

LEI GERAL DE PROTEÇÃO DE DADOS NAS MÍDIAS SOCIAIS

GENERAL DATA PROTECTION LAW ON SOCIAL MEDIA

Marcos Paulo Pereira Gomes¹Lucas Nascimento de Oliveira²

Resumo: O presente artigo evidencia a importância da lei de proteção de dados nas mídias sociais, sejam pessoas físicas ou jurídicas, resguardando-os, respeitando sua privacidade, liberdade de expressão, de obter informações de quaisquer outrem dentro do permitido, com o devido respeito a cidadania, e principalmente a legitimidade de um espaço seguro para se estar. Fundamentada na Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), foi criada para fortalecer o vínculo privativo entre pessoa e o meio digital, onde fica determinado o poder de expor suas informações, seus dados, e a seguridade que isso será inviolado, além de procurar garantir um espaço de evolução e reflexão do indivíduo na sociedade, bem como proporcionar a este um meio de se relacionar e trabalhar através das mídias sociais. Trata-se de uma pesquisa qualitativa com ênfase no referencial teórico das redes sociais.

Palavras-Chave: Privacidade; LGPD; Dados; Seguridade; Mídias sociais.

Abstract: This article wants show the importance of the data protection law in social media, whether individuals or companies, protecting them, respecting their privacy, freedom of expression, obtaining information from any other person within the allowed, with the respect to citizenship, and especially the legitimacy of a safe space. Based on Law No. 13,709/2018, the General Law of Personal Data Protection (LGPD), was created to strengthen the private bond between people and the digital environment, determining the power to expose their information, their personal data, and the confidence about the inviolate, in addition to ensure a space of evolution and reflection of the person in society, and providing them with a means of relating and working through social media. This is a qualitative research with emphasis on the theoretical framework of social networks.

Keywords: Privacy; LGPD; Data; Security; Social media.

1 INTRODUÇÃO

A facilidade de ingressar nas mídias sociais, o livre acesso a internet em todas as idades, traz consigo grandes consequências na vida de muitas pessoas. O fornecimento de dados vem sendo cada vez mais evidenciado nos formulários de

¹ Mestre em Direito pela Unimar/SP. Especialista em Direito Processual Civil pela Faculdade Anhanguera/SP. Especialista em Direito Constitucional pela FFAO. Professor do Centro Universitário Uninorte. Advogado. E-mail: marcospgomes.adv@gmail.com.

² Graduando em Direito pelo Centro Universitário Uninorte. E-mail: lucas18052@hotmail.com.

inscrições das redes, dos jogos, de qualquer aplicativo usados pelo indivíduo.

São diversas pesquisas de satisfação, em busca de um único objetivo: extrair o máximo de informações, para posteriormente, ser oferecido diversos conteúdos que cativem e façam com que as pessoas passem horas reféns do consumismo digital. Evidentemente que, nem todo mundo controla o tempo que passa na internet, tampouco tem o conhecimento sobre os perigos do excesso de dados inseridos nas plataformas.

Para tanto, A Lei Geral de Proteção de Dados foi criada para garantir que esses dados não sejam expostos, que a privacidade e direito de estar em um ambiente seguro seja garantido. No atual mundo globalizado, acelerado, onde as pessoas evitam ler os grandes regulamentos das redes sociais, tornou-se necessário um amparo legal sobre a seguridade das informações dispostas na internet.

Outro ponto importante a ser destacado é que com a grande leva de informações fornecidas, usa-se a identificação do usuário como justificativa para o acesso em várias etapas de preenchimento. Não obstante a isso, a Lei se fundamenta no respeito a privacidade, nos direitos humanos, na liberdade de expressão, e o pleno exercício da cidadania e no direito ao acesso seguro.

Nesse sentido, o presente artigo tem como intuito esclarecer e exemplificar a importância da proteção dos dados, os riscos da inserção das informações desfreçadas nas mídias sociais, e como as empresas aproveitam essas informações para alimentar o consumo digital, além de usá-los como poder de moeda nas redes sociais.

2 ORIGEM DA LEI GERAL DE PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados foi inspirada na *General Data Protection Regulation* (GDPR), o qual é um conjunto de regras sobre a privacidade e proteção de dados, que se originou na União Europeia. A referida Lei foi aprovada em 14 de agosto de 2018, e estabelece seus fundamentos descritos no artigo 2º da Lei nº 13.709/2018, sendo eles, *in verbis*:

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: I – o respeito à privacidade; II – a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV – a inviolabilidade da intimidade, da honra e da imagem; V – o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. (BRASIL, 2018)

Esta lei foi criada para garantir a privacidade dos usuários, podendo ser por pessoa jurídica ou natural, de direito privado ou público, além disso, sua origem promove novas necessidades em uma sociedade digital que exige mais transparência das situações e correlacionando o mundo atual de negócios, a informação é o meio principal da moeda de troca, sendo usada pelos usuários com o intuito de ter acesso a determinados bens, conveniências e serviços.

Portanto, a finalidade desta referida lei é determinar uma sucessão de regras que possibilitem ao indivíduo o controle do que é exposto nas mídias, e que consequentemente esteja de acordo com a “privacidade informacional”, como aponta Vieira (2007, p. 34), que considera essas informações ligadas sobre alguma pessoa, abrangendo não somente em sua esfera íntima, mas seus dados pessoais que direcionem a sua identificação como titular.

Dessa maneira, essa privacidade informacional está associada com a contextualização de direito à autodeterminação informativa, considerando que cada pessoa tem o poder de controlar e de proteger seus próprios dados pessoais, visando o avanço tecnológico e o desenvolvimento da informação (VIEIRA, 2007, p. 35). Ademais, essa autodeterminação informativa e a sua conexão com o respeito à privacidade são caracterizados como fundamentos que estão descritos através pela LGPD Lei nº 13.709/2018 no art. 2º, incisos I e II.

