por meio de provedores, classificadas, atualmente, como fonte econômica de um produto quantificativo e qualitativo, ao qual possibilita uma utilização como um produto do sistema financeiro.

Nesse sentido, em decorrência de ataques cibernéticos em provedores de informações massificadas conduziram a sociedade na aplicação de institutos de melhoramento, como o compliance e suas interfaces para proteger no ambiente corporativo os dados massificados recebidos em seus provedores.

2.1 O CONCEITO DE COMPLIANCE

Antes de enveredar sob o conceito de compliance na esfera privada, é oportuno compreender o seu significado. Nesse contexto, a palavra compliance advém do verbo inglês, to comply, que pode ser definida como conformidade. O instituto deve ser aplicado como plano principal de uma diretriz pré-estabelecida para ser dirigida a todos capazes de enfrentar a finalidade destinada. (BERTOCCELLI, 2019)
Nesse parâmetro, pode ser traduzida como:

Comply, em inglês, significa ?agir em sintonia com as regras?, o que já explica um pouquinho do termo. Compliance, em termos didáticos, significa estar absolutamente em linha com normas, controles internos e externos, além de todas as políticas e diretrizes estabelecidas para o seu negócio. (ENDEAVOR DO BRASIL, 2022, n.p)

O compliance pode-se ser definido de forma técnica como um conjunto de normas padronizadas, sob um viés ético e legal, na qual após estruturação será a matriz orientadora para o comportamento organizacional da instituição ao qual atuará no mercado, como também irá reger as atividades dos colaboradores. Dessa forma, sendo um instrumento hábil a controlar o risco de imagem, a normatização legal, chamados de riscos de compliance, as que recaem nas instituições no decorrer da sua atividade laboral. (CANDELORO, 2012).
Superada a barreira terminológica, a finalidade do compliance tem como escopo o gerenciamento adequado do risco de atividades, verificar adequadamente as normas éticas e legais, e estudar os possíveis danos tangenciais. Dessa forma, esses elementos visam a redução de perdas e danos, como também amplifica a cultura e fortalecimento corporativo nos moldes aos padrões exigidos, seja esse por lei ou na tentativa de dirimir o risco do serviço prestado.
Portanto, segundo a doutrinadora Frazão (2007, p. 42), destina-se em sua obra que o compliance é como:
(...) conjunto de ações a serem adotadas no ambiente corporativo para que se reforce anuência da empresa à legislação vigente, de modo a prevenir a ocorrência de infrações ou, já tendo ocorrido o ilícito, propiciar o imediato retorno ao contexto de normalidade e legalidade.

Nessa mesma linha de pensamento, de acordo com os autores da obra Compliance 360° (2012, n.p), referem-se o compliance a:

Um conjunto de regras, padrões, procedimentos éticos e legais que, uma vez definido e implantado, será a linha mestra que orientará o comportamento da instituição no mercado em que atua, bem como as atitudes de seus funcionários; um instrumento capaz de controlar o risco de imagem e o risco legal, os chamados ?riscos de compliance?, a que se sujeitam as instituições no curso de suas atividades.

Pode-se concluir que o conceito de compliance, em uma esfera macro, é um aglomerado de regras pré-estabelecidas através de um instrumento perpetuado por técnica de desenvolvimento, capaz de dirimir riscos e danos das atividades devolvidas pelo plano diretor.
Muito embora, o instituto "compliance" tem uma definição extensiva e não tem como fim apenas o cumprimento da legislação e de condutas éticas, pode ser compreendida também como um instrumento de diminuição de riscos, desenvolvimento corporativo sustentável e subsequentes segmentos empresariais de negócio. (ROQUE, 2019)
O compliance além de estar associado tradicionalmente a uma perspectiva organizacional aos comandos administrativos, pode ser vinculada também a uma visão de uma sociedade digital 4.0, devendo não só apresentar o compliance empresarial na esfera de redução de risco à imagem, mas sim, em uma abordagem de pré-orientação e implementação de desenvolvimento aos moldes legislativo de proteção aos dados, como objeto principal de estudos.
Portanto, é necessário a elaboração do projeto de compliance em uma visão lógica, a modo de compreender os objetivos e os componentes da aplicação do programa. Posteriormente, superado os obstáculos, aplica-se os estudos de riscos a boa governança corporativa com a implementação de programas de governança de dados objetivando auxiliar o controle de informações em conformidade aos padrões da corporação, e mitigar os danos da empresa.

2.1.1 AS GOVERNANÇAS CORPORATIVAS E A IMPLEMENTAÇÃO DOS PROGRAMAS DE COMPLIANCE

Em linhas gerais, o Instituto Brasileiro de Governança Corporativa ? IBGC (2015, n.p) discrimina o conceito de Governança Corporativa, como: ?Sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas. ?
O sistema da governança corporativa está associado ao desenvolvimento interno de uma empresa, seja ele entre a administração, sócios e funcionários, capaz de criar elos para uma estruturação de direção racional e acima de tudo nos moldes da ética e legislação.
Muito embora, a governança corporativa e o compliance sejam institutos que se assemelham em uma visão macro, os mesmos, diferenciam na aplicação prática, mas se complementam no objetivo final, sendo um instrumento para aplicação do outro.

A prática da governança corporativa, além de estimular o valor empresarial, pode-se concluir que estrutura de forma adequada a medida necessária para organizar a atividade empresarial, assim, não há que se falar em condutas prejudiciais. Por exemplo: empresários compreendem que para realizar uma instrumentalização segura aos seus sócios e administradores tendem a prejudicar o negócio empresarial, assim o autor Eggon João da Silva (2005, p.259) retrata que: ?A governança corporativa assegura tratamento equânime a todos os acionistas, inclusive minoritários, preferencialistas, nacionais e estrangeiros. Todos devem ter oportunidade de reparação caso venham a sofrer violação de seus diretores. ?

Nesse passo, as críticas ao sistema não são viáveis, tendo em vista a utilização de instrumento capaz de integralizar ao plano empresarial. Sendo assim, o programa de compliance visa amplificar a utilização de um sistema para garantir que todos possam participar de forma justa sob o aspecto legal, seja sócio ou administrador.

Em uma tangente geral, a implementação da governança corporativa ressoa em uma perspectiva segura, tanto internamente, seja auxiliando as avaliações das atividades executadas pelos sócios/administradores, quanto externamente, em relação à imagem da empresa, sendo este um fator primordial a empresas estruturadas no mercado.

A implementação da governança corporativa deve ser estruturada de acordo com as necessidades da empresa, devendo verificar o histórico de desenvolvimento do estabelecimento, pois, só a partir do status da empresa pode-se delimitar a estratégia possível para uma implementação segura e adequada. Sendo assim, um regramento mais rigoroso pode gerar consequências negativas e ineficazes, especificamente em estágios primários, pois em atividades inicias, as tomadas de decisões e a execução da atividade empresarial é primordial, sendo necessário, um aspecto negocial informal para realizar os objetivos da empresa, o que não se verifica quando existe prática de boa governança devidamente estruturadas no negócio. (KLEINDIENST, 2019)

Ao desenvolver da atividade da empresa, além da atenção a organização interna, sendo está um fator primordial da governança, ainda que no fim acabe tendo um aspecto externo por vislumbrar no mercado financeiro uma maior complexidade da entidade. O desenvolvimento da empresa, seja no faturamento, importação comercial, quantidade de funcionários, além dos controles a observância da legislação e regras internas, tendem à serem complexos, e, que necessita

de ações maiores que a própria instituição empresarial, restando necessária a implementação de sistema organizacionais aos fluxos de informações. (KLEINDIENST, 2019)

Ultrapassado a esfera conceitual e instrumentalização da política de boas práticas de governança, cabe pontuar que as empresas que possuem fluxos de informações sensíveis, conforme estipula o artigo 50 da Lei Geral de Proteção de Dados Pessoais, os controladores e operadores são responsáveis pelo tratamento de dados, devendo criar planos de adequação a legislação.

Assim, ao confeccionar as regras de boas práticas, os controladores adjuntos com a administração devem estipular através da análise da natureza dos dados coletados, a probabilidade, a finalidade e o potencial de riscos das vantagens advindas dos tratamentos dos dados verificados.

(NASCIMENTO, 2020)
É necessário pontuar que, os agentes de tratamento, após a autenticação da gravidade e sensibilidade dos dados aos riscos de operação, poderão estabelecer programa de governança em privacidade, sendo este, um instrumento amplo com normas de compliance, além dos aspectos operacionais.
Em relação ao programa de governança de privacidade, pode-se estabelecer como um aglomerado de normas-regras de boas práticas de governança, com a finalidade de executar ordens de natureza legal. (NASCIMENTO, 2020)
Portanto, os instrumentos do compliance em conjunto com a boa prática de governança, se consagram na identificação dos riscos e estruturação de medidas para a empresa, sendo respondida de forma adequada e proporcional ao suporte da tomada de decisão.
O Programa de compliance na esfera privada para análise de dados pessoais, com a finalidade de promover a segurança, deve ser constantemente monitorado e atualizado, com a implementação de ?salva vidas? em decorrência de avaliação de riscos à privacidade e o acometimento de vazamentos. (NASCIMENTO, 2020)
Portanto, os instrumentos e objetos referenciados demonstram a determinação de regras de governança no ambiente de operação de tratamento de dados pessoais, a modo que seja realizado uma estruturação nas empresas para que possibilitem a implementação de mecanismos de segurança, com a finalidade de dirimir os riscos da atividade empresarial na sociedade digital.

3 GOVERNANÇA DE DADOS

O mercado digital tem como principal ativo financeiro os dados, este considerado como ?matéria prima? de uma economia baseada no conjunto de informações, sendo que nos últimos anos, houve um aumento exponencial na coleta de dados por cooperativas, startups e novos nichos empresariais, tendo a finalidade de quantificar e gerencias os dados.
Dados, informações, conhecimento e sabedoria são os quatros estágios evolutivos da cadeia de informação, pode-se assim, compreender os dados como fatos ou registros em seu formato primário. (BEAL, 2014). Já a informação é entendida como os conjuntos processados de dados em um contexto aplicado (RÊGO, 2013). Muito embora, na sociedade da informação ?os dados são o novo petróleo?, apenas os dados isoladamente não são capazes de transformar em ativo financeiro, sendo necessário administrá-lo de forma eficaz, para que assim, as empresas adquiram vantagem competitiva.
Dessa forma, a governança de dados tem como principal objetivo atender as necessidades das empresas, ou seja, solucionar problemas, diminuir custos da administração, para que os dados transformem em saldo positivo para os negócios (TERRA, 2017).
O Data Governance Institute -DGI (2017, n.p) definiu governança de dados como ?um sistema de direitos de decisão e responsabilidades para processos relacionados à informação, executado de acordo com modelos acordados que descrevem quem pode realizar quais ações com quais informações e quando. ? Portanto, a utilização da governança de dados orienta quais os

métodos deverão ser aplicados no ciclo de vida dos dados.
Uma das atribuições da governança é o acompanhamento da operação dos dados com a finalidade de gerir que as informações estejam alinhadas com os objetivos pré-determinados na coleta primária, além disso, é necessário assegurar que as informações estejam disponíveis para acesso, quando consultadas, gozar de qualidade, consistência, auditabilidade e segurança dos dados (ESPÍNDOLA, 2018).
No âmago da cadeia evolutiva da informação uma das preocupações dentro das organizações corporativas é o receio com a proteção das informações, ou seja, a capacidade das empresas no protagonismo da segurança com os provedores internos, tendo em vista a necessidade de conformidade com a legislação pátria.
A boa governança tem como objetivo aplicável à prática do controle dos processos de operação dos dados: a prevenção de situações adversas que podem gerar o comprometimento da integralidade dos dados adquiridos pelas organizações empresariais, que por sua vez, devem ter o condão de reforçar a confidencialidade das informações. (ESPÍNDOLA, 2018).
A integração do programa de governança de dados nas corporativas empresariais, tem como o esforço principal a organização de dados, que deve ser observado por um prisma basilar, ou seja, a aplicação dos princípios como limite legal e ético no ciclo de vida dos dados.
Para Rêgo (2013), os princípios são regulamentações para compreender aplicação da governança dos dados como linha direta para os negócios, sendo: (i) A gestão de dados estratégicos, tem o dever de vislumbrar as tomadas decisões por um coeficiente tático e operacional. (ii) A governança como instituição, ou seja, a governança de dados pode ser comparada como sistema governamental, na qual dispõe de legislação, execução e jurisdição; (iii) A governança de dados como um programa, devendo ser implementado como fator permanente, não apenas um projeto temporário. Ainda, pontua-se que os princípios da Governança de dados não são limitados, tendo uma orientação basilar a cada implementação de um sistema organizacional que deve ser observado pelo prisma ético e legal.
Assim, os princípios devem incumbir os papéis que a serem preenchidos pela gestão moldar os comportamentos das empresas para a aquisição, reserva e utilização dos dados conforme as normas e políticas da corporação (TERRA, 2017).
Coleta, armazenamento, recuperação e descartes, são as quatro etapas do ciclo de vida dos dados (SANTANA, 2013), ou seja, para a aquisição de dados pelas empresas, deverão observar a vida útil do dado para não incorrer na (in) responsabilidade da utilização indevida de informações dos seus provedores.
As fases do ciclo de vida dos dados devem ser observadas pela ótica de seis objetivos, sendo eles: a qualidade, a privacidade, os direitos autorais, a integração, compartilhamento e preservação dos dados (ESPÍNDOLA, 2018). Muito embora, a lei geral de proteção de dados implementou e traçou novos objetivos para a coleta de dados pessoais, cabe destacar que os objetivos vislumbrados na Governança de dados têm como parâmetro preliminar a tomada de decisão, na qual deve ser os negócios pautados nos moldes legais e éticos vigentes.
Nesse contexto, o controle de informações é necessário, tendo em vista que na sociedade

da informação, cada vez mais o volume de dados é crescente, acarretando mais vazão e protesto por políticas públicas para a preservação dos institutos, órgãos e empresas que detenham a

informação, sendo assim, necessário sistema de organização, softwares e hardwares capazes de processar as informações, criptografar e armazenar. (MARTIGNAGO, 2019)

Assim, para otimizar o ciclo de vida dos dados e garantir que os objetivos sejam preenchidos na estruturação do gerenciamento de dados, faz-se necessário a implementação de frameworks com o intuito de garantir que o procedimento seja cumprido com maior qualidade de informação e aproveitamento financeiro para a empresa, auxiliando a tomada de decisão para redução de risco para utilização de dados. (MARTIGNAGO, 2019)

Um Framework, segundo Johnson (1991), pode ser definida como um aglomerado de objetos que colabora entre si para que atinja um conjunto de obrigações para aplicação de um domínio especifico. Já para Pinto (2000), um framework é conceituado como um software incompleto criado para ser um objeto cujo estado e comportamento são definidos pela classe. Assim, o framework é uma concepção de uma arquitetura para um edifício de subsistemas e oferece o alicerce básico para criá-los.

Muito embora, os autores defendem uma conceituação distintas acerca da concepção de frameworks, pode-se verificar que ambas se complementam, tendo em vista que o framework é um sistema pré moldado, ou seja, é um programa com intuito de ser complementado através da finalidade a ser cumprida pela gestão empresarial, sendo instanciado por classes para categorizar os dados e ser alojado em hotspot, provedores físicos, capazes de armazenar as informações coletadas pelas empresas.

Portanto, para gerenciar os ativos de dados de forma complexa, ordenada e objetiva é necessário para proteção do procedimento do ciclo de vida dos dados, determinar os modelos de frameworks para o gerenciamento dos dados. Assim, para Carvalho (2021), podem ser apresentados três domínios CobiT, DAMA DMBOK e DGI Framework, sendo apenas dois destes observados para fomento deste artigo: (i) A DAMA (DAMA DMBOK), e (ii) CobiT.

A DAMA (Data Management Association) é uma associação sem fins lucrativos, com o intuito de promover boas práticas de gestão de dados, e em 2009 fundou o DAMA-DMBoK (Data Management Body of Knowledge), sendo um corpo de conhecimento que tem como ponto fundamental esclarecer como as corporativas devem aplicar a operação otimizada dos dados. (CARVALHO, 2021)

Em sua versão 2.0, acrescenta não só uma visão macro do gerenciamento de dados, definindo padrões, terminologias e práticas, mas a integração de dados, para definir táticas,

armazenamentos e sistemas, bem como implementação da ética na operação do tratamento de dados, a definição de big data e ciência de dados e amadurecimento das informações. (LIMA, 2019).

O DAMA-DMBOK V2 é formado por 11 (onze) funções de gestão de organização de dados, sendo incorporado como cerne principal: a governança de dados, tendo em vista que os dados percorrem por toda sistemática das onzes funções ordenadas, assim segundo Honório (2021):
A primeira função é a governa de dados, sendo o pilar do framework, tem o condão de orientar e supervisionar a operação do ciclo de vida dos dados, na qual deve estabelecer um sistema de apoio a decisão dos gestores sobre os dados, sob o prisma do negócio.
A arquitetura de dados, a segunda função, pode ser conceituada como um planejamento para administrar os dados, aquisição de ativos da empresa, com o intuito de definir a finalidade das informações adquiridas com os requisitos necessário para o gerenciamento dos dados.
Por sua vez, a modelagem de dados e design, tem a função de demonstrar de forma nítida os dados, sendo o processo da descoberta, análise e representação da etapa primária da informação.
O armazenamento, uma das etapas da operação do ciclo de vida dos dados, na qual vai incluir o design, o suporte dos dados armazenados para quantificar o coeficiente valorativo das informações, até o seu descarte, devendo respeitar todo o procedimento de segurança legal vigente.
Um dos alicerces para o gerenciamento de informação é a segurança, que deve garantir a proteção dos dados, a execução de políticas e procedimento de segurança, no intuito de moderar o acesso de forma consciente e controlado, não devendo ser infringido ou acessado de forma inadequada, afim de garantir autenticação e auditoria de dados informações.
A Integração e Interoperabilidade de dados, é a função responsável pela movimentação e a concretização dos dados na interligação do armazenamento e outras plataformas.
O gerenciamento de documentos, pode ser compreendida como o gerenciamento e inclusão da vida útil dos dados e informações, encontrados em programas não estruturados, em ênfase ao conteúdo de apoio de conformidade a legislação vigente e os termos éticos formalizados para o negócio.
Dados mestre e de referência, tem como condão a manutenção dos dados compartilhados para coexistir a integralidade dos sistemas internos de gerenciamento dos dados.
Em razão da interligação entre uma linha direta com os negócios, uma das funções do DAMA-DMBOK é a Data warehousing e Business intelligence, ou seja, a implementação de

planner para o contoler da administração dos dados e suporte a decisão com o intuito de conceder aos gestores de informação emitam relatórios de equalização de valores.
Segundo Barata (2015), os metadados, na qual consiste a décima função, é promover a facilitação do acesso dos dados interligados nas multifontes do sistema integrado, como também garantir a qualidade de dados.
Por fim, o gerenciamento de qualidade de dados é a implicação das técnicas para garantir a possibilidade de aferição, melhoramento e adequação da utilidade dos dados, com o intuito de monitorar a integridade da informação primária no ciclo de vida dos dados.
Já o COBIT (Control Objectives for Information and related Technology), é um framework de suporte fundado em 1994 administrado pela ISACA (Information Systems Audit and Control Association), estruturado como um arcabouço de informação direcionadas para governança de dados e gerenciamento de informação, tem como objetivo auxiliar os profissionais de gestão na

conexão entre os problemas técnicos e os riscos do negócio. (BARATA, 2015).
Para Lima (2019), o COBIT é um framework que possui duas vertentes basilares: a gestão, que possui quatro áreas de domínios: planejamento, constituição, execução e monitoramento, e a governança que é a tomada de decisão de acordo com a gestão de dados, possuindo 37 (trinte e sete) processos integrados.
Na versão 5.0, o sistema é utilizado baseado em 05 princípio, conforme elucida Casaes (2019), Barata (2015) e Lima (2019), sendo: (i) atender às necessidades das partes interessadas; (ii) cobrir o negócio como um todo; (iii) aplicar um framework único e integrado; (iv) habilitar uma visão holística; e (v) distinção entre governança de gestão.
Um dos princípios é atender às necessidades das partes interessadas, sendo a necessidade das corporativas é satisfazer as expectativas dos seus stakeholders, proporcionando um equilíbrio na tripartite: benefícios, redução do risco e recurso disponíveis.
O segundo princípio é baseado na cobertura do negócio como um todo, ou seja, abranger a integralidade da empresa no processo, procedimento, pessoas e as relações com os habilitadores.
A aplicação do framework único e integrado, assim, o COBIT é capaz de promover uma relação completa com a Governança de dados, corroborando ao alinhamento com padrões externos e adaptabilidade dos modelos usuais de negócios.

O COBIT permite habilitar uma visão holística, ou seja, uma visão macro dos componentes que oferecem suporte para atingir as finalidades da governança de dados, na qual define como catalogadores: as políticas, processos, estruturas organizacionais, informação e ética.
Por derradeiro, o princípio da distinção entre governança de gestão, tendo em vista que ambos possuem estruturas organizacionais distintas, assim, governança tem como esforço principal que os objetivos corporativos sejam cumpridos, estabelecendo prioridades pela tomada de decisão, compliance e progresso das organizações. Por sua vez, a gestão é o planejamento, construção, execução e monitoramento das funções ornamentada com o direcionamento da governança.
Desse modo, com escalonamento dos cinco princípios é capaz de proporcionar o funcionamento otimizado do framework, destacando os seguintes processos:
O APO01: Gerenciar o framework de TI, tem como condição a otimização das atividades relacionadas ao TI, com a função principal de incluir os procedimentos e regulamentos para promover a integralidade das informações nos bancos de dados. (BARATA, 2015)
Já o APO03: Gerenciar a arquitetura corporativa, tem função primordial agrupar as informações para auxiliar as atividades e tomadas de decisões, conceituando e compartilhando as informações dos elementos dos dados, e por fim catalogar a empresa, com base na modulação e sensibilidade dos dados. (BARATA, 2015)
Nesse ínterim, a governança de dados como um sistema integrado com o programa de compliance, tem o condão de otimizar a operação de controle interno relacionado aos dados coletados pelas empresas, capaz de gerenciar as bases para o apoio de decisão ao tratamento das informações, com segurança e qualidade, garantido o ciclo da vida útil dos dados.

4 A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

As estruturas políticas, econômicas e sociais com desenvolvimento de novas tecnologias e mecanismo para a coleta de dados e informações, fez necessário modulações legislativas para a proteção da privacidade, além dos aspectos físicos, patrimoniais e morais.
A proteção à privacidade de dados foi dividida em quatros gerações: a primeira, oriunda do estado moderno, com o advento dos bancos de dados; a segunda, datada em 1980, com a expansão legislativa para a proteção à privacidade aos setores privados; a terceira geração em 1990, com o processo de tratamento de dados e o consentimento dos cidadãos; Por fim, a última dimensão, é

destinada ao protagonismo da permissão para coleta e uso dos dados pessoais, quando a lei estabeleceu a importância da titularidade das informações. (MENDES, 2014)
Nesse aspecto, é perceptível a evolução do direito aos fatores reais da sociedade e as transformações dos meios tecnológico, computacionais, genéticos e comunicativos, que por sua vez possibilitou a integração da comunicação global, e consequentemente, o rastreio dos dados através do armazenamento de informação. (SAAD, 2021).
Os legisladores ao considerar os dados pessoais como extensão ao direito à privacidade, preocuparam em tutelar constitucionalmente a proteção da população, em especial os países europeus, como: Espanha, Portugal, Hungria, Eslovênia e Rússia. (VIEIRA, 2007) Porém, só tornou-se fator primordial após o regulamento geral do Parlamento Europeu sobre a proteção de dados, n.º 2016/679, sendo necessário a adequação das empresas prestadoras de serviço na Europa ao regulamento, influenciado diretamente o Brasil para elaboração da Lei Geral de Proteção de Dados brasileira. (SAAD, 2021).
Muito embora, a Lei Geral de Proteção de Dados Pessoais - LGPD, em sua promulgação, não abarcou de forma expressa a proteção de dados como direito fundamental, a doutrina, em especial Nascimento (2020), por sua vez, já argumentava a proteção de dados e informações pessoais como direito autônomo, derivado do direito fundamental à privacidade, explicitamente no artigo 5°, X, da CRFB de 1988.
Após reiterados julgamento sobre a tutela dos dados pessoais como extensão da personalidade do indivíduo, o Supremo Tribunal Federal -STF reconheceu no Julgamento da Ação Direta de Inconstitucionalidade - ADI 6387, a existência dos dados como direito autônomo, derivada do direito fundamental a dignidade da pessoa humana, na proteção à intimidade e a centralidade do Habeas Data como autodeterminação informativa. (NASCIMENTO, 2020).
Ao compreender a necessidade da proteção aos dados pessoais, os legisladores brasileiros em votação de ? das casas legislativas (câmara e Senado Federal) em dois turnos, aprovaram a Emenda Constitucional 115 de fevereiro de 2022, alterando o artigo 5° da Constituição Federal de 1988, incluindo o inciso LXXIX, tutelando constitucionalmente a proteção aos dados pessoais, inclusive nos meios digitais.
Ressalta-se, ainda, que os dados pessoais estão interligados com o direto fundamental à privacidade, na qual representa a capacidade de a pessoa administrar sua vida, seus pertences e

propriedades materiais e imateriais, permitindo ou não a utilização dos seus dados (bens imateriais) por terceiro. (NASCIMENTO, 2020).

A privacidade, por sua vez, segundo Mendes (2008), é o direito à proteção aos comportamentos pessoais e acontecimentos de caráter íntimo, bem como as informações prestadas aos profissionais e comerciantes, em que a pessoa não deseja que se compartilhe com o público.

Para o professor William Prosser, pode-se qualificar a lesão a privacidade em quatro graus: i) o intrometimento na reclusão ou solidão na vida privada, ii) a divulgação pública de fatos privados constrangedores sobre o indivíduo; iii) a publicidade sobre o indivíduo apresentada de forma equivocada; e iv) a apropriação, para obtenção de vantagem, do nome ou da imagem do demandante (PROSSER, 1960).

A doutrina, por sua vez, defende mais uma violação à privacidade: a privacidade informacional, interligada com os fatores tecnológicos de informação. (SAAD, 2021). Assim, quando a lei ao realizar o tratamento da privacidade, refere-se como um direito líquido, ao qual será tutelado para garantir que o indivíduo tenha um local reservado, que não tenha, se desejar, a interferência de outros sujeitos, seja pessoa física ou jurídica.

Com a proteção dos dados pessoais dos titulares, através da LGPD, possibilitou ao cidadão o acesso a informações ao ciclo de vida útil dos dados pelas empresas, e a certeza de fiscalização pela Autoridade Nacional de Proteção de Dados, com a finalidade de atingir os objetivos traçados pela legislação, na qual a lei traz conceitos e delimita princípios, que devem ser mencionados.

A LGPD tem como objetivo principal: ?o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado?, com a destinação de assegurar os direitos fundamentais a liberdade e privacidade dos titulares dos dados, bem como tutelar a dignidade e a personalidade da pessoa natural. (LGPD).

A legislação está ordenada diretamente com o meio empresarial, sobretudo no que se refere aplicação aos seus destinatários que são pessoas físicas ou jurídicas que realizam a coleta e tratamento de dados no Brasil, conforme preceitua o artigo 1° da lei 13.709, de 14 de agosto de 2018.

Para compreender a LGPD, faz-se necessário elucidar os conceitos de dados pessoais: (art. 5º, I) é toda informação relacionada a pessoa natural, identificada ou identificável, sendo o dado aplicado no contexto que possibilite o reconhecimento do indivíduo. Bem como refere-se aos dados sensíveis (art. 5º, II), são todas as informações que se relaciona com pensamentos políticos, crenças, identidade biológica e física. Portanto, a legislação tem como ponto a proteção e o cuidado para a não violação dos dados pessoais e sensíveis.

Os doutrinadores, Laura Schertel e Danilo Doneda, ainda aponta cinco pilares para compreender a LGPD, sendo: i) a unidade e generalidade da aplicação da Lei; ii) a legitimação para o tratamento de dados (hipóteses autorizativas); iii) os princípios e direitos do titular; iv) as obrigações dos agentes de tratamento de dados e v) a responsabilização dos agentes.

O primeiro pilar é considerado com aplicabilidade material da legislação, ou seja, aplica-se

a qualquer operação realizada por pessoa natural ou jurídica de direito público ou privado, independentemente do meio, da sua sede ou do país onde estejam localizados os dados (Art. 3°). Considerado, assim, como uma aplicação uniforme para todos os setores público ou privados que realizam tratamento de dados.

O segundo pilar é a legitimação para o tratamento de dados, tendo em vista que a lei especificou critérios e requisitos para o reconhecimento da legitimidade, não podendo ser tratados os dados, sem que exista uma base normativa que autorize, prevista no artigo 7°, 11° ou 23° da LGPD, abordando 11 (onze) hipóteses, incluído o consentimento ou a previsão legislativa.

Destaca-se que a autorização por consentimento para ser considerado válido, deve observar os requisitos previsto no artigo 5°, XII, sendo considerado que a vontade deve ser livre, informada, inequívoca e com a finalidade determinada, consagrando os princípios norteadores da legislação.

O terceiro pilar é o conjunto de princípios e direitos que assegura o destinatário da lei a controlar a utilização do seu dado pessoal, sendo importante elencar dez princípios que estruturam a LGPD: a finalidade, a adequação, a necessidade, o livre acesso, a qualidade dos dados, a transparência, a segurança, a prevenção, a não discriminação e a responsabilização. (MENDES, DONEDA, 2018)

No que concerne, aos direitos dos titulares são expressos no artigo 18° da referida lei, que permite o titular dos dados adquirir através do controler, independentemente do momento, as informações relacionadas ao indivíduo, prevendo: acesso, confirmação, correção, anonimização, bloqueou ou eliminação e a portabilidade.

Para adentrar no cerne dos problemas enfrentados pela legislação, em especial, sobre o vazamento de dados, os dois últimos pilares serão abordados sob a perspectiva da violação e responsabilização acerca da proteção de dados nos casos incidentes de vazamento.

Assim, o quarto pilar, destina-se às obrigações dos agentes de tratamento dos dados, na qual estabeleceu limites que devem ser observados nas operações realizadas para reforçar a segurança e prevenir os problemas da atividade no tratamento de dados.

Uma das obrigações fundamentais, consiste na intitulação do encarregado pelo tratamento dos dados indicados pelo controlador, conforme artigo 41 da LGPD, que possui a função de aceitar as reclamações e comunicações dos sujeitos dos dados, receber informações da Autoridade Nacional, como deve orientar os funcionários a respeito das práticas a serem adotadas em relação à proteção de dados pessoais.

