O *COMPLIANCE* DIGITAL - INOVAÇÃO TECNOLOGICA COM ENFASE EM PROTEÇÃO DE DADOS

DIGITAL COMPLIANCE - TECHNOLOGICAL INNOVATION WITH AN EMPHASIS ON DATA PROTECTION

Paulo Cezar Dias[1]

Ana Cristina Neves Valotto Postal[2]

Rodrigo Abolis Bastos[3]

RESUMO

Os dados obtidos através de informações e cadastros em geral, têm se tornado uma nova fonte de conhecimento geradora de riqueza a ponto de ser comparado à fonte energética do petróleo. Porém a obtenção de dados não tem-se mostrado um problema, mas a maior questão é como podem ser aplicados para resolução e sua potencialização. Com a popularização das tecnologias temos uma redução severa nas relações interpessoais resultante do compartilhamento da vida própria e alheia nas redes sociais e internet. O presente estudo tem por objetivo demonstrar como a aplicação do compliance digital aliado à tecnologia pode de forma relevante potencializar um ambiente corporativo mais seguro na proteção dos dados tanto nos Setores Privado e Público e cristalino na relação entre clientes, fornecedores e administrados. Portanto, para o desenvolvimento e conclusão da pesquisa, utiliza-se do método bibliográfico, estudo doutrinário, estudos legislativos, com intuito de demonstrar, sem, contudo, esgotar o tema, como o compliance digital servirá como ferramenta de apoio nos Setores Privado e Público, prevenindo os riscos, evitando prejuízos de ordem financeira e quiçá desgaste a reputação da imagem.

Palavras-chave: Compliance. Proteção. Dados. Tecnologia

ABSTRACT

The data obtained through information and registrations in general, has become a new source of knowledge that generates wealth to the point of being compared to the energy source of oil. However, obtaining data has not been a problem, but the biggest question is how they can be applied for resolution and its enhancement. With the popularization of technologies,

[1] Professor Pós-Doutor em Direito pela Faculdade de Direito de Coimbra, Doutor em Direito pela Fadisp-São Paulo e Mestre em Direito pelo Centro Universitário Eurípides de Marília-Univem.

[2] Mestranda em Direito na área de concentração Direito e Estado na Era Digital pelo Centro Universitário Eurípides de Marília-UNIVEM/SP. Advogada. Graduada em Direito pelo Centro Universitário Eurípides de Marília-UNIVEM.

[3] Mestrando em Direito na área de concentração Direito e Estado na Era Digital pelo Centro Universitário Eurípides de Marília-UNIVEM/SP. Procurador Jurídico do Município de Marília-SP e Advogado. Graduado em Direito pelo Centro Universitário Eurípides de Marília-UNIVEM.

we have a severe reduction in interpersonal relationships resulting from sharing one's own and others' lives on social networks and the internet.

The present study aims to demonstrate how the application of digital compliance combined with technology can significantly enhance a safer corporate environment in the protection of data both in the Private and Public Sectors and crystal clear in the relationship between customers, suppliers and administrators. Therefore, for the development and conclusion of the reseach, the bibliographic method, doctrinal study, legislative studies are used, in order to demonstrate, without, however, exhausting the theme, how digital compliance will serve as a support tool in the Private and Public Sectors, preventing risks, avoiding financial losses and perhaps eroding the reputation of image.

Keywords: Compliance. Protection. Data. Technology.

1. INTRODUÇÃO

Os dados são o novo petróleo, porém com um diferencial, esse é uma fonte esgotável, enquanto os dados encontram-se à disposição, logo o maior desafio será como fazer um bom uso e de maneira coerente.

Denota-se que o *Big Data* trouxe um aumento exponencial da capacidade computacional de extrair e processar um grande volume de dados dos cidadãos, mas o *Big Data* também guarda seu lado sombrio, no que tange as questões de privacidade, segurança, de modo que, torna-se necessário a tutela a fim de evitar lesão ao direito dos cidadãos, e isso ocorreu em razão da popularização das tecnologias.

Procura-se no presente artigo traçar um panorama histórico acerca da normatização da proteção à privacidade pelo mundo, em especial a legislação pátria, tornando-se indispensável o desenvolvimento de garantias legais.

