OS MECANISMOS DA LEI GERAL DE PROTEÇÃO E DADOS E SEUS CONCEITOS APLICADOS NO BRASIL

THE MECHANISMS OF THE GENERAL DATA PROTECTION LAW AND ITS CONCEPTS APPLIED IN BRAZIL

Gabriel Gomes da Luz[1]

Matheus Oliveira Maia[2]

Rodrigo Almeida Magalhães[3]

Recebido/Received: 01.04.2023/Apr 1st, 2023

Aprovado/Approved: 09.05.2023/May 9th, 2023

RESUMO: A Lei Geral de Proteção de Dados (LGPD) é uma legislação brasileira que tem como objetivo proteger a privacidade e os dados pessoais dos cidadãos. Ela foi inspirada no Regulamento Geral de Proteção de Dados (GDPR) da União Europeia e entrou em vigor no Brasil em setembro de 2020. Dessa forma, o trabalho foi escrito, uma vez que a privacidade e os dados pessoais é um assunto de grande relevância e que sempre houve a necessidade de haver uma lei que regulamentasse a proteção destes meios. Com isso, a LGPD foi criada como uma alternativa para efetivar a proteção destes meios. O presente artigo, assim, tem por escopo apresentar uma análise conceitual ampla acerca da Lei Geral de Proteção de Dados com foco em sua aplicabilidade no Brasil, uma vez que ao analisar o contexto histórico se inspirando na GDPR nos países europeus, a efetividade da proteção de dados e da privacidade pode ser bem efetiva. Para obtenção de resultados e conclusões, utiliza-se a metodologia de pesquisa integrada, descritiva, dedutiva e a técnica de pesquisa bibliográfica. Os resultados apontam que a LGPD se inspira pela lei europeia GDPR, e que sua aplicabilidade no Brasil é complexa, sendo assim, um grande desafio para sua regulamentação ser totalmente efetiva. Logo, conclui-se que se deve realizar maior conscientização, fortalecimento da ANPD e a adaptação das leis para garantia da proteção de dados na sociedade brasileira digital atual.

[1] Acadêmico em Direito pela Pontifícia Universidade Católica de Minas Gerais (PUC/MG). Atua como pesquisador voluntário vinculado ao Programa de Iniciação Científica Voluntária (PIC-V) – PUC/MG. Gestor de gabinete no Tribunal de Justiça de Minas Gerais. Membro da ABDC. Autor de artigos jurídicos. Currículo Lattes http://lattes.cnpq.br/8300400458958350. E-mail: ganrieldaluzm123@gmail.com

[2] Acadêmico em Direito pela Pontifícia Universidade Católica de Minas Gerais (PUC/MG). Atua como pesquisador voluntário vinculado ao Programa de Iniciação Científica Voluntária (PIC-V) – PUC/MG. Atualmente é estagiário em gabinete de Juiz no Tribunal de Justiça de Minas Gerais. Autor de artigos jurídicos. Currículo Lattes: http://lattes.cnpq.br/3377231555543289. E-mail: oli.matheus.maia@gmail.com

[3] Doutor e Mestre em Direito pela Pontifícia Universidade Católica de Minas Gerais (PUC/MG). Professor do mestrado e doutorado em Direito na PUC/MG. Professor da Universidade Federal de Minas Gerais (UFMG). Advogado. Currículo Lattes: http://lattes.cnpq.br/8655351102126052. E-mail: almeidamagalhaesrodrigo@gmail.com

PALAVRAS-CHAVE: lei geral de proteção de dados (lgpd); privacidade; dados pessoais; aplicabilidade; regulamentação de dados.

ABSTRACT: The General Data Protection Law (LGPD) is a Brazilian legislation aimed at protecting the privacy and personal data of citizens. It was inspired by the General Data Protection Regulation (GDPR) of the European Union and came into effect in Brazil in September 2020. Thus, this work was written considering that privacy and personal data are of great relevance, and there has always been a need for a law to regulate the protection of these assets. In this regard, the LGPD was created as an alternative to effectively protect these assets. The scope of this article is to present a comprehensive conceptual analysis of the General Data Protection Law, focusing on its applicability in Brazil. By analyzing the historical context and drawing inspiration from the GDPR in European countries, the effectiveness of data protection and privacy can be highly effective. The integrated, descriptive, deductive research methodology and bibliographic research technique were used to obtain results and conclusions. The results indicate that the LGPD is inspired by the European GDPR and that its applicability in Brazil is complex, thus posing a major challenge for its full regulation. Therefore, it is concluded that greater awareness, strengthening of the National Data Protection Authority (ANPD), and adaptation of laws are necessary to ensure data protection in the current Brazilian digital society.
KEYWORDS: general data protection law (lgpd); privacy; personal data; applicability; data regulation.