Assim, as informações devem ser fornecidas ao proprietário dos dados, quando os dados forem coletados, como: os meios de segurança aderidos ao tratamento de dados, quais são os riscos da atividade que podem gerar lesão ao titular, pois pode gerar a mitigação dos prejuízos. (SAAD, 2021)

A lei Geral de Proteção de Dados Pessoais tem como objetivo a proteção do dados pessoais dos titulares dos dados, sendo assim, uma das obrigações principais é adoção de medidas de segurança, técnicas e administrativas hábeis a proteger os dados pessoais de acessos não autorizados, como promover a integralidade dos dados, não permitindo, assim, a alteração das informações, a prevenção de situações ilícitas ou acidentais, ou qualquer forma de tratamento

inadequado, consoante se desprende do artigo 46 da lei.
Tornou-se corriqueiro manchetes acerca do vazamento de dados por corporativas, uma das violações mais graves incidentes abarcados pela LGPD, o que ocasiona a vulnerabilidade do titular dos dados, e dos sistemas internos que são responsáveis pelo ciclo de vida útil dos dados. (SAAD,2021)
A seção de segurança de informação tem como condão as obrigações inerentes aos agentes de tratamento, devendo ser adotado pela integralidade das pessoas que realizam o tratamento de dados, garantido que os dados sejam confidenciais, bem como disponíveis nas operações de tratamento. (Art.48). Nos casos incidentais de vazamento de dados, insurge a necessidade ao controlador de informar a autoridade de proteção de dados, que podem definir as medidas para mitigação dos danos.
No entanto, com a utilização da internet, compras online, transferência virtuais e outros meios tecnológicos, criou-se uma dificuldade para atuar na segurança de dados, tendo em vista a abrangência e os domínios de redes globais, que combinados com fatores não perceptível, forma

um perfil não rastreavel capaz de ocasionar violação às diretrizes básicas da legislação, que mesmo com ações posteriores não conseguem excluir os inúmeros registros de pessoas e organizações que coletaram os dados, lesionando a confidencialidade das informações (SAAD, 2021)
Destaca-se que as obrigações aos controladores e operadores, devem ser observados desde a coleta dos dados até seu descarte, assim o artigo 46 da LGPD, introduziu o conceito de privacy by design, sendo a incorporação pelas empresas nos serviços e produtos, na qual dispõe a proteção da privacidade no centro de todo o desenvolvimento corporativo.
Embora, a legislação tenta dirimir os riscos da atividade, os prejuízos causados pelo vazamento de informações são altos, e perpassam pela inadequação do sistema de proteção, perda de credibilidade e de clientes, ocasionado uma ruptura na imagem da empresa, impossibilitando, muitas vezes de concorrer no mercado corporativo. (SAAD,2021)
Portanto, a LGPD concebeu obrigações aos agentes de tratamento de dados, para que se delimite a finalidade da utilização dos dados desde o início da concepção, devendo o controlador confeccionar relatório de impacto a privacidade, utilizando de métodos para a captação da operação do ciclo de vida dos dados, observando as mediadas adotada para aumentar a segurança e mitigar o risco do tratamento das informações, conforme artigo 3 da LGPD.
O último pilar, considerado como a responsabilidade dos agentes na incidência de ocorrência de danos derivados do tratamento de dados. A LGPD consagrou a natureza do tratamento, limitando os parâmetros ao artigo 7° da lei, nas 10 hipóteses dos incisos, vinculados a finalidade da captação dos dados, consoante prevê o artigo 6°, inciso I, II, da LGPD.
A legislação tem como regra o descarte (eliminação) dos dados ao fim do tratamento da operação (art. 16), com o intuito de mitigar os riscos presente no tratamento de dados, principalmente, no que concerne à limitação das hipóteses de tratamentos para não lesionar os direitos dos titulares.
Nos casos, em que mesmo após o término de vida útil dos dados, as empresas podem, quando permitido, armazenar dados que em situação incidentais serem objetos de violação,

principalmente nos casos de vazamento, que podem ocorrer, quando não autorizados pelo titular ou controladores, serem acessados, captados, compartilhados pela internet, para outros sujeitos ou empresas.
Assim, a Lei Geral de Proteção de dados Pessoais, em especial em seu artigo 42, dispõe que o controlador ou operador, quando realizar o exercício do tratamento de dados pessoais, vem

a ocasionar dano patrimonial, moral, individual ou coletivo em detrimento a aplicação da legislação, é obrigado a repará-lo, definindo a responsabilidade de forma objetiva.
Embora, a responsabilização objetiva não é necessária a demonstração de culpa do controlador ou operador. Faz mister esclarecer que o operador, só será responsabilizado quando os atos praticados forem contrário à legislação, ou às instruções que foram fornecidas pelo controlador. (MENDES, DONEDA, 2018)
Ainda, a legislação prevê exceções a responsabilidade objetiva (art. 43), sendo: quando o agente demonstrar que não realizou o tratamento de dados pessoais que foi atribuído, ou quando não houve violação da segurança ou a legislação, e por fim, quando for por culpa exclusiva do titular ou de terceiros.
Porém, o cenário que é vislumbrado no Brasil nos casos de vazamento de dados, é que as violações pelas instituições vêm ocorrendo, majoritariamente, sob ataques deliberados de hacker, ou falha de segurança dos controladores dos dados. (SAAD, 2021)
Dessa forma, é necessário adotar medidas para dirimir os riscos da atividade, e possibilitar o discernimento das informações acerca dos perigos de vazamento de dados, tendo em vista que a tendência é aumento significativo das violações vinculados com a crescente tecnológica. Assim, as empresas devem implementar mecanismos para a segurança das informações.

5 O COMPLIANCE EMPRESARIAL COMO INSTRUMENTO DE PROTEÇÃO DE DADOS NA ESFERA EMPRESARIAL

Em decorrência das constantes violações aos dados armazenados em provedores privados, a tutela ao direito à privacidade nos meios tecnológicos, já era pauta de debate na legislação brasileira, e já existiam mecanismos para a proteção, como: a proibição de direcionamento dos provedores em relação ao compartilhamento de dados, bem como a inibição ao monitoramento nos navegadores de internet.
Vinte e seis bilhões de dados foram vazados no Brasil em 2019, de acordo com pesquisas realizadas pelo Massachusetts Institute of Tecnology ? MIT, possibilitando a utilização de números telefônicos, score de crédito, endereço eletrônico, fotos, números de identificações e outros dados pessoais, para o cometimento de crimes cibernéticos, e a violação aos direitos dos titulares.
A utilização e uso dos dados pessoais por pessoa física ou jurídica, com sede no Brasil ou não, devem se atentar as normas gerais de proteção aos dados brasileiro, segundo Frazão, Oliva e

Abilio (2020), é a necessidade de conferir a efetividade aos direitos e prevenir a violação aos dados, através da implementação de mecanismo de compliance, como uma ferramenta capaz de promover a adequação das atividades aportadas pelas empresas.
Assim, os controladores e operadores poderão formular regras de boas práticas e governança (Art. 50), que contenha as disposições de organização interna, o regime de funcionamento, as operações, o canal de comunicação entre os encarregados e os titulares dos dados, e o procedimento de segurança.
Nessa perspectiva, considerando que a maioria das tratativas de dados perpassam por meios digitais, deve-se adotar sistema para mapear os riscos, e implementar mecanismos para minorar as vulnerabilidades apontadas pelos programas, através da alta administração, do código de ética, para proteger os dados pessoais dos titulares. (PESSOA, 2021)
Existem inúmeras formas de ocorrer o vazamento de dados, sendo através de ataques cibernéticos, sequestro de conta, furtos de dados, compartilhamento de dados por agentes ou ex-agentes da empresa, erro ou negligência, entre outros, que podem ser para adquirir dados de nomes, CPF, celulares, endereços, dados financeiros, senhas, registro de saúde ou credenciais de acesso. (SAAD, 2021)
Desse modo, para realizar o mapeamento dos problemas que as corporativas podem enfrentar, é necessário identificar os fluxos e processos de informação que percorrem os sistemas, que irão auxiliar na tomada de decisão pelas empresas. (NASCIMENTO, 2020)
A alta administração deverá colaborar ativamente no programa de compliance, seja monitorando as investigações e intervenções em situação para estabelecer controles internos em conformidade com a legislação, bem como possibilitar a interdependência dos setores para realizar as atividades designadas para o tratamento de dados (PESSOA, 2021).
Com a elaboração do código de ética pela organização possibilitará o treinamento regular das equipes, responsáveis pela tecnologia da informação, para enraizar a cultura corporativa da boa governança, com a finalidade de assegurar o respeito ao programa de compliance (NASCIMENTO, 2020)
Nesse contexto, para manter uma boa relação com seus clientes, as organizações devem instalar canais de comunicação, para que os titulares dos dados possam contatar os encarregados responsáveis pelos armazenamentos dos seus dados, e exerçam seus direitos sobre as informações contidas nos provedores. (PESSOA, 2021).

Desse modo, quando se trata de concretização a alteração cultural coportariva é preciso realizar o alinhamento dos funcionários com o código de ética, com política de privacidade, para fins de efetividade do programa de compliance de dados. (PESSOA, 2021).

5.1 A IMPLEMENTAÇÃO DE MECANISMOS DE GOVERNANÇA DE DADOS PESSOAIS

Para a efetividade da legislação em relação ao tratamento de dados, a LGPD direciona um capítulo para implementar o programa de governança em privacidade, com a finalidade das

empresas adotarem medidas técnicas, para fins de proteção e segurança dos dados pessoais. (PESSOA, 2021)
A governança em privacidade, pode ser conceituada como um conjunto de regras e práticas positivas a serem implementadas pelos agentes de tratamento, e encontra-se em conformidade com as políticas de compliance empresarial, com o objetivo de gerir os dados das empresas para estabelecer um diferencial competitivo aos negócios. (KOEPSEL,2020)
O programa integra o aperfeiçoamento do procedimento de utilização dos dados, com os requisitos pré-estabelecidos na implementação dos softwares, com a finalidade de gerir de forma otimizada os dados para preencher as diretrizes da legislação. (SAAD, 2021)
A Lei Geral de Proteção de Dados Pessoais dispôs que os controladores e operadores poderão adotar programas de governança em privacidade, que devem ser implementados com o mínimo, (art. 50, § 2°, I): a) o comprometimento dos agentes de tratamento com as políticas internas que devem garantir o cumprimento das normas e regras de boas práticas; b) que aplicação seja de forma uniforme para todo a operação de tratamento de dados; c) que a governança seja adaptativa as estruturas da empresas, sendo compatível com a densidade dos dados e operação; d) como implementar políticas de salvaguardas em relação aos titulares dos dados; e) tenha como objetivo estabelecer uma relação de confiança com sujeitos dos dados, estabelecendo situações de transparência e que possibilite a atuação do titular; g) que conte com planos de respostas a incidentes e remediações; h) seja continuamente atualizado sua base.
Nesse aspecto, devem ser adotadas medidas administrativas para que as instituições, em conformidade com a legislação, apliquem estímulos para assegurar as informações armazenadas pelas empresas, com a adoção de orientações internas que respeitem as diretrizes que inclua o uso

minimizado ou a anonimização das informações, desde a coleta dos dados, conforme artigo 46 da LGPD.
Com o mapeamento das atividades, é importante verificar: O que são esses dados?; de que forma foram coletados ?; quem são os coletores ?; existe relação entre os dados e atividade realizada ?; O que pode ocorrer com esses dados ao serem coletados? E, como são descartados da gestão organizacional da empresa? (NASCIMENTO, 2020). Dessa forma, para adotar medidas compatíveis com os riscos alertados pelos sistemas para a proteção de dados nas organizações privadas, é necessário possuir conhecimento do caminho realizado inerentes ao ciclo de vida útil dos dados.
Embora, a legislação já estabeleça diretriz mínima para o tratamento de informação, a Autoridade Nacional de Proteção de Dados - ANPD, poderá, ainda, determinar padrões técnicos para serem implementados pelo programa de governança em privacidade, devendo ser observado a qualidade de dados, as especificações do tratamento e status tecnológico, em especial a proteção aos dados sensíveis disposto na legislação. (NASCIMENTO, 2020)
Muito embora, a lei geral de proteção de dados, apenas delimita as características e os requisitos mínimos que os operadores deverão tomar para desenvolver um compliance na organização das empresas privadas em consonância com a legislação, porém não impõe um modelo específico para integração de um programa nas corporativas. (PESSOA, 2021)

Assim, para Saad (2021), as medidas técnicas que podem ser adotadas pelos agentes de tratamento de dados, são: i) o uso de firewalls, sendo um mecanismo de segurança que coleta os dados em conformidade com as regras pré estabelecido para análise de tráfego de rede, delimitando as operações de compartilhamento e captação de informações a serem cumpridas; ii) a utilização de antimalware, que consiste na proteção contra vírus que é capaz de fragilizar o sistema, apagar dados e infectar outros arquivos; iii) a utilização de criptografia dos dados, que possibilite quando ocorrer situações incidentais a não identificação do titular do direito.
Já para Fernandes e Abreu, (2014) defendem a implementação de frameworks como a DAMABOK e COBIT, para o gerenciamento de dados, pois tem como meta principal a delimitação do escopo das atividades, as funções envolvidas no tratamento e as interações a serem executadas pelo software, com a finalidade de proteger a privacidade em ambientes corporativos que gerenciam o armazenamento de informações aplicados na prevenção à fraude.

Segundo Carvalho (2021), a integração do software, através das boas práticas estabelecidas pela legislação, poderá aprimorar os aspectos de proteção à privacidade e prevenção a fraude do tratamento de coleta de dados. Tendo em vista, que os frameworks, podem balizar as métricas de qualidade dos dados que indicam uma utilização adequada e otimizada, e aponta a melhor proteção da privacidade.
Com a melhoria de processo de governança para o tratamento de dados, estabelece uma divisão entres as operações que possibilita uma automatização do ciclo de vida dos dados (coleta, utilização, armazenamento e exclusão), capaz de gerar relatório de risco, para o auxílio da tomada de decisão com o intuito de gerir de forma adequada o tratamento de dados. (CARVALHO, 2021)
Neste parâmetro, os programas de compliance com a implementação de frameworks, podem responder questionamento acerca do procedimento de tratamento de informação, dispondo de quais práticas relacionadas à governança, privacidade e segurança de dados, apresentam melhor benefício para o tratamento de dados pessoais. (CARVALHO, 2021)
Ademais, os controladores e operadores deverão adotar medidas, como o Relatório de Impacto ? DPIA), que corresponde a avaliação dos riscos e impactos relacionados com o tratamento de dados pessoais, além da anonimização, da transparência e do sigilo, deverão delimitar prazos para retenção de dados e aderir políticas seguras de informação acerca da operação de tratamento. (SILVA, 2022)
Após realizar a implementação e observância das estruturas mínimas estabelecidas pela LGPD, é necessário adotar um programa de gerenciamento de vulnerabilidades, com atualizações constantes e autocorreções alinhados com as boas práticas de atividades cotidianas, com a finalidade de proteger os dados pessoais, e promover um ambiente corporativo adequado para realizar o tratamento de dados. (SAAD, 2021)
No entanto, ao verificar que houve vazamento de dados, seja pelo recebimento de notificação ou pela veiculação na mídia, os agentes de tratamentos deverão identificar quais dados vazaram e realizar o procedimento estabelecido no programa de compliance de segurança, além de notificar as instituições. (Art. 48, caput).
De acordo com MIT, o prazo entre a comunicação à autoridade competente e a ocorrência

do fato ilícito ultrapassa 200 (duzentos) dias em média, sendo umas das preocupações para a efetividade da legislação, e a redução dos danos causados aos titulares dos bens imateriais.

A Lei Geral de Proteção de Dados, dispõe que nas situações que ocorrer a probabilidade de riscos ou violação aos direitos dos titulares, tem como obrigação do encarregado a comunicação à autoridade nacional e ao titular do dado (art. 48, caput). Sendo que o contato deve ser em período razoável (art. 48, § 1º), contendo a natureza dos dados dos titulares atingindo (art. 48, § 1º, I).
Em decorrência dos possíveis incidentes, a LGPD determinou critério para aplicação de sanções, em casos de vazamento de dados, observando as situações específicas de cada caso, disposto no art. 52, § 1º. Assim, deve ser considerada a avaliação da gravidade, a natureza das informações e do dano ocorrido (incisos I e VI), sendo necessário para este caso, tendo em vista que o compartilhamento indesejado de dados sensíveis pode ocasionar danos irremediáveis para os titulares.
Portanto, existe a necessidade da adesão aos mecanismos e técnicas para promover a efetividade dos programas internos com a finalidade de mitigar os danos, assim, a implementação de boas práticas e governança têm como fator o cumprimento da legislação, por meio de medidas de segurança. Entende-se, que a proteção integral contra falhas que possibilitam a ocorrência de ilícitos não é possível, porém essas diretrizes reduzem as possibilidades de existir desvios de condutas e criar salvaguardas para identificação dos incidentes, de forma eficaz, rápida e adequada.

6 CONSIDERAÇÕES FINAIS

A partir da permissão ao acesso dos dados pessoais, as informações coletadas passaram a integralizar as redes de tratamento de dados, tornando-se alvo de ataques cibernéticos, contribuindo para o aumento da intercorrência no ambiente corporativo, tornando-se o gerenciamento de informação um dos diferenciais no desenvolvimento do negócio.
Nesse contexto, foi imperativo o surgimento de leis que protejam os dados dos cidadãos, e que limitem a gestão das entidades públicas e privadas em relação as informações coletadas, transformando o sistema organizacionais, como compliance, em ferramentas de efetivação das normas éticas e legais. Assim, a implementação do programa alinhado com a governança corporativa é capaz de integralizar o corpo de normas internas com o intuito de adequar a legislação brasileira e criar uma cultura corporativa.
Dentro do programa de compliance, a administração em conjunto com a gestão da empresa, poderá implementar ao plano diretor, a utilização de software, sendo este capaz de possibilitar a automatização do ciclo de vida útil dos dados para realizar o auxílio da tomada de decisão, com o intuito de mitigar os possíveis danos decorrentes da violação aos dispositivos da Lei Geral de Proteção de Dados Pessoais.

Nesse sentido, para realizar uma proteção extensiva aos direitos dos titulares dos dados, a LGPD integrou ao seu corpo de normas-condutas a serem adotadas pelos operadores do tratamento de dados, com escopo de preservar a integralidade, a qualidade e o sigilos dos dados, tendo como consequência da violação, a majoração de sanções pecuniárias.
Embora, o vazamento de dados ocorra de forma ordenada, a implementação de sistema de segurança nas corporações implica na diminuição de situações incidentais por erro humano, ou inadequação dos programas empresarias, assim, devendo a gestão ensejar esforços para que a proteção dos dados seja preservada, desde a concepção do serviço.
Para a efetivação da Lei Geral de Proteção de Dados Pessoais, as empresas devem realizar a adequação de medidas de boas práticas e governança em privacidade para mitigar os possíveis danos decorrente da violação aos dados em provedores privados. Mesmo que a proteção aos dados de forma concreta não seja possível, as adoções de mecanismo de segurança podem atenuar as sanções e as perdas aos titulares dos dados.

REFERÊNCIAS

BARATA, André Mantola. Governança de dados em organizações brasileira: uma avaliação comparativa entre os benefícios previstos na literatura e os obtidos pelas organizações. 2015. Dissertação (Mestrado em Sistema de Informação) - Universidade de São Paulo, São Paulo, 2015.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, [2022]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 15 abr. 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidente da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 abr. 2023.

BERTOCCELLI, Rodrigo de Pinho. Compliance. In: CARVALHO, André Castro et. al. Manual de compliance. Rio de Janeiro: Forense, 2019. p. 35.

CANDELORO, Ana Paula; RIZZO, Maria Balbina Martins De; PINHO, Vinícius (Coord). Compliance 360: riscos, estratégias, conflitos e vaidades no mundo corporativo. São Paulo: Trevisan, 2012.

CARVALHO, A. P. Proposta de um framework de compliance à Lei Geral de Proteção a Dados Pessoais (LGPD): um estudo de caso para prevenção a fraude no contexto de big data. 2021. Dissertação (Mestrado em Engenharia Elétrica) - Universidade de Brasília, Brasília, 2021.

CARVALHO, Andre Castro. Manual de compliance. 3. ed. Rio de Janeiro: Forense, 2021.

CASAES, Júlio César Costa. Governança de dados abertos governamentais: frameworks conceitual para as Universidades Federais, baseada em uma visão sistemática, 2019. Tese (Doutorado em Engenharia e Gestão do Conhecimento). Universidade Federal de Santa Catarina, Florinaóplis, 2019.

DATA GOVERNANCE INSTITUTE (DGI). Definitions of data governance. 2017. Disponível em: http://www.datagovernance.com/adg_data_governance_definition. Acesso em: 01 mai. 2023.

ENDEAVOR DO BRASIL. Prevenindo com o Compliance para não remediar com o caixa. In: ENDEAVOR. [S. l.], 26 abr. 2017. Disponível em: https://endeavor.org.br/pessoas/compliance/. Acesso em: 15 mar. 2023.

ESPÍNDOLA, P. L.; SALM JUNIOR, J. F.; ROSA, F.; JULIANI, J. P. Governança de dados aplicada à ciência da informação: análise de um sistema de dados científicos para a área da saúde. Revista Digital de Biblioteconomia & Ciência da Informação, Campinas, v. 16, n. 3, p. 274-298, 2018.

FERNANDES, Aguinaldo Aragon; DE ABREU, Vladimir Ferraz. Implantando a governança de TI: da estratégia à gestão de processos e serviços. 4. Ed. Rio de Janeiro: Brasport, 2014.

FRAZÃO, Ana. Programas de compliance e critérios de responsabilização de pessoas jurídicas por ilícitos administrativos. In: ROSSETTI, Maristela Abla; PITTA, Andre Grunspun. Governança corporativa: avanços e retrocessos. São Paulo: Quartier Latin, 2007. p. 42

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. A Lei Geral de proteção de Dados Pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

HONÓRIO, Roseli. Modelo conceitual de governança de dados como suporte à governança do conhecimento organizacional. 2022. Dissertação (Mestrado em Engenharia e Gestão do Conhecimento) - Universidade Federal de Santa Catarina, Florianópolis, 2022.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC). Guia das melhores práticas de governança para cooperativas. São Paulo, 2015. Disponível em http://www.ibgc.org.br/ userfiles/files/2014/files/CMPGPT.pdf

JOHNSON, Ralph E.; RUSSO, Vincent. Reusing object-oriented designs. Relatório Técnico da

Universidade de Illinois, UIUCDCS 91-1696, 1991.

KLEINDIENST, Ana Cristina. Grandes temas do direito brasileiro: compliance. São Paulo: Almedina Brasil, 2019

KOEPSEL, Alice de Medeiros. Adoção e efeitos dos programas de compliance à luz da Lei Geral de Proteção de Dados Pessoais. 2020. Monografia (Graduação em Direito) -Universidade do Sul de Santa Catarina, Florianópolis, 2020.

LIMA, C., BASTOS, R. C. A criação de conhecimento apoiada pela governança de dados. In: CONGRESSO INTERNACIONAL DE CONHECIMENTO E INOVAÇÃO, 2019, Santa Catarina. Anais eletrônicos [...]. Santa Catarina Disponível em: https://proceeding.ciki.ufsc.br/index.php/ciki/article/view/647. Acesso em 10 Mar. 2023.

MARTIGNAGO, Deisi et al. Governança de dados aplicado no processo de catalogação. Revista Brasileira de Biblioteconomia e Documentação, São Paulo, V.15, n. 2, 2019.

MENDES, Gilmar Ferreira. Curso de direito constitucional. 2. ed. São Paulo: Saraiva, 2008.

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. São Paulo: Revista de Direito do Consumidor, 2018.

NASCIMENTO, Suellen Lima do. A lei Geral de Dados Pessoais e a Adoção dos Programas de compliance na sociedade da Informação. 2020. Monografia (Graduação em Direito) - Centro Universitário de Brasília, Brasília, 2020.

PESSOA, Larissa Rocha de Paula. Os desafios da Governança de dados e a realidade cultural brasileira. 2021. Dissertação (Mestrado em Direito) ? Universidade Federal do Ceará, Fortaleza, 2021.

PINTO, S. C. C. S.. Composição em Web Frameworks, 2000. Tese (Doutorado em Informática) Pontifícia Universidade Católica do Rio de Janeiro, Rio Janeiro, 2000.

PROSSER, William L. Privacy. California Law Review. California, v. 48, n. 3. p. 383 ? 423, agosto, 1960.

RÊGO, Bergson Lopes. Gestão e governança de dados: promovendo dados como ativo de valor nas empresas. 1. ed. Rio de Janeiro: Brasport, 2013,

ROQUE, Pamela Romeu. Estudos aplicados de direito empresarial: LL.C. em direito empresarial. São Paulo: Almedina, 2019.

SAAD, Carolina de Oliveira. A lei geral de proteção de dados pessoais e incidentes de segurança: regulação e prática de vazamento de dados, 2021. Monografia (Graduação em Direito). Fundação Getúlio Vargas. Rio de Janeiro, 2021.

SANTANA, Ricardo Cesar Gonçalves. Ciclo de vida dos dados e o papel da ciência da informação. In: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO. 14., 2013. Florianópolis. [?]. Florianópolis: UFSC, 2013. Disponível em: http://enancib2013.ufsc.br/index.php/enancib2013/%20XIVenancib/paper/viewFile/284/319. Acesso em: 13 mar. 2023.

SILVA, Ana Laura Fonseca. O papel das Soft Skills na implementação efetiva dos programas de compliance com foco na adequação à Lei Geral de Proteção de Dados ? Lei N° 13.709/18. 2022. Monografia (Graduação em Direito) - Universidade Federal de Ouro Preto, Ouro Preto. 2022

SILVA, Eggon João da. A defesa da ética e transparência. In: VENTURA, Luciano Carvalho. Governança corporativa. São Paulo: Saint Paul Editora, 2005, página 259.

TERRA, Priscila de Mello. A influência da governança de dados na gestão estratégica, 2017. Monografia (Bacharelado em Sistema de Informação) - Universidade Federal Fluminense, Niterói, 2017.

VAZAMENTO de dados aumentaram 493% no Brasil, segundo pesquisa do MIT.VEJA, São Paulo, 24 fev. 2021. Sociedade. Disponível em: https://vocesa.abril.com.br/sociedade/vazamentos-de-dados-aumentaram-493-no-brasil-segundo-pesquisa-do-mit. Acesso em: 15 mar. 2023.

VIEIRA, Tatiana Malta. O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante da tecnologia da informação. Porto Alegre: Sergio Antonio Fabris Editor, 2007.

==========

Arquivo 1: TCC - A IMPORTÂNCIA DO COMPLIANCE NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA - WESLEY VICENTE.pdf (8805 termos)
Arquivo 2: https://legaldictionary.net/mitigating-circumstances (1194 termos)
Termos comuns: 0
Similaridade: 0,00%
O texto abaixo é o conteúdo do documento TCC - A IMPORTÂNCIA DO COMPLIANCE NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA - WESLEY VICENTE.pdf (8805 termos)
Os termos em vermelho foram encontrados no documento https://legaldictionary.net/mitigating-circumstances (1194 termos)

==========

WESLEY VICENTE DA SILVA

A IMPORTÂNCIA DO COMPLIANCE EMPRESARIAL NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA

SALVADOR
2023

WESLEY VICENTE DA SILVA

A IMPORTÂNCIA DO COMPLIANCE EMPRESARIAL NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA

Artigo apresentado como requisito parcial para obtenção do título de Bacharel em Direito pela Universidade Católica do Salvador.

Orientador: Prof. Darlã Conceição Santos.

SALVADOR
2023

A IMPORTÂNCIA DO COMPLIANCE EMPRESARIAL NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA

Wesley Vicente da Silva1
Darlã Conceição Santos2

RESUMO: No cenário de exploração das informações como mercadoria econômica, os dados pessoais coletados por empresas privadas tornaram-se fator de tutela legislativa. Assim, surgiu a necessidade de organizar os setores privados para adequar aos moldes da Lei Geral de Proteção de Dados Pessoais ? LGPD, com o intuito de proteger a privacidade, como direito autônomo e fundamental para a tutela da pessoa humana, destacando os programas de compliance aliados as boas práticas e governança de dados. Nesse contexto, a fim de consolidar os mecanismos técnicos de segurança para a efetividade da legislação com a finalidade de mitigar os casos de vazamento de dados pessoais, a LGPD implementou medidas administrativas para inibir incidentes decorrentes das condutas infratoras a legislação. Desse modo, este trabalho tem como objetivo demonstrar a importância dos programas de compliance para a proteção aos direitos dos titulares dos dados, visando o cumprimento do ordenamento jurídico. Valendo-se do método hipotético-dedutivo, com abordagem qualitativa, utilizando da revisão bibliográfica de livros, legislação, artigos, dissertações e teses concernente à tutela de dados pessoais no Brasil para o desenvolvimento do presente artigo.

PALAVRAS-CHAVES: Compliance Empresarial. Governança corporativa. LGPD. Vazamento

de dados.

ABSTRACT: In the scenario of exploitation of information as an economic commodity, personal data collected by private companies have become a factor of legislative protection. Thus, the need arose to organize the private sectors to conform to the General Law for the Protection of Personal Data - LGPD, in order to protect privacy, as an autonomous and fundamental right for the protection of the human person, highlighting compliance programs allied with good practices and data governance. In this context, in order to consolidate the technical security mechanisms for the effectiveness of the legislation with the purpose of mitigating cases of leakage of personal data, the LGPD implemented administrative measures to inhibit incidents arising from conducts that violate the legislation. Thus, this work aims to demonstrate the importance of compliance programs to protect the rights of data subjects, aiming at compliance with the legal system. Taking advantage of the hypothetical-deductive method, with a qualitative approach, using the bibliographic review of books, legislation, articles, dissertations and theses concerning the protection of personal data in Brazil for the development of this article.

KEYWORDS: Corporate Compliance. Corporate governance. LGPD. Data leak.

1
Discente do curso de Direito da Universidade Católica do Salvador.
2
Mestre em Direito, Docente na Universidade Católica do Salvador.

1 INTRODUÇÃO

A nova moeda de troca não é apenas aquela que podemos ver, quantificar ou converter. Os moldes do mercado financeiro mudaram, sendo em questão material ou ao produto que eles precificam, postulando um novo aparato ao objeto contratual: os dados.
Muito embora, os dados pessoais, ainda para muitos, são apenas informações deslocadas acerca de fatores específicos, atualmente, podem ser conceituados como um conjunto de indicadores, regrados por um complexo condensado de informações em um fluxo crescente tangencial.
Os dados da grande massa acabam gerando indicadores que podem ser balizados e influenciados de acordo com os detentores dessa informação, apenas apartado em blocos de informações não são considerados como vetores orçamentários. Porém, direcionados para uma finalidade ordenada tem o condão de influenciar o interesse social.
Dito isso, os mecanismos postos pelo Reino Unido para possibilitar uma estruturação normativa para organizar e gerir os dados dos indivíduos, foi crucial para a criação em outros países, como no Brasil, onde instituiu-se a Lei Geral de Proteção de Dados Pessoais (LGPD). Muito

embora, a lei brasileira trouxe um arcabouço de normas reguladoras e sanções aos casos de tratamento de dados, que não foram abarcados com o marco da internet, os dados em uma visão macro constitucional já eram de forma genérica tutelados pela Constituição Federal de 1988.
Todavia, apenas a sanção da LGPD não seria, isoladamente, capaz de coibir as violações ao tratamento de dados na esfera privada, mas sim a necessidade de uma regulamentação do ciclo de vida das informações, que além de estipular os dados que podem ser utilizados ou até quando podem ser armazenados, estabelecer expressamente no bojo da norma como deve ser a proteção na operação do tratamento de dados.
De forma efêmera, conclui-se que a legislação pode delimitar os alicerces capazes de ensejar uma fiscalização, sendo estas através de mecanismo de gerenciamento de atividades, políticas de condutas e implementação de governança de dados, pois os dados hackeados ou vazados de forma isoladas, não seria possível identificar dados sensíveis, muitos menos individualizar o sujeito.
Portanto, o gerenciamento dos dados em provedores de armazenamento pode ter os riscos reduzidos de acordo com a realização de medidas de compliance para dirimir os impactos na

atividade empresarial, como também para tutelar os dados, cada vez mais acentuado como um produto orçamentário.