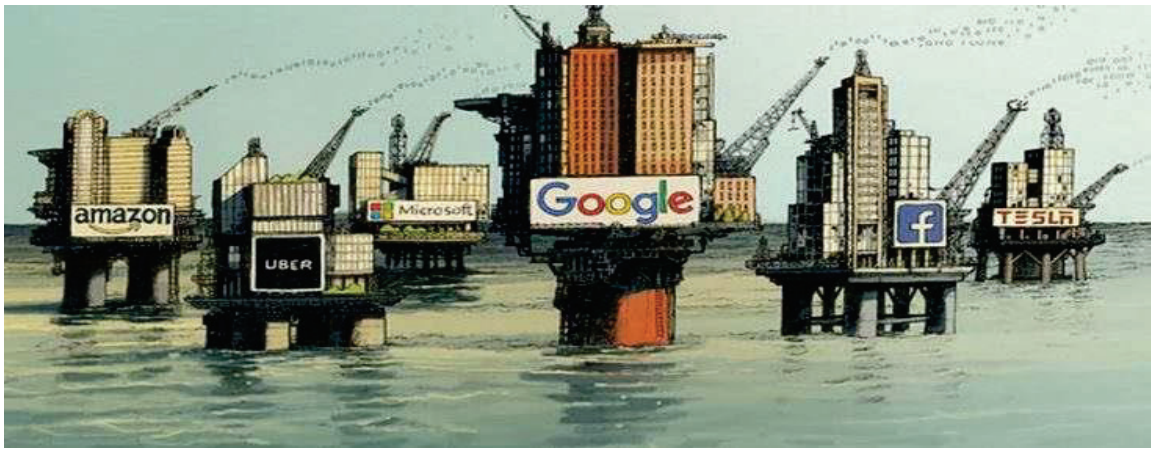
Observa-se assim a necessidade de ter um aliado das ferramentas tecnológicas, sendo o *Compliance* Digital esse escopo, capaz de direcionar o ambiente privado e público a mitigar os riscos, no manuseio deste arcabouço de dados produzidos.

2. OS DADOS COMO FONTE DE CONHECIMENTO E PODER

Morelli (2021, p. 133) cita a frase "Os dados são o novo petróleo", do matemático londrino Clive Humby que repercutiu no mundo e trouxe uma nova esperança não só de conhecimento, mas também de geração de riqueza e poder.

De acordo com Baldo (2018, p. 1): “a frase repercutiu bastante e foi uma das manifestações que começou a despertar na mente de executivos a percepção de que há muito a ganhar (ou perder) com a triagem cuidadosa ou descuidada do chamado “big data”.”

Figura 1: Dados são o novo petróleo! O que você tem feito com os seus dados?



Fonte: Revista de Segurança Eletrônica[4]

Com efeito, essa comparação ganhou força nos últimos tempos para evidenciar a transformação pela qual a sociedade e os negócios passaram a demonstrar que os dados são o novo petróleo da sociedade moderna. Esse mantra foi repetido por consultores, executivos e interessados na digitalização. Para Ajay Banga, CEO da Mastercard, a comparação faz sentido, exceto por um pequeno detalhe. "A diferença é que o petróleo vai acabar um dia. Os dados, não", afirmou durante o Master Minds, evento de inovação da Mastercard realizado em São Paulo no ano de 2019. (Revista Época, 2019).

A visão do CEO Ajay Banga faz sentido, visto que os dados apresentam fonte inesgotável, enquanto o petróleo um dia vai se erradicar. Assim enquanto o petróleo precisa localizar reservas subterrâneas para encontrá-lo, o enfoque do mundo dos dados é outro, como estão a nossa disposição localizá-los não é um problema, mas seu maior desafio é como fazer o bom uso de possibilidades infinitas.

Com isso, Morelli (2021, p. 135) expõe:

> destaca que os dados, hoje, alimentam sofisticados algoritmos que se prestam a inúmeras funções, e que potencializam resultados, podendo prever melhores momentos para a compra e venda de ações no mercado acionário, podem estimar altas e baixas de produtos no mercado futuro (e efetivamente realizar as vendas e compras que entender necessárias para assegurar o melhor preço), podem extrapolar dados de previsão de tempo e gerar previsões mais precisas de

[4] Disponível em: https://revistasegurancaeletronica.com.br/dados-sao-novo-petroleo/. Acesso em 15/09/2022

> tempestades, podem maximizar os dados de compras de consumidores e traçar padrões estimando os níveis de stress da população, padrões de consumo para o estabelecimento de propagandas direcionadas, ou até mesmo, como o célebre caso do supermercado que, usando de um algoritmo para identificar padrões de compra para oferta de promoções acabou antecipando que uma de suas consumidoras estava grávida.

Assim é certo que quem souber fazer o bom uso dos dados e aproveitar todo o seu potencial sai na frente, e claro, só tem a ganhar.

Mas segundo, Balbo (2018, p. 2): "o *big data* também possui seu lado sombrio, de modo que o perigo engloba questões de privacidade, segurança e chega à probabilidade, necessitando assim de tutela para evitar verdadeira lesão de direitos."

Dessa forma, sendo os dados relevante fonte de riqueza e poder como propiciar o seu uso sem que haja infração a direitos, inclusive fundamentais, como a privacidade?

3. DOS INSTRUMENTOS LEGAIS DE PROTEÇÃO DA PRIVACIDADE

Com a popularização das tecnologias é evidente que tivemos uma perda severa da privacidade nas relações interpessoais, resultante do compartilhamento exacerbado da vida própria e alheia nas redes sociais e internet.

Nesse passo, é certo que a proteção da privacidade ganhava relevância desde a Segunda Guerra Mundial, com o cometimento de abusos dos governos contra os cidadãos com relevante destaque para o governo Nazista.

Cabe destacar que depois que Adolf Hitler tornou-se chanceler da Alemanha, em janeiro de 1933, ele agiu rapidamente para transformar o país em uma ditadura com um único partido, e organizou uma força policial especialmente para a garantia das políticas nazistas com a persuasão do seu gabinete para declarar estado de emergência e a abolir direitos individuais, incluindo a liberdade de imprensa, de expressão e de reunião, e logicamente os indivíduos também perderam o direito à privacidade, o que significava que os nazistas podiam ler suas correspondências, escutar suas conversas telefônicas e revistar suas casas sem necessidade de mandado de busca ou apreensão.

