

VI ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

FREDERICO THALES DE ARAÚJO MARTOS

JÉSSICA AMANDA FACHIN

AIRES JOSE ROVER

Todos os direitos reservados e protegidos. Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria - CONPEDI

Presidente - Prof. Dr. Orides Mezzaroba - UFSC - Santa Catarina

Diretora Executiva - Profa. Dra. Samyra Haydêe Dal Farra Naspolini - UNIVEM/FMU - São Paulo

Vice-presidente Norte - Prof. Dr. Jean Carlos Dias - Cesupa - Pará

Vice-presidente Centro-Oeste - Prof. Dr. José Querino Tavares Neto - UFG - Goiás

Vice-presidente Sul - Prof. Dr. Leonel Severo Rocha - Unisinos - Rio Grande do Sul

Vice-presidente Sudeste - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio - Rio de Janeiro

Vice-presidente Nordeste - Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR - Ceará

Representante Discente: Prof. Dra. Sinara Lacerda Andrade - UNIMAR/FEPODI - São Paulo

Conselho Fiscal:

Prof. Dr. Caio Augusto Souza Lara - ESDHC - Minas Gerais

Prof. Dr. João Marcelo de Lima Assafim - UCAM - Rio de Janeiro

Prof. Dr. José Filomeno de Moraes Filho - Ceará

Prof. Dr. Lucas Gonçalves da Silva - UFS - Sergipe

Prof. Dr. Valter Moura do Carmo - UNIMAR - São Paulo

Secretarias

Relações Institucionais:

Prof. Dra. Daniela Marques De Moraes - UNB - Distrito Federal

Prof. Dr. Horácio Wanderlei Rodrigues - UNIVEM - São Paulo

Prof. Dr. Yuri Nathan da Costa Lannes - Mackenzie - São Paulo

Comunicação:

Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali - Rio Grande do Sul

Profa. Dra. Maria Creusa De Araújo Borges - UFPB - Paraíba

Prof. Dr. Matheus Felipe de Castro - UNOESC - Santa Catarina

Relações Internacionais para o Continente Americano:

Prof. Dr. Heron José de Santana Gordilho - UFBA - Bahia

Prof. Dr. Jerônimo Siqueira Tybusch - UFSM - Rio Grande do Sul

Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA - Maranhão

Relações Internacionais para os demais Continentes:

Prof. Dr. José Barroso Filho - ENAJUM

Prof. Dr. Rubens Beçak - USP - São Paulo

Profa. Dra. Viviane Coêlho de Séllos Knoerr - Unicritiba - Paraná

Eventos:

Prof. Dr. Antônio Carlos Diniz Murta - Fumec - Minas Gerais

Profa. Dra. Cinthia Obladen de Almendra Freitas - PUC - Paraná

Profa. Dra. Livia Gaigher Bosio Campello - UFMS - Mato Grosso do Sul

Membro Nato - Presidência anterior Prof. Dr. Raymundo Juliano Feitosa - UMICAP - Pernambuco

D597

Direito, governança e novas tecnologias I [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Aires Jose Rover; Frederico Thales de Araújo Martos; Jéssica Amanda Fachin – Florianópolis; CONPEDI, 2023.

Inclui bibliografia

ISBN: 978-65-5648-745-8

Modo de acesso: www.conpedi.org.br em publicações

Tema: Direito e Políticas Públicas na era digital

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito. 3. Governança e novas tecnologias. VI Encontro Virtual do CONPEDI (1; 2023; Florianópolis, Brasil).

CDU: 34



VI ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

Apresentação

O VI Encontro Virtual do CONPEDI, realizado em parceria com o Programa de Mestrado Profissional em "Direito, Sociedade e Tecnologias" das Faculdades Londrina e a Faculdade de Direito de Franca (FDF), ocorreu nos dias 20, 21, 22, 23 e 24 de junho de 2023. O evento teve como temática central "Direito e Políticas Públicas na Era Digital". As discussões realizadas durante o encontro, tanto nas diversas abordagens tecnológicas como nos Grupos de Trabalho (GTs), foram de grande relevância, considerando a atualidade e importância do tema.

Nesta publicação, os trabalhos apresentados como artigos no Grupo de Trabalho "Direito, Governança e Novas Tecnologias I", no dia 23 de junho de 2023, passaram por um processo de dupla avaliação cega realizada por doutores. A obra reúne os resultados de pesquisas desenvolvidas em diferentes Programas de Pós-Graduação em Direito, abordando uma parte significativa dos estudos produzidos no âmbito central do Grupo de Trabalho.

As temáticas abordadas refletem intensas e numerosas discussões que ocorrem em todo o Brasil. Elas destacam o aspecto humano da Inteligência Artificial, os desafios para a democracia e a aplicação do Direito no ciberespaço, bem como reflexões atuais e importantes sobre a regulação das plataformas digitais e as repercussões das novas tecnologias em diversas áreas da vida social.

Esperamos que, por meio da leitura dos textos, o leitor possa participar dessas discussões e obter um entendimento mais amplo sobre o assunto. Agradecemos a todos os pesquisadores, colaboradores e pessoas envolvidas nos debates e na organização do evento, cujas contribuições inestimáveis foram fundamentais, e desejamos uma leitura proveitosa!

Prof. Dr. Aires Jose Rover - Universidade Federal de Santa Catarina/SC

Profa. Dra. Jéssica Fachin - Faculdades Londrina/PR

Prof. Dr. Frederico Thales de Araújo Martos - Faculdade de Direito de Franca/SP e Universidade do Estado de Minas Gerais/MG

**COMPLIANCE DIGITAL COMO FERRAMENTA DE APOIO FRENTE AS
INOVAÇÕES TECNOLÓGICAS**

**DIGITAL COMPLIANCE AS A SUPPORT TOOL FOR TECHNOLOGICAL
INNOVATIONS**

Paulo Cezar Dias ¹
Ana Cristina Neves Valotto Postal ²
Marlene de Fátima Campos Souza ³

Resumo

O propósito do presente artigo é dirimir o entendimento acerca da tecnologia e dos meios digitais, sem esgotar o tema, a fim de compreender que as inovações tecnológicas e a ciência da comunicação tornou-se algo inerente a todos indistintamente, e como usuários deste sistema o qual não demanda mais retrocesso, depara-se com a exposição exacerbada dos dados pessoais, demandando uma proteção à privacidade destes dados, e frente a isso como as empresas independente do seu porte, devem atuar, e eis que esse artigo não somente traz a conceituação do compliance, mas sobretudo do compliance digital. O ordenamento jurídico brasileiro atual, busca regulamentar a proteção dos dados pessoais, sendo objeto de comento neste artigo. Portanto, o presente trabalho, utilizando-se do método bibliográfico de pesquisa, estudo doutrinário, estudos legislativos, objetiva demonstrar como o compliance digital em conformidade com essa normatização de toda sorte servirá como ferramenta de apoio as empresas, voltado à prevenção e mitigação dos riscos, evitando prejuízos de ordem financeira e quiçá desgaste a reputação da imagem da empresa, inclusive quanto as inovações tecnológicas as quais ainda esbarram em lacunas normativas.