2 COMPLIANCE EMPRESARIAL

A criação do compliance está entrelaçado sob o cenário econômico-social, assim, sua implementação como sistema de organização foi instaurado e aprimorado a partir dos problemas práticos estruturais para gerir uma boa governança, com intuito de assegurar a proteção e o controle que garante a qualidade do negócio.
A utilização do termo foi inicializada no mercado financeiro, especialmente após a criação do Banco Central em 1913 nos Estados Unidos da América, com a necessidade de um sistema econômico ajustável e estável. Só após 1960, com a regularização da Securities and Exchange Commission (SEC), que houve a necessidade de implementação do compliance como um programa para a integração dos procedimento, controle e monitoramento de operação interna. (CARVALHO, 2021)
Em 1977, com a Convenção Relativa à Obrigação de Diligência dos Bancos Suíços, estabeleceu os modelos auto regulatórios, com adequação de condutas e processos internos, na qual a infração tem como consequência à aplicação de sanções. (CARVALHO, 2021)
Só após esse processo de amadurecimento histórico, que o Brasil teve a necessidade de competir em escala global, implementado novos processos de segurança no sistema financeiro brasileiro.
Pode-se concluir que, após a globalização com o fenômeno da criação dos dados estruturais, houve a potencialização das informações adquiridas por meio de provedores, classificadas, atualmente, como fonte econômica de um produto quantificativo e qualitativo, ao qual possibilita uma utilização como um produto do sistema financeiro.
Nesse sentido, em decorrência de ataques cibernéticos em provedores de informações

massificadas conduziram a sociedade na aplicação de institutos de melhoramento, como o compliance e suas interfaces para proteger no ambiente corporativo os dados massificados recebidos em seus provedores.

2.1 O CONCEITO DE COMPLIANCE

Antes de enveredar sob o conceito de compliance na esfera privada, é oportuno compreender o seu significado. Nesse contexto, a palavra compliance advém do verbo inglês, to comply, que pode ser definida como conformidade. O instituto deve ser aplicado como plano principal de uma diretriz pré-estabelecida para ser dirigida a todos capazes de enfrentar a finalidade destinada. (BERTOCCELLI, 2019)
Nesse parâmetro, pode ser traduzida como:

Comply, em inglês, significa ?agir em sintonia com as regras?, o que já explica um pouquinho do termo. Compliance, em termos didáticos, significa estar absolutamente em linha com normas, controles internos e externos, além de todas as políticas e diretrizes estabelecidas para o seu negócio. (ENDEAVOR DO BRASIL, 2022, n.p)

O compliance pode-se ser definido de forma técnica como um conjunto de normas padronizadas, sob um viés ético e legal, na qual após estruturação será a matriz orientadora para o comportamento organizacional da instituição ao qual atuará no mercado, como também irá reger as atividades dos colaboradores. Dessa forma, sendo um instrumento hábil a controlar o risco de imagem, a normatização legal, chamados de riscos de compliance, as que recaem nas instituições no decorrer da sua atividade laboral. (CANDELORO, 2012).
Superada a barreira terminológica, a finalidade do compliance tem como escopo o gerenciamento adequado do risco de atividades, verificar adequadamente as normas éticas e legais, e estudar os possíveis danos tangenciais. Dessa forma, esses elementos visam a redução de perdas e danos, como também amplifica a cultura e fortalecimento corporativo nos moldes aos padrões exigidos, seja esse por lei ou na tentativa de dirimir o risco do serviço prestado.
Portanto, segundo a doutrinadora Frazão (2007, p. 42), destina-se em sua obra que o compliance é como:
(...) conjunto de ações a serem adotadas no ambiente corporativo para que se reforce anuência da empresa à legislação vigente, de modo a prevenir a ocorrência de infrações ou, já tendo ocorrido o ilícito, propiciar o imediato retorno ao contexto de normalidade e legalidade.

Nessa mesma linha de pensamento, de acordo com os autores da obra Compliance 360° (2012, n.p), referem-se o compliance a:

Um conjunto de regras, padrões, procedimentos éticos e legais que, uma vez definido e

implantado, será a linha mestra que orientará o comportamento da instituição no mercado em que atua, bem como as atitudes de seus funcionários; um instrumento capaz de controlar o risco de imagem e o risco legal, os chamados ?riscos de compliance?, a que se sujeitam as instituições no curso de suas atividades.

Pode-se concluir que o conceito de compliance, em uma esfera macro, é um aglomerado de regras pré-estabelecidas através de um instrumento perpetuado por técnica de desenvolvimento, capaz de dirimir riscos e danos das atividades devolvidas pelo plano diretor.
Muito embora, o instituto "compliance" tem uma definição extensiva e não tem como fim apenas o cumprimento da legislação e de condutas éticas, pode ser compreendida também como um instrumento de diminuição de riscos, desenvolvimento corporativo sustentável e subsequentes segmentos empresariais de negócio. (ROQUE, 2019)
O compliance além de estar associado tradicionalmente a uma perspectiva organizacional aos comandos administrativos, pode ser vinculada também a uma visão de uma sociedade digital 4.0, devendo não só apresentar o compliance empresarial na esfera de redução de risco à imagem, mas sim, em uma abordagem de pré-orientação e implementação de desenvolvimento aos moldes legislativo de proteção aos dados, como objeto principal de estudos.
Portanto, é necessário a elaboração do projeto de compliance em uma visão lógica, a modo de compreender os objetivos e os componentes da aplicação do programa. Posteriormente, superado os obstáculos, aplica-se os estudos de riscos a boa governança corporativa com a implementação de programas de governança de dados objetivando auxiliar o controle de informações em conformidade aos padrões da corporação, e mitigar os danos da empresa.

2.1.1 AS GOVERNANÇAS CORPORATIVAS E A IMPLEMENTAÇÃO DOS PROGRAMAS DE COMPLIANCE

Em linhas gerais, o Instituto Brasileiro de Governança Corporativa ? IBGC (2015, n.p) discrimina o conceito de Governança Corporativa, como: ?Sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas. ?
O sistema da governança corporativa está associado ao desenvolvimento interno de uma empresa, seja ele entre a administração, sócios e funcionários, capaz de criar elos para uma estruturação de direção racional e acima de tudo nos moldes da ética e legislação.
Muito embora, a governança corporativa e o compliance sejam institutos que se assemelham em uma visão macro, os mesmos, diferenciam na aplicação prática, mas se complementam no objetivo final, sendo um instrumento para aplicação do outro.

A prática da governança corporativa, além de estimular o valor empresarial, pode-se concluir que estrutura de forma adequada a medida necessária para organizar a atividade empresarial, assim, não há que se falar em condutas prejudiciais. Por exemplo: empresários compreendem que para realizar uma instrumentalização segura aos seus sócios e administradores tendem a prejudicar o negócio empresarial, assim o autor Eggon João da Silva (2005, p.259) retrata que: ?A governança corporativa assegura tratamento equânime a todos os acionistas, inclusive minoritários, preferencialistas, nacionais e estrangeiros. Todos devem ter oportunidade de reparação caso venham a sofrer violação de seus diretores. ?

Nesse passo, as críticas ao sistema não são viáveis, tendo em vista a utilização de instrumento capaz de integralizar ao plano empresarial. Sendo assim, o programa de compliance visa amplificar a utilização de um sistema para garantir que todos possam participar de forma justa sob o aspecto legal, seja sócio ou administrador.

Em uma tangente geral, a implementação da governança corporativa ressoa em uma perspectiva segura, tanto internamente, seja auxiliando as avaliações das atividades executadas pelos sócios/administradores, quanto externamente, em relação à imagem da empresa, sendo este um fator primordial a empresas estruturadas no mercado.

A implementação da governança corporativa deve ser estruturada de acordo com as necessidades da empresa, devendo verificar o histórico de desenvolvimento do estabelecimento, pois, só a partir do status da empresa pode-se delimitar a estratégia possível para uma implementação segura e adequada. Sendo assim, um regramento mais rigoroso pode gerar consequências negativas e ineficazes, especificamente em estágios primários, pois em atividades inicias, as tomadas de decisões e a execução da atividade empresarial é primordial, sendo necessário, um aspecto negocial informal para realizar os objetivos da empresa, o que não se verifica quando existe prática de boa governança devidamente estruturadas no negócio. (KLEINDIENST, 2019)

Ao desenvolver da atividade da empresa, além da atenção a organização interna, sendo está um fator primordial da governança, ainda que no fim acabe tendo um aspecto externo por vislumbrar no mercado financeiro uma maior complexidade da entidade. O desenvolvimento da empresa, seja no faturamento, importação comercial, quantidade de funcionários, além dos controles a observância da legislação e regras internas, tendem à serem complexos, e, que necessita

de ações maiores que a própria instituição empresarial, restando necessária a implementação de sistema organizacionais aos fluxos de informações. (KLEINDIENST, 2019)

Ultrapassado a esfera conceitual e instrumentalização da política de boas práticas de governança, cabe pontuar que as empresas que possuem fluxos de informações sensíveis, conforme estipula o artigo 50 da Lei Geral de Proteção de Dados Pessoais, os controladores e operadores são responsáveis pelo tratamento de dados, devendo criar planos de adequação a legislação.

Assim, ao confeccionar as regras de boas práticas, os controladores adjuntos com a administração devem estipular através da análise da natureza dos dados coletados, a probabilidade, a finalidade e o potencial de riscos das vantagens advindas dos tratamentos dos dados verificados. (NASCIMENTO, 2020)

É necessário pontuar que, os agentes de tratamento, após a autenticação da gravidade e sensibilidade dos dados aos riscos de operação, poderão estabelecer programa de governança em privacidade, sendo este, um instrumento amplo com normas de compliance, além dos aspectos operacionais.
Em relação ao programa de governança de privacidade, pode-se estabelecer como um aglomerado de normas-regras de boas práticas de governança, com a finalidade de executar ordens de natureza legal. (NASCIMENTO, 2020)
Portanto, os instrumentos do compliance em conjunto com a boa prática de governança, se consagram na identificação dos riscos e estruturação de medidas para a empresa, sendo respondida de forma adequada e proporcional ao suporte da tomada de decisão.
O Programa de compliance na esfera privada para análise de dados pessoais, com a finalidade de promover a segurança, deve ser constantemente monitorado e atualizado, com a implementação de ?salva vidas? em decorrência de avaliação de riscos à privacidade e o acometimento de vazamentos. (NASCIMENTO, 2020)
Portanto, os instrumentos e objetos referenciados demonstram a determinação de regras de governança no ambiente de operação de tratamento de dados pessoais, a modo que seja realizado uma estruturação nas empresas para que possibilitem a implementação de mecanismos de segurança, com a finalidade de dirimir os riscos da atividade empresarial na sociedade digital.

3 GOVERNANÇA DE DADOS

O mercado digital tem como principal ativo financeiro os dados, este considerado como ?matéria prima? de uma economia baseada no conjunto de informações, sendo que nos últimos anos, houve um aumento exponencial na coleta de dados por cooperativas, startups e novos nichos empresariais, tendo a finalidade de quantificar e gerencias os dados.
Dados, informações, conhecimento e sabedoria são os quatros estágios evolutivos da cadeia de informação, pode-se assim, compreender os dados como fatos ou registros em seu formato primário. (BEAL, 2014). Já a informação é entendida como os conjuntos processados de dados em um contexto aplicado (RÊGO, 2013). Muito embora, na sociedade da informação ?os dados são o novo petróleo?, apenas os dados isoladamente não são capazes de transformar em ativo financeiro, sendo necessário administrá-lo de forma eficaz, para que assim, as empresas adquiram vantagem competitiva.
Dessa forma, a governança de dados tem como principal objetivo atender as necessidades das empresas, ou seja, solucionar problemas, diminuir custos da administração, para que os dados transformem em saldo positivo para os negócios (TERRA, 2017).
O Data Governance Institute -DGI (2017, n.p) definiu governança de dados como ?um sistema de direitos de decisão e responsabilidades para processos relacionados à informação, executado de acordo com modelos acordados que descrevem quem pode realizar quais ações com quais informações e quando. ? Portanto, a utilização da governança de dados orienta quais os métodos deverão ser aplicados no ciclo de vida dos dados.

Uma das atribuições da governança é o acompanhamento da operação dos dados com a finalidade de gerir que as informações estejam alinhadas com os objetivos pré-determinados na coleta primária, além disso, é necessário assegurar que as informações estejam disponíveis para acesso, quando consultadas, gozar de qualidade, consistência, auditabilidade e segurança dos dados (ESPÍNDOLA, 2018).

No âmago da cadeia evolutiva da informação uma das preocupações dentro das organizações corporativas é o receio com a proteção das informações, ou seja, a capacidade das empresas no protagonismo da segurança com os provedores internos, tendo em vista a necessidade de conformidade com a legislação pátria.

A boa governança tem como objetivo aplicável à prática do controle dos processos de operação dos dados: a prevenção de situações adversas que podem gerar o comprometimento da integralidade dos dados adquiridos pelas organizações empresariais, que por sua vez, devem ter o condão de reforçar a confidencialidade das informações. (ESPÍNDOLA, 2018).

A integração do programa de governança de dados nas corporativas empresariais, tem como o esforço principal a organização de dados, que deve ser observado por um prisma basilar, ou seja, a aplicação dos princípios como limite legal e ético no ciclo de vida dos dados.

Para Rêgo (2013), os princípios são regulamentações para compreender aplicação da governança dos dados como linha direta para os negócios, sendo: (i) A gestão de dados estratégicos, tem o dever de vislumbrar as tomadas decisões por um coeficiente tático e operacional. (ii) A governança como instituição, ou seja, a governança de dados pode ser comparada como sistema governamental, na qual dispõe de legislação, execução e jurisdição; (iii) A governança de dados como um programa, devendo ser implementado como fator permanente, não apenas um projeto temporário. Ainda, pontua-se que os princípios da Governança de dados não são limitados, tendo uma orientação basilar a cada implementação de um sistema organizacional que deve ser observado pelo prisma ético e legal.

Assim, os princípios devem incumbir os papéis que a serem preenchidos pela gestão moldar os comportamentos das empresas para a aquisição, reserva e utilização dos dados conforme as normas e políticas da corporação (TERRA, 2017).

Coleta, armazenamento, recuperação e descartes, são as quatro etapas do ciclo de vida dos dados (SANTANA, 2013), ou seja, para a aquisição de dados pelas empresas, deverão observar a vida útil do dado para não incorrer na (in) responsabilidade da utilização indevida de informações dos seus provedores.

As fases do ciclo de vida dos dados devem ser observadas pela ótica de seis objetivos, sendo eles: a qualidade, a privacidade, os direitos autorais, a integração, compartilhamento e preservação dos dados (ESPÍNDOLA, 2018). Muito embora, a lei geral de proteção de dados implementou e traçou novos objetivos para a coleta de dados pessoais, cabe destacar que os objetivos vislumbrados na Governança de dados têm como parâmetro preliminar a tomada de decisão, na qual deve ser os negócios pautados nos moldes legais e éticos vigentes.

Nesse contexto, o controle de informações é necessário, tendo em vista que na sociedade da informação, cada vez mais o volume de dados é crescente, acarretando mais vazão e protesto

por políticas públicas para a preservação dos institutos, órgãos e empresas que detenham a

informação, sendo assim, necessário sistema de organização, softwares e hardwares capazes de processar as informações, criptografar e armazenar. (MARTIGNAGO, 2019)
Assim, para otimizar o ciclo de vida dos dados e garantir que os objetivos sejam preenchidos na estruturação do gerenciamento de dados, faz-se necessário a implementação de frameworks com o intuito de garantir que o procedimento seja cumprido com maior qualidade de informação e aproveitamento financeiro para a empresa, auxiliando a tomada de decisão para redução de risco para utilização de dados. (MARTIGNAGO, 2019)
Um Framework, segundo Johnson (1991), pode ser definida como um aglomerado de objetos que colabora entre si para que atinja um conjunto de obrigações para aplicação de um domínio especifico. Já para Pinto (2000), um framework é conceituado como um software incompleto criado para ser um objeto cujo estado e comportamento são definidos pela classe. Assim, o framework é uma concepção de uma arquitetura para um edifício de subsistemas e oferece o alicerce básico para criá-los.
Muito embora, os autores defendem uma conceituação distintas acerca da concepção de frameworks, pode-se verificar que ambas se complementam, tendo em vista que o framework é um sistema pré moldado, ou seja, é um programa com intuito de ser complementado através da finalidade a ser cumprida pela gestão empresarial, sendo instanciado por classes para categorizar os dados e ser alojado em hotspot, provedores físicos, capazes de armazenar as informações coletadas pelas empresas.
Portanto, para gerenciar os ativos de dados de forma complexa, ordenada e objetiva é necessário para proteção do procedimento do ciclo de vida dos dados, determinar os modelos de frameworks para o gerenciamento dos dados. Assim, para Carvalho (2021), podem ser apresentados três domínios CobiT, DAMA DMBOK e DGI Framework, sendo apenas dois destes observados para fomento deste artigo: (i) A DAMA (DAMA DMBOK), e (ii) CobiT.
A DAMA (Data Management Association) é uma associação sem fins lucrativos, com o intuito de promover boas práticas de gestão de dados, e em 2009 fundou o DAMA-DMBoK (Data Management Body of Knowledge), sendo um corpo de conhecimento que tem como ponto fundamental esclarecer como as corporativas devem aplicar a operação otimizada dos dados. (CARVALHO, 2021)
Em sua versão 2.0, acrescenta não só uma visão macro do gerenciamento de dados, definindo padrões, terminologias e práticas, mas a integração de dados, para definir táticas,

armazenamentos e sistemas, bem como implementação da ética na operação do tratamento de dados, a definição de big data e ciência de dados e amadurecimento das informações. (LIMA, 2019).
O DAMA-DMBOK V2 é formado por 11 (onze) funções de gestão de organização de

dados, sendo incorporado como cerne principal: a governança de dados, tendo em vista que os dados percorrem por toda sistemática das onzes funções ordenadas, assim segundo Honório (2021):
A primeira função é a governa de dados, sendo o pilar do framework, tem o condão de orientar e supervisionar a operação do ciclo de vida dos dados, na qual deve estabelecer um sistema de apoio a decisão dos gestores sobre os dados, sob o prisma do negócio.
A arquitetura de dados, a segunda função, pode ser conceituada como um planejamento para administrar os dados, aquisição de ativos da empresa, com o intuito de definir a finalidade das informações adquiridas com os requisitos necessário para o gerenciamento dos dados.
Por sua vez, a modelagem de dados e design, tem a função de demonstrar de forma nítida os dados, sendo o processo da descoberta, análise e representação da etapa primária da informação.
O armazenamento, uma das etapas da operação do ciclo de vida dos dados, na qual vai incluir o design, o suporte dos dados armazenados para quantificar o coeficiente valorativo das informações, até o seu descarte, devendo respeitar todo o procedimento de segurança legal vigente.
Um dos alicerces para o gerenciamento de informação é a segurança, que deve garantir a proteção dos dados, a execução de políticas e procedimento de segurança, no intuito de moderar o acesso de forma consciente e controlado, não devendo ser infringido ou acessado de forma inadequada, afim de garantir autenticação e auditoria de dados informações.
A Integração e Interoperabilidade de dados, é a função responsável pela movimentação e a concretização dos dados na interligação do armazenamento e outras plataformas.
O gerenciamento de documentos, pode ser compreendida como o gerenciamento e inclusão da vida útil dos dados e informações, encontrados em programas não estruturados, em ênfase ao conteúdo de apoio de conformidade a legislação vigente e os termos éticos formalizados para o negócio.
Dados mestre e de referência, tem como condão a manutenção dos dados compartilhados para coexistir a integralidade dos sistemas internos de gerenciamento dos dados.
Em razão da interligação entre uma linha direta com os negócios, uma das funções do DAMA-DMBOK é a Data warehousing e Business intelligence, ou seja, a implementação de

planner para o contoler da administração dos dados e suporte a decisão com o intuito de conceder aos gestores de informação emitam relatórios de equalização de valores.
Segundo Barata (2015), os metadados, na qual consiste a décima função, é promover a facilitação do acesso dos dados interligados nas multifontes do sistema integrado, como também garantir a qualidade de dados.
Por fim, o gerenciamento de qualidade de dados é a implicação das técnicas para garantir a possibilidade de aferição, melhoramento e adequação da utilidade dos dados, com o intuito de monitorar a integridade da informação primária no ciclo de vida dos dados.
Já o COBIT (Control Objectives for Information and related Technology), é um framework de suporte fundado em 1994 administrado pela ISACA (Information Systems Audit and Control Association), estruturado como um arcabouço de informação direcionadas para governança de dados e gerenciamento de informação, tem como objetivo auxiliar os profissionais de gestão na conexão entre os problemas técnicos e os riscos do negócio. (BARATA, 2015).

Para Lima (2019), o COBIT é um framework que possui duas vertentes basilares: a gestão, que possui quatro áreas de domínios: planejamento, constituição, execução e monitoramento, e a governança que é a tomada de decisão de acordo com a gestão de dados, possuindo 37 (trinte e sete) processos integrados.
Na versão 5.0, o sistema é utilizado baseado em 05 princípio, conforme elucida Casaes (2019), Barata (2015) e Lima (2019), sendo: (i) atender às necessidades das partes interessadas; (ii) cobrir o negócio como um todo; (iii) aplicar um framework único e integrado; (iv) habilitar uma visão holística; e (v) distinção entre governança de gestão.
Um dos princípios é atender às necessidades das partes interessadas, sendo a necessidade das corporativas é satisfazer as expectativas dos seus stakeholders, proporcionando um equilíbrio na tripartite: benefícios, redução do risco e recurso disponíveis.
O segundo princípio é baseado na cobertura do negócio como um todo, ou seja, abranger a integralidade da empresa no processo, procedimento, pessoas e as relações com os habilitadores.
A aplicação do framework único e integrado, assim, o COBIT é capaz de promover uma relação completa com a Governança de dados, corroborando ao alinhamento com padrões externos e adaptabilidade dos modelos usuais de negócios.

O COBIT permite habilitar uma visão holística, ou seja, uma visão macro dos componentes que oferecem suporte para atingir as finalidades da governança de dados, na qual define como catalogadores: as políticas, processos, estruturas organizacionais, informação e ética.
Por derradeiro, o princípio da distinção entre governança de gestão, tendo em vista que ambos possuem estruturas organizacionais distintas, assim, governança tem como esforço principal que os objetivos corporativos sejam cumpridos, estabelecendo prioridades pela tomada de decisão, compliance e progresso das organizações. Por sua vez, a gestão é o planejamento, construção, execução e monitoramento das funções ornamentada com o direcionamento da governança.
Desse modo, com escalonamento dos cinco princípios é capaz de proporcionar o funcionamento otimizado do framework, destacando os seguintes processos:
O APO01: Gerenciar o framework de TI, tem como condição a otimização das atividades relacionadas ao TI, com a função principal de incluir os procedimentos e regulamentos para promover a integralidade das informações nos bancos de dados. (BARATA, 2015)
Já o APO03: Gerenciar a arquitetura corporativa, tem função primordial agrupar as informações para auxiliar as atividades e tomadas de decisões, conceituando e compartilhando as informações dos elementos dos dados, e por fim catalogar a empresa, com base na modulação e sensibilidade dos dados. (BARATA, 2015)
Nesse ínterim, a governança de dados como um sistema integrado com o programa de compliance, tem o condão de otimizar a operação de controle interno relacionado aos dados coletados pelas empresas, capaz de gerenciar as bases para o apoio de decisão ao tratamento das informações, com segurança e qualidade, garantido o ciclo da vida útil dos dados.

4 A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

As estruturas políticas, econômicas e sociais com desenvolvimento de novas tecnologias e mecanismo para a coleta de dados e informações, fez necessário modulações legislativas para a proteção da privacidade, além dos aspectos físicos, patrimoniais e morais.
A proteção à privacidade de dados foi dividida em quatros gerações: a primeira, oriunda do estado moderno, com o advento dos bancos de dados; a segunda, datada em 1980, com a expansão legislativa para a proteção à privacidade aos setores privados; a terceira geração em 1990, com o processo de tratamento de dados e o consentimento dos cidadãos; Por fim, a última dimensão, é

destinada ao protagonismo da permissão para coleta e uso dos dados pessoais, quando a lei estabeleceu a importância da titularidade das informações. (MENDES, 2014)
Nesse aspecto, é perceptível a evolução do direito aos fatores reais da sociedade e as transformações dos meios tecnológico, computacionais, genéticos e comunicativos, que por sua vez possibilitou a integração da comunicação global, e consequentemente, o rastreio dos dados através do armazenamento de informação. (SAAD, 2021).
Os legisladores ao considerar os dados pessoais como extensão ao direito à privacidade, preocuparam em tutelar constitucionalmente a proteção da população, em especial os países europeus, como: Espanha, Portugal, Hungria, Eslovênia e Rússia. (VIEIRA, 2007) Porém, só tornou-se fator primordial após o regulamento geral do Parlamento Europeu sobre a proteção de dados, n.º 2016/679, sendo necessário a adequação das empresas prestadoras de serviço na Europa ao regulamento, influenciado diretamente o Brasil para elaboração da Lei Geral de Proteção de Dados brasileira. (SAAD, 2021).
Muito embora, a Lei Geral de Proteção de Dados Pessoais - LGPD, em sua promulgação, não abarcou de forma expressa a proteção de dados como direito fundamental, a doutrina, em especial Nascimento (2020), por sua vez, já argumentava a proteção de dados e informações pessoais como direito autônomo, derivado do direito fundamental à privacidade, explicitamente no artigo 5°, X, da CRFB de 1988.
Após reiterados julgamento sobre a tutela dos dados pessoais como extensão da personalidade do indivíduo, o Supremo Tribunal Federal -STF reconheceu no Julgamento da Ação Direta de Inconstitucionalidade - ADI 6387, a existência dos dados como direito autônomo, derivada do direito fundamental a dignidade da pessoa humana, na proteção à intimidade e a centralidade do Habeas Data como autodeterminação informativa. (NASCIMENTO, 2020).
Ao compreender a necessidade da proteção aos dados pessoais, os legisladores brasileiros em votação de ? das casas legislativas (câmara e Senado Federal) em dois turnos, aprovaram a Emenda Constitucional 115 de fevereiro de 2022, alterando o artigo 5° da Constituição Federal de 1988, incluindo o inciso LXXIX, tutelando constitucionalmente a proteção aos dados pessoais, inclusive nos meios digitais.
Ressalta-se, ainda, que os dados pessoais estão interligados com o direto fundamental à privacidade, na qual representa a capacidade de a pessoa administrar sua vida, seus pertences e

propriedades materiais e imateriais, permitindo ou não a utilização dos seus dados (bens imateriais) por terceiro. (NASCIMENTO, 2020).

A privacidade, por sua vez, segundo Mendes (2008), é o direito à proteção aos comportamentos pessoais e acontecimentos de caráter íntimo, bem como as informações prestadas aos profissionais e comerciantes, em que a pessoa não deseja que se compartilhe com o público.

Para o professor William Prosser, pode-se qualificar a lesão a privacidade em quatro graus: i) o intrometimento na reclusão ou solidão na vida privada, ii) a divulgação pública de fatos privados constrangedores sobre o indivíduo; iii) a publicidade sobre o indivíduo apresentada de forma equivocada; e iv) a apropriação, para obtenção de vantagem, do nome ou da imagem do demandante (PROSSER, 1960).

A doutrina, por sua vez, defende mais uma violação à privacidade: a privacidade informacional, interligada com os fatores tecnológicos de informação. (SAAD, 2021). Assim, quando a lei ao realizar o tratamento da privacidade, refere-se como um direito líquido, ao qual será tutelado para garantir que o indivíduo tenha um local reservado, que não tenha, se desejar, a interferência de outros sujeitos, seja pessoa física ou jurídica.

Com a proteção dos dados pessoais dos titulares, através da LGPD, possibilitou ao cidadão o acesso a informações ao ciclo de vida útil dos dados pelas empresas, e a certeza de fiscalização pela Autoridade Nacional de Proteção de Dados, com a finalidade de atingir os objetivos traçados pela legislação, na qual a lei traz conceitos e delimita princípios, que devem ser mencionados.

A LGPD tem como objetivo principal: ?o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado?, com a destinação de assegurar os direitos fundamentais a liberdade e privacidade dos titulares dos dados, bem como tutelar a dignidade e a personalidade da pessoa natural. (LGPD).

A legislação está ordenada diretamente com o meio empresarial, sobretudo no que se refere aplicação aos seus destinatários que são pessoas físicas ou jurídicas que realizam a coleta e tratamento de dados no Brasil, conforme preceitua o artigo 1° da lei 13.709, de 14 de agosto de 2018.

Para compreender a LGPD, faz-se necessário elucidar os conceitos de dados pessoais: (art. 5º, I) é toda informação relacionada a pessoa natural, identificada ou identificável, sendo o dado aplicado no contexto que possibilite o reconhecimento do indivíduo. Bem como refere-se aos dados sensíveis (art. 5º, II), são todas as informações que se relaciona com pensamentos políticos, crenças,

identidade biológica e física. Portanto, a legislação tem como ponto a proteção e o cuidado para a não violação dos dados pessoais e sensíveis.

Os doutrinadores, Laura Schertel e Danilo Doneda, ainda aponta cinco pilares para compreender a LGPD, sendo: i) a unidade e generalidade da aplicação da Lei; ii) a legitimação para o tratamento de dados (hipóteses autorizativas); iii) os princípios e direitos do titular; iv) as obrigações dos agentes de tratamento de dados e v) a responsabilização dos agentes.

O primeiro pilar é considerado com aplicabilidade material da legislação, ou seja, aplica-se a qualquer operação realizada por pessoa natural ou jurídica de direito público ou privado,

independentemente do meio, da sua sede ou do país onde estejam localizados os dados (Art. 3°). Considerado, assim, como uma aplicação uniforme para todos os setores público ou privados que realizam tratamento de dados.

O segundo pilar é a legitimação para o tratamento de dados, tendo em vista que a lei especificou critérios e requisitos para o reconhecimento da legitimidade, não podendo ser tratados os dados, sem que exista uma base normativa que autorize, prevista no artigo 7°, 11° ou 23° da LGPD, abordando 11 (onze) hipóteses, incluído o consentimento ou a previsão legislativa.

Destaca-se que a autorização por consentimento para ser considerado válido, deve observar os requisitos previsto no artigo 5°, XII, sendo considerado que a vontade deve ser livre, informada, inequívoca e com a finalidade determinada, consagrando os princípios norteadores da legislação.

O terceiro pilar é o conjunto de princípios e direitos que assegura o destinatário da lei a controlar a utilização do seu dado pessoal, sendo importante elencar dez princípios que estruturam a LGPD: a finalidade, a adequação, a necessidade, o livre acesso, a qualidade dos dados, a transparência, a segurança, a prevenção, a não discriminação e a responsabilização. (MENDES, DONEDA, 2018)

No que concerne, aos direitos dos titulares são expressos no artigo 18° da referida lei, que permite o titular dos dados adquirir através do controler, independentemente do momento, as informações relacionadas ao indivíduo, prevendo: acesso, confirmação, correção, anonimização, bloqueou ou eliminação e a portabilidade.

