SEMANA ACADÊMICA
REVISTA CIENTÍFICA
ISSN 2236-6717

A ATUAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) FRENTE *COMPLIANCE*

[ver artigo online]

Willames José Morais Galdino [1]
Emerson Oliveira de Faria [2]

RESUMO

No que tange a guarda e transmissão de dados pessoais, se fez necessário a criação da LGPD, para responsabilizar, controlar e restringir a coleta de dados por parte das empresas. Neste sentido, quais seriam as dificuldades de aplicar o *compliance* de forma eficiente frente a Lei Geral de Proteção de Dados no setor privado. Com a aplicabilidade da LGPD, uma vez que ela já trouxe em menos de dois anos alterações e vetos em sua Lei, além de extensão de seu *vacatio legis* prorrogada por mais de uma vez, e mesmo assim, trazendo obrigações e incertezas jurídicas para as empresas, gerando dificuldade de implantação de métodos afetivos na área de *compliance*, para que se cumpra a LGPD. Quanto aos procedimentos metodológicos, a pesquisa utilizará da metodologia qualitativa, exploratória com procedimentos de pesquisa bibliográficas (doutrinas especializadas, artigos, trabalhos monográficos e dissertações de mestrados) e documental (artigos de lei, decisões judiciais), pois a este trabalho irá descrever a aplicabilidade da LGPD com a utilização dos métodos de *compliance*.

Palavras-chave: *Compliance*. Lei geral de proteção de dados. Proteção de dados.

THE PERFORMANCE OF THE GENERAL DATA PROTECTION LAW (LGPD) FRONT COMPLIANCE

ABSTRACT

Regarding the custody and transmission of personal data, was made the creation of the LGPD is necessary to hold companies accountable, control and restrict data collection. In this sense, what are the difficulties of applying compliance efficiently in the face of the General Data Protection Law in the private sector? With the applicability of the LGPD, since it has already brought amendments and vetoes to its Law in less than two years, in addition to the extension of its vacatio legis extended more than once, and even so, bringing legal obligations and uncertainties for companies , generating difficulty in implementing affective methods in the compliance area, so that the LGPD is fulfilled. As for the methodological procedures, the research will use the qualitative methodology, exploratory with bibliographic research procedures (specialized doctrines, articles, monograph works and master's dissertations) and documentary (articles of law, judicial decisions), as this work will describe the applicability of LGPD with the use of compliance methods.

Keywords: Compliance. General data protection law. Data protection.

1 Graduando do curso de Direito da Faculdade Interamericana de Porto Velho-UNIRON. Porto Velho-RO. E-mail: willamesmorais@yahoo.com.br.
2 Orientador. Graduado em Direito, Docente do curso de Direito da Faculdade Interamericana de Porto Velho-UNIRON. Porto Velho-RO. Doutorado em Função Social do Direito - FADISP. e-mail: emerson.faria@uniron.edu.br.

http://dx.doi.org/10.35265/2236-6717-212-9370
FORTALEZA-CE. EDIÇÃO 212. V.9. ANO 2021.

INTRODUÇÃO

O presente artigo possui o intuito de estudar a Lei geral de proteção de dados (LGPD) frente *compliance.* Pois, diante de um cenário metamórfico legal e regulatório que visa estabelecer organizações éticas e responsáveis, torna-se mandatório que as empresas salteiem em uma aplicação de *Compliance* efetiva para que viabilize a execução das leis de modo mitigado e pormenorizado avaliando riscos internos e externos.

Diante disso, surge o seguinte questionamento: quais as dificuldades de aplicar o *compliance* de forma eficiente frente a Lei Geral de Proteção de Dados no setor privado? A estrutura para execução do *compliance* é composta por alguns pilares que em si exige um comprometimento de toda a empresa, e principalmente da alta-direção. Levando em consideração os procedimentos adotados pelo *compliance* para atingir um resultado eficiente, deve existir diretrizes, leis, regras e regulamentos fortemente estruturados. Pois a LGPD envolve a coleta e o armazenamento de dados pessoais e com isso as empresas terão que se adequar, o que terá um forte impacto econômico nas empresas caso não adotem as diretrizes da referida lei. Com isso podemos perceber o quão importante ter um programa de *compliance* bem estruturado, pois a LGPD não atingirá somente o setor jurídico, mas também marketing e TI dentre outras áreas.