Palavras-chave: Meios digitais, Compliance digital, Marco civil da internet, Lgpd, Inovações

Abstract/Resumen/Résumé

The purpose of this article is to resolve or understand the technology and the digital media, without exhausting the theme, in order to understand that the technological innovations and the science of communication become something inherent to all indistinctly, and as users of this system to which no further retrocess is required, we deal with the exacerbated exposure

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 do UNIVEM, constituído pelo Curso de Mestrado Acadêmico em Direito, com área de concentração o tema DIREITO E ESTADO ERA DIGITAL

³ Prof. Doutora em Ciências Sociais pela PUC - São Paulo, Mestre em Ciências Contábeis pela PUC – São Paulo, pós-graduada na área de Ciências Contábeis e Administração pelo Univem

of personal data, demanding a privacy protection of these data, and in the face of that, as companies regardless of their size, must act, and you know that this article is not only traced to the concept of compliance, more especially of digital compliance. Our current legal system, seeks to regulate the protection of two people, being the subject of comment in this Article. Therefore, this work, using the bibliographic research method, doctrinal study, legislative studies, aims to demonstrate how digital compliance in accordance with this standardization of all luck will serve as a support tool for companies, aimed at preventing and mitigating both risks, avoiding financial prejudices and it may wear down the reputation of the company's image, including how much technological innovations are still present in a regulatory gap.

Keywords/Palabras-claves/Mots-clés: Digital media, Compliance digital, Civil rights framework for the internet, Lgpd, Innovation

INTRODUÇÃO

A tecnologia tornou-se algo tão inerente na vida das pessoas, que de forma natural e hodiernamente o acesso aos meios digitais, faz com que transitem em redes sociais, acessem informações financeiras e de trabalho, relações consumeristas, lazer e nesse movimento acabam de forma espontânea inserindo os seus dados pessoais.

Por sua vez a exposição destes dados pessoais sobrevém uma vulnerabilidade nesse meio digital, tornando-se imprescindível que uma empresa, independente do seu porte, adote um programa de *compliance*, sobretudo de *compliance* digital, com intuito de mitigar os riscos que possam advir de compartilhamento e uso dos dados, vazamento, prevenção dos riscos de ciberataques, sequestros de dados, dentre outras circunstâncias que envolvam o acesso aos dados pessoais de forma ilícita e ilegal.

Observa-se que, ao mesmo tempo que a tecnologia se tornou algo positivo no cotidiano das pessoas, mas há o revés desta questão, a preocupação com essa gama de informações lançadas pelas pessoas, as quais precisam ser preservadas à sua privacidade, cabendo as empresas adotarem uma postura prudente, ética, transparente no tocante ao uso destes dados, adotando o *compliance* digital como meio de prevenção dos riscos.

Objetiva-se com o presente artigo conceituar tecnologia, meios digitais, *compliance* para melhor compreensão do *compliance* digital, e como tal conformidade pode contribuir no seio de uma empresa, face a legislação existente que regulamenta a matéria, como atualmente a Lei do Marco Civil da Internet e da Lei Geral de Proteção de Dados.

E como o *compliance* digital pode vir auxiliar uma empresa, diante de lacunas normativas existentes diante das inovações tecnológicas, na medida que o poder legiferante não consegue acompanhar tamanha velocidade destas transformações?

A metodologia utilizada no desenvolvimento deste artigo para a resposta do problema é o método bibliográfico de pesquisa, estudo doutrinário, estudos legislativos.

1- TECNOLOGIA

Tire hoje uma foto de uma sala de estar em uma residência, de um restaurante, de um shopping, de um ambiente corporativo. Tirou? Consegue observar alguém que não esteja diante de um smartphone, tablet, computador, notebook, de certo que não, correto? Já parou para pensar a humanidade sem todo esse aparato tecnológico, algo difícil de imaginar e de se conceber.

O uso da tecnologia está tão imantado em todos, que se tornou algo natural, usufruir de todas as benesses deste meio tecnológico que esse século proporciona, que sequer paramos para refletir, o que é a tecnologia, utilizada no ambiente de trabalho, no lazer, em nossas residências, e em tantos outros lugares e ocasiões.

Segundo Cavalari (2020, p. 44 *apud* VELOSO, 2011, p.3) aduz:

São diversas as conceituações de tecnologia. Em uma perspectiva mais superficial, o conceito de tecnologia pode ser aplicado a tudo aquilo que, não existindo na natureza, o ser humano inventa para expandir seus poderes, superar suas limitações físicas, tornar seu trabalho mais fácil e sua vida mais agradável. Além disso, tecnologia não é apenas instrumento, ferramenta ou equipamento tangível. Ela pode constituir-se por elementos tangíveis, como procedimentos, métodos, técnicas etc. Desta forma, ao falarmos em tecnologia, isso não significa, necessariamente, que estamos falando sobre tecnologias da informação e comunicação, embora a tendência nos dias atuais seja a de confundir tais termos, ou ainda tomá-los como sinônimos.

Pode-se contribuir ainda sobre o conceito de tecnologia, nos dizeres de Akabane e Pozo (2020, p.17-19):

Outra definição, a partir do Dicionário de Negócios, explica a tecnologia como aplicação intencional de informações no projeto, na produção e no uso de conhecimentos para desenvolver um produto ou serviço. Esse discurso definitivamente apresenta uma boa compreensão de como a tecnologia é definida. Suas variações ajudariam a entender as questões mais profundas sobre como gerenciá-la e direcioná-la para a inovação. Pode-se também considerar a tecnologia como um processo que converte conhecimento sistemático (conceitual, empírico e/ou científico) em objetos úteis para apoiar as atividades humanas. Trata-se da combinação de objetos físicos, necessidades sociais, processo e procedimento.

Logo, Cavalari (2020, *apud* MCLUHAN, 2007, p.60-61) comenta: “*Não basta entender a tecnologia como propiciadora, meio ou fonte de trabalho é necessário compreender que a tecnologia é extensão do homem.*”

As transformações sociais catalisadas pela tecnologia marcam a sociedade contemporânea, que a utiliza como meio ou fundamento de suas identidades. Passamos de uma sociedade industrial, movida por complexas engrenagens, para uma sociedade impulsionada pela hiper-informação. (CAVALARI, 2020, p.44)

Exatamente isso que a tecnologia nos proporciona uma quantidade avassaladora de informações, logo, essa conexão do homem com a tecnologia, desencadeou um acesso frenético ao mundo tecnológico, impulsionado pelo período pandêmico do COVID-19, ampliando o número de pessoas fazendo compras on-line nos supermercados, farmácias, restaurantes, e diversos outros produtos, aquisição de serviços, e por trás desta tela de computador, tablet, celular deparam-se empresas fornecendo seus bens e serviços.

Tem se visto empresas inovarem seus modelos de acesso aos clientes, para manter-se “vivas” neste mercado envolvido por um universo pandêmico, empresas inovando frente a globalização para tornarem-se competitivas.

De acordo com Akabane e Pozo (2020, p.7):

As mudanças no ambiente de negócios incluem novas tecnologias e inovações, que forcem as indústrias e as empresas a encontrarem novas maneiras de competir e sobreviver. Com o desenvolvimento constante de novos produtos, novos processos estão surgindo rapidamente para acompanhar esse momento e, assim, tornar as empresas mais eficientes e eficazes.