INTRODUÇÃO

O artigo pretende analisar a Lei Geral de Proteção de Dados (LGPD). Para isso, será construído um raciocínio lógico-argumentativo consistente em demonstrar a relevância da conclusão a que o artigo se propõe: discorrer sobre o surgimento da LGPD e os impactos iniciais que esta causa na sociedade.

Logo, pode-se apontar que a Lei Geral da Proteção de Dados foi promulgada em 2018, com o objetivo de regulamentar a organização de dados pessoais no Brasil. Com isso, o trabalho observa o contexto histórico, apontando de como surgiu a proteção de dados e o contexto na qual foi instaurada para proteger os dados brasileiros.

A aplicabilidade desta lei tem vastos impactos na sociedade e como um dos principais pode-se destacar o consentimento das pessoas ao compartilharem os seus dados pessoais e a vulnerabilidade desta transferência de dados.

Assim, o objetivo deste trabalho é demonstrar alguns conceitos para entender melhor os impactos que a LGPD pode causar e analisar a sua eficiência na sua aplicabilidade no Brasil. Inicia-se o artigo com alguns conceitos básicos, passa a

descrever o contexto do surgimento da lei no mundo e no Brasil, analisa o Marco Civil da Internet e a elevação da proteção de dados como direito fundamental.

Para essa análise a metodologia de pesquisa adotada é a integrada, analítica, dedutiva e a técnica de pesquisa bibliográfica.

O artigo foi organizado em três partes. Na primeira, foi apresentado o sistema multiportas para resolução de conflitos no Brasil, na segunda, foi discutida a aplicação dos métodos de resolução de conflitos e suas limitações e, na terceira parte, foi levantado o fluxo decisório percorrido para a resolução de conflitos.

1 CONCEITOS FUNDAMENTAIS

Para discutir sobre a LGPD, é necessário demonstrar o conceito do consentimento, pois este é um dos conceitos fundamentais ao discutir sobre proteção de dados. Isso há muita interferência da história da proteção de dados, onde previamente da promulgação da LGPD, o Marco Civil da Internet (Lei 12.965/14) em pouco tempo reivindicava o consentimento transparente dos titulares para a realização da coleta, utilização e análise dos dados pessoais.

A discussão sobre consentimento teve início quando o projeto de lei 4060/12 foi aprovado, o qual posteriormente se tornou a LGPD. No início da PL, não havia uma discussão clara sobre consentimento, e também não havia uma construção como aos padrões europeus daquela época. Ao longo dos anos, a legislação foi sofrendo várias alterações, se aproximando cada vez mais da regulamentação europeia. Logo, o consentimento foi se tornando um dos principais conceitos para a proteção de bens.

É válido ressaltar que no tratamento de dados pela LGPD deve-se aplicar os princípios da segurança, da prevenção e da transparência, uma vez que, na maioria dos casos o uso se dá pelo consentimento, mas há empresas que não informam normalmente que ao se tratar de dados de tais clientes, estes já possuem o consentimento de que a empresa realiza todas as atividades de forma segura e não dão consentimento para todas as fases de sua aplicabilidade.

Assim pode-se definir o consentimento de acordo com a LGPD (Lei nº 13.709/18, art. 5º, XII) como a “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”.

Embora o consentimento seja uma das bases legais mais conhecidas e amplamente utilizadas para o tratamento de dados pessoais, não é a única base legal disponível sob a legislação de proteção de dados, como por exemplo a Lei Geral de Proteção de Dados (LGPD) no Brasil, ou a General Data Protection Regulation (GDPR) na Europa.

Outras bases legais para o tratamento de dados pessoais podem incluir a execução de um contrato ou a realização de medidas pré-contratuais, o cumprimento de uma obrigação legal, o interesse legítimo do controlador ou de terceiros, a proteção da vida ou integridade física do titular dos dados ou de terceiros, a tutela da saúde pública, entre outras.

Portanto, é importante avaliar cuidadosamente a base legal adequada para cada atividade de tratamento de dados pessoais, considerando os requisitos legais aplicáveis, as circunstâncias específicas e os direitos dos titulares dos dados envolvidos.