Ademais, objetivo geral do artigo é descrever a aplicação do *compliance* da Lei Geral de Proteção de Dados (LGPD) dentro do setor privado e suas culturas organizacionais eficientes. Já os objetivos específicos são: demonstrar e exemplificar o uso do *compliance* no setor privado; descrever e simplificar a Lei Geral de Proteção de Dados; e elaborar um guia de compreensão de *compliance* frente a LGPD

A escolha do tema desta pesquisa está atrelada à grande modificação do cotidiano de muitos indivíduos, empresas e cidades no que tange a guarda e transmissão de dados pessoais, ainda que nosso ordenamento jurídico já abordasse o tema com legislação que direciona e indica direitos e deveres, (Lei 12.965/2014 - Marco Civil da Internet - MCI), do uso da internet se fez necessário a criação da LGPD, para responsabilizar, controlar e restringir a coleta de dados por parte das empresas.

Desta forma, este trabalho visa propor soluções de Compliance, que podem ser adaptadas para a realidade de diversos setores privados utilizando como base para esta execução a Lei nº

13.709/2018 a partir de seus fundamentos e das suas implicações práticas, examinando a motivação por trás da elaboração de uma legislação específica, focado exclusivamente na proteção de dados dos cidadãos em todos os setores.

1 CONSIDERAÇÕES PRELIMINARES SOBRE A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Com o passar do tempo a sociedade sofreu grandes modificações em sua estrutura, impactando o seu desenvolvimento e marcando fortemente momentos históricos. A primeira na sociedade agrícola, onde a economia era impulsionada pelo escambo, sendo a primeira prática comercial. A segunda modificação foi o surgimento das máquinas a vapor e a eletricidade, onde se desenvolveu a sociedade industrial. A terceira, surge após a Segunda Guerra mundial, onde o foco já não seria o que pudesse ser produzido e sim os serviços que poderiam que poderiam ser ofertados, como, os setores bancários, securitários, educacional, assistência médica e jurídica (BIONI, 2020. p. 22).

E na última década, o mundo se depara cada vez mais conectado, devido seu avanço tecnológico, gerando um aumento considerável no que diz respeito a geração e consumo de informação, aumento este gerado pela grande quantidade de dados processados pela internet, com capacidade de armazenamento e velocidade de transmissão cada vez maiores. Informações essas que podem ser utilizadas pelos mais diversos setores econômicos, sociais e governamentais.

A captação de dados é utilizada como referência social para controle jurídico dos mais diversos setores da sociedade, independentemente de quais fossem, desde levantamento de pesquisas sociais, até estudos epidemiológicos, este fato se dá devido a uma necessidade ampla do Estado de estabelecer conteúdo e traçar perfis sociais para o seu desenvolvimento socio político (TEPEDINO, 2019. p. 33).

Nesse contexto o Congresso nacional observou uma necessidade da implementação de uma legislação geral para a proteção de dados (BRASIL, 2018). Contudo observando ainda maiores necessidades de remodelação, a LGPD de 2018 foi considerada com severas lacunas interpretativas, sendo então alterada pela Lei Nº 13.853, de 8 de julho de 2019 (BRASIL, 2019)

com o objetivo de dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados.

1.2 EVOLUÇÃO HISTÓRICA DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

A sociedade, ao longo dos anos, passou por vários modelos de organização social, de forma que, em cada período, houve um elemento principal para o seu desenvolvimento. Nesse contexto, após a Segunda Guerra Mundial, percebeu-se como as informações pessoais dos cidadãos são importantes para programar ações com o intuito de um crescimento constante, conforme entendimento de Alice Koepsel (2021).

Dessa forma, diretamente relacionada ao avanço tecnológico e pela globalização, passou-se a ter uma dependência maior de bases de dados pessoais, diante dos negócios da economia digital. Logo, a informação, na sociedade atual, é o elemento central para o desenvolvimento da economia, passando-se a solicitar normas para a proteção de dados pessoais. Nota-se que, há um cenário de desigualdade perante o direito de proteção da privacidade e intimidade das pessoas com o aumento no processamento de dados, compartilhamento de informações e no progresso da inteligência artificial (KOEPSEL 2021).

Até a aprovação da Lei Geral de Proteção de Dados Pessoais, o Brasil encontrava-se apenas com normas setoriais sobre a proteção de dados pessoais por meio da Constituição Federal, do Código de Defesa do Consumidor, da Lei do Cadastro Positivo, a Lei de Acesso à Informação, Lei Carolina Dieckmann, o Marco Civil da Internet, entre outras legislações.

