FACULDADE DE DIREITO DE VITÓRIA
CURSO DE GRADUAÇÃO EM DIREITO

MARCELLY SOUZA PEREIRA

OS IMPACTOS DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) SOBRE OS CONTRATOS DE CONSUMO

VITÓRIA
2021

MARCELLY SOUZA PEREIRA

ANÁLISE DOS IMPACTOS DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) SOBRE OS CONTRATOS DE CONSUMO

Trabalho de Conclusão de Curso apresentado ao curso de Direito da Faculdade de Direito de Vitória – FDV, como requisito parcial para obtenção do grau de bacharel em Direito.

Orientadora: Prof.ª Ivana Bonesi.

VITÓRIA

2021

RESUMO

Com a ascensão da tecnologia nas relações contratuais, a grande maioria dos contratos de adesão de consumo são celebrados virtualmente. Diante desse cenário, surgiu a necessidade de uma regulamentação específica sobre a coleta de dados realizada pelos fornecedores por meio dessas contratações. Até o ano de 2018, a legislação aplicável ao tema se restringia ao Código de Defesa do Consumidor, Código Civil e Constituição Federal. Tais legislações, entretanto, tornaram-se insuficientes, na medida em que já não mais contemplavam as inovações advindas da era virtual. Surge, então, a Lei nº 13. 709/18, Lei Geral de Proteção de Dados (LGPD), com o intuito de proteger o consumidor frente às abusividades praticadas a partir de supostas permissões contidas nos contratos de consumo. Essa inovação legislativa propõe-se a zelar pelos dados pessoais dos consumidores e impedir que empresas captem, tratem e compartilhem tais informações de maneira indevida. Buscou-se, analisar as mudanças acarretadas pela lei, aos contratos de consumo. Ademais, pretendeu-se verificar se as empresas, ainda hoje, permanecem utilizando de cláusulas abusivas em seus contratos de adesão para justificar uma coleta indevida de dados. Nesse contexto, é esclarecida a atuação da Agência Nacional de Proteção de Dados (ANPD), responsável por aplicar as sanções previstas na LGPD. Por fim, chegou- se a conclusão acerca de como a LGPD vem atuando, no sentido de vedar as ilegalidades contidas nos contratos de adesão e a desenfreada por dados pessoais de consumidores.

Palavras-chave: Lei Geral de Proteção de Dados. Consentimento. Contrato de adesão. Privacidade. Dados Pessoais.

SUMÁRIO

1 INTRODUÇÃO

A Lei Geral de Proteção de Dados (LGPD), nº 13.709/18 (BRASIL, 2018), abarcou diversas inovações à temática da proteção de dados do consumidor. Apesar de já existirem certos regulamentos e leis no sentido de proteger o consumidor, frente à ascensão virtual cada vez mais evidente, foi apenas a partir da LGPD que se tornou possível uma regulamentação específica e que abrangesse os diversos tipos de abusos que os indivíduos, em uma relação contratual de consumo, pudessem ser vítimas.

Conforme será demonstrado, as inovações tecnológicas, apesar de beneficiarem o dia a dia da população, acabaram promovendo também um ambiente vulnerável ao consumidor. Anteriormente à elaboração da lei, devido à inexistência de regulamento específico acerca da proteção de dados, um indivíduo, ao se utilizar de serviços on-line, ou em ambientes físicos, se via obrigado a aceitar um contrato para acessar ou consumir o que desejasse.

A partir disso, possivelmente devido ao desconhecimento do conteúdo inserido nas cláusulas do contrato, tendo em vista a linguagem técnica e inacessível disposta, os contratantes, habitualmente, apenas concordam com os termos ali dispostos, sem efetivamente lerem o que estava inserido nas cláusulas. Deste modo, a vulnerabilidade do consumidor, que se expressa por meio de sua irrestrita concordância, mesmo desconhecendo o conteúdo contratual, acabava por permitir às empresas a captação e tratamento de seus dados, de maneira, até então, desconhecida.

Devido ao desconhecimento do conteúdo inserido nas cláusulas do contrato disposto, o consumidor não compreende estar celebrando um contrato de adesão. Essa modalidade contratual é caracterizada por ter suas cláusulas pré-determinadas e sem possibilidade de serem debatidas. Dessa forma, ao aceita-las, o consumidor permite que se utilizem de seus dados, possivelmente de maneira indevida, ocasionando transtornos, tendo em vista que a prática desenfreada culminou em diversos casos de vazamentos de informações pessoais.

A partir da exposição de tais fatos, pode-se comprovar a importância do estudo da Lei Geral de Proteção de Dados, uma vez que as situações de abusos relacionadas a utilização indevida de dados apenas cessarão a partir de uma aplicação incisiva da lei. Assim, a legislação deve atuar fiscalizando o correto tratamento de informações, vedando a atuação de corporações em desconformidade com a lei, além de atribuir sanções a quem contrariar suas disposições.

Diante desse cenário, o presente estudo se propõe a analisar os impactos da Lei Geral de Proteção de Dados sobre os contratos de consumo, até então estabelecidos por empresas e organizações, tanto em ambientes físicos quanto virtuais. Além disso, busca -se- á verificar as cláusulas de determinados contratos de consumo, utilizados no meio digital, verificando a existência, ou não, de cláusulas abusivas.

Ademais, o estudo se propõe a responder de que maneira os mecanismos da Lei, aplicados pela Agência Nacional de Proteção de Dados (ANPD) e há pouco tempo vigentes, poderão impedir a utilização de cláusulas contratuais em desconformidade com a lei, bem como as sanções aplicáveis as corporações infratoras.

2 CAPÍTULO I- O CENÁRIO DA LEGISLAÇÃO BRASILEIRA PRÉ LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

As seguintes seções do trabalho acadêmico se propõem a investigar a Lei Geral de Proteção de Dados, sua atuação desde a implementação, as diferenças entre ela e a legislação até então utilizada para regulamentar a proteção de dados dos consumidores, bem como, almeja analisar determinados contratos de consumo que possam impor ao consumidor cláusulas contratuais que firam a LGPD.

2.1 DO CÓDIGO DE DEFESA DO CONSUMIDOR E CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL.

O contexto da legislação brasileira previamente à elaboração da Lei Geral de Proteção de Dados, para a proteção do consumidor e o tratamento adequado de seus dados, era disciplinado exclusivamente por matérias elencadas no Código de Defesa do Consumidor (CDC) e pela Constituição da República Federativa do Brasil (BRASIL, 1988).

Para regular a proteção dos dados do consumidor antes da implementação da Lei Nº 13.709/18, o CDC se pautava habitualmente em matérias de contrato de adesão, uma vez que esse tipo de contrato, encontrado virtualmente e em ambientes físicos, compele o aceite integral de seus termos pelo consumidor. Quanto aos artigos utilizados por essa disciplina, o art. 43, referente ao banco de dados e cadastro, era amplamente utilizado e elucida que todo consumidor deve ter acesso a informações sobre ele, sejam elas de cadastros ou qualquer tipo de arquivo que contenha informações pessoais, é um direito assegurado a ele, saber a fonte de tais registros. Segundo Bruno Ricardo Bioni (2021, p. 211) sobre a utilização do artigo de lei supracitado:

> Nota-se a amplitude do dispositivo em questão, que alcança todo e qualquer dado pessoal do consumidor, indo muito além, portanto, dos bancos de dados de informação negativas para fins de concessão de crédito. A racional do legislador foi alcançar todo e qualquer banco de dados que atinja o livre desenvolvimento da personalidade do consumidor.

Deste modo, é evidente que o artigo de lei se preocupava em garantir a autonomia e controle do consumidor quanto a suas informações pessoais em relações de consumo.

Além da utilização do art. 43 para a proteção do consumidor, posteriormente, o art. 51 do Código de Defesa do Consumidor, o qual dispõe sobre a nulidade de cláusulas e possui o intuito de limitar os abusos cometidos por fornecedores de produtos e serviços, tornou-se amplamente utilizado em decorrência da crescente abusividade de cláusulas em diversos tipos de contratos. O art. 51 do CDC foi o primeiro a dispor sobre a nulidade de cláusulas abusivas em contratos, visando diretamente proteger o consumidor de eventuais abusos.

Sobre o art. 51 do CDC ser o primeiro artigo a dispor sobre essa nulidade, João Batista de Almeida (2003, p. 142) afirma:

> [...] O regime codificado elencou as cláusulas contratuais abusivas, hauridas da experiência estrangeira, da jurisprudência nacional e do cotidiano dos órgãos de defesa do consumidor, dentre aquelas mais costumeiramente usadas para lesar o consumidor. Após tipificá-las, o Código sancionou-as de nulidade absoluta (art. 51, seus incisos e parágrafos), com as decorrentes consequências jurídicas: tais cláusulas nunca terão eficácia; não convalescem pela passagem do tempo, nem pelo fato de não serem alegadas pelo interessado; podem ser pronunciadas de ofício pelo juiz, dispensando arguição da parte; não são supríveis e não produzem qualquer efeito jurídico, pois a declaração de nulidade retroage à data da contratação.

No que se refere à jurisprudência sobre o tema, e o livre consentimento do consumidor, destaca Bruno Ricardo Bioni (2021, p. 284) que

> em 2017 a 4ª Turma do Superior Tribunal de Justiça decidiu em recurso especial ser abusiva cláusula prevista em contrato de prestação de serviço da administração de cartão de crédito que permite ao banco compartilhar dados dos consumidores com outras instituições financeiras e de serviços de prestação ao crédito.

Para fundamentar a decisão dos ministros acerca do Recurso Especial, foi utilizado o art. 51 do Código de Defesa do Consumidor, o qual aborda e reafirma veementemente o consentimento livre do consumidor quanto à maneira que seus dados serão tratados, o que se espera ser de maneira segura e privada, não compartilhando com outras instituições, como no caso em questão.

Além do Código de Defesa do Consumidor, a matéria de proteção ao consumidor e correto tratamento de seus dados encontra previsão no Código constitucional. A

Constituição Federal possui diversos princípios norteadores relacionados à privacidade e proteção de dados, amplamente utilizados no período anterior à Lei Geral de Proteção de Dados, e até mesmo após.

Direitos como o direito à informação, elencado no art. 5º, XXXIII; à inviolabilidade do sigilo de dados, art. 5º, XII; o princípio da transparência, art. 5º, *caput* e o art. 24, VIII, o qual assegura que compete concorrentemente à União, Estados e Distrito Federal, a responsabilidade por dano ao consumidor eram e ainda são utilizados em conjunto com o Código de Defesa do Consumidor, para tentar impedir com que cláusulas abusivas em contratos de adesão lesassem o consumidor.