Nesse passo, ao lado das atrocidades que marcaram a história o conceito do Direito à Privacidade ganha existência a partir da Convenção Europeia de Direitos Humanos (1953), onde precisamente em seu artigo 8° disciplinou que "Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicilio e da sua correspondência".

Percebe-se que neste momento o mundo passou se importar com a proteção da privacidade, face os inúmeros abusos cometidos na história da humanidade e muito mais evidenciados durante a guerra pelos governos.

De acordo com Cavalari (2020, p. 52) nos EUA, surgiu o *Fair Credit Reporting Act* de 1970, com foco na regulação dos relatórios de crédito dos consumidores, e o *Privacy Act* de 1974, aplicável à Administração Pública.

Com efeito, a lei do *Fair Credit Reporting Act* (FCRA) regulamenta a coleta de informações de crédito dos consumidores e o acesso a seus relatórios de crédito e visa tratar com justiça, precisão e privacidade as informações pessoais contidas nos arquivos das agências de relatórios de crédito do sistema financeiro americano.

Já o *Privacy Act* de 1974 tem por objetivo estabelecer a regulamentação de práticas de informações justas que rege a coleta, manutenção, uso e a disseminação de informações sobre indivíduos mantidas em banco de sistemas de registros por agências federais dos EUA.

Com efeito, seguindo a história podemos evidenciar que na Convenção 108 de 1981 do Conselho da Europa disciplinou a Proteção das Pessoas Singulares, no que diz respeito ao tratamento automatizado de dados pessoais e se destacou como o primeiro instrumento internacional juridicamente vinculativo para a proteção de dados.

A nossa Constituição Federal de 1988, teve destaque no rol dos instrumentos protetivos da privacidade, conforme comprova o seu artigo 5°, inciso X, que disciplina expressamente o princípio da inviolabilidade à privacidade, vida privada, honra e imagem das pessoas, assegurando o direito à indenização pelo dano material ou moral decorrente de sua violação.

Ainda em destaque temos a Lei Federal n° 8.078, de 11 de setembro de 1990, que disciplina o Código de Defesa do Consumidor, onde mais precisamente em seu artigo 43 dispõe que o consumidor terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados, bem como, sobre as suas respectivas fontes.

De acordo com Cavalari (2020, p. 52 *apud* BIONI, 2019, p. 126):

> O Código de Defesa do Consumidor disciplinou no rol do artigo 43, os bancos de dados e cadastros dos consumidores, observa-se a amplitude do dispositivo em questão, indo muito além, portanto, dos bancos de dados de informações negativas para fins de concessão de crédito.
> De acordo com o disposto no artigo 43, § 2º, do CDC, o consumidor deverá ser notificado da abertura de um banco de dados pessoais por ele não solicitado, ou seja, a legislação consumerista optou por conferir ao consumidor o direito de controlar os seus dados pessoais, bem como em estipular que o consumidor seja capaz de autodeterminar as suas informações pessoais.

Ainda seguindo a história, temos em destaque a Carta dos Direitos Fundamentais da União Europeia de 2000, onde em seu artigo 8°, item 1, estabeleceu que todas as pessoas têm direito à proteção de dados, demarcando esta proteção o caráter pessoal.

Além disso, com a Lei Federal 12.414, de 09 de junho de 2011, o Brasil disciplinou os cadastros positivo e negativo, para fins de concessão de crédito.

De acordo com Cavalari (2020, p. 52 *apud* COSTA, 2012, p. 72), referida lei estabeleceu:

> [..]a formação do banco de dados sob um conjunto de dados relativos às operações financeiras de adimplemento para fins de concessão de crédito, analisando não somente os dados relativos às dívidas não pagas, mas também informações que possam demonstrar dados positivos sobre a capacidade financeira e histórico de adimplemento do indivíduo.

Deve ser explicitado, conforme Cavalari (2020, p. 53 *apud* MENDES, 2014, p. 146) que a tal instrumento normativo ainda consolidou:

> [...]a evolução do conceito de autodeterminação informativa no nosso ordenamento jurídico disciplinando mecanismos de controle do indivíduo sobre os seus dados, atribuindo a ele o poder de decidir se tem interesse ou não em formar esse histórico e de decidir quando deseja cancelá-lo.

Já o Marco Civil da Internet (MCI), instituído pela Lei Federal n° 12.965, de 23 de abril de 2014, disciplinou em seu artigo 7° princípios e obrigações relacionadas ao tratamento de dados pessoas na Internet, com ênfase ao consentimento expresso do usuário e a exclusão de seus dados pessoais.