Por fim, o tema elevou-se na União Europeia, circunstância em que ocorreu a aprovação do Regulamento Geral de Proteção de Dados, com o propósito de versar sobre a proteção de dados pessoais das pessoas físicas e o modo de como é realizada as operações com tais informações. Com a instituição desse regulamento, passou-se a exigir que os países que mantinham relações comerciais com a Europa, também deveriam dispor de uma legislação do mesmo nível, sob pena de aumentar a dificuldade na realização nos negócios. À vista disso, mesmo com leis esparsas voltadas a proteção dos dados pessoais sob alguma circunstância, houve a necessidade da criação de uma norma capaz de observar os princípios internacionalmente aderidos (KOEPSEL 2021).

1.2 ASPECTOS LEGISLATIVOS DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Contudo, antes mesmo da promulgação da Lei 13.709/2018, denominada Lei Geral de Proteção de Dados, o Brasil já possuía em seu ordenamento jurídico o chamado Marco Civil da Internet (MCI) (Lei 12.965/2014), onde constituiu importantes princípios, garantias e deveres para o uso da internet, e em seu artigo 3º, inciso III, já previa a proteção de dados.

Com isso, no dia 14 de agosto de 2018, foi aprovada a LGPD, porém com forte influência da lei europeia conhecida como GDPR (*General Data Protection Regulation*) (EU GDPR 2016/679), porém devido a sua complexidade para a adaptação pelas empresas, foi então permitido que sua vigência ocorresse em 18 meses a contar da publicação, o que não ocorreu de fato, pois em 27 de dezembro 2018, a Medida Provisória 869, que em seguida foi convertida na Lei 13.853 de julho de 2019, aumentando assim o *vacatio legis* para 24 meses, prorrogando seus efeitos para agosto de 2020. Mas devido a pandemia do COVID-19, foi sancionada a Lei 14.010 (BRASIL, 2020), que alterou o seu início e suas sanções para agosto de 2021.

A abordagem da LGPD vai além de questões éticas, podemos ingressar em nosso atual cenário econômico, conseguimos entender por que as empresas necessitam cada vez mais de informações de dados pessoais de seus possíveis consumidores. Para criar, fornecer, adaptar ou até mesmo influenciar a escolha de seus produtos ou serviços e assim obter competitividade frente a concorrência.

Sendo assim, após elucidar superficialmente sobre a LGPD e a área de *compliance*, observa-se que temos uma Lei que foi prorrogada e seu *vacatio legis* trazendo uma insegurança jurídica e a área de *compliance* que terá que atuar não somente nas mudanças de procedimentos, mas também na cultura organizacional da empresa.

1.3 A LEI GERAL DE PROTEÇÃO DE DADOS E A PANDEMIA DO COVID-19

Em meio à pandemia, as pessoas também encontraram *softwares* que auxiliam em atividades rotineiras e permitem o entretenimento. Exemplo disso é que os aplicativos de entrega

de alimentos prontos para o consumo se tornaram ainda mais populares. Redes de supermercados intensificaram os serviços de venda *on-line*. Em atividades de lazer e de entretenimento, popularizaram-se as *lives* como uma forma de atração artística-cultural que permite que artistas tenham acesso à audiência de centenas de milhares de pessoas, conforme entendimento de Lesandro (PONCIANO, 2021).

Esses não são necessariamente *softwares* novos, mas que foram oportunamente descobertos e apropriados pelas pessoas. O resultado é que, em meio a esse contexto adverso, os *softwares* passaram a ser usados com maior intensidade, passaram a ser usados em atividades em que não eram usados antes e passaram a ser usados por um conjunto maior de pessoas.

> Excluindo-se os engenheiros de *software*, poucas pessoas compreendem como *softwares* são programados para executarem as funções que executam. Por exemplo, quais dados sobre elas ficam armazenados no sistema do supermercado quando fazem uma compra *on-line*, o que pode ser feito com seus dados pessoais como endereço e número de cadastro de pessoa física (CPF), quais tipos de inferência de novas informações podem ser feitas a partir desses dados, e quais dados são de acesso compartilhado entre diferentes *softwares* que elas usam. Geralmente, diante de um novo *software*, a percepção de sua utilidade se sobrepõe à percepção de risco na sua forma de uso. Por isso, é natural que inicialmente as pessoas não se questionem sobre os riscos (PONCIANO, 2021, p.01).