Para adentrar no cerne dos problemas enfrentados pela legislação, em especial, sobre o vazamento de dados, os dois últimos pilares serão abordados sob a perspectiva da violação e responsabilização acerca da proteção de dados nos casos incidentes de vazamento.

Assim, o quarto pilar, destina-se às obrigações dos agentes de tratamento dos dados, na qual estabeleceu limites que devem ser observados nas operações realizadas para reforçar a segurança e prevenir os problemas da atividade no tratamento de dados.

Uma das obrigações fundamentais, consiste na intitulação do encarregado pelo tratamento dos dados indicados pelo controlador, conforme artigo 41 da LGPD, que possui a função de aceitar as reclamações e comunicações dos sujeitos dos dados, receber informações da Autoridade Nacional, como deve orientar os funcionários a respeito das práticas a serem adotadas em relação à proteção de dados pessoais.

Assim, as informações devem ser fornecidas ao proprietário dos dados, quando os dados forem coletados, como: os meios de segurança aderidos ao tratamento de dados, quais são os riscos da atividade que podem gerar lesão ao titular, pois pode gerar a mitigação dos prejuízos. (SAAD, 2021)

A lei Geral de Proteção de Dados Pessoais tem como objetivo a proteção do dados pessoais dos titulares dos dados, sendo assim, uma das obrigações principais é adoção de medidas de segurança, técnicas e administrativas hábeis a proteger os dados pessoais de acessos não autorizados, como promover a integralidade dos dados, não permitindo, assim, a alteração das informações, a prevenção de situações ilícitas ou acidentais, ou qualquer forma de tratamento inadequado, consoante se desprende do artigo 46 da lei.

Tornou-se corriqueiro manchetes acerca do vazamento de dados por corporativas, uma das violações mais graves incidentes abarcados pela LGPD, o que ocasiona a vulnerabilidade do titular dos dados, e dos sistemas internos que são responsáveis pelo ciclo de vida útil dos dados. (SAAD,2021)

A seção de segurança de informação tem como condão as obrigações inerentes aos agentes de tratamento, devendo ser adotado pela integralidade das pessoas que realizam o tratamento de dados, garantido que os dados sejam confidenciais, bem como disponíveis nas operações de tratamento. (Art.48). Nos casos incidentais de vazamento de dados, insurge a necessidade ao controlador de informar a autoridade de proteção de dados, que podem definir as medidas para mitigação dos danos.

No entanto, com a utilização da internet, compras online, transferência virtuais e outros meios tecnológicos, criou-se uma dificuldade para atuar na segurança de dados, tendo em vista a abrangência e os domínios de redes globais, que combinados com fatores não perceptível, forma

um perfil não rastreavel capaz de ocasionar violação às diretrizes básicas da legislação, que mesmo com ações posteriores não conseguem excluir os inúmeros registros de pessoas e organizações que coletaram os dados, lesionando a confidencialidade das informações (SAAD, 2021)

Destaca-se que as obrigações aos controladores e operadores, devem ser observados desde a coleta dos dados até seu descarte, assim o artigo 46 da LGPD, introduziu o conceito de privacy by design, sendo a incorporação pelas empresas nos serviços e produtos, na qual dispõe a proteção da privacidade no centro de todo o desenvolvimento corporativo.

Embora, a legislação tenta dirimir os riscos da atividade, os prejuízos causados pelo vazamento de informações são altos, e perpassam pela inadequação do sistema de proteção, perda de credibilidade e de clientes, ocasionado uma ruptura na imagem da empresa, impossibilitando, muitas vezes de concorrer no mercado corporativo. (SAAD,2021)

Portanto, a LGPD concebeu obrigações aos agentes de tratamento de dados, para que se delimite a finalidade da utilização dos dados desde o início da concepção, devendo o controlador confeccionar relatório de impacto a privacidade, utilizando de métodos para a captação da operação do ciclo de vida dos dados, observando as mediadas adotada para aumentar a segurança e mitigar o risco do tratamento das informações, conforme artigo 3 da LGPD.

O último pilar, considerado como a responsabilidade dos agentes na incidência de ocorrência de danos derivados do tratamento de dados. A LGPD consagrou a natureza do tratamento, limitando os parâmetros ao artigo 7° da lei, nas 10 hipóteses dos incisos, vinculados a finalidade da captação dos dados, consoante prevê o artigo 6°, inciso I, II, da LGPD.

A legislação tem como regra o descarte (eliminação) dos dados ao fim do tratamento da operação (art. 16), com o intuito de mitigar os riscos presente no tratamento de dados, principalmente, no que concerne à limitação das hipóteses de tratamentos para não lesionar os direitos dos titulares.

Nos casos, em que mesmo após o término de vida útil dos dados, as empresas podem, quando permitido, armazenar dados que em situação incidentais serem objetos de violação, principalmente nos casos de vazamento, que podem ocorrer, quando não autorizados pelo titular

ou controladores, serem acessados, captados, compartilhados pela internet, para outros sujeitos ou empresas.
Assim, a Lei Geral de Proteção de dados Pessoais, em especial em seu artigo 42, dispõe que o controlador ou operador, quando realizar o exercício do tratamento de dados pessoais, vem

a ocasionar dano patrimonial, moral, individual ou coletivo em detrimento a aplicação da legislação, é obrigado a repará-lo, definindo a responsabilidade de forma objetiva.
Embora, a responsabilização objetiva não é necessária a demonstração de culpa do controlador ou operador. Faz mister esclarecer que o operador, só será responsabilizado quando os atos praticados forem contrário à legislação, ou às instruções que foram fornecidas pelo controlador. (MENDES, DONEDA, 2018)
Ainda, a legislação prevê exceções a responsabilidade objetiva (art. 43), sendo: quando o agente demonstrar que não realizou o tratamento de dados pessoais que foi atribuído, ou quando não houve violação da segurança ou a legislação, e por fim, quando for por culpa exclusiva do titular ou de terceiros.
Porém, o cenário que é vislumbrado no Brasil nos casos de vazamento de dados, é que as violações pelas instituições vêm ocorrendo, majoritariamente, sob ataques deliberados de hacker, ou falha de segurança dos controladores dos dados. (SAAD, 2021)
Dessa forma, é necessário adotar medidas para dirimir os riscos da atividade, e possibilitar o discernimento das informações acerca dos perigos de vazamento de dados, tendo em vista que a tendência é aumento significativo das violações vinculados com a crescente tecnológica. Assim, as empresas devem implementar mecanismos para a segurança das informações.

5 O COMPLIANCE EMPRESARIAL COMO INSTRUMENTO DE PROTEÇÃO DE DADOS NA ESFERA EMPRESARIAL

Em decorrência das constantes violações aos dados armazenados em provedores privados, a tutela ao direito à privacidade nos meios tecnológicos, já era pauta de debate na legislação brasileira, e já existiam mecanismos para a proteção, como: a proibição de direcionamento dos provedores em relação ao compartilhamento de dados, bem como a inibição ao monitoramento nos navegadores de internet.
Vinte e seis bilhões de dados foram vazados no Brasil em 2019, de acordo com pesquisas realizadas pelo Massachusetts Institute of Tecnology ? MIT, possibilitando a utilização de números telefônicos, score de crédito, endereço eletrônico, fotos, números de identificações e outros dados pessoais, para o cometimento de crimes cibernéticos, e a violação aos direitos dos titulares.
A utilização e uso dos dados pessoais por pessoa física ou jurídica, com sede no Brasil ou não, devem se atentar as normas gerais de proteção aos dados brasileiro, segundo Frazão, Oliva e

Abilio (2020), é a necessidade de conferir a efetividade aos direitos e prevenir a violação aos dados, através da implementação de mecanismo de compliance, como uma ferramenta capaz de promover a adequação das atividades aportadas pelas empresas.
Assim, os controladores e operadores poderão formular regras de boas práticas e governança (Art. 50), que contenha as disposições de organização interna, o regime de funcionamento, as operações, o canal de comunicação entre os encarregados e os titulares dos dados, e o procedimento de segurança.
Nessa perspectiva, considerando que a maioria das tratativas de dados perpassam por meios digitais, deve-se adotar sistema para mapear os riscos, e implementar mecanismos para minorar as vulnerabilidades apontadas pelos programas, através da alta administração, do código de ética, para proteger os dados pessoais dos titulares. (PESSOA, 2021)
Existem inúmeras formas de ocorrer o vazamento de dados, sendo através de ataques cibernéticos, sequestro de conta, furtos de dados, compartilhamento de dados por agentes ou ex-agentes da empresa, erro ou negligência, entre outros, que podem ser para adquirir dados de nomes, CPF, celulares, endereços, dados financeiros, senhas, registro de saúde ou credenciais de acesso. (SAAD, 2021)
Desse modo, para realizar o mapeamento dos problemas que as corporativas podem enfrentar, é necessário identificar os fluxos e processos de informação que percorrem os sistemas, que irão auxiliar na tomada de decisão pelas empresas. (NASCIMENTO, 2020)
A alta administração deverá colaborar ativamente no programa de compliance, seja monitorando as investigações e intervenções em situação para estabelecer controles internos em conformidade com a legislação, bem como possibilitar a interdependência dos setores para realizar as atividades designadas para o tratamento de dados (PESSOA, 2021).
Com a elaboração do código de ética pela organização possibilitará o treinamento regular das equipes, responsáveis pela tecnologia da informação, para enraizar a cultura corporativa da boa governança, com a finalidade de assegurar o respeito ao programa de compliance (NASCIMENTO, 2020)
Nesse contexto, para manter uma boa relação com seus clientes, as organizações devem instalar canais de comunicação, para que os titulares dos dados possam contatar os encarregados responsáveis pelos armazenamentos dos seus dados, e exerçam seus direitos sobre as informações contidas nos provedores. (PESSOA, 2021).

Desse modo, quando se trata de concretização a alteração cultural coportariva é preciso realizar o alinhamento dos funcionários com o código de ética, com política de privacidade, para fins de efetividade do programa de compliance de dados. (PESSOA, 2021).

5.1 A IMPLEMENTAÇÃO DE MECANISMOS DE GOVERNANÇA DE DADOS PESSOAIS

Para a efetividade da legislação em relação ao tratamento de dados, a LGPD direciona um capítulo para implementar o programa de governança em privacidade, com a finalidade das empresas adotarem medidas técnicas, para fins de proteção e segurança dos dados pessoais.

(PESSOA, 2021)
A governança em privacidade, pode ser conceituada como um conjunto de regras e práticas positivas a serem implementadas pelos agentes de tratamento, e encontra-se em conformidade com as políticas de compliance empresarial, com o objetivo de gerir os dados das empresas para estabelecer um diferencial competitivo aos negócios. (KOEPSEL,2020)
O programa integra o aperfeiçoamento do procedimento de utilização dos dados, com os requisitos pré-estabelecidos na implementação dos softwares, com a finalidade de gerir de forma otimizada os dados para preencher as diretrizes da legislação. (SAAD, 2021)
A Lei Geral de Proteção de Dados Pessoais dispôs que os controladores e operadores poderão adotar programas de governança em privacidade, que devem ser implementados com o mínimo, (art. 50, § 2°, I): a) o comprometimento dos agentes de tratamento com as políticas internas que devem garantir o cumprimento das normas e regras de boas práticas; b) que aplicação seja de forma uniforme para todo a operação de tratamento de dados; c) que a governança seja adaptativa as estruturas da empresas, sendo compatível com a densidade dos dados e operação; d) como implementar políticas de salvaguardas em relação aos titulares dos dados; e) tenha como objetivo estabelecer uma relação de confiança com sujeitos dos dados, estabelecendo situações de transparência e que possibilite a atuação do titular; g) que conte com planos de respostas a incidentes e remediações; h) seja continuamente atualizado sua base.
Nesse aspecto, devem ser adotadas medidas administrativas para que as instituições, em conformidade com a legislação, apliquem estímulos para assegurar as informações armazenadas pelas empresas, com a adoção de orientações internas que respeitem as diretrizes que inclua o uso

minimizado ou a anonimização das informações, desde a coleta dos dados, conforme artigo 46 da LGPD.
Com o mapeamento das atividades, é importante verificar: O que são esses dados?; de que forma foram coletados ?; quem são os coletores ?; existe relação entre os dados e atividade realizada ?; O que pode ocorrer com esses dados ao serem coletados? E, como são descartados da gestão organizacional da empresa? (NASCIMENTO, 2020). Dessa forma, para adotar medidas compatíveis com os riscos alertados pelos sistemas para a proteção de dados nas organizações privadas, é necessário possuir conhecimento do caminho realizado inerentes ao ciclo de vida útil dos dados.
Embora, a legislação já estabeleça diretriz mínima para o tratamento de informação, a Autoridade Nacional de Proteção de Dados - ANPD, poderá, ainda, determinar padrões técnicos para serem implementados pelo programa de governança em privacidade, devendo ser observado a qualidade de dados, as especificações do tratamento e status tecnológico, em especial a proteção aos dados sensíveis disposto na legislação. (NASCIMENTO, 2020)
Muito embora, a lei geral de proteção de dados, apenas delimita as características e os requisitos mínimos que os operadores deverão tomar para desenvolver um compliance na organização das empresas privadas em consonância com a legislação, porém não impõe um modelo específico para integração de um programa nas corporativas. (PESSOA, 2021)
Assim, para Saad (2021), as medidas técnicas que podem ser adotadas pelos agentes de

tratamento de dados, são: i) o uso de firewalls, sendo um mecanismo de segurança que coleta os dados em conformidade com as regras pré estabelecido para análise de tráfego de rede, delimitando as operações de compartilhamento e captação de informações a serem cumpridas; ii) a utilização de antimalware, que consiste na proteção contra vírus que é capaz de fragilizar o sistema, apagar dados e infectar outros arquivos; iii) a utilização de criptografia dos dados, que possibilite quando ocorrer situações incidentais a não identificação do titular do direito.
Já para Fernandes e Abreu, (2014) defendem a implementação de frameworks como a DAMABOK e COBIT, para o gerenciamento de dados, pois tem como meta principal a delimitação do escopo das atividades, as funções envolvidas no tratamento e as interações a serem executadas pelo software, com a finalidade de proteger a privacidade em ambientes corporativos que gerenciam o armazenamento de informações aplicados na prevenção à fraude.

Segundo Carvalho (2021), a integração do software, através das boas práticas estabelecidas pela legislação, poderá aprimorar os aspectos de proteção à privacidade e prevenção a fraude do tratamento de coleta de dados. Tendo em vista, que os frameworks, podem balizar as métricas de qualidade dos dados que indicam uma utilização adequada e otimizada, e aponta a melhor proteção da privacidade.
Com a melhoria de processo de governança para o tratamento de dados, estabelece uma divisão entres as operações que possibilita uma automatização do ciclo de vida dos dados (coleta, utilização, armazenamento e exclusão), capaz de gerar relatório de risco, para o auxílio da tomada de decisão com o intuito de gerir de forma adequada o tratamento de dados. (CARVALHO, 2021)
Neste parâmetro, os programas de compliance com a implementação de frameworks, podem responder questionamento acerca do procedimento de tratamento de informação, dispondo de quais práticas relacionadas à governança, privacidade e segurança de dados, apresentam melhor benefício para o tratamento de dados pessoais. (CARVALHO, 2021)
Ademais, os controladores e operadores deverão adotar medidas, como o Relatório de Impacto ? DPIA), que corresponde a avaliação dos riscos e impactos relacionados com o tratamento de dados pessoais, além da anonimização, da transparência e do sigilo, deverão delimitar prazos para retenção de dados e aderir políticas seguras de informação acerca da operação de tratamento. (SILVA, 2022)
Após realizar a implementação e observância das estruturas mínimas estabelecidas pela LGPD, é necessário adotar um programa de gerenciamento de vulnerabilidades, com atualizações constantes e autocorreções alinhados com as boas práticas de atividades cotidianas, com a finalidade de proteger os dados pessoais, e promover um ambiente corporativo adequado para realizar o tratamento de dados. (SAAD, 2021)
No entanto, ao verificar que houve vazamento de dados, seja pelo recebimento de notificação ou pela veiculação na mídia, os agentes de tratamentos deverão identificar quais dados vazaram e realizar o procedimento estabelecido no programa de compliance de segurança, além de notificar as instituições. (Art. 48, caput).
De acordo com MIT, o prazo entre a comunicação à autoridade competente e a ocorrência do fato ilícito ultrapassa 200 (duzentos) dias em média, sendo umas das preocupações para a

efetividade da legislação, e a redução dos danos causados aos titulares dos bens imateriais.

A Lei Geral de Proteção de Dados, dispõe que nas situações que ocorrer a probabilidade de riscos ou violação aos direitos dos titulares, tem como obrigação do encarregado a comunicação à autoridade nacional e ao titular do dado (art. 48, caput). Sendo que o contato deve ser em período razoável (art. 48, § 1º), contendo a natureza dos dados dos titulares atingindo (art. 48, § 1º, I).
Em decorrência dos possíveis incidentes, a LGPD determinou critério para aplicação de sanções, em casos de vazamento de dados, observando as situações específicas de cada caso, disposto no art. 52, § 1º. Assim, deve ser considerada a avaliação da gravidade, a natureza das informações e do dano ocorrido (incisos I e VI), sendo necessário para este caso, tendo em vista que o compartilhamento indesejado de dados sensíveis pode ocasionar danos irremediáveis para os titulares.
Portanto, existe a necessidade da adesão aos mecanismos e técnicas para promover a efetividade dos programas internos com a finalidade de mitigar os danos, assim, a implementação de boas práticas e governança têm como fator o cumprimento da legislação, por meio de medidas de segurança. Entende-se, que a proteção integral contra falhas que possibilitam a ocorrência de ilícitos não é possível, porém essas diretrizes reduzem as possibilidades de existir desvios de condutas e criar salvaguardas para identificação dos incidentes, de forma eficaz, rápida e adequada.

6 CONSIDERAÇÕES FINAIS

A partir da permissão ao acesso dos dados pessoais, as informações coletadas passaram a integralizar as redes de tratamento de dados, tornando-se alvo de ataques cibernéticos, contribuindo para o aumento da intercorrência no ambiente corporativo, tornando-se o gerenciamento de informação um dos diferenciais no desenvolvimento do negócio.
Nesse contexto, foi imperativo o surgimento de leis que protejam os dados dos cidadãos, e que limitem a gestão das entidades públicas e privadas em relação as informações coletadas, transformando o sistema organizacionais, como compliance, em ferramentas de efetivação das normas éticas e legais. Assim, a implementação do programa alinhado com a governança corporativa é capaz de integralizar o corpo de normas internas com o intuito de adequar a legislação brasileira e criar uma cultura corporativa.
Dentro do programa de compliance, a administração em conjunto com a gestão da empresa, poderá implementar ao plano diretor, a utilização de software, sendo este capaz de possibilitar a automatização do ciclo de vida útil dos dados para realizar o auxílio da tomada de decisão, com o intuito de mitigar os possíveis danos decorrentes da violação aos dispositivos da Lei Geral de Proteção de Dados Pessoais.
Nesse sentido, para realizar uma proteção extensiva aos direitos dos titulares dos dados, a

LGPD integrou ao seu corpo de normas-condutas a serem adotadas pelos operadores do tratamento de dados, com escopo de preservar a integralidade, a qualidade e o sigilos dos dados, tendo como consequência da violação, a majoração de sanções pecuniárias.
Embora, o vazamento de dados ocorra de forma ordenada, a implementação de sistema de segurança nas corporações implica na diminuição de situações incidentais por erro humano, ou inadequação dos programas empresarias, assim, devendo a gestão ensejar esforços para que a proteção dos dados seja preservada, desde a concepção do serviço.
Para a efetivação da Lei Geral de Proteção de Dados Pessoais, as empresas devem realizar a adequação de medidas de boas práticas e governança em privacidade para mitigar os possíveis danos decorrente da violação aos dados em provedores privados. Mesmo que a proteção aos dados de forma concreta não seja possível, as adoções de mecanismo de segurança podem atenuar as sanções e as perdas aos titulares dos dados.

REFERÊNCIAS

BARATA, André Mantola. Governança de dados em organizações brasileira: uma avaliação comparativa entre os benefícios previstos na literatura e os obtidos pelas organizações. 2015. Dissertação (Mestrado em Sistema de Informação) - Universidade de São Paulo, São Paulo, 2015.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, [2022]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 15 abr. 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidente da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 abr. 2023.

BERTOCCELLI, Rodrigo de Pinho. Compliance. In: CARVALHO, André Castro et. al. Manual de compliance. Rio de Janeiro: Forense, 2019. p. 35.

CANDELORO, Ana Paula; RIZZO, Maria Balbina Martins De; PINHO, Vinícius (Coord). Compliance 360: riscos, estratégias, conflitos e vaidades no mundo corporativo. São Paulo: Trevisan, 2012.

CARVALHO, A. P. Proposta de um framework de compliance à Lei Geral de Proteção a Dados Pessoais (LGPD): um estudo de caso para prevenção a fraude no contexto de big data. 2021. Dissertação (Mestrado em Engenharia Elétrica) - Universidade de Brasília, Brasília, 2021.

CARVALHO, Andre Castro. Manual de compliance. 3. ed. Rio de Janeiro: Forense, 2021.

CASAES, Júlio César Costa. Governança de dados abertos governamentais: frameworks conceitual para as Universidades Federais, baseada em uma visão sistemática, 2019. Tese (Doutorado em Engenharia e Gestão do Conhecimento). Universidade Federal de Santa Catarina, Florinaóplis, 2019.

DATA GOVERNANCE INSTITUTE (DGI). Definitions of data governance. 2017. Disponível em: http://www.datagovernance.com/adg_data_governance_definition. Acesso em: 01 mai. 2023.

ENDEAVOR DO BRASIL. Prevenindo com o Compliance para não remediar com o caixa. In: ENDEAVOR. [S. l.], 26 abr. 2017. Disponível em: https://endeavor.org.br/pessoas/compliance/. Acesso em: 15 mar. 2023.

ESPÍNDOLA, P. L.; SALM JUNIOR, J. F.; ROSA, F.; JULIANI, J. P. Governança de dados aplicada à ciência da informação: análise de um sistema de dados científicos para a área da saúde. Revista Digital de Biblioteconomia & Ciência da Informação, Campinas, v. 16, n. 3, p. 274-298, 2018.

FERNANDES, Aguinaldo Aragon; DE ABREU, Vladimir Ferraz. Implantando a governança de TI: da estratégia à gestão de processos e serviços. 4. Ed. Rio de Janeiro: Brasport, 2014.

FRAZÃO, Ana. Programas de compliance e critérios de responsabilização de pessoas jurídicas por ilícitos administrativos. In: ROSSETTI, Maristela Abla; PITTA, Andre Grunspun. Governança corporativa: avanços e retrocessos. São Paulo: Quartier Latin, 2007. p. 42

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. A Lei Geral de proteção de Dados Pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

HONÓRIO, Roseli. Modelo conceitual de governança de dados como suporte à governança do conhecimento organizacional. 2022. Dissertação (Mestrado em Engenharia e Gestão do Conhecimento) - Universidade Federal de Santa Catarina, Florianópolis, 2022.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC). Guia das melhores práticas de governança para cooperativas. São Paulo, 2015. Disponível em http://www.ibgc.org.br/ userfiles/files/2014/files/CMPGPT.pdf

JOHNSON, Ralph E.; RUSSO, Vincent. Reusing object-oriented designs. Relatório Técnico da Universidade de Illinois, UIUCDCS 91-1696, 1991.

KLEINDIENST, Ana Cristina. Grandes temas do direito brasileiro: compliance. São Paulo: Almedina Brasil, 2019

KOEPSEL, Alice de Medeiros. Adoção e efeitos dos programas de compliance à luz da Lei Geral de Proteção de Dados Pessoais. 2020. Monografia (Graduação em Direito) -Universidade do Sul de Santa Catarina, Florianópolis, 2020.

LIMA, C., BASTOS, R. C. A criação de conhecimento apoiada pela governança de dados. In: CONGRESSO INTERNACIONAL DE CONHECIMENTO E INOVAÇÃO, 2019, Santa Catarina. Anais eletrônicos [...]. Santa Catarina Disponível em: https://proceeding.ciki.ufsc.br/index.php/ciki/article/view/647. Acesso em 10 Mar. 2023.

MARTIGNAGO, Deisi et al. Governança de dados aplicado no processo de catalogação. Revista Brasileira de Biblioteconomia e Documentação, São Paulo, V.15, n. 2, 2019.

MENDES, Gilmar Ferreira. Curso de direito constitucional. 2. ed. São Paulo: Saraiva, 2008.

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. São Paulo: Revista de Direito do Consumidor, 2018.

NASCIMENTO, Suellen Lima do. A lei Geral de Dados Pessoais e a Adoção dos Programas de compliance na sociedade da Informação. 2020. Monografia (Graduação em Direito) - Centro Universitário de Brasília, Brasília, 2020.

PESSOA, Larissa Rocha de Paula. Os desafios da Governança de dados e a realidade cultural brasileira. 2021. Dissertação (Mestrado em Direito) ? Universidade Federal do Ceará, Fortaleza, 2021.

PINTO, S. C. C. S.. Composição em Web Frameworks, 2000. Tese (Doutorado em Informática) Pontifícia Universidade Católica do Rio de Janeiro, Rio Janeiro, 2000.

PROSSER, William L. Privacy. California Law Review. California, v. 48, n. 3. p. 383 ? 423, agosto, 1960.

RÊGO, Bergson Lopes. Gestão e governança de dados: promovendo dados como ativo de valor nas empresas. 1. ed. Rio de Janeiro: Brasport, 2013,

ROQUE, Pamela Romeu. Estudos aplicados de direito empresarial: LL.C. em direito empresarial. São Paulo: Almedina, 2019.

SAAD, Carolina de Oliveira. A lei geral de proteção de dados pessoais e incidentes de segurança: regulação e prática de vazamento de dados, 2021. Monografia (Graduação em Direito). Fundação Getúlio Vargas. Rio de Janeiro, 2021.

SANTANA, Ricardo Cesar Gonçalves. Ciclo de vida dos dados e o papel da ciência da informação. In: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO. 14., 2013. Florianópolis. [?]. Florianópolis: UFSC, 2013. Disponível em: http://enancib2013.ufsc.br/index.php/enancib2013/%20XIVenancib/paper/viewFile/284/319. Acesso em: 13 mar. 2023.

SILVA, Ana Laura Fonseca. O papel das Soft Skills na implementação efetiva dos programas de compliance com foco na adequação à Lei Geral de Proteção de Dados ? Lei N° 13.709/18. 2022. Monografia (Graduação em Direito) - Universidade Federal de Ouro Preto, Ouro Preto. 2022

SILVA, Eggon João da. A defesa da ética e transparência. In: VENTURA, Luciano Carvalho. Governança corporativa. São Paulo: Saint Paul Editora, 2005, página 259.

TERRA, Priscila de Mello. A influência da governança de dados na gestão estratégica, 2017. Monografia (Bacharelado em Sistema de Informação) - Universidade Federal Fluminense, Niterói, 2017.

VAZAMENTO de dados aumentaram 493% no Brasil, segundo pesquisa do MIT.VEJA, São Paulo, 24 fev. 2021. Sociedade. Disponível em: https://vocesa.abril.com.br/sociedade/vazamentos-de-dados-aumentaram-493-no-brasil-segundo-pesquisa-do-mit. Acesso em: 15 mar. 2023.

VIEIRA, Tatiana Malta. O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante da tecnologia da informação. Porto Alegre: Sergio Antonio Fabris Editor, 2007.

==========

Arquivo 1: TCC - A IMPORTÂNCIA DO COMPLIANCE NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA - WESLEY VICENTE.pdf (8805 termos)
Arquivo 2: https://investorplace.com/stock-quotes/www-stock-quote (926 termos)
Termos comuns: 0
Similaridade: 0,00%
O texto abaixo é o conteúdo do documento TCC - A IMPORTÂNCIA DO COMPLIANCE NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA - WESLEY VICENTE.pdf (8805 termos)
Os termos em vermelho foram encontrados no documento https://investorplace.com/stock-quotes/www-stock-quote (926 termos)

==========

WESLEY VICENTE DA SILVA

A IMPORTÂNCIA DO COMPLIANCE EMPRESARIAL NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA

SALVADOR
2023

WESLEY VICENTE DA SILVA

A IMPORTÂNCIA DO COMPLIANCE EMPRESARIAL NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA

Artigo apresentado como requisito parcial para obtenção do título de Bacharel em Direito pela Universidade Católica do Salvador.

Orientador: Prof. Darlã Conceição Santos.

SALVADOR
2023

A IMPORTÂNCIA DO COMPLIANCE EMPRESARIAL NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA

Wesley Vicente da Silva1
Darlã Conceição Santos2

RESUMO: No cenário de exploração das informações como mercadoria econômica, os dados pessoais coletados por empresas privadas tornaram-se fator de tutela legislativa. Assim, surgiu a necessidade de organizar os setores privados para adequar aos moldes da Lei Geral de Proteção de Dados Pessoais ? LGPD, com o intuito de proteger a privacidade, como direito autônomo e fundamental para a tutela da pessoa humana, destacando os programas de compliance aliados as boas práticas e governança de dados. Nesse contexto, a fim de consolidar os mecanismos técnicos de segurança para a efetividade da legislação com a finalidade de mitigar os casos de vazamento de dados pessoais, a LGPD implementou medidas administrativas para inibir incidentes decorrentes das condutas infratoras a legislação. Desse modo, este trabalho tem como objetivo demonstrar a importância dos programas de compliance para a proteção aos direitos dos titulares dos dados, visando o cumprimento do ordenamento jurídico. Valendo-se do método hipotético-dedutivo, com abordagem qualitativa, utilizando da revisão bibliográfica de livros, legislação, artigos, dissertações e teses concernente à tutela de dados pessoais no Brasil para o desenvolvimento do presente artigo.

PALAVRAS-CHAVES: Compliance Empresarial. Governança corporativa. LGPD. Vazamento

de dados.

ABSTRACT: In the scenario of exploitation of information as an economic commodity, personal data collected by private companies have become a factor of legislative protection. Thus, the need arose to organize the private sectors to conform to the General Law for the Protection of Personal Data - LGPD, in order to protect privacy, as an autonomous and fundamental right for the protection of the human person, highlighting compliance programs allied with good practices and data governance. In this context, in order to consolidate the technical security mechanisms for the effectiveness of the legislation with the purpose of mitigating cases of leakage of personal data, the LGPD implemented administrative measures to inhibit incidents arising from conducts that violate the legislation. Thus, this work aims to demonstrate the importance of compliance programs to protect the rights of data subjects, aiming at compliance with the legal system. Taking advantage of the hypothetical-deductive method, with a qualitative approach, using the bibliographic review of books, legislation, articles, dissertations and theses concerning the protection of personal data in Brazil for the development of this article.

KEYWORDS: Corporate Compliance. Corporate governance. LGPD. Data leak.

1
Discente do curso de Direito da Universidade Católica do Salvador.
2
Mestre em Direito, Docente na Universidade Católica do Salvador.

