PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE DIREITO E RELAÇÕES INTERNACIONAIS
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO
ARTIGO CIENTÍFICO

A LEI GERAL DE PROTEÇÃO DE DADOS N°. 13.709/2018: UM ESTUDO SOBRE OS AVANÇOS E A EFETIVIDADE JURÍDICA

ORIENTANDA - ANNA KLARA MIRANDA TOBIAS
ORIENTADOR - PROF. DR.° GERMANO CAMPOS SILVA

GOIÂNIA - GO

2021

ANNA KLARA MIRANDA TOBIAS

A LEI GERAL DE PROTEÇÃO DE DADOS N°. 13.709/2018: UM ESTUDO SOBRE OS AVANÇOS E A EFETIVIDADE JURÍDICA

Artigo Científico apresentado à disciplina Trabalho de Curso II, da Escola de Direito e Relações Internacionais, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUCGOIÁS).

Orientador Prof.° Dr.° Germano Campos Silva

GOIÂNIA - GO
2021

ANNA KLARA MIRANDA TOBIAS

A LEI GERAL DE PROTEÇÃO DE DADOS N°. 13.709/2018: UM ESTUDO SOBRE OS AVANÇOS E A EFETIVIDADE JURÍDICA

Data da Defesa:___de_____de _____

BANCA EXAMINADORA

_____

Orientador (a): Prof. (a): Titulação e Nome Completo Nota

_____

Examinador (a) Convidado (a): Prof. (a): Titulação e Nome Completo Nota

AGRADECIMENTOS

A vida é uma jornada repleta de ciclos, com inícios e fins. Há cinco anos dei início a esta trajetória e hoje estou encerrando mais uma etapa vitoriosa, cheia de desafios, descobertas, experiências e aprendizados, na qual eu pude me reinventar e atestar minha capacidade para novos destinos.

Agradeço primeiramente à Deus, pelo dom da vida e pelas graças alcançadas, que na sua imensurável compaixão, me permitiu fazer este trabalho, mesmo quando a vida parecia não condescender e me sustentar nos dias de luta.

Aos meus pais, Francimar Miranda Tobias e Alfredo Machado Tobias, deixo o meu total sentimento de gratidão. Todo amor, dedicação, investimento e educação que recebo desde o meu nascimento forjaram a minha personalidade e me faz lutar por objetivos cada vez mais altos. Obrigada por me ensinarem a caminhar para assim poder seguir meus próprios passos.

Às minhas tias, Marina, Rosa e Eduarda, bem como os meus tios Francisco e Emanuel, por me concederem um suporte incomensurável ao longo do curso e pelo incondicional apoio em todas as muitas batalhas que encontramos pelo caminho e por toda a fé depositada em mim. Obrigada pela ajuda e apoio de vocês.

Ao meu namorado, amigo e companheiro Danyllo Guimarães Vieira, que desde o início esteve ao meu lado durante essa jornada, carrego com gratidão todos os nossos momentos vividos, agradeço pelo incentivo, apoio, paciência e carinho. Obrigada por acreditar em mim.

As amizades que construí ao longo da faculdade e para a vida, em especial a Agnes Geovanna, Danielly, Dayanne, Dyovana e Crislaine. Obrigada por todo apoio, conhecimentos, informações e materiais compartilhados ao longo desses anos, todos os aprendizados e boas memórias que vocês me proporcionaram dentro e fora dos corredores da nossa faculdade, tantos momentos que ficarão para sempre guardados.

Ao professor Germano Campos Silva pela atenção e alegria das orientações, pelo empenho, dedicação profissional e motivação para a conclusão deste trabalho.

Ao professor Walério Magalhães Bandeira, participante da banca examinadora pela disponibilidade, pelas valiosas colaborações, sugestões e ensinamentos.

A todos aqueles que passaram pelo meu caminho e tiveram algo a me ensinar durante os estágios e aos que colaboraram de forma direta ou indireta para o meu crescimento.

Logo, deixo o meu agradecimento a todos pelo apoio nos bons e maus momentos dessa jornada acadêmica. Hoje, sou o resultado de muita dedicação, força e persistência desses cinco anos do lado de cada um de vocês. Obrigada por tudo!

A LEI GERAL DE PROTEÇÃO DE DADOS N°. 13.709/2018: UM ESTUDO SOBRE OS AVANÇOS E A EFETIVIDADE JURÍDICA

Anna Klara Miranda Tobias

O artigo abordou sobre a temática da Lei Geral de Proteção de Dados nº 13.709/18, seus avanços e efetividade jurídica. Nesse sentido, o objetivo desse trabalho foi explicar e especificar a importância das garantias fundamentais a proteção de dados pessoais na atual sociedade da informação ao fazer uma abordagem sobre os aspectos principais da Lei. Por conseguinte, foi utilizado o método de abordagem hipotético-dedutivo que permite maior interação com o conteúdo a ser desenvolvido. O estudo teve também o caráter quantitativo, com ênfase na observação do cruzamento dos dados levantados com toda a pesquisa bibliográfica realizada. Em razão dos resultados e conclusões obtidos sobre o avanço e a efetividade da lei, aumenta a negociabilidade com o mercado exterior devido a adequação com legislações do exterior, a confiabilidade do usuário para com os serviços na rede, a responsabilidade das empresas e agentes de tratamento caso ocorra a violação de dados, a transparência das informações, segurança jurídica para o indivíduo e principalmente o respeito para com os princípios constitucionais. À vista disso, o trabalho busca analisar a forma que a lei irá diminuir as violações sofridas pelos no âmbito virtual, bem como a necessidade de as empresas estarem em conformidade com o novo regramento. Logo, a legislação se faz necessária acerca do tema, para, assim, evitar, a inobediência aos princípios constitucionais.

Palavras-chave: Proteção de dados. Privacidade. Sociedade informacional.

ABSTRACT

The article addressed the theme of the General Data Protection Law No. 13.709/2018, its advances and legal effectiveness. In this sense, the objective of this work was to explain and specify the importance of fundamental guarantees for the protection of personal data in the current information society when approaching the main aspects of the Law. Therefore, the hypothetical-deductive approach method that used allows greater interaction with the content to be developed. The study also had a quantitative character, with an emphasis on observing the crossing of the data collected with all the bibliographic research carried out. Due to the results and conclusions obtained on the progress and effectiveness of the law, negotiability with the foreign market increases due to the adequacy with laws from abroad, the user's reliability with the services on the network, the responsibility of the companies and treatment agents in the event of a data breach, transparency of information, legal certainty for the individual and especially respect for constitutional principles. In view of this, the work seeks to analyze the way in which the law will reduce the violations suffered by virtual users, as well as the need for companies to comply with the new regulation. Therefore, legislation is necessary on the subject, in order to avoid, therefore, disobedience to constitutional principles.

Keywords: Data protection. Privacy. Informational society.

SUMÁRIO

INTRODUÇÃO

Sob a perspectiva de uma sociedade da tecnologia da informação que permite uma maior amplitude das relações no meio digital. Nesse sentido, o seguinte estudou justificou-se pela necessidade de uma regulamentação sobre a proteção dos dados que circulam nas redes que é de grande importância, pois cada vez mais existe o aumento do compartilhamento de informações.

Diante desse cenário, em 2020 entrou em vigência a lei nº 13.709/2018, intitulada Lei Geral de Proteção de Dados (LGPD), a qual fez com que os cidadãos, Poder Público e empresas se adaptem a uma nova política de tratamento e compartilhamento de dados no Brasil.

Dessa forma, adotou-se como referencial teórico os fundamentos apresentados pelos seguintes doutrinadores, Patrícia Peck Pinheiro, Natália Masson, Ângelo Gamba Prata Carvalho e Ricardo Vieira Fernandes, deram estrutura a esse artigo científico

A metodologia utilizada nesse trabalho foi a abordagem hipotético-dedutiva, assim como foram utilizados artigos, dados estatísticos, legislações e outros materiais complementares.

Desse modo, objetivou-se analisar a importância das garantias fundamentais a proteção de dados pessoais na atual sociedade da informação abordando sobre os aspectos principais da Lei Geral de Proteção de Dados n.°13.709/2018.

Além disso, a problematização deu-se em torno dos seguintes questionamentos: Qual o impacto da lei na vida usuários? Por que a necessidade de uma lei para proteger os dados? Quais as medidas de segurança da lei para o indivíduo? Quais são os direitos protegidos pela lei?