2.1 CRONOLOGIA DAS LEIS DE PROTEÇÃO DE DADOS PESSOAIS

Antes do surgimento da lei de proteção de dados pessoais brasileira propriamente dita, era necessário decretar alguma norma para tratar sobre o determinado assunto, com o objetivo de fato proteger os dados dos cidadãos. Dessa maneira, o primeiro marco de proteção de dados pessoais está descrito na Constituição Federal no art. 5º:

Art. 5º [...] 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;
XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal. (BRASIL, 1988).

Essa garantia mesmo de forma indireta, tinha como objetivo a proteção, mesmo não se referindo aos dados virtuais. Por consequência desse fator, a próxima norma que tratava dos dados no Brasil foi o Código de Defesa do Consumidor de 1990, no art. 43 da lei nº 8.078, prevê a proteção de dados mediante a cadastros, registros, dados pessoais do consumidor e fichas. Nesse contexto, ainda não condizia ao âmbito virtual.

No entanto, ainda era necessária uma lei específica para sancionar os problemas que futuramente iriam acontecer. Mas após alguns anos, no ano de 2011, referente ao banco de dados regulados pelo CDC, a Lei 12.414/2011, a qual denominada por Lei do Cadastro Positivo, tendo como intuito novas regras sobre as informações cadastrais do cidadão.

Dessa forma, depois de todas essas tentativas, somente em 2014 que o Brasil conquistou um mecanismo eficiente de proteção de dados com o Marco Civil da Internet, sendo sancionada pela presidente Dilma Rousseff em 23 de abril de 2014, essa lei buscava estabelecer garantias, direitos, deveres e os princípios para a utilização da Internet no país.

Em comparação aos outros países, o Brasil estabeleceu a lei de proteção de dados de maneira eficiente tardia. Dessa forma, como já visto anterior, a lei estabelecida antes da LGPD, não conquistaram seu principal objetivo de forma efetiva que era a proteção dos dados, e juntamente com a evolução da sociedade, as mesmas não eram eficazes e suficientes para garantir a estabilidade jurídica nesta sociedade.

Em relação ao marco civil da internet (Lei nº12.965/2014), a LGPD se tornou um instrumento legal para complementá-lo, pois o este apresentava uma vulnerabilidade, mediante a sua aplicabilidade em casos onde as entidades

responsáveis pelo tratamento dos dados são estrangeiras, logo era necessária uma lei que abrangia essa modalidade também.

Portanto, de acordo com Strasser e Oliveira (2020), a LGPD assegura a extensão e incidência dos direitos fundamentais no ambiente virtual na sua totalidade, possibilitando desenvolver relações de transferência internacional de dados entre países ou até organismos internacionais, onde oferece um nível elevado de proteção.

Com a evolução da sociedade, conseqüentemente obteve os avanços tecnológicos, promovendo a eclosão da internet, a qual tem como principal objetivo o compartilhamento de dados e informações, considerada uma ferramenta de desenvolvimento social e econômico atualmente, abrangendo interações entre pessoas de qualquer lugar, logo de uma maneira ampla, aonde acontece um difícil controle dos fluxos de informações em suas camadas.

Portanto, a internet possibilitou que muitas práticas sociais pudessem passar para a forma digital, promovendo uma facilidade de diversas necessidades humanas, no entanto, também é uma ferramenta para desenvolver problemas incalculáveis. Logo, bastante acessível, ao realizar distribuições, compartilhamentos, e dentre outros benefícios, mas este irrestrito acesso coletivo a informações pode se transformar em uma fonte de problemas (LÉVY, 2011, p. 133).

2.2 RESPONSABILIDADES E OBJETIVOS DA LGPD

Nessa ideologia, a LGPD determina suas responsabilidades, ao buscar mitigar riscos e estabelecer regras específicas referente ao tratamento de dados pessoais, além disso, não se restringe ao proteger somente os dados por meio virtual, mas a todas as formas pela qual os dados podem ser utilizados e coletados. No entanto, são no âmbito virtual que se condensam os diversos desafios e maiores preocupações, mediante a proteção de dados (FRAZÃO; TEPEDINO; OLIVIA, 2019).

Destarte que a Lei Geral de Proteção de Dados tem como papel importante ao estimular a autonomia dos titulares dos dados, vendo a necessidade e o seguinte controle que os mesmos devem exercer sobre os seus dados. Com o intuito de

limitar os excessos e ilicitudes que permeiam o mercado movido pelos dados pessoais (FRAZÃO, 2019a, p. 31).

De acordo com essa Lei nº 13.709/2018, não é possível coletar, tratar ou usar os dados pessoais dos usuários sem a permissão de maneira expressiva dos mesmos. Ademais, a lei proíbe o uso dos dados pessoais para prática de discriminação abusiva ou ilícita, visto que a LGPD se aplica a qualquer pessoa, seja jurídica ou física, de direito privado ou público, independentemente de onde estejam localizados seus dados, conforme o art. 3º da Lei Geral de Proteção de Dados.

A LGPD, desde quando entrou em vigor, está possibilitando que as empresas entrem em conformidade com as suas políticas de privacidade para estabelecer as exigências previstas pela lei. As empresas de redes sociais como Facebook, Instagram e Whatsapp, a cada dia estão se adequando para promover um maior controle em relação à privacidade para os seus usuários, logo disponibilizando novas configurações de segurança e novos termos de serviços.

Além disso, no começo deste ano, as políticas de privacidades destas redes sociais apresentaram novas atualizações que declarava estar em decorrência com a LGPD. Como por exemplo, do WhatsApp, aonde aconteceu mudanças no aplicativo, no começo do ano, o qual poderá compartilhar dados dos seus usuários com outros aplicativos, ademais, a empresa postou que está seguindo o aviso de privacidade de acordo com o que a lei impõe. (OLIVEIRA, 2021).

É válido destacar que a Autoridade Nacional de Proteção de Dados (ANPD), é o órgão federal responsável por fiscalizar e aplicar a LGPD, com qualificação de órgão integrante da Presidência da República, dotada de autonomia técnica e decisória prevista no artigo 55-B, com jurisdição no território nacional e com sede e foro no Distrito Federal.

Portanto tem como intuito implementar, zelar e fiscalizar os direitos fundamentais de liberdade e de privacidade. (BRASIL, 2019). Logo, a sua importância vai além de dar segurança em relação aos dados dos usuários, também possibilita que o país se enquadre em parâmetros impostos por outros países para ocorrer negociações internacionais sobre o determinado assunto.