Todavia, tais matérias relacionadas no Código consumerista e no texto constitucional são disciplinadas por dispositivos legais de ordem geral e princípio lógica e, por vezes, revelam-se insuficientes para o tratamento do tema, tendo em vista as transformações pelas quais o tratamento de dados pessoais está percorrendo. Segundo Rizatto Nunes (2009, p. 79), “[...] passou-se o século XX inteiro aplicando-se basicamente o Código Civil de 1916 para as relações de consumo, fundado na tradição do direito civil europeu do século anterior, até a entrada em vigor do Código de Defesa do Consumidor”.

Atrelado à esse entendimento, com a era digital cada vez mais presente, o tratamento de dados tende a ocorrer cada vez mais de maneira digital, em detrimento do aparato constitucional até então regulador da matéria, o qual se tornou arcaico e abriu margem para que abusos com dados pessoais ocorressem cada vez com mais frequência, principalmente quando relacionados aos conhecidos contratos de adesão.

2.2 DOS CONTRATOS DE ADESÃO E CONSENTIMENTO DO CONSUMIDOR

Anteriormente à promulgação da Lei Geral de Proteção de Dados, como já citado, a proteção de dados do consumidor era regulada, predominantemente, pelo Código de Defesa do Consumidor, inclusive quanto à matéria de contratos de adesão, amplamente utilizada para regular a celebração de contratos entre fornecedor e consumidor, desde o “mero” aceite dos chamados Termos de Uso de um determinado *site*, até a celebração de grandes compras, em comércios físicos ou eletrônicos.

Os exemplos citados abordam situações em que o consumidor necessita compartilhar diversos dados particulares com um sistema digital, seja em ambiente físico ou virtual. Contudo, como o surgimento da LGPD ocorreu apenas décadas após, alguns anos após essa prática de coleta ser implementada, até então não existia legislação específica sobre o tema. Assim, o consumidor, mesmo sem ter conhecimento do exato teor das cláusulas do contrato de adesão que estava aceitando, o fazia para poder ter acesso ao serviço que desejava, seja para poder acessar um *site*, adquirir descontos em loja ou similares, colocando-os assim em uma situação de desigualdade e vulnerabilidade.

De acordo com Cláudia de Lima Marques (2002, p. 106), sobre os contratos, majoritariamente de adesão, não permitirem ao consumidor debater as cláusulas antes de concordar com os termos, é disposto que “as cláusulas contratuais assim elaboradas não têm, portanto, como objetivo realizar o justo equilíbrio nas obrigações das partes, ao contrário, destinam-se a reforçar a posição econômica e jurídica do fornecedor que as elabora.” Assim, é evidente que o consumidor se encontra em condição de vulnerabilidade ao concordar com os chamados Termos de Uso, a partir de um simples *click.*

Além da disparidade e desequilíbrio entre as partes devido ao contrato de adesão aceito pelo consumidor, em 2018, uma pesquisa realizada pela Universidade de York, em Toronto, e a Universidade Connecticut, concluiu que 86% dos participantes da pesquisa leram os termos de uso de um ambiente digital que desejavam acessar, em menos de 1 minuto, o que claramente não é suficiente para que o consumidor concorde realmente com as cláusulas dos termos postos.

A legislação brasileira não obriga *websites* a utilizarem ferramentas responsáveis por estipularem ditames e condições para que um usuário possa utilizar seus serviços, bem como não determina que lojas de ambientes físicos coletem dados de seus clientes e consumidores. Contudo, a maior parte dos *sites* e ambientes físicos o faz, por meio da ferramenta intitulada Termos de Uso.

As cláusulas do Termo estão suscetíveis a pequenas mudanças que variam de acordo com o interesse do fornecedor do produto. Contudo, ainda assim, costumam seguir um modelo e determinadas características, dentre elas, as letras miúdas que discorrem sobre as cláusulas do contrato em questão, o que pode ser um problema, como assevera Bruno Bioni:

> Políticas de privacidade e termos de uso com textos longos e pouco claros não transmitem, na maioria das vezes, uma mensagem adequada para que o consumidor seja cientificado a respeito do fluxo dos seus dados pessoais. Ao revés, acaba por desinforma-lo, trazendo ainda maior assimetria de informações, desconsiderando pois, o resultado ótimo/ esperado de transparência que tal canal de comunicação deve propiciar. (BIONI, 2021, p. 306)

Como já mencionado, para que o usuário acesse o *site* que deseja, é necessário o consentimento integral dos Termos de Uso da plataforma. Contudo, como no cenário anterior à Lei Geral de Proteção de Dados não havia previsão expressa sobre tratamento de dados pessoais, e principalmente sanções às empresas que não fossem transparentes com o consumidor, diversas cláusulas abusivas passaram e integrar contratos de adesão, devido à suas letras minúsculas que descreviam o teor do concreto, associadas com o pouco entendimento do consumidor sobre as cláusulas ali dispostas.

Nesse sentido, é válido o entendimento de Pinheiro (2018, p. 30) acerca do tema, de que “a informação passou a ser a principal moeda de troca utilizada pelos usuários para ter acesso a determinados bens, serviços ou conveniências”. Deste modo, é visível que com a era virtual cada vez mais presente na atualidade e mais pessoas utilizando-se da *internet*, como expressam os dados de 2017 colhidos pelo Instituto Brasileiro de Geografia e Estatística (IBGE) (2018), de que o Brasil possuía nesse ano aproximadamente 69,9% de sua população com acesso à *internet*, as informações pessoais dos usuários realmente passaram a ser de extrema impotência, entretanto, o motivo para tal valia, até então não era tão questionado.

2.3 GRANDES CASOS DE VAZAMENTO DE DADOS PESSOAIS

Devido à crescente, e até mesmo desgovernada, coleta de dados de usuários por diversos websites, os quais deveriam ser tratados de maneira sigilosa e segura no banco de dados, há poucos anos se tornou recorrente os escândalos de vazamento

de dados de usuários, e dentre esses imensos vazamentos, destaca-se o do Facebook e sua grande polêmica, manchete de vários portais de comunicação no ano de 2018.

De acordo com a Revista Forbes (DADOS..., 2018), e diversos outros portais de comunicação mundiais, a empresa Facebook, teve as informações pessoais de aproximadamente oitenta e sete milhões de seus usuários comprometidas. Dentre esses dados, o de quatrocentos e quarenta e três mil brasileiros foram expostos, o que por si só já seria algo extremamente negligente. Contudo, a situação se intensificou ainda mais quando foi descoberto que os dados vazados dos usuários foram cedidos à Cambridge Analytica, empresa britânica responsável pelo tratamento e coleta de dados dos usuários do *site* e que teria utilizado os dados pessoais aos quais teve acesso para influenciar diretamente nas eleições presidenciais de Donald Trump, no ano de 2016.

Sobre o vazamento de dados ocorrido, e a maneira pela qual foram captados pela empresa, é disposto:

> O vazamento de dados teria ocorrido no ano de 2013, momento em que a empresa britânica disponibilizou um aplicativo vinculado com a plataforma do Facebook, que tinha como finalidade traçar um perfil do usuário da rede, através de um quiz de perguntas. Uma vez coletadas estas informações, era possível traçar um perfil de pensamento de determinado usuário, pois na época as políticas da plataforma eram permissíveis a tal ponto.”. (Wendt Júnior; Ehrhardt e da Silva, 2019, p. 3)

Como elucidado, por meio do simples *quiz* de perguntas e respostas elaborado pela empresa Cambridge Analytica e vinculado ao usuário do Facebook, foi possível a captação de interesses dos usuários, por meio de seus dados, os quais foram utilizados no ano de 2016 pela empresa. Após a captação e um minucioso estudo para compreender as opiniões e tendências políticas de cada usuário da rede social, a corporação passou a enviar e direcionar todo o tipo de propaganda eleitoral e mensagens políticas favoráveis à Donald Trump, com a intenção de captar mais eleitores para o candidato à presidência.

Tais ocorridos são verdadeiros escândalos para os consumidores pois, ao compartilharem suas informações pessoais, tanto em ambiente físico quanto on-line,

possuem a certeza de que seus dados serão bem armazenados, tendo em vista que, no caso em questão, trata-se de uma enorme corporação, o Facebook, que possibilitou que outra empresa lesasse milhões de usuários da plataforma ao redor do mundo.

Tal polêmica culminou em olhares e questionamentos do mundo inteiro sobre a privacidade de dados, e principalmente sobre as políticas realizadas em cada país para impedir com que outros vazamentos aconteçam.

3 CAPÍTULO II- A CONSCIENTIZAÇÃO MUNDIAL SOBRE A NECESSIDADE DA TUTELA DA COLETA DE DADOS AO REDOR DO MUNDO

3.1 DA AMEAÇA DE GRANDES CORPORAÇÕES À DEMOCRACIA

A democracia passou por diversas evoluções históricas até alcançar sua consolidação, nos países que a possuem como regime político. No Brasil, a democracia foi interrompida por diversos momentos da história, devido à ditadura militar, vigente entre o período de 1964 a 1985. Somente após esse período, foi reestabelecida a democracia, em conjunto com a elaboração e promulgação da Constituição Federal da República do Brasil, de 1988, instaurando-se, assim, o Estado Democrático de Direito, vigente até a atualidade e que preza integralmente pela soberania do povo, e o respeito aos direitos humanos e às garantias constitucionais.

De acordo com Alexandre de Moraes (2005, p. 18), sobre o Estado Democrático de Direito e sua atuação, é elucidado:

> O Estado Democrático de Direito, que significa a exigência de reger-se por normas democráticas, com eleições, periódicas e pelo povo, bem como o respeito das autoridades públicas aos direitos e garantias fundamentais, proclamado no caput do artigo, adotou, igualmente o parágrafo único, o denominado princípio democrático, ao afirmar que “todo poder emana do povo, que o exerce por meio de seus representantes eleitos ou diretamente, nos termos desta Constituição.

Para Adriano Sant’Ana Pedra (2010), acerca da instauração do Estado Democrático de Direito, após longos anos de instabilidade política,

> O sentimento constitucional presente em cada momento vivido passa a permear a realização da Constituição, e a natureza dinâmica da Constituição, como organismo vivo que é, permite que ela possa acompanhar a evolução das circunstâncias sociais, políticas e econômicas.