Dois riscos relevantes são a segurança e a privacidade no uso de *softwares*. Quanto à privacidade há um "paradoxo" entre percepção e comportamento. As pessoas dizem se preocupar com a privacidade, mas elas agem como se essa preocupação não existisse. Há três perfis de pessoas quanto às suas percepções de privacidade: há aquelas pessoas que nunca se preocupam; há aquelas pessoas que sempre se preocupam; e há aquelas pessoas que se preocupam menos quando percebem que há benefícios diante do risco. O terceiro perfil é o mais comum. A análise de risco e benefício está muito presente em modelos de privacidade. Porém, para que as pessoas façam tal análise, elas precisam conhecer igualmente os benefícios do *software* e os riscos associados ao uso dele (PONCIANO, 2021).

> Sem conhecer como o *software* faz o que ele faz, as pessoas não sabem realmente qual é o risco em usá-lo. O risco se revela quando algo ruim e inesperado ocorre. Fotos, vídeos e áudios com conteúdo sensível podem ser publicados por uma pessoa sem seu conhecimento e intenção, basta um desconhe-

> cimento das configurações do *software* ou de seu funcionamento padrão. Durante uma interação, dados pessoais e considerados sensíveis podem ser coletados e publicados na internet. Uma vez publicada, a informação se dissemina rapidamente e se torna difícil removê-la completamente (PONCIANO, 2021, p.01).

Durante uma *live*, várias informações são coletadas e mantidas sobre as pessoas que estão assistindo. Elas podem perder o controle de o que exatamente é feito com essas informações e passarem a ser alvo de diversas ações indesejadas. Assim, uma primeira exposição ao risco pode ser danosa o suficiente. É necessária uma proteção ou uma mitigação de danos se algo ruim ocorrer. Uma proteção legal é muitas vezes empregada nesse caso.

> No Brasil, a Lei nº 13.709, chamada Lei Geral de Proteção de dados Pessoais (LGPD), tem relevância nesse contexto de segurança e privacidade. A LGPD disciplina como empresas e entes públicos podem tratar informações de pessoas. Ela é inspirada na lei europeia, *General Data Protection Regulation* (GDPR), que está em vigor desde 25 de maio de 2018. Embora a GDPR e a LGPD não sejam leis específicas para *software*, elas abordam amplamente o tratamento de dados pessoais e têm aplicabilidade quando esse tratamento é feito por um *software*. É necessária uma proteção legal para as pessoas que têm seus dados pessoais tratados indevidamente. Assim, no Brasil, a LGPD é uma lei importante para proteção das pessoas diante do uso do intensivo de *software* e, por isso, ela se torna um imperativo na sociedade pós-pandemia (PONCIANO, 2021, p.01).

Pensando no futuro, a perspectiva é que os efeitos deste momento histórico causado pela pandemia de covid-19 sejam sentidos por vários anos. Fala-se muito sobre no "novo normal". Há razões para se crer que algumas novas formas de atuação são irreversíveis. No que se refere ao uso intensivo de *software*, o fundamento para esse argumento está no fato de que não se trata de uma mudança de curso, mas sim da intensificação de um processo que já estava ocorrendo antes da pandemia. A sociedade pós-pandemia tende a ser uma sociedade fortemente interconectada por *software*. É excelente que seja assim, pois é fundamental que os *softwares* sejam colocados à serviço da sociedade.

A área de Engenharia de *Software* busca o desenvolvimento de técnicas que permitam a construção de *softwares* que estejam cada vez mais aderentes às demandas da sociedade. Os tópicos de privacidade, segurança, transparência, aplicabilidade e interpretabilidade de software

estão sendo fortemente estudados em todo o mundo e também no Brasil. Para além dos *softwares* em si, a forma como as pessoas usam os *softwares* também é relevante. Assim, legislação e a educação a esse respeito são fundamentais. A pandemia acelerou o processo de inserção de *softwares* em diversos setores da sociedade. A sociedade precisa acelerar sua compreensão sobre o que isso significa, para usufruir dos benefícios e mitigar os riscos, conforme entendimento de Lesandro (PONCIANO, 2021).

1.4 A *COMPLIANCE* NA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

O *compliance*, consiste em um estado eficaz de conformidade, seguindo uma orientação normativa de comportamento com importância jurídica por força de contrato, regimento ou lei, sendo sua maior característica o cumprimento por meio de sistemas complexos de políticas, procedimentos e controles internos.

Sendo assim, pode-se verificar a complexidade da implantação de um programa de *compliance* frente as empresas públicas e privadas, onde existem ramos de atuação diversificadas, legislações especificas de acordo com seu ramo, levando em consideração até mesmo legislações extraterritoriais.