E a muito esperada e importante Lei Federal n° 13.709, de 14 de agosto de 2018, - Lei Geral de Proteção de Dados – LGPD, e que teve sua vigência somente no ano de 2020 de acordo com Cavalari (2020, p. 54 *apud* BLUM & MALDONADO, 2018, p. 25 e 26):

> [...]anuncia como submetidos ao regulamento qualquer pessoa natural ou pessoa jurídica, de direito público ou privado, que realize algum tipo de operação de tratamento de dados. Nessas operações de tratamento estão incluídas a coleta, produção, recepção, classificação e processamento de dados pessoais. São excluídos da aplicação do tratamento de dados pessoais que forem feitos por pessoa física, para fins particulares e não comerciais ou dados para fins exclusivamente jornalísticos, artísticos e acadêmicos.

Com efeito, é certo que a LGPD protege pessoas físicas, já as pessoas jurídicas que se sentirem lesadas podem recorrer ao Código de Defesa do Consumidor como instrumento normativo de proteção.

De acordo com Bezerra & Watz (2014):

> ainda que a internet tenha propiciado mais democratização na concessão de vozes por meio de uma proliferação de polos emissores, por ela também espreita uma miríade de ameaças a liberdades democráticas, principalmente contra a defesa da privacidade, que em teoria apregoada consensualmente por quase todos os atores envolvidos na rede, é posta em xeque por ações de espionagem e vigilância de governos e grandes empresas, de modo que a neutralidade da rede, por sua vez, é ponto de divergência entre o interesse público e de provedoras de internet, no Brasil e ao redor do mundo.

Aliás, tanto o Marco Civil da Internet como Lei Geral de Proteção de Dados, tentam resolver o maior problema criado pela internet: proteger dados sem inviabilizar a atividade econômica além do estritamente necessário.

Assim, podemos observar que a inovação tecnológica e os meios de comunicação são indispensáveis nos ambientes corporativos, todavia, a necessidade de adequação quanto à compreensão do que se trata a privacidade online e o tratamento de dados são indispensáveis nos ambientes corporativos, uma vez o compartilhamento de dados pessoais quando utilizados no intuito de prejudicar alguém, ou a própria organização podem trazer danos imensuráveis. (CAVALARI, 2020, p. 54)

4. O *COMPLIANCE* DIGITAL NA PROTEÇÃO DE DADOS

Com a inovação tecnológica houve uma expansão em diversos ramos da sociedade, inclusive do mundo dos negócios, nesse passo é certo que hodiernamente empresa que pretende integrar a tal transformação precisa se adequar para estimular a tomada de risco, incentivar a inovação e desenvolver um ambiente de trabalho corporativo.

Nesse passo, conforme Cavalari (2020, p. 47 *apud* JIMENE, 2019) destaca:

> [...]atualmente os dados corporativos das organizações encontram-se armazenados em diferentes ambientes: servidores da empresa ou em nuvem, notebooks, celulares, tablets, smartwatchs, pendrives e aplicações de Internet, corporativas ou muitas vezes particulares, de modo que, nos dias atuais, WhatsApp, Facebook e LinkedIn, por exemplo, são ferramentas utilizadas, ao mesmo tempo, para marcar o jantar com a família e fechar grandes negócios.

Assim, com o *Big Data* é evidente o aumento da capacidade computacional de extração e processamento de grande volume de dados, com repercussão no contexto da economia compartilhada e do capitalismo de vigilância, os quais se valem da mineração das informações produzidas pelos usuários de dispositivos computacionais para o possível fomento econômico dos dados. (SILVA, 2019)

De acordo com Cavalari (2020, p. 48 *apud* GALLOWAY, 2017, p. 259), destaca que: "o capitalismo de vigilância referido acima nada mais é senão a venda dos dados que fornecemos, em sua grande maioria gratuita, às grandes empresas de tecnologia, como *Google, Facebook, Apple e Amazon* – os quatro maiores cavaleiros dentro tantas outras."

Com efeito, segundo Valadares (2021, p. 2), explica que ante a intensidade da interação com novas tecnologias e do uso da Internet, nota-se a vigência de uma "economia da dádiva", com fornecimento de serviços gratuitos em troca da coleta massiva de dados, mas com a superexposição às novas tecnologias e aos sistemas de inteligência artificial (IA) possuem peso significativo na própria formação da personalidade, da subjetividade de cada indivíduo, justamente por lidarem com o processamento constante de informações de cunho muito íntimo e sensível das pessoas naturais.

Assim, diante dos apontamentos acima verifica-se a relevante importância da proteção dos dados no mundo, de modo que é indispensável o desenvolvimento de garantias legais para a proteção da privacidade a decorrente da colheita de informações dos administrados e pelos governos, por exemplo Edward Snowden no *Wikileaks* – bem como os grandes vazamentos e controle de temas, inclusive eleições – a exemplo disso o caso da empresa *Cambridge Analytica*, fazendo a sociedade se preocupar com o trânsito tão rápido de dados e, principalmente, com o destino e utilização dos mesmos. (CAVALARI, 2020, p. 48),

Com efeito, Aragão (2022, p. 47) destaca que o escândalo que estourou em 2017, envolvendo a empresa inglesa *Cambridge Analytica* e o *Facebook*, demonstrou em primeira mão a instrumentalização dos dados de usuários para fins políticos, conforme ressaltado por estudos sobre o crescimento das redes, o uso das informações é feito de forma irregular, sem que as pessoas saibam que seus dados estão sendo processados.