Com a globalização e uma nova sociedade organizada em rede de compartilhamentos, surgem novos riscos a serem tutelados, que até então não eram sequer imagináveis ao Direito. A manipulação da tecnologia gera riscos de efeitos colaterais, sendo que assim cresce a sensação de insegurança nesta nova sociedade, agora já atenta e preocupada com os riscos. (TONIN, 2017, p.265/268)

E eis que se a tecnologia arrebatou a todos, que conectados em seus equipamentos buscam informações, serviços, produtos, do outro lado empresas saciando essas novas necessidades, tem-se um alerta, pessoas lançando seus dados pessoais, tornando-se assim vulneráveis em um ambiente desconhecido.

Aduz Cavalari (2020, *apud* MENDES, SARLET, e COELHO, 2015. p. 96) quanto a esse ponto:

O desenvolvimento tecnológico pressupõe um regime jurídico sobre a tecnologia desenvolvida nos mais diversos ambientes, no âmbito do Estado, do mercado e da sociedade, revelando-se no uso do poder de coação do Estado, na disciplina e na limitação das decisões dos agentes, bem como na intervenção e operação dos setores tecnológicos de qualquer tipo, tudo para garantir-lhes os investimentos necessários e promover o bem estar dos consumidores e usuários, de modo a alcançar o incremento da eficiência econômica e o suprimento das necessidades sociais. E se hoje utilizando-se dos meios digitais as pessoas propagam seus dados, os quais necessitam de proteção, isso decorre em razão do uso da tecnologia.

2-1 MEIOS DIGITAIS

A priori observa-se o que prelaiona Cavalari (2020, p.40):

Atualmente, todas as atividades que exercemos em nosso cotidiano apresentam relação ao meio digital. Redes sociais, informações de trabalho, acesso às informações financeiras, tudo isso fazemos em nosso dia a dia sem se quer ao menos perceber. Nessa rotina, diversos são os dados pessoais lançados por meio de aceite que tão rapidamente concedemos nos termos de uso e condições de aplicativos, visitação em sites.

Certo que a tecnologia impulsionou o desenvolvimento tecnológico, engendrando os meios digitais, algo capaz de auxiliar e simultaneamente causar danos incalculáveis as pessoas e as empresas. Imprescindível aclarar o que venha a ser meios digitais para melhor compreensão da temática.

Conceitua-se meios digitais:

Em geral, o termo refere-se a qualquer mídia que utiliza, como meio, um computador ou equipamento digital para criar, explorar, finalizar ou dar continuidade a um projeto que tem como suporte a internet, comunicação online ou offline, produções gráficas, videogames, conteúdos audiovisuais etc. Se opõe também às mídias analógicas, usufruindo assim das vantagens técnicas dos meios digitais como uma maior agilidade na manipulação e criação de conteúdo. Além disso, o conteúdo pode ser reproduzido e reutilizado sem perda de qualidade, o que garante um fluxo de trabalho muito mais dinâmico e multimidiático, favorecendo assim a interdisciplinaridade ou a integração entre os diferentes meios, sendo essa uma característica marcante desse tipo de mídia e processo de trabalho¹.

E contribuem Andréa, Arquite e Camargo (2020) sobre o que venha a ser a internet:

A Internet se resume, portanto, em uma rede no qual inúmeros dispositivos de comunicação são conectados com o objetivo de realizar compartilhamento de dados de forma constante manualmente ou de forma autônoma entre si, por exemplo, a internet das coisas. A internet das coisas nada mais é do que a interconexão entre diversos objetos presentes no nosso cotidiano de forma constante e autônoma, sendo controlada pelo detentor das coisas.

Já os dados, dentro da internet, constituem-se em conjunto de informações que são compartilhadas entre os dispositivos integrantes da rede, representadas através de códigos binários (0 e 1), que são “descriptografados” e “lidos” pelo dispositivo receptor. Os computadores, por processarem qualquer arquivo de forma binária, recebem e armazenam os dados da mesma forma e, que, após o processamento dos dados, transformam no elemento compartilhado. Este, pode ser um documento, uma imagem, um texto, um filme ou praticamente qualquer outra coisa. O conjunto dos referidos dados forma o que é chamado de big data.

Andréa, Arquite e Camargo (2020 *apud* ALVES, 2013), explicam acerca dos algoritmos para que se possa compreender o passo a passo deste meio digital:

são basicamente conjuntos de informações efetuadas para que uma máquina execute determinado procedimento. Trata-se de um mero “guia” contendo elementos que, seguidos em uma ordem lógica pelo computador, correspondem a uma ação. Utilizados no campo da programação por empresas e demais instituições, quando possuem um número suficiente de informações sobre um usuário, poderão traçar o perfil e sugerir opções de seu gosto de forma automática, apenas baseando-se em experiências anteriores.

E no tocante aos *cookies* Andréa, Arquite e Camargo (2020 *apud* SOUZA, 2018, p. 26) expõem:

os *cookies*, por sua vez, compõem a principal tecnologia de rastreamento e monitoramento de usuários na Internet. Permitem a análise de navegação do usuário

¹WIKIPEDIA.

Disponível

em:

https://pt.wikipedia.org/wiki/M%C3%ADdia_digital#:~:text=outras%20m%C3%ADdias%20interativas-.Conceito,videogames%2C%20conte%C3%BAdos%20audiovisuais%2C%20etc. Acesso em: 13 set 2022.

por um período certo de tempo, funcionando da seguinte forma: em regra, a empresa coloca um *cookie* de rastreamento (*tracking cookie*) em um instrumento denominado DTE (*data terminal equipment*), que ordinariamente converte informações do usuário em sinais quando se acessa algum *website* que contém tais tecnologias. Essencialmente, os *cookies* são arquivos de texto simples, armazenados pelo navegador frequentado, contendo informações básicas acerca das preferências dos usuários.

Cavalari (2020 *apud* SILVA, 2019) complementa:

Com o aumento da capacidade de processamento dos dados pelos computadores é que se observa o fenômeno da *Big Data*, ou seja, a capacidade computacional de obter e processar grande volume de dados. E com isso, a partir dela, vê-se o 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.

E Cavalari (2020 *apud* GALLOWAY, 2017. p. 259) explica o que significa esse capitalismo de vigilância:

O capitalismo de vigilância referido acima nada mais é senão a venda dos dados que fornecemos, em sua grande parte gratuitamente, às grandes empresas de tecnologia, como Google, Facebook, Apple e Amazon – os quatro maiores cavaleiros – e tantas outras.

Denota-se que, quando a pessoa acessa os serviços por meios digitais, e simplesmente não paga por este serviço, é porque o produto é a pessoa, a moeda de troca é a pessoa e os dados dela.

Percebe-se que, os meios digitais é a porta de entrada dos dados dos usuários, que utilizando-se de equipamentos (computador, notebook, tablet, smartwhatches) conectados à internet, trafegam em sites, em ambientes virtuais, projetam seus dados e na grande maioria das vezes de forma inconsciente, pois no afã de pesquisar informações de forma rápida clica-se em aceites, sem ler o conteúdo do termo de uso disponibilizado, preenchem cadastros, pesquisas, e inúmeras outras maneiras de divulgação, sequer vislumbrando tão vulneráveis se encontram expostos.