> Cada mercado ou cada área de atuação requerer práticas, análises e cuidados distintos. A área de *compliance* precisa customizar o seu programa de maneira que ela reflita todas as necessidades do mercado em que atua, desde a aplicação de normas, leis e regulamentos gerais, inclusive extraterritoriais, passando por averiguação sobre eventual existência de regulamentação específica aplicável, até as práticas do mercado em si (CRESPO, 2020, p. 37).

Para que um programa de *compliance* seja efetivo alguns pilares devem ser considerados em seu escopo: “O apoio da alta-direção e liderança; Código de ética, políticas e procedimentos; Educação, comunicação e treinamento; Monitoramento e auditoria; Helpline; Investigação/aplicação e medidas de correção e Mapeamento de risco” (CRESPO, 2020, p. 37). Dessa forma demonstra-se que o *compliance*, é muito mais que somente uma ideia derivada de um termo em inglês e que envolve execução de políticas e procedimentos.

A implementação de um programa de *compliance* nos dias atuais aborda não somente questões procedimentais, mas também éticas, pois sua aplicabilidade após a promulgação da

Lei 13.709/2018, Lei Geral de Proteção de Dados (LGPD), nos traz para um problema contemporâneo, onde a informação, o risco de tratamento de dados e/ou informação é delicado tanto para as empresas quanto para terceiros (colaboradores, consumidores e fornecedores) (CRESPO, 2020).

Os dados/informação disponibilizados ou não em redes, são protegidos pela LGPD, limitando o uso de dados autorizados e somente os que forem realmente necessários, garantindo assim o direito à privacidade. Direito este já ratificado pelo ordenamento, pela Declaração Universal dos Direitos Humanos (DUDH) brasileiro no dia 10 de dezembro de 1948, onde consta: "Art. 12 - Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação" (BRASIL, 1948).

E incluída em nossa Constituição Federal de 1988, em seu artigo 5º, inciso X dispõe que: "São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação" (BRASIL, 1988).

Desta forma, é de suma importância a aplicação do *compliance* de forma eficiente frente a Lei Geral de Proteção de Dados (LGPD) dentro do setor privado, pois segundo Giovanni Saavedra:

> (...) *Compliance* não é, portanto, uma metodologia, um sistema, um programa ou uma nova forma de consultoria. *Compliance* é a maneira através da qual mudamos o mundo no nosso ambiente de trabalho. Isso é tão verdade que, quando perdemos esse foco, quando *Compliance* vira uma mera metodologia ou um mero sistema de gestão é que os problemas começam a surgir e as fraudes se multiplicam (SAAVEDRA, 2020, p.01).

Neste sentido, a *compliance* terá como de evitar a ocorrência de irregularidades no que diz respeitos aos dados pessoais dos clientes de uma determinada empresa, por meio da aplicação de medidas e procedimentos contra a disponibilização de informações ou dados não autorizados pelo portador dos dados.

1.4.1. Os desafios e impactos da Lei Geral de Proteção de Dados (LGPD)

Os dados pessoais são extremamente sigilosos, nesse sentido, as empresas devem solicitar o consentimento do consumidor para utilizar os dados que foram compartilhados, podendo ser revogado a qualquer momento pelo consumidor.

Desta forma, a Lei Geral de Proteção da Dados - Lei 13.709 (BRASIL, 2018) visa proteger os dados pessoais dos consumidores. As empresas podem utilizar os dados compartilhados desde que o consumidor tenha autorizado tal ato, ou seja, tenha consentido a utilizar os dados compartilhados.

A LGPD também determina que empresas reportem à Autoridade Nacional de Proteção de Dados (ANPD) incidentes de segurança que possam colocar em risco dados dos consumidores, além de uma série de outras regulamentações exigindo conformidades e especificando sanções administrativas – incluindo multas.

O fato é que muitas empresas, entidades e o próprio governo não estão preparadas para a mudança cultural que a nova legislação exigirá: atualmente os dados podem estar espalhados por vários sistemas, podem estar em poder de parceiros ou ainda sendo tratados para várias finalidades distintas dentro da mesma organização. Por isso, a partir da LGPD, há alguns aspectos importantes que precisam ser:

> (I) É preciso indicar explicitamente um Data Privacy Officer (encarregado pelo tratamento de dados pessoais); (II) É preciso ter um inventário, uma política de retenção e backup de dados dos cidadãos e consumidores; (III) É necessária uma revisão ou ajustes de contratos com terceiros e a redação de um código de conduta para funcionários e terceiros para proteger a privacidade dos consumidores; (IV) É preciso fazer gestão de consentimentos, definir políticas e emitir avisos de privacidade; (V) É necessário ter um time de respostas a incidentes com dados ou violações de privacidade; (VI) É preciso ter ferramentas para gerenciamento de conformidade com a LGPD (SANTIN, 2021, p.01).