Assim, a partir dos conceitos apresentados referentes à evolução da Constituição e o Estado Democrático de Direito vigente no país, é fundamental dizer que tal Estado foi estruturado a partir de determinados pilares, os quais se mantém até a atualidade, para manter a organização do Estado Democrático e compromissos firmados com o povo.

Dentre esses pilares, tem-se o direito à privacidade, que de acordo com Bruno Ricardo Bioni (2021, p. 138) “[...] o direito à privacidade é basilar à própria democracia, e, ao

mesmo tempo, condição essencial ao livre desenvolvimento da personalidade dos cidadãos". Assim, é evidente que o direito à privacidade, enquanto aparato fundamental para a estrutura do Estado Democrático deve ser estritamente respeitado.

Ainda nesse sentido, acerca da sociedade em que se vive e à tutela dos direitos fundamentais, Leandro Rodrigues e Pastora Leal discorrem que

> Nessa sociedade complexa, os direitos fundamentais do cidadão demandam proteção e vigilância, não apenas por violações praticadas pelo Estado, mas por abusos cometidos por entes sociais e econômicos que gozam de muita força nas relações mais cotidianas. (2018, p. 15)

Direcionando a discussão à tutela da proteção de dados, a partir do entendimento dos autores, entende-se a privacidade como peça fundamental na questão, pois, com a falha proteção de dados dos consumidores por parte das empresas que as coletavam e armazenavam de maneira indevida, transtornos de enorme proporção passaram a ocorrer, não prejudicando "exclusivamente" os milhões de consumidores que sofreram o vazamento de seus dados, mas sim a democracia por inteiro, visto que se iniciou um poderio desmedido de grandes corporações, as quais detinham inúmeros dados pessoais de consumidores e que podiam se utilizar das informações coletadas da maneira que julgassem benéficas para si.

A empresa britânica Cambridge Analytica é um grande exemplo de corporação que se envolveu em uma polêmica de repercussão mundial no ano de 2016, relacionada à utilização indevida dos dados de milhões de usuários da rede social Facebook. A empresa, atuante na área de análise de dados e consultoria política, foi contratada para atuar no planejamento da campanha presidencial de Donald Trump, em 2016, no entanto, a maneira pela qual recorreram para cativar eleitores foi ilícita e implicou em diversos transtornos.

A coleta indevida de dados de usuários se iniciou no ano de 2013. De acordo com a BBC Brasil (ENTENDA...2018), a empresa Cambridge Analytica lançou na rede social Facebook um aplicativo com diversas e simples perguntas para que os usuários da plataforma respondessem, o que, inicialmente, parecia apenas uma pesquisa despretensiosa, pois o aplicativo alegava que as informações colhidas seriam

utilizadas apenas para fins acadêmicos. No entanto, ao final do teste, o usuário deveria concordar com os termos de uso do aplicativo e os fins que os dados colhidos seriam utilizados, os quais não se limitavam às respostas do teste realizado.

Por não se atentarem às entrelinhas, diversos usuários do Facebook que responderam o teste não perceberam que o aceite ao aplicativo implicaria no compartilhamento de seu perfil com a Cambridge Analytica, bem como o compartilhamento de informações de todos os amigos desse usuário na rede social, ou seja, em apenas um teste respondido, a Cambridge Analytica possuiria informações de dezenas de pessoas.

Ao final do teste realizado pela Cambridge, eles armazenaram, de acordo com a revista eletrônica Exame (AGRELA, 2018), aproximadamente oitenta e sete milhões de informações pessoais de usuários da plataforma Facebook, os quais foram utilizados posteriormente para influenciar no voto dos americanos a favor de Donald Trump.

Por já possuir, desde o ano de 2013, as informações pessoais de milhões de usuários de redes sociais, e potenciais eleitores americanos, a Cambridge Analytica atuou de maneira ilegal quando contratada para atuar na campanha e aumentar a popularidade do candidato à presidência dos Estados Unidos Donald Trump pois, de acordo com Beck e Fornasier (2019, p. 184):

> [...] A CA agia fora da lei, pois esta: (i) mantinha uma política contínua de coleta ilícita de dados pessoais; (ii) parte dos funcionários categorizam indivíduos, eleitores, usando seu próprio software O.C.E.A.N.; (iii) outros funcionários de grau sênior destinavam a maior parte dos recursos da CA para eleitores indecisos que poderiam, por exemplo, mudar de opinião entre votar a favor do Partido Republicano ou do Partido Democrata. A CA rotulou esses perfis de usuários como the persuadables (os persuadíveis). A empresa também fazia uso da rede social Facebook com a prática de ataques-focais (microtargeting,3 em inglês) de seus usuários, muitas vezes utilizando-se – de forma intencional – de notícias falsas (Fake News) para manipular tendências políticas de eleitores, resultando em uma ruptura da democracia e gerando, de forma deliberada, uma sociedade polarizada.

A partir do exposto e da maneira pela qual a corporação Cambridge Analytica se utilizava para cativar eleitores, é evidente que tal manobra ilegal foi uma enorme ameaça para a instituição democrática, visto que o poder que apenas uma corporação detinha em suas mãos, a partir de dados pessoais de milhões de pessoas, era tão

grande, que resultou na vitória da disputa presidencial de Donald Trump. Assim, a partir do resultado da eleição e, posteriormente, com a descoberta desse escândalo contra a democracia e à privacidade de dados pessoais, grande parte dos países iniciou uma mobilização em prol da elaboração de leis referentes ao correto tratamento de dados da população.

3.2 O SURGIMENTO DA TUTELA DE DADOS PESSOAIS NA UNIÃO EUROPEIA.

A União Europeia, composta por seus Estados-Membros, é uma grande referência de sistema de proteção de dados e privacidade do consumidor no mundo. Possuindo uma política de proteção de dados já antiga, estima-se que a tutela de dados pessoais e privacidade passou a ser debatida na Europa em meados de 1950, por meio de diretivas europeias, da Declaração Universal dos Direitos Humanos (UNITED NATIONS, [1948]) e da Declaração Europeia dos Direitos do Homem (EUROPEAN COURT OF HUMAN RIGHTS, [2012]).

Acerca da política de proteção de dados ser matéria amplamente discutidas há anos pela União Europeia, bem como o cerne de sua tutela, Renato Opice Blum (2020, p. 107) elucida:

> A proteção de dados pessoais já não era matéria nova nos Estados- Membros da União Europeia quando da aprovação da primeira diretiva sobre o assunto. A privacidade, como conceito geral, é de fato, instituto muito mais antigo, encontrando referências diretas na Declaração Universal de Direitos Humanos, por exemplo. É importante notar, nesse passo, que a União Europeia desenvolveu seu conceito de proteção de dados pessoais com base em normas de Direitos Humanos, o que explica a estreita relação entre proteção de dados, privacidade e da dignidade humana.

Sobre a tutela da privacidade do sistema europeu, o artigo 8º da Declaração Europeia de Direitos do Homem, adotado pelo Conselho da Europa no ano de 1950, disciplina *in verbis* “Art. 8. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência” (EUROPEAN COURT OF HUMAN RIGHTS, [2013], p. 11). Deste modo, é possível perceber a importância desse pilar na União Europeia muitos anos antes de outros países iniciarem discussões acerca da privacidade dos cidadãos.

Além do artigo citado, ainda nessa época, a União Europeia, por meio da Declaração Universal de Direitos Humanos, já previa uma norma referente à atuação do Estado frente à intromissões de terceiros na vida privada de cada indivíduo. Sobre os artigos da década de cinquenta indicarem limites a interferências externas sobre a vida de particulares, o artigo 12 da Declaração Universal de Direitos Humanos expressa, *in verbis*

> Art. 12. Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei (UNITED NATIONS, 1948, p. 3).

Assim, é evidente que a tutela da proteção de vida privada e informações pessoais já eram debatidas e indicavam que o tema seria cada vez mais explorado e consolidado com o passar do tempo.

Atualmente, na União Europeia, a matéria da proteção de dados e privacidade é regulamentada pela lei *General Data Protection Regulation* (GDPR), entrada em vigor no ano de 2018, e por outras diretivas, as quais tornam a tutela da privacidade de informações pessoais bem completa e abrangente, uma vez que os diversos regulamentos sobre o tema amparam um consumidor sempre que algum direito seu for violado. Sobre as regulamentações sobre o tema, é disposto:

> O sistema, atualmente vigente de proteção de dados pessoais é regulamentado não apenas pelo GDPR, mas também por diretivas, regulamentos, decisões vinculantes e orientações de diferentes níveis hierárquicos, criando um quadro legal em diversas camadas que partem sempre de orientações gerais e estabelecem normas cada vez mais especificas sobre os direitos e obrigações relativos aos dados pessoais. (BLUM, 2020, p. 107)

“Qando o RGPD entrou em vigência, criou-se uma influência internacional para que outros países também passassem a normatizar o tema de proteção de dados”. (PANEK, 2019, p. 20). Deste modo, é evidente que a União Europeia, enquanto pioneira na matéria de proteção de dados pessoais, e se atualizando cada vez mais especialmente devido à promulgação da RGPD, influenciou diretamente diversos outros regulamentos que seriam implementados por outros países posteriormente, como por exemplo a lei de proteção de dados pessoais do Brasil, intitulada Lei Geral de Proteção de Dados.

3.3 DA CRIAÇÃO E IMPLEMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS NO BRASIL

A lei nº 13.709/2018, intitulada Lei Geral de Proteção de Dados, foi sancionada em 14 de agosto de 2018 pelo então presidente da república Michel Temer, porém, apenas entrou em vigor, parcialmente, no ano de 2020, e sua implementação total, ou seja, com as referidas sanções atribuídas pela lei, apenas entraram em vigência no mês de agosto de 2021.

A LGPD foi criada em um cenário de necessidade de proteção de dados pessoais efetivo, frente as diversas inovações tecnológicas na era digital. As informações dos cidadãos se tornaram cada vez mais cobiçadas por empresas e corporações que consideravam a captação de dados pessoais interessantes para sua atuação, e as colhiam de maneira exorbitante devido à inexistência de lei que regulasse especificamente a proteção de dados de consumidores.