Seguidamente, o trabalho abordou acerca da efetividade e avanço da lei, em razão do grande volume de vazamento e violação de dados, pois com o uso inadequado de dados pessoais pode causar danos ao indivíduo, tais como a privacidade, intimidade, sigilo e entre outras consequências.

À vista disso, a primeira sessão tratou da evolução da sociedade informacional e a vulnerabilidade das informações no âmbito virtual, as dificuldades da segurança da informação e como a privacidade e o sigilo são imprescindíveis para assegurar o titular dos dados.

Em sequência, a segunda sessão versou sobre as terminologias da lei, fundamentos e princípios que remetem a Carta Magna, a aplicação da lei sobre o

âmbito territorial e material, os requisitos para o tratamento adequado dos dados e o direito do indivíduo para com a legislação visto que é a parte mais prejudicada nas relações.

Nesse contexto, a terceira sessão aludiu sobre as figuras do tratamento de dados e a sua responsabilidade civil por danos, assim como as políticas existentes para uma boa prática de governança, a atividade da Autoridade Nacional de Proteção de Dados para com a orientação e fiscalização da norma e a aplicabilidade das sanções administrativa.

Logo, a Lei Geral de Proteção de Dados envolve toda a sociedade, as empresas e entidades públicas principalmente terão que se enquadrar às inovações. O direito tem papel fundamental na adaptação e criação de normas de acordo com os avanços sociais em vista das demandas tecnológicas.

1 A PRIVACIDADE DE DADOS NA SOCIEDADE DA INFORMAÇÃO

A revolução tecnológica e a comunidade pós-industrial formam a base histórica da sociedade informacional, este conceito relaciona-se com uma combinação de elementos que ensejam uma nova relação socioeconômica na modernidade. A internet e os avanços nas telecomunicações são componentes fundamentais nessa expansão, que é em sua essência computacional e informática.

Neste sentido, preceitua a autora Maria Julia Giannasi:

> A definição mais comum de Sociedade da Informação enfatiza as inovações tecnológicas. A ideia-chave é que os avanços no processamento, recuperação e transmissão da informação permitiram aplicação das tecnologias de informação em todos os cantos da sociedade, devido a redução dos custos dos computadores, seu aumento prodigioso de capacidade de memória, e sua aplicação em todo e qualquer lugar, a partir da convergência e imbricação da computação e das telecomunicações. (GIANNASI, 1999, p.21).

Nessa nova era marcada pelo intenso consumo de componentes digitais e dados informacionais é possível afirmar que, a internet tornou-se uma esfera pública de informações com alcance mundial voltada para a produção de conteúdo, dados e imagens que em muitos casos fica fora de controle e entra em evidente colisão aos direitos humanos fundamentais à informação, à privacidade de dados, sigilo e a intimidade.

No que se refere ao indivíduo, ele se torna representado por um perfil de dados, sejam eles, números, rotinas de gastos, compras pela internet. Esta é a nova

percepção do sujeito, que passa a reivindicar a proteção à privacidade, por se tratar de um direito fundamental, reconhecido como direito de personalidade, com características de indisponibilidade, intransmissibilidade, inalienabilidade e imprescritibilidade.

Nessa perspectiva, demonstra o autor Carlos Roberto Gonçalves:

> O reconhecimento dos direitos da personalidade como categoria de direito subjetivo é relativamente recente, como reflexo da Declaração dos Direitos do Homem, de 1789 e de 1948, das Nações Unidas, bem como da Convenção Europeia de 1950. No âmbito do direito privado, sua evolução tem-se mostrado lenta. No Brasil, têm sido tutelados em leis especiais e principalmente na jurisprudência, a quem coube a tarefa de desenvolver a proteção à intimidade do ser humano, sua imagem, seu nome, seu corpo e sua dignidade. O grande passo para a proteção dos direitos da personalidade foi dado com o advento da Constituição Federal de 1988, que expressamente a eles se refere no art. 5º, X, nestes termos: "X — 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." (GONÇALVES, 2011, p.152).

A privacidade em si, tradicionalmente é vista como o direito de estar sozinho e a salvo da percepção alheia, entretanto, em virtude das inúmeras tecnologias, elas permitem ao indivíduo estar inserido em um ambiente virtual coletivo a qualquer hora e lugar, sujeito a exposições públicas e opiniões diversas.

Ademais, em meio a esta sociedade da informação, surge o dilema que tange a proteção da personalidade e do direito à privacidade que lhe é inerente, em face de sua eventual violação e consequentes danos que podem ser irreparáveis aos que se encontram envolvidos.

Desta maneira, os instrumentos tecnológicos dos quais dispomos para aprimorar as relações sociais e econômicas nem sempre alcançam sua finalidade, pois além de serem utilizados de forma benéfica e democrática, eles podem também servir para a incitação do ódio e desrespeito.

À vista disso, a coletividade fica desprotegida em razão das ilicitudes cometidas no meio digital, como no caso de divulgação indevida de informações como fotos, vídeos e documentos pessoais.

Posto isto, a violação à intimidade, à honra e à imagem tem a sua devida importância e deve ser coibida e em caso de sua ocorrência no âmbito virtual, a comprovação de autoria se torna um pouco mais complexa do que deveria, em razão da dificuldade de identificação real do indivíduo por trás do dispositivo.

Em suma, a privacidade de dados na sociedade da informação é uma novidade,

visto que nesse novo cenário socioeconômico pautado pelas novas tecnologias com o modo de vida e comunicação das pessoas foi alterado, à medida em que as conexões se tornam mais rápidas e interativas.

1.1 A ERA DOS DADOS NA INTERNET E A VULNERABILIDADE DE SISTEMAS

É imprescindível afirmar que nos encontramos em uma era de dados informacionais, a qual dependemos da tecnologia, como prova disso é comum ver grandes empresas do ramo da tecnologia no topo do valor de mercado, por exemplo, a Google, Apple e Amazon, em meio a tantas informações é necessário que as organizações estejam cada vez mais rápidas, variadas e precisas, pois os dados são o novo combustível das tecnologias atuais.

Conforme nos expõe o autor Carl Sagan:

> [...] criamos uma civilização global em que elementos cruciais – como as comunicações, o comércio, a educação e até a instituição democrática do voto – dependem profundamente da ciência e da tecnologia. (SAGAN, 1997, p. 37)

Nesse sentido, a era informacional de dados é uma realidade, a medida em que nos relacionamos com o outro de forma interativa via web e sempre estamos conectados o tempo todo, independente de lugar e hora, a possibilidade de fazer coisas simultaneamente por meio de um aparelho celular ou computador, facilita a rotina do usuário e como consequência os torna geradores de dados e informações.

Assim sendo, elucida Ana Cavalcanti e Samyra Sanches:

> De forma resumida, podemos, numa ordem cronológica, dizer que a sociedade passou da economia agrícola [...] para a economia industrial [...], e, por último (a partir de 1960 até o presente momento), para a economia informacional. [...] destaca três ondas de transformações da sociedade: a primeira onda é a da economia agrícola, tendo por base a propriedade da terra como instrumento de poder; a segunda onda é a industrial, em que a riqueza é proveniente da combinação de trabalho, propriedade e capital e, finalmente, a terceira onda, conhecida como a informacional, iniciada com os grandes veículos de comunicação e da tecnologia digital. (CAVALCANTI; SANCHES, 2018, p. 04)

A respeito dessa nova revolução, as tecnologias da informação avançam de maneira rápida, as principais mudanças notáveis com o progresso tecnológico, será no âmbito da internet das coisas, inteligência artificial, impressões 3D, utilização de realidade aumentada, drones, bem como a autonomia do maquinário agrícola. Esse

desenvolvimento vai tornar o trabalho mais rápido, eficiente e seguro e para que isso dê certo, é fundamental muita informação e conectividade, além de leis adaptadas a essa realidade.

No entanto, quando se trata de problemas no campo da tecnologia, o maior deles é a segurança da informação, segundo o estudo anual da IBM (International Business Machines Corporation) em parceria com o Instituto Ponemon, chamado de “Custo de Violação de Dados 2017”, foi revelado um aumento histórico de incidentes nesse âmbito.

Nesse sentido, o resultado do estudo supramencionado está publicado no portal www.tiiside.com.br, o qual apontou que o valor para reparar as invasões virtuais foi cerca de R$ 4.72 milhões, distribuídos em despesas com investigação, controle de danos, reparos, ações judiciais e multas, sendo assim, a cada ano torna-se mais difícil e caro o gerenciamento de crise sobra a vulnerabilidade de dados.