E sempre há o outro lado da moeda, porque se as pessoas disponibilizam seus dados através dos meios digitais, tem alguém recepcionando esses dados, e deste lado oposto encontram-se as empresas, e sempre bom deixar consignado independente do porte, está lá amealhando esse arsenal de dados, que precisam ser por certo preservados.

Cavalari (2020 *apud* JIMENE e VAINZOF, 2018) complementa:

Atualmente os dados corporativos das organizações encontram-se armazenados em diferentes ambientes: servidores da empresa ou em nuvem, *notebooks*, celulares, *tablets*, *smartwatches*, *pendrives* e aplicações de Internet, corporativas ou muitas vezes particulares.

Fato é 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.

Deste modo, pode-se ter uma noção do local de armazenamento destes dados por parte de uma empresa, mas essa corporação seria ciente da importância do dado de uma pessoa, dos riscos inerentes pela ausência de proteção e cuidado de forma idônea deste dado, é isso que o *compliance* visa instruir e dar o devido regramento.

2- COMPLIANCE

O *compliance* é estar em conformidade, sendo uma prática empresarial que impõe padrões internos para o cumprimento de normas, observância de leis e regulamentos internos e externos, formulação de diretrizes nacionais e internacionais, buscando mitigar o risco atrelado à reputação e à regularização legal. Neste diapasão cria-se um código de conduta, que defina a postura ética da empresa. (CAVALARI, 2020, p. 41)

Magalhães Júnior (2018 *apud* CANDELORO, RIZZO e PINHO, 2012, p.30) por sua vez conceitua:

Compliance significa agir de acordo com uma regra, uma instrução, um comando ou pedido. Não se pode confundir o *Compliance* com o mero cumprimento de regras formais e informais, sendo o seu alcance bem mais amplo, ou seja, “é um conjunto de regras, padrões, procedimentos éticos e legais, que, uma vez definido e implantado, será a linha mestra que orientará o comportamento da instituição no mercado em que atua, bem como a atitude dos seus funcionários.

É possível “copiar” o *compliance* da empresa vizinha? É preciso analisar a o seu segmento, a estrutura da sua empresa, a atividade inerente, para iniciar uma concepção de quais riscos a empresa poderá deparar-se no departamento de compras, recursos humanos, tecnologia da informação, financeiro, tributário, comercial, trabalhista, contábil, logo o *compliance* está inserido em uma transversalidade, cuja empresa até pode compilar pontos do *compliance* da empresa vizinha, mas o primordial é procurar conhecer os riscos do seu próprio negócio, visando preveni-los e mitiga-los ao máximo. Estar em *compliance* é minimizar a chance de perda financeira e de dano a reputação à imagem da empresa.

Não obstante a empresa estar em *compliance*, em ocorrendo o evento danoso, é possível apresentar a autoridade competente o programa de conduta da empresa, imediatamente pôr-se-á investigar o motivo pelo qual efetivou o evento, conter o evento se ainda persistir no tempo,

punir os infratores, ao passo que não estando em *compliance* a empresa já deixa de apresentar seu padrão de conduta, que dependendo do dano se assemelhará a um avião em queda livre, visto que, até a empresa entender e identificar o ocorrido, tomar atitude(s), infelizmente os prejuízos financeiros e riscos a imagem tornar-se-ão algo imensurável.

Mas há que se conceber que não basta uma empresa estar simplesmente em *compliance*, essa rotina deve ser fiscalizada, deve-se avaliar as mudanças na legislação, no cenário econômico, financeiro, para ir galgando a sua atualização, sob pena de ficar um programa obsoleto, também passível de ocorrência dos eventos danosos, devido à ausência de ingerência no cotidiano desta empresa.

Magalhães Júnior (2018, apud RIBEIRO E DINIZ, 2015, p.87-105) complementa:

a implantação de uma política de *Compliance* é essencial para empresas que prezam pela eficiência e buscam perenizar e aumentar os seus lucros, pois a transparência, a ética e a confiança são condições legais, e não apenas itens de ostentação. Para as autoras "a implantação da política de *Compliance* é uma ferramenta poderosa, principalmente se obtida a partir da cooperação, pois estimula naturalmente um ambiente com transparência, ética e confiança, auxiliando no desenvolvimento pleno da empresa e da sociedade". Além disso, "a implantação de uma política de *Compliance* auxilia não somente no desenvolvimento da empresa, mas principalmente da sociedade, porque os comportamentos adotados em cada seara tendem a ser copiados e replicados, estimulando a transparência, a ética e a confiança em qualquer relação, bases para uma verdadeira sustentabilidade.

Segundo Cavalari (2020 apud LAMBOY, 2017, p.9) o *compliance* é então uma estratégia não apenas voltada a obter ganho de valor e competitividade em longo prazo, mas também contribui decisivamente para a própria sobrevivência da organização, sem olvidar que não estando em *compliance*, o custo a que estarão sujeitas sofrer incidência, poderão ser bem maiores.

O *Compliance* é uma responsabilidade de todos os funcionários, estagiários, colaboradores, prestadores de serviço e fornecedores da empresa, sem distinção da função exercida. Estes são os responsáveis primários pela condução dos processos, controles e riscos.

A autora Cavalari (2020, p. 42) aduz que, de acordo com a Associação Brasileira dos Bancos Internacionais (ABBI) e a Federação Brasileira de Bancos (FEBRABAN), a função de *compliance*, aplicável às organizações em geral, possui o seguinte escopo:

Assegurar, quanto a: Leis – aderência e cumprimento; Princípios Éticos e Normas de Conduta – existência e observância; Regulamentos e Normas – implementação, aderência e atualização; Procedimentos e Controle Interno -existência e observância; Sistemas de Informações – implementação e funcionalidade; Planos de Contingência – implementação e efetividade, por meio de testes periódicos; Segregação de funções – adequada implementação a fim de evitar o conflito de interesses; Relatório do sistema de controles internos (Gestão de *compliance*) – avaliação dos riscos e dos

controles internos – elaboração com base nas informações obtidas junto às diversas áreas da instituição, visando apresentar a situação qualitativa do sistema de controles internos; Políticas Internas – que previnam problemas de não conformidade com leis e regulamentações.

Impõe-se 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. (CAVALARI, 2020, p. 49)

Quanto ao risco do *compliance* pode-se entender:

É o risco de sanções legais ou regulatórias, perdas financeiras ou danos reputacionais, bem como de medidas administrativas ou criminais decorrentes da falta de cumprimento de disposições legais e regulamentares, normas de mercado local e internacional ou decorrentes de compromissos assumidos por meio de códigos de autorregulação, padrões técnicos ou códigos de conduta.²

Verifica-se que a empresa que faz sua gestão de riscos, identificando as atividades voltadas a minimizar as incertezas que podem prejudicar os projetos e o desempenho do seu negócio, busca evitar o evento surpresa seja através de fatores internos ou externos. (MAGALHÃES JÚNIOR, 2018)

Segundo Magalhães Júnior (2018) pontuando acerca da classificação dos riscos:

O Instituto Brasileiro de Governança Corporativa – IBGC também trata da classificação dos riscos (IBGC, 2007. p. 18). Nessa classificação, os riscos primeiramente são categorizados quanto a sua origem em externos e internos. Riscos externos são “ocorrências associadas ao ambiente macroeconômico, político, social, natural ou setorial em que a organização opera”. Enquanto que os riscos internos correspondem aos eventos “originados na própria estrutura da organização, pelos seus processos, seu quadro de pessoal ou de seu ambiente de tecnologia”.

