



ÉTICA E RESPONSABILIDADE SOCIAL

AULA 6



Prof. Claudio Marlus Skora



CONVERSA INICIAL

Metodologias gerenciais da ética e da responsabilidade social

Infelizmente, a mídia tem como pauta frequente, quase diária, a ocorrência de problemas ambientais e sociais. Isso acontece, obviamente, porque o assunto é de interesse das pessoas. Cada vez mais pessoas estão engajadas em atividades em defesa do desenvolvimento sustentável e as mídias sociais favorecem isso. Sabendo disso, as organizações buscaram minimizar seus impactos socioambientais e evitar que suas marcas fossem atreladas a ações que infringissem a ética, além de atentar-se às mudanças de legislação que passaram a exigir esse comportamento.

Para se adequar às normas existentes e não impactar os *stakeholders* com notícias que pudessem prejudicar a sua imagem, as organizações recorrem a ferramentas de gestão que possam ser implantadas de maneira alinhada à estratégia do negócio. Muitas dessas metodologias são compatíveis com as diversas vertentes de gestão empresarial, pois têm caráter orientativo, o que garante liberdade de adaptação para cada diferente realidade organizacional. É relevante apontar, em adição, que elas também podem ter intensidade diferente quanto a cada uma das dimensões da sustentabilidade, sendo a orientação de ação de responsabilidade da empresa ser definida sobre a ótica social, econômica ou ambiental.

Sabe-se que as realidades organizacionais são complexas, pois estas estão inseridas em um mundo complexo. Ao se tratar de responsabilidade social, isso não seria diferente. Barbieri e Cajazeira (2021) defendem que “uma questão tão complexa como a responsabilidade social empresarial, que envolve assuntos tão diversos e com inúmeras interações entre eles, só pode ser suficientemente inserida em uma organização por meio de várias ferramentas de gerenciamento.” É por esse motivo, então, que se procurou padronizar técnicas de gestão e uniformidade de conceitos para que fossem evitadas dúvidas semânticas entre organizações, pesquisadores, clientes, colaboradores e todas as demais partes interessadas. Foi nesse contexto, então, que surgiram elementos como o *compliance* e a governança corporativa, exigidos hoje de empresas que se apresentam ao mercado em busca de investidores.

Da mesma forma, foi estabelecido padrões de governança corporativa, que foram disseminados via *benchmarking*, popularizando o que se conhece por melhores práticas de gestão neste tópico. Como elementos recentes de preocupação ética,



surge também a preocupação com a proteção de dados pessoais, por meio de legislação que norteia ações nesse sentido, fruto de tempos em que *big datas* orientam ações de *marketing*, recursos humanos e registram cada ação de cada pessoa, seja no mundo virtual ou físico. Pelo fato de que o mundo contemporâneo não pode ser compreendido sem que se considere a importância das pessoas jurídicas que o habitam, e mesmo o poder que estas possuem nas pessoas físicas que as compõem, é que esta aula objetiva apresentar algumas metodologias corporativas de ética e responsabilidade social.

TEMA 1 – COMPLIANCE

1.1 Compreendendo o conceito

Compliance, obviamente, é uma palavra inglesa derivada do verbo *to comply* e adotada em português como forma de expressar *estar em conformidade*. A tradução do termo *compliance* está associada à compreensão do que é aceito pela maioria como o que é correto e que, por isso, está em conformidade com alguma determinação *a priori*. Outras formas de entender *compliance* estão associadas à compatibilidade, adequação, harmonia.

Idowu *et al.* (2015) aponta que esse termo, quando inserido no meio organizacional, está alinhado à vontade de atender a um desejo, solicitação ou demanda para cumprir com normas como leis, tratados, acordos, especificações, políticas e padrões estabelecidos. Outra maneira de entendê-lo não é somente pelo fim da ação (estar em *compliance*), mas também pelo processo de se fazer o que é necessário ou esperado para fazer (buscar o *compliance*) ou, mais ainda, como um comportamento esperado (viver em *compliance*).

Se essas ações são feitas em virtude de conformidade regulatória, Idowu *et al.* (2015) descrevem, então, que o *compliance* versa sobre o objetivo ou a meta que corporações ou setores públicos aspiram conseguir cumprir leis e regulamentos relevantes. Nota-se, porém, muitos regulamentos que regem os diversos setores da economia e, por isso, essa tarefa não parece ser das mais fáceis. Estar em *compliance*, ou seja, em harmonia com as leis, exige capacidade de planejamento severa, de modo a que se possa garantir que todos os requisitos de governança necessários possam ser atendidos sem a duplicação desnecessária de esforços e uso de recursos.



Belarmino (2020) descreve que o termo teve repercussão no Brasil a partir da década de 1990, durante o governo Collor de Mello. Tal fato deriva das medidas econômicas tomadas durante esse governo, que impulsionou o comércio internacional e a globalização em terras nacionais. O intercâmbio entre agentes internos e externos resultou na pressão para que as organizações brasileiras passassem a adotar regras de transparência na gestão, as quais já eram praticadas no exterior.

Um dos primeiros setores a adotar essas medidas foi o de finanças, que engloba bancos, corretoras de valores e demais instituições correlatas. Para estes, o cumprimento de normas é necessário para garantir a transparência e para prevenir ou evitar fraudes, como apontam Idowu *et al.* (2015). Por isso, os colaboradores de organizações desse setor são encorajados a realizar capacitações frequentes sobre as leis que regem as atividades financeiras, a obter certificações específicas para que possam trabalhar no setor ou, ainda, aceitar o monitoramento de sua comunicação interna como forma de comprovar que suas atitudes estão *em compliance* com as políticas internas e com aquelas determinadas pelos órgãos regulatórios.

Espera-se que, dessa maneira, a instituição financeira – ou qualquer outra organização – possa abraçar a responsabilidade que a empresa possui em ser transparente, de modo a incentivar uma postura ética de toda a cadeia em que sua indústria está alocada. Para exemplificar o conjunto de regulamentos que podem afetar uma empresa, Barbieri e Cajazeira (2013) elencam alguns instrumentos normativos, conforme os objetivos gerais destes:

Quadro 1 – Instrumentos normativos de responsabilidade social



Objetivos	Exemplos
Prover orientações processuais específicas para implantar e manter sistemas da gestão, programas e atividades, facilitando a mensuração de resultados.	Norma ISO 9001 Norma ISO 14001 Norma SA 8000 Norma AA 1000 Norma OHSAS 18001 Norma ABNT NBR 16001 Norma AFNOR SD 21000 Norma ISO 26000
Garantir a transparência da comunicação com suas partes interessadas.	Balanco Social Indicadores Ethos de Responsabilidade Social GRI – <i>Global Reporting Initiatives</i> Norma ISO 14063
Garantir a integração e compatibilidade entre sistemas de gestão.	Projeto Sigma Guia ISO 72 Critérios de Excelência do Prêmio Nacional da Qualidade PAS 99

Fonte: Barbieri e Cajazeira (2013).

Pela pequena lista de alguns dos regulamentos, mandatórios ou não, que existem e podem nortear uma organização, é que se estruturaram setores, departamentos ou equipes de *compliance* nas empresas, que são responsáveis pelos programas em acompanhar e fiscalizar se estas estão em conformidade com as leis. Sobre este tema, versa o próximo tópico.