Em comparação ao ano de 2016, a quantia gasta era de R$ 4.31 milhões e ao realizar esse levantamento, foram avaliadas 166 organizações de 12 segmentos. Consoante a pesquisa, os ataques maliciosos são uma das principais causas da violação de dados, em cerca de 44% dos casos, nas posições seguintes estão: falhas humanas, com 31%, falha nos sistemas 25%. As empresas mais afetadas foram aquelas voltadas para as indústrias de serviços, finanças e tecnologia.

A empresa Cisco Systems, apresentou um levantamento que dentre 115 mil aparelhos conectados a redes empresariais, cerca de 106 mil apresentaram vulnerabilidades conhecidas de softwares. Em razão disso, a Lei Geral de Proteção de Dados n° 13.709/2018, dispõe sobre várias questões a respeito de como legislar no âmbito virtual, bem como é preciso uma política efetiva de proteção, que requer investimento tecnológico e mudança de cultura.

Os sistemas de informação a todo momento estão recolhendo dados pessoais dos usuários, dessa forma, a privacidade é essencial pois a medida em que ocorre alguma exposição indevida, o titular acaba sendo prejudicado, bem como a empresa que teve acesso a esses dados que arcará com as devidas responsabilidades.

Para que exista uma melhora na coleta de informações, tratamento e armazenamento de dados é necessário a adoção de medidas cabíveis e a adequação a Lei Geral de Proteção de Dados nº 13.709/2018, que fora inspirada na lei da União Europeia GDPR e busca trazer medidas de segurança e transparência aos usuários brasileiros.

No que diz respeito a vulnerabilidade de sistemas, ela é uma fragilidade que permite a um sujeito restringir a garantia da informação de um sistema, é a ligação entre a falha ou suscetibilidade de falha no sistema, o acesso a falha e a capacidade de utilizá-la em seu benefício.

À vista disso, para que ocorra o ataque o indivíduo deve dispor de no mínimo um meio de instrumento e estratégia que possa favorecer a conexão dele a uma vulnerabilidade do sistema, que pode ser entendida também como uma superfície de ataque e que consequentemente termina em um rompimento de segurança quando efetuado com sucesso.

Os grandes facilitadores de ações de hackers ou usuários mal intencionados, são os sistemas ultrapassados, que não possuem as devidas melhorias em termos de proteção ao usuário e atualizações, esses consequentemente estão mais propensos a ataques. A seguridade desses institutos é uma recomendação expressa, porém, muita das vezes as empresas não seguem uma estratégia adequada, a fim de atender as necessidades do seu ambiente.

Ao realizar transações online é preciso ter bastante cuidado quanto ao compartilhamento de informações, as invasões podem ocorrer a partir de várias origens, basta apenas uma conta de e-mail para estar sujeito a um tipo de ataque comum, o *phishing,* que consiste no furto de dados de forma “mascarada”, por meio de um site falso do banco por exemplo e que dá acesso a números de cartões de crédito, contas bancárias, senhas e outros dados pessoais sensíveis.

À frente disso, temos o crescimento dos ataques, sendo assim, é preciso que exista o investimento por parte das empresas em equipes especializadas, aparelhos mais modernos e o estímulo a segurança. Além disso, com a gestão adequada de vulnerabilidade juntamente com a aplicação da legislação é possível minimizar os ataques que acarretem grandes prejuízos aos envolvidos.

No que tange as determinações referentes a Lei Geral de Proteção de Dados nº 13.709/2018, é indispensável, que as empresas possam garantir a boa prática de governança e a privacidade de dados, conforme estabelecido na mencionada lei as regras sobre a segurança no controle, coleta, armazenamento e transmissão de dados pessoais na rede, exigem que a empresa obtenha o consentimento do titular dos dados, fato que assegura a identificação e proteção das informações em um banco de dados mais amplo.

Logo, a segurança cibernética é uma decisão estratégica dentro da empresa

em vista dos ataques, planejar uma adequação as novas normas são essenciais e indispensáveis, porém requer tempo e envolve a identificação de riscos e a análise dos respectivos problemas encontrados até que, enfim, chegue a uma solução.

1.2 O DIREITO À PRIVACIDADE E SIGILO DE DADOS

O progresso tecnológico das últimas décadas relacionado a utilização das novas formas de comunicação via *web*, é um grande marco do século XXI. A acessibilidade de forma prática e instantânea que ocorre na internet faz com que o armazenamento de informações, consequentemente de dados pessoais contribuem para uma nova transformação da sociedade.

Diante disso, essa inovação trouxe consigo alguns questionamentos para o ordenamento jurídico e para ciência em geral, no que tange aos direitos humanos, mais especificamente à aqueles que são necessários para assegurar a vida do indivíduo, tais como: a vida privada, a intimidade e o sigilo de dados, dado que a vulnerabilidade dos sistemas se torna cada vez mais frequente, ocasionando a violação ou a quebra de sigilo dos meios de comunicação eletrônicos, acarretando a diminuição ou retirada do caráter privativo das informações.

Neste contexto, os autores Pablo Stolze Gagliano e Rodolfo Pamplona Filho assim se manifestam:

> Com o avanço tecnológico, os atentados à intimidade e à vida privada, inclusive por meio da rede mundial de computadores (Internet), tornaram-se muito comuns. Não raro, determinadas empresas obtêm dados pessoais do usuário (profissão, renda mensal, hobbies), com o propósito de ofertar os seus produtos, veiculando a sua publicidade por meio dos indesejáveis spams, técnica ofensiva à intimidade e à vida privada. (FILHO; GAGLIANO, 2008, p.106)

À vista disso, o direito à privacidade tem grande relevância para essa sociedade informacional, é fundamental a toda e qualquer pessoa, bem como a proteção da integridade moral do sujeito, o artigo 12 da Declaração Universal dos Direitos do Homem, de 1948, dispõe: "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".

Nesse sentido a autora Nathalia Masson expõe:

> A privacidade representa a plena autonomia do indivíduo em reger sua vida do modo que entender mais correto, mantendo em seu exclusivo controle as

> informações à sua vida doméstica (familiar e afetiva), aos seus hábitos, escolhas, segredos, etc., sem se submeter ao crivo (e à curiosidade) da opinião alheia. (MASSON, 2015, p.218)

A matéria que concerne à privacidade no Brasil está estabelecida no artigo 5º, inciso X, da Constituição Federal de 1988, a qual versa: “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”. Entretanto, é notório ressaltar que esse direito não deve ser definido unicamente pelo segredo ou modo de “estar só”, visto que, com o aumento das interações via *web*, são poucas as informações que ainda se encontram em sigilo absoluto.

A falta de precaução com ações executadas no meio virtual é intrigante, a quantidade de informações e dados obtidos por meios ilegais tem aumentado, não existe um controle adequado para que essas situações sejam coibidas, dentre elas estão a coleta de informações sem o consentimento do usuário e por meio de compras na rede, ocasionando traçamento do perfil do indivíduo e até mesmo a partir do acesso em vários endereços *web*.

Nos casos mencionados, o Superior Tribunal Justiça (STJ) manifesta no sentido da retirada da possibilidade do uso de imagem ou dados que foram adquiridos por meio ilícito e sem a autorização do titular, como no disposto a seguir:

> Com o desenvolvimento da tecnologia, passa a existir um novo conceito de privacidade, sendo o consentimento do interessado o ponto de referência de todo o sistema de tutela da privacidade, direito que toda pessoa tem de dispor com exclusividade sobre as próprias informações, nelas incluindo o direito à imagem. (REsp 1168547 / RJ RECURSO ESPECIAL 2007/0252908-3 Ministro LUIS FELIPE SALOMÃO (1140) T4 - QUARTA TURMA 11/05/2010 DJe 07/02/2011).

Nesse sentido, a Lei Geral de Proteção de Dados Pessoais nº 13.709/2018, também estabelece em seu artigo 7º inciso I, como condição para que seja realizado o tratamento de dados pessoais, o fornecimento do consentimento dado pelo titular das informações, a fim de garantir a segurança aos envolvidos.

Posto isso, outra problemática acerca da intimidade e privacidade são as informações prestadas em cadastros virtuais quanto mais a utilização, maior o compartilhamento de informações, o que por um lado facilita a prestação de serviço para empresa e por outro pode acarretar o acesso para usuários de má fé.