O artigo 1º da Lei Geral de Proteção de Dados (BRASIL, 2018), aborda o cerne e objetivo da lei, destacando que seu objeto é o tratamento de dados pessoais, em ambientes físicos ou digitais, por pessoa natural ou jurídica, de direito público ou privado, almejando assim a defesa de direitos fundamentais do cidadão, bem como os pilares de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Embasada em diretrizes europeias e na GDPR, a Lei Geral de Proteção de Dados preza diretamente pela privacidade do cidadão, privacidade esta regulada no Brasil inicialmente pela Constituição da República Federativa do Brasil, mas que atualmente, com a vigência da LGPD, passou a atuar de maneira específica e de acordo com as necessidades atuais. Além da privacidade, o art. 2º da LGPD destaca os princípios norteadores que efetivam o exercício de direitos e garantias fundamentais dos cidadãos brasileiros, como exposto:

> Art. 2º- 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, art. 2º).

Deste modo, é possível perceber que a LGPD preza integralmente pelos direitos e garantias fundamentais, bem como pelo correto e consentido tratamento de dados pessoais dos cidadãos brasileiros, desde que a tutela desses direitos ocorra em território nacional, ou por empresa que atue simultaneamente em âmbito internacional e, também, no Brasil, como é disposto:

> Está presente a extraterritorialidade da LGPD na medida em prevê que, para sua aplicação, o tratamento ou apenas a coleta de dados ocorra em território nacional, ou a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços localizados em território nacional. Portando uma empresa que coleta os dados de pessoas que estejam no território brasileiro, mesmo que haja internacionalmente, se sujeitará aos termos da LGPD (PANEK, 2019, p. 20).

Ainda no certame do tratamento de dados de usuários coletados por empresas, é disciplinado no art. 6º da LGPD, os princípios reguladores dessa matéria, o qual informa em seu *caput*, que, para o correto tratamento, além de se observar a boa- fé, deve-se respeitar os seguintes princípios da Lei Geral de Proteção de Dados: I - finalidade; II - adequação; III - necessidade; IV - livre acesso; V - qualidade dos dados; VI - transparência; VII - segurança; VIII - prevenção; IX - não discriminação; X - responsabilização e prestação de contas (BRASIL, 2018).

Apesar de todos os artigos da Lei Geral de Proteção de Dados serem cruciais para a correta estruturação da tutela da privacidade de dados, alguns artigos se destacam para a efetivação e cumprimento da lei, sendo um deles o art. 7º. O sétimo artigo da LGPD apresenta os requisitos para o tratamento de dados pessoais, os quais, em suma, destacam a figura do consentimento do titular, bem como elucidam a importância dessa figura, sendo vedado qualquer tipo de coleta, tratamento e compartilhamento de dados, sem os devidos requisitos legais, exceto em casos excepcionais, elencados no mesmo artigo.

Sobre a necessidade do consentimento do titular de dados, a partir da aplicação da nova lei, Fernanda Maia (2020, p. 6), explica

> A LGPD elevou o nível de exigências do consentimento e, em sua redação, a lei define que o consentimento deverá necessariamente representar uma manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. Neste sentido, vale frisar que um consentimento genérico, sem uma finalidade específica, não seria considerado válido para a LGPD.

Dito isso, é possível perceber que a Lei Geral de Proteção de Dados possui critérios para a efetivação da figura do consentimento. Contudo, a legislação brasileira não especificou o conceito dos critérios, quais sejam, o consentimento “livre, informado e inequívoco”. Deste modo, a doutrina brasileira, tendo como base e inspiração no Regulamento Geral sobre a Proteção de Dados Europeu (GDPR), extraiu os conceitos dos critérios do art. 5º, XII, da lei brasileira, a partir de fonte internacional.

No entendimento de Opice Blum (2020) acerca do primeiro critério, o consentimento livre deve ocorrer, como o próprio nome diz, sem nenhum tipo de pressão ao consumidor e titular dos dados em questão. Devendo assim, ser facultado a este a opção de selecionar quais dados pessoais são de seu interesse compartilhar, a empresa com que deseja compartilhar, e de que maneira, sendo vedado os tipos de consentimento chamados “tudo ou nada”, tendo em vista que o consumidor não é obrigado a concordar com todas as cláusulas de determinado contrato, quando houver finalidades diferentes para o uso de seus dados. Assim, o autor entende que é facultado ao consumidor escolher sua destinação.

Ainda assegura o autor que, de acordo com a lei, não serão considerados lícitas as informações ou cláusulas de empresas que indiquem que o acesso do consumidor à determinado produto ou site está condicionado ao compartilhamento de seus dados pessoais, tendo em vista que, o consumidor pode simplesmente se opor em informar seus dados e ainda assim querer acessar tal produto ou *site*. Entretanto, é sabido que diversas plataformas ou serviços ainda vedam o acesso do consumidor ao que ele deseja, caso não “cooperem”, informando todos os dados solicitados. Em suma, o consentimento livre visa que o consumidor não precise aceitar termos que não deseja, atribui mais autonomia e poder de escolha a ele.

Como bem assegura Opice Blum (2020) acerca do segundo critério, o consentimento informado, este apenas é alcançado quando é informado ao titular dos dados que se almeja captar, em uma coleta de dados segura e de acordo com a lei, informações claras e precisas acerca dos dados pessoais, o que remete diretamente ao art. 9º da Lei Geral de Proteção de Dados (BRASIL, 2018).

Ainda de acordo com Opice Blum (2020, p. 24), acerca do consentimento informado, deve-se observar algumas premissas para a efetivação da informação, por parte do consumidor, sendo elas expressas a seguir

> a) finalidades específicas do tratamento;
> b) forma e duração do tratamento, guardados os segredos comercial e industrial;
> c) identificação e informações de contato do controlador;
> d) informações acerca do uso compartilhado de dados pelo controlador e a finalidade; e) responsabilidades dos agentes que realizarão o tratamento; e
> f) direitos do titular, aí se incluindo menção à possibilidade de confirmação de tratamento de dados, acesso, atualização, retificação, anonimização, eliminação, além de outros dispostos nos arts. 17 a 22 da Lei.

Ademais, a pesquisa de Opice Blum (2020) destaca que, acerca do terceiro critério, o consentimento inequívoco, este deve ocorrer quando o controlador ou empresa, os quais desejam realizar o tratamento de dados de usuários, informarem da maneira mais clara e evidente possível que o consumidor autorizou que seus dados fossem tratados pelo operador em questão. Tal autorização pode ocorrer por diversos meios, com a autorização escrita ou um *click* no *site* em questão. O crucial nesse critério é que seja possível confirmar que o consumidor realmente consentiu com a utilização de seus dados pessoais.

A partir dos critérios reguladores do consentimento, Caitlin Mulholland, a respeito da importância dos dados pessoais, entende

> Parte-se da ideia de que os dados são elemento constituinte da identidade da pessoa e que devem ser protegidos na medida em que compõem parte fundamental de sua personalidade, que deve ter seu desenvolvimento privilegiado, por meio do reconhecimento de sua dignidade (2018, p. 171).

A partir do exposto, compreende-se que devido à importância dos dados pessoais, enquanto componentes da personalidade do indivíduo, há restrições quanto à sua aplicação. Deste modo, acerca das impossibilidades de “consentimento” e configuração de consentimento equivocado do consumidor, Blum (2020, p. 25) comenta

> Opções pré-selecionadas ou o mero silêncio passivo não serão considerados manifestação do consentimento inequívoco, não havendo espaço para dúvida acerca da efetiva intenção do titular. Na ausência de certeza, certamente se estará em momento de insegurança para o controlador, o que pode ensejar o entendimento de ilicitude do tratamento dos dados pessoais, com as consequências negativas daí decorrentes.

3.4 DOS MECANISMOS DA LGPD NO CONTROLE DE ABUSOS NO TRATAMENTO DE DADOS DE CONSUMIDORES

Com a introdução da Lei Geral de Dados no ordenamento jurídico brasileiro, surge a figura da Autoridade Nacional de Proteção de Dados (ANPD). Esse mecanismo, tem sua função estabelecida pelo art. 55- J, da própria LGPD e suas atribuições principais, de acordo com os incisos I e IV, possuem enfoque no zelo da proteção de dados pessoais, bem como a fiscalização e aplicação de sanções, quando não respeitadas as imposições da lei.

A ANPD foi regulamentada tardiamente e passou por diversas intempéries. Apesar da vigência da LGPD não ter sido prorrogada como um todo, as sanções nela previstas serão adicionáveis pela Autoridade Nacional de Proteção de Dados (ANPD) apenas em 1º de agosto de 2021 (Lei nº 14. 010/ 2020) (BIONI, 2021, p. 13).

A partir disso, é possível perceber a morosidade do processo de aprovação da regulamentação da Agência, prejudicando diretamente a Lei Geral da Proteção de Dados, uma vez que estaria atuando de forma incompleta.

Quanto à sua composição, ela é composta pelo conselho diretor, ouvidoria, corregedoria, conselho nacional de proteção de dados pessoais e privacidade, órgão de assessoramento técnico e administração especializada (MONTEIRO, 2019). Além de suas atribuições estarem elencadas no art. 55-J, o artigo 5º, inciso XIX, referente à autoridade nacional, reafirma a importância dessa Agência, quanto à promoção de segurança para os consumidores, em relação a seus dados pessoais, atuando principalmente na aplicação de sanções à empresas que se considerem imunes a um tratamento de dados consonância com a lei.

Atualmente, com a vigência e aplicabilidade da lei, caso ocorram casos de vazamento de dados, devido à um tratamento inadequado, as empresas não sairão ilesas e deverão arcar financeiramente com as sanções previstas na lei. O art. 52 da LGPD elenca um rol de sanções administrativas a serem aplicadas pela ANPD, em caso de descumprimento com a lei. Dentre os incisos, vale ressaltar o II, pois indica que em casos de infração pessoas jurídicas de grupo privado ou corporações, podem pagar

multa de até 2% de seu faturamento anual, podendo chegar a até R$ 50.000.000,00 (cinquenta milhões de reais) por infração (BRASIL, 2018).

Para além disso, os incisos X e XII são igualmente necessários para o rol de sanções previstas, ainda no art. 52. O primeiro indica que em caso de configuração de tratamento de dados inadequado, o banco de dados da determinada empresa ficará suspenso por 6 meses ou mais, a depender da regularização do tratamento por parte da empresa infringente. Quanto ao segundo, é uma consequência ainda mais drástica e prevê a proibição do exercício de tratamento de dados, devido às punições atribuídas não terem sido retificadas. O que demonstra, assim, a seriedade com que as empresas devem tratar a legislação acerca do tratamento de dados dos consumidores.