De acordo com Magalhães Júnior (2018, *apud* DAMODARAN, 2009, p.26):

A gestão de riscos por parte da empresa, representada pelo conjunto de atividades voltadas a minimizar as incertezas que podem prejudicar os projetos e o desempenho das organizações, mostra-se fundamental para evitar que a empresa seja surpreendida pela ocorrência de fatores internos ou externos que possam prejudicar o seu desempenho. É por isso que a identificação dos fatores de risco constitui a primeira etapa de qualquer metodologia de gestão. O tipo de risco, a sua probabilidade de ocorrência, ou o seu impacto, variam ao longo do desenvolvimento do negócio. Essas são as razões que justificam o detalhamento pormenorizado no trabalho de identificação dos fatores de risco, a cada fase evolutiva de qualquer que seja o empreendimento (DAMODARAN, 2009. p. 368-369).

² FEBRABAN (Federação Brasileira de Bancos). GUIA | BOAS PRÁTICAS DE COMPLIANCE Edição revista e atualizada 2018. Disponível em: https://cmsarquivos.febraban.org.br/Arquivos/documentos/PDF/febraban_manual_compliance_2018_2web.pdf. Acesso em: 08 set 2022.

Assim, [...] as organizações que atuam com ética e evitam conflitos jurídicos, processos judiciais, acabam por diminuir, portanto, os riscos legais e os seus custos. Também resta claro, não ser possível tratar da importância do *compliance*, sem falar de ética e transparência. (CAVALARI, 2020, p.43)

Observa-se que, o *compliance* implantado em uma empresa, visa também o atingimento do estado de conformidade e sustentabilidade da empresa, possibilitando o aumento da prevenção de atos ilícitos, redução de perdas financeiras e de danos à reputação e imagem.

No tocante ao dano à reputação e imagem, tem-se que Magalhães Júnior (2018, *apud* MENEZES, 2011, p.16-20) contribui:

Warren Buffet certa vez disse que “*se você perder o dinheiro da empresa, eu irei compreender. Se você prejudicar a nossa reputação, eu serei impiedoso*” (MENEZES, 2011). Tal declaração vem confirmar que o valor da marca para as empresas é de vital importância³, visto que compõe um ativo financeiro intangível e valioso. Tal conceito recebeu o nome de *brand equity*⁴.

Detalha Cavalari (2020, *apud* GLITZ e GULARTE, 2018) como implementar um programa de *compliance*:

Para a implementação de um programa de integridade utilizam-se alguns elementos, tais como a: criação e informação de um código de conduta, que defina a postura ética empresarial, um canal de denúncias, que possibilite aos *stakeholders* denunciarem atos ilícitos, de forma anônima, e a contratação de um *compliance officer*, o profissional que será responsável pela informação e fiscalização no cumprimento do programa de integridade.

E conceitua Cavalari (2020, *apud* LAMBOY, 2017, p. 43) acerca do *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 empresa estar em *compliance*, consiste manter-se com seu programa de conformidade atualizado, apto as rotinas da organização, em consonância com a legislação vigente, em

³ Hoje em dia, o valor da marca passou a ser um componente importante do valor total da empresa. Isso pode ser constatado em diversas negociações feitas no mercado em que o patrimônio da marca eleva o preço de venda. E explica por que a Unilever pagou US\$ 930 milhões pela Kibon em outubro de 1997, valor quase três vezes superior às vendas dessa companhia no ano anterior. Por isso, são também considerados, na avaliação e na compra de empresas, os seus ativos intangíveis e todo o trabalho de construção de uma marca de sucesso na mente dos consumidores.” (SERRALVO, 2008, p. 19).

⁴ Definido como o ativo (ou o passivo) da marca ligado ao nome e ao símbolo de uma marca que se agrega a um produto ou serviço (ou deles se subtrai). Esses ativos podem ser agrupados em quatro dimensões: conscientização de marca, qualidade percebida, associações de marca e fidelidade à marca.” (AAKER; JOACHIMSTHALER, 2007, p. 28).

constante treinamento e fiscalização dos atos dos colaboradores, visando manter o respeito, a ética e a transparência com os *stakeholders*.

3.1 COMPLIANCE DIGITAL

A análise dos riscos e adoção de medidas preventivas visando a adequação das empresas às legislações aplicáveis às tecnologias da informação, segurança da informação e proteção de dados, torna-se a função essencial do *compliance* digital.

A empresa independente do seu porte, necessita após a implantação do *compliance* digital, ater-se a uma revisão periódica das políticas de controle e análises de riscos, por meio de uma fiscalização evolutiva e efetiva.

Ressalta-se que o *compliance* digital agrega a empresa um ambiente seguro e eficiente, resultando numa relação transparente e ética com os *stakeholders*.

Por certo que a legislação atual, auxilia a empresa no direcionamento da implantação do *compliance* digital, a fim de preservar os dados pessoais e sensíveis dos usuários, dentro de uma política de privacidade.

Observa-se que a normatização sobre proteção de dados surgiu após mais de três décadas de existência da rede mundial de computadores, e, mesmo a internet sendo regulamentada, estamos com vários movimentos tecnológicos a frente, os quais as normas não acompanham com a mesma velocidade, como exemplo, a chegada da WEB 3.0 e o ambiente do metaverso, algo que necessita de forma premente de inúmeras regulamentações no âmbito civilista, penal, tributário, e diversas outras áreas do direito.

Sem sombra de dúvidas, diante de uma lacuna normativa frente aos avanços tecnológicos, por certo que será o *compliance digital*, quem ditará o comportamento de uma empresa, não importa o seu porte, uma gama de conformidades, regras internas e externas capazes de dar diretrizes aos colaboradores nessa seara tecnológica, visando implantar a ética e transparência neste meio corporativo.

Não significa que uma empresa tornar-se-á investida do poder legiferante, apenas diante da ausência da norma, face as inúmeras inovações tecnológicas, pode-se avaliar como preservar os dados dos usuários, proteger sua privacidade, adotando medidas a serem inseridas no *compliance* digital, de tal modo que, possa mitigar os eventuais riscos, até que sobrevenha uma norma jurídica capaz de ditar as regras de conduta.

O *compliance* digital é primordial em uma empresa, na medida que está tornando-se costumeiro os casos de vazamento de dados de usuários por parte de grandes corporações, pois dá mais enfoque, mas com certeza não menos importantes empresas de médio e pequeno porte podem passar a enfrentar esse problema com a vigência da Lei Geral de Proteção de Dados.