Nessa perspectiva, é abordado no Código de Defesa do Consumidor em seu artigo 43 parágrafo 2º, em que estabelece a qualquer consumidor ter acesso as informações existentes em cadastros, registros, fichas e dados pessoais relativos a ele, bem como a abertura de qualquer um dos anteriores deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.

No que diz respeito a inviolabilidade do sigilo de dados no artigo 5º, inciso XII dispõe que é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, em casos que possuem ordem judicial e para fins de investigação criminal ou processual penal. Dessa forma, pode-se considerar uma norma correlata ao direito fundamental à privacidade disposto pelo artigo 5º, inciso X, visto que ambas visam resguardar as informações veiculadas pelos cidadãos e a sua vida privada.

O sigilo em si, nada mais é que um segredo a não ser revelado e ao que se trata do sigilo de correspondências, é importante afirmar que os dados e informações ali prestadas não podem ser violados, sob o risco de penalidades. Ao estender esse entendimento ao momento aos avanços da sociedade, com a comunicação por e-mails, aplicativos de mensagens, torna complicado preservar o sigilo e a privacidade dos indivíduos.

Nesse contexto aborda a autora Nathalia Masson:

> Os dados que podem revelar aspectos da privacidade de um indivíduo ficam resguardados sob sigilo, em inédita proteção constitucional, introduzida pela Constituição Federal de 1988 no inciso XII do art. 5º. [...] estes são os chamados dados sensíveis referentes às informações telefônicas, bancárias e fiscais da pessoa, bem como à sua orientação sexual, crença religiosa, e o valor de sua remuneração. Qualquer intervenção estatal direcionada a romper o sigilo desses dados deverá ser devidamente fundamentada e somente poderá ser determinada pela autoridade competente [...]. Por fim, quanto aos dados não sensíveis, é bom frisar que não estão protegidos pelo sigilo, pois são informações públicas e de livre circulação por terceiros. Para exemplificar, pensemos no nome do sujeito, no seu estado civil, na sua filiação, o número de CPF, no seu endereço ou -mail. (MASSON, 2015, p.223)

Deste modo, a Lei Geral de Proteção de Dados Pessoais nº13.709/2018, regulamenta sobre o tratamento de dados sensíveis à medida que versa sobre a qualificação dos dados sensíveis, em seu artigo 5º, inciso II, é todo aquele “dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural”. Assim sendo, em consequência da proteção

legislativa, o trânsito das informações pode-se tornar mais eficaz preservando o estado democrático de direito.

2 CONSIDERAÇÕES SOBRE A LEI GERAL DE PROTEÇÃO DE DADOS

No tocante do desenvolvimento econômico global e a crescente inovação tecnológica, tornou-se necessário a formulação de legislações específicas que versem sobre a proteção de dados, as quais tenham por finalidade garantir aos cidadãos uma maior segurança jurídica em relação a tramitação de informações e dados pessoais no âmbito virtual.

Sobre esse aspecto argumenta a autora Patrícia Peck Pinheiro:

> O motivo que inspirou o surgimento de regulamentações de proteção de dados pessoais de forma mais consciente e consolidada a partir dos anos 1990 está diretamente relacionado ao próprio desenvolvimento do modelo de negócios da economia digital, que passou a ter uma dependência muito maior dos fluxos internacionais de base de dados, especialmente relacionados às pessoas, viabilizados pelos avanços tecnológicos e pela globalização. (PINHEIRO, 2020, p.17)

Em razão do grande volume de armazenamento e compartilhamento simultâneo em diversas plataformas, os dados que antes eram fornecidos e mantidos de forma física ganham espaço e praticidade em áreas da *web*, permitindo um maior controle para aqueles que os tratam.

Os primeiros marcos regulatórios a respeito da proteção de dados se iniciaram por volta da década de 1970 e atualmente se encontram estabelecidos em quase todo o mundo. Em virtude das pesquisas realizadas pela UNCTAD (United Nations Conference on Trade and Development – Conferência das Nações Unidas sobre Comércio e Desenvolvimento), entre 195 nações cerca de 132 possuem algum tipo de normatização acerca da privacidade e proteção de dados.

Ao que concerne o cenário internacional, dentre as leis com maior impacto e influência está a Lei da União Europeia, a GDPR (General Data Protection Regulation-Regulamento Geral de Proteção de Dados). A GDPR inspirou a legislação brasileira, a LGPD (Lei Geral de Proteção de Dados), que passa a englobar regras do mesmo nível em que as regulações mais pertinentes do assunto no âmbito mundial.

Por conseguinte, com a aprovação da LGPD o Brasil integra o grupo de países que possuem legislações exclusivas que regulamentam a política de privacidade de dados pessoais. A fim de garantir os direitos constitucionais, bem como estimular o

desenvolvimento da economia e da inovação por meio da transparência na utilização, compartilhamento e armazenamento de dados pessoais.

Nesse sentido, atesta a Professora Laura Schertel Mendes:

> A importância do modelo de lei geral reside no fato de que ela constrói uma arquitetura regulatória que busca consolidar o tema de proteção de dados pessoais como um setor de políticas públicas, composto por instrumentos estatutários, sancionatórios, assim como por um órgão administrativo, responsável pela implementação e aplicação da legislação. (MENDES, 2014, p. 58)

À vista disso, a legislação brasileira não previa de forma específica o direito a proteção de dados, o assunto era tratado de forma superficial, era assegurado por leis esparsas e pelos os direitos fundamentais abarcados pela Carta Magna em seu artigo 5º, inciso X e XII de forma que a proteção de dados propriamente dita só foi ensejada a partir do advento da Lei Geral de Proteção de Dados.

Nessa perspectiva constitucional, a especialista Patrícia Peck Pinheiro versa:

> É evidente que o direito à privacidade constitui um limite natural ao direito à informação. No entanto, não há lesão a direito se houver consentimento, mesmo que implícito, na hipótese em que a pessoa demonstra de algum modo interesse em divulgar aspectos da própria vida. Assim como há limites naturais ao direito à privacidade quando atinge interesses coletivos. Neste caso, a predominância do interesse coletivo sobre o particular requer verificação caso a caso. (PINHEIRO, 2013, p.43)

Nesse contexto, o caminho percorrido para a promulgação da LGPD fora bastante moroso e vinha tramitando no parlamento desde o ano de 2012, ao ser sancionada pelo ex-Presidente Michel Temer no dia 14 de agosto de 2018 e depois publicada no Diário Oficial da União (DOU).

A sua vigência ocorreria nos próximos 18 meses, o que de fato não aconteceu, decorreram-se assim vários vetos dentre eles um que impossibilitava a criação da Agência Nacional de Proteção de Dados (ANPD), que é a entidade fiscalizadora do cumprimento da Lei Geral de Proteção de Dados que depois foi aprovada e sancionada pelo presidente Jair Bolsonaro como a Lei nº 13.853/2019.

A LGPD tinha a previsão de vigência a partir do ano de 2021 desde que fosse findado o período de crise na saúde pública em razão da pandemia de COVID-19, apesar do ocorrido, o Senado Federal aprovou a vigência para a data de 18/09/2020 e em suas disposições finais, prorroga para 1º de agosto de 2021 a aplicação sanções administrativas da respectiva lei.

Nesse aspecto, a partir do mês de agosto de 2021, a ANPD terá autoridade

para aplicar sanções administrativas na forma de multas de até 2% do faturamento com limite de até R$ 50.000.000 (cinquenta milhões de reais).

Vale ressaltar que, a Lei Geral de Proteção de Dados tem por objetivo a autonomia dos titulares perante os seus dados, entendam os motivos da coleta de informações e decidam qual empresa pode ou não ter acesso a eles. A legislação também inova resguardando tanto as informações digitais, quanto físicas, por exemplo, aquelas obtidas em formulários presenciais.

Sob essa ótica, com a vigência da lei, as organizações estão buscando se adequar as medidas impostas, sendo assim, quando os usuários adentram aos *sites* estão recebendo avisos de *cookies*, que são arquivos criados pelos *websites* tornando a navegação mais econômica e fácil.

Os *cookies* são responsáveis por identificar e armazenar informações sobre os usuários visitantes, bem como podem lembrar as preferências e fornecer um conteúdo de forma mais assertiva ao estabelecer o perfil consumidor de cada usuário.