De acordo com Aragão (2022, p. 47 *apud* CALDAS, 2019), é certo que o uso das informações é feito de forma irregular, sem que as pessoas saibam que seus dados estão sendo processados. Envolvida tanto na campanha presidencial de Donald Trump, nos Estados Unidos, quanto na campanha do *Brexit,* no Reino Unido, a *Cambridge Analytica* analisava o *big data* e

direcionava ações nas redes sociais aos usuários que estariam mais propensos a mudar de opinião, para alterar as previsões eleitorais através da manipulação do voto.

Aliás, o caso Edward Snowden no *Wikileaks*, trouxe à tona que celulares, computadores e a Internet podem ser aplicados para monitorar as conversas, atividades e deslocações de cidadãos comuns e até pessoas importantes, tais como por exemplo políticos brasileiros, como o caso do monitoramento de Dilma Rousseff em diálogos com os seus principais assessores (CAVALARI, 2020, p. 48).

Além disso, em punição o *Facebook* foi multado em 5 bilhões de dólares – aproximadamente 18,7 bilhões de reais – por ter violado as regras de privacidade de seus usuários no caso *Cambridge Analytica*. A multa, recorde no setor de tecnologia, coincide com a punição que a própria empresa tinha previsto em abril, quando apresentou seus resultados (CAVALARI, 2020, p. 48).

E os abusos não pararam só em escândalos políticos, pois recentemente a Comissão de Proteção de Informações Pessoais da Coreia do Sul apontou que o *Google* e a *Meta* violaram as leis de privacidade do país, coletando informações de usuários para anúncios personalizados, onde a *Meta*, dona do *Facebook, Instagram, Messenger* e *WhatsApp*, recebeu uma multa de cerca de 44 milhões de dólares – aproximadamente R$ 227 milhões e o *Google* foi autuado em US$ 50 milhões, que representa cerca de 258 milhões de reais (Revista Olhar Digital, 2022).

Nesse passo, Cavalari (2020, p 49 *apud* SILVA 2019), destaca que:

> A atenção do legislador sobre a temática privacidade e proteção de dados dos usuários, se volta à proteção da privacidade daqueles, levando em consideração o expressivo aumento dos maiores players desse cenário, quais sejam, as empresas de tecnologia.

Aliás, de acordo com Blum (2018, p. 66), tanto pelo *General Data Protection Regulation GDPR* quanto pela a Lei Geral da Proteção de Dados – LGPD, ao regulamento da responsabilidade pelo tratamento, uso, coleta, armazenamento e transferência dos dados, são disciplinadas diversas condutas a serem respeitadas pelas organizações para que possam estar em conformidade com as normas.

Com efeito, Blum (2018, p. 13), vai além destacando que o *compliance* digital adquire maior atenção, pois o dever de guarda e proteção dos dados envolve, pela norma vigente no Brasil, não apenas os dados digitais, mas também o meio físico, de modo que a conformidade não pode se limitar ao banco de dados e arquivos digitais, devendo também atentar para arquivos físicos em papel ou em outro meio de armazenamento.

Nesse passo, de acordo com Frazão, Oliva e Abílio (2019, p. 695) observa-se que o *compliance* de dados não se limita apenas ao relacionamento com consumidores, mas acaba por repercutir em várias esferas da atividade empresarial, a demandar adaptação também de setores que, inicialmente, não estariam diretamente relacionados com a LGPD. O *compliance* de dados assume caráter transversal, a tornar necessário rever os padrões de conduta estabelecidos para cumprimento de outras normas. Remeta-se, mais uma vez, à relação de trabalho: as regras de conformidade adotadas nesse setor deverão ser atualizadas para contemplar também os preceitos da LGDP, evitando-se, por exemplo, a coleta de dados desnecessários ou cujo emprego possa ser considerado discriminatório.

Em complemento ao entendimento em referência Cavalari (2020, p. 49 *apud* ASSIS 2018, p. 91), a implementação de um Programa de *Compliance* impõe a observância de deveres de prevenção e análise de riscos, mediante adoção de uma cultura corporativa ética e transparente nas atividades organizacionais, mediante a identificação de funções e de responsabilidades, as quais também devem estar normatizadas e documentadas, de modo que as responsabilidades devem ser claras e bem definidas para que cada área responsável pela gestão de riscos e controles conheça seus limites e obrigações na estrutura organizacional, pois é comum pessoas agirem da mesma forma e obterem resultados diferentes.

Mas, diante de todo o contexto apresentado, quais são os elementos para a aplicação do *compliance* em proteção de dados? Por certo um dos requisitos é a criação e informação de um código de conduta, que defina a postura ética empresarial.

Segundo, Costa & Medeiros (2019, p. 86) o código de conduta será o principal documento do Programa de *Compliance*, pois nele estarão inseridos os valores que guia a corporação e serão impostos a todos os funcionários, fornecedores, parceiros e quaisquer outras organizações e pessoas que se relacionem com a empresa.

Portanto, o Programa de *Compliance* terá como um de seus objetivos, por meio do código de conduta, transferir a todos os que compõem a empresa a missão, a visão e os valores daquela, almejando que estes sejam assimilados e absorvidos pelos que compõem a companhia e passem a agir de forma mais íntegra nas relações interpessoais ao representarem a organização, conforme Costa & Medeiros (2019, p. 86).