Pelo resultado da evolução e o desenvolvimento tecnológico destaca-se o contínuo progresso da privacidade, a vista disso, surgiu o conhecido como o direito à

autodeterminação informativa, o qual se denomina no fortalecimento da função do titular dos dados como imagem ativa no fornecimento das informações, desencadeando todo o fluxo de seus dados, que se inicia a partir da sua veracidade, exatidão, operação até chegar o seu intuito final que é de sua coleta.

Essa autodeterminação é encontrada expressa no artigo 2º, inciso segundo, da Lei nº 13.709/2018, que consiste em envolver de uma maneira significativa o consentimento do titular dos dados, obtendo como obrigação em declarar a vontade do titular em divulgar ao operador, além da real compreensão do motivo, finalidade e como será concedido esse manuseio.

Deste modo, o “permitir” não pode ser definido como uma concordância final, pois, a mesma pode estar contaminada com vícios de consentimentos, que visto nesse contexto pode até provocar a nulidade deste ato. Logo, no artigo 5º da LGPD, inciso XII, que condiz que o consentimento, se refere a “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”.

Nesse sentido o consentimento informativo inserido no cenário atual como uma ferramenta relevante na participação ativa do proprietário dos dados, e em todo o desenvolvimento de conhecimentos e conseqüentemente a anuência de tratamento dos dados pessoais (TEPEDINO; TEFFÉ; FRAZÃO; OLIVA, 2019, p.291).

Para que o titular dos dados possa autorizar o tratamento por terceiros, deve estar ciente das finalidades, de maneira específica e bem delimitada, logo, necessitam está em conformidade com a situação de uso dos dados. Portanto, isso significa que o tratamento dos dados precisa ser pautado com objetivos legítimos e específicos, de modo amplo, sendo divulgado pelos usuários para que eles possam ser esclarecidos de maneira suficiente para sustentar a sua decisão em relação à autorização do manejo de seus dados (BOFF; FORTES; FREITAS, 2018, p.107).

Nesse contexto, e a posição de vulnerabilidade o qual o titular dos dados está inserido, é atribuído à ele, o operador ou controlador, assegurar ao titular a máxima transparência ao conceder a autorização, promovendo um conhecimento completo de todas as etapas do tratamento de seus dados, como já mencionado desde sua coleta até a sua exclusão, e nesse sentido, a aplicação prática da

autodeterminação informativa no âmbito virtual, sendo apontado na LGPD, é executado por meio da contínua busca pela transparência no tratamento dos dados pessoais, resguardando a privacidade de seus usuários.

3 REDES SOCIAIS

A princípio, a rede social é considerada como uma plataforma que surgiu a partir da origem da internet, a qual proporciona uma construção de relações sociais. Ademais, de acordo com Hirata (2014), a rede social se concretiza em ser uma categoria das mídias sociais, a qual é caracterizada por tornar interativo o diálogo entre pessoas. E é assim que é possível se estar informado, ao vivo dos acontecimentos do Brasil e do mundo.

Xavier, Olenski, Acosta, Sallum e Saraiva (2020) fizeram uma análise do crescimento das redes sociais como estratégia de apoio a vigilância de saúde durante a pandemia do COVID-19 que parou o mundo nos anos de 2020 até meados de 2022, e exemplifica o impacto negativo tanto na saúde pública, pois essa doença obrigou o isolamento social, até a disponibilização da vacina no SUS, quanto no alto índice de acesso as mídias sociais para que as pessoas pudessem se entreter em suas casas.

Ainda, os autores supracitados retratam que apenas em português, no Twitter, foi coletado mais de 7,7 milhões de postagens durante apenas 62 dias. Diante do consumo desenfreado para se estar conectado, cita-se Dhar (2013) e Concolato, (2017), para expor outro componente relativo a esse grande acesso:

Com o aumento do poder de processamento computacional e dos dispositivos conectados, como smartphones, tablets e sensores, há um grande crescimento na geração de dados, de formatos variados e em velocidades cada vez maiores. Esses fatores representam características do que se convencionou chamar de era de Big Data, em que o grande desafio é extrair informação útil desses grandes e variados conjuntos de dados. (DHAR, 2013; CONCOLATO, 2017)

Consoante a isso, Ribeiro (2021) retrata o grande índice de trabalhos presenciais que migraram para apresentações on-line, as lojas adotaram as redes sociais para se manter no mercado, e como o usuário pode se proteger diante de

tantas informações instantâneas e a diversidade de produtos e acessos que as mídias apresentam:

Cabe ao titular de dados verificar atentamente a política de cookies, o aviso de privacidade, os termos de uso e o que cada uma delas fará com os dados, qual a finalidade de fornecer esses dados, qual a necessidade de serem coletados, se há proteção e transparência em relação a eles, se são compartilhados com outras empresas e, se sim, com quem. (RIBEIRO, 2021)

É de suma importância para se proteger, que o usuário troque suas senhas periodicamente, evitar o preenchimento dos formulários que pedem os e-mails, endereço, CPF, e principalmente a inserção de cartões de crédito em sites de compras de aplicativos. Toda inscrição em qualquer rede social, usa os e-mails inseridos para noticiar propagandas, oferecer produtos ou registrar algum tipo de informação posta nas redes. (RIBEIRO, 2021).

Paralelo a isso, Teixeira, Faria, Silva e Oliveira (2021) evidenciam:

A interpretação da LGPD não pode ser realizada sem a observação de seus princípios norteadores, sendo essencial é necessário entender a forma com a qual a privacidade alterou-se diante da sociedade informacional, moldando-se para dar ao indivíduo o poder de controle sobre a coleta e tratamento de seus dados pessoais. (TEIXEIRA; FARIA; SILVA; OLIVEIRA, 2021)

Teixeira, Faria, Silva e Oliveira (2021) reforçam ainda que essa revolução tecnológica e exponencial “trouxe uma necessidade econômico-social da proteção de bens materiais”, e do outro lado, “observará que a revolução da informática trouxe a necessidade da imposição de limites éticos a coleta, utilização e distribuição de informações pessoais”. A coleta de dados acontece em todos momentos, *online* ou *offline*.