Outro mecanismo atribuído pela Lei Geral de Proteção de Dados são os agentes de tratamento de dados, representados pela figura do controlador e operador, como elencado no 5º, IX da lei. Acerca dos agentes de tratamento e suas atribuições, é destacado:

> Art. 5º Para os fins desta Lei, considera-se:
> 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 [...] (BRASIL, 2019, art. 5º).

Ainda nesse sentido, no tocante às atribuições do controlador e operador, pode-se afirmar que:

> Ambas as figuras são responsáveis pelo tratamento de dados, mas é caracterizado o controlador aquele que toma as decisões, será o encarregado pela proteção de dados e pela disponibilização de informações seja à Autoridade Nacional quanto ao usuário titular. O controlador também será responsável pela entrega do relatório de impacto à proteção de dados pessoais, prevista pela lei. Ademais, em caso da necessidade de prova sobre a obtenção do consentimento do usuário para tratamento dos dados, o ônus será do controlador (PANEK, 2019, p. 24).

Além dos agentes controlador e operador, já indicados, há uma terceira figura para efetivação e controle do tratamento de dados pessoais, sendo esta intitulada, encarregada e elencada no art. 41 da LGPD. As atribuições do encarregado, o qual será indicado pelo controlador, será a de manter comunicação com os titulares de dados, aceitar reclamações, prestar esclarecimentos, bem como, adotar providências quando solicitado.

4 CAPÍTULO III- DO CONSENTIMENTO DO CONSUMIDOR

4.1 DOS CONTRATOS DE ADESÃO PÓS- LGPD E AS CLÁUSULAS ABUSIVAS

Como visto no capítulo anterior, a Lei Geral de Proteção de Dados trouxe diversas inovações em seus artigos, os quais almejam a proteção e segurança do consumidor, ao fornecer seus dados pessoais, em ambiente on-line ou físico. Anteriormente à elaboração da referida lei, não havia previsão específica acerca das ilicitudes e abusividades cometidas por empresas com os consumidores, além das disposições do Código de Defesa do Consumidor.

Assim, as cláusulas de contratos eletrônicos, majoritariamente de adesão, uma vez que são os tipos de contrato que não conferem ao consumidor o poder de debater cláusulas, acabavam por forçar os usuários de seus serviços a consentir com termos que eles não concordavam necessariamente, ou sequer liam. Acerca da definição de contrato de adesão, Maria Helena Diniz, elucida

> [...] é aquele em que a manifestação da vontade de uma das partes se reduz a mera anuência a uma proposta da outra, como nos ensina R. Limongi França. Opõe-se a ideia de contrato paritário, por inexistir a liberdade de convenção, visto que exclui qualquer possibilidade de debate e transigência entre as partes, pois um dos contratantes se limita a aceitar as cláusulas e condições previamente redigidas e impressas pelo outro [...], aderindo a uma situação contratual já definida em todos os seus termos (DINIZ, 2009, p. 367).

Todavia, após a vigência da Lei Geral de Proteção de Dados, os contratos de adesão foram “prejudicados”, uma vez que um dos pilares da LGPD é o consentimento do consumidor. Consentimento esse que nos contratos de adesão ocorre de maneira forçada pois, como expresso acima por Maria Helena Diniz (2009, p, 367), “um dos contratantes se limita à aceitar as cláusulas”, ou seja, caso um consumidor que deseja usufruir de um serviço não concorde com os termos do contrato de adesão, quanto ao uso de seus dados, dificilmente poderá usufruir o serviço desejado.

Ainda nesse sentido, mesmo após o início de vigência da Lei Geral de Proteção de Dados, bem como da aplicação de sanções e fiscalização realizada pela Agência Nacional de Proteção de Dados, algumas empresas continuam a desrespeitar a letra da lei e buscam forçam o consumidor a aceitar suas cláusulas propostas.

O Mercado Livre é uma das empresas que mesmo após a vigência da lei, insiste em descumpri-la, ao informar, na Declaração de Finalidade e Confidencialidade do *site*, o seguinte

> O Mercado Livre coleta suas informações pessoais para que você possa desfrutar de nossos serviços e para poder aprimorá-los continuamente.
> Em alguns casos, as informações serão fornecidas por você mesmo, ao registrar-se ou ao fornecer informações ao utilizar algum de nossos serviços. Em outros, nós as coletamos automaticamente, como quando navega em nossas páginas, utiliza nossos serviços. Também podemos coletar suas informações por meio de outras fontes confiáveis (MERCADO LIVRE, 2021, p. 1).

Após a leitura da cláusula 3 da Declaração de Finalidade e Confidencialidade intitulada “Quais informações coletamos e processamos”, é possível perceber que o *site* destaca inicialmente que a coleta de dados poderá ocorrer quando o próprio usuário compartilhar suas informações com *site*, ou poderão ser coletadas de maneira automática. Contudo, esse tipo de coleta automática é expressamente vedado pela LGPD, devido à figura do consentimento, elencada no art. 7º, I da lei, a qual declara que o tratamento de dados só poderá ocorrer com o expresso consentimento do titular dos dados, consentimento esse, também complementado pelo art. 5º, XII, que informa que o consentimento deverá ser manifestado livremente, informado e inequívoco.

Além da cláusula abusiva disposta acima, o *site* do Mercado Livre, ainda na cláusula 3, traz mais informações que vão de encontro à Lei de Proteção de Dados e suas disposições, tendo em vista que, acerca da obrigação de compartilhamento de informações pessoais com a plataforma, é estabelecido

> Queremos que saiba que não é obrigado a nos fornecer as informações pessoais indicadas abaixo; no entanto, trata-se de um requisito essencial para que possa contratar e/ou ter qualquer tipo de relacionamento com o Mercado Livre e, caso não forneça essas informações, não seremos capazes de lhe fornecer nossos serviços ou nossa capacidade de fazê-lo poderá ser significativamente prejudicada. A imprecisão ou inexatidão dos dados pessoais que você fornecer poderá ocasionar a suspensão dos Serviços. Da mesma forma, o Mercado Livre poderá suspender ou desabilitar permanentemente os usuários que violarem esta Declaração de Privacidade (MERCADO LIVRE, 2021, p. 1).

Diante do exposto, é possível perceber que o Mercado Livre informa a seus clientes em potencial que caso não concordem em informar os dados solicitados pela plataforma, não poderão usufruir de seus serviços, o que configura uma calamitosa ilicitude, pois certamente deixará muitos consumidores “sem saída”, tendo em vista que vários deles podem precisar se utilizar unicamente dos serviços do Mercado Livre, não podendo recorrer à outro *site*, e assim acabam compartilhando forçadamente

seus dados, recaindo no ideal da manifestação do consentimento do consumidor, que nesse caso, será forçada e em descumprimento com o estipulado pelo art. 5º, I da Lei nº 13.709/18.

O uso e tratamento inadequado dos dados pessoais, não se limita ao Mercado Livre. Atualmente, ainda encontra-se diversas outras plataformas de serviços on-line que não se aperfeiçoaram e regulamentaram a coleta de dados da empresa, recaindo assim em atividade ilícita e passível de sanções. O site OLX é outro exemplo de plataforma que coleta automaticamente informações do usuário ao baixar o aplicativo da empresa, como disposto a seguir

> [...]
> g) Informações coletadas automaticamente. Quando você acessa os Sites ou serviços de terceiros, a OLX pode receber e registrar informações de seu navegador ou dispositivo em nossos servidores, como por exemplo Identificador de Publicidade do Android, do iOS ou de outros sistemas operacionais análogos, bem como dados de localização recebidos a partir dos sensores do dispositivo. Além desses dados, também podemos coletar de dados sobre publicidade no dispositivo, incluindo cliques efetuados a partir dele, impressões e tempo de permanência em publicidade (OLX, 2020, p. 1).

A partir da cláusula de Política de Privacidade do site da OLX, é possível perceber que a plataforma atua em desconformidade com a lei, praticando abuso com o consumidor, uma vez que, a partir do momento em que se baixa o aplicativo em celular, ou qualquer aparelho móvel, o *site* já faz a captura automática dos dados, indicando as informações que serão recolhidas, a seguir:

> Cumprindo os requisitos de transparência, detalhamos abaixo os dados do seu dispositivo que podem ser coletados se você se utiliza de um dos nossos apps:
> (i) Identificadores anônimos de publicidade do dispositivo, atributos do dispositivo móvel e aplicativos instalados no respectivo aparelho;
> (ii) Dados dos sensores do aparelho;
> (iii) Dados anonimizados de localização do aparelho por meio de GPS ou rede celular (OLX, 2020, p. 1).

Contudo, a partir do entendimento do que são considerados dados pessoais, para a Lei Geral de Proteção de Dados, não seria possível esse tipo de rastreio do aparelho, por meio de GPD ou rede celular. Acerca do conceito de dados pessoais (WARCKS, P. 26, 1989 *apud* OLIVEIRA 2017, on-line) evidencia

> Dados pessoais consistem nos fatos, informações, ou opiniões que dizem respeito a um indivíduo e que seria razoável esperar que ele considerar como íntimo ou compassivo, e portanto querer reter, ou pelo menos restringir a sua coleta, utilização ou circulação.

A partir do conceito apresentado, referente ao conceito e quais informações podem ser consideradas como dados pessoais, pode-se afirmar que a localização e endereço são informações consideradas particulares de cada indivíduo, pois são informações que remetem à identificação de um indivíduo. Assim, interpreta-se que para serem recolhidas por empresas, necessitam do consentimento do titular dos dados. Os art. 5º, XII; 7º § 5º da Lei Geral de Proteção de Dados expressam que o consumidor deverá concordar com o uso de suas informações para tal finalidade, qual seja, permissão para ser localizado.

Além disso, o art. 6º, I, II, III e VI são essenciais para o entendimento de que tais captações não podem ocorrer de maneira automática. O artigo e seus incisos citados referem-se aos princípios importantes para a LGPD, quais sejam a finalidade, adequação, necessidade e transparência da atividade de tratamento de dados, o que, no caso em questão, não ocorreu.

4.2 O CONSENTIMENTO COMO CONDIÇÃO DE VALIDADE DOS CONTRATOS DE ADESÃO

O contrato é, possivelmente, o negócio jurídico mais utilizado e importante no ordenamento jurídico, quando se almeja conciliar desejos da coletividade e alcançar determinada finalidade. De acordo com Tartuce (2017, p.612), “em uma visão clássica e moderna, o contrato pode ser conceituado como sendo um negócio jurídico bilateral ou plurilateral que visa à criação, modificação ou extinção de direitos e deveres com conteúdo patrimonial”.

