

FACULDADE SANTO AGOSTINHO
UNIDADE SETE LAGOAS
CURSO DE DIREITO

NATHÁLIA DIANA RUBIM AVELAR

**A LEGISLAÇÃO BRASILEIRA E A FRAGILIDADE PRÁTICA DA PROTEÇÃO AO
DIREITO DE PRIVACIDADE NO TOCANTE AOS COOKIES DIGITAIS**

Sete Lagoas

2021

NATHÁLIA DIANA RUBIM AVELAR

**A LEGISLAÇÃO BRASILEIRA E A FRAGILIDADE PRÁTICA DA PROTEÇÃO AO
DIREITO DE PRIVACIDADE NO TOCANTE AOS COOKIES DIGITAIS**

Atividade apresentada à disciplina
Trabalho de Curso II, como requisito
parcial de avaliação.

Professor Orientador: Me Franklin
Vinicius Dutra Marques

Sete Lagoas

2021

Dedico este trabalho aos meus pais, Vanessa e Paulo, que sempre me apoiaram e incentivaram a conquistar meus sonhos e ser uma mulher independente. Dedico também ao meu primo Magno (*in memoriam*) que sempre me servirá de inspiração.

AGRADECIMENTOS

Agradeço, primeiramente, a Deus por ter me dado a oportunidade de escolha e de estar cursando um curso superior. Curso este que tenho muito orgulho e que honrarei no exercício da profissão. Agradeço a Ele, também, pela minha saúde, por toda experiência adquirida, por todas pessoas e profissionais maravilhosos que conheci nesta jornada.

Agradeço ao meu pai e minha mãe por sempre me incentivarem a ser uma mulher independente e correr através dos meus sonhos. Por sempre me apoiarem em tudo e por me proporcionarem a oportunidade de fazer uma faculdade. Obrigada por todos os conselhos, ajuda, incentivo quando titubeei em desistir e colo quando precisei. Obrigada por acreditarem em mim e me fazerem quem eu sou.

Agradeço os professores por todo conhecimento transmitido, paciência e a motivação de lutar por um futuro melhor. Agradeço em especial, o meu orientador deste trabalho de curso, Me. Franklin Marques, pela dedicação, zelo, paciência e companheirismo na construção deste trabalho para que fosse realizado da melhor maneira possível.

Onde tive a oportunidade de iniciar o meu primeiro estágio, onde aprendi a ser humana e sensível em uma profissão que, ainda, é muito desigual e fria aos vulneráveis, onde aprendi deixar os preconceitos de lado para lutar pelos que não são ouvidos e que o fim maior do direito deve ser a busca do direito à dignidade, em toda sua forma.

Minha eterna gratidão à Terceira Vara Cível de Sete Lagoas onde estagiei com muita felicidade por dois anos e que só um “muito obrigado” não basta para retribuir todo conhecimento que foi me ensinado, todo carinho e felicidade diária. Foi neste lugar que obtive o aprendizado que levarei por toda vida, tanto no espaço profissional quanto pessoal.

Não poderia me esquecer dos amigos que a sala de aula me presenteou, em que compartilhei emoções, felicidade, nervosismo e que agradeço por toda motivação, companheirismo e risadas, em especial à Amanda, Isadora, Kevin e Rayane.

Por fim, agradeço a todos meus amigos e meus primos, em especial ao Luiz Felipe e à Núbia, que estiveram sempre comigo, que estiveram sempre me ajudando, apoiando e torcendo por mim. E a cada um que de alguma forma esteve comigo nesta árdua, porém feliz, jornada. Meus eternos agradecimentos a todos!