A Secretaria Nacional do Consumidor (Senacon) órgão vinculado ao Ministério da Justiça e Segurança multou o Facebook no valor de R\$ 6,6 milhões em razão de vazamento de dados de usuários brasileiros. Segundo o Senacon no ano de 2018, os dados de 87 milhões de usuários em todo o mundo, incluindo 443 mil brasileiros, foram repassados à Cambridge Analytica, consultoria britânica de Marketing Político, contratada para a campanha eleitoral do ex-presidente dos Estados Unidos Donald Trump, e esse compartilhamento deu-se para o recebimento de conteúdos relacionados ao então político na época.

A investigação do Senacon concluiu no mesmo ano de 2018, que o compartilhamento ilegal dos dados dos brasileiros ocorreu por meio da instalação do ‘*This Is Your Digital Life*’, um aplicativo de teste de personalidade. Em razão de apresentar falhas ao informar os usuários sobre as configurações de privacidade, a Secretaria entendeu que o Facebook cometia prática abusiva.⁵

O caso Cambridge Analytica teve o mesmo destino nos Estados Unidos, onde a Comissão Federal de Comércio (FTC, na sigla em inglês), agência encarregada de proteger os consumidores, multou o Facebook no valor de 5 bilhões de dólares, valor considerado recorde no setor de tecnologia. (POZZI, 2019)

Essa autuação não foi a primeira, pois o Facebook celebrou em novembro de 2011, um acordo com as autoridades americanas envolvendo caso similar, admitindo que enganou os consumidores ao dizer que protegia suas informações quando, na verdade, ela as compartilhava sem informá-los.

Denota-se em ambos os casos, que os dados de usuários, os quais deveriam ser protegidos foram vazados, violando por completo a política de privacidade, por parte de uma empresa que tem o dever de resguardá-los.

Na mesma esteira a rede social Instagram foi compelida a pagar a título de multa, o valor de 405 milhões de euros, o equivalente a R\$ 2.101.950.000 (Dois bilhões, cento e um milhão, novecentos e cinquenta mil reais), devido a falhas no tratamento de dados pessoais de menores

⁵ Revista Exame. Disponível em: Instagram. Acesso em 25 ago 2022.

de idade. Essa decisão é considerada uma das mais duras aplicadas pela Comissão Irlandesa de Proteção de Dados (DPC) desde 2018, quando o Regulamento Geral sobre a Proteção de Dados (RGPD), concedeu mais poderes aos reguladores, a fim de proteger os consumidores da dominação do Facebook, Google, Apple e Twitter.

Neste caso o regulador que supervisora pela União Europeia a empresa Meta (empresa-mãe do Instagram e Facebook), havia aberto uma investigação no final de 2020, para determinar se a rede social havia colocado em ação barreiras necessárias visando proteger os dados dos usuários, principalmente no caso de menores, visto que é obrigatório ter no mínimo 13 anos para se abrir uma conta nesta rede social⁶.

Percebe-se que, todas as empresas independentes do porte ou atuação na sociedade, utilizará das inovações tecnológicas, isso é fato, e não tem mais retrocesso, de modo que, a velocidade e a quantidade exacerbada de dados, faz com que essas organizações se atentem a segurança da informação, ao tratamento destes dados em consonância aos ditames da legislação que regem essa matéria.

Com efeito, acredita-se que o *compliance digital* servirá tanto para casos em que já há uma regulamentação na legislação brasileira, como a Lei do Marco Civil da Internet, da Lei Geral de Proteção de Dados, até situações as quais a regulamentação não acompanhou as inovações tecnológicas, devendo a empresa procurar avaliar os possíveis riscos, visando mitigá-los, até que sobrevenha lei que regulamente a matéria.

4 REGULAMENTAÇÃO MARCO CIVIL DA INTERNET E LGPD

Com as inovações tecnológicas, sem olvidar os meios de comunicação nas empresas, torna-se imprescindível a adequação da privacidade on-line concomitante ao tratamento e proteção dos dados dos usuários, visto que, o compartilhamento de dados pessoais e informações sendo usados com o objetivo de causar prejuízo ao detentor destes ou a própria empresa, pode ocasionar danos de grande monta, e eis que o Brasil detém normas cujo objeto engloba a proteção dos dados pessoais e sensíveis, vulneráveis neste novo universo.

Essa tecnologia da informação e comunicação, impulsionando de maneira avassaladora a disseminação dos dados dos usuários, culminaria na proteção da privacidade, não obstante ser de outra área, mas coube ao direito tratar da regulamentação.

⁶ Revista Exame. Disponível em: Instagram. Acesso em 06 set 2022.

No contexto jurídico, embora há várias legislações esparsas disciplinando acerca dos dados pessoais e sua eventual proteção, mas foi com a Lei 12.965/2014⁷, denominada Lei do Marco Civil da Internet que pode-se considerar o nascedouro e principal documento legislativo, que regulamentou o direito digital, estabelecendo princípios, garantias e deveres no que tange ao uso da Internet no Brasil.

Cavalari (2020, *apud* SOUZA, LEMOS e BOTTINO, 2017. p. 19/20) contribui:

Sob tais premissas, importa referir o Marco Civil da Internet (MCI – 12.965/2014) pelo fato de ter como pilares fundamentais a neutralidade de rede, a liberdade de expressão e a proteção da privacidade.

O artigo 7 do MCI introduz princípios e obrigações relacionadas ao tratamento de dados pessoais na Internet, os quais incluem, por exemplo, o consentimento expresso do usuário para o tratamento de dados pessoais, bem como a possibilidade de titulares requererem a exclusão de seus dados pessoais fornecidos a provedor com o qual não mantém mais relação contratual.

Enquanto o Brasil iniciava seu processo de legislação, buscando preservar os dados pessoais diante ao acesso à tecnologia da informação e comunicação, não menos em outras partes do mundo, esse também era o cerne da preocupação e da busca pela regulamentação da privacidade, de tal sorte que idealizada em 2012, mas somente aprovada em 2016, a GDPR - *General Data Protection Regulation*, foi instituída com o intuito de regular a proteção dos dados dos cidadãos de países que fazem parte da União Europeia.

Andréa, Arquite e Camargo (2020) explica sobre a GDPR - *General Data Protection Regulation* agregando o seguinte conteúdo:

Trata-se de um regulamento geral no qual todas as empresas que exerçam algum tipo de atividade (remunerada ou não) em algum país da Europa devem possuir um tratamento especial no tocante aos dados dos seus usuários. Essa lei praticamente abrange o mundo inteiro, e, de fato, atinge uma parcela considerável das empresas internacionais, haja vista que a maioria delas presta algum tipo de serviço ou comercializa algum produto em, ao menos, algum lugar da Europa.

Já em suas primeiras considerações, o Parlamento Europeu e o Conselho da União Europeia, através da GDPR, definiram que a proteção dos dados pessoais seria um direito fundamental que está presente não apenas nessa legislação, mas na Carta dos Direitos Fundamentais da União Europeia (art. 8, n. 1) e no Tratado sobre o Funcionamento da União Europeia (art. 16, n. 1).