Posto isso, o que se refere a tempos anteriores os dados eram armazenados sem a devida autorização do usuário e nem sempre as empresas adequam as notificações de *cookies* da forma correta, em alguns casos ainda não é possível fazer a recusa de acesso a eles, o que afeta o direito de privacidade do usuário.

2.1 DEFINIÇÕES E PRINCÍPIOS ESTABELECIDOS NA LEI

A partir dos fatos mencionados anteriormente, a LGPD veio para trazer legitimidade as questões jurídicas relacionadas a proteção de dados dos cidadãos. Em razão disso, ela apresenta fundamentos, terminologias e princípios que são essenciais e devem ser objeto de estudo e interpretação adequada para que exista uma boa aderência.

Nesse seguimento, pode-se abordar que os principais fundamentos tratados no artigo 2º da lei, são acerca do respeito a privacidade, liberdade de expressão informação, comunicação e opinião, inviolabilidade da intimidade, direitos humanos e a dignidade, de modo que muitos desses elementos encontram-se na Constituição Federal.

À vista disso, abordam os autores Márcio Cots e Ricardo Oliveira:

> [...] o Direito passou a atribuir a privacidade o status de direito fundamental da pessoa humana, como podemos verificar no artigo 12, da Declaração Universal dos Direitos Humanos, no inciso X do artigo 5º da Constituição Federal brasileira, disposição que passou a emanar efeitos a outros diplomas

> legais, como é o caso do Código Civil, Marco Civil da Internet, entre outros, entre os quais se encontra a LGPD. (COTS; OLIVEIRA, 2019, p.51)

Em seguida, ao que se trata das definições é possível abordar sobre o titular dos dados que é caracterizado pelo artigo 5°, inciso V da respectiva lei, como sendo a pessoa natural a quem se referem os dados pessoais que são objetos de tratamento.

Nesse sentido os autores Angelo Carvalho e Ricardo Fernandes abordam:

> Nessa esteira, ao titular dos dados é assegurada uma série de direitos subjetivos frente ao responsável pelo tratamento destes. Destacam-se a garantia da confirmação da existência de tratamento; o amplo acesso aos dados quando requisitado; a anonimização, bloqueio ou eliminação de dados desnecessários ou excessivos; a portabilidade de dados pessoais a outro fornecedor de serviço ou produto; e a revogação do consentimento. (CARVALHO; FERNANDES, 2018, p.356)

Outro ponto é a definição de tratamento de dados que é tida também no artigo 5º, inciso X como a operação realizada com as informações pessoais, bem como as atividades que envolvem a coleta, produção, acesso, utilização, armazenamento eliminação, entre outros aspectos.

Nessa perspectiva, os autores Angelo Carvalho e Ricardo Fernandes expõem:

> Como é possível observar, diversas são as atividades que englobam o tratamento de dados. Em linhas gerais, na dinâmica do Big Data, os dados são coletados das mais variadas formas, como em transações comerciais, pesquisas de mercado e de estilo de vida, censo de registros e interações em meios digitais. O armazenamento se dá em enormes bancos de dados, isto é, um “conjunto estruturado de dados pessoais, localizado em um ou em vários locais, em suporte eletrônico ou físico. O processamento consiste em técnicas de análise e refinamento dos dados, com o intuito de deles extrair informações úteis e valiosas. Por fim, a difusão está associada à ideia de mercado de dados pessoais, que pode ser entendida como interações econômicas voltadas à compra e venda de informações. (CARVALHO; FERNANDES, 2018, p.356)

Ademais, o conceito de dados pessoais que está definido no artigo 5º, inciso I como as informações de uma pessoa natural, passíveis de identificação ou já identificadas, possuindo ramificações como os dados “sensíveis” estabelecidos pelo inciso II e estão relacionadas a características particulares dos indivíduos bem como suas escolhas pessoais.

A lei também intitula quem serão os agentes responsáveis para a realização do tratamento de dados, o controlador, o operador e o encarregado que são descritos conforme o artigo 5º, inciso VI, VII e VIII como pessoas naturais ou jurídicas, de direito público ou privado, cabendo a recepção de dados, decisões, execução e comunicação

das informações entre os envolvidos.

Nesse seguimento, existe ainda a anonimização e abordada no mesmo artigo nos incisos XI que é utilização de meios técnicos, dos quais um dado é impossibilitado de associar-se de maneira direta ou indireta ao indivíduo.

Em seguida o inciso XII trata do consentimento como sendo uma manifestação livre, informada e inequívoca para a concretização do acolhimento de dados por uma instituição, não sendo o único motivo para autorizar o tratamento de dados, mas sim uma das hipóteses estabelecidas pelo artigo 7° da LGPD.

Sob o prisma do consentimento e a liberdade do indivíduo de pensamento e manifestação, versa a especialista em constitucional Nathalia Masson:

> Insta destacar que ao titular dessa liberdade permite-se expressar sentimentos ideias e impressões de variadas formas, seja por mensagens faladas ou escritas, como também por gestos, expressões corporais, imagens, etc. Até mesmo manter o silêncio é prerrogativa aqui assegurada, já que ninguém pode ser forçado por particulares ou pelo Estado a se manifestar sem vontade. Em sum, todas as maneiras que o indivíduo possui para se exprimir encontram guarida constitucional. (MASSON, 2015, p.239)

À vista disso, os princípios são indispensáveis ao ordenamento jurídico, dessa forma, nesse sentido a LGPD versa em seu artigo 6º as premissas que devem ser seguidas: a boa-fé, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

Destarte, dentre os princípios citados, tem-se como um dos principais o da finalidade, minimização da coleta e o da retenção mínima, eles significam que à medida em que os dados são utilizados para atos específicos eles devem atender ao seu fim determinado, cabendo a observação de que somente os dados minimamente necessários devem ser coletados e a possibilidade de exclusão imediata dos dados após o cumprimento de sua função.

2.2 APLICAÇÃO TERRITORIAL E MATERIAL

Ao que diz respeito a aplicação territorial e extraterritorial das normas da LGPD, é explanado no art. 3º o qual define: “aplica-se a qualquer operação de tratamento de dados realizada por pessoa natural ou pessoa jurídica de direito público ou de direito privado, independente do meio, do país de sua sede ou do país onde estejam localizados os dados”. Dessa forma, as normas da LGPD em seu alcance nacional

devem ser obedecidas pela União, Estados, Distrito Federal e Municípios.

Nesse entendimento, as atividades de tratamento de dados pessoais, bem como a aplicação da lei no âmbito nacional e internacional, estão descritas nas hipóteses do art.3º da LGPD, como as operações ocorridas no território nacional, as atividades que tiverem por objetivo a oferta ou o fornecimento de bens ou serviços no Brasil ou que os dados estejam localizados no território e se os dados pessoais forem coletados no país.

Sob essa ótica, segue o entendimento da especialista e autora Patrícia Peck Pinheiro:

> A LGPD tem alcance extraterritorial, ou se, efeitos internacionais, na medida em que se aplica também aos dados que sejam tratados fora do Brasil, desde que a coleta tenha ocorrido em território nacional ou por oferta de produto ou serviço para indivíduos no território nacional ou por oferta de produto ou serviço para indivíduos no território nacional ou que estivessem no brasil. Desse modo, os dados pessoais tratados por uma empresa de serviço de *cloud computing* que armazene o dado fora do país terá que cumprir as exigências da LGPD. (PINHEIRO, 2020, p. 40)

É importante ressaltar que a lei não é aplicada em relação a residência ou no domicílio do titular dos dados, mas sim com base na sua localização da coleta dos dados no Brasil, diferentemente das normas de competência processual civil e penal, bem como da aplicação territorial estabelecida pela Lei de Introdução às normas do Direito Brasileiro (LINDB) que utilizam o domicílio do indivíduo.

A cerca do assunto, a autora Patrícia Peck Pinheiro expõe:

> A delimitação da aplicabilidade da lei em relação aos tipos de dados que são considerados regulados pela LGPD demonstra que o tratamento de dados pessoais deve seguir um proposito certo e funcional, mas que não supere a liberdade de informação e expressão, a soberania, segurança e defesa do Estado. Da mesma forma, o uso doméstico com fins não econômicos não recebe a aplicação da lei, tendo em vista que um dos focos de ação do dispositivo é regular as atividades cujo objetivo seja oferta ou fornecimento de bens ou serviços. (PINHEIRO, 2020, p. 77)

A LGPD apenas faz menção ao termo “localizados” que se refere aos titulares dos dados. Desse modo, a sua localização é um dos parâmetros para determinar a aplicação da lei, outra informação é que ao indivíduo mesmo que estrangeiro aceitar os termos de uso de tratamento de dados no Brasil, estará sujeito a aplicação da lei.