Outro conceito fundamental da LGPD e que teve forte influência nas discussões no Congresso Nacional é sobre o dado pessoal. Para conseguir entender e conceituar o dado pessoal de uma forma mais clara é necessário entender que existem duas vertentes cabíveis de interpretação para contextualizar o dado pessoal de forma moderna, ou seja, o embate entre a acepção expansionista sobre pessoas “identificáveis” ou reducionista á uma pessoa identificada. Segundo a teoria reducionista, “somente pode ser classificado como dado pessoal aquele que corresponde a uma pessoa específica, ou seja, um documento de identidade, um dado biológico único. Diferentemente da acepção expansionista, na qual “não demanda uma relação direta e perfeita entre uma pessoa e um dado para que tal dado possa ser caracterizado como um dado pessoal”. (COSTA, 2019, p.23)

Após ter em vista as duas teorias sobre o dado pessoal, a LGPD adotou o significado expansionista, ou seja, todo dado pessoal é uma informação relacionada a uma pessoa identificada ou identificável, portanto a doutrina brasileira interpreta que os dados pessoais não se limitam.

2 CONTEXTO HISTÓRICO

2.1 Mundial

No início de 2018 havia pouco conteúdo sobre os debates envolvendo a privacidade no Brasil, (a LGPD é de agosto de 2018, e desde 2014 já havia um anteprojeto de lei para sua implementação no Brasil, porém com a implantação da Regulação/Regulamento Geral de Proteção de Dados Europeia (popularmente conhecida como GDPR), este serviu de inspiração para várias implementações de diversas leis a respeito da proteção de dados.

Inclusive um momento que podemos utilizar como inspiração para realizar a implantação de leis para a proteção de dados é a desordem que foi instaurada nos Estados Unidos em que houve violação de dados, em que foi conhecido como o "Caso Cambridge", em que a empresa Cambridge Analytica mostrou as pessoas em nível mundial o poder e o controle que podem ser adquiridos com a posse de dados.

2.2 Caso Cambridge

O caso da Cambridge Analytica foi conhecido por uma empresa com este nome, utilizou informações de mais de 50 milhões de pessoas sem o consentimento delas para realizar propaganda política. Estes dados foram retirados do Facebook através de um aplicativo lançado para realizar um teste psicológico nas redes sociais. Logo, aqueles usuários que participaram deste teste entregaram afora de suas informações, mas também de todas as pessoas adicionadas como amigas no perfil para esta empresa (Privacidade hacekada, netflix, 2019).

Após dois dias sobre a publicação desta notícia o valor do Facebook foi encolhido em Us$ 35 bilhões (aproximadamente R$ 115,5 bilhões) na bolsa de valores de tecnologia dos EUA. Com isto, a empresa começou a ser investigada pelas autoridades dos EUA e do Reino Unido, fazendo com que o CEO do Facebook Mark Zuckerberg testemunhasse diante à um comitê legislativo.

Nesta época, muitos se perguntaram como que foi extraído estes dados, e segundo Christopher Wylie ex-funcionário da Cambridge Analytica, relatou que o esquema começou em 2014, ou seja, dois anos antes das eleições americana e três anos antes do Brexit. ("Entenda o escândalo de uso político de dados que derrubou

valor do Facebook e o colocou na mira de autoridades". BBC News Brasil. 20 de março de 2018).

A pergunta que estava na maioria das pessoas era como que o aplicativo realizou a coleta de dados e Wylie afirmou que além do conhecimento de que muitos usuários não ficam lendo os longos termos de condição e uso, havia uma brecha do facebook em colher os dados das amizades dos usuários que usaram o aplicativo, ou seja, através de uma pessoa que realizasse o uso do aplicativo havia a coleta não apenas de um dado, mas de vários dados.

Os dados coletados eram os nomes, profissões, localização, além de comportamentos habituais que eram retirados da rede de contatos. Muitos acharam que Cambridge tinha utilizado algum hacker para obter dados do Facebook, porém foi relatado que eles utilizaram uma "brecha" que o aplicativo tinha para se aproveitar da situação. Assim, o Facebook observou a "brecha" e corrigiu ela com o passar dos meses, porém acionou a justiça afirmando que a empresa por difamar pela ocultação da "brecha", ou seja, não reportou o problema ao Facebook.

Portanto, a partir deste caso o mundo percebeu a importância dos dados e começaram a realizar vários conhecimentos sobre esta área, um dos principais países que deram esta importância foi o Brasil.