3.1 O NOVO TERMO FILTROS BOLHAS

Na atualidade, por meio das redes sociais, um novo termo vem ganhando conhecimento entre os indivíduos, filtro bolhas, o qual é caracterizado pelo uso de algoritmos e a manipulação de dados pessoais por meio desse artifício,

consequentemente ferindo o respeito à privacidade e escolha de informações exposta sobre os usuários e titulares dos dados por meio das redes.

Além disso, as redes sociais mais conhecidas no mundo como por exemplos, Facebook, Instagram e Twitter, e agora recentemente o TikTok também, usam esse recurso com o intuito de filtrar as informações, conteúdos para chegarem ao indivíduo, logo, selecionando gostos e preferências dos usuários. No entanto, é algo indefinido por que esses algoritmos acham o que é melhor para essa pessoa, muitas das vezes roubando a escolha do próprio indivíduo.

Portanto, como conceitua Eli Pariser (FREITAS; BORGES; RIOS, 2016), os chamados filtro-bolhas atuam analisando o comportamento dos usuários, dessa forma, observado as atividades desses internautas com o propósito de formar um padrão de conteúdo, visando os interesses desse internauta.

Entretanto, anteriormente, essas redes sociais apresentavam suas publicações de ordem cronológicas, mas com o crescente aumento de usuários, foi necessário criar novos recursos, um deles foi o conhecido como Edge Rank, o qual filtra publicações, mas possui três aspectos relevantes dessa ferramenta, referente a Eli Pariser, sendo eles.

O primeiro é a afinidade: quanto mais próxima a nossa amizade com alguém-o que é determinado pelo tempo que passamos interagindo com a pessoa e investigando seu perfil -, maior será a probabilidade de que o Facebook nos mostre suas atualizações. O segundo é o peso relativo de cada tipo de conteúdo: atualizações sobre relacionamentos, por exemplo, têm peso grande; todos gostam de saber quem está namorando quem [...] O terceiro é o tempo: itens mais recentes têm mais peso do que postagens mais antigas (FREITAS; BORGES; RIOS, 2016, p. 3).

Dessa maneira, com esse recurso, o usuário passa mais tempo nas redes sociais, por consequência de estar sempre disponíveis conteúdos de seus interesses e de seus gostos, e com esse mecanismo de mapear o perfil das pessoas, são serviços altamente lucrativos, gerando e transformando as redes sociais como um meio de comércio.

3.2 VAZAMENTO DE DADOS VIRTUAIS

Um exemplo de um grave e catastrófico quadro de vazamentos massivos de dados é o caso que aconteceu em 2018 da Cambridge Analytica, a qual é uma empresa americana que coletou informações pessoais de 50 milhões de usuários, através da rede social Facebook. De acordo com essa situação, a empresa usou esses dados para realizar propaganda política, e conseguiram esses dados por meio de um teste psicológico disponível nesse aplicativo.

Outro acontecimento em 2018 foi à acusação do Ministério Público do Distrito Federal a empresa pública de tecnologia, a qual é vinculada ao Ministério da Fazenda, sendo apontado por divulgar bases de dados pessoais de brasileiros da Receita Federal para um site na web, conhecido como Consulta Pública.

Além disso, o aspecto interessante sobre esse caso foi à atualização dos dados disponibilizados no site e como esses dados eram apresentados no mesmo. De acordo com o ofício feito pelo MP-DF, o qual foi enviado ao MPF: “A estruturação dos dados foi um indicativo de que a base de dados utilizada tinha origem na administração pública”.

Dessa forma, é de suma importância uma reflexão sobre a moralidade, motivando a criação de novas legislações para a criação de um cenário de segurança jurídica com a padronização de normas e práticas, em conformidade com a lei. Portanto, vale ressaltar que a LGPD não tipifica crimes virtuais, mas estabelece regras preventivas sobre a coleta e tratamento dos dados.

Além disso, as redes sociais são meios que promoveu muito o mercado publicitário, aonde libera as empresas a terem acesso as informações pessoais dos usuários, para facilita redefinir preferências, trazendo sugestões que induzem ao consumo. No entanto, nesse cenário, com condutas ilegais e abusivas, sendo assim o consumidor possui menor proteção (SILVA, 2020).

Com essa situação, a LGPD determina que todos os dados pessoais podem somente ser compartilhados mediante a liberação prévia do titular. Mas, para a obtenção dos processamentos dos dados pessoais pelas empresas sem o consentimento do titular, na lei discorrem hipóteses específicas dependendo de cada caso no Art. 11, inciso II da lei nº 13.709 (BRASIL, 2018).

Outro mecanismo, ferramenta que está estruturado no meio virtual que podem manipular usuários através da plataforma usada são os bots, em abreviação

de robôs. É relevante ressaltar o seu uso o qual é abundante em campanhas políticas. Ademais, o seu uso nas redes sociais pode realizar as seguintes tarefas, “seguir pessoas, postar e direcionar mensagens, inserir links ou hashtags. Muitas vezes servem para multiplicar as informações distribuídas na rede, passando-se por contas de pessoas reais” (ITAGIBA, 2017, p.3).

3.3 PRIVACIDADE NAS MÍDIAS SOCIAIS

77

Sobre isso, Diniz (2010), esclarece:

A privacidade revela a pretensão do indivíduo, de grupos ou instituições de decidir, por si, quando, como e até que ponto uma informação sobre eles pode ser comunicada a outrem, e deste esclarecimento temos desdobramentos que dizem respeito ao direito à intimidade, como direito da personalidade e garantido constitucionalmente, o direito de ficar em paz ou de ser deixado só e o direito do respeito à vida privada.