RESUMO

O presente trabalho de curso aborda a questão do direito de privacidade, no tocante aos *cookies* digitais, e como têm sido a aplicação empírica da legislação brasileira. Na atual era informacional, o cotidiano dos indivíduos está sendo, cada vez mais, realizado nos meios digitais e com isso, o fluxo de informações, em especial, os dados pessoais estão sendo mais compartilhados e expostos. Percebe-se que, gradativamente, o compartilhamento, a venda e o vazamento de dados têm sido notícias e situações comuns em nossas vidas. Quem nunca recebeu inúmeros *spams*, mensagens e ofertas via e-mail ou sms sem ter compartilhado seu contato a essas empresas? Ou até mesmo sofreu prejuízos ou fraudes por ter tido seus dados vazados? Desse modo, a questão que surge e que busca solucionar com a presente pesquisa é: por qual motivo a aplicabilidade do direito à privacidade, em relação aos meios informacionais, a exemplo dos *cookies*, não é consumada mesmo com a legislação brasileira, constitucional e infraconstitucional, possuindo muitos dispositivos legais a fim de resguardar tal direito? Assim, por meio da pesquisa bibliográfica, legal e jurisprudencial este estudo procurou entender o que está ocorrendo. A hipótese levantada no início do trabalho é a ineficácia da legislação brasileira. No entanto, ao final do trabalho a hipótese não foi confirmada, uma vez que a legislação específica do tratamento de dados pessoais digitais, a lei 13.709/18, até o momento, não está em pleno vigor. Não podendo, assim, julgar como está sendo aplicada, pois ainda, não está em vigência. Deste modo, a conclusão do trabalho ficou em aberto, mas, por outro lado, conseguiu atingir o objetivo de pesquisar e analisar como está sendo o processo de efetivação do direito de privacidade nos meios digitais.

Palavras-chaves: Direito de Privacidade. Lei de Proteção de Dados Pessoais (LGPD). Direito e Tecnologia.

LISTA DE FIGURAS

Figura 1 - Ações estratégicas vinculadas ao objetivo estratégico 1	36
Figura 2 - Ações estratégicas vinculadas ao objetivo estratégico 2	36
Figura 3 - Ações estratégicas vinculadas ao objetivo estratégico 3	37

SUMÁRIO

1 INTRODUÇÃO	9
2 OS DADOS PESSOAIS E O USO DE INFORMAÇÕES DE NAVEGAÇÃO – COMPREENDENDO O QUE SÃO OS COOKIES E COMO SÃO UTILIZADOS	11
2.1 Considerações Iniciais	11
2.2 Dados Digitais	12
2.3 Dados digitais segundo a Lei 13.709/18.....	13
2.4 Uso de informações de navegação – <i>Cookies</i>	15
2.5 Como os cookies são utilizados e os seus impactos.....	17
3 A LEGISLAÇÃO BRASILEIRA EM RELAÇÃO AOS COOKIES E AO DIREITO DE PRIVACIDADE.....	21
3.1 Os direitos de personalidade – Código Civil de 2002	21
3.2 O direito de privacidade	23
3.3 O código de defesa do consumidor (lei nº 8.078/90)	27
3.4 A lei de proteção de dados pessoais – LGPD (lei nº 13.709/2018).....	29
4 COMO A VIOLAÇÃO DO DIREITO DE PRIVACIDADE ESTÁ SENDO TRATADO NA PRÁTICA PELA LGPD E PELOS TRIBUNAIS	34
4.1 As sanções previstas na LGPD e como são realizadas	34
4.2 Como a violação aos direitos de privacidade estão sendo julgados pelos tribunais brasileiros.....	39
5 CONSIDERAÇÕES FINAIS	46

1 INTRODUÇÃO

Atualmente, percebe-se que a chamada quarta revolução industrial, iniciada a partir dos anos 2000, está sendo a responsável pelo aumento exponencial do fluxo de informações digitais. Um destes fluxos de informações são os *cookies* digitais, responsáveis pelo rastreamento e monitoramento dos usuários dos meios informacionais. A legislação brasileira, constitucional e infraconstitucional, conta com muitos dispositivos legais a fim de proteger a privacidade dos cidadãos. No entanto, intui-se que a aplicabilidade do direito à privacidade não é respeitada, a exemplo dos *cookies* digitais e assim, surge o problema da presente pesquisa: a legislação brasileira, em sua aplicação prática, tem sido suficiente para resguardar o direito de privacidade diante de vários casos de violação e vazamento de dados pessoais?

Assim, a hipótese que se constrói é: a legislação brasileira não é eficaz, na prática, não apresentando ainda os mecanismos para efetivar o direito de privacidade dos indivíduos nos meios digitais, especialmente quanto aos *cookies*.

