MAYARA AVELAR SILVA

IMPLEMENTAÇÃO DE PROGRAMAS DE *COMPLIANCE* A PARTIR DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

LAVRAS - MG
2021

MAYARA AVELAR SILVA

IMPLEMENTAÇÃO DE PROGRAMAS DE *COMPLIANCE* A PARTIR DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Monografia apresentada à Universidade Federal de Lavras, como parte das exigências do Curso de Direito, para a obtenção do título de Bacharel.

Prof. Me. Sthéfano Bruno Santos Divino
Orientador

LAVRAS - MG
2021

RESUMO

A presente pesquisa versa sobre a Lei Geral de Proteção de Dados (Lei n.º 13.709/2018) e seus principais impactos no ambiente empresarial. Verifica-se o enorme desafio enfrentado pelas empresas diante da nova normativa, pois devem preocupar-se com garantir que suas atividades que envolvam o tratamento de dados estejam em consonância com as disposições da lei. O objetivo da pesquisa é identificar e analisar os principais mecanismos recomendados às empresas para se adequarem à Lei Geral de Proteção de Dados, pautando-se nos princípios da prevenção, segurança, responsabilidade e prestação de contas e nas regras de boas práticas e de governança nela previstos. Para tanto, utiliza-se os métodos indutivo e qualitativo, a partir da pesquisa documental, com a análise das disposições da normativa, e do levantamento bibliográfico, no qual se inclui doutrinas especializadas, artigos científicos e trabalhos acadêmicos. Ao fim, conclui-se pela necessidade de implementação de um programa de *compliance* pelas empresas que, para ser efetivo, deve ser baseado na observação de elementos mínimos, que envolvam o mapeamento dos dados, análise de riscos e a aplicação de mecanismos que atendam às especificidades da empresa. Verifica-se que, embora a tarefa de adequação apresente alguns desafios e custos, estes podem ser contrabalanceados com os benefícios decorrentes da atuação em conformidade com a LGPD.

Palavras-chave: Lei Geral de Proteção de Dados. Proteção de dados. Segurança. Prevenção. Boas práticas. Governança. *Compliance*.

ABSTRACT

This research is about the General Data Protection Law (Law No. 13.709 / 2018) and its main impacts on the business environment. There is an enormous challenge faced by companies owing to the new regulations, as they must be concerned with ensuring that their activities involving the processing of previous data in accordance with the provisions of the law. The objective of the research is to identify and analyze the main methods recommended to companies to comply with the General Data Protection Law, based on the principles of prevention, security, responsibility and accountability and on the rules of good practices and governance provide in it. For this purpose, inductive and qualitative methods are used, based on documentary research, with the provisions of the regulation's analysis, and the bibliographic survey, which includes specialized doctrines, scientific articles and academic works. In the end, the conclusion is that companies need to implement a compliance program that, to be effective, it must be based on the observation of elements which involve data mapping, risk analysis and the application of mechanisms that considers the company's specificities. It appears that, although the adaptation task has some challenges and costs, these can be balanced with the benefits arising from acting in accordance with the GDPL.

Keywords: General Data Protection Law. Data protection. Compliance. Security. Prevention. Good practices. Governance**.**

SUMÁRIO

1 INTRODUÇÃO

A sociedade contemporânea é reconhecidamente marcada pelo intangível processamento e circulação de dados pessoais, em razão dos constantes avanços tecnológicos que permitem a sua coleta e utilização para diversos fins. Não se pode olvidar que os dados têm constituído importante elemento econômico, na medida em que as empresas têm cada vez mais investido em mecanismos que viabilizem o seu tratamento a fim de impulsionarem o seu poder econômico.

É cediço que muitos são os riscos que surgem com a utilização desmedida de dados, o que vem sendo frequentemente demonstrado através da midiatização de irregularidades no seu tratamento por empresas públicas e privadas, dentre as quais se incluem desde a sua coleta irregular até sua exposição a terceiros, que podem ocasionar graves danos à esfera de direitos de seus titulares, sobretudo, à sua privacidade.

Diante deste cenário, a proteção de dados ganhou visibilidade no âmbito jurídico mundial, uma vez que se torna cada vez mais patente a sua devida regulamentação. Neste contexto, o Regulamento Geral sobre Proteção de Dados (UNIÃO EUROPEIA, 2016) surgiu como um relevante modelo a ser seguido por legislações de todo o mundo, oferecendo uma tutela específica aos dados pessoais de modo que atenda às necessidades atuais.

Nesse passo, no Brasil se deu origem à Lei Geral de Proteção de Dados (LGPD - Lei n.º 13.709/2018), que entrou em vigor em agosto de 2020 e trouxe consigo diversas modificações e inovações no cenário jurídico brasileiro a respeito da proteção de dados, considerando que, até então, não existia no país legislação específica sobre o tema.

O principal intuito da lei é assegurar a tutela efetiva de dados pessoais, estabelecendo regras e parâmetros a fim de que o seu tratamento ocorra mediante práticas seguras, que previnam potenciais riscos atinentes à violação dos direitos dos seus titulares. Portanto, as empresas que efetuem o tratamento de dados devem estar dispostas a adotarem uma série de mudanças e aprimoramentos no seu âmbito interno para se adequarem à nova normativa.

Assim, tendo em vista que o presente trabalho tem como objetivo identificar e analisar mecanismos que viabilizem a adequação à normativa, o que pode ser possível por meio da adoção de um programa de *compliance*, importante traçar o caminho perseguido até atingi-lo.

Primeiramente, cumpre esclarecer que os métodos utilizados são o indutivo e qualitativo por meio dos quais, aproveitando-se da pesquisa documental e do levantamento bibliográfico, procura-se analisar as disposições presentes na Lei Geral de Proteção de Dados (BRASIL, 2018), bem como considerações, argumentos e sugestões trazidos pelos principais autores que

se dedicam à temática, a fim de avaliar de que forma as empresas podem garantir a efetiva adequação à lei.

No primeiro capítulo, é abordada a relevância da coleta e tratamento de dados no âmbito empresarial, dada a importância econômica que representa neste contexto, demonstrando ainda quais são as principais finalidades para as quais as empresas os utilizam. Também são analisadas algumas técnicas de processamento de dados e suas principais implicações no que tange aos direitos dos indivíduos. Neste capítulo, também é demonstrado em que medida as empresas estão preparadas em relação à nova normativa bem como os desafios enfrentados para a sua adequação.

Em seguida, há a dedicação de uma análise mais objetiva da LGPD, através da explicação de sua origem, da delimitação do seu escopo de aplicação, além da descrição de alguns parâmetros introduzidos pela Lei, sobretudo, dos princípios que revelam o seu viés preventivo e das regras de boas práticas e da governança a serem implementadas pelas empresas.

Por fim, no terceiro capítulo, são tecidas as considerações sobre o conceito de *compliance*, sua importância e aplicação prática em face da Lei Geral de Proteção de Dados, além de serem considerados os principais incentivos à adoção do programa neste contexto.

Verifica-se que, para o programa de *compliance* seja efetivo, recomenda-se a adoção de uma série de medidas a serem tomadas que representam mudanças significativas no interior das empresas. Portanto, o processo de adequação à LGPD é uma tarefa que demanda empenho e apresenta custos e desafios, razão pela qual devem ser levados em consideração os benefícios decorrentes de uma atuação que atendam aos ditames da lei.

2 TRATAMENTO DE DADOS NO ÂMBITO EMPRESARIAL

A expansão da disponibilização e circulação de dados tornou-se a propulsora do que se pode denominar *economia digital*, em que o acesso às informações pode se dar de maneira quase ilimitada, de forma virtual e imediata (MOURA, 2019). Dessa forma que empresas e, principalmente, novos modelos de negócio têm se baseado na coleta de dados e informações no desempenho de suas atividades.

Assim, tem-se considerado os dados o *novo petróleo* (LEADERS, 2017) por se tratar de um grande ativo econômico. Como elucida Gropp e Motta (2020, p. 72):

> (...) é possível se utilizar o termo "novo petróleo" para referir-se aos dados de forma a compreender a magnitude do valor que estes apresentam, de forma que discute-se a mineração dos dados, nos aspectos técnicos, como a organização de camadas para capturas dos dados, processamento, análise; aspectos comerciais como a venda de dados, ações de marketing direcionadas através da modulação de comportamentos, em específico dos consumidores.

De acordo com pesquisa realizada por Marty Swant (2020), as marcas mais valiosas em 2020 estão relacionadas às empresas do setor tecnológico, como *Amazon*, *Apple*, *Google* e *Facebook,* as quais nutrem-se de dados e informações para oferecerem ao consumidor seu produto.

Embora muitas dessas empresas[1] forneçam os seus serviços sem exigir qualquer valor monetário em troca, é certo que não se trata de serviços gratuitos, vez que os usuários pagam com suas próprias informações privadas. Como afirma Silveira, Avelino e Souza (2016, p. 220), "gerado pelas identidades e comportamentos, pelos indivíduos e suas ações em redes digitais, os dados pessoais são a moeda paga pelo uso gratuito de plataformas, sites e serviços online. Dados pessoais se tornaram um importante bem econômico".

Empresas de diversos setores têm investido significativamente na formação de bancos de dados e no desenvolvimento de algoritmos e técnicas para ampliar as possibilidades do seu uso e gerar resultados, principalmente redes sociais, como o Facebook e o Instagram, e àquelas ligadas ao *e-commerce* (comércio eletrônico) que estão em exponencial expansão no mercado, a exemplo da *Amazon*, *Netshoes* e *Wallmart*.

[1] A título de exemplo, o *Facebook* disponibiliza gratuitamente o cadastro e acesso de seus usuários por tempo indeterminado, podendo ser realizadas publicações, divulgações, comentários sem a cobrança de nenhum valor, embora as informações disponibilizadas pelos usuários sejam de grande utilidade para a empresa, como será analisado.

A *Amazon*, reconhecida pelo seu serviço de *streaming* e comércio de eletrônicos, é uma das pioneiras no uso da tecnologia de mecanismos de recomendação a partir do uso de dados de seus consumidores. Dada a quantidade de informações e produtos com que os consumidores se deparam ao acessarem o comércio digital, a Amazon introduziu o sistema de 360 graus, visando sanar a dificuldade de identificarem o que melhor atende às suas necessidades e desejos (MARR, 2016, p. 288-289)

Assim, a empresa recorre à uma filtragem colaborativa, por meio da qual identifica o que o consumidor deseja com base não apenas nos seus próprios registros pesquisa, de compra e avaliação dos produtos, mas também mediante o que as pessoas com perfis similares compraram.

O *Facebook*, por sua vez, é uma das redes sociais mais utilizadas no mundo todo que, acordo com Vitório (2021), fechou o ano de 2020 com 2,8 bilhões de usuários. Portanto, detém um gigantesco banco de dados com informações específicas sobre seus usuários, como o local onde moram, trabalham, estudam, quem são seus familiares e amigos e quais são seus interesses em relação a livros, filmes e outros produtos, seja através de informações diretamente fornecidas pelo usuário ou por meio de suas curtidas em publicações e páginas.

Tanto grandes empresas quanto empresas menores que não dispõem de acesso a grande quantidade de dados e recursos suficientes para desenvolvimento de marketing recorrem à plataforma do *Facebook* para anunciarem seus produtos, a qual os direciona para potenciais consumidores com base na análise dos dados de seus usuários.

Além do compartilhamento de mensagens, publicações de conteúdo e anúncios, o Facebook também possui uma ferramenta de execução de softwares:

> Mais de meio milhão de aplicativos foram criados para o Facebook até agora, muitos dos quais aproveitam o acesso que tem, por meio de APIs extensas (interfaces de programas de aplicativos), aos dados de usuários do Facebook. Esses aplicativos, por sua vez, reúnem dados sobre como são usados para que seus desenvolvedores utilizem para direcionar anúncios para seus próprios clientes (MARR, 2016, p. 71)[2].