2.3 Explorando os Conceitos da LGPD e sua Semelhança com a GDPR: Protegendo a Privacidade dos Dados Pessoais

A GDPR (Regulamento Geral de Proteção de Dados da União Europeia) entrou em vigor em 25 de maio de 2018, ela normatiza a proteção dos dados pessoais no âmbito da União Europeia, tendo uma aplicação transnacional. A GDPR é considerada como um marco para garantir aos titulares informações precisas sobre os motivos das decisões automatizadas. Essa garantia pode ser definida como um direito do titular de ser informado sobre como são tomadas as decisões, bem como de solicitar revisão.

O Brasil tem na sua legislação (LGPD) a mesma proporção da GDPR sobre o controle e operação dos dados pessoais. Na GDPR em seu artigo quinto, inciso um, podemos visualizar que:

> Artigo 5. Princípios relativos ao tratamento de dados pessoais
> I. Os dados pessoais são:

> a) Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados («licitude, lealdade e transparência»);
> b) Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89.,n.1 («limitação das finalidades»);
> c) Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados («minimização dos dados»);

Com isso, pode-se notar que este artigo demonstra a essência dos dados pessoais, ou seja, o titular dos dados possuí direitos de que seus dados devem ser tratados de forma lícita, leal e com transparência, para justamente oferecer o consentimento a ele, o uso necessário dos dados no mundo contemporâneo. Além disto, e notória a limitação das finalidades justamente para o Estado simplificar o sistema de segurança e ter eficácia em suas medidas para o controle de dados dos seus cidadãos.

No artigo 5º da Lei Geral de Proteção de Dados pode-se visualizar o conceito de dados, bem como suas espécies. Cuja redação importa transcrever:

> Art. 5º Para os fins desta Lei, considera-se:
> I - Dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - 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;
> III - Dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
> IV - Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
> V - Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
> VI - Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII - Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

Portanto, pode-se observar que o Brasil praticamente se espelhou na mesma essência da segurança da GDPR, utilizando vários conceitos para efetivar o controle de dados de forma clara e precisa.

O conceito de titular, no contexto da proteção de dados pessoais, refere-se à pessoa natural a quem os dados pessoais se referem e que é protegida pela legislação de proteção de dados. Conforme o artigo 5º da LGPD, é mencionado que o titular é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

O titular dos dados possui o direito de fornecer seus próprios dados para quem desejar, uma vez que se trata de um direito personalíssimo. Isso significa que o titular tem o controle sobre suas informações pessoais e pode decidir com quem compartilhá-las.

A proteção de dados pessoais garante que o titular mantenha o controle sobre suas informações, mesmo após fornecê-las a terceiros. Mesmo que o titular compartilhe seus dados com outras pessoas ou organizações, ele não perde sua condição de titular e continua a ter direitos e proteção em relação ao tratamento desses dados. Essa abordagem coloca o titular no centro do sistema de proteção de dados, enfatizando sua autonomia e direitos sobre suas informações pessoais.

Já o controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem compete tomar as decisões referentes ao tratamento de dados pessoais. Em outras palavras, é o responsável por determinar a finalidade e os meios do tratamento dos dados pessoais. O controlador toma as decisões sobre como os dados serão coletados, utilizados, armazenados e compartilhados. Ele possui o poder de decisão e controle sobre o tratamento dos dados pessoais. É sua responsabilidade garantir que o tratamento seja realizado em conformidade com a legislação de proteção de dados.

Por fim, O operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. O operador atua sob as instruções do controlador, executando as atividades de tratamento dos dados em nome dele. O operador pode ser um terceiro contratado pelo controlador para realizar determinadas tarefas de processamento de dados, como fornecer serviços de armazenamento em nuvem, processamento de pagamentos ou envio de comunicações. O operador não toma decisões sobre o tratamento dos dados, mas age de acordo com as instruções e orientações do controlador.

A proteção de dados pessoais exige que tanto o controlador quanto o operador adotem medidas de segurança técnicas e administrativas para proteger os dados pessoais contra acesso não autorizado, perda, destruição, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Além disso, tanto o controlador quanto o operador são responsáveis por manter registros das operações de tratamento de dados realizadas e são responsáveis por reparar

quaisquer danos causados a terceiros em caso de violação à legislação de proteção de dados.

Em caso de incidente de privacidade que cause lesão ao titular dos dados, a responsabilidade civil entre o controlador e o operador é distribuída de acordo com o estágio da operação em que ocorreu a falha. Em certos casos, pode haver solidariedade entre eles, ou seja, ambos podem ser responsabilizados conjuntamente.