Outro elemento primordial para um bom Programa de *Compliance* será um canal de denúncias, que possibilite aos *stakeholders* denunciarem atos ilícitos, de forma anônima.

De acordo com Moura (2016, p. 17 *apud* BOAVENTURA 2009) termo *stakeholder* surgiu em 1963 e foi inicialmente utilizado na área de administração em memorando interno do *Stanford Research Institute* (SRI). O conceito de *stakeholder* indicava todos os grupos dos quais a empresa dependia, e sem eles, a organização deixaria de existir. De acordo com o referido documento,

os grupos de *stakeholders* englobavam acionistas, empregados, clientes, fornecedores, credores e a sociedade, e propunha que os gestores conhecessem as necessidades destes entes e alinhassem aos objetivos.

Com efeito, para as implicações do Programa de *Compliance* Digital é de suma relevância existência de um canal de denuncias anônimas, para que os *stakeholders,* possam identificar e denunciar os problemas para assim atuar na prevenção dos riscos e prejuízos.

Ainda outro elemento importante é a contratação de um *compliance officer*, que será responsável pela informação e fiscalização no cumprimento do programa de integridade.

Crespo (2021, p. 100) destaca que na medida em que as empresas entenderam a necessidade de investir em *Compliance*, nasceu uma nova profissão: a do *Compliance Officer* e no mundo, desde o início dos anos 2000 esta posição tem sido muito procurada. A SCCE apresenta em seu *website* que possui mais de 7.500 profissionais da área de *Compliance,* espalhados ao redor do mundo, como seus associados. Já no Brasil, desde o advento da lei anticorrupção em 2013, esta posição, que já era importante em multinacionais, tem sido cada vez mais requisitada e valorizada.

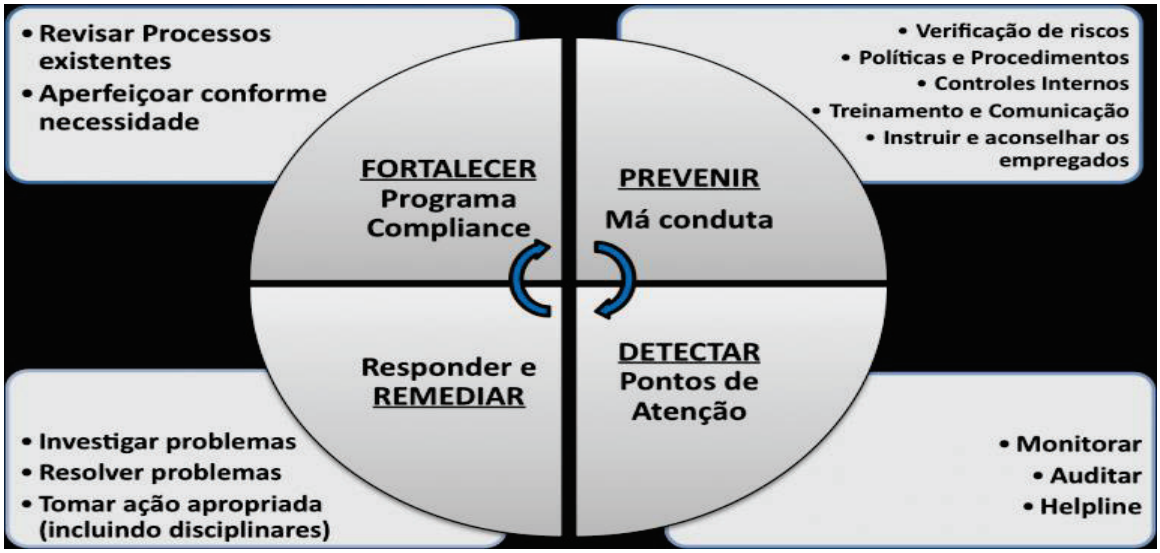
Nesse passo, é certo que o trabalho deste profissional é garantir o mapeamento, prevenção e gerenciamento de riscos para a empresa e sua reputação, assim como para seus colaboradores, conselho e investidores. Em razão da ampla necessidade de entender e antecipar riscos distintos, muitas empresas preferem ter advogados como responsáveis pelo programa de *Compliance,* outras optam por colocar nesta posição profissionais que tenham conhecimento e expertise mais específicos relacionados à área onde a referida instituição entende estar mais exposta a risco. Assim o *Compliance Officer* possui dentre suas obrigações três principais pilares importantes: PREVENIR, DETECTAR e RESPONDER (CRESPO, 2021, p. 100).

Cavalari (2020, p.50 *apud* LAMBOY 2017, 43) ainda complementa destacando que o *compliance officer*:

> é peça fundamental e indispensável para a efetividade, supervisão e gerenciamento do programa de *compliance* e para que ele atinja os seus objetivos na empresa. Ele é um agente promotor da integridade na organização, um gestor da integridade. Pode ser contratado pela própria organização, ou ser profissional terceirizado, ou até mesmo empresa terceirizada para desempenhar tais funções.