O *Facebook Analytics*, como é chamado o mecanismo desenvolvido para este fim, funciona como uma ferramenta para análise de dados, fornecendo relatórios, dados

[2] Tradução livre. Do original: "*Over half a million apps have been created for Facebook so far, most of which take the advantage of access they have, via the extensive APIs (application program interfaces), to Facebook user data. These apps in turn gather data about how they are used that their developers use to target ads at their own customers*."

demográficos e segmentos relacionados aos seus usuários às empresas que a utilizam, proporcionando-lhes um direcionamento para seu negócio e seu marketing.

Assim é que muitos modelos de negócios têm sido desenvolvidos sob o prisma central do processamento de dados, de forma que dificilmente interagimos com o ambiente tecnológico mantendo informações privadas *intocáveis.* Nos dizeres de Mendes (2019, p. 1):

> Do ponto de vista do indivíduo, o conceito de "ubiquidade no processamento de dados" (ubiquitous computing; Mattern, 2008) parece ser ainda mais significativo ao indicar como todos os âmbitos da vida estão marcados pelo tratamento de dados pessoais. Isso se dá em razão dos inúmeros equipamentos eletrônicos que fazem parte do nosso dia a dia e que armazenam todo tipo de informação pessoal de maneira ininterrupta.

A este contexto convém remeter o que Bioni chama de *economia da vigilância* (2018, p. 42). Como aduz o autor (BIONI, 2018, p. 42), "é a observação permanente do comportamento dos indivíduos que a movimenta, sendo as suas informações pessoais a matéria-prima a ser explorada para a geração de riqueza. Mais do que isso, há um 'varejo dos dados pessoais'".

Assim, a economia digital trouxe às empresas a possibilidade de exploração da mina de riqueza da sociedade tecnológica, os dados pessoais, tornando sua campanha publicitária mais eficiente e seus negócios ainda mais lucrativos com a adoção de métodos cada vez mais especializados que atendam aos seus interesses.

Ocorre que a utilização dos dados em larga escala surtiu efeitos não só econômicos, também causando impacto sobre a esfera de direitos dos titulares, na medida em que as empresas se apropriam de técnicas que nem sempre são utilizadas com o consentimento, transparência, finalidade e segurança devidos.

2.1 Técnicas de processamento de dados e suas implicações

Para a análise das técnicas desenvolvidas e utilizadas pelas empresas para a coleta e processamento de dados e das consequências delas advindas, é importante compreender como a intensificação do fluxo de dados acarretou no meio sociológico o denominado *informacionismo*, que "trata das informações dos indivíduos (dados pessoais) e informações gerais e bem como a forma como tais elementos são retratados e manuseados no mundo prático" (SANTOS, 2019, p. 18).

Com o desenvolvimento tecnológico, ampliou-se a capacidade de armazenamento e comunicação de informações. Conforme Doneda (2006, p. 172), houve uma mudança qualitativa nos dados devido ao surgimento de novos métodos, algoritmos e técnicas utilizados

com este objetivo. Para o autor (DONEDA, 2006, p. 12), com o aumento do fluxo informacional há "uma capacidade técnica cada vez maior de recolher, processar e utilizar a informação".

A partir disso, tornou-se possível a existência do fenômeno conhecido como *Big Data*, um "conceito ligado à velocidade de processamento de dados em crescimento exponencial, que permitiu que de um grande número multivariado de dados, fosse possível extrair informações com excelência e velocidade" (SANTOS, 2019, p. 21).

A definição do *Big Data* geralmente é extraída com base em cinco características intrínsecas concebidas como "os cinco V's do *Big Data*", a saber: volume, velocidade, variedade, valor e veracidade.

> O volume diz respeito ao tamanho e quantidade de dados gerados; a velocidade trata da dinâmica de crescimento e processamento de dados, ou seja, refere-se à rapidez com que os dados são gerados e distribuídos; a variedade diz respeito à diversidade de origens, formas e formatos dos dados; o valor é o significado que pode ser atribuído ao dado por meio da sua análise; e a veracidade se refere à autenticidade, reputação da origem, confiabilidade dos dados (PEREIRA, 2015 apud FELINI; SARAIVA NETO, 2018, p. 4)

No *Big data*, as informações são encontradas em seu estado bruto, sendo a utilização destes dados potencializada por meio da sua conexão com um determinado contexto, oportunidade em que passa a produzir novos significados. Tudo isto é possível com o auxílio das técnicas de processamento, filtragem e organização das informações extraídas.

Neste contexto, muito tem-se adotado a técnica de *profiling*, ou perfilização, relacionada à construção de perfis utilizada pelas empresas em diversas circunstâncias e com diferentes objetivos, sendo assim elucidada por Doneda (2006, p. 173):

> Nela, os dados pessoais são tratados, com o auxílio de métodos estatísticos, técnicas de inteligência artificial e outras mais, com o fim de obter uma "metainformação", que consistiria numa síntese de hábitos, preferências pessoais e outros registros da vida dessa pessoa. O resultado pode ser utilizado para traçar um quadro das tendências de futuras decisões, comportamentos e destinos de uma pessoa ou grupo.

O *profiling* não possui definição específica na legislação brasileira, no entanto, Zanatta (2019, p. 7) defende que a Lei Geral de proteção de Dados (LGDP) permite a inferência a um *certo conceito interpretativo*, referindo-se à perfilização como um "processo automatizado de tratamento de dados que objetiva a análise e predição de comportamentos pessoais, profissionais, de consumo e de crédito".

Este mecanismo permite a coleta e refinamento de dados e informações que as empresam têm utilizado para o oferecimento de uma maior diversidade de produtos e serviços,

por meio de uma maior conexão com as necessidades e interesses dos seus consumidores, o que propicia uma amenização dos riscos da atividade econômica.

Aproveitando-se desta técnica, as empresas tendem a utilizar cada vez mais a chamada publicidade comportamental, em que a partir da coleta e união de informações a respeito dos consumidores é possível traçar um perfil e direcioná-los a produtos e serviços que se enquadrem em seus interesses, como fazem a *Amazon* e o *Facebook* (MARR, 2016), conforme já demonstrado.

> (...) a publicidade dirigida, comportamental ou online behavior advertising (...) é realizada através de monitoramento das atividades online e dos dados pessoais dos usuários com a finalidade de compreender um possível futuro consumidor, tornando os anúncios dirigidos e mais relevantes no ambiente virtual (TATEOKI, 2017, p. 71)

Embora se trate de um importante instrumento para as empresas impulsionarem o sucesso das suas atividades, a perfilização pode representar um grande risco à esfera de direitos dos titulares de dados. A criação de um perfil para o consumidor pode significar um mal na medida em que tende a criar uma previsão do comportamento e de decisões de uma pessoa ou grupo baseando-se em seus registros. Tal situação se traduz no cerceamento da liberdade de escolha do indivíduo a partir do que pode ser considerado uma manipulação da sua vontade, o que, na maioria das vezes, ocorre sem que o consumidor tenha ciência disso.

> A partir do momento em que um perfil eletrônico é a única parte da personalidade de uma pessoa visível a outrem, as técnicas de previsão de padrões de comportamento podem levar a uma diminuição de sua esfera de liberdade, visto que entes com os quais ela se relaciona levam em consideração o pressuposto de que ela adotará um comportamento pré-definido de acordo com seu determinado perfil aliado a técnicas preditivas de seu comportamento, o que tem como consequência uma efetiva diminuição de sua liberdade de escolha (DONEDA, 2016, p. 174).

Para Mendes (2014, p. 111), a técnica de *profiling* viabiliza a tomada de decisões relacionadas a consumidores, trabalhadores e cidadãos no geral, exercendo influência sobre o seu acesso a oportunidades sociais. Nesse sentido, afirma que:

> (...) os riscos da técnica de construção de perfis não residem apenas na sua grande capacidade de junção de dados; na realidade, a ameaça consiste exatamente na sua enorme capacidade de combinar diversos dados de forma inteligente, formando novos elementos informativos (MENDES, 2014, p. 111).

Tendo em vista que a ideia da perfilização é a segmentação de dados, baseada na criação de padrões de comportamento e na classificação do indivíduo a partir de seus dados, essa prática

pode levar a uma discriminação com a privação de determinados indivíduos do acesso a bens e a serviços.

Dessa forma, considerando o intenso fluxo de dados representado pelo *Big Data* e a adoção de práticas como o *profiling*¸ revela-se a necessidade da discussão acerca das questões atinentes aos direitos e interesses dos titulares, que envolvem a obtenção do seu consentimento para a coleta e tratamento de dados, a transparência em relação à finalidade para a qual está sendo coletado, entre outros fatores que deveriam ser considerados em toda e qualquer operação realizada com os dados. Verifica-se a imaturidade de muitas empresas em relação a este assunto, de modo que sua irregularidade só vem a ser reconhecida após a ocorrência de danos aos titulares dos dados.

2.2 Estudo de casos: por uma demonstração fática da irregularidade da coleta e tratamento de dados

Com a larga expansão da utilização de dados e informações e de mecanismos por meio dos quais são coletados e processados, é patente que também se expandiram os riscos, que podem ser observados desde e coleta ou acesso sem a autorização do titular, nas técnicas que envolvem seu processamento, como no *profiling*, até sua utilização com finalidades indevidas e armazenamento inseguro, que permite a ocorrência de vazamentos e exposição indevida. Por tais razões que são frequentemente noticiados casos que demonstram irregularidades no tratamento de dados, especialmente por grandes empresas.

Em 2018, Cadewalladr e Graham-Harrison (2018) anunciaram que a Cambridge Analytica, empresa britânica especializada em mineração e análise da dados, coletava dados pessoais de usuários do Facebook sem sua autorização por meio da sua participação em testes de personalidade. Segundo a denúncia, os dados eram utilizados para criação de um perfilamento que lhes direcionasse notícias falsas e anúncios de cunho político personalizado, a fim de influenciar no referendo em relação à saída do Reino Unido da União Europeia, o Brexit[3] e nas eleições presidenciais dos Estados Unidos que resultaram na vitória de Donald Trump.

Além de uma negação à liberdade de escolha, o caso foi interpretado como uma própria violação à democracia, na medida em que era apresentada aos eleitores a projeção de um

[3] No deslinde do caso, Cambridge Analityca se considerou culpada ao se recusar a prestar informações sobre dados de um usuário britânico e sobre como tinha obtido as informações sobre ele (PRESSE, 2018).

candidato moldado, de forma que "(...) em um cenário de manipulação do eleitor por propaganda eleitoral direcionada a grupos ou perfis pré-selecionados, a qualidade do voto, como expressão do exercício da cidadania, é severamente prejudicada" (MARTINS, TATEOKI, 2019, p. 145).

Somado à questão do caso representar a violação ao consentimento dos titulares em relação à coleta de seus dados, também se verifica a desmedida proporção com que estes elementos são utilizados para finalidades diversas daquelas para os quais os titulares os disponibilizam, bem como o notável prejuízo acarretado pelo seu uso indevido.

No entanto, a problemática da irregularidade no tratamento de dados não se resume a estas questões. Também carece de análise em que medida as empresas estão preparadas para garantir uma segurança efetiva aos dados a partir do momento em que os detém, com a proteção de sua exposição a terceiros.

Nesse interim, tem-se o caso do Banco Inter que foi acusado, em Ação Civil Pública (DISTRITO FEDERAL, 2018), pelo vazamento de dados pessoais de milhares de clientes, funcionários e executivos[4]. De acordo com as investigações, foi constatado o comprometimento dos dados de mais de 19 mil correntistas, dos quais 13.207 se incluíam dados bancários, como número da conta, senha, endereço, CPF e telefone (DISTRITO FEDERAL, 2018).

Segundo argumento utilizado pelo Ministério Público do Distrito Federal e Territórios (DISTRITO FEDERAL, 2018), autor da ação, por se tratar do primeiro banco 100% digital, que utiliza "tecnologias móveis que permitem aos seus usuários um controle rápido e "seguro" das contas, deveria oferecer um grau de segurança além daquele oferecido pelos bancos tradicionais, considerando a própria natureza de suas atividades".