1.2 Programas de *compliance*

Belarmino (2020, p. 70) nos apresenta que os programas de *compliance* objetivam “influenciar o comportamento das pessoas, promovendo a implementação de uma cultura corporativa ética, bem como impulsionando condutas em conformidade com regulamentos internos, externos e com as leis, proporcionando maior credibilidade para a empresa”.

Pela visão dos *stakeholders* de uma empresa, se esta possui um programa de *compliance*, é mais fácil dar credibilidade a seus atos. A empresa, perante estes, passa a ter mais integridade e, em épocas de cultura de cancelamento “pipocando” em redes sociais, a preocupação com a imagem deve ser mandatória. Certamente que seguir as normas não pode ser apenas uma obrigatoriedade derivada da lei ou da preocupação com a imagem. Reforça-se o argumento de que o comportamento ético e transparente perante a todos e internalizado na cultura organizacional tem muitas vantagens, tais como:

- incremento da reputação diante dos *stakeholders*;



- ser exemplo e conscientizar colaboradores das virtudes do bom comportamento;
- prevenir riscos derivados das atividades da organização;
- reduzir custos oriundos de possíveis penalizações;
- antecipar soluções para problemas identificados; e
- identificar práticas ilícitas em sua cadeia produtiva ou em outras organizações.

Como apresentado nesta lista, além da visão comportamental e mercadológica sobre os objetivos de um programa de *compliance*, há também fatores pecuniários que fazem com que seja útil ter um programa de ajuste às leis. Se uma empresa está em conformidade, evita-se o pagamento de multas, processos judiciais e outras despesas que possam ser atribuídas em virtude do descumprimento de normas, como defende Bento (2018). Tal programa coloca a organização em um sistema de vigília e prevenção constante, prevendo e minimizando riscos relacionados a problemas jurídicos e processos judiciais, como crê Belarmino (2020).

1.3 Etapas de implantação de programas de *compliance*

Dependendo da fonte de consulta utilizada, será apresentado diferentes etapas – tanto na sua quantidade e na sua forma – para a implantação de um programa de *compliance*. Tal variação reside em muitos aspectos, tais como a quantidade de normas existentes para regular o setor da empresa, o número de profissionais alocados, o faturamento e tantos outros aspectos. Certamente, não existe uma forma única de se fazer isso, até mesmo porque um programa de *compliance* tem implicações diretas na cultura organizacional – influenciando e sendo influenciada por ela – e no estilo de liderança do corpo diretivo da organização. Uma das formas de implantação e um programa de conformidade nas empresas são apresentados no Quadro 2.

Quadro 2 – Etapas de implantação de um programa de *compliance*

Etapas	Descrição
Análise dos riscos envolvidos com as atividades da organização	Devem ser identificados riscos inerentes às atividades da organização. Esses riscos incluem aqueles que podem ser ocasionados por desvios de conduta dos colaboradores em virtude de suas interações internas e externas e, em adição, derivados de relações com o poder público e setor privado. Uma vez identificados, devem ser estruturadas regras de orientação de comportamento coerentes com os valores organizacionais e com a normatização preconizada pelos órgãos fiscalizadores.
Estrutura de planos de ação	Estipule planos de ação para a implantação do programa de <i>compliance</i> de modo que este seja compreensível para todo o time. Nesse planejamento, deve-se incluir modos de prevenir fraudes, bem como



	facilitar a identificação dos responsáveis. No plano deve constar quais mudanças serão necessárias para que a empresa fique em <i>compliance</i> com as regras regulatórias internas e externas.
Detalhamento do código de ética	Um documento formal deve ser elaborado, de modo a conscientizar todos os <i>stakeholders</i> – internos e externos – das diretrizes e regras de conduta defendidas e exigidas pela organização.
Formação da equipe, setor ou departamento de <i>compliance</i>	Um time deve ser formado para que a estes sejam direcionadas as denúncias de falta de cumprimento das normas. Dependendo do tamanho da organização, é salutar estabelecer meios para que as denúncias sejam sigilosas.
Planeje e execute a capacitação dos colaboradores	A transparência e a acessibilidade devem ser os norteadores chaves para um programa de <i>compliance</i> . O documento deve ser compreendido por todos, mediante capacitações, de maneira que não somente o documento seja de conhecimento, mas também os mecanismos de denúncia e fiscalização das condutas. Salutar não envolver somente o público interno, informando a cadeia produtiva também.
Crie formas de verificar a efetividade do programa	A equipe de <i>compliance</i> deve ser empoderada com autoridade para investigar possíveis desvios de conduta. Há sistemas que permitam fazer isso de modo agrupado, registrando entradas e as respectivas respostas apuradas por esta equipe. Além disso, por meio da sistematização, podem ser identificados padrões de comportamento indesejados e com isso criar uma visão preditiva e, com isso, estabelecer reforços de capacitações ou mudanças de normatizações.
Estabeleça a maneira de monitorar o cumprimento do programa e de retroalimentá-lo	Uma rotina de funcionamento do programa de <i>compliance</i> deve ser estabelecida; além disso, deixar evidente a existência do monitoramento para assegurar o cumprimento integral do código de ética. As análises das informações devem estimular revisões do programa de <i>compliance</i> e evitar tanto os desvios como suas perdas.

Fonte: Sikora, 2021.

Essas regras denotam os passos para a criação de um programa de *compliance* generalista, para organizações de porte médio a grande. Informa-se, como é de se esperar, que outros portes devem buscar a adequação dos passos de modo que a criação deste time de *compliance* não seja disforme do restante da organização. É salutar lembrar que as organizações atuam em diferentes setores e estes são fiscalizados de diferentes formas. Por exemplo, prestadores de serviço têm em quantidade e complexidade menos regulamentos a se cumprir que uma indústria química. Assim, também o setor de atuação irá inspirar o quanto específico deve ser o programa de *compliance* criado.

Um ponto deve ser deixado claro. Coimbra e Manz (2010, p. 6), descrevem que “a cada dia, aumenta o número de consumidores críticos, que procuram não só bens de consumo, mas também valores e comportamento das organizações de acordo com esses valores”. Com esse pensamento, pode-se entender que o *compliance* tem por função derivada criar vantagens competitivas



para as organizações que o implementam, dado que isso permite melhoria da reputação, aumento na eficiência e melhor alocação de recursos.

Outro efeito relevante diz respeito ao ambiente de trabalho, medido por meio do clima e da cultura organizacional. Com regras claras e bem estabelecidas, os colaboradores tendem a ficar mais seguros, uma vez que estão protegidos pela flexibilidade ética que porventura podem ter seus dirigentes. Com um código de ética formalizado, estes estão empoderados a se negar a praticar determinadas atitudes que firam o estabelecido.