Nessa perspectiva, a utilização da localização é algo complexo, pois quando o titular acessa a internet é possível modificar o lugar do endereço de IP (Internet Protocol – Protocolo de Internet) que representa um conjunto de regras para a

comunicação pela internet para que exista a troca de informações com um site, ele é protocolo que identifica uma rede ou um dispositivo na internet, trata-se de um número único que comporta identificação de cada aparelho por meio de uma rede privada virtual (VPN – *Virtual Private Network*) .

Ao que diz respeito a esse processo de alteração de IP, em regra ele não é feito para fins ilícitos, a exemplo disso, o próprio buscador Google faz isso em prol da proteção da segurança e privacidade *online* do usuário tornando difícil a localização exata do utilizador. Logo, o reconhecimento do local de tratamento de dados pessoais e a descrição na legislação não é simples e pode-se demonstrar controversa nesse ponto.

Cabe mencionar ainda, quais são as situações de inaplicabilidade da LGPD que estão estabelecidas em seu art. 4º:

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos; II - realizado para fins exclusivamente: a) jornalístico e artísticos; ou b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei; III - realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais; ou IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei. (Brasil, 2018)

Nesse cenário, em razão da preocupação da privacidade de dados para fins comerciais, não é viável a exigência para o cidadão que possui informações pessoais de amigos e familiares em celulares, atender as medidas impostas pela LGPD, levando em consideração os custos envolvidos, tais como a contratação de profissionais especializados, a aquisição de sistemas de segurança da informação entre outros.

Em suma, para a aplicação da LGPD deve ser observada a localização onde foi realizada a coleta das informações, visto que é uma exceção à regra o domicílio do da pessoa, atentando-se também as configurações de IP que podem alertar sobre diferentes locais gerando assim conflitos de interesses.

2.3 REQUISITOS PARA O TRATAMENTO DE DADOS E OS DIREITOS DO TITULAR

No que tange aos requisitos para o tratamento de dados definido pela LGPD em seu art. 7º, foram estabelecidas hipóteses, sendo assim, o parágrafo 3º alude que a coleta dos dados do titular, deve ser necessária para a execução da finalidade específica, aplicando-se também a transferência de dados entre as empresas, exceto nos casos de legítimo interesse do controlador, predominando os direitos e as liberdades fundamentais do indivíduo.

Nesse âmbito discorre a especialista na área digital, Patrícia Peck Pinheiro:

> Outro ponto da LGPD que demonstra influência da GDPR na criação do documento brasileiro diz respeito aos requisitos aplicados ao tratamento de dados pessoais. A LGPD destaca que o tratamento de dados pessoais deve observar a boa-fé e possuir finalidade, limites, prestação de contas, garantir a segurança por meio de técnicas e medidas de segurança, assim como a transparência e possibilidade de consulta aos titulares. (PINHEIRO,2020, p.84)

Por conseguinte, sobre o artigo 7º, inciso VII cabe mencionar sua importante ênfase a respeito da tutela do tratamento de dados nos casos em que for necessário proteger a vida, a incolumidade física do titular, bem como de terceiros. Desse modo nota-se a relevância disposição dessa na lei, visto que a vida é o maior bem jurídico do nosso ordenamento.

Nesse ponto de vista, segue o disposto pela autora de constitucional Nathalia Masson:

> A vida humana é o bem jurídico mais importante dentre todos os direitos constitucionalmente tutelados, afinal, estar vivo é um pressuposto elementar para se usufruir dos demais direitos e liberdades garantidos na Constituição Federal. (MASSON, 2015, p.212)

O consentimento do titular de dados é imprescindível para a coleta de dados no meio virtual, em razão do aumento da vulnerabilidade das informações contidas na *web*. Nesse sentido no art. 8 da LGPD evidencia que o consentimento deve ser demonstrado por meio escrito ou outro modo que prove a sua manifestação, tendo em vista que o silêncio ou omissão não são considerados, possuindo livre escolha de recusa e revogação.

Sob esse aspecto alude a autora Patrícia Peck Pinheiro:

> Ao mesmo tempo, as empresas devem ter a liberdade de utilizar os dados de maneira transparente e ética em troca de um serviço ou acesso, tendo em vista que o desenvolvimento econômico também deve ser garantido a esses sujeitos. Importante destacar que cabe à instituição que realiza o tratamento

> a capacidade de demonstrar que estava legítima (detinha o registro do consentimento ou se enquadrava nas hipóteses de exceção). Como já observado, considerando o cenário brasileiro de preocupação com segurança, houve cuidado com a questão de trazer garantias de exceções de consentimento, por exemplo na situação da proteção de crédito. (PINHEIRO, 2020, p.85-86)

Em relação a transparência das informações, o art. 9 da LGPD apresenta que o titular tem o direito do acesso facilitado, disponibilizado de forma clara e adequada para atender o princípio do livre acesso à informação, assegurada a gratuidade na prestação das informações.

Conforme, o art. 10 da LGPD quando existir o legítimo interesse do controlador ele deverá fundamentar as finalidades necessárias para o ato e somente utilizará os dados reais estritamente precisos, tendo em vista, as garantias jurídicas a proteção de privacidade do usuário.

Há, também, o tratamento de dados pessoais denominado como “sensível” (inciso II, do art. 5º da LGPD), eles exigem mais cautela pois tratam sobre a origem racial ou étnica, convicções religiosas ou filosóficas, opiniões políticas, filiação sindical, questões genéticas, biométricas e sobre a saúde ou a vida sexual de uma pessoa, desde que com o seu consentimento explicito.

A respeito dos direitos do titular de dados é importante ressaltar que o art. 17 reforça a importância da titularidade dos dados, a pessoa física será resguardada no âmbito do direito a intimidade, liberdade e privacidade garantidos na Constituição Federal, cabendo as entidades operadoras e controladoras informar e cumprir com o estabelecido.

Nesse seguimento, entende a autora Patrícia Peck Pinheiro:

> Um dos objetivos da LGPD é assegurar a proteção e o livre desenvolvimento da personalidade da pessoa natural. É possível relacionar essa garantia da pessoa natural à titularidade de seus dados à inviolabilidade de sua vida privada, pontuada por meio do art. 5°, X, da Constituição Federal e do art. 21 do Código Civil, haja vista que as informações pessoais da pessoa fazem parte de sua privacidade, ainda mais no contexto digital. (PINHEIRO,2020, p.99)

À vista disso, algumas garantias expressas ao titular dos dados são: a confirmação da existência do tratamento e seu acesso, a correção de dados incompletos, inexatos ou desatualizados, anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade, portabilidade dos dados a outro fornecedor de serviço ou produto, a revogação do consentimento, dentre outros.

Nesse aspecto versa a especialista Patrícia Peck Pinheiro:

> O direito dos titulares dos dados de livre acesso às informações relativas ao tratamento é reiterado de maneira enumerativa pelo art. 18, cuja a preocupação é garantir que o titular possa assegurar que seus dados estão sendo tratados de forma segura, verídica e cumprindo a sua finalidade. (PINHEIRO, 2020, p.101)

Por fim, os art. 21 e 22 da LGPD, ambos visam resguardar o titular no sentido de que em nenhum momento, as informações que forem coletadas podem ser utilizadas para seu prejuízo e caso alguma ação resulte em dano, poderá o indivíduo recorrer a defesa de seus interesses em juízo, seja de forma individual ou coletiva, bem como ilustra o art. 5, XXXIV, da Constituição Federal que assegura a todos o direito de acesso à justiça e defesa de direitos dos cidadãos.

3 A LEI GERAL DE PROTEÇÃO DE DADOS E A RESPONSABILIDADE DOS AGENTES DE TRATAMENTO

A Lei Geral de Proteção de Dados, dispõe em seu Capítulo VI seção I e II, sobre os agentes de tratamento de dados pessoais, sendo eles: o controlador a quem compete as decisões relativas ao tratamento, o operador que realiza o tratamento em nome do controlador e por fim, o encarregado que com autonomia e estabilidade, é o responsável por atender as demandas dos titulares, interagir com a autoridade nacional e orientar os contratados quanto às práticas de proteção de dados pessoais.