Acidentes como este têm sido recorrentes no Brasil[5] e representam enorme prejuízos financeiros para as empresas, tanto pelos gastos com a reparação dos danos, quanto pela perda de credibilidade, custos estes que podem ser muito superiores aos que poderiam ser dispendidos com adoção de políticas e mecanismos de proteção de dados.

Para além dessa questão, não se pode olvidar o impacto negativo que o vazamento de dados reflete sobre os seus titulares, ao representar uma violação à sua privacidade. A

[4] O Banco Inter admitiu o vazamento, pois teria identificado um incidente de segurança em seu sistema, tendo alguns dados sido acessados e divulgados. O banco fechou um acordo com o MPDFT, se comprometendo a pagar 1,5 milhão de reais a título de indenização (REDAÇÃO, 2018).

[5] No início de 2021, houve o vazamento de dados de mais de 223 milhões de pessoas, dentre os quais se incluía o número do CPF, renda, benefícios do INSS, entre outros que, de acordo o hacker responsável, teriam sido provenientes das operadoras Claro e Vivo. No entanto, as empresas negaram a ocorrência de vazamento em seus sistemas e o caso ainda está sendo investigado (CORACCINI, 2021).

privacidade à que se refere não é aquela compreendida apenas como um direito de manter dados e informações da sua vida privada em sigilo (WARREN; BRANDEIS, 1890), mas como direito inerente à personalidade humana, com intuito de proteger a própria pessoa titular.

Assim, é inegável o relevo que a temática assume na discussão jurídica atual, tendo em vista a necessidade de se oferecer uma tutela específica e eficaz, voltada para a proteção de dados no âmbito de sua utilização por empresas brasileiras e estrangeiras.

Por essa razão, no Brasil, deu-se origem à Lei Geral de Proteção de Dados, considerada um marco preponderante à temática na medida em que representa um papel positivo tanto para consumidores, quanto para empresas, uma vez que pretende oferecer segurança aos dados pessoais e minimizar riscos e prejuízos para ambos.

2.3 O despreparo das empresas na adequação à LGPD

Até o surgimento da Lei Geral de Proteção de Dados (Lei n.º 13.709/2018) a questão da privacidade e a matéria atinente a proteção de dados e informações era regida por leis esparsas, como o Marco Civil da Internet (BRASIL, 2014), Código de Defesa do Consumidor (BRASIL, 1990) e a Lei de Acesso à Informação (BRASIL, 2011). Dessa forma, a nova normativa vem suprir a carência de uma legislação unificada que ofereça regulamentação específica ao tratamento de dados e informações pessoais no Brasil.

A LGPD (BRASIL, 2018) foi publicada em 14 de agosto de 2018 e entrou em vigor em 1º de agosto de 2020, embora as penalidades pelo desrespeito às suas disposições só serão aplicadas a partir de agosto de 2021.

O cenário pandêmico gerou uma situação de incerteza quanto ao início de vigência da lei. Em junho de 2020, a data foi redefinida para maio de 2021 pelo art. 4º da Medida Provisória n.º 959 e, em agosto, foi alterada para dezembro de 2020 (BRASIL, 2020). No entanto, em 18 de setembro, a Medida Provisória foi aprovada com a decretação da prejudicialidade do referido dispositivo, sendo declarada, portanto, a vigência imediata da Lei, retroagindo à data original, ou seja, 1º de agosto de 2020. Assim, empresas acabaram perdendo seu foco na adequação, por vislumbrarem o então adiamento da vigência.

Pesquisas realizadas pela Serasa Experian (2020) avaliaram a jornada de amadurecimento e adequação das empresas brasileiras à LGPD entre os anos de 2019 e 2020. O primeiro estudo foi realizado em fevereiro e março de 2019 com 508 empresas entrevistadas em todo o país e, o segundo, em março e abril de 2020, com 513 empresas.

Os dados apontaram que, em 2019, 66% das empresas consideravam ter níveis mediano e alto de conhecimento sobre a LGPD e 65% avaliaram estar preparadas, índices que subiram para 71% e 73%, respectivamente, em 2020 (SERASA EXPERIAN, 2020). Dentre o total de empresas entrevistadas, o ramo tecnológico foi o que mais se destacou pelo alto nível de conhecimento e preparação, representando 91% e 93% (SERASA EXPERIAN, 2020).

Já em pesquisa realizada pelo ICTS Protiviti, publicada no mês de março de 2020, evidenciou-se que 84% de 192 empresas analisadas ainda não haviam se adequado às exigências da nova normativa. A pesquisa foi realizada com empresas de diversos setores, desde o varejo e agropecuária aos setores de saúde e educação, entre micro, médias e grandes empresas.

Conforme depreende-se do levantamento realizado, nota-se a carência de foco na implantação de medidas eficientes para segurança de dados e na prevenção de risco, verificando-se que apenas 13,5% das empresas entrevistadas possuíam mapeamento de risco de segurança da informação e proteção de dados e plano formal de mitigação, além de que somente 17,7% possuíam gestão sobre o tratamento de dados pessoais por terceiros (ICTS PROTIVITI, 2020).

A pesquisa apontou ainda que o porte da empresa exerce grande influência sobre o seu nível de adequação, demonstrando que, no geral, as grandes empresas estavam mais preparadas, ainda que em baixo nível, do que as micro e pequenas empresas. Esta disparidade pode ser evidenciada ao serem analisados os quesitos de adequação à normativa considerados na pesquisa, restando demonstrado que, no que tange a existência de programa de segurança informacional, por exemplo, 65,7% das empresas de grande porte entrevistadas estariam adequadas, contra 24,6% das micro e pequenas empresas (ICTS POTIVITI, 2020).

Um novo levantamento foi realizado pela ICTS Protiviti (apud CILURZO, 2020) entre abril e setembro de 2020, no qual contou com a participação de 296 empresas, das quais 82% ainda se encontravam em atraso com as ações de adequação, havendo, portanto, um aumento pequeno no percentual de preparação das empresas à nova normativa.

Portanto, é possível vislumbrar uma modesta melhora neste cenário nos últimos dois anos, embora os números representem que ainda há um grande número de empresas que estão despreparadas, sobretudo, micro e pequenas empresas, que não possuem uma cultura de implementação de programas e políticas de proteção de dados.

O fato é que a transformações repentinas em decorrência do Covid-19, tais como as medidas de isolamento, mudanças nos modelos de negócios e no hábito dos consumidores além

de prejudicar o processo de adequação das empresas, ressaltaram ainda mais a necessidade de medidas que propiciem a proteção de dados, tendo em vista a intensificação da sua circulação.

O crescimento do uso da tecnologia por empresas e trabalhadores, dada a adequação de muitas empresas ao *home office* com a aderência de soluções de trabalho e comunicação, aumentou a demanda por videoconferências, acesso a banco de dados em nuvem, recursos de rede e, consequentemente, a potencialidade da violação de dados.

Além dessa questão, houve o aumento da demanda dos consumidores por compras online em razão do isolamento social, o que veio acompanhado de um crescimento significativo no número de golpes no comércio eletrônico. Pesquisas da ClearSale (apud BUSSOLA, 2021) demonstraram que as tentativas de fraude cresceram 83,7% no primeiro trimestre de 2021 em comparação com o mesmo período do ano anterior, batendo 601 mil casos. Este tipo de situação se torna possível muitas vezes pela ausência de mecanismos de segurança que garantam a proteção de dados, que, consequentemente, terminam por vir a conhecimento de terceiros e utilizados indevidamente.

Assim, é perceptível a imaturidade de muitas empresas em matéria de dados, o que vem a ser uma questão preocupante não somente em razão da urgente necessidade da adequação formal à LGPD (BRASIL, 2018), que já se encontra em vigor, como também em virtude dos possíveis riscos advindos do tratamento de dados sem a sua devida proteção.

Embora a pandemia tenha desviado o foco das empresas desta questão, o fato é que o assunto jamais esteve em tamanha demanda como no cenário atual, o que requer das empresas o empenho necessário para adequação à nova normativa, tendo-se em vista que a lei não representa apenas um ônus à atividade empresarial, mas sim, um norte para à minimização de riscos envolvendo dados pessoais.

Dessa forma, uma vez realizada esta análise introdutória a fim de demonstrar os reflexos da coleta e da utilização de dados pessoais pelas empresas e as irregularidades evidenciadas no seu tratamento, passa-se ao estudo da Lei Geral de Proteção de Dados (BRASIL, 2018) que, inspirada no Regulamento Geral sobre Proteção de Dados (RGPD) estruturado pela União Europeia (2016), objetiva unificar a matéria de proteção de dados pessoais no Brasil, estabelecendo parâmetros para que as empresas atuem com a devida segurança, a fim de prevenir infortúnios decorrentes do irregular tratamento de dados.

3 DADOS PESSOAIS SOB A ÉGIDE DA LGPD

A Lei Geral de Proteção de Dados surgiu em um momento em que o ordenamento jurídico brasileiro se viu compelido à criação de um diploma normativo que tratasse com maior abrangência e profundidade a questão dos dados pessoais, em alinhamento aos padrões internacionais, tendo em vista a publicação do Regulamento Geral sobre Proteção de Dados (RGPD) pela comunidade europeia, em 2016, e a repercussão mundial do escândalo da *Cambrige Analytica.*

Sucedendo a Diretiva 95/46/CE (UNIÃO EUROPEIA, 1995), relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, o RGPD foi elaborado com a pretensão de proteger os dados pessoais de forma que pudesse atender às necessidades atuais, em meio ao contexto de virtualização das relações pessoais e comerciais, "servindo como uma lei com poder coercitivo e um escopo muito mais abrangente que incorpora em seu texto noções modernas sobre captação e circulação de dados para cidadãos europeus que usem a Internet" (BEZERRA, 2019, p. 30).

Como leciona Pinheiro (2020, p. 18), o regulamento europeu ocasionou um *efeito dominó*, ao exigir que os países e empresas que mantivessem relações comerciais com a União Europeia tenham uma legislação no mesmo nível que o RGPD (UNIÃO EUROPEIA, 2016), sob pena de sofrer algum tipo de barreira econômica ou dificuldade de fazer negócios com os países do bloco. Ainda que alguma empresa não europeia não se encaixe diretamente aos elementos que ensejam a incidência do regulamento, para estabelecer relações comerciais com empresas submetidas ao RGPD é necessário que também esteja em conformidade com este.

Assim se impulsionou a criação da Lei Geral de Proteção de Dados (BRASIL, 2018) no Brasil, que teve como inspiração a normativa europeia, trazendo diversos conceitos, princípios e mecanismos de proteção, padronizando e unificando o tratamento da matéria e objetivando oferecer uma tutela mais efetiva aos dados pessoais e seus titulares.

Uma vez compreendida a origem da LGPD (BRASIL, 2018) no contexto mundial, cumpre esclarecer o seu âmbito de incidência, que se revela em grande amplitude haja vista não estabelecer limites territoriais para sua aplicação. No mais, a LGPD (BRASIL, 2018) traz alguns princípios que revelam o seu intuito de fomentar a evitar e mitigar riscos provenientes do tratamento de dados, o que pode se concretizar através da adoção de boas práticas e de governança pelas empresas.

3.1 Âmbito de aplicação da LGPD

O escopo de proteção da Lei Geral de Proteção de Dados (BRASIL, 2018) recai sobre os dados de pessoas físicas, incidindo sobre todos aqueles que realizem o tratamento dos seus dados pessoais, sejam pessoas físicas ou pessoas jurídicas de direito público ou privado, independentemente do meio que utilizem. O objeto da normativa é evidenciado com clareza logo no primeiro dispositivo, que assim estabelece:

> Art. 1º. Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Logo, a lei não tem como objeto de proteção os dados de pessoas jurídicas, sendo estas apenas sujeito ativo no tratamento de dados, estando sujeitas às regras e sanções previstas na legislação.

Ao tratar do âmbito territorial de incidência da lei no art. 3º, *caput* (LGPD, BRASIL, 2018), percebe-se o seu caráter de extraterritorialidade, por ultrapassar os limites fronteiriços do país ao não se levar em consideração a nacionalidade dos envolvidos para a sua aplicação.