Em sentido complementar, as empresas também se protegem de atitudes de seus colaboradores, de maneira que podem publicizar que um comportamento antiético é penalizado internamente, uma vez que isso não condiz com o que a empresa defende, dado que isso é informado no código de ética. Quanto a essa afirmação, cabe reforçar uma distinção. Quando se trata de *compliance*, pela exposição feita até esse momento, pode-se perceber que o termo tem relação com o grau de conformidade perante os regulamentos, isto é, está sendo abordado o respeito ao direito e as normas. Porém, quando se abordam aspectos éticos e alusivos aos valores da atuação da organização passa-se a compreender o que é a *governança corporativa*, o que significa dizer que essa é uma definição mais ampla, relacionando-se a melhor forma pela qual uma organização deve ser administrada, incluindo elementos de eficiência e impessoalidade na gestão.

TEMA 2 – GOVERNANÇA CORPORATIVA

2.1 Definição de governança corporativa

A necessidade de um sistema de governança se intensificou a partir da Segunda Guerra Mundial com a expansão do mercado de ações e, como resultado, se intensificou a dispersão da propriedade empresarial em contraposição ao seu controle. Com a abertura do capital negociado em bolsas de valores, as empresas contavam um número de acionistas que não necessariamente tinha a premissa de tomar decisões, exceto, obviamente, o acionista majoritário. Da década de 1980 em diante, tal fato ficou ainda mais em voga. Acidentes ambientais e crises éticas com consequências desastrosas para a sociedade ocorreram e a opinião pública passou a responsabilizar as empresas por essas atitudes, deflagrando crises de imagem. Além disso, foram ajuizados



pedidos de ressarcimento pelos danos causados aos investidores e para a sociedade como um todo. Como resultado, surgiu um ambiente de conflito de agência, ou seja, discordâncias graves entre acionistas e dirigentes pelas atitudes destes.

Como resultado dessas pelejas, mudanças da legislação ambiental e econômica foram realizadas e um movimento pela adoção de comportamento ético por parte das organizações ganhou corpo. Intensificam-se, então, os estudos teóricos para que fossem delineados sistemas de relacionamento entre os diretores, acionistas e demais *stakeholders* que passaram a ser compreendido como *governança corporativa*. Belarmino (2020, p. 68-69) acredita que “quanto mais transparente for a governança de uma empresa, mais credibilidade ela terá no mercado e, conseqüentemente, maior será seu valor entre acionistas e possíveis investidores”.

O conceito mais difundido em terras nacionais para Governança Corporativa (GC) foi estabelecido pelo Instituto Brasileiro de Governança Corporativa, o IBGC (2015, p. 20), a saber:

Governança corporativa é o 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. As boas práticas de governança corporativa convertem princípios básicos em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor econômico de longo prazo da organização, facilitando seu acesso a recursos e contribuindo para a qualidade da gestão da organização, sua longevidade e o bem comum.

É certo pensar, como apontam Simões e Souza (2020), que o conceito de governança corporativa pode diferir conforme o pesquisador consultado. Há quase sempre uma pequena variação, porém, em essência, se mantém o que aponta o IBGC (2015). Por exemplo, Collares (2020) a compreende como o sistema que gerencia a forma pela qual os acionistas asseguram o retorno de seus próprios investimentos, bem como respondem às pressões externas e internas de forma a que proporcione alinhamento entre as atitudes dos gestores com as necessidades dos acionistas, pacificando arestas e objetivando melhoria de desempenho organizacional. Collares (2020) ainda acredita que dessa forma materializa-se o processo de retroalimentação das ações de monitoramento, recompensa e retorno.

Kempner-Moreira e Freire (2020), em concordância, também creem que a governança estabelece premissas para o relacionamento entre os diferentes



agentes que habitam as organizações em seus diferentes papéis. Para eles, a governança corporativa estabelece as condições de mediação da relação entre as partes envolvidas, possibilitando, assim, as regras de negociação e definindo os papéis a serem desempenhados por cada agente. Percebe-se, à luz de Hedlund *et al.* (2021, p. 4148), que:

um dos principais objetivos da GC é minimizar os conflitos de agência, a divergência de interesses entre proprietário/mandante e o agente designado para representá-lo, para tanto as práticas de GC possuem um conjunto de mecanismos de estímulos, para que os comportamentos dos administradores estejam engajados com o melhor interesse da empresa.

Quanto aos benefícios da adoção da governança corporativa nas organizações, há consenso entre os listados a seguir.

- realizar ações concretas a partir dos valores organizacionais;
- alinhar os interesses dos *stakeholders* de modo que as ações sejam direcionadas aos melhores objetivos estratégicos;
- proporcionar a tomada das decisões estratégicas de modo colegiado e transparente;
- preservar os valores organizacionais garantindo credibilidade e visão de longo prazo;
- promover a integridade e, com isso, facilitar o acesso a financiamento externo para investimentos;
- valorizar a marca mediante melhoria da imagem organizacional; e
- promover a sucessão empresarial por meio da preparação de herdeiros e administradores, em caso de empresas familiares.

Hedlund *et al.* (2021, p. 4148) nos lembra que a governança corporativa nos apresenta com práticas de gestão que devam ser “implantadas e elaboradas com a finalidade de fidelizar a organização e os agentes internos e externos assim buscando benefícios com este novo instrumento”. Com a produção dessas práticas, passou-se a socializar os conhecimentos, por meio de *benchmarking*. Popularizou-se, assim, o reconhecimento de práticas recomendadas de governança o que será tratado a seguir.

2.2 Princípios básicos de governança corporativa

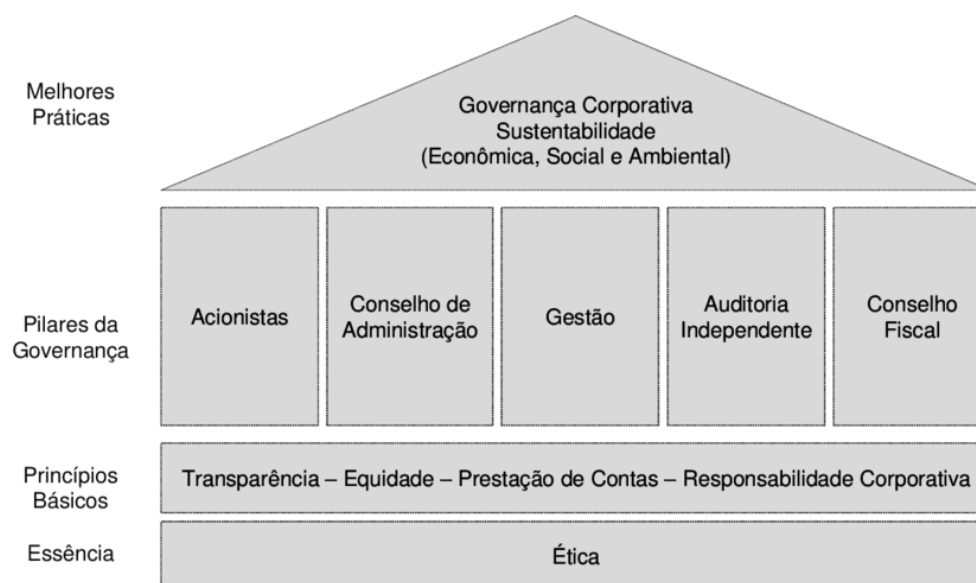


Passaglia e Rocha-Pinto (2014) relatam que ao longo do tempo criou-se um ambiente favorável para a discussão sobre a necessidade de aprimorar a governança corporativa. Os interesses diversos dos agentes de uma organização – no caso, privada – são inúmeros. Uma organização de grande porte possui a assembleia geral, o conselho de administração e a diretoria executiva. Há órgãos internos e externos que executam atividades de auditoria e fiscalização, a exemplo de conselho fiscal, comitê de auditoria, auditoria externa (também chamada de auditoria independente) e auditoria interna, como apresenta o IBGC (2015). Para dar conta de disseminar comportamentos e ações que sejam aceitos pelos todos os agentes é que se popularizaram os princípios básicos de direcionamento da governança corporativa.