E, com isto, o objetivo geral da pesquisa é corroborar a hipótese apresentada e demonstrar que a legislação brasileira não é eficaz quanto ao direito de privacidade em relação aos dados pessoais dos seus usuários no meio digital. Para tanto, deve-se esclarecer o que são os cookies digitais, analisar o ordenamento jurídico brasileiro em relação ao direito de privacidade, pesquisar porque a legislação está sendo falha para se chegar ao final e discutir eventuais soluções.

A escolha do presente tema foi engendrada por se tratar de um assunto de grande relevância social devido ao novo cotidiano das pessoas e com grandes repercussões jurídicas e que ainda, por ser um assunto, relativamente, novo, demanda muita pesquisa, estudo e discussão, tanto por parte do meio acadêmico, entre os operadores do direito e o Poder Público para que a tutela do direito de privacidade seja efetivada nos ambientes digitais.

O método de abordagem utilizado neste trabalho foi o hipotético-dedutivo, por iniciar-se através da identificação do problema, apresentado como uma lacuna na legislação brasileira e a hipótese que foi construída diante deste problema. Já o

método de procedimento foi o monográfico, com base em bibliografias sobre o tema, publicações acadêmicas, a própria legislação brasileira e as decisões judiciais relativas ao tema.

Por fim, a estruturação do trabalho se dá em três capítulos, com a finalidade de ser o mais compreensível, objetivo e claro o possível, o primeiro capítulo trata-se de uma questão mais técnica e tem o objetivo de explicar sobre os dados pessoais, os cookies e suas peculiaridades técnicas, além de explicar também como são utilizados. O segundo capítulo ficou a cargo de pesquisar e analisar o direito de privacidade em si e toda legislação brasileira concernente a esse assunto e o último capítulo foi responsável por debater como o direito de privacidade em relação aos dados digitais está sendo aplicado na prática.

Deste modo, a partir desta estruturação, problemas, hipóteses e objetivos apresentados, o presente trabalho procura pesquisar, analisar e estudar o tema da privacidade digital, especialmente, em relação aos *cookies*, e como é tratado na legislação brasileira. Com isso, busca-se com esta pesquisa, contribuir de alguma forma no cenário acadêmico e jurídico para o novo cenário que está sendo construído com a inovação tecnológica.

2 OS DADOS PESSOAIS E O USO DE INFORMAÇÕES DE NAVEGAÇÃO – COMPREENDENDO O QUE SÃO OS COOKIES E COMO SÃO UTILIZADOS

2.1 Considerações Iniciais

No início de 1960, houve a Terceira Revolução Industrial, chamada também de Revolução Técnico-Científica ou Informacional, que foi responsável pela inovação na área da informática, telecomunicações e robótica, o que permitiu o desenvolvimento de aplicações tecnológicas aos processos industriais. As atividades que mais destacaram durante esse processo foi o desenvolvimento de computadores e softwares e dos meios de comunicação, como a telefonia e a internet. (SANTOS, 2019, p. 25)

A partir dos anos 2000, o mundo vivenciou, e ainda vivencia, a Quarta Revolução Industrial. Entre os destaques desta revolução industrial têm-se o crescimento exponencial da capacidade de computação e a combinação de tecnologias físicas, digitais e biológicas as quais propiciam a realidade aumentada, a realidade virtual e outras. (Ibidem)

O marco deste ciclo é a integração do mundo virtual e o mundo real. Com isto, houve a intensificação dos fluxos de informação e assim, a possibilidade de registro de, praticamente, todos os atos realizados cotidianamente através dos meios informatizados.

Com isso, a sociedade atual, conforme Bruno Ricardo Bioni (2020), está encravada por uma nova forma de organização em que a informação é o elemento nuclear para o desenvolvimento da economia, substituindo os recursos que outrora estruturavam as sociedades agrícola, industrial e pós-industrial. Com a informação ocupando o protagonismo social e econômico na sociedade contemporânea, esta vem sendo chamada de sociedade da informação.

Pois bem, esses atos realizados no ambiente virtual são transformados em informações e estas são armazenadas, possibilitando, assim, a identificação dos indivíduos que o praticaram. Os dados de identificação dos indivíduos são importantes para o funcionamento das redes e também para sua proteção, até mesmo para que a

pessoa por trás do computador sintam-se minimamente responsáveis por seus atos na internet. No entanto, esses dados podem e têm sido utilizados indiscriminadamente pelas empresas que os comercializam, o que, se realizado de maneira clandestina, sem a prévia informação e coleta do consentimento do usuário, caracteriza uma violação ao direito de privacidade.