A lei preconiza que deve ser observada a existência de pelo menos uma das três hipóteses nela previstas, quais sejam: que o tratamento dos dados seja realizado no território brasileiro (art. 3º, inciso I); que a atividade de tratamento tenha por objetivo a oferta que o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional (art. 3º, inciso II), ou; que os dados tenham sido coletados em território nacional (art. 3º, inciso III).

Portanto, a LGPD (BRASIL, 2018) não se limita apenas às pessoas que estejam domiciliadas ou estabelecidas no Brasil, tendo efeito sobre qualquer pessoa que tenha seus dados no país tratados. Também não está circunscrita apenas às empresas brasileiras, podendo ser aplicada à toda empresa, nacional ou estrangeira, que realize a coleta ou o tratamento de dados em território nacional.

Assim, uma vez compreendido o escopo de aplicação da LGPD, faz-se necessário analisar uma série de princípios norteadores ao tratamento de dados trazidos pela lei, dos quais é possível extrair a percepção de um viés preventivo da normativa, uma vez que pretende oferecer uma assistência à figura do consentimento que, se não estiver acompanhado de outros mecanismos, se revela ineficaz à devida proteção de dados.

3.2 Para além do consentimento: o dever de prevenção, segurança e prestação de contas no tratamento de dados

É cediço que o consentimento desempenha um papel central no âmbito das operações que envolvem dados pessoais, sendo tratado, por vezes, como elemento legitimador à realização de seu tratamento. Nesse sentido, definindo o consentimento como "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento[6] de seus dados pessoais para uma finalidade determinada" (art. 5º, inciso XII), a LGPD o trata como uma das hipóteses autorizativas ao tratamento de dados, inclusive de dados pessoais sensíveis (art. 7º, inciso I e art. 11, inciso I).

Ocorre que, em diversas situações, o consentimento se mostra insuficiente para garantir a autonomia do indivíduo no exercício do seu poder decisório sobre o uso dos seus dados pessoais. Exemplo paradigmático neste contexto é a adoção das políticas de privacidade, instrumento utilizado pelas empresas no ambiente virtual para obter o consentimento dos usuários para o uso de seus dados, sobre o qual Bioni (2018, p. 162) se assim posiciona:

> Em meio a esse descompasso, o próprio mercado se autorregulou. O surgimento das políticas de privacidade é uma resposta a essa demanda regulatória. Por meio de tal técnica contratual, colher-se-ia o prescrito e necessário consentimento para legitimar toda e qualquer operação de tratamento dos dados pessoais.
> Ocorre que tal mecanismo tem se mostrado falho por inúmeras razões, seja porque ele reforça a aventada assimetria do mercado informacional, seja porque se trata de uma ferramenta que não capacita, efetivamente, o cidadão para exercer controle sobre as suas informações pessoais.

Devido à sua insuficiência se considerado de maneira isolada, reconhece-se a relevância de diversos instrumentos trazidos pela LGPD (BRASIL, 2018) que auxiliam na validação e eficácia do consentimento. Neste contexto, os princípios gerais estabelecidos pela normativa cumprem papel de suma importância, devendo ser observados em toda e qualquer situação que envolva o tratamento de dados pessoais, sendo eles: finalidade; adequação; necessidade; livre acesso; qualidade dos dados; transparência; segurança; prevenção; não discriminação; responsabilização e prestação de contas, previstos no art. 6º, incisos I ao X da LGPD (BRASIL, 2018).

---

[6] Art. 5º. [..]. X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração" (LGPD, 2018).

A observância aos princípios é preponderante ainda que a figura do consentimento não seja fator autorizativo para o tratamento dos dados, como na eventual dispensa do consentimento, na qual inclui-se a hipótese do tratamento de dados tornados manifestadamente públicos pelo titular (art. 7º, §4º), o que não desobriga os agentes de tratamento das obrigações previstas na lei, especialmente no que concerne aos princípios gerais nela previstos (art. 7º, §6º).

Todavia, assumem relevância neste cenário, os princípios da segurança, da prevenção e da responsabilização e prestação de contas, previsto no art. 6º, incisos VII, VII e X, respectivamente, uma vez que oferecem parâmetros aos agentes de tratamento[7] na proteção dos dados pessoais a adotarem instrumentalidades técnicas capazes de tornar o consentimento do titular mais eficaz.

O princípio da segurança refere-se à "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais dos acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão", nos termos do art. 6º, inciso VII da LGPD (BRASIL, 2018). Em outras palavras:

> (...) o princípio da segurança impõe a quem efetue o tratamento de dados pessoais eventual responsabilidade por procedimentos, meios e tecnologias que garantam a proteção dos dados pessoais de acessos por terceiros, tais como, por exemplo, as decorrentes de invasões por hackers (FLUMIGNAN; FLUMGINAN, 2020, p. 133).

A importância deste princípio pode ainda ser evidenciada tendo em vista a dedicação pela lei de uma seção exclusiva ao tratamento da segurança e sigilo dos dados, assim dispondo:

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (LGPD, BRASIL, 2018).

Ressalta-se que as referidas medidas deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução (art. 46, §2º), portanto, a obrigação não se restringe

[7] A LGPD (BRASIL, 2018) considera como agentes de tratamento o controlador e o operador (Art. 5º, inciso IX). O controlador é a "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais" (art. 5º, inciso VI) e o operador é a "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador" (art. 5º, inciso VII).

ao setor de tecnologia de informação da empresa, se estendendo por todo o período em que os dados estão sob a guarida do agente de tratamento.

Inegavelmente, o princípio da segurança está intimamente relacionado ao princípio da prevenção, definido pelo art. 6º, inciso VIII da LGPD (BRASIL, 2018) como a "adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais". Assim, a partir da adoção de mecanismos de segurança capazes de impedir acessos não autorizados a dados pessoais e sua utilização indevida, previne-se a ocorrência de danos aos titulares decorrentes do tratamento de seus dados.

Além da observância destes princípios, a lei exige a comprovação da sua eficácia em atendimento ao princípio da responsabilização e prestação de contas, que o art. 6º, inciso X da LGPD (BRASIL, 2018) define como a "demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas".

Em decorrência deste princípio, Moraes e Queiroz (2019, p. 130) admitem a existência de uma "responsabilidade proativa" ou "responsabilidade ativa" na LGPD (BRASIL, 2018), ao unir a responsabilização à prestação de contas, uma vez que não será suficiente o mero cumprimento dos artigos da Lei. Neste sentido:

> (...) Exige-se, em síntese, atitudes conscientes, diligentes e proativas por parte das empresas em relação à utilização dos dados pessoais. Assim, a partir de agosto de 2020, quando entra em vigor a LGPD, qualquer empresa que processe dados pessoais, terá não apenas que cumprir a lei, mas também terá que provar que está em conformidade com a Lei. Caberá às empresas, em vez de à Administração Pública, a responsabilidade de identificar os próprios riscos e escolher e aplicar as medidas apropriadas para mitigá-los (MORAES; QUEIROZ, 2019, p. 130).

À luz destes princípios, percebe-se a importância da adoção de uma postura preventiva e proativa que garanta segurança pelas empresas, através de medidas eficazes de proteção de dados que sejam capazes de suprir a ineficiência da figura do consentimento. Percebe-se que a própria lei se incumbiu de estabelecer normas norteadoras ao atendimento concreto destes princípios, recomendando, para tanto, a adoção de boas práticas e da governança.

3.3 Das Boas Práticas e da Governança

Com o objetivo de estimular a proatividade dos agentes de tratamento de dados a adotarem uma cultura organizacional protetiva aos dados pessoais, a lei lhes faculta a criação

de regras de boas práticas e de governança, referentes a mecanismos internos e externos de controle que sejam capazes de assegurar a segurança aos dados. Como esclarece Carvalho, Mattiuzzo e Ponce (2021, p. 371):

> Ainda que mecanismos sancionatórios sejam essenciais para que se garanta a efetividade de uma política pública, na medida em que o objetivo central da política é sempre gerar cumprimento e adequação comportamental, e não mera punição, a prevenção e a orientação são peças-chave do sistema que se pretende construir.

A implementação de mecanismos de segurança deve partir das boas práticas da governança corporativa que, de acordo com o Instituto Brasileiro de Governança Corporativa (2015, p. 20), é definida como:

> (...) o sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas.

Nesse sentido, a LGPD (BRASIL, 2018) dispõe que:

> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

A Lei (BRASIL, 2018) é clara ao prezar pelos princípios da segurança e da prevenção, nos termos do art. 50, §2º, em que dispõe que, na sua aplicação, o controlador deverá considerar "a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados", recomendando a implementação de um programa de governança em privacidade (art. 50, §2º, inciso I) que, no mínimo,

> a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
> b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;

> c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
> d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
> e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
> f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
> g) conte com planos de resposta a incidentes e remediação; e
> h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas (art. 50, §2º, I).

A LGPD (BRASIL, 2018) ainda recomenda que seja demonstrada a efetividade do programa de governança "em especial, a pedido da autoridade nacional[8] ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei" (art. 51, §2º, inciso II).

Portanto, os agentes de tratamento de dados devem refletir sobre seus sistemas de governança a adoção de mecanismos adequados a proteção de dados, assegurando que sejam eficazes e que atendam aos requisitos mínimos estabelecidos pela LGPD, bem como a fim de garantir que a empresa atue em conformidade com a legislação em sua totalidade.

Dessa forma, como demonstrado, a LGPD confere uma abordagem didática e orientadora ao tratamento de dados pessoais, pautada em princípios que visam a mitigação de riscos e estabelecendo parâmetros para a sua concretização, a partir da recomendação da adoção de boas práticas e da governança em relação à proteção de dados. Dessa forma, os programas de *compliance* revelam-se essenciais à implementação das práticas às quais lei se refere, cumprindo demonstrar como o programa pode ser aplicado à proteção de dados.

[8] Art. 5º. [...] XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional (LGPD, 2018).

4 IMPLEMENTAÇÃO DE PROGRAMAS DE *COMPLIANCE* À PROTEÇÃO DE DADOS

Como já observado, a lei faculta aos agentes de tratamento a implementação de regras de boas práticas e de governança no âmbito da corporação a fim de garantir segurança durante a realização do tratamento de dados. Revela-se crucial que as empresas pensem em meios de adequação à LGPD (BRASIL, 2018), estruturando programas de *compliance* que envolva o desenvolvimento de mecanismos ou melhoria daqueles já existentes para a proteção de dados

De início, faz-se mister mencionar, que, seja qual for seu escopo de aplicação, o *compliance* não possui um modelo único que possa ser efetivo em todas as empresas. No entanto, é possível moldar o programa às necessidades de cada pessoa jurídica, a partir de requisitos mínimos.

Portanto, cumpre esclarecer os elementos delineadores do *compliance* para o melhor entendimento do que vem a ser este programa, bem como os requisitos essenciais à sua efetividade a serem observados durante a sua estruturação e funcionamento, sobretudo quando aplicado à proteção de dados.

4.1 O conceito de *compliance* e os requisitos para sua efetividade

Para a análise de como o programa de *compliance* pode ser aplicado à proteção de dados, é fundamental compreender o seu significado, suas funções e aplicações práticas, uma vez que assume papel fundamental no direcionamento dos agentes de tratamento em relação a sua atuação a fim de atender aos preceitos estabelecidos pela LGPD (BRASIL, 2018).

Nas palavras de Simonsen (2018, p. 105):

> O termo *compliance* já é, por si só, explicativo, pois vem do verbo *to comply*, que significa agir e estar em conformidade com uma requisição ou regra. Dessa forma, estar em *compliance* significa que a empresa atua alinhada ao seu arcabouço normativo e regulatório.

O Conselho Administrativo de Defesa Econômica (CADE 2016, p. 09) oferece uma definição mais completa do termo, referindo-se ao *compliance* como “um conjunto de medidas internas que permite prevenir ou minimizar os riscos de violação às leis decorrentes de atividade praticada por um agente econômico e de qualquer um de seus sócios ou colaboradores”.