De maneira similar ao conceito apresentado, Gagliano e Pamplona Filho (2017, p. 63) compreendem

> Entendemos que o contrato é um negócio jurídico por meio do qual as partes declarantes, limitadas pelos princípios da função social e da boa-fé objetiva, autodisciplinam os efeitos patrimoniais que pretendem atingir, segundo a autonomia das suas próprias vontades.

Contudo, devido às transformações da sociedade e, consequentemente, do negócio jurídico, o contrato não é visto mais apenas como um instrumento para que partes envolvidas entrem em um consenso, a partir de seus interesses contrapostos.

Atualmente, é necessário se atentar à função social do contrato, prevista no art. 421 do Código Civil.

Além de se observar esse artigo legal para a concretização de um contrato, é de extrema importância se atentar para a manifestação da vontade, haja vista que a proposta e a aceitação das partes são essenciais para a celebração do negócio jurídico.

“A aceitação é a aquiescência a uma proposta formulada. Trata-se da manifestação de vontade concordante do aceitante ou oblato que adere à proposta que lhe fora apresentada [...]” (GAGLIANO; PAMPLONA FILHO, 2017, p.169). O conceito de aceitação, como elucidado, retrata a manifestação das partes de maneira a consentir com as cláusulas de um contrato. De acordo com o Código Civil, elencado em art. 432, o legislador compreende que, em caso de negócio jurídico, caso o proponente dispense aceitação expressa, ou que não seja habitual esse tipo de manifestação, reputar-se-á concluído o contrato, caso a recusa não seja informada em tempo hábil.

A partir do entendimento Legal, é possível extrair que o ordenamento jurídico civil permite que, em relações civis, a manifestação de vontade dos indivíduos possa se dar de maneira expressa ou tácita. Contudo, deve-se observar que a possibilidade de manifestação tácita da vontade só deve ocorrer em situações previstas pela lei. Acerca da possibilidade de manifestação tácita, Maria Helena Diniz destaca

> Ter-se-á aceitação tácita quando: a) não for usual aceitação expressa. Por exemplo, quando um industrial costuma todos os anos enviar seus produtos a certa pessoa que os recebe e na época oportuna os paga, e, se num dado momento não convier a esta pessoa o recebimento da mercadoria, deverá avisar o industrial, sob pena de continuar vinculada ao negócio (RT, 232:227 e 231: 304; RF, 161:278); b) o ofertante dispensar a aceitação. Por exemplo, se alguém reserva acomodação num hotel, dizendo que chegará tal dia, se o hoteleiro não expedir a tempo a negativa, o contrato estará firmado (DINIZ, 1999, p. 774).

Todavia, há autores civilistas que criticam veementemente o art. 432 do Código Civil, por entenderem que quem se cala, não necessariamente consente. Segundo Flavio Tartuce

> O dispositivo é criticado por parte da doutrina, pelo fato de contrariar a regra contida no art. 111 do Código Civil, pela qual, quem cala não consente: “O silêncio importa anuência, quando as circunstâncias ou os usos o autorizarem, e não for necessária a declaração de vontade expressa”. (TARTUCE, 2017, p.194).

Desse modo, pode-se perceber que a manifestação de vontade tácita em contratos civilistas é permitida apenas quando a lei se manifestar com a devida anuência. Para além disso, ao abordar as relações consumeristas, especialmente a manifestação de vontade, anuência dos indivíduos e o silêncio destes, o ordenamento jurídico consumerista possui entendimento diverso. Cristiano Chaves e Nelson Rosenvald, acerca do silêncio contratual, entendem que

> Para além do Código Civil, nas relações consumeristas, entendeu o legislador que é inaplicável a regra do artigo 111 do Código Civil. O silêncio do consumidor remete frequentemente a condutas abusivas do fornecedor de produtos e serviços. O artigo 39, III, do CDC, taxa como abusiva a prática da remessa de produtos e serviços sem a prévia solicitação do consumidor, como o envio de cartões de crédito. A inércia do consumidor não importará em aceitação, pois o produto enviado será considerado "amostra grátis" (parágrafo único, art. 39, Lei n. 8.078/90) (FARIAS; ROSENVALD, 2012, p. 94).

A partir do exemplo, é evidente que o Código Consumerista veda a aplicação da manifestação tácita da vontade, uma vez que o CDC pressupõe a figura do consumidor como parte vulnerável de uma relação contratual. Deste modo, caso ele se silencie acerca do aceite de termos de uso de determinado *site* ou produto, não presume-se seu consentimento, devendo haver assim a manifestação expressa de sua vontade.

O Mercado Livre e a OLX, exemplos de plataformas que atuam em desacordo com a Lei Geral de Proteção de Dados, ferem diretamente a manifestação do consentimento do consumidor, por se utilizarem de mecanismos que, sem o aceite do consumidor, começam a rastreá-lo, ou silenciam os consumidores no sentido de não poderem debater cláusulas do contrato de adesão, e os obriga a concordar com os termos, sob risco de não conseguirem acessar o produto que deseja, manifestando assim desacordo com a lei e consumidor.

A partir dessa ótica, Bruna Lyra Duque e Adriano Pedra (2013, p. 7) entendem que

> O direito não tem o condão de impor condutas ao psiquismo humano e não pode obrigar o indivíduo a pensar, agir ou nutrir sentimentos dessa ou daquela maneira; mas pode corrigir distorções nas relações jurídicas e vincular os atores sociais ao respeito à norma jurídica.

Deste modo, cabe à legislação regulamentadora da proteção de dados aplicar as medidas dispostas na lei, tendo em vista que a lei se encontra em vigência há anos e

atualmente ainda é desrespeitada por diversas empresas e corporações, desregulando a relação jurídica entre os indivíduos.

4.3 AS SANÇÕES APLICÁVEIS À UTILIZAÇÃO DE CLÁUSULAS VIOLADORAS DOS DIREITOS PROTEGIDOS PELA LGPD

A Agência Nacional de Proteção de Dados (ANPD) é um órgão da administração Pública previsto nos artigos da Lei Geral de Proteção de Dados. A criação da ANPD foi sancionada no ano de 2019, pela lei nº 13.853/19, entretanto, uma de suas funções, referente à aplicação de sanções administrativas, apenas entrou em vigor em 1º de agosto de 2021, dois anos após a lei ser sancionada.

Acerca da competência da Agência, de acordo com o art. 55-J, incisos I, III e IV da Lei Geral de Proteção de Dados, serão as atribuições da ANPD

> I - Zelar pela proteção dos dados pessoais, nos termos da legislação; (Incluído pela Lei nº 13.853, de 2019)
> II - Zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei; (Incluído pela Lei nº 13.853, de 2019)
> III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Lei nº 13.853, de 2019)
> IV - Fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso; (Incluído pela Lei nº 13.853, de 2019) (BRASIL, 2018, art. 55-J).

De acordo com os artigos legais supracitados, pode-se interpretar que a Agência Nacional possui como principais atribuições o zelo pela proteção de dados, a elaboração de diretrizes, bem como a fiscalização e aplicação de sanções em caso de tratamento de dados realizado em desconformidade com a lei.

No certame das sanções administrativas atribuídas pela Agência, as quais entraram em vigor e puderam ser aplicadas apenas a partir agosto desse ano, estão distribuídas entre os artigos 52, 53 e 54 da LGPD, os quais elencam variados tipos de sanções, desde o pagamento de multas por infrações, até a impossibilidade de se manter um banco de dados, em definitivo (BRASIL, 2018).

O art. 52 e seus incisos elencam um rol de possíveis infrações a serem cometidas por pessoas jurídica de direito privado, grupo ou conglomerado e suas sanções. Dentre as penalidades do artigo, tem-se a aplicação de advertências, até que se regule à infração cometida (inciso I), até sanções financeiramente mais gravosas, como destaca o inciso II

> II- Multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; (BRASIL, 2018, art. 52)

Assim, é possível perceber que as infrações ao tratamento de dados podem resultar em multas extremamente caras para a empresa infratora. Além das infrações citadas, algumas sanções ainda são mais gravosas às empresas, por serem definitivas. Ou seja, não permitem que a corporação pague a multa e voltem a realizar a coleta de dados, como o inciso XII do art. 52 evidencia, ao proferir que dentre as sanções que podem ser atribuídas pela Agência, está a proibição parcial ou total do exercício de atividades relacionas a tratamento de dados.

O art. 53 da lei, por sua vez, informa que é de competência da Agência Nacional estipular o cálculo do valor base, para as sanções administrativas que serão aplicadas à empresas, se configurado exercício de atividade em desconformidade com a lei.

Por fim, o art. 54, último referente às sanções administrativas da ANPD, indica os vetores que deverão ser analisados para se atribuir sanção à determinada empresa, sendo eles a gravidade da falta e a extensão do dano ou prejuízo causado pelo tratamento de dados indevido.

Para além disso, no que se refere ainda aos critérios para aplicação de sanções administrativas:

> Nos termos da Lei, a aplicação de sanções requer, ainda, criteriosa apreciação e ponderação de diversas circunstâncias, dentre as quais a gravidade e a natureza das infrações e dos direitos pessoais afetados, a condição econômica do infrator, o grau do dano, a cooperação do infrator, a adoção de política de boas práticas e governança e a pronta adoção de medidas corretivas (BRASIL, 2021)

Contudo, notadamente, as sanções administrativas não se limitam às empresas e corporações. Assim, as infrações que podem ser cometidas por órgãos públicos, estão

elencadas na letra da lei em conjunto com as sanções aplicáveis à pessoas jurídicas de direito privado e ocorrerão da maneira disposta

> Os órgãos e as entidades públicas poderão ser punidos com todas as sanções administrativas previstas na LGPD, salvo as sanções pecuniárias. Ademais, a LGPD prevê a possibilidade de responsabilização de agentes públicos, nos termos previstos na Lei nº 8.112, de 11 de dezembro de 1990 (Estatuto do Servidor Público), na Lei nº 8.429, de 2 de junho de 1992 (Lei da Improbidade Administrativa) e na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) (BRASIL, 2021)

Em vista disso, pode-se dizer que a ideia da Lei Geral de Proteção de Dados, em conjunto com o mecanismo de aplicação de sanções, contemplado pela ANPD, é a de penalizar não apenas empresas que desacatem a legislação, captando, tratando e compartilhando os dados de maneira ilegal, mas sim os próprios órgãos públicos, estes não sairão ilesos em caso de uso indevido de dados, o que demonstra a ideia de uniformidade da lei, não perdoando nenhum tipo de responsabilização por infração.