Nesta contextualização, a privacidade se caracteriza como uma ideia a possibilitar um espaço reservado e seguro, podendo ser inviolável a repressão dos indivíduos que estão por fora, de maneira a proporcionar a evolução do indivíduo como um ser reflexivo, além de garantir por meio da prática da privacidade outros direitos possam ser possíveis. Desse modo, a privacidade também viabiliza o direito à liberdade e suas categorias, no entanto para existir a privacidade, é indispensável à tutela da autodeterminação de cada pessoa como direito fundamental. Mediante a isso, é impossível assegurar o direito à privacidade sem o exercício da liberdade, consequentemente não é possível ter liberdade se não houver privacidade.

Logo, é importante mencionar a visão de Marques Júnior, que o direito à privacidade se destaca em dois sentidos:

Duas características dos direitos da personalidade merecem registro. A primeira delas é que tais direitos, atribuídos a todo ser humano e reconhecidos pelos textos constitucionais modernos em geral, são oponíveis toda a coletividade e também ao Estado. A segunda característica peculiar dos direitos da personalidade consiste em que nem sempre sua violação produz um prejuízo que tenha repercussões econômicas ou patrimoniais, o que ensejará formas variadas de reparação, como o direito de resposta, a divulgação de desmentidos de caráter geral e/ou a indenização pelo dano moral (MARQUES JÚNIOR, 2018, p. 23).

Nesse sentido, o direito à privacidade pode ser compreendido como um direito subjetivo de qualquer indivíduo, considerando não somente a obrigação de terceiros a respeitar o espaço do próximo, além disso, de possibilitar o efetivo controle das suas informações de caráter pessoal, podendo ser classificadas como sensíveis ou não.

Portanto, para uma construção teórica dos direitos fundamentais, se idealiza duas noções, sendo a primeira os direitos fundamentais conceituados como regras, associados ao jus positivismo e ao legalismo exegético, visto que essa situação é mais comum em ordenamentos jurídicos mais fechados. Já a segunda noção é entendida sobre os direitos fundamentais como princípios, que se encontra vinculada ao constitucionalismo e sistemas mais abertos (QUEIROZ, 2002).

Mediante a referente lei LGPD, em relação à privacidade se caracteriza como a autodeterminação de informação bem como o seu livre desenvolvimento da personalidade os quais estão positivados como fundamentos desta lei. As garantias legislativas da mesma são definidas como mecanismos que podem explorar pensamentos do inconsciente dos usuários, conseqüentemente manipulando e extraindo dados desses indivíduos de forma indiscriminada.

Portanto, de acordo com Carvalho (2018) como esses dispositivos podem respeitar o direito fundamental a privacidade e a autodeterminação informativa, sem invadir esse espaço contextualizado. A partir desse momento começa os questionamentos e surge a problemática, pela perspectiva de essas redes explorarem os dados dos indivíduos sem esclarecer definitivamente onde, como e para que essas informações serão usadas.

Dessa maneira o desrespeito à privacidade das pessoas demonstra de maneira mais abrangente, desde uma pequena filtragem ou manipulação de dados que aos poucos para um leigo que não tem noções de funcionamento desses dispositivos, podendo evoluir para situações mais catastróficas, visto nível de vazamentos de dados ou vendas do mesmo para grandes empresas, como já descrito, por exemplo, o caso da Cambridge Analytica.

4 O CONSUMIDOR VIRTUAL E SEUS DADOS PESSOAIS

Mediante a vulnerabilidade do consumidor quando se trata em âmbito virtual, se refere principalmente sobre seus dados pessoais. Mesmo por um lado, a transação à distância beneficiar no avanço tecnológico e evolução social, em outra parte a economia digital introduz dificuldades no meio da defesa do consumidor.

Dessa maneira, essas dificuldades são consideradas desde em matéria de jurisdição e as aplicações das leis até as relações direcionadas a proteção e defesa do consumidor em ligação a sua agravada situação de vulnerabilidade, que se origina a partir da relação contratual eletrônica, no âmbito virtual, automático e célere, aonde é usado pelos fornecedores que dessa forma proporciona seus serviços e produtos aos usuários sendo conhecido como consumidor.

No entanto, esses consumidores sem conhecimento aprofundado na internet encontram-se o conhecido como vulnerabilidade técnica, como Marques (2002, p. 76) explica que esses usuários mesmo sem ser especialista do meio virtual, negociam, compram sem medo e por causa disso, eles necessitam de uma proteção maior e mais afetiva nesse âmbito de negociações virtuais.

Anteriormente mesmo sem ainda vim à tona a respeito da Lei Geral de Proteção de Dados, era mencionado uma discussão sobre a necessidade de uma proteção maior para os consumidores virtuais, sendo citado por Marques (2002, p. 76-77) “parece ser a finalidade maior da doutrina brasileira e dos projetos de leis existentes sobre o assunto”, além de visar uma melhora na posição jurídica contratual do consumidor, sendo caracterizado como um leigo no comércio virtual, e ainda considerado como um elo mais fraco.

Portanto, esse novo avanço comercial torna o consumidor vulnerável em ligação aos seus dados pessoais, conseqüentemente pondo em risco sua intimidade e sua privacidade. Em relação em como funciona essa atividade do consumidor em interação o âmbito virtual, esse mecanismo, é dividido em dois, de acordo com Vieira (2007, p. 195), que explica sendo “pela formação de arquivos com informações pessoais” e pela “vigilância do comportamento das pessoas”.

Dessa forma, vale ressaltar que a internet gira em torno de informações, e mediante a isso, possibilita que a intimidade e a vida privada de usuários possam ser exploradas. Mecanismo que empresas utilizam para personalizar o marketing disponibilizando eficiência aos serviços oferecidos. Deste modo surge a denominada

sociedade de informação a qual atua como uma ameaça a privacidade de seus usuários.

Destarte que a vulnerabilidade do cliente no meio virtual está relacionada com a constatação de que os seus dados pessoais são dispostos na rede. Logo, destaca a sociedade interconectada através da internet, que tem como principal fundamento a informação, que pode fornece os dados pessoais em várias formas, sendo elas nome, número de celular, número do cartão, isso em cada visita a uma página eletrônica diferente. Além disso, essas informações pessoais dos consumidores acabam sendo comercializadas a terceiros, muita das vezes sem o conhecimento do usuário (FERREIRA, 2008, p. 171).