Os princípios básicos estabelecem os fundamentados na conduta ética, sendo aceitos pela maioria da comunidade empresarial e científica dedicadas ao assunto, e devem estar presentes no exercício das funções e responsabilidades dos órgãos que exercem a governança das companhias, como apontam Passaglia e Rocha-Pinto (2014).

De acordo com o IBGC (2015, p. 20), os princípios básicos de governança corporativa “permeiam, em maior ou menor grau, todas as práticas do código (de conduta), e sua adequada adoção resulta em um clima de confiança tanto internamente quanto nas relações com terceiros.” A forma como se integram à essência, os princípios básicos, os pilares e as práticas da governança corporativa são apresentados na figura 1.

Figura 1 – Essência, princípios básicos, pilares e práticas da governança corporativa



Fonte: Silva (2010).



Para evitar dúvidas quanto à compreensão semântica, discute-se o entendimento acerca de cada princípio. Sobre a transparência, o IBGC (2015, p. 20) relata que “consiste no desejo de disponibilizar para as partes interessadas as informações que sejam de seu interesse e não apenas aquelas impostas por disposições de leis ou regulamentos”. Há de se destacar que estas não envolvem apenas aspectos do desempenho econômico-financeiro, devendo incluir também elementos que garantam uma visão de êxito de longo prazo.

O IBGC (2015, p. 20) aponta que a equidade diz respeito ao “tratamento justo e isonômico de todos os sócios e demais partes interessadas (*stakeholders*), levando em consideração seus direitos, deveres, necessidades, interesses e expectativas”. Quanto ao terceiro elemento, a mesma fonte consultada aponta que o *accountability*, ou a prática constante de prestação de contas, representa os procedimentos de demonstração contábil-financeira de maneira clara, concisa, compreensível e tempestiva, “assumindo integralmente as consequências de seus atos e omissões e atuando com diligência e responsabilidade no âmbito dos seus papéis”, segundo o IBGC (2015, p. 21). Como princípio aponta-se a responsabilidade corporativa. Nesse aspecto, o IBGC (2015, p. 20) aponta que:

Os agentes de governança devem zelar pela viabilidade econômico-financeira das organizações, reduzir as externalidades negativas de seus negócios e suas operações e aumentar as positivas, levando em consideração, no seu modelo de negócios, os diversos capitais (financeiro, manufaturado, intelectual, humano, social, ambiental, reputacional etc.) no curto, médio e longo prazos.

Ainda lembrando da figura 1, percebe-se que, a partir da ética como essência da governança corporativa e dos princípios, surgem aqueles agentes que devem garantir a efetividade da aplicação daquilo que se denomina das melhores práticas de governança, tema abordado no próximo tópico.

TEMA 3 – MELHORES PRÁTICAS DE GOVERNANÇA CORPORATIVA

3.1 Mecanismos para a governança

Silva, (2010, p. 44) aponta que “não há uma completa convergência sobre a correta aplicação das práticas de governança nos mercados, entretanto, pode-se afirmar que todos se baseiam nos princípios de transparência, independência e prestação de contas (*accountability*) como meio para atrair investimentos aos



negócios”. Percebe-se, então, que, para o autor, os princípios básicos possuem força no sentido de orientar as ações em prol da governança corporativa.

Obviamente que os princípios não possuem perspectiva prescritiva, mas, sim, orientativa. É preciso, porém, fazer com que a busca da conformidade e o rigor ao respeito aos padrões éticos sejam colocados em ação. É tarefa de todos os agentes de governança (indivíduos e órgãos envolvidos no sistema de governança, tais como sócios, administradores, conselheiros fiscais, auditores, conselho de administração, conselho fiscal e outros) empenhar-se para que a empresa consolide um sistema de gestão que envolva valores como honestidade, integridade, responsabilidade, independência, visão de longo prazo e preocupação genuína com os impactos causados por suas atividades, como defende o IBGC (2015).

É pela ação desses agentes, e, concomitantemente, pela reflexão destes sobre a identidade da organização, que um sistema de governança pode ser desenhado em termos práticos, fazendo com que o código de conduta interno conduza a empresa a obter e manter a conformidade ou o *compliance*. Não há apenas um só sistema para todos os tipos de organização, mas pode-se dizer que existem algumas práticas – derivadas de mecanismos internos e externos que podem ser consideradas como adequadas para as empresas em geral.

Fiorini, Junior e Alonso (2016) defendem que um sistema de governança é considerado eficiente quando combina diferentes mecanismos com o objetivo de assegurar as melhores decisões de interesse dos *stakeholders*. Esses autores apresentam os principais mecanismos internos citados na literatura para uma boa governança corporativa.

- **Conselho de administração:** considerado o principal mecanismo de governança. Por meio da constituição de um conselho, interesses dos acionistas são representados e pode-se monitorar e supervisionar a diretoria. Exige-se que o conselho seja ativo, atuando com independência e integridade, como defendem Fiorini, Junior e Alonso (2016).
- **Sistema de remuneração:** deixar transparente valores e forma de remuneração dos executivos é crucial para que interesses de acionistas e do board executivo estejam alinhados. O resultado financeiro pode ser obtido de várias formas, mas nunca de maneira que comprometa a existência da empresa em longo prazo. Fiorini, Junior e Alonso (2016,



p. 4) defendem que “a vinculação da remuneração com o desempenho é um mecanismo adicional comum para o alinhamento dos interesses”.

- **Concentração acionária:** há controvérsia sobre os benefícios acerca do número de acionistas e os respectivos percentuais destes na participação do capital social. De modo geral, Fiorini, Junior e Alonso (2016) apontam que a concentração em poucos sócios é mais vantajosa, uma vez que há menos interesses para se gerenciar. Por outro lado, em estruturas com dispersa concentração acionária, a menor possibilidade de pressão pode levar a implantação de um sistema de gestão mais profissional e impessoal. O relevante aqui é cotejar a concentração acionária com o modo correto de lidar com a disparidade e diversidade de interesses dos *stakeholders*.