Para que seja possível o aprofundamento no assunto, faz-se necessária a explicação do que são os *cookies*, como são utilizados, a sua importância na sociedade informacional, bem como, os conceitos básicos utilizados no meio técnico informacional e no âmbito jurídico, especialmente com base na lei nº 13.709/2018, que ficou conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD).

2.2 Dados Digitais

A palavra “dados”, segundo o dicionário Michaelis (2020), é um substantivo masculino plural, tem origem do latim “*datum*” e cuja tradução é: aquilo que se dá. O seu significado pode ser explicado como informações que identificam o indivíduo.

Em termos gerais, dados digitais podem ser utilizados como sinônimo de informações digitais. Porém, no vocabulário técnico da informática, dado é diferente de informação. Em outras palavras, em sentido técnico, esses dois termos não se confundem, embora isso aconteça na linguagem coloquial, como será explicado a seguir.

Para poder compreender tais conceitos técnicos, é necessário fazer a diferença entre um dado bruto e dado processado. Segundo Leandro Pinho (2019), os dados brutos são as informações isoladas, seja ela numérica, textual ou alfanumérica (que são os que possui símbolos, letras e, ou, números), por exemplo: uma data “01.01.01”, um número qualquer “1234”, uma palavra “paz”, um nome “Maria”, um e-mail, um endereço ou um telefone do usuário.

Esses dados, quando são cadastrados, são dados isolados e considerados como brutos, pois sozinhos não são capazes de transmitir nenhuma informação. Após o cadastramento desses dados brutos, eles serão armazenados de forma inter-

relacionada e agrupada, adicionando a eles um contexto e importância, de modo que, assim, passam a representar informações. Nesse momento, então, passam a serem chamados de dados processados.

Dessa forma, uma palavra para os computadores, por exemplo, “Maria”, é apenas uma sequência de letras, quando interpretada como dado bruto. Contudo, ela é um nome e, quando processada, transforma-se em um dado processado e, conseqüentemente, em uma informação.

Portanto, os dados brutos são apenas dados, não significando tecnicamente informações. A seu turno, dados processados são, de fato, informações digitais. Logo, é correto afirmar que toda informação digital é um dado digital, mas nem todo dado digital é uma informação digital.

2.3 Dados digitais segundo a Lei 13.709/18

Já no âmbito jurídico, a lei nº 13.709/2018 (LGPD), responsável pela proteção de dados pessoais no ambiente virtual, em seu art. 5º, elenca os conceitos dos principais termos técnicos utilizados em sua redação. Assim, é imprescindível trazer esses conceitos para a boa compreensão do tema a luz da legislação brasileira. Portanto, conforme prescreve a referida lei:

Art. 5º Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. (BRASIL, 2018)

Sobre o assunto, explica Gabrielle Bezerra Sales Sarlet (2020, p. 19): “dados pessoais são todas as informações de caráter personalíssimo caracterizadas pela identificabilidade e pela determinabilidade do seu titular”.

Assim, os dados pessoais são todas as informações da pessoa, física ou jurídica, que possam ser utilizadas para identificá-la, como por exemplo, o nome e

sobrenome, endereço, CPF, RG, data de nascimento. Em outras palavras, são todos os dados que são capazes de identificar o indivíduo e determiná-lo.

Já os dados pessoais sensíveis da pessoa física, caracterizados no inciso II do art. 5º da lei em comento, são aqueles que versam sobre: “[...] origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico” (BRASIL, 2018). Sendo assim, os dados sensíveis são aqueles que dizem respeito às características sociais, políticas e subjetivas dos indivíduos.

Por fim, os dados anonimizados são aqueles incapazes de revelar a identidade de uma pessoa. Sobre esse assunto, é interessante o esclarecimento de Bruno Ricardo Bioni (2019, p. 69):

Essa inaptidão pode ser fruto de um processo pelo qual é quebrado o vínculo entre o(s) dado(s) e seu(s) respectivo(s) titular(es), o que é chamado de anonimização. Esse processo pode se valer de diferentes técnicas que buscam eliminar tais elementos identificadores de uma base de dados, variando entre: a) supressão; b) generalização; c) randomização e; d) pseudoanonimização.