4.1 CONSENTIMENTO DO TITULAR DOS DADOS NA LGPD

A LGPD dispõe em alguns dispositivos determinando o consentimento ao registrar de maneira escrita e uma forma de manifestação livre, sendo informado e claramente ao titular dos dados concorde com o tratamento de suas informações pessoais para a tal finalidade, referente ao inciso XII do artigo 5º “XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”.

Na prática, esse consentimento é garantido por um simples clique onde o usuário concorda mediante ao contrato de adesão pelas redes sociais consequentemente autorizando o uso de seus dados através da plataforma, como já descrito neste artigo a ferramenta cookies.

Logo, apesar de redes sociais como, por exemplo, Instagram, Facebook, Twitter terem esses termos de uso e privacidade, que podem ser visto e estão disponíveis a qualquer momento, poucos usuários veem. De acordo com um levantamento realizado pela Folha, 4 horas e meia seriam necessários para ler os regulamentos de uma rede social, sendo as mais usadas no país.

Mas também, nesses termos de adesão, além de serem extensos, esses regulamentos possuem uma linguagem técnica que exigem conhecimentos jurídicos, sendo não muito convidativa a sua leitura. Dessa forma, é comum encontrar política

de privacidade e uso de dados que não exemplifiquem ou simplifiquem de maneira exata e minuciosa quais os dados e informações que irão ser usados, como, para que e quais os impactos que o uso do mesmo traz.

Portanto, não deveria ser uma prioridade dessas redes sociais como, por exemplo, Instagram e Facebook disponibilizar de uma forma detalhada e assertiva a extração das informações dos usuários. Além disso, muitas pessoas usam essas redes para seu entretenimento e diversão, mas vale lembrar que há muito lucro e negócios com os dados dos usuários. Dessa forma, o modo de consentimento do titular dos dados estabelecidos pela LGPD, não está sendo respeitado por essas plataformas.

Referente a esta lei no inciso XVII, artigo 5º e também os princípios de livre acesso e transparência que estão inseridos nos artigos 6º e 8º, disponibilizando através desses dispositivos que devem impor ao usuário as informações necessárias, sendo detalhadas e assertivas, sobre as formas de coleta de seus dados, os critérios e parâmetros de realização do mesmo, além das formas de processamento dos dados e os resultados dentro de outros aspectos importantes e relevantes para o consentimento do usuário.

Todavia, a LGPD não trata de formas específicas, melhores ou piores condições de consentimento juridicamente eficazes, pois compreende essa questão de forma abrangente, noutra escala, expondo limites históricos e sociais para qualquer forma de cessão de dados pessoais, independente de seus adjetivos. Por mais que a vigência dessa lei venha a significar um marco jurídico para a proteção de dados pessoais no Brasil, ela precisa ser visto no contexto da economia política que lhe recebe que é da mercantilização dos dados em uma economia da vigilância. (FORNASIER; KNEBEL, 2020, p. 5).

No entanto, diante das situações citadas acima, é apresentado um padrão mundial na maneira de garantir o consentimento ou até mesmo por meio das dificuldades relacionando a outros modelos e formas de garantir esse consentimento por meio legítimo, sempre visando oferecer uma melhor e prática visão ao usuário, logo a LGPD falha nesse aspecto, ao reconhecer essa forma, que ainda apresenta frágil e não necessariamente tão simplificada sendo considerada válida.

4.2 FORNECEDOR X CONSUMIDOR VIRTUAL

Com os grandes avanços tecnológicos, o Marco Civil da internet possibilita uma garantia aos usuários do consentimento dos seus dados sendo disponibilizados sua coleta, armazenamento e utilidade de suas informações pessoais, mediante ao Código de Defesa do Consumidor, o qual busca estabelecer um reequilíbrio na conexão entre o consumidor e o fornecedor, visando em proteger o consumidor das mais diversas maneiras de abusividade contratuais.

No entanto, este Código de Defesa do Consumidor, não engloba em todas as possíveis situações em relação de consumo. Esta relação em caso sendo o consumo digital o qual vai além de tudo isso, não se resumindo somente na ligação do fornecedor (provedor) e consumidor.

Mediante a isso, visa à necessidade de estender a proteção à relação comercial no meio virtual, sendo compreendida por Bioni (2019, p. 12-13) “com a inteligência gerada pela ciência mercadológica, especialmente quanto à segmentação dos bens de consumo (marketing) e a sua promoção (publicidade), os dados pessoais dos cidadãos converteram-se em um fator vital para a engrenagem da economia da informação”.

Portanto, a privacidade do consumidor se transforma em moeda de troca, nessa nova era de informação, como citado por Vieira (2007, p. 197), a empresa Blockbuster utiliza esse mecanismo armazenando registros eletrônicos contendo informações pessoais para disponibilizar “descontos”, gerando lucro para a empresa com essa ideia de comercialização.

Outro exemplo é a empresa Geocities, a qual possibilita páginas na internet gratuitas somente se seus usuários preenchessem formulários com seus dados pessoais, como formação educacional, profissão, endereço e áreas de interesse, com o intuito de coletar essas informações para vendê-los para as empresas de marketing.

Dessa forma, é visto como essencial a preservação do princípio da dignidade do indivíduo de acordo com os direitos de personalidade, sendo este direito protegido pela Constituição de 1988, “limite e a tarefa primordial dos poderes do Estado, da coletividade e de cada indivíduo, constituídos sob uma dualidade”, que mediante a Gonçalves (2013, p. 5) relaciona o direito defensivo e o direito

prestacional, considerando o primeiro quanto à proteção da esfera individual envolvendo o Poder Público e dos compatriotas. Já no segundo caso, se refere quanto à ação do Poder Público com a finalidade de garantir a não interferência de terceiros na intimidade e na vida privada de outros cidadãos.

4.3 PENALIDADES DA LGPD MEDIANTE A LEI

Mediante as sanções estabelecidas no artigo 52 da LGPD, por consequência dos descumprimentos relacionados a esta lei, começaram a serem aplicadas em agosto do ano passado de 2021, a qual foi aprovada em 2018. Dessa forma, a Autoridade Nacional de Proteção de Dados (ANPD) poderá aplicar penalidades mediante cada desacordo.