A ideia central do *compliance* é que funcione como um manual interno de conduta que discipline as atividades empresariais, implementando rotinas e práticas para prevenção de riscos

que possam ensejar a responsabilização empresarial em razão do descumprimento de obrigações legais.

De maneira mais geral, consoante elucida Cueva (2018, p. 54),

> (...) pode-se entender o compliance não apenas como a observância de comandos legais e regulatórios, mas também como o cumprimento de outras exigências, tais como normas éticas, padrões de conduta fixados no seio das organizações e expectativas dos *stakeholders*.

De acordo com Cueva (2018, p. 57), uma das funções da adoção de programas de *compliance* seria a de proteger a empresa, isto é, de "evitar infrações de regras por meio de medidas organizacionais preventivas". Desse modo, a responsabilidade dos membros da administração das empresas não se limitaria apenas ao dever de evitar infrações, mas compreende também o dever de evitar que seus subordinados cometam infrações (CUEVA, 2018, p. 59).

Salienta-se mais uma vez que não existe uma fórmula única de *compliance*, pois este deve se adequar às peculiaridades de cada empresa e requer que sejam permanentemente analisados os riscos e as normas jurídicas aplicáveis. No entanto, faz-se mister a observância de elementos mínimos a fim de estruturar programas de *compliance* efetivos uma vez que se for "um programa de fachada, que não preencha os requisitos mínimos ou que os preencha apenas formalmente, pode de fato resultar em penalidades maiores do que aquelas que seriam aplicáveis em sua ausência" (CUEVA, 2018, p. 61).

O CADE (2016, p. 15-16) elucida que existem alguns pontos comuns a programas considerados robustos, isto é, existem características que são sempre aplicadas de alguma forma a programas de *compliance* efetivos, embora possam não ser incorporadas sempre da mesma maneira. Trata-se de requisitos mínimos essenciais para a garantia da efetividade do programa e aplicáveis a qualquer corporação, consideradas as especificidades de cada uma.

O primeiro desses requisitos é o comprometimento que, segundo o CADE (2016, p. 16), na prática, concretiza-se por meio do envolvimento da alta direção, de recursos adequados e autonomia e independência do gestor do programa.

É cediço que a atuação dos membros do alto escalão de uma empresa constitui o exemplo de gestão e ética que reflete sobre o comportamento de seus funcionários, razão pela qual o seu comprometimento é um importante fator para a efetividade do programa, uma vez que se revela crucial para a implementação do *compliance* na cultura empresarial.

Neste sentido, segundo Frazão, Oliva e Abilio (2018, p. 690), a garantia do êxito do programa requer que "os administradores da sociedade tornem inequívoco, mediante adoção de

atos concretos, que a organização está empenhada na observância das leis e normas internas, conferindo-lhe papel primordial – inclusive em confronto com as metas empresariais".

Os atos concretos que revelam o envolvimento da alta direção se traduzem, por exemplo, na alocação de recursos que sejam capazes de garantir a efetividade do programa, os quais podem ser representados pela disponibilização de profissionais qualificados e treinados para o seu monitoramento.

Em complemento, faz-se necessária a independência dos responsáveis pela gestão dos programas, a fim de que sejam capazes de exercer influência sobre as decisões da organização.

> (...) deve-se assegurar ao setor autonomia e independência para implementar as políticas, procedimentos e controles adequados, o que inclui acesso aos recursos necessários para o desempenho dessa atividade e a possibilidade de tomar decisões sem que seja necessário consultar outras áreas (FRAZÃO; OLIVA; ABILIO, 2018, p. 690).

O segundo requisito de um programa de *compliance* efetivo refere-se à análise de riscos, pautado na ideia de que "programas bem estruturados são normalmente precedidos e acompanhados da realização de uma análise aprofundada dos riscos aos quais a entidade está exposta em suas atividades" (CADE, 2016, p. 19).

Deve-se considerar que os riscos variam de acordo com a atividade, o porte, complexidade, entre outras características da empresa, o que reforça a ideia de não ser possível a constituição de um modelo único de *compliance*, sendo necessária a sua personalização de acordo com os riscos específicos de cada organização. Salienta-se que o intuito é "tentar antecipar as principais áreas de exposição da pessoa jurídica para que sejam tomadas medidas preventivas proporcionais aos riscos identificados" (FRAZÃO; OLIVA; ABILIO, 2018, p. 690).

Uma vez identificados os riscos da empresa, toma importância o terceiro requisito: a sua mitigação. Cabe a empresa estudar e implementar os mecanismos necessários e mais eficientes de acordo com os riscos evidenciados.

Ganha relevância neste contexto a elaboração de Códigos de Ética e de Conduta, "documentos escritos que consubstanciam os valores e princípios da entidade, a serem observados por todos (inclusive terceiros), bem como orienta quais as condutas são aceitas e quais são vedadas" (FRAZÃO; OLIVA; ABILIO, 2018, p. 689). Esses instrumentos são o cerne da implementação do *compliance*, pois é através deles que são constituídas as regras que regularão as atividades internas da empresa.

Nesse ínterim, a realização de treinamentos com os colaboradores da empresa é de grande valia para que tenham conhecimento a respeito dos objetivos e regras do programa, compreendam a sua importância, além de ter a oportunidade de esclarecer suas dúvidas sobre os procedimentos (CADE, 2016, p. 21).

Por último, e não menos importante, tem-se a revisão do programa, ou seja, uma vez implementado, é necessário que o programa de *compliance* passe por constante monitoramento, a fim de identificar a necessidade de readaptações e atualizações, tendo em vista o dinamismo da atividade empresarial, mudanças legislativas e outros fatores que, se não forem acompanhados, podem comprometer a efetividade do programa.

No caso do *compliance* à proteção de dados, é interessante observar que a própria LGPD (BRASIL, 2018) estabelece parâmetros para os agentes de tratamento desenvolvam seus programas de conformidade, como infere-se do art. 50, § 2º, ao apontar os elementos mínimos a serem observados pelo programa de governança em privacidade, os quais estão intimamente relacionados aos requisitos gerais do *compliance.*

Portanto, cumpre esclarecer, em linhas gerais, qual o caminho a ser percorrido pela empresa para implementar um programa de *compliance* efetivo, sob a ótica dos requisitos gerais e daqueles estabelecidos pela própria lei, de modo que garanta a efetiva proteção aos dados pessoais em atendimento aos ditames da LGPD (BRASIL, 2018).

4.2 Aplicação do *compliance* à proteção de dados

De início, a instauração do programa de *compliance* com foco sobre a LGPD demanda a realização do mapeamento de todas os processos, sistemas e atividades da empresa que envolvam o tratamento de dados pessoais a fim de que seja avaliada a existência e o nível de potenciais riscos.

Para que haja uma identificação inequívoca destes riscos, deve-se antes analisar:

> (I) em que momentos há a utilização de dados pessoais; (II) que dados são esses; (III) como e por quem esses dados foram coletados; (IV) como a utilização desses dados se relaciona com a atividade desenvolvida; (V) o que ocorre com esses dados uma vez que ingressam e, por fim, (VI) se e como saem do controle da organização (FRAZÃO; OLIVA; ABILIO, 2018, p. 700).

Desse modo, será possível ter um controle do ciclo de vida dos dados que perpassam pela empresa e, então, analisar se o seu tratamento está em consonância com os ditames da

LGPD (BRASIL, 2018), sobretudo com o art. 7º[9], que dispõe sobre as hipóteses em que o tratamento de dados poderá ser realizado.

Salienta-se que é dever do controlador e do operador manter registros sobre as operações de tratamento de dados pessoais que realizarem, consoante dispõe o art. 37 da LGPD (BRASIL, 2018)[10], o que viabiliza, em grande medida, o maior conhecimento e controle sobre os dados que estão sendo tratados pela empresa.

Uma vez realizado este mapeamento dos dados, será possível identificar qual o nível dos riscos envolvidos de acordo com as características dos dados identificados.

> A matriz de risco deverá ter em conta: se o dado pessoal é de uma categoria especial (considerando, por exemplo, a categoria de dados sensíveis da própria LGPD), as finalidades do tratamento, a existência de prazo de retenção legal de dados, eventual risco que o tratamento representa para os direitos e liberdades fundamentais do titular, bem como medidas de segurança ou minimização de riscos já adotadas (CARVALHO; MATTIUZZO; PONCE, 2020, p. 377).

No caso dos dados pessoais sensíveis, percebe-se a regulação mais restritiva que a lei lhes confere, autorizando a sua utilização apenas nas hipóteses previstas no art. 11[11], o que

---

[9]Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular; II - para o cumprimento de obrigação legal ou regulatória pelo controlador; III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro; VIII - para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente; (BRASIL, 2018).

[10] Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse (BRASIL, 2018).

[11] Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em

justifica a necessidade da adoção de condutas mais rígidas para a mitigação de riscos, que se revelam em maior potencial em comparação aos dados pessoais não sensíveis.

Frazão, Oliva e Abílio (2018, p. 701) asseveram:

> Outro importante risco que deve ser abordado no programa de *compliance* consiste em garantir que o sistema de tratamento permitirá o pleno exercício dos direitos dos titulares. Ou seja, deve-se investigar se os dados são acessíveis pelos titulares, se a tecnologia empregada permite o efetivo apagamento, se é possível identificar a totalidade dos dados de uma mesma pessoa tratados dentro da entidade.

Sendo assim, faz-se necessário esclarecer se o tratamento dos dados está em consonância com os direitos dos titulares, sobretudo, com o seu direito à informação e ao controle sobre seus dados, em atendimento aos ditames do art. 18 da LGPD (BRASIL, 2018).

Como bem aponta Nunes (2019, p. 55):

> (...) antes do advento da LGPD, os dados coletados pela empresa, a partir do momento que configuravam em sua base de dados, ficavam sob sua posse indefinidamente, sendo utilizados para diversas funções que não a que originou a coleta, sem o menor conhecimento de seu titular.

Assim, a partir da lógica da nova normativa, a empresa controladora deverá manter sob sua posse somente aqueles dados que possuam o devido embasamento legal. Neste contexto, cumpre observar as situações em que deverá ser cessado o tratamento dos dados previstas na LGPD, dentre as quais se incluem a "verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada" (art. 15, I) e o "fim do período de tratamento" (art. 15, II). Constatada uma destas hipóteses, é certo que o ideal é que a empresa promova a eliminação dos dados em questão.[12]

Durante as fases de mapeamento dos dados e avaliação dos riscos, revela-se crucial a elaboração do Relatório de Impacto pelo controlador, documento este que poderá ser solicitado

---

processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (...) (BRASIL, 2018).

[12] Art. 5º. XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado (BRASIL, 2018);

pela Autoridade Nacional de Proteção de Dados (ANPD)[13] a qualquer momento (art. 38, caput, LGPD). De acordo com a normativa (BRASIL, 2018):

> Art. 38
> [...]
> Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

O Relatório de Impacto ainda cumpre o papel de facilitar o controle sobre a atuação da empresa no que tange ao tratamento de dados, podendo ser consultado a qualquer momento, uma vez que nele devem constar todas as informações relativas aos dados tratados.

A partir do diagnóstico dos dados e da identificação dos riscos, faz-se necessário avaliar as medidas que podem ser adotadas pela empresa para tornar possível que os dados identificados e os riscos evidenciados recebam a devida atenção.

4.3 Elementos de um programa de *compliance* à proteção de dados

A análise realizada viabiliza uma visão ampla a respeito da melhor conduta a ser adotada pela empresa a fim de promover a segurança dos dados com a prevenção e mitigação dos riscos, ou seja, torna-se possível o concreto atendimento à LGPD (BRASIL, 2018).

De acordo com Frazão, Oliva e Abílio (2018, p. 706), é elemento fundamental para a robustez do programa de *compliance* que a sua organização seja compatível com o risco da atividade, o que consiste em "assegurar que a estrutura corporativa será capaz de cumprir as determinações legais (...) mediante a adoção de procedimentos especificamente desenhados para as hipóteses de tratamento".