Do ponto de vista dos mecanismos externos, defendem Fiorini, Junior e Alonso (2016), que estes existem em maior número e complexidade e sua aplicação variará de acordo com o porte e setor de atuação da organização. É pacífico, porém, que alguns deles são essenciais, tais como:

- **Proteção legal aos investidores:** há muitos regulamentos que impedem que decisões do corpo diretivo gere danos aos investidores. Atender a esses regulamentos diminui a existências de conflitos de interesses que porventura surjam em virtude de medidas implantadas pelo corpo diretivo.
- **Fiscalização dos agentes de mercado:** Fiorini, Junior e Alonso (2016, p. 4) apontam que “este item traz maior transparência para empresa e aumenta a pressão para que os executivos tomem decisões de forma a maximizar o valor da empresa em detrimento aos seus próprios interesses”.
- **Estrutura de capitais:** a estrutura de capital ou de financiamento da organização também é um dos mecanismos de governança. A transparência quanto ao endividamento deixa claro o poder que de fato uma organização possui para manter tanto o fluxo de caixa como o pagamento de dividendos aos acionistas e das dívidas aos credores. Sobre isso, ensinam Fiorini, Junior e Alonso (2016, p. 4) que “os executivos precisam equilibrar suas decisões de investimento e endividamento para não inviabilizar as operações da empresa ou aumentar o risco de falência”.
- **Possibilidade de aquisição hostil e grau de competição no mercado:** por pressões de fusões e aquisições há receio por parte dos executivos



de perderem seus empregos. Considera-se que esse fato potencializa que gestores busquem fazer bons trabalhos de modo que a organização não corra riscos e encontre na associação ou na venda a saída para uma crise interna.

O IBGC (2015) defende que as boas práticas sejam implantadas pelas organizações para que se estabeleçam estratégias de comunicação e programas de treinamento com a finalidade de disseminar, entre as partes interessadas, políticas, procedimentos, normas e práticas baseadas no código de conduta da organização. Há o pensamento também de que as ações devem estar atreladas a processos efetivos e estes, por sua vez, mensurados por indicadores formais que permitam o contínuo acompanhamento. O acompanhamento permitirá a reflexão sobre o estado das coisas e o *feedback* que, de fato, gera o monitoramento dos padrões de conduta adotados e o efetivo engajamento da alta administração nos mecanismos de conformidade da organização, como defende o IBGC (2015). Analisando indicadores, cotejando ações realizadas com práticas e processos, há possibilidade de responsabilizar aqueles que cometem desvios e, pelo aprendizado gerado, as práticas implantadas podem ser novamente desenhadas.

TEMA 4 – PROTEÇÃO DE DADOS PESSOAIS (LGPD)

4.1 A necessidade da proteção dos dados pessoais

A crescente importância da interação entre as organizações e todas as partes interessadas na sociedade por meio de atividades de responsabilidade social ganhou, no Brasil, recentemente, mais um ponto de atenção. Pozzetti (2019), relata que o avanço das tecnologias de coleta, processamento e interpretação de dados pessoais permite uma série de ações de *marketing* mais eficientes e customizadas em setores públicos e privados, uma vez que há exposição de padrões comportamentais nas diversas mídias sociais em diferentes dispositivos. Pozzetti (2019) ainda descreve que dados pessoais, hábitos, preferências de consumo e posições políticas no ambiente digital são exemplos de análises feitas por empresas e governos para entender perfis do comportamento social de indivíduos. Informa ainda, este autor, que a posse de dados se converteu em patrimônio das empresas e o uso destes necessitam, de alguma forma, serem regulados por algum tipo de regramento que possa gerar



transparência e aplique os preceitos constitucionais do direito à vida privada, como discorre Pozzetti (2019).

Para Doneda (2011), o tratamento de dados pessoais, em particular por processos automatizados, é uma atividade de risco para as pessoas. Para ele, esse risco “se concretiza na possibilidade de exposição e utilização indevida ou abusiva de dados pessoais, na eventualidade desses dados não serem corretos e representarem erroneamente seu titular” (Doneda, 2011, p. 92). Vê-se, então, que o volume e o tratamento de dados pessoais armazenadas em bancos eletrônicos e sistematizados é poderoso. No sentido aqui exposto, um dado, como aponta Idowu *et al.* (2015), é basicamente um pedaço de uma escolha, uma decisão de compra, uma característica física ou comportamental, por exemplo. Porém, quando esses dados sobre uma mesma pessoa são agrupados ao longo do tempo revelam informações da vida deste indivíduo, isso é potencialmente valioso para os negócios. Tão poderoso que permite a possibilidade de manipulação para que essas pessoas possam acreditar que a expressão de uma minoria – a qual faz parte de sua bolha de interação – representa o pensamento da maioria. Outro exemplo, é a de que todos os seus conhecidos estão adquirindo determinados produtos ou serviços que o levam a atribuir um grau de notoriedade e necessidade para a aquisição.

As medidas paliativas para evitar a manipulação de pessoas por meio do controle de seus dados deve se dar, pela experiência de se Idowu *et al.* (2015), por meio da transparência e proteção do acesso aos dados. Estas devem ser duas exigências desejáveis pela sociedade na tentativa de assegurar que a vida cotidiana das pessoas possa acontecer de maneira sustentável e socialmente responsável.

Percebe-se, nesse ponto, a convergência da ética, da responsabilidade social e da proteção dos dados. A existência de uma legislação que permita proteger as pessoas do uso indevido de suas informações pessoais por parte das organizações (públicas ou privadas) é a garantia inicial para um sentimento de que as escolhas destas são feitas de acordo com suas vontades, e não pela pressão e orientação de um algoritmo. Doneda (2011), com base em legislações europeias sobre o tema, apresenta alguns princípios que devem nortear a proteção dos dados pessoais como direito fundamental de todos, de acordo com o Quadro 3.

Quadro 3 – Princípios de orientação para o marco regulatório de proteção de dados pessoais



Princípios	Descrição
Princípio da publicidade (ou da transparência),	A existência de um banco de dados com dados pessoais deve ser de conhecimento público, seja por meio da exigência de autorização prévia para funcionar, da notificação a uma autoridade sobre sua existência ou do envio de relatórios periódicos.
Princípio da exatidão	Os dados armazenados devem ser fiéis à realidade, o que compreende a necessidade de que sua coleta e seu tratamento sejam feitos com cuidado e correção, e de que sejam realizadas atualizações periódicas conforme a necessidade.
Princípio da finalidade	Qualquer utilização dos dados pessoais deve obedecer à finalidade comunicada ao interessado antes da coleta de seus dados. Esse princípio possui grande relevância prática; com base nele, fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que se pode, a partir dele, estruturar um critério para valorar a razoabilidade da utilização de determinados dados para certa finalidade (fora da qual haveria abusividade).
Princípio do livre acesso	O indivíduo deve ter acesso ao banco de dados no qual suas informações estão armazenadas, podendo obter cópias desses registros, com a consequente possibilidade de controle destes; após esse acesso e de acordo com o princípio da exatidão, as informações incorretas poderão ser corrigidas e aquelas obsoletas ou impertinentes poderão ser suprimidas ou pode-se proceder a eventuais acréscimos.
Princípio da segurança física e lógica	Os dados devem ser protegidos contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado.

Fonte: Elaborado com base em Doneda (2011).

Foram esses princípios que, mesmo separados, fracionados, condensados ou adaptados, formaram a espinha dorsal de diversos marcos legais sobre o tema pelo mundo, “formando o núcleo das questões com as quais o ordenamento deve se deparar ao procurar fornecer sua própria solução ao problema da proteção dos dados pessoais”, como aponta Doneda (2011, p. 101). No caso brasileiro, à luz desses, foi criada a Lei Geral de Proteção de Dados (LGPD), assunto que é objeto do tema a seguir.