Para as empresas, incluindo o governo, claramente se observa que a LGPD implicará em um processo lento, custoso e contínuo, envolvendo mais aspectos de gestão de processos e pessoas do que a compra de pacotes de software de *ciber* segurança para proteção de informações pessoais – mas é preciso considerar que o mercado carece de profissionais qualificados nas áreas de segurança e privacidade, conforme entendimento de Altair Olivo (2020).

Já para a sociedade o processo de implementação da LGPD é repleto de desafios: se em um primeiro momento passaremos pela adaptação, que envolve novas práticas e tecnologias a serem implementadas para respeitar os direitos de privacidade do cidadão consumidor, há também questões referentes à fiscalização da lei, ainda cercada por dúvidas e questões em aberto para toda a população.

1.5 AÇÕES DA *COMPLIANCE* NA LEI GERAL DE PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados (LGPD) do Brasil, assim como o GDPR, deve ser vista pelas empresas como um passo para uma gestão de dados pessoais mais compreensiva na era moderna. Dessa forma, ações de *compliance não* devem ser deixadas para o último minuto, mas tratadas com a mesma seriedade que qualquer outra grande decisão estratégica de negócios. Abaixo, seguem algumas dicas para que as empresas cumpram a nova lei, conforme entendimento de Jorge (RIBKIN, 2020).

1.5.1. Dos dados e informações pessoais

A LGPD vale para as empresas que coletam dados pessoais, ou seja, informações que podem identificar alguém, seja no universo online, como no offline. Além de dados como nome, RG e CPF, a lei prevê também o tratamento de dados sensíveis, como informações de origem racial ou étnica, de saúde, religião e opinião política (RIBKIN, 2020).

Se cometidas infrações, a empresa corre o risco de pagar uma multa de até 2% de seu faturamento, limitada a R$ 50 milhões por infração. Além disso, os dados tratados irregularmente poderão ser bloqueados ou eliminados e a atividade de tratamento de dados pela empresa poderá ser suspensa ou mesmo proibida, conforme entendimento de Jorge (RIBKIN, 2020).

Muitas vezes, a empresa pode achar que não coleta nenhum dado relevante ou não percebe a amplitude dos dados que têm – dados pessoais, por exemplo, são mais do que só nomes. Portanto, o melhor ponto de partida é simplesmente conhecer os tipos de dados que sua empresa coleta e onde eles estão armazenados. Criar um mapa visual de todos os dados ajuda a organização a construir um quadro abrangente e supervisionar melhor as informações.

1.5.2. Do gerenciamento de dados

Uma vez que a empresa tenha construído um cenário dos dados relevantes que coleta e armazena, é hora de olhar para quem tem acesso a eles e como eles estão sendo usados. Equipes e departamentos diferentes acessam os mesmos dados de formas diversas e os usam para diferentes propósitos (RIBKIN, 2020).

Seja o time de marketing inserindo dados de possíveis clientes ou a área de RH lidando com dados dos seus funcionários, é essencial que a organização implemente procedimentos padronizados e fluxos de trabalho para lidar com dados pessoais, e que os funcionários só tenham acesso a eles quando necessários para sua função nos negócios, conforme entendimento de Jorge (RIBKIN, 2020).

Gerenciar os dados significa ter visibilidade de como eles vivem na empresa, mesmo que não estejam no local. A conformidade com a LGPD também depende de como fornecedores terceiros cumprem a lei.

1.5.3 Da proteção de dados

O terceiro passo para o *compliance* com a lei é garantir que os controles certos de segurança estejam em ordem para proteger as informações, o que não significa apenas o uso de criptografia. A LGPD requer monitoramento e diligência constantes e uma ação muito mais rápida no caso de uma violação de dados. A tecnologia tem um papel muito importante nessa jornada, mas não sozinha. É necessária uma combinação de técnicas de segurança, fluxos de trabalho padronizados, educação interna, controle de acesso, soluções de backup, entre outras estratégias, conforme entendimento de Jorge (RIBKIN, 2020).

1.5.4. Do armazenamento de documentos

Um dos capítulos mais importantes da Lei Geral de Proteção de Dados é sobre os direitos do titular. O texto prevê que o indivíduo tem o direito de corrigir dados, deletar infor-

mações desnecessárias e excessivas e revogar o consentimento quando quiser. Os negócios deverão cumprir e comprovar que atenderam a esses pedidos, por isso a visibilidade dos dados é tão crucial, conforme entendimento de Jorge (RIBKIN, 2020).