Em resumo, o controlador é o agente responsável por tomar as decisões sobre o tratamento dos dados pessoais, enquanto o operador realiza o tratamento em nome do controlador, seguindo suas instruções. Ambos devem adotar medidas de segurança e são responsáveis pela conformidade com a legislação de proteção de dados.

2.4 Aprimorando a Aplicabilidade da LGPD no Brasil: Medidas para Fortalecer a Proteção de Dados e Privacidade

Com a aprovação do Regulamentação Geral de Proteção de Dados (GDPR) feita pela União Europeia e com o vazamento sobre o caso Cambridge, foi necessário pôr em pauta a relevante necessidade em que o Brasil havia que aprimorar sua legislação de proteção de dados de uma maneira mais rígida. Deste modo, buscando orientar a coleta, os usos, os dados armazenados e o processamento de dados tanto públicos quanto privados, foi necessário enquadrar a legislação de acordo com um padrão internacional.

Danyelle e Aires (ROVER, PINTO, PEIXOTO, 2020, p. 19) enfatizam que a inclusão digital no Brasil se apresenta como um grande desafio no Brasil, uma vez que demanda a aperfeiçoamento da legislação brasileira. Logo, o intuito do Brasil em aprimorar sua legislação sobre a proteção de dados também é estimulado para pleitear seu ingresso na Organização para a Cooperação e Desenvolvimento Econômico (OCDE), pois com este ingresso o Brasil iria ter um conhecimento mais robusto sobre a proteção de dados não de forma jurídica, mas na forma de adequar os objetivos do Estado com a sua sociedade, ou seja, para enriquecer e adequar o padrão internacional ao seu sistema.

Nesse contexto, em 14 de agosto de 2018 foi sancionada a Lei Federal n 13.709/2018, conhecida como LGPD dispõe que:

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

No artigo 3 em seu inciso III da LGPD, demonstra-se que:

> Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
> III - os dados pessoais objeto do tratamento tenha sido coletados no território nacional.
> § 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.
> § 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.

Logo, percebe-se que o artigo 3º da Lei Geral de Proteção de Dados (LGPD) estabelece o âmbito de aplicação da legislação. Ele define os tipos de entidades e atividades que estão sujeitos às disposições da LGPD. O artigo em questão afirma que a lei se aplica a todas as operações de tratamento de dados pessoais realizadas por pessoas físicas ou jurídicas, de direito público ou privado, com fins comerciais ou não.

Em outras palavras, o artigo 3º determina que a LGPD se aplica a todas as empresas, organizações e órgãos públicos que realizam atividades de coleta, armazenamento, processamento e compartilhamento de dados pessoais no território brasileiro. Essa abrangência é ampla e engloba desde pequenas empresas até grandes corporações, independentemente do setor em que atuam.

É importante ressaltar que o artigo 3º também estabelece que a LGPD se aplica mesmo quando as operações de tratamento de dados são realizadas fora do território brasileiro, desde que os dados se refiram a indivíduos localizados no Brasil ou a atividades realizadas no país.

Em resumo, o artigo 3º da LGPD define o escopo de aplicação da lei, determinando quais entidades e atividades estão sujeitas às suas disposições, visando proteger os direitos dos titulares dos dados pessoais e promover a segurança e privacidade dessas informações.

Porém é necessário observar que sua aplicabilidade ainda há um potencial de ser mais efetiva, uma vez que, se aplicada as seguintes medidas, a sociedade terá maior proteção de sua privacidade e de seus dados pessoais.

A primeira medida é a conscientização e educação, tendo em vista que é fundamental promover uma maior conscientização e educação sobre a importância

da proteção de dados pessoais, tanto entre as organizações como entre os cidadãos. A divulgação e o esclarecimento dos direitos e obrigações previstos na LGPD podem ajudar a criar uma cultura de respeito à privacidade e à segurança dos dados.

Outra medida que deve ser adotada é a fiscalização e o seu devido cumprimento, uma vez que, é necessário que haja um efetivo processo de fiscalização e cumprimento das disposições da LGPD. Os órgãos responsáveis pela aplicação da lei devem buscar recursos mais adequados e gerenciar com autoridade para ter maior efetividade para investigar possíveis violações, além de aplicar penalidades em caso de descumprimento.