A seguir apresentamos um quadro demonstrativo do Programa de *Compliance* da EMBRAER que sintetiza os entendimentos em referência e que pode ser usado em qualquer Programa de *Compliance*, inclusive o Digital, para assim obter a extração de seus melhores resultados:

Figura 2: Programa de Compliance da EMBRAER



Fonte: Instituto Brasileiro de *Compliance* - IBC[5]

Pela demonstração acima deve ser observado que o Programa de *Compliance* dever ser aplicado de forma cíclica, e em uma espécie de *loop* infinito, para assim se manter atualizado e com tomadas de decisões precisas aptas prevenir riscos prejuízos e com aplicabilidade tanto nos setores público e privado.

Dessa forma, é certo que com as inovações tecnológicas e as transformações trazidas por instrumentos normativos, inclusive GDPR e LGPD, o Programa de *Compliance* Digital torna-se um aliado das ferramentas tecnológicas no ambiente da corporação, posto que, diante da rotina procedimental será possível observar e corrigir os riscos, bem como formular medidas de prevenção para respeitar as regras aplicáveis às tecnologias da informação, repelindo danos que possam resultar em prejuízos, tais como aplicação de multas e sanções que possam macular a integridade e credibilidade no meio social.

5 CONSIDERAÇÕES FINAIS

No decorrer dos tempos os dados passaram a ter grande valor a ponto de serem comparados ao petróleo, conforme a frase citada pelo matemático londrino Clive Humb - "Os dados são o novo petróleo" com repercussão mundial e até nos negócios, onde esse verdadeiro mantra foi

[5] Disponível em: Página do Instituto Brasileiro de *Compliance* - https://ibcompliance.com.br/2016/11/25/vale-conhecer-e-analisar-o-programa-de-compliance-da-embraer/. Acesso em 15/09/2022.

repetido de modo que Ajay Banga, CEO da Mastercard, destacou tal comparação faz sentido, exceto por um pequeno detalhe que o petróleo vai acabar um dia.

Dessa forma, podemos concluir que os dados são uma fonte inesgotável de possibilidades, geradores de benefícios para aqueles que souberem aproveitar o seu potencial no cruzamento para obtenção de resultados, que podem potencializar diversos ramos da sociedade, inclusive na implementação de políticas públicas.

Por certo, aliado à aceleração do crescimento tecnológico criou-se uma verdadeira redução da privacidade dos dados lançados no meio digital - canais e *internet,* a ponto de desencadear no mundo uma preocupação para a obtenção de instrumentos legais reguladores decorrentes de uma evolução histórica até chegar no Brasil a Lei nº 13.709, de 14 de agosto de 2018, a tão conhecida Lei Geral de Proteção de Dados – LGPD.

Nesse passo, vimos que o *Compliance* Digital apresenta elementos essenciais tais como: o código de conduta, o canal de denúncias e a contratação de um *compliance officer*, para assim viabilizar a adoção de ações de prevenção, detecção e de resposta para obtenção de resultados significativos para o ambiente corporativo.

Nesta seara, o Programa de *Compliance* deve ser cíclico, em *loop* infinito, para assim manter uma atualização constante para propiciar o seu alto grau de eficiência, e como resultado privilegiará um ambiente corporativo mais seguro e eficiente, bem como para a construção de relações cristalinas com fornecedores, clientes e administrados, tanto nos Setores Privado e como Público.

REFERÊNCIAS

ARAGÃO, M. de A. G. O IMPACTO DO FACEBOOK SOBRE O SUL GLOBAL: O QUE ACONTECE QUANDO NÃO SE IMPORTA O SUFICIENTE. Disponível em: http://periodicos.pucminas.br/index.php/fronteira/article/view/26210/19928. Acesso em 15/09/2022.

BALDO, Wallace. COMO O OMBUDSMAN DE DADOS PODE REFORÇAR A MULTIDISCIPLINARIDADE NA COMUNICAÇÃO ORGANIZACIONAL? Disponível em: https://portalintercom.org.br/anais/nacional2018/resumos/R13-0334-1.pdf. Acesso em: 10/09/2022.

BEZERRA, Arthur Coelho; WALTZ, Igor. PRIVACIDADE, NEUTRALIDADE E INIMPUTABILIDADE DA INTERNET NO BRASIL: AVANÇOS E DEFICIÊNCIAS NO PROJETO DO MARCO CIVIL. REVISTA DE ELETRÔNICA INTERNACIONAL DE ECONOMIA POLÍTICA DA INFORMAÇÃO DA COMUNICAÇÃO E DA CULTURA, Florianópolis, v.16, n.2, p.157-171, maio/ago. 2014.

BLUM, Renato Opice. MALDONADO, Viviane. COMENTÁRIOS AO GDPR: REGULAMENTO GERAL DE PROTEÇÃO DE DADOS DA UNIÃO EUROPÉIA. São Paulo. Thomson Reuters Brasil. 2018, p. 13 e 66.

BRASIL. Lei Federal nº 8.078, de 11 de setembro de 1990 – Código de Defesa do Consumidor. Disponível em: https://www2.senado.leg.br/bdsf/bitstream/handle/id/496457/000970346.pdf. Acesso em: 11/09/2022.