4.4 OS MEIOS DE SE COMBATER A UTILIZAÇÃO DE CLÁUSULAS ABUSIVAS E VEDAR O TRATAMENTO INDEVIDO DE DADOS.

O advento da Lei Geral de Proteção de Dados abarcou diversas inovações para a temática da proteção de dados do consumidor. Entretanto, o caminho a se percorrer e mudanças a serem implementadas por empresas que almejam captar dados de seus consumidores são constantes.

A LGPD foi sancionada no ano de 2018, mas entrou em vigência, parcialmente, apenas dois anos depois, em 2020. A Lei Geral de Proteção de Dados não vigorou de maneira completa no ano anterior, pois a Agência Reguladora de Proteção de Dados ainda não poderia exercer seu poder de atribuir sanções administrativas. Esse mecanismo entrou em vigência apenas em agosto de 2021, assim, cumulando-se o tempo entre a lei ser sancionada, entrar em vigor e a possibilidade de aplicação de sanções. Pode-se dizer que as empresas do país teriam tempo suficiente para se adequarem, de acordo com as novas imposições da lei. Entretanto, na realidade, não foi isso o que ocorreu.

De acordo com a Revista Exame (LOPES, 2021), acerca da adequação das empresas à lei, anos após a sua publicação, afirma-se

> Quase 40% das empresas ainda não tem condições de cumprir integralmente o dispositivo. É o que mostra pesquisa da Fundação Dom Cabral (FDC) com 207 companhias, sendo 95% de médio e grande porte, de áreas como finanças, seguros, varejo, agronegócio, saúde, química e construção (LOPES, 2021, p. 1).

A partir dos dados informados pela reportagem, é notório que mesmo após o decurso de dois anos para adequação à LGPD, não foi tempo suficiente para praticamente quarenta por cento das empresas do país. Tais dados podem levar a uma conclusão lógica de que a simetria com a lei é algo que deverá ser constante e estar sempre em análise pelas empresas, para garantir uma adequação completamente e conformidade com a legislação.

A garantia de uma política de tratamento de dados, para as empresas, em consonância com a lei, combatendo cláusulas abusivas e vedando o tratamento de dados indevido, pode-se dar a partir de um núcleo específico que atuaria exercendo essa finalidade.

Neste sentido, será necessário que as empresas optem por programas de *compliance*, que consiste em um conjunto de disciplinas para que se cumpram as normas regulamentares, as políticas e as diretrizes estabelecidas para as atividades das empresas, para evitar o acontecimento de irregularidades e as sanções impostas pela lei (BARRETO FILHO, 2019).

Deste modo, as empresas, ao optarem pelo tratamento de dados de seus consumidores, deverão possuir mecanismo próprio para que não ocorra nenhuma ilicitude ou vazamento de dados pessoais pois, caso ocorra, além das sanções que serão atribuídas pela lei, pode ser imputada à empresa uma imagem negativa, implicando em transtornos, principalmente os financeiros, devido à penalizações administrativas que a empresa deverá arcar, bem como por uma possível rejeição do público, pela empresa, por sua fama negativa.

Ainda nesse sentido, a legislação contempla no art. 41 a figura do encarregado de proteção de dados pessoais

> O encarregado pelo tratamento de dados pessoais, internacionalmente conhecido como Data Protection Officer (DPO), possui a função de atuar como canal de comunicação entre instituição, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). (BRASIL, 2018, art. 41).

Como exposto, tal funcionário atuará de maneira semelhante a um núcleo de *compliance*, fiscalizando o tratamento de informações coletadas pela empresa e garantindo que sejam utilizadas de acordo com a disposição da lei. Além disso, é o responsável por manter contato com a ANPD, se necessário, e atender as demandas dos próprios titulares de dados.

Sob outra perspectiva, considerando as medidas de fiscalização estabelecidas pela LGPD, esta ocorre a partir da constituição da Agência Nacional de Proteção de Dados. Elencada no capítulo IX da LGPD e artigos subsequentes. A ANPD é um órgão independente e parte do Poder Executivo do Governo Federal criada com atribuições de fiscalizar e divulgar como toda a informação pessoal e dados pessoais que circulam e são utilizados pelas empresas devem ser tratados, ou seja, fazer cumprir a LGPD. (TEIXEIRA, 2021).

Assim, a partir da interpretação e conceito da ANPD, pode- se dizer que a Agência possui o dever de fiscalizar o cumprimento da lei, por parte das empresas, corporações e órgãos públicos que optem por desenvolverem suas atividades captando dados de consumidores, proporcionando assim um ambiente virtual e físico com o devido comprometimento e seriedade que os dados pessoais necessitam.

Diante desse contexto, pode-se dizer que o país possui uma legislação completa sobre o tratamento de dados pessoais, com o exercício da fiscalização em vigência, desde agosto de 2021, sendo capaz de aplicar sanções administrativas quando necessário. Entretanto, a atuação deve ocorrer em conjunto com o olhar das empresas e corporações, não apenas por parte da Agência.

As empresas que atuam operando dados de consumidores, por razões comerciais, desejam manter sua prática de captação, sem receber nenhum tipo de sanção, que limite suas atividades. Assim, o que se espera das corporações é que para que suas atividades não recaiam em ilegalidade, efetivamente contratem um núcleo de fiscalização ou compliance dedicado a fiscalizar o tratamento, possibilitando assim uma coleta de dados constantemente verificada por especialistas e de acordo com a legislação.

Tal prática das empresas, consequentemente, facilitará o trabalho da ANPD, reduzindo a necessidade de se atribuir sanções administrativas, tendo em vista que haverá um consenso sobre a importância do que está sendo tutelado, nesse caso, um tratamento de dados adequado.

Dado o exposto, o que se espera das empresas que trabalham com captação de dados, e da lei, é uma fiscalização em conjunto, uma vez que a LGPD nunca propôs uma proibição ao tratamento e acesso de empresas aos dados de consumidores, o que sempre se almejou foi uma captação de acordo com a legalidade, preservando o mais valioso nessas relações de consumo, as informações pessoais dos indivíduos.
Em conclusão, respeitando o bem tutelado pela LGPD e atuando em conjunto, entre a legislação vigente e as empresas e corporações, os embates entre elas podem ser minimizados. Isso viabilizará um ambiente de captação, tratamento e compartilhamento de dados de consumidores, como propõe a LGPD, correto e respeitando as informações pessoais dos consumidores.

5 CONSIDERAÇÕES FINAIS

A ascensão das relações virtuais proporciona uma série de facilidades e comodidades para os indivíduos que, provavelmente, há meio século, não poderiam ser sequer imaginadas.

As diversas praticidades no dia a dia do consumidor, possibilitadas pelo avanço do meio virtual, transferiram o consumo para uma realidade imediatista. A viabilidade de se realizar variados tipos de compra do conforto de casa, por exemplo, é um fator que há alguns anos não era cogitado, além disso, o próprio acesso à informação passou a ocorrer de maneira mais instantânea, fazendo com que o consumidor não dependesse mais de meios físicos para acessar as notícias.

Os ilimitados recursos, disponibilizados para os indivíduos, também geram um problema de proporções significativas, relacionado à proteção de dados. É extremamente comum em uma compra on-line, logo ao acessar o *site*, se deparar com os Termos de Uso, com a Política de Dados e com os chamados *cookies* de uma plataforma, os quais informam, ou pelo menos deveriam informar, de que maneira as informações pessoais que um indivíduo compartilha com o *site*, serão utilizadas.

Em ambiente físico isso também ocorre, mas de maneira diferente. Nesses locais, os fornecedores e lojistas costumam atribuir descontos aos consumidores que informarem o CPF ou se cadastrarem no sistema da loja, para que assim acumulem dados de diversos consumidores.

O questionamento acerca do motivo de empresas oferecerem promoções a seus clientes em troca de seus dados pessoais, ou as plataformas virtuais informarem, em um primeiro acesso, a sua política de privacidade, foi algo questionado quando a prática da coleta se iniciou.

Entretanto, pouco tempo depois do início dessas atividades, já foi possível entender que as empresas estavam se utilizando dos dados de indivíduos para determinados fins. Algumas companhias os comercializavam, lucrando, ou até mesmo

armazenando- os de maneira precária, o que resultou em diversos transtornos e vazamentos de informações pessoais de consumidores.

Os escândalos de vazamento de dados foram cruciais para que o mundo focasse na proteção de dados e se questionasse acerca da maneira pela qual as informações compartilhadas, ou captadas, por empresas estavam sendo utilizadas. Tal questionamento se fez necessário, uma vez que em apenas um vazamento de dados específico, como o do Facebook, centenas de milhões de dados foram comprometidos, com o agravamento de que, nessa situação específica, o usuário sequer foi informado que estaria compartilhando suas informações ao acessar a plataforma.

Deste modo, foi a partir dos diversos vazamentos de dados ocorridos, que muitos países passaram a se atentar e iniciaram elaboração de leis com enfoque na proteção de dados, tendo em vista a comprovação de que a segurança dos dados pessoais no meio virtual e físico, com os dados pessoais dos consumidores, praticamente inexistia, não recebendo a mínima atenção e amparo, necessários.

A partir disso, no ano de 2018, o Brasil publicou sua primeira Lei Geral de Proteção de Dados, nº 13.709/18. A lei visa a regular as atividades de tratamento de dados no país, também por meio da Agência Nacional de Proteção de Dados, a qual age no sentido de fiscalizar e principalmente atribuir sanções administrativas às empresas infratoras.

Em um cenário de instabilidade e escassa regulação sobre o tema, a elaboração da LGPD consistiu em enorme avanço. Por meio de dispositivos específicos e abrangentes, que se propõem a regular o modo pelo qual diversas empresas captam, tratam e compartilham dados, vedando ilicitudes e atribuindo sanções que variam de multas, até a impossibilidade de a corporação operar com tratamento de dados.

Assim, a Lei Geral de Proteção de Dados tende a ser uma garantia ao titular de dados de que suas informações serão efetivamente protegidas, tendo em vista que promove um tratamento uniforme, que não discrimina nem restringe sua aplicabilidade e os efeitos decorrentes de sua atuação, apenas a empresas e corporações específicas,

pois, como elencado em seus artigos, os próprios órgãos públicos estão passíveis de infrações, caso atuem em desconformidade com a lei.