A GDPR trouxe uma grande influência para o nosso legislador pátrio em muitos dos artigos, como nas hipóteses nas quais os dados pessoais sensíveis poderão ser tratados pelo controlador de forma taxativa, ou seja, apenas dentro daquelas hipóteses descritas em lei é que poderão ser utilizadas. A principal e mais simples delas é mediante a autorização de forma específica e destacada do titular ou responsável legal pelos dados. Outras, também relevantes, poderão ocorrer mesmo sem o consentimento do seu titular, mediante cumprimento de obrigação legal, proteção à vida do titular ou terceiro, exercício regular de direitos, entre outros.

⁷ BRASIL. **Lei n. 12.965 de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 13 set 2022.

POLIDO *et al* (2018, p.4) acrescenta:

Sua abrangência, ambição legislativa e maturidade conceitual corroboram a ideia de que esse é um autêntico regulamento-modelo, no qual diversas outras iniciativas nacionais, regionais e intracomunitárias também serão espelhadas em busca de padrões normativos uniformes na proteção de dados pessoais. Não seria exagero afirmar que o GDPR nasce como “monstro normativo”, um Leviatã a induzir condutas de conformidade (*compliance*) por parte de agentes nas esferas pública e privada no campo da proteção de dados pessoais e especialmente identificáveis nos ambientes informacional e digital.

Por certo que, diante de uma economia globalizada, a proteção aos dados e a privacidade, fez com que o Brasil fosse compelido a adotar uma legislação própria assim como a União Europeia, sob pena de prejuízos imensuráveis, editando assim a Lei Federal nº 13.709/2018⁸ – Lei Geral de Proteção de Dados – LGPD, em vigor desde setembro de 2020.

Doravante, a partir do arcabouço de regramentos lançados pela GDPR quanto pela LGPD em que pese ao regulamento da responsabilidade pelo tratamento, uso, coleta, armazenamento e transferência dos dados dos usuários, pode-se extrair as condutas que devem ser adotadas pelas empresas, com vistas a estar de encontro e em conformidade com essas normas.

Ressalta-se que tanto o Marco Civil da Internet como a LGPD, buscam solucionar os problemas ocasionados pela internet, no tocante a proteção dos dados dos usuários sem contudo trazer transtornos a atividade econômica além do estritamente necessário, sem olvidar que auxiliam as corporações nas diretrizes para mitigarem seus riscos, prevenindo a incidência de atos ilícitos, passíveis de prejuízos financeiros de grande monta, sem contar a mancha na reputação da imagem da empresa, mácula que dependendo do episódio não tem como precificar ou apagar da memória e da sua história.

PAIVA e COSTA (2020, *apud* ABILIO, FRAZÃO e OLIVA, 2019, p. 681) contribui:

Um dos preceitos mais importantes inerentes à LGPD, é o de considerar a proteção dos dados pessoais da pessoa natural como um direito fundamental. Esse fato se justifica na medida em que todas as demais previsões dessa lei serão norteadas nesse sentido. Assim sendo, destaca-se como uma das principais características desse diploma legal o seu fomento preventivo, que estabelece procedimentos mandatórios para os controladores e operadores de dados pessoais, tais como os deveres atinentes à implementação de severas políticas de segurança afim de proteger esses dados de acessos não autorizados.

A tecnologia da informação e da comunicação, trouxe a demanda de se atentar aos direitos fundamentais a fim de proteger os dados pessoais por meio da Lei Geral de Proteção de Dados Pessoais, tendo em vista que os dados dos usuários são um dos mais importantes direitos

⁸ BRASIL. **Lei n. 13.709 de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm Acesso em: 13 set 2022.

inerentes à vida humana, pois trata da privacidade do indivíduo e que, se não tutelados, poderão acarretar inúmeros danos.

O principal fundamento presente na Lei Geral de Proteção de Dados é o respeito à privacidade do indivíduo, fundamento já cristalizado na forma da Constituição Federal, prescrito no artigo 5º, inciso X, inclusive na Declaração Universal dos Direitos Humanos (art. 12).

Cavalari (2020, *apud* BIONI, 2019. pag. 132) traz compreensão a norma:

Com efeito, verifica-se ao todo que os dispositivos fazem menção expressa à necessidade do consentimento do usuário para a coleta, uso, armazenamento e tratamento de seus dados pessoais, tal como para transferência a terceiros, sendo possível verificar a autodeterminação do cidadão para que ele, uma vez cientificado do respeito do fluxo de seus dados pessoais, possa controlá-lo por meio do consentimento. Essa ideia de controle atravessa desde a fase de coleta e compartilhamento dos dados com terceiros até o direito de deletá-los junto ao prestador de serviços e produtos de Internet ao término da relação.

Cavalari (2020, *apud* BLUM e MALDONADO, 2018. pag 25/26) acrescenta:

A Lei Geral de Proteção de Dados 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 a Lei Geral de Proteção de Dados, eis que surge a Autoridade Nacional de Proteção de Dados - ANPD, órgão responsável pela regulação e fiscalização da conduta das empresas frente a proteção da privacidade e dos dados dos usuários.

Polido (2022), posiciona que para o ano de 2022 deve-se esperar três grandes frentes para a ANPD no Brasil:

Sendo a primeira de expansão regulatória (com novas regulamentações, diretrizes e orientações), a segunda de atuação fiscalizatória e sancionatória pelo órgão e a terceira de cooperação reforçada com outras instituições no Brasil e exterior. Não diferentemente, a ANPD caminhará em suas iniciativas educativas e estratégicas na área de proteção de dados, mas também deve avançar na gradual instauração de processos administrativos para apuração de violação à Lei Geral de Proteção de Dados, com imposição de sanções e multas a empresas, espelhando-se na prática internacional.

No tocante a ANPD, podemos traçar mais uma ponderação de Polido (2022):

Importante aqui que sejam ponderados valores e objetivos relacionados às políticas de privacidade e governança de proteção de dados; a atuação regulatória deve encontrar estímulos para que a aplicação da LGPD não seja feita de modo refratário a

princípios de inovação e desenvolvimento de modelos de negócios entre agentes econômicos, particularmente rumo à expansão da economia digital.

Denota-se que, o Brasil não ficou para atrás, legislando com vistas a proteção dos dados dos usuários, tratando inclusive como um direito fundamental, concedendo amparo as pessoas diante da vulnerabilidade dos seus dados, mas ao mesmo tempo dando suporte as empresas, implantarem seus códigos de conduta e postura, a fim de estar em conformidade com a norma vigente frente as inovações tecnológicas, possibilitando não somente segurança, mas competitividade nesta economia globalizada.

CONCLUSÃO

A tecnologia tornou-se a extensão do homem, algo tão natural, que nenhum indivíduo atualmente consegue-se imaginar apartado deste meio tecnológico, e conceituando de forma simples, a tecnologia é tudo que não existindo na natureza, o ser humano inventa para expandir seus poderes, superar suas limitações físicas, tornar seu trabalho mais fácil e sua vida mais agradável. Considera-se a tecnologia como um processo que converte conhecimento sistemático (conceitual, empírico e/ou científico) em objetos úteis para apoiar as atividades humanas.