1 INTRODUÇÃO

A nova moeda de troca não é apenas aquela que podemos ver, quantificar ou converter. Os moldes do mercado financeiro mudaram, sendo em questão material ou ao produto que eles precificam, postulando um novo aparato ao objeto contratual: os dados.
Muito embora, os dados pessoais, ainda para muitos, são apenas informações deslocadas acerca de fatores específicos, atualmente, podem ser conceituados como um conjunto de indicadores, regrados por um complexo condensado de informações em um fluxo crescente tangencial.
Os dados da grande massa acabam gerando indicadores que podem ser balizados e influenciados de acordo com os detentores dessa informação, apenas apartado em blocos de informações não são considerados como vetores orçamentários. Porém, direcionados para uma finalidade ordenada tem o condão de influenciar o interesse social.
Dito isso, os mecanismos postos pelo Reino Unido para possibilitar uma estruturação normativa para organizar e gerir os dados dos indivíduos, foi crucial para a criação em outros países, como no Brasil, onde instituiu-se a Lei Geral de Proteção de Dados Pessoais (LGPD). Muito

embora, a lei brasileira trouxe um arcabouço de normas reguladoras e sanções aos casos de tratamento de dados, que não foram abarcados com o marco da internet, os dados em uma visão macro constitucional já eram de forma genérica tutelados pela Constituição Federal de 1988.
Todavia, apenas a sanção da LGPD não seria, isoladamente, capaz de coibir as violações ao tratamento de dados na esfera privada, mas sim a necessidade de uma regulamentação do ciclo de vida das informações, que além de estipular os dados que podem ser utilizados ou até quando podem ser armazenados, estabelecer expressamente no bojo da norma como deve ser a proteção na operação do tratamento de dados.
De forma efêmera, conclui-se que a legislação pode delimitar os alicerces capazes de ensejar uma fiscalização, sendo estas através de mecanismo de gerenciamento de atividades, políticas de condutas e implementação de governança de dados, pois os dados hackeados ou vazados de forma isoladas, não seria possível identificar dados sensíveis, muitos menos individualizar o sujeito.
Portanto, o gerenciamento dos dados em provedores de armazenamento pode ter os riscos reduzidos de acordo com a realização de medidas de compliance para dirimir os impactos na

atividade empresarial, como também para tutelar os dados, cada vez mais acentuado como um produto orçamentário.

2 COMPLIANCE EMPRESARIAL

A criação do compliance está entrelaçado sob o cenário econômico-social, assim, sua implementação como sistema de organização foi instaurado e aprimorado a partir dos problemas práticos estruturais para gerir uma boa governança, com intuito de assegurar a proteção e o controle que garante a qualidade do negócio.
A utilização do termo foi inicializada no mercado financeiro, especialmente após a criação do Banco Central em 1913 nos Estados Unidos da América, com a necessidade de um sistema econômico ajustável e estável. Só após 1960, com a regularização da Securities and Exchange Commission (SEC), que houve a necessidade de implementação do compliance como um programa para a integração dos procedimento, controle e monitoramento de operação interna. (CARVALHO, 2021)
Em 1977, com a Convenção Relativa à Obrigação de Diligência dos Bancos Suíços, estabeleceu os modelos auto regulatórios, com adequação de condutas e processos internos, na qual a infração tem como consequência à aplicação de sanções. (CARVALHO, 2021)
Só após esse processo de amadurecimento histórico, que o Brasil teve a necessidade de competir em escala global, implementado novos processos de segurança no sistema financeiro brasileiro.
Pode-se concluir que, após a globalização com o fenômeno da criação dos dados estruturais, houve a potencialização das informações adquiridas por meio de provedores, classificadas, atualmente, como fonte econômica de um produto quantificativo e qualitativo, ao qual possibilita uma utilização como um produto do sistema financeiro.
Nesse sentido, em decorrência de ataques cibernéticos em provedores de informações

massificadas conduziram a sociedade na aplicação de institutos de melhoramento, como o compliance e suas interfaces para proteger no ambiente corporativo os dados massificados recebidos em seus provedores.

2.1 O CONCEITO DE COMPLIANCE

Antes de enveredar sob o conceito de compliance na esfera privada, é oportuno compreender o seu significado. Nesse contexto, a palavra compliance advém do verbo inglês, to comply, que pode ser definida como conformidade. O instituto deve ser aplicado como plano principal de uma diretriz pré-estabelecida para ser dirigida a todos capazes de enfrentar a finalidade destinada. (BERTOCCELLI, 2019)
Nesse parâmetro, pode ser traduzida como:

Comply, em inglês, significa ?agir em sintonia com as regras?, o que já explica um pouquinho do termo. Compliance, em termos didáticos, significa estar absolutamente em linha com normas, controles internos e externos, além de todas as políticas e diretrizes estabelecidas para o seu negócio. (ENDEAVOR DO BRASIL, 2022, n.p)

O compliance pode-se ser definido de forma técnica como um conjunto de normas padronizadas, sob um viés ético e legal, na qual após estruturação será a matriz orientadora para o comportamento organizacional da instituição ao qual atuará no mercado, como também irá reger as atividades dos colaboradores. Dessa forma, sendo um instrumento hábil a controlar o risco de imagem, a normatização legal, chamados de riscos de compliance, as que recaem nas instituições no decorrer da sua atividade laboral. (CANDELORO, 2012).
Superada a barreira terminológica, a finalidade do compliance tem como escopo o gerenciamento adequado do risco de atividades, verificar adequadamente as normas éticas e legais, e estudar os possíveis danos tangenciais. Dessa forma, esses elementos visam a redução de perdas e danos, como também amplifica a cultura e fortalecimento corporativo nos moldes aos padrões exigidos, seja esse por lei ou na tentativa de dirimir o risco do serviço prestado.
Portanto, segundo a doutrinadora Frazão (2007, p. 42), destina-se em sua obra que o compliance é como:
(...) conjunto de ações a serem adotadas no ambiente corporativo para que se reforce anuência da empresa à legislação vigente, de modo a prevenir a ocorrência de infrações ou, já tendo ocorrido o ilícito, propiciar o imediato retorno ao contexto de normalidade e legalidade.

Nessa mesma linha de pensamento, de acordo com os autores da obra Compliance 360° (2012, n.p), referem-se o compliance a:

Um conjunto de regras, padrões, procedimentos éticos e legais que, uma vez definido e

implantado, será a linha mestra que orientará o comportamento da instituição no mercado em que atua, bem como as atitudes de seus funcionários; um instrumento capaz de controlar o risco de imagem e o risco legal, os chamados ?riscos de compliance?, a que se sujeitam as instituições no curso de suas atividades.

Pode-se concluir que o conceito de compliance, em uma esfera macro, é um aglomerado de regras pré-estabelecidas através de um instrumento perpetuado por técnica de desenvolvimento, capaz de dirimir riscos e danos das atividades devolvidas pelo plano diretor.
Muito embora, o instituto "compliance" tem uma definição extensiva e não tem como fim apenas o cumprimento da legislação e de condutas éticas, pode ser compreendida também como um instrumento de diminuição de riscos, desenvolvimento corporativo sustentável e subsequentes segmentos empresariais de negócio. (ROQUE, 2019)
O compliance além de estar associado tradicionalmente a uma perspectiva organizacional aos comandos administrativos, pode ser vinculada também a uma visão de uma sociedade digital 4.0, devendo não só apresentar o compliance empresarial na esfera de redução de risco à imagem, mas sim, em uma abordagem de pré-orientação e implementação de desenvolvimento aos moldes legislativo de proteção aos dados, como objeto principal de estudos.
Portanto, é necessário a elaboração do projeto de compliance em uma visão lógica, a modo de compreender os objetivos e os componentes da aplicação do programa. Posteriormente, superado os obstáculos, aplica-se os estudos de riscos a boa governança corporativa com a implementação de programas de governança de dados objetivando auxiliar o controle de informações em conformidade aos padrões da corporação, e mitigar os danos da empresa.

2.1.1 AS GOVERNANÇAS CORPORATIVAS E A IMPLEMENTAÇÃO DOS PROGRAMAS DE COMPLIANCE

Em linhas gerais, o Instituto Brasileiro de Governança Corporativa ? IBGC (2015, n.p) discrimina o conceito de Governança Corporativa, como: ?Sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas. ?
O sistema da governança corporativa está associado ao desenvolvimento interno de uma empresa, seja ele entre a administração, sócios e funcionários, capaz de criar elos para uma estruturação de direção racional e acima de tudo nos moldes da ética e legislação.
Muito embora, a governança corporativa e o compliance sejam institutos que se assemelham em uma visão macro, os mesmos, diferenciam na aplicação prática, mas se complementam no objetivo final, sendo um instrumento para aplicação do outro.

A prática da governança corporativa, além de estimular o valor empresarial, pode-se concluir que estrutura de forma adequada a medida necessária para organizar a atividade empresarial, assim, não há que se falar em condutas prejudiciais. Por exemplo: empresários compreendem que para realizar uma instrumentalização segura aos seus sócios e administradores tendem a prejudicar o negócio empresarial, assim o autor Eggon João da Silva (2005, p.259) retrata que: ?A governança corporativa assegura tratamento equânime a todos os acionistas, inclusive minoritários, preferencialistas, nacionais e estrangeiros. Todos devem ter oportunidade de reparação caso venham a sofrer violação de seus diretores. ?

Nesse passo, as críticas ao sistema não são viáveis, tendo em vista a utilização de instrumento capaz de integralizar ao plano empresarial. Sendo assim, o programa de compliance visa amplificar a utilização de um sistema para garantir que todos possam participar de forma justa sob o aspecto legal, seja sócio ou administrador.

Em uma tangente geral, a implementação da governança corporativa ressoa em uma perspectiva segura, tanto internamente, seja auxiliando as avaliações das atividades executadas pelos sócios/administradores, quanto externamente, em relação à imagem da empresa, sendo este um fator primordial a empresas estruturadas no mercado.

A implementação da governança corporativa deve ser estruturada de acordo com as necessidades da empresa, devendo verificar o histórico de desenvolvimento do estabelecimento, pois, só a partir do status da empresa pode-se delimitar a estratégia possível para uma implementação segura e adequada. Sendo assim, um regramento mais rigoroso pode gerar consequências negativas e ineficazes, especificamente em estágios primários, pois em atividades inicias, as tomadas de decisões e a execução da atividade empresarial é primordial, sendo necessário, um aspecto negocial informal para realizar os objetivos da empresa, o que não se verifica quando existe prática de boa governança devidamente estruturadas no negócio. (KLEINDIENST, 2019)

Ao desenvolver da atividade da empresa, além da atenção a organização interna, sendo está um fator primordial da governança, ainda que no fim acabe tendo um aspecto externo por vislumbrar no mercado financeiro uma maior complexidade da entidade. O desenvolvimento da empresa, seja no faturamento, importação comercial, quantidade de funcionários, além dos controles a observância da legislação e regras internas, tendem à serem complexos, e, que necessita de ações maiores que a própria instituição empresarial, restando necessária a implementação de sistema organizacionais aos fluxos de informações. (KLEINDIENST, 2019)

Ultrapassado a esfera conceitual e instrumentalização da política de boas práticas de governança, cabe pontuar que as empresas que possuem fluxos de informações sensíveis, conforme estipula o artigo 50 da Lei Geral de Proteção de Dados Pessoais, os controladores e operadores são responsáveis pelo tratamento de dados, devendo criar planos de adequação a legislação.

Assim, ao confeccionar as regras de boas práticas, os controladores adjuntos com a administração devem estipular através da análise da natureza dos dados coletados, a probabilidade, a finalidade e o potencial de riscos das vantagens advindas dos tratamentos dos dados verificados. (NASCIMENTO, 2020)

É necessário pontuar que, os agentes de tratamento, após a autenticação da gravidade e sensibilidade dos dados aos riscos de operação, poderão estabelecer programa de governança em privacidade, sendo este, um instrumento amplo com normas de compliance, além dos aspectos operacionais.
Em relação ao programa de governança de privacidade, pode-se estabelecer como um aglomerado de normas-regras de boas práticas de governança, com a finalidade de executar ordens de natureza legal. (NASCIMENTO, 2020)
Portanto, os instrumentos do compliance em conjunto com a boa prática de governança, se consagram na identificação dos riscos e estruturação de medidas para a empresa, sendo respondida de forma adequada e proporcional ao suporte da tomada de decisão.
O Programa de compliance na esfera privada para análise de dados pessoais, com a finalidade de promover a segurança, deve ser constantemente monitorado e atualizado, com a implementação de ?salva vidas? em decorrência de avaliação de riscos à privacidade e o acometimento de vazamentos. (NASCIMENTO, 2020)
Portanto, os instrumentos e objetos referenciados demonstram a determinação de regras de governança no ambiente de operação de tratamento de dados pessoais, a modo que seja realizado uma estruturação nas empresas para que possibilitem a implementação de mecanismos de segurança, com a finalidade de dirimir os riscos da atividade empresarial na sociedade digital.

3 GOVERNANÇA DE DADOS

O mercado digital tem como principal ativo financeiro os dados, este considerado como ?matéria prima? de uma economia baseada no conjunto de informações, sendo que nos últimos anos, houve um aumento exponencial na coleta de dados por cooperativas, startups e novos nichos empresariais, tendo a finalidade de quantificar e gerencias os dados.
Dados, informações, conhecimento e sabedoria são os quatros estágios evolutivos da cadeia de informação, pode-se assim, compreender os dados como fatos ou registros em seu formato primário. (BEAL, 2014). Já a informação é entendida como os conjuntos processados de dados em um contexto aplicado (RÊGO, 2013). Muito embora, na sociedade da informação ?os dados são o novo petróleo?, apenas os dados isoladamente não são capazes de transformar em ativo financeiro, sendo necessário administrá-lo de forma eficaz, para que assim, as empresas adquiram vantagem competitiva.
Dessa forma, a governança de dados tem como principal objetivo atender as necessidades das empresas, ou seja, solucionar problemas, diminuir custos da administração, para que os dados transformem em saldo positivo para os negócios (TERRA, 2017).
O Data Governance Institute -DGI (2017, n.p) definiu governança de dados como ?um sistema de direitos de decisão e responsabilidades para processos relacionados à informação, executado de acordo com modelos acordados que descrevem quem pode realizar quais ações com quais informações e quando. ? Portanto, a utilização da governança de dados orienta quais os métodos deverão ser aplicados no ciclo de vida dos dados.

Uma das atribuições da governança é o acompanhamento da operação dos dados com a finalidade de gerir que as informações estejam alinhadas com os objetivos pré-determinados na coleta primária, além disso, é necessário assegurar que as informações estejam disponíveis para acesso, quando consultadas, gozar de qualidade, consistência, auditabilidade e segurança dos dados (ESPÍNDOLA, 2018).

No âmago da cadeia evolutiva da informação uma das preocupações dentro das organizações corporativas é o receio com a proteção das informações, ou seja, a capacidade das empresas no protagonismo da segurança com os provedores internos, tendo em vista a necessidade de conformidade com a legislação pátria.

A boa governança tem como objetivo aplicável à prática do controle dos processos de operação dos dados: a prevenção de situações adversas que podem gerar o comprometimento da integralidade dos dados adquiridos pelas organizações empresariais, que por sua vez, devem ter o condão de reforçar a confidencialidade das informações. (ESPÍNDOLA, 2018).

A integração do programa de governança de dados nas corporativas empresariais, tem como o esforço principal a organização de dados, que deve ser observado por um prisma basilar, ou seja, a aplicação dos princípios como limite legal e ético no ciclo de vida dos dados.

Para Rêgo (2013), os princípios são regulamentações para compreender aplicação da governança dos dados como linha direta para os negócios, sendo: (i) A gestão de dados estratégicos, tem o dever de vislumbrar as tomadas decisões por um coeficiente tático e operacional. (ii) A governança como instituição, ou seja, a governança de dados pode ser comparada como sistema governamental, na qual dispõe de legislação, execução e jurisdição; (iii) A governança de dados como um programa, devendo ser implementado como fator permanente, não apenas um projeto temporário. Ainda, pontua-se que os princípios da Governança de dados não são limitados, tendo uma orientação basilar a cada implementação de um sistema organizacional que deve ser observado pelo prisma ético e legal.

Assim, os princípios devem incumbir os papéis que a serem preenchidos pela gestão moldar os comportamentos das empresas para a aquisição, reserva e utilização dos dados conforme as normas e políticas da corporação (TERRA, 2017).

Coleta, armazenamento, recuperação e descartes, são as quatro etapas do ciclo de vida dos dados (SANTANA, 2013), ou seja, para a aquisição de dados pelas empresas, deverão observar a vida útil do dado para não incorrer na (in) responsabilidade da utilização indevida de informações dos seus provedores.

As fases do ciclo de vida dos dados devem ser observadas pela ótica de seis objetivos, sendo eles: a qualidade, a privacidade, os direitos autorais, a integração, compartilhamento e preservação dos dados (ESPÍNDOLA, 2018). Muito embora, a lei geral de proteção de dados implementou e traçou novos objetivos para a coleta de dados pessoais, cabe destacar que os objetivos vislumbrados na Governança de dados têm como parâmetro preliminar a tomada de decisão, na qual deve ser os negócios pautados nos moldes legais e éticos vigentes.

Nesse contexto, o controle de informações é necessário, tendo em vista que na sociedade da informação, cada vez mais o volume de dados é crescente, acarretando mais vazão e protesto

por políticas públicas para a preservação dos institutos, órgãos e empresas que detenham a

informação, sendo assim, necessário sistema de organização, softwares e hardwares capazes de processar as informações, criptografar e armazenar. (MARTIGNAGO, 2019)
Assim, para otimizar o ciclo de vida dos dados e garantir que os objetivos sejam preenchidos na estruturação do gerenciamento de dados, faz-se necessário a implementação de frameworks com o intuito de garantir que o procedimento seja cumprido com maior qualidade de informação e aproveitamento financeiro para a empresa, auxiliando a tomada de decisão para redução de risco para utilização de dados. (MARTIGNAGO, 2019)
Um Framework, segundo Johnson (1991), pode ser definida como um aglomerado de objetos que colabora entre si para que atinja um conjunto de obrigações para aplicação de um domínio especifico. Já para Pinto (2000), um framework é conceituado como um software incompleto criado para ser um objeto cujo estado e comportamento são definidos pela classe. Assim, o framework é uma concepção de uma arquitetura para um edifício de subsistemas e oferece o alicerce básico para criá-los.
Muito embora, os autores defendem uma conceituação distintas acerca da concepção de frameworks, pode-se verificar que ambas se complementam, tendo em vista que o framework é um sistema pré moldado, ou seja, é um programa com intuito de ser complementado através da finalidade a ser cumprida pela gestão empresarial, sendo instanciado por classes para categorizar os dados e ser alojado em hotspot, provedores físicos, capazes de armazenar as informações coletadas pelas empresas.
Portanto, para gerenciar os ativos de dados de forma complexa, ordenada e objetiva é necessário para proteção do procedimento do ciclo de vida dos dados, determinar os modelos de frameworks para o gerenciamento dos dados. Assim, para Carvalho (2021), podem ser apresentados três domínios CobiT, DAMA DMBOK e DGI Framework, sendo apenas dois destes observados para fomento deste artigo: (i) A DAMA (DAMA DMBOK), e (ii) CobiT.
A DAMA (Data Management Association) é uma associação sem fins lucrativos, com o intuito de promover boas práticas de gestão de dados, e em 2009 fundou o DAMA-DMBoK (Data Management Body of Knowledge), sendo um corpo de conhecimento que tem como ponto fundamental esclarecer como as corporativas devem aplicar a operação otimizada dos dados. (CARVALHO, 2021)
Em sua versão 2.0, acrescenta não só uma visão macro do gerenciamento de dados, definindo padrões, terminologias e práticas, mas a integração de dados, para definir táticas,

armazenamentos e sistemas, bem como implementação da ética na operação do tratamento de dados, a definição de big data e ciência de dados e amadurecimento das informações. (LIMA, 2019).
O DAMA-DMBOK V2 é formado por 11 (onze) funções de gestão de organização de

dados, sendo incorporado como cerne principal: a governança de dados, tendo em vista que os dados percorrem por toda sistemática das onzes funções ordenadas, assim segundo Honório (2021):
A primeira função é a governa de dados, sendo o pilar do framework, tem o condão de orientar e supervisionar a operação do ciclo de vida dos dados, na qual deve estabelecer um sistema de apoio a decisão dos gestores sobre os dados, sob o prisma do negócio.
A arquitetura de dados, a segunda função, pode ser conceituada como um planejamento para administrar os dados, aquisição de ativos da empresa, com o intuito de definir a finalidade das informações adquiridas com os requisitos necessário para o gerenciamento dos dados.
Por sua vez, a modelagem de dados e design, tem a função de demonstrar de forma nítida os dados, sendo o processo da descoberta, análise e representação da etapa primária da informação.
O armazenamento, uma das etapas da operação do ciclo de vida dos dados, na qual vai incluir o design, o suporte dos dados armazenados para quantificar o coeficiente valorativo das informações, até o seu descarte, devendo respeitar todo o procedimento de segurança legal vigente.
Um dos alicerces para o gerenciamento de informação é a segurança, que deve garantir a proteção dos dados, a execução de políticas e procedimento de segurança, no intuito de moderar o acesso de forma consciente e controlado, não devendo ser infringido ou acessado de forma inadequada, afim de garantir autenticação e auditoria de dados informações.
A Integração e Interoperabilidade de dados, é a função responsável pela movimentação e a concretização dos dados na interligação do armazenamento e outras plataformas.
O gerenciamento de documentos, pode ser compreendida como o gerenciamento e inclusão da vida útil dos dados e informações, encontrados em programas não estruturados, em ênfase ao conteúdo de apoio de conformidade a legislação vigente e os termos éticos formalizados para o negócio.
Dados mestre e de referência, tem como condão a manutenção dos dados compartilhados para coexistir a integralidade dos sistemas internos de gerenciamento dos dados.
Em razão da interligação entre uma linha direta com os negócios, uma das funções do DAMA-DMBOK é a Data warehousing e Business intelligence, ou seja, a implementação de

planner para o contoler da administração dos dados e suporte a decisão com o intuito de conceder aos gestores de informação emitam relatórios de equalização de valores.
Segundo Barata (2015), os metadados, na qual consiste a décima função, é promover a facilitação do acesso dos dados interligados nas multifontes do sistema integrado, como também garantir a qualidade de dados.
Por fim, o gerenciamento de qualidade de dados é a implicação das técnicas para garantir a possibilidade de aferição, melhoramento e adequação da utilidade dos dados, com o intuito de monitorar a integridade da informação primária no ciclo de vida dos dados.
Já o COBIT (Control Objectives for Information and related Technology), é um framework de suporte fundado em 1994 administrado pela ISACA (Information Systems Audit and Control Association), estruturado como um arcabouço de informação direcionadas para governança de dados e gerenciamento de informação, tem como objetivo auxiliar os profissionais de gestão na conexão entre os problemas técnicos e os riscos do negócio. (BARATA, 2015).

Para Lima (2019), o COBIT é um framework que possui duas vertentes basilares: a gestão, que possui quatro áreas de domínios: planejamento, constituição, execução e monitoramento, e a governança que é a tomada de decisão de acordo com a gestão de dados, possuindo 37 (trinte e sete) processos integrados.
Na versão 5.0, o sistema é utilizado baseado em 05 princípio, conforme elucida Casaes (2019), Barata (2015) e Lima (2019), sendo: (i) atender às necessidades das partes interessadas; (ii) cobrir o negócio como um todo; (iii) aplicar um framework único e integrado; (iv) habilitar uma visão holística; e (v) distinção entre governança de gestão.
Um dos princípios é atender às necessidades das partes interessadas, sendo a necessidade das corporativas é satisfazer as expectativas dos seus stakeholders, proporcionando um equilíbrio na tripartite: benefícios, redução do risco e recurso disponíveis.
O segundo princípio é baseado na cobertura do negócio como um todo, ou seja, abranger a integralidade da empresa no processo, procedimento, pessoas e as relações com os habilitadores.
A aplicação do framework único e integrado, assim, o COBIT é capaz de promover uma relação completa com a Governança de dados, corroborando ao alinhamento com padrões externos e adaptabilidade dos modelos usuais de negócios.

O COBIT permite habilitar uma visão holística, ou seja, uma visão macro dos componentes que oferecem suporte para atingir as finalidades da governança de dados, na qual define como catalogadores: as políticas, processos, estruturas organizacionais, informação e ética.
Por derradeiro, o princípio da distinção entre governança de gestão, tendo em vista que ambos possuem estruturas organizacionais distintas, assim, governança tem como esforço principal que os objetivos corporativos sejam cumpridos, estabelecendo prioridades pela tomada de decisão, compliance e progresso das organizações. Por sua vez, a gestão é o planejamento, construção, execução e monitoramento das funções ornamentada com o direcionamento da governança.
Desse modo, com escalonamento dos cinco princípios é capaz de proporcionar o funcionamento otimizado do framework, destacando os seguintes processos:
O APO01: Gerenciar o framework de TI, tem como condição a otimização das atividades relacionadas ao TI, com a função principal de incluir os procedimentos e regulamentos para promover a integralidade das informações nos bancos de dados. (BARATA, 2015)
Já o APO03: Gerenciar a arquitetura corporativa, tem função primordial agrupar as informações para auxiliar as atividades e tomadas de decisões, conceituando e compartilhando as informações dos elementos dos dados, e por fim catalogar a empresa, com base na modulação e sensibilidade dos dados. (BARATA, 2015)
Nesse ínterim, a governança de dados como um sistema integrado com o programa de compliance, tem o condão de otimizar a operação de controle interno relacionado aos dados coletados pelas empresas, capaz de gerenciar as bases para o apoio de decisão ao tratamento das informações, com segurança e qualidade, garantido o ciclo da vida útil dos dados.

4 A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

As estruturas políticas, econômicas e sociais com desenvolvimento de novas tecnologias e mecanismo para a coleta de dados e informações, fez necessário modulações legislativas para a proteção da privacidade, além dos aspectos físicos, patrimoniais e morais.
A proteção à privacidade de dados foi dividida em quatros gerações: a primeira, oriunda do estado moderno, com o advento dos bancos de dados; a segunda, datada em 1980, com a expansão legislativa para a proteção à privacidade aos setores privados; a terceira geração em 1990, com o processo de tratamento de dados e o consentimento dos cidadãos; Por fim, a última dimensão, é

destinada ao protagonismo da permissão para coleta e uso dos dados pessoais, quando a lei estabeleceu a importância da titularidade das informações. (MENDES, 2014)
Nesse aspecto, é perceptível a evolução do direito aos fatores reais da sociedade e as transformações dos meios tecnológico, computacionais, genéticos e comunicativos, que por sua vez possibilitou a integração da comunicação global, e consequentemente, o rastreio dos dados através do armazenamento de informação. (SAAD, 2021).
Os legisladores ao considerar os dados pessoais como extensão ao direito à privacidade, preocuparam em tutelar constitucionalmente a proteção da população, em especial os países europeus, como: Espanha, Portugal, Hungria, Eslovênia e Rússia. (VIEIRA, 2007) Porém, só tornou-se fator primordial após o regulamento geral do Parlamento Europeu sobre a proteção de dados, n.º 2016/679, sendo necessário a adequação das empresas prestadoras de serviço na Europa ao regulamento, influenciado diretamente o Brasil para elaboração da Lei Geral de Proteção de Dados brasileira. (SAAD, 2021).
Muito embora, a Lei Geral de Proteção de Dados Pessoais - LGPD, em sua promulgação, não abarcou de forma expressa a proteção de dados como direito fundamental, a doutrina, em especial Nascimento (2020), por sua vez, já argumentava a proteção de dados e informações pessoais como direito autônomo, derivado do direito fundamental à privacidade, explicitamente no artigo 5°, X, da CRFB de 1988.
Após reiterados julgamento sobre a tutela dos dados pessoais como extensão da personalidade do indivíduo, o Supremo Tribunal Federal -STF reconheceu no Julgamento da Ação Direta de Inconstitucionalidade - ADI 6387, a existência dos dados como direito autônomo, derivada do direito fundamental a dignidade da pessoa humana, na proteção à intimidade e a centralidade do Habeas Data como autodeterminação informativa. (NASCIMENTO, 2020).
Ao compreender a necessidade da proteção aos dados pessoais, os legisladores brasileiros em votação de ? das casas legislativas (câmara e Senado Federal) em dois turnos, aprovaram a Emenda Constitucional 115 de fevereiro de 2022, alterando o artigo 5° da Constituição Federal de 1988, incluindo o inciso LXXIX, tutelando constitucionalmente a proteção aos dados pessoais, inclusive nos meios digitais.
Ressalta-se, ainda, que os dados pessoais estão interligados com o direto fundamental à privacidade, na qual representa a capacidade de a pessoa administrar sua vida, seus pertences e

propriedades materiais e imateriais, permitindo ou não a utilização dos seus dados (bens imateriais) por terceiro. (NASCIMENTO, 2020).

A privacidade, por sua vez, segundo Mendes (2008), é o direito à proteção aos comportamentos pessoais e acontecimentos de caráter íntimo, bem como as informações prestadas aos profissionais e comerciantes, em que a pessoa não deseja que se compartilhe com o público.

Para o professor William Prosser, pode-se qualificar a lesão a privacidade em quatro graus: i) o intrometimento na reclusão ou solidão na vida privada, ii) a divulgação pública de fatos privados constrangedores sobre o indivíduo; iii) a publicidade sobre o indivíduo apresentada de forma equivocada; e iv) a apropriação, para obtenção de vantagem, do nome ou da imagem do demandante (PROSSER, 1960).

A doutrina, por sua vez, defende mais uma violação à privacidade: a privacidade informacional, interligada com os fatores tecnológicos de informação. (SAAD, 2021). Assim, quando a lei ao realizar o tratamento da privacidade, refere-se como um direito líquido, ao qual será tutelado para garantir que o indivíduo tenha um local reservado, que não tenha, se desejar, a interferência de outros sujeitos, seja pessoa física ou jurídica.

Com a proteção dos dados pessoais dos titulares, através da LGPD, possibilitou ao cidadão o acesso a informações ao ciclo de vida útil dos dados pelas empresas, e a certeza de fiscalização pela Autoridade Nacional de Proteção de Dados, com a finalidade de atingir os objetivos traçados pela legislação, na qual a lei traz conceitos e delimita princípios, que devem ser mencionados.

A LGPD tem como objetivo principal: ?o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado?, com a destinação de assegurar os direitos fundamentais a liberdade e privacidade dos titulares dos dados, bem como tutelar a dignidade e a personalidade da pessoa natural. (LGPD).

A legislação está ordenada diretamente com o meio empresarial, sobretudo no que se refere aplicação aos seus destinatários que são pessoas físicas ou jurídicas que realizam a coleta e tratamento de dados no Brasil, conforme preceitua o artigo 1° da lei 13.709, de 14 de agosto de 2018.

Para compreender a LGPD, faz-se necessário elucidar os conceitos de dados pessoais: (art. 5º, I) é toda informação relacionada a pessoa natural, identificada ou identificável, sendo o dado aplicado no contexto que possibilite o reconhecimento do indivíduo. Bem como refere-se aos dados sensíveis (art. 5º, II), são todas as informações que se relaciona com pensamentos políticos, crenças,

identidade biológica e física. Portanto, a legislação tem como ponto a proteção e o cuidado para a não violação dos dados pessoais e sensíveis.