BRASIL. Lei Federal 12.414, de 09 de junho de 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm#:~:text=LEI%20N%C2%BA%2012.414%2C%20DE%209%20DE%20JUNHO%20DE%202011.&text=Disciplina%20a%20forma%C3%A7%C3%A3o%20e%20consulta,forma%C3%A7%C3%A3o%20de%20hist%C3%B3rico%20de%20cr%C3%A9dito. Acesso em: 12/09/2022.

BRASIL. Constituição da República do Brasil. Disponível em http://www.planalto.gov.br/ccivil_03/constituicao/constituicao67.htm Acesso em 11/09/2022.

BRASIL. Lei nº 12.965, de 23 de abril de 2014 – Marco Civil da Internet. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 12/09/2022.

CARTA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA DE 2000. Disponível em http://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em 11/09/2022.

CAVALARI. Ana Paula França. O COMPLIANCE DIGITAL COMO TECNOLOGIA DE GESTÃO. Disponível em: http://www.esars.com.br/ebooks/E-BOOK_ELAS_NA_ADVOCACIA_COMPLETO.pdf. Acesso em: 11/09/22.

CRESPO. Liana Irani Affonso Cunha. COMPLIANCE OFFICER E EFETIVIDADE: SOBRE AS CONDIÇÕES NECESSÁRIAS PARA GARANTIR A AÇÃO EFETIVA DO PROGRAMA DE COMPLIANCE. Disponível em: https://dspace.mackenzie.br/bitstream/handle/10899/28412/Liana%20Irani%20Affonso%20Cunha%20Crespo.pdf?sequence=1&isAllowed=y. Acesso em: 16/09/2022.

CONVENÇÃO 108. Conselho da Europa. Proteção de Dados Pessoais. Disponível em http://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf. Acesso em 10/09/2022.

CONVENÇÃO EUROPÉIA DOS DIREITOS DO HOMEM. Tribunal Europeu dos Direitos do Homem. Disponível em https://www.echr.coe.int/Documents/Convention_POR.pdf Acesso em 09/09/2022.

COSTA. Fernando Medeiros Costa. MEDEIROS Nilton Carvalho Lima de. ELEMENTOS ÉTICOS NO DESENVOLVIMENTO DO CÓDIGO DE CONDUTAPARA IMPLEMENTAÇÃO DE UM PROGRAMA DE COMPLIANCE. Disponível em: https://indexlaw.org/index.php/direitoempresarial/article/view/5592/pdf. Acesso em: 15/09/2022.

"DADOS SÃO O NOVO PETRÓLEO", DIZ CEO DA MASTERCARD – EXCETO POR UM PEQUENO DETALHE. Revista Época. Disponível em: https://epocanegocios.globo.com/Empresa/noticia/2019/07/dados-sao-o-novo-petroleo-diz-ceo-da-mastercard.html. Acesso em 10/09/2022.

FRAZÃO. Ana. OLIVA. Milena Donato. ABILIO, Vivianne da Silveira. COMPLIANCE DE DADOS PESSOAIS E SUAS REPERCUSSÕES NO DIREITO BRASILEIRO. 1 ed., São Paulo: Thomson Reuters Brasil, 2019.

GOOGLE E META SÃO MULTADOS POR ROUBAR INFORMAÇÕES DE USUÁRIOS NA COREIA DO SUL. Revista Olhar Digital, 2022. Disponível em: https://olhardigital.com.br/2022/09/14/internet-e-redes-sociais/google-e-meta-sao-multados-por-roubar-informacoes-de-usuarios-na-coreia-do-sul/. Acesso em: 15/09/2022.

MORELLI. Lucas, CONSIDERAÇÕES SOBRE DIREITO E TECNOLOGIA E A EVOLUÇÃO DO DIREITO PRIVADO. Disponível em: https://periodicosunimes.unimesvirtual.com.br/index.php/direito/article/viewFile/1221/1023. Acesso em: 10/09/2022.

MOURA. Rosicler Oliveira de. A INFLUÊNCIA DOS STAKEHOLDERS NO DESEMPENHO ORGANIZACIONAL EM EMPRESAS ESTATAIS FEDERAIS. Disponível em: https://bibliotecadigital.fgv.br/dspace/handle/10438/16985. Acesso em: 15/09/2022.

O INÍCIO DO TERROR NAZISTA. Enciclopédia do Holocausto. Disponível em: https://encyclopedia.ushmm.org/content/pt-br/article/the-nazi-terror-begins. Acesso em: 10/09/2022.

SILVA. Fabiani Oliveira Borges. A RESPONSABILIDADE DO COMPLIANCE OFFICER NA PROTEÇÃO DE DADOS PESSOAIS. Revista de Direito e Novas Tecnologias. vol. 3/2019 | Abr - Jun / 2019 | DTR\2019\35399.

VALADARES. Heloisa de Carvalho Feitosa. PRIVACIDADE, PROTEÇÃO DE DADOS E AUTODETERMINAÇÃOINFORMATIVA: entre a visão patrimonial e de direito fundamental. Disponível em: https://periodicos.unesc.net/ojs/index.php/AnaisDirH/article/view/7522/6377. Acesso em 15/09/2022.