4.2 A Lei Geral de Proteção de Dados Pessoais (LGPD)

Por meio da Lei n. 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), foram regulamentados os aspectos referentes ao “tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural” (Brasil, 2018).

Em síntese, a intencionalidade desta lei é estabelecer a segurança jurídica, por meio da padronização de normas e práticas dos dados pessoais de todo cidadão que esteja no Brasil. A abrangência da lei versa ao processamento de conteúdo de pessoas, brasileiras ou não, que estão no território brasileiro, dados estes obtidos em qualquer tipo de suporte (papel, eletrônico, virtuais, som,



imagem etc.). A lei estabelece as seguintes hipóteses para o tratamento de dados (Brasil, 2018).

- com consentimento do titular;
- para cumprimento de obrigação legal ou regulatória pelo responsável pelo tratamento;
- para tratamento e uso compartilhado de dados necessários à execução de políticas públicas;
- para realização de estudos por órgãos de pesquisa;
- para proteção da vida ou integridade física do titular ou de terceiros;
- para tutela da saúde, com procedimento realizado por profissionais da área ou entidades sanitárias;
- para execução de contrato ou procedimentos preliminares relacionados a um contrato;
- para pleitos em processos judiciais, administrativos ou arbitrais; e
- para proteção do crédito, nos termos do Código de Defesa do Consumidor.

Cabe esclarecer a que tipos de dados a lei está tratando. Pelo quadro 4, temos uma distinção entre eles (Brasil, 2018).

Quadro 4 – Princípios de orientação para o marco regulatório de proteção de dados pessoais

Dados brutos	São dados registrados em uma base de dados e que não passaram por tratamento, ou seja, por procedimentos de extração de informações, consolidação e levantamento estatístico e outros.
Dados tratados	São dados submetidos a exemplos de procedimentos técnicos ou metodológicos, tais como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.
Dados pessoais	São dados relacionados à pessoa física identificada ou identificável. A vinculação direta de um dado a uma pessoa a torna pessoa física identificada, como o nome, por exemplo. Já a pessoa física identificável é aquela cujas características podem ser descobertas pelo conjunto de dados. É errôneo pensar que os dados pessoais são aqueles que identificam claramente alguém, pois, também são quaisquer informações que façam referência indireta à pessoa, como o gênero, orientação política ou ainda, padrões de consumo.
Dados sensíveis	São aqueles que, em caso de acesso e mal uso, podem gerar discriminação. Enquadram-se nessa categoria informações sobre origem racial ou étnica; convicções religiosas; opiniões políticas; filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político e dados referentes à saúde ou vida sexual, e dados genéticos ou biométricos.

Fonte: Elaborado com base em Brasil (2018).



Adicionalmente, a lei também aborda aspectos quanto ao compartilhamento de informações com organismos internacionais, porém, com isso, pede-se que sejam obedecidos protocolos seguros e respeito as exigências legais. Percebe-se, à luz do que foi apresentado, que o consentimento é o elemento essencial da legislação. Por meio do consentimento obtido dos cidadãos, uma organização pode tratar os dados e, com eles, tomar decisões e acessar esta pessoa com interesses diversos. De acordo com a legislação, poderão ser tratados os dados sem consentimento do indivíduo, desde que estes sejam destinados a cumprir obrigações legais; executar contratos; defender direitos em processo; preservar a vida e a integridade física de uma pessoa, entre outras possibilidades, desde que não se prejudiquem os direitos fundamentais desta pessoa (Brasil, 2018). É definido pela lei que as atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios, conforme (Brasil, 2018, p. 1):

- I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
- II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
- III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
- IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
- V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
- VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
- VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
- VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
- IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

A Lei n. 13.709/2018 ainda aponta que o tratamento dos dados deve ser feito levando em consideração sua finalidade e necessidade, sendo essas comunicadas ao cidadão. Da mesma forma, um indivíduo pode solicitar que suas informações armazenadas possam ser deletadas ou ainda, ele tem o poder de revogar consentimentos ou ainda, pedir a transferência de seus dados para



outros fornecedores se isso for de seu interesse. Em caso de registro automático dos dados, mediado por máquinas e com interesse de estabelecer um perfil da pessoa – seja este pessoal, comportamental, profissional, de consumo, de crédito) –, o indivíduo deve ser informado que pode intervir, pedindo revisão desse procedimento feito por máquinas.

A lei esclareceu os papéis de alguns agentes e criou também agentes de tratamento de dados apontando suas respectivas atribuições nas organizações. Assim, devem existir (Brasil, 2018):

- o controlador, ou seja, aquele que toma as decisões sobre o tratamento de dados;
- o operador, com atribuição de realizar o tratamento solicitado pelo controlador; e
- o encarregado, que em nome da instituição interage com autoridade nacional e os cidadãos – a esta função denomina-se *Data Protection Officer*, o DPO.

Na descrição dos agentes de tratamento de dados foi citada a existência de uma autoridade nacional. Trata-se da Autoridade Nacional de Proteção de Dados Pessoais, a ANPD. Sua atribuição é regular e orientar, preventivamente, sobre como aplicar a lei. Adicionalmente, também irá fiscalizar o cumprimento da LGPD e, em comprovado delito, penalizar os envolvidos. As multas serão pesadas, e os valores poderão chegar a 2% do faturamento anual da organização no Brasil – e no limite de R\$ 50 milhões por infração (Brasil, 2018). Caberá à ANPD a determinação dos níveis de penalidade, de acordo com a gravidade da falha e, assim, imputar a multa a aqueles que descumprirem os termos desta lei.

Sobre este aspecto, o que norteia a Lei n. 13.709/2018 é a gestão de riscos. As medidas preventivas de segurança, a adoção de práticas exitosas e a busca por certificações que empoderam os processos de gestão devem ser a forma pela qual as empresas podem se proteger dos rigores da lei. Trata-se, pois, de incluir os cuidados com os dados na agenda de preocupação da governança corporativa. Como pontos de observação para as empresas quanto à LGPD, citam-se as seguintes preocupações (EY Brasil, 2020, p. 1):

- Os websites dispõem de políticas de privacidade em linguagem clara, acessível e transparente aos usuários (titulares dos dados pessoais)?
- Foram registradas as operações de tratamento de dados pessoais que a companhia realiza?



- Todas as atividades foram devidamente enquadradas nas hipóteses de legalização de tratamento da LGPD?
- A empresa já dispõe de um canal de comunicação específico para que os titulares exerçam seus direitos relativos aos seus dados pessoais?
- Foram realizadas campanhas de conscientização e/ou treinamentos para disseminar entre os colaboradores da companhia os conceitos e as diretrizes que devem ser observados nas atividades de tratamento de dados?
- Houve a indicação de um Encarregado de Dados (DPO – Data Protection Officer)?
- Foram mapeadas as responsabilidades do DPO?
- Foi criado um Comitê de Privacidade para apoiar o Conselho de Administração? Ou onde melhor se encaixa este papel nos Comitês atuais?
- Houve investimento na transformação da segurança da informação para amparar os novos requerimentos de privacidade da LGPD?