Uma medida que deve ser amplamente discutida é a cooperação internacional, uma vez que a LGPD tem como objetivo harmonizar as normas brasileiras de proteção de dados com padrões internacionais, como o GDPR. É importante fortalecer a cooperação e o intercâmbio de informações entre autoridades de proteção de dados de diferentes países, a fim de garantir uma proteção efetiva em um contexto globalizado.

Por fim, é necessário o fortalecimento da Autoridade Nacional de Proteção de Dados (ANPD), uma vez que a ANPD é o órgão responsável pela regulamentação e fiscalização da LGPD no Brasil. Logo, para que a aplicabilidade da LGPD seja mais efetiva no Brasil, é necessário o fortalecimento da ANPD, para que assim seja garantido a autonomia, recursos e capacidade técnica para desempenhar suas funções de forma eficiente.

3 MARCO CIVIL DA INTERNET

O Marco Civil da Internet é uma lei que regula o uso da internet do Brasil, ela entrou em vigor a partir de 2014 e é conhecida como “Constituição da Internet”, na qual foi uma das primeiras legislações instauradas no Brasil com o tema da internet. A finalidade que ela foi instaurada foi para o estabelecimento de garantias, direitos e deveres para disciplinar o uso da internet no Brasil.

Quando havia as discussões sobre as legislações sobre o uso da internet em 2007 e em 2009, já havia um movimento de negação a implementação da lei. Este fato ocorre principalmente pela norma criar muitos encargos e incumbências às empresas fornecedoras de internet. Porém, estes encargos geram uma proteção ao

usuário e fortificam a liberdade, o respeito e a boa-fé nas redes ondes os usuários usufruem da internet. Com esta proteção se constitui a neutralidade da rede, ou seja, não há uma divisa como nas televisões a cabo em que são adquiridos pacotes de funcionalidades distintas com preços proporcionalmente divididos a quantidade de funcionalidades de cada pacote.

A neutralidade tem como finalidade oferecer maior liberdade ao usuário de usufruir seu produto com maior funcionalidade e fazendo com que seu preço do mercado seja mais acessível, podemos observar isso nos novos serviços lançados nos últimos tempos como Netflix, Youtube e Skype. Estes serviços executam muitos vídeos e geram um consumo de dados acentuado e contínuo, devido a informação ser processada imediatamente no vídeo, ou seja, sem atrasos no procedimento de dados, pois se ocorrer os atrasos, os vídeos não vão carregar e os provedores para acessarem estes dados vão demorar para corrigirem o procedimento.

Tendo o conhecimento das funcionalidades dos procedimentos de como são feitos os serviços de internet, podemos observar como que as empresas podiam se “aproveitar” por não ter uma norma padronizada do serviço. Como o cliente pagava por funcionalidades as empresas tentavam excluir do seu pacote de dados o uso de um serviço ou até mesmo limitavam os dados de conexão para o acesso do programa. Com isso o cliente estava dependente da boa-fé da fornecedora do serviço para usufruir da internet.

Logo, um dos aspectos fundamentais do Marco Civil da Internet é a garantia da neutralidade da rede, que impede que as empresas provedoras de internet realizem qualquer tipo de discriminação ou restrição no acesso dos usuários aos conteúdos disponíveis na rede.

Essa limitação das empresas fornecedoras de internet é importante para preservar a privacidade dos usuários e garantir a igualdade de acesso à informação. Sem a neutralidade da rede, as empresas poderiam selecionar e restringir o acesso a determinados conteúdos, serviços ou aplicativos com base em interesses comerciais ou políticos, prejudicando a liberdade de expressão e o acesso à informação diversificada.

Ao garantir a neutralidade da rede, o Marco Civil da Internet protege a privacidade dos usuários, pois as empresas provedoras de internet não podem monitorar ou restringir seletivamente o tráfego de dados com base em seu conteúdo,

origem, destino ou protocolo. Isso impede que informações pessoais e comportamentais sejam coletadas e utilizadas sem o consentimento dos usuários.

Além disso, o Marco Civil da Internet também estabelece a importância da privacidade dos usuários ao tratar do armazenamento e da proteção de dados pessoais. A legislação determina que as empresas provedoras de internet devem adotar medidas de segurança adequadas para proteger as informações dos usuários contra acesso não autorizado, perda ou vazamento.

A privacidade é um elemento essencial para o exercício pleno da liberdade de expressão, do acesso à informação e da participação na sociedade digital. O Marco Civil da Internet reconhece a importância da privacidade como um direito fundamental dos usuários da internet, garantindo que as empresas fornecedoras de internet não possam violar a privacidade dos usuários por meio da limitação do acesso à rede ou da coleta indiscriminada de dados.