Os doutrinadores, Laura Schertel e Danilo Doneda, ainda aponta cinco pilares para compreender a LGPD, sendo: i) a unidade e generalidade da aplicação da Lei; ii) a legitimação para o tratamento de dados (hipóteses autorizativas); iii) os princípios e direitos do titular; iv) as obrigações dos agentes de tratamento de dados e v) a responsabilização dos agentes.

O primeiro pilar é considerado com aplicabilidade material da legislação, ou seja, aplica-se a qualquer operação realizada por pessoa natural ou jurídica de direito público ou privado,

independentemente do meio, da sua sede ou do país onde estejam localizados os dados (Art. 3°). Considerado, assim, como uma aplicação uniforme para todos os setores público ou privados que realizam tratamento de dados.

O segundo pilar é a legitimação para o tratamento de dados, tendo em vista que a lei especificou critérios e requisitos para o reconhecimento da legitimidade, não podendo ser tratados os dados, sem que exista uma base normativa que autorize, prevista no artigo 7°, 11° ou 23° da LGPD, abordando 11 (onze) hipóteses, incluído o consentimento ou a previsão legislativa.

Destaca-se que a autorização por consentimento para ser considerado válido, deve observar os requisitos previsto no artigo 5°, XII, sendo considerado que a vontade deve ser livre, informada, inequívoca e com a finalidade determinada, consagrando os princípios norteadores da legislação.

O terceiro pilar é o conjunto de princípios e direitos que assegura o destinatário da lei a controlar a utilização do seu dado pessoal, sendo importante elencar dez princípios que estruturam a LGPD: a finalidade, a adequação, a necessidade, o livre acesso, a qualidade dos dados, a transparência, a segurança, a prevenção, a não discriminação e a responsabilização. (MENDES, DONEDA, 2018)

No que concerne, aos direitos dos titulares são expressos no artigo 18° da referida lei, que permite o titular dos dados adquirir através do controler, independentemente do momento, as informações relacionadas ao indivíduo, prevendo: acesso, confirmação, correção, anonimização, bloqueou ou eliminação e a portabilidade.

Para adentrar no cerne dos problemas enfrentados pela legislação, em especial, sobre o vazamento de dados, os dois últimos pilares serão abordados sob a perspectiva da violação e responsabilização acerca da proteção de dados nos casos incidentes de vazamento.

Assim, o quarto pilar, destina-se às obrigações dos agentes de tratamento dos dados, na qual estabeleceu limites que devem ser observados nas operações realizadas para reforçar a segurança e prevenir os problemas da atividade no tratamento de dados.

Uma das obrigações fundamentais, consiste na intitulação do encarregado pelo tratamento dos dados indicados pelo controlador, conforme artigo 41 da LGPD, que possui a função de aceitar as reclamações e comunicações dos sujeitos dos dados, receber informações da Autoridade Nacional, como deve orientar os funcionários a respeito das práticas a serem adotadas em relação à proteção de dados pessoais.

Assim, as informações devem ser fornecidas ao proprietário dos dados, quando os dados forem coletados, como: os meios de segurança aderidos ao tratamento de dados, quais são os riscos da atividade que podem gerar lesão ao titular, pois pode gerar a mitigação dos prejuízos. (SAAD, 2021)

A lei Geral de Proteção de Dados Pessoais tem como objetivo a proteção do dados pessoais dos titulares dos dados, sendo assim, uma das obrigações principais é adoção de medidas de segurança, técnicas e administrativas hábeis a proteger os dados pessoais de acessos não autorizados, como promover a integralidade dos dados, não permitindo, assim, a alteração das informações, a prevenção de situações ilícitas ou acidentais, ou qualquer forma de tratamento inadequado, consoante se desprende do artigo 46 da lei.

Tornou-se corriqueiro manchetes acerca do vazamento de dados por corporativas, uma das violações mais graves incidentes abarcados pela LGPD, o que ocasiona a vulnerabilidade do titular dos dados, e dos sistemas internos que são responsáveis pelo ciclo de vida útil dos dados. (SAAD,2021)

A seção de segurança de informação tem como condão as obrigações inerentes aos agentes de tratamento, devendo ser adotado pela integralidade das pessoas que realizam o tratamento de dados, garantido que os dados sejam confidenciais, bem como disponíveis nas operações de tratamento. (Art.48). Nos casos incidentais de vazamento de dados, insurge a necessidade ao controlador de informar a autoridade de proteção de dados, que podem definir as medidas para mitigação dos danos.

No entanto, com a utilização da internet, compras online, transferência virtuais e outros meios tecnológicos, criou-se uma dificuldade para atuar na segurança de dados, tendo em vista a abrangência e os domínios de redes globais, que combinados com fatores não perceptível, forma

um perfil não rastreavel capaz de ocasionar violação às diretrizes básicas da legislação, que mesmo com ações posteriores não conseguem excluir os inúmeros registros de pessoas e organizações que coletaram os dados, lesionando a confidencialidade das informações (SAAD, 2021)

Destaca-se que as obrigações aos controladores e operadores, devem ser observados desde a coleta dos dados até seu descarte, assim o artigo 46 da LGPD, introduziu o conceito de privacy by design, sendo a incorporação pelas empresas nos serviços e produtos, na qual dispõe a proteção da privacidade no centro de todo o desenvolvimento corporativo.

Embora, a legislação tenta dirimir os riscos da atividade, os prejuízos causados pelo vazamento de informações são altos, e perpassam pela inadequação do sistema de proteção, perda de credibilidade e de clientes, ocasionado uma ruptura na imagem da empresa, impossibilitando, muitas vezes de concorrer no mercado corporativo. (SAAD,2021)

Portanto, a LGPD concebeu obrigações aos agentes de tratamento de dados, para que se delimite a finalidade da utilização dos dados desde o início da concepção, devendo o controlador confeccionar relatório de impacto a privacidade, utilizando de métodos para a captação da operação do ciclo de vida dos dados, observando as mediadas adotada para aumentar a segurança e mitigar o risco do tratamento das informações, conforme artigo 3 da LGPD.

O último pilar, considerado como a responsabilidade dos agentes na incidência de ocorrência de danos derivados do tratamento de dados. A LGPD consagrou a natureza do tratamento, limitando os parâmetros ao artigo 7° da lei, nas 10 hipóteses dos incisos, vinculados a finalidade da captação dos dados, consoante prevê o artigo 6°, inciso I, II, da LGPD.

A legislação tem como regra o descarte (eliminação) dos dados ao fim do tratamento da operação (art. 16), com o intuito de mitigar os riscos presente no tratamento de dados, principalmente, no que concerne à limitação das hipóteses de tratamentos para não lesionar os direitos dos titulares.

Nos casos, em que mesmo após o término de vida útil dos dados, as empresas podem, quando permitido, armazenar dados que em situação incidentais serem objetos de violação, principalmente nos casos de vazamento, que podem ocorrer, quando não autorizados pelo titular

ou controladores, serem acessados, captados, compartilhados pela internet, para outros sujeitos ou empresas.
Assim, a Lei Geral de Proteção de dados Pessoais, em especial em seu artigo 42, dispõe que o controlador ou operador, quando realizar o exercício do tratamento de dados pessoais, vem

a ocasionar dano patrimonial, moral, individual ou coletivo em detrimento a aplicação da legislação, é obrigado a repará-lo, definindo a responsabilidade de forma objetiva.
Embora, a responsabilização objetiva não é necessária a demonstração de culpa do controlador ou operador. Faz mister esclarecer que o operador, só será responsabilizado quando os atos praticados forem contrário à legislação, ou às instruções que foram fornecidas pelo controlador. (MENDES, DONEDA, 2018)
Ainda, a legislação prevê exceções a responsabilidade objetiva (art. 43), sendo: quando o agente demonstrar que não realizou o tratamento de dados pessoais que foi atribuído, ou quando não houve violação da segurança ou a legislação, e por fim, quando for por culpa exclusiva do titular ou de terceiros.
Porém, o cenário que é vislumbrado no Brasil nos casos de vazamento de dados, é que as violações pelas instituições vêm ocorrendo, majoritariamente, sob ataques deliberados de hacker, ou falha de segurança dos controladores dos dados. (SAAD, 2021)
Dessa forma, é necessário adotar medidas para dirimir os riscos da atividade, e possibilitar o discernimento das informações acerca dos perigos de vazamento de dados, tendo em vista que a tendência é aumento significativo das violações vinculados com a crescente tecnológica. Assim, as empresas devem implementar mecanismos para a segurança das informações.

5 O COMPLIANCE EMPRESARIAL COMO INSTRUMENTO DE PROTEÇÃO DE DADOS NA ESFERA EMPRESARIAL

Em decorrência das constantes violações aos dados armazenados em provedores privados, a tutela ao direito à privacidade nos meios tecnológicos, já era pauta de debate na legislação brasileira, e já existiam mecanismos para a proteção, como: a proibição de direcionamento dos provedores em relação ao compartilhamento de dados, bem como a inibição ao monitoramento nos navegadores de internet.
Vinte e seis bilhões de dados foram vazados no Brasil em 2019, de acordo com pesquisas realizadas pelo Massachusetts Institute of Tecnology ? MIT, possibilitando a utilização de números telefônicos, score de crédito, endereço eletrônico, fotos, números de identificações e outros dados pessoais, para o cometimento de crimes cibernéticos, e a violação aos direitos dos titulares.
A utilização e uso dos dados pessoais por pessoa física ou jurídica, com sede no Brasil ou não, devem se atentar as normas gerais de proteção aos dados brasileiro, segundo Frazão, Oliva e

Abilio (2020), é a necessidade de conferir a efetividade aos direitos e prevenir a violação aos dados, através da implementação de mecanismo de compliance, como uma ferramenta capaz de promover a adequação das atividades aportadas pelas empresas.
Assim, os controladores e operadores poderão formular regras de boas práticas e governança (Art. 50), que contenha as disposições de organização interna, o regime de funcionamento, as operações, o canal de comunicação entre os encarregados e os titulares dos dados, e o procedimento de segurança.
Nessa perspectiva, considerando que a maioria das tratativas de dados perpassam por meios digitais, deve-se adotar sistema para mapear os riscos, e implementar mecanismos para minorar as vulnerabilidades apontadas pelos programas, através da alta administração, do código de ética, para proteger os dados pessoais dos titulares. (PESSOA, 2021)
Existem inúmeras formas de ocorrer o vazamento de dados, sendo através de ataques cibernéticos, sequestro de conta, furtos de dados, compartilhamento de dados por agentes ou ex-agentes da empresa, erro ou negligência, entre outros, que podem ser para adquirir dados de nomes, CPF, celulares, endereços, dados financeiros, senhas, registro de saúde ou credenciais de acesso. (SAAD, 2021)
Desse modo, para realizar o mapeamento dos problemas que as corporativas podem enfrentar, é necessário identificar os fluxos e processos de informação que percorrem os sistemas, que irão auxiliar na tomada de decisão pelas empresas. (NASCIMENTO, 2020)
A alta administração deverá colaborar ativamente no programa de compliance, seja monitorando as investigações e intervenções em situação para estabelecer controles internos em conformidade com a legislação, bem como possibilitar a interdependência dos setores para realizar as atividades designadas para o tratamento de dados (PESSOA, 2021).
Com a elaboração do código de ética pela organização possibilitará o treinamento regular das equipes, responsáveis pela tecnologia da informação, para enraizar a cultura corporativa da boa governança, com a finalidade de assegurar o respeito ao programa de compliance (NASCIMENTO, 2020)
Nesse contexto, para manter uma boa relação com seus clientes, as organizações devem instalar canais de comunicação, para que os titulares dos dados possam contatar os encarregados responsáveis pelos armazenamentos dos seus dados, e exerçam seus direitos sobre as informações contidas nos provedores. (PESSOA, 2021).

Desse modo, quando se trata de concretização a alteração cultural coportariva é preciso realizar o alinhamento dos funcionários com o código de ética, com política de privacidade, para fins de efetividade do programa de compliance de dados. (PESSOA, 2021).

5.1 A IMPLEMENTAÇÃO DE MECANISMOS DE GOVERNANÇA DE DADOS PESSOAIS

Para a efetividade da legislação em relação ao tratamento de dados, a LGPD direciona um capítulo para implementar o programa de governança em privacidade, com a finalidade das empresas adotarem medidas técnicas, para fins de proteção e segurança dos dados pessoais.

(PESSOA, 2021)
A governança em privacidade, pode ser conceituada como um conjunto de regras e práticas positivas a serem implementadas pelos agentes de tratamento, e encontra-se em conformidade com as políticas de compliance empresarial, com o objetivo de gerir os dados das empresas para estabelecer um diferencial competitivo aos negócios. (KOEPSEL,2020)
O programa integra o aperfeiçoamento do procedimento de utilização dos dados, com os requisitos pré-estabelecidos na implementação dos softwares, com a finalidade de gerir de forma otimizada os dados para preencher as diretrizes da legislação. (SAAD, 2021)
A Lei Geral de Proteção de Dados Pessoais dispôs que os controladores e operadores poderão adotar programas de governança em privacidade, que devem ser implementados com o mínimo, (art. 50, § 2°, I): a) o comprometimento dos agentes de tratamento com as políticas internas que devem garantir o cumprimento das normas e regras de boas práticas; b) que aplicação seja de forma uniforme para todo a operação de tratamento de dados; c) que a governança seja adaptativa as estruturas da empresas, sendo compatível com a densidade dos dados e operação; d) como implementar políticas de salvaguardas em relação aos titulares dos dados; e) tenha como objetivo estabelecer uma relação de confiança com sujeitos dos dados, estabelecendo situações de transparência e que possibilite a atuação do titular; g) que conte com planos de respostas a incidentes e remediações; h) seja continuamente atualizado sua base.
Nesse aspecto, devem ser adotadas medidas administrativas para que as instituições, em conformidade com a legislação, apliquem estímulos para assegurar as informações armazenadas pelas empresas, com a adoção de orientações internas que respeitem as diretrizes que inclua o uso

minimizado ou a anonimização das informações, desde a coleta dos dados, conforme artigo 46 da LGPD.
Com o mapeamento das atividades, é importante verificar: O que são esses dados?; de que forma foram coletados ?; quem são os coletores ?; existe relação entre os dados e atividade realizada ?; O que pode ocorrer com esses dados ao serem coletados? E, como são descartados da gestão organizacional da empresa? (NASCIMENTO, 2020). Dessa forma, para adotar medidas compatíveis com os riscos alertados pelos sistemas para a proteção de dados nas organizações privadas, é necessário possuir conhecimento do caminho realizado inerentes ao ciclo de vida útil dos dados.
Embora, a legislação já estabeleça diretriz mínima para o tratamento de informação, a Autoridade Nacional de Proteção de Dados - ANPD, poderá, ainda, determinar padrões técnicos para serem implementados pelo programa de governança em privacidade, devendo ser observado a qualidade de dados, as especificações do tratamento e status tecnológico, em especial a proteção aos dados sensíveis disposto na legislação. (NASCIMENTO, 2020)
Muito embora, a lei geral de proteção de dados, apenas delimita as características e os requisitos mínimos que os operadores deverão tomar para desenvolver um compliance na organização das empresas privadas em consonância com a legislação, porém não impõe um modelo específico para integração de um programa nas corporativas. (PESSOA, 2021)
Assim, para Saad (2021), as medidas técnicas que podem ser adotadas pelos agentes de

tratamento de dados, são: i) o uso de firewalls, sendo um mecanismo de segurança que coleta os dados em conformidade com as regras pré estabelecido para análise de tráfego de rede, delimitando as operações de compartilhamento e captação de informações a serem cumpridas; ii) a utilização de antimalware, que consiste na proteção contra vírus que é capaz de fragilizar o sistema, apagar dados e infectar outros arquivos; iii) a utilização de criptografia dos dados, que possibilite quando ocorrer situações incidentais a não identificação do titular do direito.
Já para Fernandes e Abreu, (2014) defendem a implementação de frameworks como a DAMABOK e COBIT, para o gerenciamento de dados, pois tem como meta principal a delimitação do escopo das atividades, as funções envolvidas no tratamento e as interações a serem executadas pelo software, com a finalidade de proteger a privacidade em ambientes corporativos que gerenciam o armazenamento de informações aplicados na prevenção à fraude.

Segundo Carvalho (2021), a integração do software, através das boas práticas estabelecidas pela legislação, poderá aprimorar os aspectos de proteção à privacidade e prevenção a fraude do tratamento de coleta de dados. Tendo em vista, que os frameworks, podem balizar as métricas de qualidade dos dados que indicam uma utilização adequada e otimizada, e aponta a melhor proteção da privacidade.
Com a melhoria de processo de governança para o tratamento de dados, estabelece uma divisão entres as operações que possibilita uma automatização do ciclo de vida dos dados (coleta, utilização, armazenamento e exclusão), capaz de gerar relatório de risco, para o auxílio da tomada de decisão com o intuito de gerir de forma adequada o tratamento de dados. (CARVALHO, 2021)
Neste parâmetro, os programas de compliance com a implementação de frameworks, podem responder questionamento acerca do procedimento de tratamento de informação, dispondo de quais práticas relacionadas à governança, privacidade e segurança de dados, apresentam melhor benefício para o tratamento de dados pessoais. (CARVALHO, 2021)
Ademais, os controladores e operadores deverão adotar medidas, como o Relatório de Impacto ? DPIA), que corresponde a avaliação dos riscos e impactos relacionados com o tratamento de dados pessoais, além da anonimização, da transparência e do sigilo, deverão delimitar prazos para retenção de dados e aderir políticas seguras de informação acerca da operação de tratamento. (SILVA, 2022)
Após realizar a implementação e observância das estruturas mínimas estabelecidas pela LGPD, é necessário adotar um programa de gerenciamento de vulnerabilidades, com atualizações constantes e autocorreções alinhados com as boas práticas de atividades cotidianas, com a finalidade de proteger os dados pessoais, e promover um ambiente corporativo adequado para realizar o tratamento de dados. (SAAD, 2021)
No entanto, ao verificar que houve vazamento de dados, seja pelo recebimento de notificação ou pela veiculação na mídia, os agentes de tratamentos deverão identificar quais dados vazaram e realizar o procedimento estabelecido no programa de compliance de segurança, além de notificar as instituições. (Art. 48, caput).
De acordo com MIT, o prazo entre a comunicação à autoridade competente e a ocorrência do fato ilícito ultrapassa 200 (duzentos) dias em média, sendo umas das preocupações para a

efetividade da legislação, e a redução dos danos causados aos titulares dos bens imateriais.

A Lei Geral de Proteção de Dados, dispõe que nas situações que ocorrer a probabilidade de riscos ou violação aos direitos dos titulares, tem como obrigação do encarregado a comunicação à autoridade nacional e ao titular do dado (art. 48, caput). Sendo que o contato deve ser em período razoável (art. 48, § 1º), contendo a natureza dos dados dos titulares atingindo (art. 48, § 1º, I).
Em decorrência dos possíveis incidentes, a LGPD determinou critério para aplicação de sanções, em casos de vazamento de dados, observando as situações específicas de cada caso, disposto no art. 52, § 1º. Assim, deve ser considerada a avaliação da gravidade, a natureza das informações e do dano ocorrido (incisos I e VI), sendo necessário para este caso, tendo em vista que o compartilhamento indesejado de dados sensíveis pode ocasionar danos irremediáveis para os titulares.
Portanto, existe a necessidade da adesão aos mecanismos e técnicas para promover a efetividade dos programas internos com a finalidade de mitigar os danos, assim, a implementação de boas práticas e governança têm como fator o cumprimento da legislação, por meio de medidas de segurança. Entende-se, que a proteção integral contra falhas que possibilitam a ocorrência de ilícitos não é possível, porém essas diretrizes reduzem as possibilidades de existir desvios de condutas e criar salvaguardas para identificação dos incidentes, de forma eficaz, rápida e adequada.

6 CONSIDERAÇÕES FINAIS

A partir da permissão ao acesso dos dados pessoais, as informações coletadas passaram a integralizar as redes de tratamento de dados, tornando-se alvo de ataques cibernéticos, contribuindo para o aumento da intercorrência no ambiente corporativo, tornando-se o gerenciamento de informação um dos diferenciais no desenvolvimento do negócio.
Nesse contexto, foi imperativo o surgimento de leis que protejam os dados dos cidadãos, e que limitem a gestão das entidades públicas e privadas em relação as informações coletadas, transformando o sistema organizacionais, como compliance, em ferramentas de efetivação das normas éticas e legais. Assim, a implementação do programa alinhado com a governança corporativa é capaz de integralizar o corpo de normas internas com o intuito de adequar a legislação brasileira e criar uma cultura corporativa.
Dentro do programa de compliance, a administração em conjunto com a gestão da empresa, poderá implementar ao plano diretor, a utilização de software, sendo este capaz de possibilitar a automatização do ciclo de vida útil dos dados para realizar o auxílio da tomada de decisão, com o intuito de mitigar os possíveis danos decorrentes da violação aos dispositivos da Lei Geral de Proteção de Dados Pessoais.
Nesse sentido, para realizar uma proteção extensiva aos direitos dos titulares dos dados, a

LGPD integrou ao seu corpo de normas-condutas a serem adotadas pelos operadores do tratamento de dados, com escopo de preservar a integralidade, a qualidade e o sigilos dos dados, tendo como consequência da violação, a majoração de sanções pecuniárias.
Embora, o vazamento de dados ocorra de forma ordenada, a implementação de sistema de segurança nas corporações implica na diminuição de situações incidentais por erro humano, ou inadequação dos programas empresarias, assim, devendo a gestão ensejar esforços para que a proteção dos dados seja preservada, desde a concepção do serviço.
Para a efetivação da Lei Geral de Proteção de Dados Pessoais, as empresas devem realizar a adequação de medidas de boas práticas e governança em privacidade para mitigar os possíveis danos decorrente da violação aos dados em provedores privados. Mesmo que a proteção aos dados de forma concreta não seja possível, as adoções de mecanismo de segurança podem atenuar as sanções e as perdas aos titulares dos dados.

REFERÊNCIAS

BARATA, André Mantola. Governança de dados em organizações brasileira: uma avaliação comparativa entre os benefícios previstos na literatura e os obtidos pelas organizações. 2015. Dissertação (Mestrado em Sistema de Informação) - Universidade de São Paulo, São Paulo, 2015.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, [2022]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 15 abr. 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidente da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 abr. 2023.

BERTOCCELLI, Rodrigo de Pinho. Compliance. In: CARVALHO, André Castro et. al. Manual de compliance. Rio de Janeiro: Forense, 2019. p. 35.

CANDELORO, Ana Paula; RIZZO, Maria Balbina Martins De; PINHO, Vinícius (Coord). Compliance 360: riscos, estratégias, conflitos e vaidades no mundo corporativo. São Paulo: Trevisan, 2012.

CARVALHO, A. P. Proposta de um framework de compliance à Lei Geral de Proteção a Dados Pessoais (LGPD): um estudo de caso para prevenção a fraude no contexto de big data. 2021. Dissertação (Mestrado em Engenharia Elétrica) - Universidade de Brasília, Brasília, 2021.

CARVALHO, Andre Castro. Manual de compliance. 3. ed. Rio de Janeiro: Forense, 2021.

CASAES, Júlio César Costa. Governança de dados abertos governamentais: frameworks conceitual para as Universidades Federais, baseada em uma visão sistemática, 2019. Tese (Doutorado em Engenharia e Gestão do Conhecimento). Universidade Federal de Santa Catarina, Florinaóplis, 2019.

DATA GOVERNANCE INSTITUTE (DGI). Definitions of data governance. 2017. Disponível em: http://www.datagovernance.com/adg_data_governance_definition. Acesso em: 01 mai. 2023.

ENDEAVOR DO BRASIL. Prevenindo com o Compliance para não remediar com o caixa. In: ENDEAVOR. [S. l.], 26 abr. 2017. Disponível em: https://endeavor.org.br/pessoas/compliance/. Acesso em: 15 mar. 2023.

ESPÍNDOLA, P. L.; SALM JUNIOR, J. F.; ROSA, F.; JULIANI, J. P. Governança de dados aplicada à ciência da informação: análise de um sistema de dados científicos para a área da saúde. Revista Digital de Biblioteconomia & Ciência da Informação, Campinas, v. 16, n. 3, p. 274-298, 2018.

FERNANDES, Aguinaldo Aragon; DE ABREU, Vladimir Ferraz. Implantando a governança de TI: da estratégia à gestão de processos e serviços. 4. Ed. Rio de Janeiro: Brasport, 2014.

FRAZÃO, Ana. Programas de compliance e critérios de responsabilização de pessoas jurídicas por ilícitos administrativos. In: ROSSETTI, Maristela Abla; PITTA, Andre Grunspun. Governança corporativa: avanços e retrocessos. São Paulo: Quartier Latin, 2007. p. 42

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. A Lei Geral de proteção de Dados Pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

HONÓRIO, Roseli. Modelo conceitual de governança de dados como suporte à governança do conhecimento organizacional. 2022. Dissertação (Mestrado em Engenharia e Gestão do Conhecimento) - Universidade Federal de Santa Catarina, Florianópolis, 2022.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC). Guia das melhores práticas de governança para cooperativas. São Paulo, 2015. Disponível em http://www.ibgc.org.br/ userfiles/files/2014/files/CMPGPT.pdf

JOHNSON, Ralph E.; RUSSO, Vincent. Reusing object-oriented designs. Relatório Técnico da Universidade de Illinois, UIUCDCS 91-1696, 1991.

KLEINDIENST, Ana Cristina. Grandes temas do direito brasileiro: compliance. São Paulo: Almedina Brasil, 2019

KOEPSEL, Alice de Medeiros. Adoção e efeitos dos programas de compliance à luz da Lei Geral de Proteção de Dados Pessoais. 2020. Monografia (Graduação em Direito) -Universidade do Sul de Santa Catarina, Florianópolis, 2020.

LIMA, C., BASTOS, R. C. A criação de conhecimento apoiada pela governança de dados. In: CONGRESSO INTERNACIONAL DE CONHECIMENTO E INOVAÇÃO, 2019, Santa Catarina. Anais eletrônicos [...]. Santa Catarina Disponível em: https://proceeding.ciki.ufsc.br/index.php/ciki/article/view/647. Acesso em 10 Mar. 2023.

MARTIGNAGO, Deisi et al. Governança de dados aplicado no processo de catalogação. Revista Brasileira de Biblioteconomia e Documentação, São Paulo, V.15, n. 2, 2019.

MENDES, Gilmar Ferreira. Curso de direito constitucional. 2. ed. São Paulo: Saraiva, 2008.

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. São Paulo: Revista de Direito do Consumidor, 2018.

NASCIMENTO, Suellen Lima do. A lei Geral de Dados Pessoais e a Adoção dos Programas de compliance na sociedade da Informação. 2020. Monografia (Graduação em Direito) - Centro Universitário de Brasília, Brasília, 2020.

PESSOA, Larissa Rocha de Paula. Os desafios da Governança de dados e a realidade cultural brasileira. 2021. Dissertação (Mestrado em Direito) ? Universidade Federal do Ceará, Fortaleza, 2021.

PINTO, S. C. C. S.. Composição em Web Frameworks, 2000. Tese (Doutorado em Informática) Pontifícia Universidade Católica do Rio de Janeiro, Rio Janeiro, 2000.

PROSSER, William L. Privacy. California Law Review. California, v. 48, n. 3. p. 383 ? 423, agosto, 1960.

RÊGO, Bergson Lopes. Gestão e governança de dados: promovendo dados como ativo de valor nas empresas. 1. ed. Rio de Janeiro: Brasport, 2013,

ROQUE, Pamela Romeu. Estudos aplicados de direito empresarial: LL.C. em direito empresarial. São Paulo: Almedina, 2019.

SAAD, Carolina de Oliveira. A lei geral de proteção de dados pessoais e incidentes de segurança: regulação e prática de vazamento de dados, 2021. Monografia (Graduação em Direito). Fundação Getúlio Vargas. Rio de Janeiro, 2021.

SANTANA, Ricardo Cesar Gonçalves. Ciclo de vida dos dados e o papel da ciência da informação. In: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO. 14., 2013. Florianópolis. [?]. Florianópolis: UFSC, 2013. Disponível em: http://enancib2013.ufsc.br/index.php/enancib2013/%20XIVenancib/paper/viewFile/284/319. Acesso em: 13 mar. 2023.

SILVA, Ana Laura Fonseca. O papel das Soft Skills na implementação efetiva dos programas de compliance com foco na adequação à Lei Geral de Proteção de Dados ? Lei N° 13.709/18. 2022. Monografia (Graduação em Direito) - Universidade Federal de Ouro Preto, Ouro Preto. 2022

SILVA, Eggon João da. A defesa da ética e transparência. In: VENTURA, Luciano Carvalho. Governança corporativa. São Paulo: Saint Paul Editora, 2005, página 259.

TERRA, Priscila de Mello. A influência da governança de dados na gestão estratégica, 2017. Monografia (Bacharelado em Sistema de Informação) - Universidade Federal Fluminense, Niterói, 2017.

VAZAMENTO de dados aumentaram 493% no Brasil, segundo pesquisa do MIT.VEJA, São Paulo, 24 fev. 2021. Sociedade. Disponível em: https://vocesa.abril.com.br/sociedade/vazamentos-de-dados-aumentaram-493-no-brasil-segundo-pesquisa-do-mit. Acesso em: 15 mar. 2023.

VIEIRA, Tatiana Malta. O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante da tecnologia da informação. Porto Alegre: Sergio Antonio Fabris Editor, 2007.

==========

Arquivo 1: TCC - A IMPORTÂNCIA DO COMPLIANCE NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA - WESLEY VICENTE.pdf (8805 termos)
Arquivo 2: https://www.questionsanswered.net/article/inspiring-quotes-history?utm_content=params%3Ao%3D740012%26ad%3DdirN%26qo%3DserpIndex&ueid=7071288f-9e02-4d51-a234-80c758412ac5 (803 termos)
Termos comuns: 0
Similaridade: 0,00%
O texto abaixo é o conteúdo do documento TCC - A IMPORTÂNCIA DO COMPLIANCE NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA - WESLEY VICENTE.pdf (8805 termos)
Os termos em vermelho foram encontrados no documento
https://www.questionsanswered.net/article/inspiring-quotes-history?utm_content=params%3Ao%3D740012%26ad%3DdirN%26qo%3DserpIndex&ueid=7071288f-9e02-4d51-a234-80c758412ac5 (803 termos)

==========

WESLEY VICENTE DA SILVA

A IMPORTÂNCIA DO COMPLIANCE EMPRESARIAL NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA

SALVADOR
2023

WESLEY VICENTE DA SILVA

A IMPORTÂNCIA DO COMPLIANCE EMPRESARIAL NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA

Artigo apresentado como requisito parcial para obtenção do título de Bacharel em Direito pela Universidade Católica do Salvador.

Orientador: Prof. Darlã Conceição Santos.

SALVADOR
2023

A IMPORTÂNCIA DO COMPLIANCE EMPRESARIAL NA PREVENÇÃO DO VAZAMENTO DE DADOS NA ESFERA PRIVADA

Wesley Vicente da Silva1
Darlã Conceição Santos2

RESUMO: No cenário de exploração das informações como mercadoria econômica, os dados pessoais coletados por empresas privadas tornaram-se fator de tutela legislativa. Assim, surgiu a necessidade de organizar os setores privados para adequar aos moldes da Lei Geral de Proteção de Dados Pessoais ? LGPD, com o intuito de proteger a privacidade, como direito autônomo e fundamental para a tutela da pessoa humana, destacando os programas de compliance aliados as boas práticas e governança de dados. Nesse contexto, a fim de consolidar os mecanismos técnicos de segurança para a efetividade da legislação com a finalidade de mitigar os casos de vazamento de dados pessoais, a LGPD implementou medidas administrativas para inibir incidentes decorrentes das condutas infratoras a legislação. Desse modo, este trabalho tem como objetivo demonstrar a importância dos programas de compliance para a proteção aos direitos dos titulares dos dados, visando o cumprimento do ordenamento jurídico. Valendo-se do método hipotético-dedutivo, com abordagem qualitativa, utilizando da revisão bibliográfica de livros, legislação,

artigos, dissertações e teses concernente à tutela de dados pessoais no Brasil para o desenvolvimento do presente artigo.