A LGPD trouxe para o Brasil a necessidade da adequação das empresas a uma das principais garantias que uma pessoa deve ter, em momentos que a vida é muito influenciada pelos meios digitais, qual seja, a privacidade sobre suas informações disponibilizadas nos diferentes meios. Por meio dessa legislação, espera-se que o país seja despertado acerca da importância dos dados pessoais e dos respectivos reflexos destes em reflexos em direitos como o livre desenvolvimento da personalidade da pessoa natural e a liberdade.

TEMA 5 – RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

5.1 A fiscalização da adequação à lei

A LGPD criou um documento de comunicação entre a ANPD e as organizações que realizam o tratamento de dados (Brasil, 2018). Trata-se do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), também conhecido internacionalmente como *Data Protection Impact Assessment* (DPIA), que se refere à “documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco” (Brasil, 2018, p. 1).

A lei ainda aponta que a ANPD tem a prerrogativa de solicitar este relatório motivada por denúncia ou fiscalização, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial. Dos agentes do poder público, também poderá ser pedida a apresentação do documento, cabendo à ANPD “sugerir a adoção de padrões e



de boas práticas para os tratamentos de dados pessoais pelo Poder Público” (Brasil, 2018, p. 1).

Sobre o conteúdo do RIPD, a Lei n. 13.709/2018 descreve que este “deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados” (Brasil, 2018, p. 1). Vainzof (2021, p. 1) mostra situações em que a elaboração do RIPD é recomendada de maneira voluntária, ou seja, sem que seja pressionada pela fiscalização da ANPD:

- 1) Envolver dados sensíveis;
- 2) Envolver dados pessoais relacionados a condenações criminais;
- 3) Envolver dados financeiros, incluindo status social;
- 4) Envolver dados de vulneráveis;
- 5) Envolver geolocalização;
- 6) For capaz de afetar sensivelmente a segurança pessoal do indivíduo ou sua integridade física/psíquica;
- 7) De acordo com o volume de dados: a) número de titulares envolvidos, seja por meio de um número específico, ou por meio de percentual da população pertinente; b) do volume de dados e/ou a diversidade de dados diferentes tratados; c) da duração da atividade de tratamento de dados ou a sua pertinência; d) da dimensão geográfica da atividade de tratamento;
- 8) Avaliação ou classificação dos titulares, incluindo definição de perfis e análise preditiva;
- 9) Decisões automatizadas que produzam efeitos jurídicos ao titular ou o afetem significativamente, como o tratamento que possa implicar a exclusão ou a discriminação de indivíduos;
- 10) Tratamento dos dados empeça os titulares dos dados de exercer um direito ou de utilizar um serviço ou um contrato;
- 11) Controle sistemático, utilizado para observar, monitorar ou controlar os titulares dos dados;
- 12) Estabelecer correspondências ou combinar conjuntos de dados com origem em duas ou mais operações de tratamento de dados realizadas com diferentes finalidades e/ou por diferentes controladores; e
- 13) Utilização de soluções inovadoras ou aplicação de novas soluções tecnológicas ou organizacionais.

Vainzof (2021, p. 1) também elenca motivos pelos quais a realização do relatório deveria ser obrigatória. Suas recomendações partem da análise da LGPD, em virtude do risco da publicização dos dados tratados de certa pessoa. Considera o autor, por exemplo, que organizações que tratem dados biométricos ou genéticos de titulares vulneráveis ou utilizados para decisões automatizadas, que tenham alto volume de dados sensíveis, ou ainda alto volume de dados em espaços públicos teriam que estabelecer rotina de prestação de contas da forma como mitigam possíveis falhas ao atendimento do que é preconizada pela lei.

Sabe-se então que a ANPD poderá solicitar a elaboração do RIPD dos controladores, um dos agentes de tratamento de dados, na situação que este tratamento apresentar alto risco, de acordo com parâmetros previamente estabelecidos pela lei. Quanto ao encarregado, também denominado de DPO, suas atribuições no RIPD são as seguintes:

- avaliar a pertinência sobre o momento de realização do RIPD;
- opinar sobre a realização interna ou externa, por meio de consultoria, do documento, bem como sobre a metodologia a ser empregada;
- auxiliar na elaboração por meio do esclarecimento dos encaminhamentos (administrativos ou técnicos) a serem implantados com a intencionalidade de mitigar riscos quanto aos direitos dos titulares de dados; e
- identificar se a avaliação de impacto foi corretamente descrita no RIPD e se as soluções encontradas estão em *compliance* com o marco regulatório do tema.

Fica, porém, a dúvida quanto ao processo de elaboração do RIPD e seu conteúdo, o que será tema do próximo tópico.

5.2 Etapas da elaboração do relatório

De acordo com a legislação referente ao tratamento dos dados pessoais, foi criado o documento de divulgação da forma pela qual as organizações zelam pelo cumprimento a lei, porém, não de uma maneira prescritiva, que pudesse pacificar entendimentos sobre forma e conteúdo. Tal fato tem a sua razão de ser, uma vez que as organizações possuem diferentes formas de uso dos dados pessoais e um modelo prévio poderia forçar a existências de realidades distintas daquilo que na prática existe.

Pode-se, porém, à luz do que detalha Dodt (2020), estabelecer etapas básicas de elaboração do documento, como apontado na figura 2.





Figura 2 – Etapas de elaboração do RIPD

Fonte: Dodt (2020).

A etapa inicial consiste em identificar a necessidade de um RIPD, ou seja, se este é motivado por uma exigência da ANPD ou não. Em caso de inexistência de pedido formal da ANPD, recomenda-se que a organização o providencie o mais cedo possível, pois “com essa abordagem, certamente será mais fácil para sua organização incorporar o tratamento de quaisquer dos riscos identificados durante o tratamento de dados pessoais”, conforme Dodt (2020, p. 1).

Como etapa dois, surge a necessidade de descrever o tratamento de dados pessoais. Neste momento, os elaboradores devem apontar com detalhes a maneira com que os dados são tratados pela organização. Dodt (2020, p. 1) recomenda que devam ser fornecidos “detalhes sobre como as informações dentro da operação de tratamento são coletadas, armazenadas, usadas e descartadas, incluindo até mesmo o desenho do fluxo dos dados pessoais nos processos de negócio”.

Parte-se para a próxima etapa, momento de realizar o processo de consulta a todos os *stakeholders* envolvidos na forma pela qual a organização realiza o tratamento de dados. A intencionalidade desta ação consiste em assegurar que a empresa possui prontidão de ação quanto ao assunto e, também, ter canais de comunicação com operadores de dados da organização (terceiros fornecedores de soluções de TI, por exemplo) além de, adicionalmente, com especialistas em segurança da informação que poderão fornecer relatos de autoridade e pertinência de procedimentos quando necessário.

Dodt (2020, p. 1) descreve que a etapa seguinte é identificar no documento a “base legal para o tratamento de dados pessoais, ou como sua organização garantirá a qualidade e a minimização dos dados”. O próximo passo é relatar a essência do documento, ou seja, demonstrar como a empresa busca reduzir os riscos envolvidos no tratamento a um nível aceitável, de acordo com o preconizado pela legislação e reforçado pelo entendimento dos especialistas. Dodt (2020, p. 1) acredita que isso “exigirá uma visão clara de todas as ameaças e vulnerabilidades durante o tratamento de dados pessoais e deve resultar em um catálogo de riscos, incluindo a probabilidade e a gravidade de qualquer impacto sobre os direitos e liberdades dos indivíduos, cujos dados serão coletados e/ou tratados”.