Por fim, a Lei Geral de Proteção de Dados e seus mecanismos de atuação, possibilitaram que as diversas cláusulas abusivas encontradas em contratos de consumo fossem classificadas como ilegais, pois, como já abordado, anteriormente à elaboração da LGPD, não havia lei específica que regulamentasse a proteção de dados. Isto culminava em diversas abusividades praticadas por empresas, as quais, com o advento da lei, atualmente não são mais permitidas, transformando, assim, o negócio jurídico dos contratos de consumo, em um tipo de contrato que não o lesa ou prejudica.

REFERÊNCIAS

AGRELA, Lucas. **O escândalo de vazamento de dados do Facebook é muito pior do que parecia.** [*S. l.*]: Exame, 2018. Disponível em: https://exame.com/tecnologia/o-escandalo-de-vazamento-de-dados-do-facebook-e-muito-pior-do-que-parecia/. Acesso em: 27 ago. 2021.

ALMEIDA, João Batista de. **Manual de direito do consumidor**. São Paulo: Saraiva, 2003.

BARRETO FILHO, Marcelo Vandré Ribeiro. **Os contornos jurídicos da lei geral de proteção de dados frente ao consumo no ambiente virtual**. 2019. Trabalho de Conclusão de Curso (Graduação em Direito) – Universidade Federal da Paraíba, Santa Rita, 2019. Disponível em: https://repositorio.ufpb.br/jspui/bitstream/123456789/16373/1/MVRBF27092019.pdf. Acesso em: 08 set. 2021.

BBC News, Brasil. Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira das autoridades. **BCC News**, Brasil, 20 mar. 2018. Disponível em: https://www.bbc.com/portuguese/internacional-43461751. Acesso em: 27 ago. 2021.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais:** a função e os limites do consentimento. 3. ed. Rio de Janeiro, 2021.

BRASIL. Autoridade Nacional de Proteção de Dados. **Sanções Administrativas: O que muda após 1º de agosto de 2021**. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/sancoes-administrativas-o-que-muda-apos-1o-de-agosto-de-2021. Acesso em: 13 out. 2021.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 21 ago. 2021.

BRASIL. **Lei Nº 8.078, de 11 de setembro de 1990**. Código de Defesa do Consumidor. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 22 ago. 2021.

BRASIL. **Lei Nº. 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/Lei/L13709.htm. Acesso em: 22 ago. 2021.

BRASIL. **Lei N. 14.010, de 10 de junho de 2020**. Dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do coronavírus (Covid-19). Brasília, DF: Presidência da

República, 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L14010.htm. Acesso em: 02 out. 2021.

DADOS de 87 mil usuários do Facebook vazaram. [*S. l.*]: Forbes, 2018. Disponível em: https://forbes.com.br/colunas/2018/04/facebook-diz-que-dados-de-87-milhoes-de-pessoas-foram-vazados/. Acesso em: 28 ago. 2021.

DINIZ, Maria Helena. **Código Civil anotado**. 14. ed. rev. e atual. São Paulo: Saraiva, 2009.

DINIZ, Maria Helena. **Código Civil Anotado**. 5. ed. São Paulo: Saraiva, 1999.

DUQUE, Bruna Lyra; PEDRA, Adriano Sant'Ana. Os deveres fundamentais e a solidariedade nas relações privadas. **Revista de Direitos Fundamentais e Democracia**, Curitiba, v. 14, n. 14, p. 147-161, jul./dez. 2013. Disponível em: file:///C:/Users/USUARIO/Downloads/Os_deveres_fundamentais_e_a_solidariedad.pdf. Acesso em: 09 out. 2021.

EUROPEAN COURT OF HUMAN RIGHTS**. Convenção Europeia dos Direitos do Homem**. França: Council of Europe, [2013]. Disponível em: https://www.echr.coe.int/Documents/Convention_POR.pdf. Acesso em: 14 set. 2021.

FARIAS, Cristiano Chaves de. ROSENVALD, Nelson. **Curso de Direito Civil**. v. 4. Salvador: Editora JusPodivm, 2012.

FORNAISER, M. de O., & BECK, C. (2020). CAMBRIDGE ANALYTICA: Escândalo, legado e possíveis futuros para a democracia. *Revista Direito Em Debate*, *29*(53), 182–195. Disponível em: https://www.revistas.unijui.edu.br/index.php/revistadireitoemdebate/article/view/10033. Acesso em: 01 set. 2021.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. **Novo curso de direito civil**: Contratos: Teoria Geral. v. 4. 13. ed. São Paulo: Saraiva, 2017.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). **Acesso à Internet e à televisão e posse de telefone móvel celular para uso pessoal**: 2017. Rio de Janeiro: IBGE, 2018. Disponível em: https://biblioteca.ibge.gov.br/index.php/biblioteca-catalogo?view=detalhes&id=2101631. Acesso em: 30 ago. 2021.

LOPES, André. **Sanções da LGPD entram em vigor, mas apenas como advertências**. [*S. l.*]: Exame, 2021. Disponível em: https://exame.com/tecnologia/sancoes-da-lgpd-entram-em-vigor-mas-apenas-como-advertencias/. Acesso em: 29 set. 2021.

MAIA, Fernanda (coord.). **LGPD**: Aplicação prática das bases legais: as hipóteses para tratamento de dados pessoais da LGPD. [*S. l.*]: LDPG Acadêmico, [2020]. Disponível em: https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2020/09/lgpd-aplicacao-pratica-das-bases-legais.pdf. Acesso em: 19 set. 2021.

MARQUES, Cláudia de Lima. **Contratos no Código de Defesa do Consumidor**: o novo regime das relações contratuais. 4. ed. rev., atual. e ampl. São Paulo: Editora Revista dos Tribunais, 2002.

MERCADO LIVRE. Privacidade. **Declaração de privacidade e confidencialidade da informação do Mercado Livre**. Osasco: Mercado Livre, 2021. Disponível em: https://www.mercadolivre.com.br/privacidade/declaracao-privacidade. Acesso em: 20 set. 2021.

MONTEIRO, Yasmin Souza. **A efetividade dos mecanismos de proteção de dados pessoais na lei 13.709/2018**. 2019. Artigo Científico (Graduação em Direito) – Faculdade de Ciências Jurídicas e Sociais (FAJS), Centro Universitário de Brasília (UniCEUB), Brasília, 2019.

MORAES, Alexandre de. **Direito Constitucional**. 18 ed. São Paulo: Atlas, 2005.
MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). **Revista de Direitos e Garantias Fundamentais**, [*s. l.*], v. 19, n. 3, p. 159-180, 2018. Disponível em: https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1603/pdf. Acesso em: 12 out. 2021.

NUNES, Luis Antônio Rizzato**. Curso de direito do consumidor**. 4. ed. São Paulo: Saraiva, 2009.

OBAR, Jonathan A.; OELDORF-HIRSCH, Anne. The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services. **Information, Communication & Society**, [*s. l.*], p. 1-20, 2018. Disponível em: https://ssrn.com/abstract=2757465. Acesso em: 27 ago. 2021.

OLX. Central de Ajuda. **Política de privacidade**. Rio de Janeiro: OLX, 2020. Disponível em: https://ajuda.olx.com.br/s/article/politica-de-privacidade#ancora2. Acesso em: 20 set. 2021.

OPICE BLUM, Renato. **Proteção de Dados**: Desafios e Soluções na Adequação à Lei. 2. ed. Rio de Janeiro: Editora Forense, 2020.

PANEK. Lin Cristina Tung. **Lei Geral de Proteção de Dados nº 13. 709/18**: uma análise dos principais aspectos e do conceito privacidade na sociedade informacional. 2019. Monografia (Graduação em Direito) – Faculdade de Direito, Universidade Federal do Paraná, Paraná, 2019. Disponível em: https://acervodigital.ufpr.br/bitstream/handle/1884/68114/TCC%20FINAL%20-%20lgpd.pdf?sequence=1&isAllowed=y-. Acesso em: 12 set. 2021.

PEDRA, Adriano Sant'Ana. As mutações constitucionais e o limite imposto pelo texto da constituição: Uma análise da experiência latino-americana. **Revista Brasileira De Estudos Políticos**, [*s. l.*], v. 101, p. 7-36, 2010. Disponível em: https://doi.org/10.9732/116. Acesso em: 12 out. 2021.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais**: comentários à Lei 13.709/2018. 2. ed. São Paulo: Saraiva Educação, 2020.

RODRIGUES, Leandro Nascimento; LEAL, Pastora do Socorro Teixeira. A eficácia dos direitos fundamentais nas relações privadas à luz da jurisprudência do STF: análise crítica do RE 201.819-8 e ADI 4815. **Revista de Direitos e Garantias Fundamentais**, [*s. l.*], v. 19, n. 2, p. 11-42, 2018. Disponível em: https://doi.org/10.18759/rdgf.v19i2.1085. Acesso em: 11 out. 2021.

SOBRINHO, Nayara da S. A proteção de dados pessoais no *e-commerce*: Análise da aplicação da LGPD diante da vulnerabilidade do consumidor. Artigo científico. (Graduação em Direito) -Centro universitário UNIFAGIC, Manhaçu, 2019.

TARTUCE, Flávio. **Direito civil 3**: Teoria Geral dos Contratos em espécie. 12. ed. Rio de Janeiro: Forense, 2017.

TEIXEIRA, Álvaro. O que é ANPD [Autoridade Nacional de Proteção de Dados]. Tecnoblog. 2021. Disponível em: https://tecnoblog.net/409033/o-que-e-anpd-autoridade-nacional-de-protecao-de-dados/. Acesso em: 08 out. 2021.

UNITED NATIONS. **Universal Declaration of Human Rights**. Paris: UN, [1948]. Disponível em: https://www.un.org/en/about-us/universal-declaration-of-human-rights. Acesso em: 20 set. 2021.

WENDT JÚNIOR, Alido A.; EHRHARDT, Fabiano F.; SILVA, Rosane Leal da. Sociedade em rede: caso Cambridge Analytica e a Lei Nº 13.709/2018 uma análise do seu potencial de proteção aos dados dos usuários. *In*: CONGRESSO INTERNACIONAL DE DIREITO E CONTEMPORANEIDADE, 5., 2019. Santa Maria, RS. **Anais** [...]. Santa Maria, RS: UFSM, 2019. Disponível em: https://www.ufsm.br/app/uploads/sites/563/2019/09/5.17.pdf. Acesso em: 05 set. 2021.