PALAVRAS-CHAVES: Compliance Empresarial. Governança corporativa. LGPD. Vazamento de dados.

ABSTRACT: In the scenario of exploitation of information as an economic commodity, personal data collected by private companies have become a factor of legislative protection. Thus, the need arose to organize the private sectors to conform to the General Law for the Protection of Personal Data - LGPD, in order to protect privacy, as an autonomous and fundamental right for the protection of the human person, highlighting compliance programs allied with good practices and data governance. In this context, in order to consolidate the technical security mechanisms for the effectiveness of the legislation with the purpose of mitigating cases of leakage of personal data, the LGPD implemented administrative measures to inhibit incidents arising from conducts that violate the legislation. Thus, this work aims to demonstrate the importance of compliance programs to protect the rights of data subjects, aiming at compliance with the legal system. Taking advantage of the hypothetical-deductive method, with a qualitative approach, using the bibliographic review of books, legislation, articles, dissertations and theses concerning the protection of personal data in Brazil for the development of this article.

KEYWORDS: Corporate Compliance. Corporate governance. LGPD. Data leak.

1
Discente do curso de Direito da Universidade Católica do Salvador.
2
Mestre em Direito, Docente na Universidade Católica do Salvador.

1 INTRODUÇÃO

A nova moeda de troca não é apenas aquela que podemos ver, quantificar ou converter. Os moldes do mercado financeiro mudaram, sendo em questão material ou ao produto que eles precificam, postulando um novo aparato ao objeto contratual: os dados.
Muito embora, os dados pessoais, ainda para muitos, são apenas informações deslocadas acerca de fatores específicos, atualmente, podem ser conceituados como um conjunto de indicadores, regrados por um complexo condensado de informações em um fluxo crescente tangencial.
Os dados da grande massa acabam gerando indicadores que podem ser balizados e influenciados de acordo com os detentores dessa informação, apenas apartado em blocos de informações não são considerados como vetores orçamentários. Porém, direcionados para uma

finalidade ordenada tem o condão de influenciar o interesse social.
Dito isso, os mecanismos postos pelo Reino Unido para possibilitar uma estruturação normativa para organizar e gerir os dados dos indivíduos, foi crucial para a criação em outros países, como no Brasil, onde instituiu-se a Lei Geral de Proteção de Dados Pessoais (LGPD). Muito embora, a lei brasileira trouxe um arcabouço de normas reguladoras e sanções aos casos de tratamento de dados, que não foram abarcados com o marco da internet, os dados em uma visão macro constitucional já eram de forma genérica tutelados pela Constituição Federal de 1988.
Todavia, apenas a sanção da LGPD não seria, isoladamente, capaz de coibir as violações ao tratamento de dados na esfera privada, mas sim a necessidade de uma regulamentação do ciclo de vida das informações, que além de estipular os dados que podem ser utilizados ou até quando podem ser armazenados, estabelecer expressamente no bojo da norma como deve ser a proteção na operação do tratamento de dados.
De forma efêmera, conclui-se que a legislação pode delimitar os alicerces capazes de ensejar uma fiscalização, sendo estas através de mecanismo de gerenciamento de atividades, políticas de condutas e implementação de governança de dados, pois os dados hackeados ou vazados de forma isoladas, não seria possível identificar dados sensíveis, muitos menos individualizar o sujeito.
Portanto, o gerenciamento dos dados em provedores de armazenamento pode ter os riscos reduzidos de acordo com a realização de medidas de compliance para dirimir os impactos na

atividade empresarial, como também para tutelar os dados, cada vez mais acentuado como um produto orçamentário.

2 COMPLIANCE EMPRESARIAL

A criação do compliance está entrelaçado sob o cenário econômico-social, assim, sua implementação como sistema de organização foi instaurado e aprimorado a partir dos problemas práticos estruturais para gerir uma boa governança, com intuito de assegurar a proteção e o controle que garante a qualidade do negócio.
A utilização do termo foi inicializada no mercado financeiro, especialmente após a criação do Banco Central em 1913 nos Estados Unidos da América, com a necessidade de um sistema econômico ajustável e estável. Só após 1960, com a regularização da Securities and Exchange Commission (SEC), que houve a necessidade de implementação do compliance como um programa para a integração dos procedimento, controle e monitoramento de operação interna. (CARVALHO, 2021)
Em 1977, com a Convenção Relativa à Obrigação de Diligência dos Bancos Suíços, estabeleceu os modelos auto regulatórios, com adequação de condutas e processos internos, na qual a infração tem como consequência à aplicação de sanções. (CARVALHO, 2021)
Só após esse processo de amadurecimento histórico, que o Brasil teve a necessidade de competir em escala global, implementado novos processos de segurança no sistema financeiro brasileiro.
Pode-se concluir que, após a globalização com o fenômeno da criação dos dados estruturais,

houve a potencialização das informações adquiridas por meio de provedores, classificadas, atualmente, como fonte econômica de um produto quantificativo e qualitativo, ao qual possibilita uma utilização como um produto do sistema financeiro.
Nesse sentido, em decorrência de ataques cibernéticos em provedores de informações massificadas conduziram a sociedade na aplicação de institutos de melhoramento, como o compliance e suas interfaces para proteger no ambiente corporativo os dados massificados recebidos em seus provedores.

2.1 O CONCEITO DE COMPLIANCE

Antes de enveredar sob o conceito de compliance na esfera privada, é oportuno compreender o seu significado. Nesse contexto, a palavra compliance advém do verbo inglês, to comply, que pode ser definida como conformidade. O instituto deve ser aplicado como plano principal de uma diretriz pré-estabelecida para ser dirigida a todos capazes de enfrentar a finalidade destinada. (BERTOCCELLI, 2019)
Nesse parâmetro, pode ser traduzida como:

Comply, em inglês, significa ?agir em sintonia com as regras?, o que já explica um pouquinho do termo. Compliance, em termos didáticos, significa estar absolutamente em linha com normas, controles internos e externos, além de todas as políticas e diretrizes estabelecidas para o seu negócio. (ENDEAVOR DO BRASIL, 2022, n.p)

O compliance pode-se ser definido de forma técnica como um conjunto de normas padronizadas, sob um viés ético e legal, na qual após estruturação será a matriz orientadora para o comportamento organizacional da instituição ao qual atuará no mercado, como também irá reger as atividades dos colaboradores. Dessa forma, sendo um instrumento hábil a controlar o risco de imagem, a normatização legal, chamados de riscos de compliance, as que recaem nas instituições no decorrer da sua atividade laboral. (CANDELORO, 2012).
Superada a barreira terminológica, a finalidade do compliance tem como escopo o gerenciamento adequado do risco de atividades, verificar adequadamente as normas éticas e legais, e estudar os possíveis danos tangenciais. Dessa forma, esses elementos visam a redução de perdas e danos, como também amplifica a cultura e fortalecimento corporativo nos moldes aos padrões exigidos, seja esse por lei ou na tentativa de dirimir o risco do serviço prestado.
Portanto, segundo a doutrinadora Frazão (2007, p. 42), destina-se em sua obra que o compliance é como:
(...) conjunto de ações a serem adotadas no ambiente corporativo para que se reforce anuência da empresa à legislação vigente, de modo a prevenir a ocorrência de infrações ou, já tendo ocorrido o ilícito, propiciar o imediato retorno ao contexto de normalidade e legalidade.

Nessa mesma linha de pensamento, de acordo com os autores da obra Compliance 360° (2012, n.p), referem-se o compliance a:

Um conjunto de regras, padrões, procedimentos éticos e legais que, uma vez definido e implantado, será a linha mestra que orientará o comportamento da instituição no mercado em que atua, bem como as atitudes de seus funcionários; um instrumento capaz de controlar o risco de imagem e o risco legal, os chamados ?riscos de compliance?, a que se sujeitam as instituições no curso de suas atividades.

Pode-se concluir que o conceito de compliance, em uma esfera macro, é um aglomerado de regras pré-estabelecidas através de um instrumento perpetuado por técnica de desenvolvimento, capaz de dirimir riscos e danos das atividades devolvidas pelo plano diretor.
Muito embora, o instituto "compliance" tem uma definição extensiva e não tem como fim apenas o cumprimento da legislação e de condutas éticas, pode ser compreendida também como um instrumento de diminuição de riscos, desenvolvimento corporativo sustentável e subsequentes segmentos empresariais de negócio. (ROQUE, 2019)
O compliance além de estar associado tradicionalmente a uma perspectiva organizacional aos comandos administrativos, pode ser vinculada também a uma visão de uma sociedade digital 4.0, devendo não só apresentar o compliance empresarial na esfera de redução de risco à imagem, mas sim, em uma abordagem de pré-orientação e implementação de desenvolvimento aos moldes legislativo de proteção aos dados, como objeto principal de estudos.
Portanto, é necessário a elaboração do projeto de compliance em uma visão lógica, a modo de compreender os objetivos e os componentes da aplicação do programa. Posteriormente, superado os obstáculos, aplica-se os estudos de riscos a boa governança corporativa com a implementação de programas de governança de dados objetivando auxiliar o controle de informações em conformidade aos padrões da corporação, e mitigar os danos da empresa.

2.1.1 AS GOVERNANÇAS CORPORATIVAS E A IMPLEMENTAÇÃO DOS PROGRAMAS DE COMPLIANCE

Em linhas gerais, o Instituto Brasileiro de Governança Corporativa ? IBGC (2015, n.p) discrimina o conceito de Governança Corporativa, como: ?Sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas. ?
O sistema da governança corporativa está associado ao desenvolvimento interno de uma empresa, seja ele entre a administração, sócios e funcionários, capaz de criar elos para uma estruturação de direção racional e acima de tudo nos moldes da ética e legislação.
Muito embora, a governança corporativa e o compliance sejam institutos que se assemelham em uma visão macro, os mesmos, diferenciam na aplicação prática, mas se complementam no objetivo final, sendo um instrumento para aplicação do outro.

A prática da governança corporativa, além de estimular o valor empresarial, pode-se concluir que estrutura de forma adequada a medida necessária para organizar a atividade empresarial, assim, não há que se falar em condutas prejudiciais. Por exemplo: empresários compreendem que para realizar uma instrumentalização segura aos seus sócios e administradores tendem a prejudicar o negócio empresarial, assim o autor Eggon João da Silva (2005, p.259) retrata que: ?A governança corporativa assegura tratamento equânime a todos os acionistas, inclusive minoritários, preferencialistas, nacionais e estrangeiros. Todos devem ter oportunidade de reparação caso venham a sofrer violação de seus diretores. ?

Nesse passo, as críticas ao sistema não são viáveis, tendo em vista a utilização de instrumento capaz de integralizar ao plano empresarial. Sendo assim, o programa de compliance visa amplificar a utilização de um sistema para garantir que todos possam participar de forma justa sob o aspecto legal, seja sócio ou administrador.

Em uma tangente geral, a implementação da governança corporativa ressoa em uma perspectiva segura, tanto internamente, seja auxiliando as avaliações das atividades executadas pelos sócios/administradores, quanto externamente, em relação à imagem da empresa, sendo este um fator primordial a empresas estruturadas no mercado.

A implementação da governança corporativa deve ser estruturada de acordo com as necessidades da empresa, devendo verificar o histórico de desenvolvimento do estabelecimento, pois, só a partir do status da empresa pode-se delimitar a estratégia possível para uma implementação segura e adequada. Sendo assim, um regramento mais rigoroso pode gerar consequências negativas e ineficazes, especificamente em estágios primários, pois em atividades inicias, as tomadas de decisões e a execução da atividade empresarial é primordial, sendo necessário, um aspecto negocial informal para realizar os objetivos da empresa, o que não se verifica quando existe prática de boa governança devidamente estruturadas no negócio. (KLEINDIENST, 2019)

Ao desenvolver da atividade da empresa, além da atenção a organização interna, sendo está um fator primordial da governança, ainda que no fim acabe tendo um aspecto externo por vislumbrar no mercado financeiro uma maior complexidade da entidade. O desenvolvimento da empresa, seja no faturamento, importação comercial, quantidade de funcionários, além dos controles a observância da legislação e regras internas, tendem à serem complexos, e, que necessita de ações maiores que a própria instituição empresarial, restando necessária a implementação de sistema organizacionais aos fluxos de informações. (KLEINDIENST, 2019)

Ultrapassado a esfera conceitual e instrumentalização da política de boas práticas de governança, cabe pontuar que as empresas que possuem fluxos de informações sensíveis, conforme estipula o artigo 50 da Lei Geral de Proteção de Dados Pessoais, os controladores e operadores são responsáveis pelo tratamento de dados, devendo criar planos de adequação a legislação.

Assim, ao confeccionar as regras de boas práticas, os controladores adjuntos com a administração devem estipular através da análise da natureza dos dados coletados, a probabilidade, a finalidade e o potencial de riscos das vantagens advindas dos tratamentos dos dados verificados. (NASCIMENTO, 2020)

É necessário pontuar que, os agentes de tratamento, após a autenticação da gravidade e sensibilidade dos dados aos riscos de operação, poderão estabelecer programa de governança em privacidade, sendo este, um instrumento amplo com normas de compliance, além dos aspectos operacionais.

Em relação ao programa de governança de privacidade, pode-se estabelecer como um aglomerado de normas-regras de boas práticas de governança, com a finalidade de executar ordens de natureza legal. (NASCIMENTO, 2020)

Portanto, os instrumentos do compliance em conjunto com a boa prática de governança, se consagram na identificação dos riscos e estruturação de medidas para a empresa, sendo respondida de forma adequada e proporcional ao suporte da tomada de decisão.

O Programa de compliance na esfera privada para análise de dados pessoais, com a finalidade de promover a segurança, deve ser constantemente monitorado e atualizado, com a implementação de ?salva vidas? em decorrência de avaliação de riscos à privacidade e o acometimento de vazamentos. (NASCIMENTO, 2020)

Portanto, os instrumentos e objetos referenciados demonstram a determinação de regras de governança no ambiente de operação de tratamento de dados pessoais, a modo que seja realizado uma estruturação nas empresas para que possibilitem a implementação de mecanismos de segurança, com a finalidade de dirimir os riscos da atividade empresarial na sociedade digital.

3 GOVERNANÇA DE DADOS

O mercado digital tem como principal ativo financeiro os dados, este considerado como ?matéria prima? de uma economia baseada no conjunto de informações, sendo que nos últimos anos, houve um aumento exponencial na coleta de dados por cooperativas, startups e novos nichos empresariais, tendo a finalidade de quantificar e gerencias os dados.

Dados, informações, conhecimento e sabedoria são os quatros estágios evolutivos da cadeia de informação, pode-se assim, compreender os dados como fatos ou registros em seu formato primário. (BEAL, 2014). Já a informação é entendida como os conjuntos processados de dados em um contexto aplicado (RÊGO, 2013). Muito embora, na sociedade da informação ?os dados são o novo petróleo?, apenas os dados isoladamente não são capazes de transformar em ativo financeiro, sendo necessário administrá-lo de forma eficaz, para que assim, as empresas adquiram vantagem competitiva.

Dessa forma, a governança de dados tem como principal objetivo atender as necessidades das empresas, ou seja, solucionar problemas, diminuir custos da administração, para que os dados transformem em saldo positivo para os negócios (TERRA, 2017).

O Data Governance Institute -DGI (2017, n.p) definiu governança de dados como ?um

sistema de direitos de decisão e responsabilidades para processos relacionados à informação, executado de acordo com modelos acordados que descrevem quem pode realizar quais ações com quais informações e quando. ? Portanto, a utilização da governança de dados orienta quais os métodos deverão ser aplicados no ciclo de vida dos dados.

Uma das atribuições da governança é o acompanhamento da operação dos dados com a finalidade de gerir que as informações estejam alinhadas com os objetivos pré-determinados na coleta primária, além disso, é necessário assegurar que as informações estejam disponíveis para acesso, quando consultadas, gozar de qualidade, consistência, auditabilidade e segurança dos dados (ESPÍNDOLA, 2018).

No âmago da cadeia evolutiva da informação uma das preocupações dentro das organizações corporativas é o receio com a proteção das informações, ou seja, a capacidade das empresas no protagonismo da segurança com os provedores internos, tendo em vista a necessidade de conformidade com a legislação pátria.

A boa governança tem como objetivo aplicável à prática do controle dos processos de operação dos dados: a prevenção de situações adversas que podem gerar o comprometimento da integralidade dos dados adquiridos pelas organizações empresariais, que por sua vez, devem ter o condão de reforçar a confidencialidade das informações. (ESPÍNDOLA, 2018).

A integração do programa de governança de dados nas corporativas empresariais, tem como o esforço principal a organização de dados, que deve ser observado por um prisma basilar, ou seja, a aplicação dos princípios como limite legal e ético no ciclo de vida dos dados.

Para Rêgo (2013), os princípios são regulamentações para compreender aplicação da governança dos dados como linha direta para os negócios, sendo: (i) A gestão de dados estratégicos, tem o dever de vislumbrar as tomadas decisões por um coeficiente tático e operacional. (ii) A governança como instituição, ou seja, a governança de dados pode ser comparada como sistema governamental, na qual dispõe de legislação, execução e jurisdição; (iii) A governança de dados como um programa, devendo ser implementado como fator permanente, não apenas um projeto temporário. Ainda, pontua-se que os princípios da Governança de dados não são limitados, tendo uma orientação basilar a cada implementação de um sistema organizacional que deve ser observado pelo prisma ético e legal.

Assim, os princípios devem incumbir os papéis que a serem preenchidos pela gestão moldar os comportamentos das empresas para a aquisição, reserva e utilização dos dados conforme as normas e políticas da corporação (TERRA, 2017).

Coleta, armazenamento, recuperação e descartes, são as quatro etapas do ciclo de vida dos dados (SANTANA, 2013), ou seja, para a aquisição de dados pelas empresas, deverão observar a vida útil do dado para não incorrer na (in) responsabilidade da utilização indevida de informações dos seus provedores.

As fases do ciclo de vida dos dados devem ser observadas pela ótica de seis objetivos, sendo eles: a qualidade, a privacidade, os direitos autorais, a integração, compartilhamento e preservação dos dados (ESPÍNDOLA, 2018). Muito embora, a lei geral de proteção de dados implementou e traçou novos objetivos para a coleta de dados pessoais, cabe destacar que os objetivos vislumbrados

na Governança de dados têm como parâmetro preliminar a tomada de decisão, na qual deve ser os negócios pautados nos moldes legais e éticos vigentes.
Nesse contexto, o controle de informações é necessário, tendo em vista que na sociedade da informação, cada vez mais o volume de dados é crescente, acarretando mais vazão e protesto por políticas públicas para a preservação dos institutos, órgãos e empresas que detenham a

informação, sendo assim, necessário sistema de organização, softwares e hardwares capazes de processar as informações, criptografar e armazenar. (MARTIGNAGO, 2019)
Assim, para otimizar o ciclo de vida dos dados e garantir que os objetivos sejam preenchidos na estruturação do gerenciamento de dados, faz-se necessário a implementação de frameworks com o intuito de garantir que o procedimento seja cumprido com maior qualidade de informação e aproveitamento financeiro para a empresa, auxiliando a tomada de decisão para redução de risco para utilização de dados. (MARTIGNAGO, 2019)
Um Framework, segundo Johnson (1991), pode ser definida como um aglomerado de objetos que colabora entre si para que atinja um conjunto de obrigações para aplicação de um domínio especifico. Já para Pinto (2000), um framework é conceituado como um software incompleto criado para ser um objeto cujo estado e comportamento são definidos pela classe. Assim, o framework é uma concepção de uma arquitetura para um edifício de subsistemas e oferece o alicerce básico para criá-los.
Muito embora, os autores defendem uma conceituação distintas acerca da concepção de frameworks, pode-se verificar que ambas se complementam, tendo em vista que o framework é um sistema pré moldado, ou seja, é um programa com intuito de ser complementado através da finalidade a ser cumprida pela gestão empresarial, sendo instanciado por classes para categorizar os dados e ser alojado em hotspot, provedores físicos, capazes de armazenar as informações coletadas pelas empresas.
Portanto, para gerenciar os ativos de dados de forma complexa, ordenada e objetiva é necessário para proteção do procedimento do ciclo de vida dos dados, determinar os modelos de frameworks para o gerenciamento dos dados. Assim, para Carvalho (2021), podem ser apresentados três domínios CobiT, DAMA DMBOK e DGI Framework, sendo apenas dois destes observados para fomento deste artigo: (i) A DAMA (DAMA DMBOK), e (ii) CobiT.
A DAMA (Data Management Association) é uma associação sem fins lucrativos, com o intuito de promover boas práticas de gestão de dados, e em 2009 fundou o DAMA-DMBoK (Data Management Body of Knowledge), sendo um corpo de conhecimento que tem como ponto fundamental esclarecer como as corporativas devem aplicar a operação otimizada dos dados. (CARVALHO, 2021)
Em sua versão 2.0, acrescenta não só uma visão macro do gerenciamento de dados, definindo padrões, terminologias e práticas, mas a integração de dados, para definir táticas,

armazenamentos e sistemas, bem como implementação da ética na operação do tratamento de dados, a definição de big data e ciência de dados e amadurecimento das informações. (LIMA, 2019).

O DAMA-DMBOK V2 é formado por 11 (onze) funções de gestão de organização de dados, sendo incorporado como cerne principal: a governança de dados, tendo em vista que os dados percorrem por toda sistemática das onzes funções ordenadas, assim segundo Honório (2021):

A primeira função é a governa de dados, sendo o pilar do framework, tem o condão de orientar e supervisionar a operação do ciclo de vida dos dados, na qual deve estabelecer um sistema de apoio a decisão dos gestores sobre os dados, sob o prisma do negócio.

A arquitetura de dados, a segunda função, pode ser conceituada como um planejamento para administrar os dados, aquisição de ativos da empresa, com o intuito de definir a finalidade das informações adquiridas com os requisitos necessário para o gerenciamento dos dados.

Por sua vez, a modelagem de dados e design, tem a função de demonstrar de forma nítida os dados, sendo o processo da descoberta, análise e representação da etapa primária da informação.

O armazenamento, uma das etapas da operação do ciclo de vida dos dados, na qual vai incluir o design, o suporte dos dados armazenados para quantificar o coeficiente valorativo das informações, até o seu descarte, devendo respeitar todo o procedimento de segurança legal vigente.

Um dos alicerces para o gerenciamento de informação é a segurança, que deve garantir a proteção dos dados, a execução de políticas e procedimento de segurança, no intuito de moderar o acesso de forma consciente e controlado, não devendo ser infringido ou acessado de forma inadequada, afim de garantir autenticação e auditoria de dados informações.

A Integração e Interoperabilidade de dados, é a função responsável pela movimentação e a concretização dos dados na interligação do armazenamento e outras plataformas.

O gerenciamento de documentos, pode ser compreendida como o gerenciamento e inclusão da vida útil dos dados e informações, encontrados em programas não estruturados, em ênfase ao conteúdo de apoio de conformidade a legislação vigente e os termos éticos formalizados para o negócio.

Dados mestre e de referência, tem como condão a manutenção dos dados compartilhados para coexistir a integralidade dos sistemas internos de gerenciamento dos dados.

Em razão da interligação entre uma linha direta com os negócios, uma das funções do DAMA-DMBOK é a Data warehousing e Business intelligence, ou seja, a implementação de

planner para o contoler da administração dos dados e suporte a decisão com o intuito de conceder aos gestores de informação emitam relatórios de equalização de valores.

Segundo Barata (2015), os metadados, na qual consiste a décima função, é promover a facilitação do acesso dos dados interligados nas multifontes do sistema integrado, como também garantir a qualidade de dados.

Por fim, o gerenciamento de qualidade de dados é a implicação das técnicas para garantir a possibilidade de aferição, melhoramento e adequação da utilidade dos dados, com o intuito de monitorar a integridade da informação primária no ciclo de vida dos dados.

Já o COBIT (Control Objectives for Information and related Technology), é um framework

de suporte fundado em 1994 administrado pela ISACA (Information Systems Audit and Control Association), estruturado como um arcabouço de informação direcionadas para governança de dados e gerenciamento de informação, tem como objetivo auxiliar os profissionais de gestão na conexão entre os problemas técnicos e os riscos do negócio. (BARATA, 2015).
Para Lima (2019), o COBIT é um framework que possui duas vertentes basilares: a gestão, que possui quatro áreas de domínios: planejamento, constituição, execução e monitoramento, e a governança que é a tomada de decisão de acordo com a gestão de dados, possuindo 37 (trinte e sete) processos integrados.
Na versão 5.0, o sistema é utilizado baseado em 05 princípio, conforme elucida Casaes (2019), Barata (2015) e Lima (2019), sendo: (i) atender às necessidades das partes interessadas; (ii) cobrir o negócio como um todo; (iii) aplicar um framework único e integrado; (iv) habilitar uma visão holística; e (v) distinção entre governança de gestão.
Um dos princípios é atender às necessidades das partes interessadas, sendo a necessidade das corporativas é satisfazer as expectativas dos seus stakeholders, proporcionando um equilíbrio na tripartite: benefícios, redução do risco e recurso disponíveis.
O segundo princípio é baseado na cobertura do negócio como um todo, ou seja, abranger a integralidade da empresa no processo, procedimento, pessoas e as relações com os habilitadores.
A aplicação do framework único e integrado, assim, o COBIT é capaz de promover uma relação completa com a Governança de dados, corroborando ao alinhamento com padrões externos e adaptabilidade dos modelos usuais de negócios.

O COBIT permite habilitar uma visão holística, ou seja, uma visão macro dos componentes que oferecem suporte para atingir as finalidades da governança de dados, na qual define como catalogadores: as políticas, processos, estruturas organizacionais, informação e ética.
Por derradeiro, o princípio da distinção entre governança de gestão, tendo em vista que ambos possuem estruturas organizacionais distintas, assim, governança tem como esforço principal que os objetivos corporativos sejam cumpridos, estabelecendo prioridades pela tomada de decisão, compliance e progresso das organizações. Por sua vez, a gestão é o planejamento, construção, execução e monitoramento das funções ornamentada com o direcionamento da governança.
Desse modo, com escalonamento dos cinco princípios é capaz de proporcionar o funcionamento otimizado do framework, destacando os seguintes processos:
O APO01: Gerenciar o framework de TI, tem como condição a otimização das atividades relacionadas ao TI, com a função principal de incluir os procedimentos e regulamentos para promover a integralidade das informações nos bancos de dados. (BARATA, 2015)
Já o APO03: Gerenciar a arquitetura corporativa, tem função primordial agrupar as informações para auxiliar as atividades e tomadas de decisões, conceituando e compartilhando as informações dos elementos dos dados, e por fim catalogar a empresa, com base na modulação e sensibilidade dos dados. (BARATA, 2015)
Nesse ínterim, a governança de dados como um sistema integrado com o programa de compliance, tem o condão de otimizar a operação de controle interno relacionado aos dados coletados pelas empresas, capaz de gerenciar as bases para o apoio de decisão ao tratamento das

informações, com segurança e qualidade, garantido o ciclo da vida útil dos dados.

4 A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

As estruturas políticas, econômicas e sociais com desenvolvimento de novas tecnologias e mecanismo para a coleta de dados e informações, fez necessário modulações legislativas para a proteção da privacidade, além dos aspectos físicos, patrimoniais e morais.
A proteção à privacidade de dados foi dividida em quatros gerações: a primeira, oriunda do estado moderno, com o advento dos bancos de dados; a segunda, datada em 1980, com a expansão legislativa para a proteção à privacidade aos setores privados; a terceira geração em 1990, com o processo de tratamento de dados e o consentimento dos cidadãos; Por fim, a última dimensão, é

destinada ao protagonismo da permissão para coleta e uso dos dados pessoais, quando a lei estabeleceu a importância da titularidade das informações. (MENDES, 2014)
Nesse aspecto, é perceptível a evolução do direito aos fatores reais da sociedade e as transformações dos meios tecnológico, computacionais, genéticos e comunicativos, que por sua vez possibilitou a integração da comunicação global, e consequentemente, o rastreio dos dados através do armazenamento de informação. (SAAD, 2021).
Os legisladores ao considerar os dados pessoais como extensão ao direito à privacidade, preocuparam em tutelar constitucionalmente a proteção da população, em especial os países europeus, como: Espanha, Portugal, Hungria, Eslovênia e Rússia. (VIEIRA, 2007) Porém, só tornou-se fator primordial após o regulamento geral do Parlamento Europeu sobre a proteção de dados, n.º 2016/679, sendo necessário a adequação das empresas prestadoras de serviço na Europa ao regulamento, influenciado diretamente o Brasil para elaboração da Lei Geral de Proteção de Dados brasileira. (SAAD, 2021).
Muito embora, a Lei Geral de Proteção de Dados Pessoais - LGPD, em sua promulgação, não abarcou de forma expressa a proteção de dados como direito fundamental, a doutrina, em especial Nascimento (2020), por sua vez, já argumentava a proteção de dados e informações pessoais como direito autônomo, derivado do direito fundamental à privacidade, explicitamente no artigo 5°, X, da CRFB de 1988.
Após reiterados julgamento sobre a tutela dos dados pessoais como extensão da personalidade do indivíduo, o Supremo Tribunal Federal -STF reconheceu no Julgamento da Ação Direta de Inconstitucionalidade - ADI 6387, a existência dos dados como direito autônomo, derivada do direito fundamental a dignidade da pessoa humana, na proteção à intimidade e a centralidade do Habeas Data como autodeterminação informativa. (NASCIMENTO, 2020).
Ao compreender a necessidade da proteção aos dados pessoais, os legisladores brasileiros em votação de ? das casas legislativas (câmara e Senado Federal) em dois turnos, aprovaram a Emenda Constitucional 115 de fevereiro de 2022, alterando o artigo 5° da Constituição Federal de 1988, incluindo o inciso LXXIX, tutelando constitucionalmente a proteção aos dados pessoais, inclusive nos meios digitais.
Ressalta-se, ainda, que os dados pessoais estão interligados com o direto fundamental à

privacidade, na qual representa a capacidade de a pessoa administrar sua vida, seus pertences e

propriedades materiais e imateriais, permitindo ou não a utilização dos seus dados (bens imateriais) por terceiro. (NASCIMENTO, 2020).

A privacidade, por sua vez, segundo Mendes (2008), é o direito à proteção aos comportamentos pessoais e acontecimentos de caráter íntimo, bem como as informações prestadas aos profissionais e comerciantes, em que a pessoa não deseja que se compartilhe com o público.

Para o professor William Prosser, pode-se qualificar a lesão a privacidade em quatro graus: i) o intrometimento na reclusão ou solidão na vida privada, ii) a divulgação pública de fatos privados constrangedores sobre o indivíduo; iii) a publicidade sobre o indivíduo apresentada de forma equivocada; e iv) a apropriação, para obtenção de vantagem, do nome ou da imagem do demandante (PROSSER, 1960).