Portanto, caberá ao controlador adotar os mecanismos que sejam adaptados às características das operações realizadas, às particularidades dos dados e aos impactos e riscos à privacidade evidenciados (art. 50, §2º, II e III, LGPD), personalizando o programa de *compliance* às necessidades e especificidades da empresa.

4.3.1 Código de Conduta

[13] Art. 5°. XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional (BRASIL, 2018);

A implementação do *compliance* à LGPD requer a elaboração e adequação de documentos internos aos princípios atinentes ao tratamento de dados. Nesta seara, ganha destaque o Código de Conduta como elemento capaz de orientar as atividades internas da empresa, revelando-se indispensável na medida em que sua funcionalidade é inerente à essência do conceito de *compliance.*

Quanto ao conteúdo deste documento, Frazão, Oliva e Abílio (2018, 703) explicam que:

> (...) deve explicitar quais dados podem ser coletados ou tratados, em quais hipóteses e para que finalidades. Impõe-se que preveja pormenorizada e concretamente os comportamentos que devem ser adotados para cada hipótese de tratamento, ressaltando passo a passo os procedimentos a serem realizados.

Assim, o Código de Conduta cumpre o papel de estabelecer especificadamente as principais orientações quanto aos procedimentos a serem adotados internamente a fim de assegurar o correto tratamento de dados à luz das normas que regem a matéria.

Além do mais,

> Podem contar também com as instruções gerais e valores que devem guiar os funcionários e a alta administração nas decisões que envolvam o tratamento de dados pessoais, a incorporar condutas que traduzam sua política de privacidade (FRAZÃO; OLIVA; ABÍLIO, 2018, p. 702).

No entanto, não basta a criação de um documento com linguagem técnica de difícil compreensão, o que viria a ser um óbice à sua efetiva implementação.

> (...) é necessário que o documento seja de fácil acesso a todos os colaboradores internos e externos da organização e tenha linguagem clara – ou seja, que o conteúdo seja compreensível não apenas para um especialista no tema, mas para qualquer pessoa que queira e precise entender o funcionamento dos mecanismos (CARVALHO; MATTIUZZO; PONCE, 2021, p. 379).

Dessa forma, o Código de Conduta se porta como um instrumento capaz de dar as orientações indispensáveis aos funcionários da empresa, para que sempre atuem em conformidade com as regras estabelecidas pela LGPD (BRASIL, 2018).

Nessa seara, é importante a indicação de um responsável por garantir que as regras introduzidas sejam bem compreendidas e cumpridas pelos funcionários, razões pelas quais a LGPD traz a figura do encarregado.

4.3.2 A figura do encarregado

Uma das previsões evidenciadas na LGPD (BRASIL, 2018) é que o controlador indique o encarregado pelo tratamento de dados (Art. 41, *caput*) que se refere à "pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados", consoante prevê o art. 5º, inciso VII, da lei (BRASIL, 2018).

Segundo Redecker e Ballico (2020, p. 145):

> (...) pode ser pessoa natural ou jurídica, operando como canal de comunicação entre o titular dos dados, o controlador e os órgãos competentes (como a autoridade nacional), além de possuir a função de lidar com qualquer informação ou fato relacionado ao tratamento de dados.

De acordo com Pinheiro (2018, p. 119), a designação de um encarregado "busca garantir que as informações fiquem centralizadas e que o controlador se certifique de que a aplicação das normas receberá efetiva validação".

A figura do encarregado na legislação brasileira se assemelha ao *Data Officer Protection* (DPO) estabelecido pelo GDPR (UNIÃO EUROPEIA, 2016), embora ao contrário da normativa europeia, a LGPD não disponha sobre qualquer requisito de formação necessário ao exercício desta função.[14]Todavia, segundo Pinheiro (2018, p. 120):

> A experiência tem mostrado que as habilidades necessárias para execução de todas as atividades do Encarregado (DPO) são híbridas, ou seja, exigem tanto conhecimento da própria legislação como também sobre atendimento e relacionamento com titulares (que podem ter dois tipos de perfis principais: o de consumidor final e o de funcionário, em que os canais de diálogos normalmente são atendidos ou por uma Ouvidoria ou SAC ou então por um RH ou Canal de Denúncias). Além disso, também deve ter conhecimentos técnicos, especialmente de ciber segurança e se possível de governança de dados.

Este conhecimento multidisciplinar do encarregado é exigível na medida em que a lei estabelece várias funções a serem por este exercidas. Dentre suas atribuições, o encarregado será responsável pelo recebimento de reclamações e comunicações dos titulares, prestando os devidos esclarecimentos e adotando providências, além de receber as comunicações da ANPD adotando também as providências, consoante art. 41, § 2º, incisos I e II da LGPD (BRASIL, 2018).

[14] Art. 37. Nº 5. O encarregado da proteção de dados é designado com base nas suas qualidades profissionais e, em especial, nos seus conhecimentos especializados no domínio do direito e das práticas de proteção de dados [...] (UNIÃO EUROPEIA, 2016).

Ademais, cumpre ao encarregado a orientação dos funcionários e contratados em relação às regras do programa de *compliance* à proteção de dados, bem como executar outras atribuições determinadas pelo controlador ou estabelecidas em normas complementares nos termos do art. 41, § 2º, incisos III e IV (BRASIL, 2018).

A orientação efetuada pelo encarregado, que se traduz na oferta de treinamentos, por exemplo, é de suma importância principalmente quando direcionada aos funcionários da empresa que trabalham com tecnologia da informação, pois devem ter conhecimento acerca dos requisitos de segurança previstos na lei (art. 46), e sobre "a necessidade de aprimoramento constante dos sistemas diante de falhas ocorridas interna ou externamente" (FRAZÃO; OLIVA; ABILIO, 2018, p. 709).

Ressalta-se que a existência da figura de um encarregado nem sempre é obrigatória, podendo ser eventualmente dispensada a sua necessidade pela ANPD, a depender da natureza e porte da entidade ou do volume de operações de tratamento de dados, conforme preconiza o art. 41, §3º (BRASIL, 2018). Assim, é certo que no caso de micro e pequenas empresas que não lidam com grande volume de operações de dados, não será exigida a indicação de um encarregado.

No entanto, as pessoas jurídicas devem compreender a importância deste instrumento para a construção de práticas de *compliance* à LGPD na medida em que:

> (...) representará a implementação de *canal de comunicação*, tanto *interno*, para fins de esclarecimentos sobre as condutas a serem adotadas no caso concreto, como *externo*, isto é, direcionado ao titular do dado, concentrando as requisições por ele realizadas, analisando a pertinência dos pedidos, instruindo os funcionários sobre como proceder, bem como garantindo o respeito aos ritos e prazos previstos na LGPD organização (FRAZÃO; OLIVA; ABILIO, 2018, p. 708).

Assim, embora incumba aos controladores e operadores a formulação de regras de boas práticas e de governança (art. 50, caput, LGPD, 2018), será de responsabilidade do encarregado difundir os processos e práticas na organização, garantindo que o programa de *compliance* seja efetivamente implantado, razão pela qual deve haver certa independência e autonomia no exercício das suas funções.

No mais, uma vez tecidas as principais considerações a respeito do responsável por conduzir as atividades relacionadas à implementação do programa de *compliance*¸ resta compreender a importância da tecnologia nesta seara, à luz do conceito do *privacy by design*, de extremo valor no âmbito da proteção de dados.

4.3.3 *Privacy by design*

Se, por um lado, a tecnologia pode viabilizar a violação à privacidade do indivíduo por meio do acesso aos seus dados, por outro lado, pode ser uma importante aliada no desenvolvimento de mecanismos para um bom *compliance* à proteção de dados.

De acordo com os ensinamentos de Mendes e Fonseca (2020, p. 520), da mesma forma que o Direito não consegue garantir que o ambiente virtual seja favorável aos dados pessoais, também a tecnologia não é capaz de sozinha proteger os indivíduos de violações aos seus direitos fundamentais. Por essa razão, deve-se reconhecer a importância de alinhá-los, a fim de "estruturar parâmetros regulatórios e institucionais compatíveis com os valores ético-sociais e os preceitos jurídicos de determinada sociedade" (MENDES; FONSECA, 2020, p. 520).

No contexto da proteção de dados, relevante é a figura da metodologia conhecida como *privacy by design* (ou privacidade desde a concepção), que pode ser assim compreendida:

> O seu conceito fundamental implica que as organizações devem sempre criar produtos e serviços, que, desde o início, estejam de acordo com as diretrizes de um sistema de gestão de *compliance* digital ou de dados, bem como das melhores práticas de *Compliance* de dados e que essas medidas sejam aplicadas diretamente nas tecnologias, nos sistemas e nas práticas vinculadas a todo o ciclo de vida dos produtos e serviços das organizações e empresas (SAAVEDRA, 2021, p. 738).

Assim, o *privacy by design* é concebido como uma estratégia para a adoção de mecanismos tecnológicos com o intuito de garantir a efetiva proteção aos dados dos indivíduos durante toda o ciclo de vida dos produtos ou serviços ofertados, desde a sua concepção até o seu destino final. O seu fundamento é encontrado no art. 46, §2º da LGPD (BRASIL, 2018), que dispõe que as medidas de segurança, técnicas e administrativas de proteção de dados deverão ser observadas desde a concepção do produto ou serviço até a sua execução.

A importância deste conceito é corroborada por Frazão, Oliva e Abílio (2018, p. 708), ao afirmarem:

> Daí a necessidade de que os programas de *compliance* de dados não se limitem apenas à previsão de princípios ou regras de comportamento, mas visem também à adoção de tecnologias que possam ser compatíveis com a eficácia de tais regras. É essa uma das principais preocupações decorrentes da ideia de *privacy by design*, em que a escolha da tecnologia utilizada na oferta de produtos e serviços é pensada, desde o início, para a proteção dos dados pessoais.

Consoante leciona Bioni (2020, p.167), faz parte desta metodologia a adoção da *Privacy Enhancing Technologies*/PETs, que em seu sentido literal, "é capaz de abarcar toda e qualquer tecnologia que seja amigável e facilitadora à privacidade". Neste sentido, é importante a adoção de tecnologias de segurança essenciais à tutela da privacidade, do início ao fim do tratamento dos dados.

> Os padrões de segurança aplicados devem garantir a confidencialidade, integridade e disponibilidade dos dados pessoais durante todo o seu ciclo de tratamento, incluindo, entre outros, métodos de destruição segura, criptografia apropriada, e métodos fortes de controle de acesso e registro (BRASIL, 2020, p. 52)

O *privacy by design* revela-se um importante alicerce da figura do consentimento e da realização da vontade do titular na medida em que:

> Trata-se de estimular a incorporação da ideia de *autodeterminação informativa* nos sistemas, códigos, arquiteturas e procedimentos tecnológicos: aplicar o direito fundamental à proteção de dados na concepção e na aplicação das tecnologias que permeiam os serviços e produtos disponíveis aos usuários. É que, em ordem de se alcançar um consentimento material e efetivo, antes é preciso preencher diversas condições tecnológicas para tanto. Em especial, ao máximo quanto tecnologicamente possível, (I) aumentar a confiança dos indivíduos no sistema utilizado e no tratamento de dados realizado, assegurando que ambos serão livres e adequados, longe de manipulações, interceptações ou acessos indevidos, bem como (II) permitir que o titular dos dados possa configurar e determinar suas preferências acerca do que é feito com os desdobramentos virtuais de sua personalidade (MENDES; FONSECA, 2021, p. 103).

Nesta seara, relevante é a atuação da alta administração para a introdução, desenvolvimento e manutenção da cultura do *privacy by design*, tornando viável, por meio da disponibilização dos recursos necessários, a implementação destes mecanismos tecnológicos em todos os setores da empresa.