Assim, a limitação das empresas fornecedoras de internet, aliada aos princípios e direitos estabelecidos pelo Marco Civil da Internet, desempenha um papel crucial na proteção da privacidade dos usuários e na promoção de um ambiente digital mais igualitário e democrático.

Há também outro aspecto que é sanado pela neutralidade da rede é a concorrência desleal, uma vez que, De acordo com Rayssa Alves pode-se observar que:

> Além disso, a neutralidade de rede busca evitar a concorrência desleal, pois normalmente o provedor de internet também é a empresa que fornece telefonia. Neste caso, ela não poderia limitar ou impedir o acesso a programas que façam ligações telefônicas, como é o caso do Skype, que também faz ligações nacionais e internacionais, normalmente a preços mais módicos. Afinal, a Lei do Marco Civil busca sempre manter a liberdade e proteção do usuário (ALVES, RAYSSA, 2017, p.90).

A autora relata que já ocorreu uma situação interessante no Brasil, sobre um possível delito da neutralidade de rede. Acerca de 2015, a empresa TIM estabeleceu uma campanha publicitária chamada “TIM Whatsapp”, em que seus clientes poderiam ter o acesso gratuito do aplicativo Whatsapp e que poderiam mandar suas mensagens sem o consumo de nenhum dado de sua franquia de internet ou mesmo sem precisar de ter créditos no celular para tanto.

Neste caso, pode-se observar que a Tim privilegia o Whatsapp, pois há outros aplicativos que realizam o mesmo serviço, porém são necessários dados para ter o acesso, logo podemos observar a grande relevância que o Marco Civil da Internet

realizou e observamos a necessidade que a lei se expanda para diversas ocasiões para acompanhar dinamicamente a Era digital.

4 EMENDA CONSTITUCIONAL Nº 115/22: A PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL

A constituição da república Portuguesa já dispunha em seu texto desde o ano de 1976 a proteção em face do uso da informática e, em parte, também a questão dos dados pessoais.

Partindo-se da premissa portuguesa foi promulgada a EC nº 115 de 22, no Brasil, a qual dispunha sobre a conveniência e oportunidade da inserção de um direito à proteção de dados pessoais na CF, ficou, de certo modo, superada. De acordo com o texto da EC 115, foi acrescido um inciso LXXIX ao artigo 5º, CF, dispondo que "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais". (Incluído pela Emenda Constitucional nº 115, de 2022).

Ora, tal direito fundamental já era possível se abstrair de uma leitura ampla acerca do disposto no artigo art. 5º, X, da Carta Cidadã, direito à privacidade- ligado ao princípio da inviolabilidade, sobretudo das comunicações.

Portanto, a inserção de tal direito de forma autônoma possibilitou um maior reforço à aplicação da Lei Geral de Proteção de Dados, bem como a sua utilização com respaldo na própria constituição federal, o que legitima de forma dobrada a sua aplicabilidade.

A EC 115/22 também incluiu os incisos XXVI e XXX, respectivamente, aos artigos 21 e 22 da Carta Magna, atribuindo à União competência para organizar e fiscalizar a proteção e o tratamento de dados pessoais, bem como competência privativa para legislar sobre a matéria.

Portanto, conclui-se que, além da LGPD, Código de Defesa do Consumidor, Código Civil, Lei de Acesso à Informação, Lei do Cadastro Positivo e Marco Civil da Internet, impõe-se ao Estado (isso já independentemente da inserção do direito à proteção de dados pessoais no texto constitucional, mas com ainda mais razões com a sua positivação expressa!), por força de seus deveres de proteção, não apenas zelar pela consistência constitucional do marco normativo infraconstitucional (inclusive da LGPD) no tocante aos diplomas legais isoladamente considerados,

mas também de promover sua integração e harmonização produtiva, de modo a superar eventuais contradições e assegurar ao direito fundamental à proteção de dados, sua máxima eficácia e efetividade (SARLET, 2022).

Logo, podemos destacar os seguintes questionamentos desta emenda:

a) Até que ponto a Emenda Constitucional nº115/22 garante efetivamente a proteção dos dados pessoais como direito fundamental?
b) Quais são as medidas e salvaguardas específicas necessárias para garantir a proteção adequada dos dados pessoais dos cidadãos, levando em consideração o rápido avanço da tecnologia e a crescente ameaça à privacidade?
c) Como a legislação atual deve se adaptar para lidar com os desafios e as demandas emergentes relacionadas à proteção de dados pessoais, considerando a importância crescente desse direito fundamental na sociedade digital atual?