Ao que concerne a responsabilidade civil na LGPD, cabe ressaltar que as diretrizes não serão aplicáveis em todos os casos, dependendo da relação jurídica estabelecida propiciando o alcance de outras áreas do direito, como o direito do consumidor que é reconhecido pela referida lei em seu art. 45 a qual menciona que quando houver violação de direito do titular nas relações de consumo, cabe a regra da legislação específica.

Nesse seguimento, a LGPD o art. 42, abarca a responsabilidade civil alternada do controlador ou operador, caso a relação jurídica for de natureza consumidora, serão empregadas as normas do código de consumidor. O parágrafo 1º excepciona a regra do caput, permitindo a responsabilidade solidária em dois casos específicos para que exista efetiva indenização ao titular.

Desse modo, na primeira situação, o operador terá responsabilidade solidária quando descumprir a LGPD ou não obedecer a orientações lícitas do controlador, no segundo caso a solidariedade será entre os controladores que designarem em grupo, medidas que infrinjam a proteção de dados ou às regras técnicas cabíveis, sendo

assim, cabe a dispensa da solidariedade nos casos em que forem atendidas as exigências do art. 43 da lei, dentre as quais estão a culpa for exclusiva da vítima.

Ao que tange o disposto do art. 42 parágrafo 2º, o juiz, no processo civil que reconhecer a hipossuficiência do titular poderá aplicar a inversão do ônus da prova quando da sua produção ou ela lhe resultar onerosa.

Desse modo, pode-se dizer que a responsabilidade civil da LGPD é em regra subjetiva e nos casos em que couber a aplicação do CDC ela será objetiva. Cabe ainda mencionar a relação do assunto com outras legislações, tais como o art. 373, § 1º do Código de Processo Civil e o art. 6º, VIII do Código do Consumidor.

Em vista disso, autora Patrícia Peck Pinheiro disserta:

> Mediante a apresentação de provas suficientes que isentem de responsabilidade os agentes de tratamento de dados (que são o controlador e/ou o operador), a mesma isenção de responsabilidade lhe deverá ser garantida. (PINHEIRO, 2020, p.122)

Ao que estabelece o art. 44, ele abrange as condições de ilicitude no tratamento de dados e em seu parágrafo único dispõe que é responsabilidade do controlador e operador reparar o dano em razão da violação da lei que resulte o dano patrimonial, moral, individual ou coletivo.

Logo, a LGPD não trata a respeito da na responsabilidade civil do encarregado, porém ela caberá, quando esse ofício for exercido por uma pessoa natural ou jurídica separada do controlador e do operador em uma relação de consumo. Nesse caso, por estar dentro da rede de produção, ele poderá ser responsabilizado pelo dano causado de forma solidária, bem como sobre o exercício inadequado de suas funções, por ação ou omissão.

3.1 DA SEGURANÇA E BOAS PRÁTICAS

No que diz respeito a segurança e sigilo de dados na LGPD, é importante que exista o estabelecimento de boas práticas para o seu tratamento. Nesse aspecto, os sistemas utilizados para essa finalidade necessitam ser organizados a fim de satisfazer os requisitos de boa governança, princípios e as demais normas previstas nesta Lei e às complementares.

Nesse cenário, alude a especialista Patrícia Peck Pinheiro:

> No âmbito da promoção da segurança da informação, os processos e procedimentos devem assegurar a disponibilidade, integridade e confidencialidade de todas as formas de informação, ao longo de todo o ciclo de vida do dado. Dessa maneira, para que o tratamento de dados pessoais seja assegurado de maneira eficiente e suficiente, cabe aos agentes

> responsáveis por esse tratamento a adoção de medidas de segurança técnicas adequadas e especificas para esse tipo de procedimento. (PINHEIRO, 2020, p. 124)

Nesse cenário, os controladores e operadores dentro de sua habilitação, podem estabelecer de forma individual ou em conjunto com associações, normativas que determinem as condições de organização, os padrões técnicos, diretrizes de segurança, entre outros, nos termos do artigo 50, caput, da LGPD.

Nessa perspectiva, os agentes ou outra pessoa que venha a intervir no tratamento, fica obrigado a comprometer-se com a segurança da informação mesmo após o seu término. Além disso, o controlador deve cientificar à ANPD e ao titular sobre a possibilidade de incidente de segurança que acarrete dano ou risco possa acarretar risco ou dano considerável.

Ao estabelecer as regras, os agentes de tratamento devem considerar os requisitos, bem como, a gravidade dos riscos e dos benefícios para o titular. Ademais, as normas de boas práticas e de governança precisam estar atualizadas e publicadas com periodicidade e devem ter o reconhecimento da ANPD.

Em seguida, cabe mencionar o Guia do Programa de Governança em Privacidade (PGP) que é o conjunto de normas que visam as boas práticas e governança, tendo por objetivo garantir que as instituições estejam adequadas as diretrizes da LGPD.

Nesse sentido, o PGP estabelece que a sua estruturação necessita conter três etapas das quais pode-se citar: a iniciação e o planejamento, seguida da construção e execução e por fim o monitoramento das informações.

No que se refere a etapa de iniciação e planejamento ela deve conter as informações iniciais dos dados e a identificação dos dados mais importantes. A construção e execução trata da gestão e proteção dos direitos individuais, assim como do consentimento, rastreamento e responsabilidade no caso de descumprimento.

Por fim, a etapa de monitoramento engloba os informativos sobre o desempenho do gerenciamento e dos resultados. Desse modo, é notável que ao executar o programa sejam cumpridas as determinações de comprometimento, segurança e clareza dos processos conforme o artigo 50, § 2º, da LGPD, de modo que também exista o empenho dos colaboradores e o reexame e atualização do programa sempre que for necessário.

3.2 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS E SANÇÕES APLICÁVEIS

A ANPD, criada pela Lei nº 13.853/2019 que a definiu como sendo um órgão da administração pública direta e a ela foi conferida autonomia técnica e decisória. Além disso, sua natureza jurídica é transitiva podendo ser mudada pelo Poder Executivo para uma entidade da administração pública indireta, submetida a regulamentação especial e vinculada à Presidência da República. A mudança deve ocorrer no prazo de até 02 (dois) anos da entrada em vigor da estrutura regimental da autoridade.

Desse modo, a ANPD é a conexão entre o governo e o povo visto que permite ao público o envio de dúvidas, denúncias e recomendações relacionadas à lei. A autoridade tem o papel de orientar os órgãos governamentais e as empresas em vista da execução das normas de tratamento de dados pessoais.

À vista disso, os autores Ricardo Vieira De Carvalho Fernandes e Angelo Gamba Prata De Carvalho versam:

> A ANPD é fundamental para garantir a aplicação e observância da LGPD. É a Autoridade que estabelecerá diretrizes para a promoção da proteção de dados pessoais no Brasil. Em resumo, a ANPD deverá zelar pela proteção dos dados pessoais, elaborar a Política Nacional de Proteção de Dados e da Privacidade, nos termos da LGPD, fiscalizar e aplicar sanções em caso de violação às leis pertinentes, atender petições de titulares de dados contra os responsáveis pelo seu tratamento, regulamentar matérias sobre proteção de dados, entre outras atividades. (CARVALHO; FERNANDES, 2018, p.362)

As entidades, empresas e organizações que incidirem nos vazamentos de dados, mesmo que de forma acidental, serão punidas com medidas administrativas. Nos artigos. 52 ao 54 da LGPD são previstas as sanções em virtude de infrações cometidas.

Sob esse entendimento, aborda a escritora Patrícia Peck Pinheiro:

> A imputação de sanções administrativas faz com que os entes responsáveis pelo tratamento de dados pessoais atentem-se à garantia da segurança das informações que estão utilizando. Dessa forma, observa-se que a LGPD busca estimular a aplicação de seus dispositivos em caráter preventivo. (PINHEIRO, 2020, p.130)

As penalidades administrativas incluem a advertência, com a indicação de prazo para correção das quais pode-se citar: multa simples de até 2% do faturamento,

limitada a R$ 50.000.000,00 por infração, multa diária, publicização da infração, bloqueio e eliminação dos dados pessoais.