Uma vez que a organização compreende que suas vulnerabilidades devem ser tornadas públicas, mediante o RIPD, a organização informa como pretende implantar ou como implantou medidas para tratar o risco. Os verbos atrelados a esta etapa são mitigar, evitar, transferir ou aceitar os riscos. Deve-se ter em mente que a extinção do risco é quase impossível, porém, Dodt (2020) aponta que deve-se buscar reduzir sua probabilidade e impacto a níveis aceitáveis.

Chega-se, então, ao momento de formalização do documento, obtendo a assinatura dos responsáveis pelos diagnósticos realizados e também daqueles que possuem poder sobre as decisões mencionadas. O RIPD, vale lembrar, nada mais é do que a externalização da forma pela qual uma organização – pública ou privada – gerencia o tratamento dos dados pessoais. Ele é relevante, uma vez que pode vir demonstrar fragilidades quanto ao tema e que poderão ser avaliadas, não apenas pela ANPD, mas também pelos especialistas ou cidadãos comuns interessados no tema. Isso faz pensar que sua elaboração deve ser realizada por profissionais capacitados, com experiência e conhecimento suficiente, evitando um prejuízo pecuniário por meio das pesadas multas que envolvem a LGPD, incluindo ainda a de imagem, pela divulgação ou vazamento de informações pessoais sensíveis seja realizada.

FINALIZANDO

As corporações fazem parte da rotina das pessoas. Por meio das empresas, adquirimos produtos e serviços cotidianamente, construindo uma relação de simbiose entre pessoas físicas e jurídicas em que a existência de um e de outros estão indefinidamente conjuntas.

Por pressões legais ou em virtude da imagem, a responsabilidade social passa a ser incorporada como mais um dos vários processos das organizações. As empresas, mais do que práticas filantrópicas, busca desenvolver programas sociais como medidas para o fortalecimento da própria imagem e também como resultado derivado para o desenvolvimento interno de competências de seus colaboradores.

Dar conta da adequação ao marco legal que regula as organizações exige metodologias gerenciais para a demonstração das virtudes éticas e das ações de responsabilidade social de maneira adequada. Certamente isso representa a necessidade de procedimentos internos para este fim, o que foi abordado nesta



aula. Estar em *compliance*, como o jargão corporativo divulga, agrega benefícios gigantes para as empresas, pois evita riscos de perdas financeiras e de reputação, dado limita a incidência de fraudes. Por meio da governança corporativa, os *stakeholders* podem ter ciência de que as estratégias e seus processos vinculados estão sendo corretamente implantados, uma vez que estes são públicos, por meio desta adoção de prestação de contas na empresa aos seus acionistas.

Por meio da adoção das melhores práticas de governança, obtidas pelo *benchmarking*, os riscos organizacionais são avaliados e, desta maneira, mais segurança aos *stakeholders* é propiciada diante de um investimento. Em tempos de responsabilidade social, eficiência e transparência passam a reger as normas do bom comportamento.

Se a divulgação aos interessados é salutar em termos das decisões tomadas pela empresa, o mesmo não se aplica aos dados pessoais armazenados em bancos de informação sobre os clientes. Descuidar das informações pessoais de outrem de modo que se tornem públicos pode gerar pesadas multas para as corporações, como proclama a LGPD.

Estar ciente que cuidar dos dados das pessoas é uma obrigação é a intencionalidade desta recente legislação. As informações agrupadas podem expor pessoas em seus comportamentos ou, ainda, propiciar exclusões e perseguições, o que é abominável não apenas por responsabilidade social, mas fundamentalmente, pelo respeito às individualidades.



REFERÊNCIAS

- BARBIERI, J. C.; CAJAZEIRA, J. E. R. **Métodos para integrar a responsabilidade social na gestão**. Disponível em: <<https://www.ethos.org.br/cedoc/metodos-para-integrar-a-responsabilidade-social-na-gestao/>>. Acesso em: 7 set. 2021.
- BARBIERI, J. C.; CAJAZEIRA, J. E. R. **Responsabilidade Social, Empresarial e Empresa Sustentável: da Teoria à Prática**. 2. ed. São Paulo, Editora Saraiva, 2013.
- BELARMINO, A. P. O Compliance na Percepção de Micro e Pequenos Empresários. **Revista Metropolitana de Governança Corporativa**, v. 5, n. 2, p. 65-87, 2020.
- BENTO, A. M. Fatores relevantes para estruturação de um programa de compliance. **Revista da FAE**, v. 21, n. 1, 2018. p. 98-109.
- BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 7 set. 2021.
- COIMBRA, M. A.; MANZI, V. A. **Manual de Compliance**. São Paulo: Atlas, 2010.
- DODT, C. **LGPD: Como criar um RIPDP – Relatório de Impacto à Proteção de Dados Pessoais**. Disponível em: <<https://www.profissionaisiti.com.br/relatorio-impacto-protecao-dados-pessoais-lgpd/>>. Acesso em: 7 set. 2021.
- DONEDA, D. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law**. v. 12, n. 2, 2011, p. 91-108.
- EY BRASIL. **Privacidade e proteção de dados**. Disponível em: <https://www.ey.com/pt_br/ey-governanca-corporativa/privacidade-e-protecao-de-dados>. Acesso em: 7 set. 2021.
- FIORINI, F. A.; JUNIOR, N. A.; ALONSO, V. L. C. **Governança Corporativa: Conceitos e Aplicações**. XIII Simpósio de Excelência em Gestão e Tecnologia, SEGet, 2016.
- HEDLUND, P. R. *et al.* A Relação entre Governança Corporativa e Teoria da Agência no Gerenciamento de Conflitos. **Gestão e Sociedade**, v. 15, n. 41, p. 4144-4162, 2021.



IBGC. Instituto Brasileiro de Governança Corporativa. **Código das melhores práticas de governança corporativa**. 5. ed. São Paulo: IBGC, 2015.

IDOWU, S. O. *et al.* **Dictionary of Corporate Social Responsibility: CSR, Sustainability, Ethics and Governance**. Springer International Publishing: Switzerland, 2015.

PASSAGLIA, L. F.; ROCHA-PINTO, S. R. Governança de participação societária: Fatores críticos para a redução do conflito de agência entre holding e controladas. **Revista de Negócios da FURB**, v. 19, n. 1, 2014, p. 3-26.

POZZETTI, D. *et al.* Proteção de dados no Brasil e no mundo. **KPMG Business Magazine**. v. 1, n. 44, 2019, p. 18-21.

SILVA, E. C. da. **Governança corporativa nas empresas**. 2. ed. São Paulo: Atlas, 2010.

VAINZOF, R. **A LGPD e o Relatório de Impacto à Proteção de Dados Pessoais**. Disponível em: <<https://www.conjur.com.br/2021-jun-28/rony-vainzof-lgpd-relatorio-impacto-protecao-dados>>. Acesso em: 7 set. 2021.