Estes questionamentos estão justamente interligados, ao que foi apresentado anteriormente, uma vez que foi discutido que não há a efetividade em totalidade na aplicação da LGPD, em que há medidas com o fortalecimento da ANPD para garantir a proteção adequada dos dados pessoais dos cidadãos. Por fim, há também a necessidade da adaptação das normas, que é o questionamento deste presente capítulo, uma vez que já há uma emenda que discorre sobre a devida proteção e que pode tornar mais efetiva a proteção de dados no Brasil.

CONSIDERAÇÕES FINAIS

No entanto, esse cenário mudou em 14 de agosto de 2018, com a entrada em vigor da lei de 2018. 13.709/2018, a lei Geral de Proteção de Dados Pessoais - LGPD, que dispõe sobre o tratamento de dados pessoais por pessoas físicas ou jurídicos de direito público ou privado, inclusive dados digitais, com o objetivo de resguardar o princípio da liberdade e da confidencialidade, bem como o livre desenvolvimento da personalidade da pessoa natural.

Além de ser a primeira lei geral nacional sobre o tema, a importância da Lei Geral de Proteção de Dados está na introdução de regras para o tratamento de dados pessoais. Estas regras vão desde os princípios que regem a proteção de dados pessoais, aos fundamentos legais que podem justificar o tratamento de

dados, às verificações e responsabilização dos envolvidos no tratamento de dados pessoais.

A referida lei também proporciona à pessoa física a quem os dados pessoais se referem a possibilidade de solicitar informações como confirmação da existência do tratamento de seus dados pessoais, acesso a dados, correção de dados incompletos, eliminação de dados desnecessários e portabilidade de dados pessoais dados para outro fornecedor de produtos e serviços.

Em resumo, o mencionado diploma normativo deu início a uma nova cultura de privacidade e proteção de dados no país, logo reforçada pela Emenda Constitucional nº 115/22, que exigia a conscientização de toda a sociedade sobre a importância dos dados pessoais das pessoas físicas, bem como jurídicas, como liberdade, privacidade e livre desenvolvimento da personalidade.

REFERÊNCIAS

AGOSTINELLI, J. **A importância da lei geral de proteção de dados pessoais no ambiente online**. Etic, Presidente Prudente, v. 14, n. 14, 2018.

ALVES, R. de C. A lei do Marco Civil, A INTERNET E AS STARTUPS. In Barbosa, A. F. M., Pimenta, E. G., & Fonseca, M. L. (Orgs.), **Legal Talks**: Startups à luz do direito brasileiro (Cap. 6). Porto Alegre, RS: Editora Fi, 2017.

BARBOSA, A. F. M., PIMENTA, E. G., & FONSECA, M. L. (Orgs.). **Legal Talks**: Startups à luz do direito brasileiro [recurso eletrônico]. Porto Alegre, RS: Editora Fi, 2017.

BASTOS, L. C., & BARBOSA, A. F. Os impactos da LGPD para empresas. In: BASTOS, L. C., & SILVA, L. J. M. (Orgs). **Aspectos Relevantes da Lei Geral de Proteção de Dados**. São Paulo: Expert Editora Digital, 2021.

BECHARA, GABRIELA E RODRIGUES, HORACIO. “Marco Civil da Internet no Brasil: Conquistas e Desafios”, Direito, Governança e Novas Tecnologias”, Equipe Editorial **Index Law Journal**, junho de 2020.

BIONI, Bruno Ricardo. **Xeque Mate**: o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. São Paulo, 2015.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Diário Oficial da União, Brasília, 1, dez. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm/. Acesso em: 07 mai. 2023.

COSTA, R. V. D. F. **A Transferência Internacional de Dados na Lei nº 13.709/18 e a Administração de Recursos de Terceiros no Brasil**. Trabalho de Conclusão de

Curso em Pós-Graduação - INSPER, São Paulo, 2019. Disponível em: https://repositorio.insper.edu.br/handle/11224/2334/.

MACIEL, R. F. **Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais** (Lei nº 13.709/18). Goiânia: RM Digital Education, 2019.

MURARI, G. A. C., SCHIAVON, I. N., & BARRETOS, R. A. **Dados pessoais: tratamento realizado pelo poder público à luz da Lei Geral de Proteção de Dados**. Revista Judiciária.