Dessa maneira, para que o controlador dos dados pessoais possa pôr em ordem a atividade de tratamento de dados, o legislador listou na LGPD outras formas de punições administrativas pontuais, são elas: as disposições de suspensão parcial, suspensão limitada, proibição parcial e proibição total dos dados pessoais:

> 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:
> [...]
> X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
> XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
> XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (BRASIL, 2018).

De acordo com § 1º, do artigo 52, da LGPD, essas medidas serão impostas quando for posterior ao processo administrativo, desde que haja observância as garantias da ampla defesa e do contraditório com base na análise do caso concreto.

Outrossim, cabe mencionar que o disposto no artigo supramencionado não elide a aplicação das medidas administrativas, combinadas com as civis ou penais delimitadas no Código de Defesa do Consumidor e em legislação específica.

Nesse sentido, além do processo administrativo para a aplicação das sanções da LGPD, a lei também determina que as determinações de suspensão e proibição apenas poderão ser empregadas nos casos em que já tiver sido imposta ao menos uma sanção de multa simples, multa diária ou publicização da infração e bloqueio dos dados pessoais ou eliminação dos dados pessoais:

> Art. 52. [...]
> § 6º As sanções previstas nos incisos X, XI e XII do caput deste artigo serão aplicadas:
> I - somente após já ter sido imposta ao menos 1 (uma) das sanções de que tratam os incisos II, III, IV, V e VI do caput deste artigo para o mesmo caso concreto; e (BRASIL, 2018).

Portanto, pode-se dizer que as sanções estabelecidas na LGPD devem ser executadas obedecendo a proporcionalidade da violação cometida, assim como a dimensão do dano provocado para que exista o julgamento correto das infrações

cometidas contra o titular.

CONCLUSÃO

A *priori,* acerca da problemática de proteção dos dados pessoais, discorreu-se sobre o desenvolvimento da sociedade informacional e o seu avanço no tempo, bem como os direitos à privacidade e intimidade até o surgimento da Lei Geral de Proteção de Dados e a sua aplicação jurídica.

Conforme as informações expostas, pode-se compreender a importância de uma lei para regulamentar os dados nas relações virtuais, na medida em que a evolução tecnológica proporciona novas maneiras de integração social. Dessa maneira, buscou-se esclarecer os aspectos principais da normativa estabelecida pela LGPD que alcança as populações, governos e empresas.

Em razão do que foi apresentado, entende-se que a melhor forma de proteção para a privacidade dos cidadãos é a informação e a partir de então saber como seus dados são coletados e monitorados para tomar as providências cabíveis.

A LGDP veio para suprir lacunas existentes de normas esparsas, com isso, ela prevê mecanismos de tutela e uma Autoridade Nacional, traz segurança jurídica, desenvolvendo novos mercados no Brasil e colocando o país em níveis considerados adequados para cooperações econômicas e transições que envolvam o compartilhamento de dados.

Ademais, com a adequação das empresas com a lei, pode resultar no aumento de novos negócios, levando em consideração o investimento feito, bem como a responsabilização da empresa que aderiu as normas segurança o que acarreta em confiabilidade dos fornecedores e consumidores.

Portanto, o direito tem papel essencial na organização da sociedade e deve incentivar o avanço de marcos regulatórios técnicos conforme as necessidades sociais, observados também os valores éticos. Os dados são imprevisíveis e precisam ser norteados por preceitos constitucionais para que permaneçam equiparados com o Estado Democrático de Direito.

REFERÊNCIAS

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/constituicao.htm. Acesso em 02 de set. de 2020.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a Lei Geral de Proteção de Dados. Diário Oficial da União, Brasília, DF, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em 02 de set. de 2020.

BRASIL. Serpro. Governo Federal. **Como cumprir a LGPD?** Mais que multas que afetem o caixa, não aplicar a nova lei pode abalar a reputação diante dos clientes e a confiança em seus produtos e serviços. 2020. Disponível em: https://www.serpro.gov.br/lgpd/empresa/como-cumprir-a-lgpd. Acesso em: 02 fev. 2021.

BRASIL. GOVERNO FEDERAL. **Guia de Elaboração de Programa de Governança em Privacidade**. 2020. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-dedados/GuiaProgramaGovernanaemPrivacidade.pdf. Acesso em: 05 dez. 2021

BRASIL. Superior Tribunal de Justiça. (4. Turma) Recurso Especial nº 1168547 RJ 2007/0252908-3. Relator: Ministro Luiz Felipe Salomão. Brasília, DF, 11 de maio de 2010. Brasília, 07 fev. 2011. Disponível em: https:// stj.jusbrasil.com.br/jurisprudencia/19128034/recurso-especial-resp-1168547-rj-2007-0252908-3-stj. Acesso em: 02 de set. 2020.

CAPANEMA, Walter Aranha. **A responsabilidade civil na Lei Geral de Proteção de Dados**. 2020. Disponível em: https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_6_a_responsabilidade_civil.pdf?d=637250347559005712. Acesso em: 05 fev. 2021.

CARDOSO, Oscar Valente. **Onde se aplica a Lei Geral de Proteção de Dados?** 2020. Disponível em: https://www.orzil.org/noticias/106574/. Acesso em: 07 dez. 2020.

CARVALHO, Angelo Gamba Prata; FERNANDES, Ricardo Vieira de Carvalho. **Tecnologia Jurídica & Direito Digital: II Congresso Internacional de Direito, Governo e Tecnologia**. Belo Horizonte: Fórum, 2018.

COTS, Marcio; OLIVEIRA, Ricardo. **Lei geral de proteção de dados comentada**. 3. ed. São Paulo: Revista dos Tribunais, 2019. 263 p.

HENRIQUE, Antônio; MEDEIROS, Henrique. **Metodologia Científica na Pesquisa Jurídica**, 9ª ed. São Paulo: Ed Atlas, 2017.

KAUER, Gisele. **LGPD: Quais são os direitos dos titulares?** Disponível em: https://www.infranewstelecom.com.br/lgpd-quais-sao-os-direitos-dos-titulares/. Acesso em: 07 dez. 2020.

MACHADO, Raphael *et al*. **Privacidade e Proteção de Dados**: Cenário Internacional e seu relacionamento com a Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil. 2020. Disponível em: https://seginfo.com.br/2020/11/26/privacidade-e-

protecao-de-dados-cenario-internacional-e-seu-relacionamento-com-a-lei-geral-de-protecao-de-dados-pessoais-lgpd-no-brasil/. Acesso em: 27 nov. 2020.

MASSON, Nathália. **Manual de Direito Constitucional**. 3. Ed. rev., ampl. e atual. Salvador: JusPodivm, 2015.

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

NETTO, Thais. **Boas Práticas de Governança na proteção de Dados: o Programa de Governança em Privacidade**. 2020. Disponível em: https://direitoreal.com.br/artigos/boas-praticas-de-governanca-na-protecao-dedados-o-programa-de-governanca-em-privacidade. Acesso em: 10 fev. 2021.

NETTO, Thais. **Aplicação de Sanções Administrativas na LGPD - Lei Geral de Proteção de Dados**. 2020. Disponível em: https://direitoreal.com.br/artigos/aplicacao-de-sancoes-administrativas-na-lgpd lei-geral-de-proteção-de-dados. Acesso em: 15 mar. 2021.

NETTO, Thaís. **Aplicabilidade e Inaplicabilidade da LGPD**. 2020. Disponível em: https://direitoreal.com.br/artigos/aplicabilidade-e-inaplicabilidade-da-lgpd. Acesso em: 07 dez. 2020.

PINHEIRO, Patrícia Peck. **Direito Digital**. 5. Ed. rev., atual. e ampl. de acordo com as Leis n. 12.735 e 12.737. São Paulo: Saraiva, 2013.

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

SELEME, Mariana Pigatto. **Lei geral de proteção de dados**: por que precisamos dela? 2019. Disponível em: https://www.migalhas.com.br/depeso/305072/lei-geral-de-protecao-de-dados---por-que-precisamos-dela. Acesso em: 27 nov. 2020.

VIEIRA, Victor Rodrigues Nascimento. **Lei Geral de Proteção de Dados:** Requisitos e hipóteses para o tratamento de dados pessoais. 2020. Disponível em: https://vieiravictor.jusbrasil.com.br/artigos/768221472/lei-geral-de-protecao-de-dados-requisitos-e-hipoteses-para-o-tratamento-de-dados-pessoais. Acesso em: 07 dez. 2020.