Nesse contexto, o conjunto dessas informações compõe os perfis digitais. Tais perfis são composições das informações fornecidas pelos usuários, unindo os dados pessoais e sensíveis. Contemporaneamente, tais perfis digitais possuem grande valor, pois nossa atual sociedade pode ser vista como tecnológica, consumerista e informacional. Assim, tais perfis, carregam informações que possuem valor econômico, pois podem ser utilizados por órgãos privados com objetivos comerciais, para caracterização do mercado consumidor e estímulo ao consumo, ou mesmo por órgãos governamentais, para fins de investigações tributárias e criminais, por exemplo. A esse respeito, explica Demócrito Filho (2002, p. 432):

Se, por um lado, a coleta de informações pessoais pode favorecer negócios, facilitar decisões governamentais ou até mesmo melhorar a qualidade de vida material da sociedade como um todo, outros valores necessitam ser considerados à luz da privacidade individual.

Diante desse cenário, faz-se necessário e urgente analisar essas práticas, a fim de verificar se o direito de privacidade está sendo resguardado ou violado através

da comercialização desses dados. Na prática, já se percebe que o que acontece é a coleta desses perfis e sua manipulação através dos *cookies* visando atender as estratégias de marketing das empresas que financiam os provedores de serviços e tecnologia. Para tanto, é relevante entender primeiramente o que são os *cookies* digitais, os quais serão analisados no próximo tópico.

2.4 Uso de informações de navegação – *Cookies*

Neste ponto, o foco do presente estudo direciona-se a uma parte mais técnica acerca dos dados pessoais, aprofundando-se em uma de suas vertentes, que são os *cookies* de navegação na internet. Para tal, partimos das explicações apresentadas por Paul Deitel e Altieres Rohr, importantes autores especializados no assunto:

Os *cookies*, em geral, são pequenos trechos de texto acondicionados no *browser* ou navegador Web utilizado pelo usuário, usados para armazenar informações. É uma ferramenta para personalizar páginas Web e permitir que acessos futuros do usuário ao site sejam de modo personalizado, pois podem ser reativados quando o usuário retornar à página web, identificando informações outrora coletadas e serem aplicadas naquele momento de acesso. (DEITEL, 2010 apud NETO, 2018, p. 1501)

O *cookie* é um recurso básico da web. Ele é criado quando um site solicita ao navegador que uma informação seja armazenada. Por exemplo, quando você faz *login* em um site, o site pede que o navegador armazene um código. Toda vez que você visitar outra página naquele site, o navegador enviará o código. O site estará preparado para saber que o internauta com aquele código é você e o manterá logado no sistema. (ROHR, 2010 apud NETO, 2018, p. 1502)

Em outros termos, os *cookies* são a principal tecnologia de rastreamento e monitoramento de usuários na rede. Eles permitem a análise de navegação do usuário por certo período de tempo. Os *cookies* podem ser classificados por diversas maneiras. Duas classificações importantes para a compreensão deste trabalho são: aquela que os caracteriza como temporários de sessão ou persistentes; e aquela que os distingue como de primeira parte ou de terceiros.

O *cookie* temporário, também conhecido como *cookie* “de sessão”, e conforme ensina Queiroz (2011, apud NETO, 2018, p. 1.503): “será gravado apenas enquanto durar a navegação em determinado site, ou seja, durante a sessão

estabelecida entre o navegador e aplicação web. ” Assim, trata-se daquele *cookie* que permanece no computador do usuário apenas enquanto ele está visitando o *site* ou o aplicativo e duram somente até o navegador ser fechado.

Por outro lado, os *cookies* persistentes são aqueles que permanecem no computador ou celular até que sejam removidos manualmente pelo usuário ou até a data especificada pelo site. Sobre o tema, de acordo com Rohr, (2010, apud, NETO, 2018, p. 1503)

Por questões técnicas, a data máxima hoje é o ano de 2038 —é claro que você não vai ficar com o mesmo computador até 2038, portanto essa é uma data simbólica. Alguns chamam os *cookies* marcados com validade até 2038 como “*cookies* eternos” por representarem a intenção do site de nunca remover aquele cookie.