Empregando-se o *privacy by design*, com a adoção dos mecanismos tecnológicos aptos a proteger efetivamente os dados das pessoas que se relacionem com a empresa, é possível comprovar o seu comprometimento com a adequação à LGPD. Importante notar que a lei traz alguns aspectos positivos em relação àqueles que demonstram estar em conformidade com suas disposições

4.4 Estímulos à adoção de *compliance* à LGPD

Conforme demonstrado, a implementação de um efetivo programa de *compliance* possui inúmeros desafios, que abrangem a mudança da cultura organizacional, alocação de recursos, contratação de profissionais especializados, treinamentos, além da colaboração dos diversos setores da empresa. Assim sendo, é certo que o tempo, energia e custos dispendidos são significativos, no entanto, há que se considerar que:

> Ao lado dos chamados custos de manutenção, contudo, há também os custos decorrentes da não conformidade. Ao contrário dos primeiros, nos quais se incluem os custos para executar e promover a política de *compliance*, (...) o segundo refere-se aos custos decorrentes da não observância do *compliance* (Frazão; Medeiros, 2018, p. 80).

Primeiramente, cumpre observar que a LGPD (BRASIL, 2018) prevê a possibilidade de responsabilização civil do controlador ou operador que a infringirem:

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

Embora não haja qualquer referência expressa do legislador em relação a natureza da responsabilidade aplicada aos agentes de tratamento, ou seja, se seria de ordem objetiva ou subjetiva, a partir da análise sistemática e textual da LGPD (BRASIL, 2018) entende-se pela aplicação da responsabilidade subjetiva. Como bem explicam Gualda e Matta (2020):

> (...) a LGPD não apresenta determinação expressa sobre a responsabilização independente de culpa. Além disso, o dispositivo aponta que a conduta do agente de tratamento deve ser em violação da legislação de proteção de dados pessoais, isto é, diante da inobservância do cumprimento dos deveres trazidos pela lei, o que coloca em cena a culpa em sentido amplo como fundamento da responsabilização. A reprovabilidade da conduta do agente de tratamento se vincula à violação do dever de observar os preceitos da LGPD.

Vale dizer que a LGPD (BRASIL, 2018) ainda estabelece no art. 44, parágrafo único que “responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano”.

Assim, é compreensível que não basta a verificação do mero desempenho do tratamento de dados para imputar a responsabilidade, sendo necessário demonstrar a presença de culpa,

seja pela violação aos ditames da normativa, seja por não adotar as medidas de segurança adequadas.

Dessa forma, é patente que a empresa que disponha de mecanismos de *compliance* esteja mais apta a demonstrar a ausência do elemento da culpa diante da ocorrência de possíveis danos a titulares de dados.

Salienta-se que a LGPD (2018) ainda traz a excludente de responsabilidade àqueles que atuarem em conformidade com a lei, dispondo que os agentes de tratamento não serão responsabilizados se demonstrado que, "embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados" (art. 43, II).

Portanto, uma vez adotados bons mecanismos de proteção de dados a partir da estruturação de um programa de *compliance*, será mais facilmente comprovada a atuação em consonância com a legislação, o que pode ocorrer, por exemplo, por meio de Relatório do Impacto que seja mantido atualizado, permitindo o afastamento da responsabilização.

A LGPD (BRASIL, 2018) também estabelece um rol taxativo de sanções administrativas a serem aplicadas diante da infração das normas contidas na lei, dentre as quais se incluem a advertência, com indicação de prazo para adoção de medidas corretivas, sob pena de multa diária (art. 52, I e II)[15], bem como a aplicação de multa de 2% do faturamento da empresa (art. 52, I).

Ocorre que a adoção de mecanismos de segurança e de políticas de boas práticas e de governança pode ser considerada como atenuante no momento de aplicação das sanções, consoante ao que dispõe o art. 52, §1º, incisos VIII e IX da LGPD (BRASIL, 2018).

No entanto, os incentivos à adoção de um programa de *compliance* não se limitam ao favorecimento em relação à responsabilização e sanções previstas na lei, pois também reflete sobre a imagem da empresa perante os titulares dos dados com os quais lida.

> (...) a adoção de programas de *compliance* robustos, além de garantir o cumprimento das normas de proteção de dados, contribui para a construção de ambiente de confiança entre os titulares – essencial em um mundo em que o disseminado uso de dados pessoais aparenta ser processo irreversível – e

[15] Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: I - advertência, com indicação de prazo para adoção de medidas corretivas; II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; III - multa diária, observado o limite total a que se refere o inciso II; [...] (BRASIL, 2018)

> representa diferencial competitivo (FRAZÃO; OLIVA; ABILIO, 2018, p. 708);

Não se pode olvidar os reflexos o *compliance* à proteção de dados podem emitir sobre as relações negociais, na medida em que a tendência é que empresas nacionais e estrangeiras negociem preferencialmente com aquelas que estão em conformidade com as normas de proteção de dados vigentes, justamente pela confiança e credibilidade que transparecem.

> O *compliance* tem sido visto pelo governo, sociedade e mercado como o mecanismo capaz de extirpar os atos ilícitos do meio negocial e disseminar a cultura de integridade nos negócios. Não apenas, as organizações têm paulatinamente exigido que seus fornecedores se alinhem às práticas de *compliance*, sob pena de não mais se relacionarem com eles. Conclui-se que estar em *compliance* é imperativo no que tange ao aspecto regulatório, concorrencial e negocial (PEREIRA; TORCHIA, 2020, p. 14)

Assim, não obstante os custos envolvidos com o desenvolvimento e manutenção de um bom programa de *compliance* à proteção de dados, deve-se considerar as contrapartidas dele advindas, que se traduzem em benefícios de ordem jurídica, econômica e reputacional, evitando a ocorrência de desgastes prejudiciais às empresas.

Portanto, como restou demonstrado, a implementação de um bom programa de *compliance*, observados seus requisitos mínimos, configura um importante aliado ao efetivo atendimento aos ditames da LGPD. Dessa forma, cumpre as empresas desenvolveram seus programas de acordo com as suas singularidades, observando os incentivos advindos de sua atuação em conformidade com a nova normativa.

5. CONCLUSÃO

O intenso fluxo de dados verificado no cenário tecnológico atual tornou os dados pessoais um importante elemento econômico, que passou a ser peça central na chamada "economia digital". Empresas têm cada vez mais investido na implementação de tecnologias sofisticadas a fim de realizar a coleta e processamento destes dados para utilizá-los para fins diversos, embora seu objetivo central tenha sempre o cunho econômico.

Como visto, esse tratamento de dados em larga escala, na maioria das vezes, não é acompanhado por mecanismos que garantam a sua proteção. Assim é que se verifica em diversos casos desdobramentos negativos advindos do tratamento irregular de dados.

A Lei Geral de Proteção de Dados (BRASIL, 2018) vem cumprir importante papel protetivo trazendo consigo significativas mudanças neste canário, uma vez que a proteção de dados deve ser tratada com prioridade neste contexto. A partir de uma abordagem ampla do tratamento de dados pessoais e à luz de princípios dela extraídos, a lei se traduz em um sistema pautado na prevenção e segurança, em que a adoção de mecanismos de prevenção e mitigação de riscos são cruciais para o atendimento à normativa.

Dessa forma, a LGPD prevê o programa de governança em privacidade, delineando diretrizes de boas práticas e de governança a serem implementadas pelas empresas com o intuito de promover o cumprimento das normas impostas pela lei através de medidas internas de adequação. Assim, entende-se que a implementação desse programa pode ser concretizada a partir da lógica do *compliance.*

Para que o programa de *compliance* surta os efeitos desejados, é necessário o atendimento aos seus requisitos mínimos, que compreendem o mapeamento de todos os dados tratados pela empresa, a avaliação dos riscos de acordo com os dados identificados, de modo que, a partir deste diagnóstico, sejam implementados os mecanismos adequados à cada empresa. Neste sentido, os principais elementos a serem observados são a criação de um Código de Conduta, a nomeação do encarregado responsável por conduzir o programa, além da incorporação do *privacy by design* na cultura da empresa.

Embora a adequação à LGPD seja inadiável, tendo em vista que a legislação já se encontra em vigor, a mudança cultural no ambiente interno das empresas e a estruturação e implementação de mecanismos de proteção de dados demandam um bom planejamento e tempo, uma vez que não é possível, e nem recomendável, que seja implementado da noite para o dia.

A acomodação e resistência às mudanças de hábitos já consolidados no interior das empresas pode representar um óbice à implementação dos novos mecanismos, o que requer o comprometimento da alta administração neste processo, a fim de conscientizar os colaboradores da necessidade de adequação à LGPD e garantir todos os recursos necessários para a efetivação do *compliance.*

Deve-se ter em conta que, embora seja necessário dispender tempo e recurso humano, financeiro e técnico para a implementação do programa, tais fatores podem ser contrabalanceados com os benefícios advindos da atuação em conformidade com a LGPD. Estes estímulos consistem desde a atenuação das sanções administrativas e o afastamento de responsabilização civil previstos pela lei, até os reflexos sobre sua credibilidade perante os titulares de dados e outras empresas, sejam estas nacionais ou estrangeiras.

Assim, longe de representar um ônus a atividade empresarial e às relações comerciais, a LGPD pretende fortalecer a segurança e prevenção aos riscos atinentes ao tratamento de dados pessoais, a fim de que as empresas se adequem aos parâmetros de proteção exigidos no contexto mundial, uma vez que a tendência é que cada vez mais países e empresas exijam a conformidade como pressuposto para realizar negociações.

REFERÊNCIAS BIBLIOGRÁFICAS

BEZERRA, André Luís Martins; WEBERBAUER, Paul Hugo (Orient.). **A Lei 13.709/18 e os novos desafios da proteção de dados pessoais e identidade**. 42 p. Trabalho de Conclusão de Curso (graduação em Direito) - Universidade Federal de Pernambuco, Faculdade de Direito do Recife, Recife, 2019. Disponível em: https://repositorio.ufpe.br/handle/123456789/36323. Acesso em: 15 dez. 2020.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 2. ed. Rio de Janeiro: Forense, 2018 [Versão Minha Biblioteca]. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530988777/cfi/6/40!/4/260/2@0:94.9. Acesso em: 01 ago. 2020.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990.** Dispõe sobre a proteção do consumidor e dá outras providências, Brasília, 11 set. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 02 ago. 2020.

_____. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal (...), e dá outras providências, Brasília, 18 nov. 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 02 ago. 2020.

_____ **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, Brasília, 23 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 02 ago. 2020.

_____. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD), Brasília, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 22 dez. 2020.

_____. **Medida provisória nº 959, de 29 de abril de 2020** (Convertida na Lei nº 14.058 de 2020). (...) Prorroga a *vacatio legis* da Lei nº 13.709, de 14 de agosto de 2018, que estabelece a Lei Geral de Proteção de Dados (LGPD), Brasília, 29 abr. 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv959.htm. Acesso em: 02 ago. 2020.

_____. **Guia de boas práticas**: Lei Geral de Proteção de Dados. Portal gov.br, Brasília, ago. 2020. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-de-boas-praticas-lei-geral-de-protecao-de-dados-lgpd. Acesso em: 14 mai. 2021.

BUSSOLA. Com crescimento do e-commerce, fraudes digitais aumentaram 83,7%. **Exame**, 11 mai. 2021. Disponível em: https://exame.com/bussola/com-crescimento-do-e-commerce-fraudes-digitais-aumentaram-837/. Acesso em: 15 mai. 2021.

CADWALLADR, Carole; CARRAM-HARRISON, Emma. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. **The Guardian**, 17 de mar. 2018. Disponível em: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. Acesso em: 01 ago. 2020.

CARVALHO, Vinicius Marques de; MATTIUZZO, Marcela; PONCE, Paula Pedigoni. Boas práticas e Governança na LGPD. In: DONEDA, Danilo et al. (Coord.) **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, p. 371-384, 2021 [Versão Minha Biblioteca]. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992200/cfi/6/2!/4/2@0:0. Acesso em: 10 mai. 2021.

CILURZO, André. ICTS Protiviti**:** 82% das empresas ainda estão despreparadas para cumprir a LGPD. **ICTS**, 11 dez. 2020. Disponível em: https://icts.com.br/icts-news/icts-protiviti-82-das-empresas-ainda-estao-despreparadas-para-cumprir-a-lgpd. Acesso em: 10 mai. 2021.