Primeiramente, as empresas que não se adequam aos prazos de acordo com a legislação, sofrem uma advertência, além da possibilidade de se ter uma multa simples sobre o faturamento, que pode ser de até 2% do faturamento da pessoa jurídica. Sendo o limite estipulado em 50 milhões de reais por infração cometida.

Outra penalidade é a multa diária, parecida com a anterior, também será limitada 50 milhões de reais, porém, seguindo a notoriedade da infração, acontece à divulgação pública da infração, causando enormes prejuízos à imagem da empresa e o bloqueio dos dados, que as impede de usar quaisquer informações coletadas até que a situação se regularize. E para finalizar, tem a eliminação dos dados pessoais, a qual a LGPD obriga a empresa a eliminar por completo os dados coletados em seus serviços.

5 CONSIDERAÇÕES FINAIS

Mediante a este assunto, pode-se concluir que por consequências dos grandes avanços tecnológicos no âmbito virtual, viu-se a necessidade de criar normas essenciais para acompanhar a evolução dos dias atuais, sendo assim, a Lei Geral de Proteção de Dados Pessoais foi um progresso principalmente para o espaço virtual, viabilizando para o consumidor poder usufruir das redes sociais com

segurança e privacidade.

Além disso, esta Lei nº 13.709/2018 prioriza os fundamentos da privacidade e respeito dos direitos humanos, possibilitando a liberdade de expressão nas mídias sociais, promovendo a correlação entre a pessoa e o meio virtual, de acordo com as necessidades de cada pessoa, facilitando e priorizando as pesquisas que ajudam tanto o usuário como também as empresas a venderem e promover os seus produtos.

Outro aspecto importante foi à autodeterminação informativa que é caracterizada como a ferramenta necessária na parte ativa dos dados dos titulares, o qual condiz com o seu consentimento, referindo à livre manifestação, o qual favorece o desenvolvimento de conhecimentos informativos ao ser realizado o tratamento dos dados pessoais.

Portanto, a LGPD providencia um papel de suma importância ao estimular a autonomia do titular, propiciando o autocontrole que o mesmo executa com os seus dados. E em conformidade com a lei, suas políticas direcionada as empresas de redes sociais, obteve mudanças após muitos vazamentos e compartilhamentos de dados pessoais sem a permissão de seus retrospectivos donos foi estabelecido penalidades, as quais são aplicadas pela falta dessa conscientização esta foi à solução deste problema.

Diante disso, o presente artigo objetivou discorrer sobre um tema que avança juntamente com a tecnologia, com está lei em vigor ofereceu mais segurança e privacidade aos usuários e as empresas como foi detalhado. No entanto, é necessário que seja informado de maneira clara e objetiva todas as informações importantes, principalmente nos sites e redes sociais, os quais os clientes compartilham os seus dados e que ainda se encontra um receio nesse aspecto de divulgar sem a conscientização do proprietário dos dados, obtendo a necessidade de proteção de dados no âmbito virtual.

REFERÊNCIAS

BOFF, Salete Oro; FORTES, Vinícius Borges; FREITAS, Cinthia Obraden de Almendra. **Proteção de Dados e Privacidade**. Rio de Janeiro, Lumen Juris, 2018.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidente da República, 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em 20 de abril de 2022.

BRASIL. **Lei Geral de Proteção de Dados Pessoais - Lei nº 13.709/2018**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 27 de outubro de 2021.

BRASIL. **Lei nº 13.853, de 8 de julho de 2019**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 17 de Março de 2022.

CARVALHO, Vitor Miguel Barros de. **O Direito fundamental à privacidade ante a monetização de dados pessoais na internet**: apontamentos legais para uma perspectiva regulatória. Trabalho de Conclusão de Curso- UFRN. Natal. 2018.

COELHO, Gabriela. MP-DF acusa empresa pública de vender dados pessoais de brasileiros. **Revista Consultor Jurídico**, 2018. Disponível em: <https://www.conjur.com.br/2018-mai-31/mp-df-acusa-empresa-publica-vender-dados-brasileiros>. Acesso em: 13 de julho de 2022.

CONCOLATO, Claude E.; CHEN, Li M. Data science: A new paradigm in the age of big-data science and analytics. **New Mathematics and Natural Computation**, v.13, n. 2, p.119-143, 2017.

COSTA, Ramon Silva; OLIVEIRA, Samuel Rodrigues de. Os direitos da personalidade frente à sociedade de vigilância: privacidade, proteção de dados pessoais e consentimento nas redes sociais. **Revista Brasileira de Direito Civil em Perspectiva**, Belém, v. 5, n. 2, p. 22-41, Jul/Dez, 2019. Disponível em: <https://indexlaw.org/index.php/direitocivil/article/view/5778/pdf>. Acesso em: 28 de Outubro de 2021.

CUNHA, Juliana. **O que são os metadados?** Safernet. 2019. Disponível em: <http://new.safernet.org.br/node/199>. Acesso em: 13 de Julho de 2022.

DHAR, V. Data science and prediction. **Communications of the ACM**, v.56, p.64-73, 2013.

DINIZ, Maria Helena. **Dicionário Jurídico**. V.2. São Paulo: Saraiva, 2010, p. 751.

FORNASIER, Mateus de Oliveira; KNEBEL, Noberto Milton Paiva. O titular de dados como sujeito de direito no capitalismo de vigilância e mercantilização dos dados na Lei Geral de Proteção de Dados. **Revista Direito e Práxis**, Rio de Janeiro. 2020.

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVIA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. 1ed.

Thomson Reuters Brasil, São Paulo, 2019.

FREITAS, Carlos Eduardo Pereira; BORGES, Messias Vasconcelos; RIOS, José Riverson Araújo Cysne. O algoritmo classificatório no feed do Instagram. In: **CONGRESSO BRASILEIRO DE CIÊNCIA DA COMUNICAÇÃO**, 39, 5-9 set. 2016, São Paulo (SP). Anais... São Paulo: Intercom, 2016. Disponível em: <https://repositorio.ufc.br/handle/riufc/44471>. Acesso em: 16 abr. 2022.