Da tecnologia, surgiram os meios digitais, que se compreende como qualquer mídia que pode utilizar-se de computadores, tablets, notebooks, smartwatch, enfim todo equipamento digital, utilizado pelo homem para criar, explorar, finalizar ou dar continuidade a um projeto que tem como suporte a internet, comunicação on-line ou off-line, produções gráficas, videogames, conteúdos audiovisuais etc.

As pessoas indistintamente estão ligadas as redes sociais, sites, informações financeiras, de trabalho, enfim uma gama de acessos, utilizando-se dos recursos da tecnologia, que por sua vez subsidiados pelos meios digitais.

E os acessos tão comum no cotidiano, faz com que as pessoas em simples cliques fechem negócios, agendem compromissos de lazer, trabalho, visitem sites, concedam aceites em termos de uso e condições de aplicativos sem ler o conteúdo, tudo de forma tão ligeira e automática, em busca de informações, afinal já somos a sociedade da hiper informação.

Assim, os dados das pessoas encontram-se lançados na rede mundial de computadores, livres, vulneráveis, de toda sorte, sem dar-se conta da dimensão do risco desta disponibilização,

pois não se pode mensurar efetivamente o que as empresas que capturam esses dados podem fazer, se compartilhar, vazar, ou mesmo serem vítimas de ciberataques.

Não obstante o *compliance* ser um ato de conformidade, no qual empresas empreendem esforços para compilar seu código de conduta e ética, impondo padrões internos para o cumprimento das normas vigentes, regulamentos internos e externos, formulação de diretrizes nacionais e internacionais, com intuito de prevenção de riscos, a fim de evitar prejuízos de ordem financeiro e danos à imagem, temos nesse movimento de inovações tecnológicas o *compliance* digital, a verdadeira adequação às legislações aplicáveis às tecnologias da informação, segurança da informação e proteção de dados.

Por certo que, os dados pessoais e sensíveis passaram a ganhar relevância, importância, preocupação, face a vulnerabilidade diante dos avanços tecnológicos, o que por um lado tornou-se uma benesse a todos, inclusive facilidades as empresas, meio de sobrevivência, estar atrelado a tecnologia gera competitividade, mas teve a intervenção do direito, que vindo a proteger a privacidade dos dados, edita normas próprias e contundentes a matéria.

Assim a Lei do Marco Civil da Internet e Lei Geral de Proteção de Dados, veio de encontro ao anseio da proteção dos dados dos usuários, que utilizando-se dos meios digitais, transitam a todo instante na internet, bem como, conceder uma diretriz as empresas de como atuar neste cenário tecnológico, auxiliando de sobremaneira a empresa que pretenda implantar seu *compliance* digital, visto que, há um norte a seguir, estar em conformidade com essa legislação, traz segurança, ética, transparência a empresa perante a sociedade.

Desta forma, é o *compliance* digital quem vai reger as diretrizes de uma empresa, em total respeito e conformidade com as normas em vigor (LMCI e LGPD), e ditando condutas a serem seguidas na corporação em razão de alguma lacuna normativa que se faça presente diante das novidades tecnológicas, buscando mitigar os riscos, preservar a imagem, o financeiro, e estabelecer uma sólida relação com a sociedade e os stakeholders.

REFERÊNCIAS:

AAKER, David A.; JOACHIMSTHALER, Erich. **COMO CONSTRUIR MARCAS LÍDERES**. 1. ed. Porto Alegre: Bookman, 2007.

AKABANE, Getulio K. e, POZO, Hamilton. **INOVAÇÃO, TECNOLOGIA E SUSTENTABILIDADE. HISTÓRICO, CONCEITOS E APLICAÇÕES**. São Paulo: Érica, 2020.

ANDRÉA, Gianfranco Faggin Mastro, ARQUITE, Higor Roberto Leite e CAMARGO, Juliana Moreira. **PROTEÇÃO DOS DADOS PESSOAIS COMO DIREITO FUNDAMENTAL: A EVOLUÇÃO DA TECNOLOGIA DA INFORMAÇÃO E A LEI GERAL DE PROTEÇÃO DE DADOS NO BRASIL. REVISTA DE DIREITO CONSTITUCIONAL E INTERNACIONAL.** vol. 121/2020 | p. 115 - 139 | Set - Out / 2020 | DTR\2020\11423. São Paulo: Ed. RT. Disponível em: <http://revistadostribunais.com.br/maf/app/document?stid=st-rql& marg=DTR-2020-11423>. Acesso em: 10 set 2022.

CAVALARI, Ana Paula França. **O COMPLIANCE DIGITAL COMO TECNOLOGIA DE GESTÃO.** In: Elas na advocacia. Porto Alegre: OAB/RS, 2020. p. 40-59. ISBN 978-65-0000-58-0.

MAGALHÃES JÚNIOR, Danilo Brum de. **GERENCIAMENTO DE RISCO, COMPLIANCE E GERAÇÃO DE VALOR: OS COMPLIANCE PROGRAMAS COMO FERRAMENTA PARA MITIGAÇÃO DE RISCOS REPUTACIONAIS NAS EMPRESAS.** Revista dos Tribunais | vol. 997/2018 | p. 575 - 594 | Nov / 2018 | DTR\2018\20828.

PAIVA, Mariza de Souza, e COSTA, Samara Silva. **COMPLIANCE DIGITAL E PROTEÇÃO DE DADOS: A LGPD E A RESPONSABILIDADE CIVIL DAS STARTUPS.** XI Congresso RECAJ-UFMG Inteligência Artificial, Startups, Lawtechs e Legal Techs, 2020. p.6-12.

POLIDO, Fabrício Bertini Pasquot. **DIREITO, TECNOLOGIA E INOVAÇÃO EM 2022: PRIMEIRAS IMPRESSÕES PARA O BRASIL.** Disponível em <https://www.conjur.com.br/2022-jan-17/fabricio-polido-direito-tecnologia-inovacao-2022>. Acesso em: 07 set 2022.

POLIDO, Fabrício B. Pasquot et al. **GDPR E SUAS REPERCUSSÕES NO DIREITO BRASILEIRO: PRIMEIRAS IMPRESSÕES DE ANÁLISE COMPARATIVA.** Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2018. Disponível em: <http://irisbh.com.br/wp-content/uploads/2018/06/GDPR-e-suas-repercussões-no-direito-brasileiro-Primeiras-impressões-de-análise-comparativa-PT.pdf>. Acesso em: 10 set 2022.

POZZI, Sandro. **EUA MULTAM FACEBOOK EM 5 BILHÕES DE DOLÁRES POR VIOLAR PRIVACIDADE DOS USUÁRIOS.** Data: 13 jul 2019. Disponível em

https://brasil.elpais.com/brasil/2019/07/12/economia/1562962870_283549.html.

Acesso em 09 set 2022.

TONIN, Alexandre Baraldi. **COMPLIANCE: UMA VISÃO DO COMPLIANCE COMO FORMA DE MITIGAÇÃO DE RESPONSABILIDADE**. Revista dos Tribunais | vol. 983/2017 | p. 265 - 288 | Set / 2017 | DTR\2017\5536.

SERRALVO, Francisco Antonio. **GESTÃO DE MARCAS NO CONTEXTO BRASILEIRO**. 1. ed. São Paulo: Saraiva, 2008.