CONSELHO ADMINISTRATIVO DE DEFESA ECONÔMICA (CADE). **Guia Programas de *Compliance***. Ministério da Justiça, Brasília, 2016. Disponível em: https://cdn.cade.gov.br/Portal/centrais-de-conteudo/publicacoes/guias-do-cade/guia-compliance-versao-oficial.pdf. Acesso em: 15 mai. 2021.

CORACCINI, Raphael. Novo vazamento expõe dados telefônicos de mais de 100 milhões de brasileiros. **CNN Brasil *Business***, 11 fev. 2021. Disponível em: https://www.cnnbrasil.com.br/business/2021/02/10/novo-vazamento-expoe-dados-telefonicos-de-mais-de-100-milhoes-de-brasileiros. Acesso em: 04 jun. 2021.

CUEVA, Ricardo Villas Bôas. Funções e finalidades dos programas de *compliance*. In*:* CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (Coord.). ***Compliance*:** Perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, p. 53-69, 2018.

DISTRITO FEDERAL. **Ação Civil Pública por Danos Morais Coletivos**. Ministério Público do Distrito Federal e Territórios. Brasília, 30 jul. 2018. Disponível em: https://www.mpdft.mp.br/portal/pdf/noticias/julho_2018/Ação_Danos_Banco_Inter_CS.pdf. Acesso em: 25 jul. 2020.

_____. MPDFT ajuíza ação contra o Banco Inter por vazamento de dados pessoais. **Ministério Público do Distrito Federal e Territórios,** 31 Jul. 2018. Disponível em: https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2018/10211-mpdft-ajuiza-acao-contra-o-banco-inter-por-vazamento-de-dados-pessoais. Acesso em: 25 jul. 2020.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

FENILI, Maiara Bonetti; SARAIVA NETO, Pery. Novos marcos legais sobre proteção de dados pessoais e seus impactos na utilização e tratamento de dados para fins comerciais. **Revista de Estudos Jurídicos e Sociais.** v. 1, n. 1, 2018. Disponível em: https://rejus.univel.br/ojs/index.php/revista/article/view/46. Acesso em: 17 jul. 2020.

FLUMIGNAN. Silvano José Gomes; FLUMIGNAN, Wévertton Gabriel Gomes. Princípios que regem o tratamento de dados no Brasil. In: LIMA, Cíntia Rosa Pereira de (Coord.). **Comentários à lei geral de proteção de dados**: Lei n. 13.709/2018, com alteração da lei 13.853/2019. São Paulo: Almedina, 2020. p. 123-140.

FRAZÃO, Ana; MEDEIROS, Ana Rafaela Martinez. Desafios para a efetividade dos programas de compliance. In: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana. ***Compliance***: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, p. 71-104, 2018.

FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. *Compliance* de Dados Pessoais. In: FRAZÃO, Ana Frazão; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coord). **A Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro**. São Paulo: Revista dos Tribunais, p. 676-715, 2019.

GROPP, Maria Eduarda; MOTTA, Jefferson Holliver. A Mineração de Dados e os Direitos de Personalidade dos Consumidores: Análise da Privacidade na Era Digital. *In:* VEIGA; F. S.; GONÇALVES, R. M. (Edit.); BENEVIDES, S. H. S.; GAUDÊNCIO, F. S. **Governança e Direitos Fundamentais:** revisitando o debate entre o público e o privado, 1. ed. Porto: IBEROJUR, p. 65-74, 2020. Disponível em: https://dialnet.unirioja.es/servlet/libro?codigo=769268. Acesso em: 20 jul. 2020.

GUALDA, Diego; MATTA, Laura Aliende da. Responsabilidade subjetiva na LGPD. **Machado Meyer**. 04 dez. 2020. Disponível em: https://www.machadomeyer.com.br/pt/inteligencia-juridica/publicacoes-ij/tecnologia/responsabilidade-subjetiva-na-lgpd. Acesso em: 19 jun. 2021.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC). **Código das melhores práticas de governança corporativa**. 5. ed. São Paulo: IBGC, 2015. Disponível em: https://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=21138. Acesso em: 17 de abr. 2021.

ICTS PROTIVITI. Resultados da avaliação de adequação à LGPD. **ICTS**, mar. 2020. Disponível em: https://www.protiviti.com/sites/default/files/brazil/solutionsindustries/infografico_-_resultados_da_avaliacao_de_adequacao_a_lgpd_-_marco_2020.pdf. Acesso em: 22 dez. 2020.

LEADERS. The world's most valuable resource is no longer oil, but data. **The Economist**, 06 mai. 2017. Disponível em: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. Acesso em: 07 ago. 2020.

MARR, Bernard. ***Big Data in Practice:*** *how 45 successful companies used big data analytics to deliver extraordinary results*. 1nd ed. Wiley, 2016.

MARTINS, Marcelo Guerra; TATEOKI, Victor Augusto. Proteção de dados pessoais e democracia: fake news, manipulação do eleitor e o caso da Cambridge Analytica. **Revista Eletrônica Direito e Sociedade-REDES**, v. 7, n. 3, 2019. Disponível em: https://revistas.unilasalle.edu.br/index.php/redes/article/view/5610. Acesso em: 30 jul. 2020.

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

_____. Privacidade e dados pessoais. Proteção de dados pessoais: fundamento, conceitos e modelo de aplicação. Panorama Setorial da Internet. n. 2. ano 11, jun, 2019. Disponível em:

https://cetic.br/media/docs/publicacoes/6/15122520190717-panorama_setorial_ano-xi_n_2_privacidade_e_dados_pessoais.pdf. Acesso em 02 set. 2020.

MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. **Revista Estudos Institucionais**, v. 6, n. 2, p. 507-533, set. 2020. Disponível em: https://www.estudosinstitucionais.com/REI/article/view/521/510. Acesso em: 13 mai. 2021.

_____. Proteção de dados para além do consentimento: tendências de materialização. In: DONEDA, Danilo et al. (Coord.) **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, p. 90-112, 2021, [Versão Minha Biblioteca]. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992200/cfi/6/2!/4/2@0:0. Acesso em: 12 mai. 2021.

MORAES, Maria Celina Bodin de. QUEIROZ, João Quinelato de. Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGPD. **Proteção de Dados Pessoais:** avanço tecnológico. Cadernos Adenauer. Ano XX (2019), n.°3. Rio de Janeiro: Fundação Konrad Adenauer, p. 113-135, out. 2019.

MOURA, Clarissa Maria Lima. **Dados pessoais como ativo na economia digital:** a tutela jurídica na legislação nacional e europeia acerca da manipulação de dados sensíveis para fins econômicos. 2019. 58 f. Trabalho de Conclusão de Curso (graduação em Direito) - Faculdade de Direito do Recife - CCJ - Universidade Federal de Pernambuco, Recife, 2019. Disponível em: https://repositorio.ufpe.br/handle/123456789/37157. Acesso em: 20 jul. 2020.

NUNES, Gabriela Victória Miranda. **Governança e Boas Práticas na Lei Geral de Proteção de Dados:** dos programas de *compliance.* 2019, p. 67. Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade de Brasília, Brasília, 2019. Disponível em: https://bdm.unb.br/handle/10483/25080. Acesso em: 17 mai. 2021.

PEREIRA, Fernanda Maria; TORCHIA, Bruno. Como o *compliance* pode ser um diferencial na gestão das organizações. **Revista Científica Faculdade Unimed**, v. 1, n. 3, p. 11-14, 2020. Disponível em: https://doi.org/10.37688/rcfu.v1i3. Acesso em: 15 mai. 2021.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais:** comentários à Lei n. 13.709/2018 (LGPD). 2. ed. São Paulo: Saraiva Educação, 2020.

PRESSE, France. Cambridge Analytica se declara culpada em caso de uso de dados do Facebook. **G1**, 09 jan. 2019. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2019/01/09/cambridge-analytica-se-declara-culpada-por-uso-de-dados-do-facebook.ghtml. Acesso em: 21 jul. 2020.

REDAÇÃO. Banco Inter vai pagar R$ 1,5 milhão por vazamento de dados de clientes. **Veja**, 19 dez. 2018. Disponível em: https://veja.abril.com.br/economia/banco-inter-vai-pagar-r-15-milhao-por-vazamento-de-dados-de-clientes/. Acesso em: 05 jun. 2021.

REDECKER, Ana Cláudia; BALLICO, Louise Finger. O papel dos agentes de tratamento na Lei Geral de Proteção de Dados (LGPD). **Revista Jurídica Luso-brasileira,** [...], Ano 6, n. 5, p. 125-170, 2020. Disponível em: https://www.cidp.pt/revistas/rjlb/2020/5/2020_05_0125_0170.pdf. Acesso em: 13 mai. 2021.

SAAVEDRA, Giovani Agostini. *Compliance* de dados. *In*: DONEDA, Danilo et al. (Coord.) *In:* **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, p. 729-743, 2021 [Versão Minha Biblioteca]. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992200/cfi/6/96!/4/260/4@0:85.4.

SANTOS, Viviane Bezerra de Menezes. **Lei Geral de Proteção de Dados**: fundamentos e *compliance*. Trabalho de Conclusão de Curso (Graduação em Direito) – Universidade Federal do Ceará, Faculdade de Direito, Fortaleza, 2019. Disponível em: http://www.repositorio.ufc.br/handle/riufc/49370. Acesso em: 07 ago. 2020.

SERASA EXPERIAN**.** Pesquisa LGPD (Lei Geral de Proteção de Dados Pessoais: como as empresas de preparam para atender à nova regulamentação. **Serasa Experian**, [s. l.], [2020]. Disponível em: https://www.serasaexperian.com.br/images-cms/wp-content/uploads/2020/11/03225812/White-Paper-Serasa-Experian-LGPD-Como-as-Empresas-se-prepararam.pdf. Acesso em: 15 mai. 2021.

SILVEIRA, Sergio Amadeu; AVELINO, Rodolfo; SOUZA, Joyce. A privacidade e o mercado de dados pessoais. **Liinc em Revista**. v. 12, n. 2, p. 217-230, 2016. Disponível em: https://doi.org/10.18617/liinc.v12i2.902. Acesso em: 16 mai. 2021.

SIMONSEN, Ricardo. Os requisitos de um bom programa de *compliance*. In: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana. ***Compliance***: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, p. 105-128, 2018.

SWANT, Marty. **The World's Most Valuable Brands.** Forbes [s. l., s. d.]. Disponível em: https://www.forbes.com/powerful-brands/list/. Acesso em: 19 jul. 2020.

TATEOKI, Victor Augusto. A proteção de dados pessoais e a publicidade comportamental. **Revista Juris UniToledo**. v. 2, n. 1, p. 62-75, 2017. Disponível em: http://ojs.toledo.br/index.php/direito/article/view/113. Acesso em: 15 mai. 2021.

UNIÃO EUROPEIA. **Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995**. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados, [s. l.], 24 out. 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:31995L0046. Acesso em: 10 dez. 2020.

_____. Regulamento (EU) 2016/679 Parlamento Europeu e do Conselho, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, [s. l.], L 119, p. 1, 04 mai. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 10 dez. 2020.

VITORIO, Tamires. Facebook fica mais perto de 3 bilhões de usuários ativos e receita cresce em 2020. **Exame,** 27 jan. 2021. Disponível em: https://exame.com/tecnologia/facebook-fica-mais-perto-de-3-bilhoes-de-usuarios-ativos-e-receita-cresce-em-2020/. Acesso em: 18 fev. 2021.

WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. In: **Harvard Law Review**, vol. 4, no. 5, p. 193–220, 1890. Disponível em: https://www.jstor.org/stable/1321160?seq=1#metadata_info_tab_contents. Acesso em: 07 ago. 2020.

ZANATTA, Rafael A. F. **Perfilização, Discriminação e Direitos:** do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados Pessoais, 2019. Disponível em: https://www.researchgate.net/publication/331287708_Perfilizacao_Discriminacao_e_Direitos_do_Codigo_de_Defesa_do_Consumidor_a_Lei_Geral_de_Protecao_de_Dados_Pessoais. Acesso em: 01 ago. 2020.