A doutrina, por sua vez, defende mais uma violação à privacidade: a privacidade informacional, interligada com os fatores tecnológicos de informação. (SAAD, 2021). Assim, quando a lei ao realizar o tratamento da privacidade, refere-se como um direito líquido, ao qual será tutelado para garantir que o indivíduo tenha um local reservado, que não tenha, se desejar, a interferência de outros sujeitos, seja pessoa física ou jurídica.

Com a proteção dos dados pessoais dos titulares, através da LGPD, possibilitou ao cidadão o acesso a informações ao ciclo de vida útil dos dados pelas empresas, e a certeza de fiscalização pela Autoridade Nacional de Proteção de Dados, com a finalidade de atingir os objetivos traçados pela legislação, na qual a lei traz conceitos e delimita princípios, que devem ser mencionados.

A LGPD tem como objetivo principal: ?o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado?, com a destinação de assegurar os direitos fundamentais a liberdade e privacidade dos titulares dos dados, bem como tutelar a dignidade e a personalidade da pessoa natural. (LGPD).

A legislação está ordenada diretamente com o meio empresarial, sobretudo no que se refere aplicação aos seus destinatários que são pessoas físicas ou jurídicas que realizam a coleta e tratamento de dados no Brasil, conforme preceitua o artigo 1° da lei 13.709, de 14 de agosto de 2018.

Para compreender a LGPD, faz-se necessário elucidar os conceitos de dados pessoais: (art. 5º, I) é toda informação relacionada a pessoa natural, identificada ou identificável, sendo o dado aplicado no contexto que possibilite o reconhecimento do indivíduo. Bem como refere-se aos dados sensíveis (art. 5º, II), são todas as informações que se relaciona com pensamentos políticos, crenças,

identidade biológica e física. Portanto, a legislação tem como ponto a proteção e o cuidado para a não violação dos dados pessoais e sensíveis.

Os doutrinadores, Laura Schertel e Danilo Doneda, ainda aponta cinco pilares para compreender a LGPD, sendo: i) a unidade e generalidade da aplicação da Lei; ii) a legitimação

para o tratamento de dados (hipóteses autorizativas); iii) os princípios e direitos do titular; iv) as obrigações dos agentes de tratamento de dados e v) a responsabilização dos agentes.
O primeiro pilar é considerado com aplicabilidade material da legislação, ou seja, aplica-se a qualquer operação realizada por pessoa natural ou jurídica de direito público ou privado, independentemente do meio, da sua sede ou do país onde estejam localizados os dados (Art. 3°). Considerado, assim, como uma aplicação uniforme para todos os setores público ou privados que realizam tratamento de dados.
O segundo pilar é a legitimação para o tratamento de dados, tendo em vista que a lei especificou critérios e requisitos para o reconhecimento da legitimidade, não podendo ser tratados os dados, sem que exista uma base normativa que autorize, prevista no artigo 7°, 11° ou 23° da LGPD, abordando 11 (onze) hipóteses, incluído o consentimento ou a previsão legislativa.
Destaca-se que a autorização por consentimento para ser considerado válido, deve observar os requisitos previsto no artigo 5°, XII, sendo considerado que a vontade deve ser livre, informada, inequívoca e com a finalidade determinada, consagrando os princípios norteadores da legislação.
O terceiro pilar é o conjunto de princípios e direitos que assegura o destinatário da lei a controlar a utilização do seu dado pessoal, sendo importante elencar dez princípios que estruturam a LGPD: a finalidade, a adequação, a necessidade, o livre acesso, a qualidade dos dados, a transparência, a segurança, a prevenção, a não discriminação e a responsabilização. (MENDES, DONEDA, 2018)
No que concerne, aos direitos dos titulares são expressos no artigo 18° da referida lei, que permite o titular dos dados adquirir através do controler, independentemente do momento, as informações relacionadas ao indivíduo, prevendo: acesso, confirmação, correção, anonimização, bloqueou ou eliminação e a portabilidade.
Para adentrar no cerne dos problemas enfrentados pela legislação, em especial, sobre o vazamento de dados, os dois últimos pilares serão abordados sob a perspectiva da violação e responsabilização acerca da proteção de dados nos casos incidentes de vazamento.

Assim, o quarto pilar, destina-se às obrigações dos agentes de tratamento dos dados, na qual estabeleceu limites que devem ser observados nas operações realizadas para reforçar a segurança e prevenir os problemas da atividade no tratamento de dados.
Uma das obrigações fundamentais, consiste na intitulação do encarregado pelo tratamento dos dados indicados pelo controlador, conforme artigo 41 da LGPD, que possui a função de aceitar as reclamações e comunicações dos sujeitos dos dados, receber informações da Autoridade Nacional, como deve orientar os funcionários a respeito das práticas a serem adotadas em relação à proteção de dados pessoais.
Assim, as informações devem ser fornecidas ao proprietário dos dados, quando os dados forem coletados, como: os meios de segurança aderidos ao tratamento de dados, quais são os riscos da atividade que podem gerar lesão ao titular, pois pode gerar a mitigação dos prejuízos. (SAAD, 2021)
A lei Geral de Proteção de Dados Pessoais tem como objetivo a proteção do dados pessoais dos titulares dos dados, sendo assim, uma das obrigações principais é adoção de medidas de

segurança, técnicas e administrativas hábeis a proteger os dados pessoais de acessos não autorizados, como promover a integralidade dos dados, não permitindo, assim, a alteração das informações, a prevenção de situações ilícitas ou acidentais, ou qualquer forma de tratamento inadequado, consoante se desprende do artigo 46 da lei.

Tornou-se corriqueiro manchetes acerca do vazamento de dados por corporativas, uma das violações mais graves incidentes abarcados pela LGPD, o que ocasiona a vulnerabilidade do titular dos dados, e dos sistemas internos que são responsáveis pelo ciclo de vida útil dos dados. (SAAD,2021)

A seção de segurança de informação tem como condão as obrigações inerentes aos agentes de tratamento, devendo ser adotado pela integralidade das pessoas que realizam o tratamento de dados, garantido que os dados sejam confidenciais, bem como disponíveis nas operações de tratamento. (Art.48). Nos casos incidentais de vazamento de dados, insurge a necessidade ao controlador de informar a autoridade de proteção de dados, que podem definir as medidas para mitigação dos danos.

No entanto, com a utilização da internet, compras online, transferência virtuais e outros meios tecnológicos, criou-se uma dificuldade para atuar na segurança de dados, tendo em vista a abrangência e os domínios de redes globais, que combinados com fatores não perceptível, forma

um perfil não rastreavel capaz de ocasionar violação às diretrizes básicas da legislação, que mesmo com ações posteriores não conseguem excluir os inúmeros registros de pessoas e organizações que coletaram os dados, lesionando a confidencialidade das informações (SAAD, 2021)

Destaca-se que as obrigações aos controladores e operadores, devem ser observados desde a coleta dos dados até seu descarte, assim o artigo 46 da LGPD, introduziu o conceito de privacy by design, sendo a incorporação pelas empresas nos serviços e produtos, na qual dispõe a proteção da privacidade no centro de todo o desenvolvimento corporativo.

Embora, a legislação tenta dirimir os riscos da atividade, os prejuízos causados pelo vazamento de informações são altos, e perpassam pela inadequação do sistema de proteção, perda de credibilidade e de clientes, ocasionado uma ruptura na imagem da empresa, impossibilitando, muitas vezes de concorrer no mercado corporativo. (SAAD,2021)

Portanto, a LGPD concebeu obrigações aos agentes de tratamento de dados, para que se delimite a finalidade da utilização dos dados desde o início da concepção, devendo o controlador confeccionar relatório de impacto a privacidade, utilizando de métodos para a captação da operação do ciclo de vida dos dados, observando as mediadas adotada para aumentar a segurança e mitigar o risco do tratamento das informações, conforme artigo 3 da LGPD.

O último pilar, considerado como a responsabilidade dos agentes na incidência de ocorrência de danos derivados do tratamento de dados. A LGPD consagrou a natureza do tratamento, limitando os parâmetros ao artigo 7° da lei, nas 10 hipóteses dos incisos, vinculados a finalidade da captação dos dados, consoante prevê o artigo 6°, inciso I, II, da LGPD.

A legislação tem como regra o descarte (eliminação) dos dados ao fim do tratamento da operação (art. 16), com o intuito de mitigar os riscos presente no tratamento de dados, principalmente, no que concerne à limitação das hipóteses de tratamentos para não lesionar os

direitos dos titulares.
Nos casos, em que mesmo após o término de vida útil dos dados, as empresas podem, quando permitido, armazenar dados que em situação incidentais serem objetos de violação, principalmente nos casos de vazamento, que podem ocorrer, quando não autorizados pelo titular ou controladores, serem acessados, captados, compartilhados pela internet, para outros sujeitos ou empresas.
Assim, a Lei Geral de Proteção de dados Pessoais, em especial em seu artigo 42, dispõe que o controlador ou operador, quando realizar o exercício do tratamento de dados pessoais, vem

a ocasionar dano patrimonial, moral, individual ou coletivo em detrimento a aplicação da legislação, é obrigado a repará-lo, definindo a responsabilidade de forma objetiva.
Embora, a responsabilização objetiva não é necessária a demonstração de culpa do controlador ou operador. Faz mister esclarecer que o operador, só será responsabilizado quando os atos praticados forem contrário à legislação, ou às instruções que foram fornecidas pelo controlador. (MENDES, DONEDA, 2018)
Ainda, a legislação prevê exceções a responsabilidade objetiva (art. 43), sendo: quando o agente demonstrar que não realizou o tratamento de dados pessoais que foi atribuído, ou quando não houve violação da segurança ou a legislação, e por fim, quando for por culpa exclusiva do titular ou de terceiros.
Porém, o cenário que é vislumbrado no Brasil nos casos de vazamento de dados, é que as violações pelas instituições vêm ocorrendo, majoritariamente, sob ataques deliberados de hacker, ou falha de segurança dos controladores dos dados. (SAAD, 2021)
Dessa forma, é necessário adotar medidas para dirimir os riscos da atividade, e possibilitar o discernimento das informações acerca dos perigos de vazamento de dados, tendo em vista que a tendência é aumento significativo das violações vinculados com a crescente tecnológica. Assim, as empresas devem implementar mecanismos para a segurança das informações.

5 O COMPLIANCE EMPRESARIAL COMO INSTRUMENTO DE PROTEÇÃO DE DADOS NA ESFERA EMPRESARIAL

Em decorrência das constantes violações aos dados armazenados em provedores privados, a tutela ao direito à privacidade nos meios tecnológicos, já era pauta de debate na legislação brasileira, e já existiam mecanismos para a proteção, como: a proibição de direcionamento dos provedores em relação ao compartilhamento de dados, bem como a inibição ao monitoramento nos navegadores de internet.
Vinte e seis bilhões de dados foram vazados no Brasil em 2019, de acordo com pesquisas realizadas pelo Massachusetts Institute of Tecnology ? MIT, possibilitando a utilização de números telefônicos, score de crédito, endereço eletrônico, fotos, números de identificações e outros dados pessoais, para o cometimento de crimes cibernéticos, e a violação aos direitos dos titulares.
A utilização e uso dos dados pessoais por pessoa física ou jurídica, com sede no Brasil ou não, devem se atentar as normas gerais de proteção aos dados brasileiro, segundo Frazão, Oliva e

Abilio (2020), é a necessidade de conferir a efetividade aos direitos e prevenir a violação aos dados, através da implementação de mecanismo de compliance, como uma ferramenta capaz de promover a adequação das atividades aportadas pelas empresas.
Assim, os controladores e operadores poderão formular regras de boas práticas e governança (Art. 50), que contenha as disposições de organização interna, o regime de funcionamento, as operações, o canal de comunicação entre os encarregados e os titulares dos dados, e o procedimento de segurança.
Nessa perspectiva, considerando que a maioria das tratativas de dados perpassam por meios digitais, deve-se adotar sistema para mapear os riscos, e implementar mecanismos para minorar as vulnerabilidades apontadas pelos programas, através da alta administração, do código de ética, para proteger os dados pessoais dos titulares. (PESSOA, 2021)
Existem inúmeras formas de ocorrer o vazamento de dados, sendo através de ataques cibernéticos, sequestro de conta, furtos de dados, compartilhamento de dados por agentes ou ex-agentes da empresa, erro ou negligência, entre outros, que podem ser para adquirir dados de nomes, CPF, celulares, endereços, dados financeiros, senhas, registro de saúde ou credenciais de acesso. (SAAD, 2021)
Desse modo, para realizar o mapeamento dos problemas que as corporativas podem enfrentar, é necessário identificar os fluxos e processos de informação que percorrem os sistemas, que irão auxiliar na tomada de decisão pelas empresas. (NASCIMENTO, 2020)
A alta administração deverá colaborar ativamente no programa de compliance, seja monitorando as investigações e intervenções em situação para estabelecer controles internos em conformidade com a legislação, bem como possibilitar a interdependência dos setores para realizar as atividades designadas para o tratamento de dados (PESSOA, 2021).
Com a elaboração do código de ética pela organização possibilitará o treinamento regular das equipes, responsáveis pela tecnologia da informação, para enraizar a cultura corporativa da boa governança, com a finalidade de assegurar o respeito ao programa de compliance (NASCIMENTO, 2020)
Nesse contexto, para manter uma boa relação com seus clientes, as organizações devem instalar canais de comunicação, para que os titulares dos dados possam contatar os encarregados responsáveis pelos armazenamentos dos seus dados, e exerçam seus direitos sobre as informações contidas nos provedores. (PESSOA, 2021).

Desse modo, quando se trata de concretização a alteração cultural coportariva é preciso realizar o alinhamento dos funcionários com o código de ética, com política de privacidade, para fins de efetividade do programa de compliance de dados. (PESSOA, 2021).

5.1 A IMPLEMENTAÇÃO DE MECANISMOS DE GOVERNANÇA DE DADOS

PESSOAIS
Para a efetividade da legislação em relação ao tratamento de dados, a LGPD direciona um capítulo para implementar o programa de governança em privacidade, com a finalidade das empresas adotarem medidas técnicas, para fins de proteção e segurança dos dados pessoais. (PESSOA, 2021)
A governança em privacidade, pode ser conceituada como um conjunto de regras e práticas positivas a serem implementadas pelos agentes de tratamento, e encontra-se em conformidade com as políticas de compliance empresarial, com o objetivo de gerir os dados das empresas para estabelecer um diferencial competitivo aos negócios. (KOEPSEL,2020)
O programa integra o aperfeiçoamento do procedimento de utilização dos dados, com os requisitos pré-estabelecidos na implementação dos softwares, com a finalidade de gerir de forma otimizada os dados para preencher as diretrizes da legislação. (SAAD, 2021)
A Lei Geral de Proteção de Dados Pessoais dispôs que os controladores e operadores poderão adotar programas de governança em privacidade, que devem ser implementados com o mínimo, (art. 50, § 2°, I): a) o comprometimento dos agentes de tratamento com as políticas internas que devem garantir o cumprimento das normas e regras de boas práticas; b) que aplicação seja de forma uniforme para todo a operação de tratamento de dados; c) que a governança seja adaptativa as estruturas da empresas, sendo compatível com a densidade dos dados e operação; d) como implementar políticas de salvaguardas em relação aos titulares dos dados; e) tenha como objetivo estabelecer uma relação de confiança com sujeitos dos dados, estabelecendo situações de transparência e que possibilite a atuação do titular; g) que conte com planos de respostas a incidentes e remediações; h) seja continuamente atualizado sua base.
Nesse aspecto, devem ser adotadas medidas administrativas para que as instituições, em conformidade com a legislação, apliquem estímulos para assegurar as informações armazenadas pelas empresas, com a adoção de orientações internas que respeitem as diretrizes que inclua o uso

minimizado ou a anonimização das informações, desde a coleta dos dados, conforme artigo 46 da LGPD.
Com o mapeamento das atividades, é importante verificar: O que são esses dados?; de que forma foram coletados ?; quem são os coletores ?; existe relação entre os dados e atividade realizada ?; O que pode ocorrer com esses dados ao serem coletados? E, como são descartados da gestão organizacional da empresa? (NASCIMENTO, 2020). Dessa forma, para adotar medidas compatíveis com os riscos alertados pelos sistemas para a proteção de dados nas organizações privadas, é necessário possuir conhecimento do caminho realizado inerentes ao ciclo de vida útil dos dados.
Embora, a legislação já estabeleça diretriz mínima para o tratamento de informação, a Autoridade Nacional de Proteção de Dados - ANPD, poderá, ainda, determinar padrões técnicos para serem implementados pelo programa de governança em privacidade, devendo ser observado a qualidade de dados, as especificações do tratamento e status tecnológico, em especial a proteção aos dados sensíveis disposto na legislação. (NASCIMENTO, 2020)
Muito embora, a lei geral de proteção de dados, apenas delimita as características e os

requisitos mínimos que os operadores deverão tomar para desenvolver um compliance na organização das empresas privadas em consonância com a legislação, porém não impõe um modelo específico para integração de um programa nas corporativas. (PESSOA, 2021)
Assim, para Saad (2021), as medidas técnicas que podem ser adotadas pelos agentes de tratamento de dados, são: i) o uso de firewalls, sendo um mecanismo de segurança que coleta os dados em conformidade com as regras pré estabelecido para análise de tráfego de rede, delimitando as operações de compartilhamento e captação de informações a serem cumpridas; ii) a utilização de antimalware, que consiste na proteção contra vírus que é capaz de fragilizar o sistema, apagar dados e infectar outros arquivos; iii) a utilização de criptografia dos dados, que possibilite quando ocorrer situações incidentais a não identificação do titular do direito.
Já para Fernandes e Abreu, (2014) defendem a implementação de frameworks como a DAMABOK e COBIT, para o gerenciamento de dados, pois tem como meta principal a delimitação do escopo das atividades, as funções envolvidas no tratamento e as interações a serem executadas pelo software, com a finalidade de proteger a privacidade em ambientes corporativos que gerenciam o armazenamento de informações aplicados na prevenção à fraude.

Segundo Carvalho (2021), a integração do software, através das boas práticas estabelecidas pela legislação, poderá aprimorar os aspectos de proteção à privacidade e prevenção a fraude do tratamento de coleta de dados. Tendo em vista, que os frameworks, podem balizar as métricas de qualidade dos dados que indicam uma utilização adequada e otimizada, e aponta a melhor proteção da privacidade.
Com a melhoria de processo de governança para o tratamento de dados, estabelece uma divisão entres as operações que possibilita uma automatização do ciclo de vida dos dados (coleta, utilização, armazenamento e exclusão), capaz de gerar relatório de risco, para o auxílio da tomada de decisão com o intuito de gerir de forma adequada o tratamento de dados. (CARVALHO, 2021)
Neste parâmetro, os programas de compliance com a implementação de frameworks, podem responder questionamento acerca do procedimento de tratamento de informação, dispondo de quais práticas relacionadas à governança, privacidade e segurança de dados, apresentam melhor benefício para o tratamento de dados pessoais. (CARVALHO, 2021)
Ademais, os controladores e operadores deverão adotar medidas, como o Relatório de Impacto ? DPIA), que corresponde a avaliação dos riscos e impactos relacionados com o tratamento de dados pessoais, além da anonimização, da transparência e do sigilo, deverão delimitar prazos para retenção de dados e aderir políticas seguras de informação acerca da operação de tratamento. (SILVA, 2022)
Após realizar a implementação e observância das estruturas mínimas estabelecidas pela LGPD, é necessário adotar um programa de gerenciamento de vulnerabilidades, com atualizações constantes e autocorreções alinhados com as boas práticas de atividades cotidianas, com a finalidade de proteger os dados pessoais, e promover um ambiente corporativo adequado para realizar o tratamento de dados. (SAAD, 2021)
No entanto, ao verificar que houve vazamento de dados, seja pelo recebimento de notificação ou pela veiculação na mídia, os agentes de tratamentos deverão identificar quais dados

vazaram e realizar o procedimento estabelecido no programa de compliance de segurança, além de notificar as instituições. (Art. 48, caput).
De acordo com MIT, o prazo entre a comunicação à autoridade competente e a ocorrência do fato ilícito ultrapassa 200 (duzentos) dias em média, sendo umas das preocupações para a efetividade da legislação, e a redução dos danos causados aos titulares dos bens imateriais.

A Lei Geral de Proteção de Dados, dispõe que nas situações que ocorrer a probabilidade de riscos ou violação aos direitos dos titulares, tem como obrigação do encarregado a comunicação à autoridade nacional e ao titular do dado (art. 48, caput). Sendo que o contato deve ser em período razoável (art. 48, § 1º), contendo a natureza dos dados dos titulares atingindo (art. 48, § 1º, I).
Em decorrência dos possíveis incidentes, a LGPD determinou critério para aplicação de sanções, em casos de vazamento de dados, observando as situações específicas de cada caso, disposto no art. 52, § 1º. Assim, deve ser considerada a avaliação da gravidade, a natureza das informações e do dano ocorrido (incisos I e VI), sendo necessário para este caso, tendo em vista que o compartilhamento indesejado de dados sensíveis pode ocasionar danos irremediáveis para os titulares.
Portanto, existe a necessidade da adesão aos mecanismos e técnicas para promover a efetividade dos programas internos com a finalidade de mitigar os danos, assim, a implementação de boas práticas e governança têm como fator o cumprimento da legislação, por meio de medidas de segurança. Entende-se, que a proteção integral contra falhas que possibilitam a ocorrência de ilícitos não é possível, porém essas diretrizes reduzem as possibilidades de existir desvios de condutas e criar salvaguardas para identificação dos incidentes, de forma eficaz, rápida e adequada.

6 CONSIDERAÇÕES FINAIS

A partir da permissão ao acesso dos dados pessoais, as informações coletadas passaram a integralizar as redes de tratamento de dados, tornando-se alvo de ataques cibernéticos, contribuindo para o aumento da intercorrência no ambiente corporativo, tornando-se o gerenciamento de informação um dos diferenciais no desenvolvimento do negócio.
Nesse contexto, foi imperativo o surgimento de leis que protejam os dados dos cidadãos, e que limitem a gestão das entidades públicas e privadas em relação as informações coletadas, transformando o sistema organizacionais, como compliance, em ferramentas de efetivação das normas éticas e legais. Assim, a implementação do programa alinhado com a governança corporativa é capaz de integralizar o corpo de normas internas com o intuito de adequar a legislação brasileira e criar uma cultura corporativa.
Dentro do programa de compliance, a administração em conjunto com a gestão da empresa, poderá implementar ao plano diretor, a utilização de software, sendo este capaz de possibilitar a

automatização do ciclo de vida útil dos dados para realizar o auxílio da tomada de decisão, com o intuito de mitigar os possíveis danos decorrentes da violação aos dispositivos da Lei Geral de Proteção de Dados Pessoais.
Nesse sentido, para realizar uma proteção extensiva aos direitos dos titulares dos dados, a LGPD integrou ao seu corpo de normas-condutas a serem adotadas pelos operadores do tratamento de dados, com escopo de preservar a integralidade, a qualidade e o sigilos dos dados, tendo como consequência da violação, a majoração de sanções pecuniárias.
Embora, o vazamento de dados ocorra de forma ordenada, a implementação de sistema de segurança nas corporações implica na diminuição de situações incidentais por erro humano, ou inadequação dos programas empresarias, assim, devendo a gestão ensejar esforços para que a proteção dos dados seja preservada, desde a concepção do serviço.
Para a efetivação da Lei Geral de Proteção de Dados Pessoais, as empresas devem realizar a adequação de medidas de boas práticas e governança em privacidade para mitigar os possíveis danos decorrente da violação aos dados em provedores privados. Mesmo que a proteção aos dados de forma concreta não seja possível, as adoções de mecanismo de segurança podem atenuar as sanções e as perdas aos titulares dos dados.

REFERÊNCIAS

BARATA, André Mantola. Governança de dados em organizações brasileira: uma avaliação comparativa entre os benefícios previstos na literatura e os obtidos pelas organizações. 2015. Dissertação (Mestrado em Sistema de Informação) - Universidade de São Paulo, São Paulo, 2015.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, [2022]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 15 abr. 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidente da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 abr. 2023.

BERTOCCELLI, Rodrigo de Pinho. Compliance. In: CARVALHO, André Castro et. al. Manual de compliance. Rio de Janeiro: Forense, 2019. p. 35.

CANDELORO, Ana Paula; RIZZO, Maria Balbina Martins De; PINHO, Vinícius (Coord). Compliance 360: riscos, estratégias, conflitos e vaidades no mundo corporativo. São Paulo: Trevisan, 2012.

CARVALHO, A. P. Proposta de um framework de compliance à Lei Geral de Proteção a Dados Pessoais (LGPD): um estudo de caso para prevenção a fraude no contexto de big data. 2021. Dissertação (Mestrado em Engenharia Elétrica) - Universidade de Brasília, Brasília, 2021.

CARVALHO, Andre Castro. Manual de compliance. 3. ed. Rio de Janeiro: Forense, 2021.

CASAES, Júlio César Costa. Governança de dados abertos governamentais: frameworks conceitual para as Universidades Federais, baseada em uma visão sistemática, 2019. Tese (Doutorado em Engenharia e Gestão do Conhecimento). Universidade Federal de Santa Catarina, Florinaóplis, 2019.

DATA GOVERNANCE INSTITUTE (DGI). Definitions of data governance. 2017. Disponível em: http://www.datagovernance.com/adg_data_governance_definition. Acesso em: 01 mai. 2023.

ENDEAVOR DO BRASIL. Prevenindo com o Compliance para não remediar com o caixa. In: ENDEAVOR. [S. l.], 26 abr. 2017. Disponível em: https://endeavor.org.br/pessoas/compliance/. Acesso em: 15 mar. 2023.

ESPÍNDOLA, P. L.; SALM JUNIOR, J. F.; ROSA, F.; JULIANI, J. P. Governança de dados aplicada à ciência da informação: análise de um sistema de dados científicos para a área da saúde. Revista Digital de Biblioteconomia & Ciência da Informação, Campinas, v. 16, n. 3, p. 274-298, 2018.

FERNANDES, Aguinaldo Aragon; DE ABREU, Vladimir Ferraz. Implantando a governança de TI: da estratégia à gestão de processos e serviços. 4. Ed. Rio de Janeiro: Brasport, 2014.

FRAZÃO, Ana. Programas de compliance e critérios de responsabilização de pessoas jurídicas por ilícitos administrativos. In: ROSSETTI, Maristela Abla; PITTA, Andre Grunspun. Governança corporativa: avanços e retrocessos. São Paulo: Quartier Latin, 2007. p. 42

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. A Lei Geral de proteção de Dados Pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

HONÓRIO, Roseli. Modelo conceitual de governança de dados como suporte à governança do conhecimento organizacional. 2022. Dissertação (Mestrado em Engenharia e Gestão do Conhecimento) - Universidade Federal de Santa Catarina, Florianópolis, 2022.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC). Guia das melhores práticas de governança para cooperativas. São Paulo, 2015. Disponível em http://www.ibgc.org.br/ userfiles/files/2014/files/CMPGPT.pdf

JOHNSON, Ralph E.; RUSSO, Vincent. Reusing object-oriented designs. Relatório Técnico da Universidade de Illinois, UIUCDCS 91-1696, 1991.

KLEINDIENST, Ana Cristina. Grandes temas do direito brasileiro: compliance. São Paulo: Almedina Brasil, 2019

KOEPSEL, Alice de Medeiros. Adoção e efeitos dos programas de compliance à luz da Lei Geral de Proteção de Dados Pessoais. 2020. Monografia (Graduação em Direito) -Universidade do Sul de Santa Catarina, Florianópolis, 2020.

LIMA, C., BASTOS, R. C. A criação de conhecimento apoiada pela governança de dados. In: CONGRESSO INTERNACIONAL DE CONHECIMENTO E INOVAÇÃO, 2019, Santa Catarina. Anais eletrônicos [...]. Santa Catarina Disponível em: https://proceeding.ciki.ufsc.br/index.php/ciki/article/view/647. Acesso em 10 Mar. 2023.

MARTIGNAGO, Deisi et al. Governança de dados aplicado no processo de catalogação. Revista Brasileira de Biblioteconomia e Documentação, São Paulo, V.15, n. 2, 2019.

MENDES, Gilmar Ferreira. Curso de direito constitucional. 2. ed. São Paulo: Saraiva, 2008.

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. São Paulo: Revista de Direito do Consumidor, 2018.

NASCIMENTO, Suellen Lima do. A lei Geral de Dados Pessoais e a Adoção dos Programas de compliance na sociedade da Informação. 2020. Monografia (Graduação em Direito) - Centro Universitário de Brasília, Brasília, 2020.

PESSOA, Larissa Rocha de Paula. Os desafios da Governança de dados e a realidade cultural brasileira. 2021. Dissertação (Mestrado em Direito) ? Universidade Federal do Ceará, Fortaleza, 2021.

PINTO, S. C. C. S.. Composição em Web Frameworks, 2000. Tese (Doutorado em Informática) Pontifícia Universidade Católica do Rio de Janeiro, Rio Janeiro, 2000.

PROSSER, William L. Privacy. California Law Review. California, v. 48, n. 3. p. 383 ? 423, agosto, 1960.

RÊGO, Bergson Lopes. Gestão e governança de dados: promovendo dados como ativo de valor nas empresas. 1. ed. Rio de Janeiro: Brasport, 2013,

ROQUE, Pamela Romeu. Estudos aplicados de direito empresarial: LL.C. em direito empresarial. São Paulo: Almedina, 2019.

SAAD, Carolina de Oliveira. A lei geral de proteção de dados pessoais e incidentes de segurança: regulação e prática de vazamento de dados, 2021. Monografia (Graduação em Direito). Fundação Getúlio Vargas. Rio de Janeiro, 2021.

SANTANA, Ricardo Cesar Gonçalves. Ciclo de vida dos dados e o papel da ciência da informação. In: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO. 14., 2013. Florianópolis. [?]. Florianópolis: UFSC, 2013. Disponível em: http://enancib2013.ufsc.br/index.php/enancib2013/%20XIVenancib/paper/viewFile/284/319. Acesso em: 13 mar. 2023.

SILVA, Ana Laura Fonseca. O papel das Soft Skills na implementação efetiva dos programas de compliance com foco na adequação à Lei Geral de Proteção de Dados ? Lei N° 13.709/18. 2022. Monografia (Graduação em Direito) - Universidade Federal de Ouro Preto, Ouro Preto. 2022

SILVA, Eggon João da. A defesa da ética e transparência. In: VENTURA, Luciano Carvalho. Governança corporativa. São Paulo: Saint Paul Editora, 2005, página 259.

TERRA, Priscila de Mello. A influência da governança de dados na gestão estratégica, 2017. Monografia (Bacharelado em Sistema de Informação) - Universidade Federal Fluminense, Niterói, 2017.

VAZAMENTO de dados aumentaram 493% no Brasil, segundo pesquisa do MIT.VEJA, São Paulo, 24 fev. 2021. Sociedade. Disponível em: https://vocesa.abril.com.br/sociedade/vazamentos-de-dados-aumentaram-493-no-brasil-segundo-pesquisa-do-mit. Acesso em: 15 mar. 2023.

VIEIRA, Tatiana Malta. O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante da tecnologia da informação. Porto Alegre: Sergio Antonio Fabris Editor, 2007.