GOMES, Rodrigo Dias de Pinho. **Privacidade em perspectivas**: Desafios à privacidade: Big Data, Consentimento, Legítimos Interesses e Novas Formas de Legitimar o Tratamento de Dados Pessoais. Editora Lumen Juris, Rio de Janeiro, p. 233, 2018.

HERNANDES, Raphael. Leitura de 'termos e condições' de serviços na internet exige 4,5 horas. **Folha de S. Paulo**. 2017. Disponível em: <https://www1.folha.uol.com.br/tec/2017/12/1945132>. Acesso em: 16 abr. 2022.

HIRATA, Alessandro. O Facebook e o direito à privacidade. **Revista de informação legislativa**, v. 51, n. 201, p. 17-27, jan./mar. 2014. Disponível em: <http://www2.senado.leg.br/bdsf/handle/id/502950>. Acesso em: 27 out. 2021.

ITAGIBA, Gabriel. Fake news e Internet: Esquemas, bots e a disputa pela atenção. **Instituto de Tecnologia e Sociedade do Rio**, p.3, 2017. Disponível em: https://itsrio.org/wp-content/uploads/2017/04/v2_fake-news-e-internet-bots.pdf. Acesso em: 14 jul. 2022.

LÉVY, Pierre. *Cibercultura*. 1.Ed. São Paulo: Editora 24. 2011. 133p.

MARQUES JÚNIOR, William Paiva. Obstáculos impostos a efetividade do direito personalíssimo a privacidade na Era do Big Data: uma problemática da sociedade contemporânea. **Direito Civil Contemporâneo II**. 01 ed. Florianópolis, CONPEDI, 2018, V. 01, P. 23-43. Disponível em: <http://site.conpedi.org.br/publicacoes/0ds65m46/41oo8qd1>. Acesso em 16 abr. 2022.

MARQUES, Claudia Lima. A proteção do consumidor de produtos e serviços estrangeiros no Brasil: primeiras observações sobre os contratos à distância no comércio eletrônico. **Revista da Faculdade de Direito da UFRGS**, v. 21, p. 65-99, mar. 2002. Disponível em: <https://seer.ufrgs.br/revfacdir/article/download/72366/40931>. Acesso em 27 out. 2021.

MEDEA, Guilherme. A sociedade do Big Data e os impactos da LGPD. **Migalhas**, 2021. Disponível em: <https://www.migalhas.com.br/depeso/345225/a-sociedade-do-big-data-e-os-impactos-da-lgpd>. Acesso em: 14 jul.2022.

MORAIS, José Luiz Bolzan de; MENEZES NETO, Elias Jacob de. **Marco Civil da Internet**: A insuficiência do marco civil da internet na proteção das comunicações

privadas armazenadas e do fluxo de dados a partir do paradigma da surveillance. Atlas, São Paulo, 2014.

OLIVEIRA, Christiane. **Lei geral de proteção de dados pessoais (lgpd), lei nº 13.709/2018**: Direito à privacidade aplicada às redes sociais. 2021. 19f. Trabalho de Conclusão de Curso (Escola de Direito e Relações Internacionais) – Pontifícia Universidade Católica de Goiás, Goiânia, 2021.

OLIVEIRA, Jordan Vinícius de Oliveira; SILVA, Lorena. Abbas da Cookies de navegador e história da internet: Desafios à lei brasileira de proteção de Dados pessoais. **Revista de Estudos Jurídicos UNESP**, a.22, n.36, 2018. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/handle/123456789/1576.pdf>. Acesso em: 17 de março de 2022.

QUEIROZ, Cristina, M.M. **Direitos Fundamentais: teoria geral**. Editora Coimbra. 2002.

RIBEIRO, Cinthya Imano Vicente. **LGPD**: Como proteger a privacidade na era das redes sociais, 2021. Disponível em: <https://aphoffmann.com.br/igpd-como-protetger-a-privacidade-na-era-das-redes-sociais/>. Acesso em: 25 out. 2021.

SILVA, Carlos Mendes Monteiro da; BRITO, Dante Ponte de. A publicidade nas redes sociais e seus impactos na cultura do consumismo. **Revista Jurídica Cesumar**, v.20, n.1, p.89-101, janeiro/abril 2020. Disponível em: <https://periodicos.unicesumar.edu.br/index.php/revjuridica/article/view/7516/631>. Acesso em: 27 out. 2021.

STRASSER, Francislaine de Almeida Coimbra; OLIVEIRA, Myllena Gonçalves de. O advento da Internet e seus desafios no campo jurídico brasileiro. **Colloquium Socialis**. ISSN: 2526-7035, 3(4), 6–19, 2020. Disponível em: <http://journal.unoeste.br/index.php/cs/article/view/3357>. Acesso em: 27 de Outubro de 2021.

TEIXEIRA, Ana Clara Campos; FARIA, Evânia Gizele Rodrigues de; SILVA, Fabiana Maria da; OLIVEIRA, Jhenifer Cristiny. Lei Geral de Proteção dos Dados: LGPD para Mídias Sociais. **Revista Projetos Extensionistas**. v. 1, n. 2, p. 235-240, jul./dez. 2021. Disponível em: <https://periodicos.fapam.edu.br/index.php/RPE/article/view/514/269>. Acesso em: 25 de outubro de 2022.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Consentimento e Proteção de Dados Pessoais na LGPD in Lei Geral de Proteção Pessoais e suas Repercussões no Direito Brasileiro**. Revista dos Tribunais, São Paulo, 2019.

XAVIER, Fernando; OLENSCKI, João Rodrigo W.; ACOSTA, André Luis; SALLUM, Maria Anice Mureb; SARAIVA, Antonio Mauro. Análise de redes sociais como

estratégia de apoio à vigilância em saúde durante a Covid-19. **Estudos Avançados.** 2020, v. 34, n. 99, pp. 261-282. Disponível em: <https://doi.org/10.1590/s0103-4014.2020.3499.016>. Acessado em 25 out. 2022.

Recebido em: 15/09/2022

Aprovado em: 28/10/2022