Assim, o cumprimento contínuo da LGPD também requer uma documentação e auditoria de quais dados a empresa está coletando, para qual propósito está sendo usado e por quanto tempo será armazenado.

1.5.5. Do aprimoramento

Um dos benefícios de controlar constantemente os processos de proteção de dados é a oportunidade de revisá-los e melhorá-los sempre. Com o mundo digital evoluindo e se expandindo constantemente, é seguro dizer que as responsabilidades sobre privacidade e proteção de dados também continuarão a crescer. Dessa forma, os negócios terão que continuar a melhorar para cumprir com a lei.

1.6 EFEITOS DA ADOÇÃO DOS PROGRAMAS DE *COMPLIANCE* DE DADOS PESSOAIS

Em vista das características da Lei nº 13.709 de 2018, juntamente com o conceito de *compliance* e dos requisitos para efetividade deste programa, é notório o papel de tal ferramenta na garantia do cumprimento da legislação referente à proteção de dados pessoais. Além da observância da legislação de proteção de dados pessoais, a adoção de boas práticas colabora na construção de uma relação de confiança com o titular dos dados, mediante uma atuação transparente, de modo a representar um diferencial competitivo nos negócios, conforme entendimento de Alice (KOEPSE, 2020).

A implementação desses programas demonstra que o tratamento de dados pessoais está sendo realizado de forma regular pelos agentes de tratamento, podendo, inclusive, servir como isenção de responsabilidade civil.

Ainda, a adoção de políticas de boas práticas e governança, ou melhor, programas de *compliance*, consiste como parâmetro para a fixação das sanções administrativas previstas na

Lei Geral de Proteção de Dados Pessoais, sendo, portanto, um critério atenuante no momento da definição da sanção por eventual descumprimento (KOEPSE, 2020).

Dessa forma, o *compliance* de dados pessoais tente a auxiliar os agentes de tratamento a aplicar normas de proteção de dados eficazes e, por causa disso, conduzirá a entidade a manter toda sua atividade de acordo com a legislação, utilizando a segurança da informação para diminuir incidentes que resultem na responsabilidade empresarial.

CONSIDERAÇÕES FINAIS

A informação é o principal elemento de desenvolvimento da sociedade atual. Com o surgimento de normas sobre proteção de dados pessoais está diretamente ligado aos avanços tecnológicos, perante uma maior utilização de bases de dados pessoais. Até o momento em que a Lei Geral de Proteção de Dados Pessoais foi aprovada, o Brasil, encontrava-se somente com normas correlatas sobre proteção de dados pessoais, como o Código de Defesa do Consumidor, a Lei de Acesso à Informação, o Marco Civil da Internet, dentre outros.

Com a chegada deste tema na União Europeia, ocorreu a aprovação do Regulamento Geral de Proteção de Dados. Ocasião que, por consequência, passou-se a exigir dos países que mantinham relações comerciais com aquele bloco o mesmo nível de proteção de dados. Assim, por influência, resultou na Lei 13.709 de 14 de agosto de 2018.

A Lei Geral de Proteção de Dados Pessoais dispõe acerca do tratamento de dados pessoais, até mesmo nos meios digitais, tanto por pessoa natural quanto por pessoa jurídica de direito público ou privado. E, possui como objetivo proteger os direitos de liberdade e privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural.

Ao realizar tal tratamento, deve-se observar a boa-fé e os princípios da finalidade, adequação, necessidade, qualidade dos dados, transparência, livre acesso, segurança, prevenção, não discriminação, responsabilização e prestação de contas. Como também, é necessário o enquadramento em alguma base legal para realizar qualquer operação com dados pessoais, dados pessoais sensíveis ou dados pessoais de crianças e adolescentes. Destaca-se que o consentimento é apenas uma das possibilidades que autorizam o tratamento.

Nesse sentido, a LGPD prevê um programa de governança em privacidade, sendo um conjunto de diretrizes de boas práticas e governança, equiparado aos programas de *compliance*,

ISSN 2236-6717

com o propósito de cumprimento de normas legais e internas e a realização de uma gestão de riscos, por meio de boas práticas. Para tal programa produzir efeitos, é necessário que haja a identificação dos riscos e medidas que possam responder a eles de modo adequado e proporcional, além da elaboração de um código de ética, o suporte da alta administração, treinamentos periódicos, e na adoção de canais de comunicação.

Ademais, a pandemia de COVID-19 demonstra que, a despeito da necessidade de se garantir a proteção da vida e da saúde da população, não se pode excluir a tutela dos direitos fundamentais da pessoa humana, evidenciando-se, assim, a urgente necessidade da entrada em vigor da LGPD, que vem sendo sucessiva e indevidamente adiada, a fim de se garantir segurança às relações sociais e jurídicas que envolvam o tratamento de dados pessoais.

Além disso, é de suma importância a superação do atual estado de calamidade pública, respaldando a grande preocupação com a privacidade de dados pessoais decorrente da maciça coleta, tratamento e manipulação de dados sensíveis e ligados à saúde. Isso pode gerar um efeito discriminatório intenso aos portadores de vírus, demandando, portanto, critérios efetivos e diferenciados contra incidentes de vazamentos desses dados pessoais.

Logo, a instauração de programas de *compliance* de dados pessoais é essencial para assegurar a observância da legislação de proteção de dados, além de consistir em um critério atenuante para a fixação da sanção administrativa por eventual descumprimento da LGPD, e de demonstrar o regular tratamento de dados, podendo, ainda, afastar a responsabilidade civil.

REFERÊNCIAS BIBLIOGRÁFICAS

BIONI, Bruno Ricardo. **Proteção de Pessoais a função e os limites do consentimento**. Rio de Janeiro, RJ. Editora Forense, 2020.

BRASIL, **Lei 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD) (2018). Brasília, DF: Senado, 2018.

BRASIL, **Lei 13.853, de 08 de julho de 2019.** Alteração da Lei Geral de Proteção de Dados Pessoais (LGPD) (2019). Brasília, DF: Senado, 2019.

BRASIL, **Lei nº 14.010, de 10 de junho de 2020**. Dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do coronavírus (Covid-19). Disponível em: https://www.in.gov.br/en/web/dou/-/lei-n-14.010-de-10-de-junho-de-2020-261279456. Acesso em: 19 mar. 2021.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Presidência da República, (2016). Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 29 set. 2020.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Presidência da República, (2016). Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 29 set. 2020.

Canal *Compliance*. **Saavedra GRC governance, risk and compliance**. Disponível em: http://www.ccompliance.com.br/saavedragrc/#:~:text=Compliance%20%C3%A9%20a%20maneira%20atrav%C3%A9s,e%20as%20fraudes%20se%20multiplicam. Acesso em 20 nov. 2020.

CRESPO, Marcelo Xavier de Freitas. **Compliance no Direito Digital.** Volume 3. São Paulo, Thomson Reuters, 2020.

Declaração Universal dos Direitos Humanos – tradução. Disponível em: https://www.oas.org/dil/port/1948%20Declara%C3%A7%C3%A3o%20Universal%20dos%20Direitos%20Humanos.pdf. Acesso em: 20 nov. 2020.

KOEPSEL, Alice de Medeiros. **Adoção e efeitos dos programas de *compliance* à luz da lei geral de proteção de dados pessoais.** Disponível em: https://riuni.unisul.br/bitstream/handle/12345/9626/MONOGRAFIA%20-%20ALICE%20KOEPSEL.pdf?sequence=1&isAllowed=y. Acesso em: 01 jun. 2021.

RIBKIN, Jorge. **Lei Geral de Proteção de Dados: 5 ações de *compliance* que devem começar já.** Disponível em: https://cio.com.br/tendencias/lei-geral-de-protecao-de-dados-5-acoes-de-compliance-que-devem-comecar-ja/. Acesso em: 22 abr. 2021.

SANTIN, Altair Olivo. **Os desafios e impactos da lei geral de proteção de dados.** Disponível em: https://www.anoreg.org.br/site/2019/10/14/artigo-os-desafios-e-impactos-da-lei-geral-de-protecao-de-dados-por-altair-olivo-santin/. Acesso em: 19 mar. 2021.

TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro.** São Paulo, SP. Revista dos Tribunais, 2019.

PONCIANO, Lesandro**. Pandemia e a importância da Lei Geral de Proteção de Dados Pessoais.** Disponível em: https://minasfazciencia.com.br/2020/09/09/pandemia-e-a-importancia-da-lei-geral-de-protecao-de-dados-pessoais/#:~:text=No%20Brasil%2C%20a%20Lei%20n%C2%BA,contexto%20de%20seguran%C3%A7a%20e%20privacidade.&text=Assim%2C%20no%20Brasil%2C%20a%20LGPD,imperativo%20na%20sociedade%20p%C3%B3s%2Dpandemia. Acesso em: 01 jun. 2021.