É interessante perceber que esses *cookies* são utilizados quando o navegador fornece a opção de guardar o *login* e por sistemas de publicidade e *marketing* da internet, para determinar qual o perfil do usuário para oferecer campanhas publicitárias com maior potencial de gerar interesse de consumo no usuário.

Em uma outra classificação, percebe-se que os *cookies* “de primeira parte”, são aqueles definidos pelo site ou aplicativo que o usuário está acessando e só podem ser lidos por esse mesmo site. Em tese, as informações prestadas ficaram restritas àquele site que o usuário optou por acessar.

Por outro lado, os *cookies* de terceiros são os que surgem com o inter-relacionamento entre os sites que mantêm relação comercial. Eles são manuseados por sites diferentes daquele em que o usuário está navegando e têm como objetivo rastrear as visitas dos usuários nos sites que eles anunciam.

É verdade que essa utilização de informação de navegação pode ser útil e necessária para bom funcionamento da internet. Por exemplo, elas podem melhorar os serviços oferecidos pelos sites e permitem que o site reconheça o dispositivo, para que não seja necessário repetir as informações durante a sessão, fazendo que o acesso seja mais rápido e mais bem adaptado graficamente. Contudo, os *cookies* também podem e têm sido usados, deliberadamente, por sites anunciantes, os quais têm comercializado esses arquivos, realizando uma conduta que pode ser compreendida como violação ao direito de privacidade.

Diante desse contexto, o presente estudo busca demonstrar como esse mecanismo eletrônico viola o direito de privacidade, até qual ponto esse direito é violado, como a legislação brasileira protege esse direito fundamental e se a legislação brasileira se adequa ao dispositivo constitucional que protege a privacidade, quando aplicado ao ambiente digital.

2.5 Como os cookies são utilizados e os seus impactos

Como visto anteriormente, os *cookies* são os dados coletados durante a navegação em uma página na web e são usados tanto para o bom e eficiente funcionamento da internet, quanto para capitalização de informações para diversos fins. Essas informações podem ser utilizadas por entes públicos quanto por entes privados. O presente estudo tem como objetivo o estudo da coleta das informações pelas grandes empresas privadas contraposto ao direito de privacidade, por isto, o foco se resumirá à ao manuseio da informação do usuário por essas empresas.

Com a mudança de comportamento social e econômico que se observa em nossa sociedade atual, em que as atividades cotidianas vêm sendo realizadas cada vez mais de maneira *on-line*, as informações e os dados gerados por seus usuários se transformaram em um valioso produto com valor econômico agregado. Conforme bem-dito por Bruno Ricardo Bioni (2020, p. 12)

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.

O que explica a grande importância dos *cookies* pelo mercado publicitário é que eles são uma forma de publicidade personificada. Esta, é mais eficiente do que a velha publicidade em que as propagandas eram feitas em massa e assim, ineficientes, por não se aterem claramente o seu público-alvo.

Já a publicidade personificada, ou direcionada “é uma prática que procura personalizar, ainda que parcialmente, tal comunicação social, correlacionando-a a um

determinado fator que incrementa a possibilidade de êxito da indução ao consumo”. (BIONI, 2020, p. 15)

Dentro das espécies de publicidade personificada há a publicidade comportamental *on-line* que se caracteriza como mais eficiente das publicidades direcionadas pois, esta permitiu uma personalização ainda maior entre os compradores e vendedores por meio dos *cookies* digitais. Conforme explicitado pelo supracitado autor:

Por meio do registro da navegação dos usuários cria-se um rico retrato das suas preferências, personalizando-se o anúncio publicitário. A abordagem publicitária passa a ser atrelada com precisão ao perfil do potencial consumidor. Sabe-se o que ele está lendo, quais os tipos de *websites* acessados, enfim, tudo aquilo em que a pessoa está efetivamente interessada e, em última análise, o que ela está mais suscetível a consumir com base nesse perfil comportamental (BIONI, 2020, p. 17)

Além de toda a sua importância para se chegar exatamente ao consumidor alvo os *cookies* reduziram os custos publicitários, exatamente pelo mesmo motivo.

Assim, os dados pessoais dos usuários são essenciais no atual mecanismo da economia, o que faz que nossos dados sejam acessados e monitorados a todo momento pelos navegadores e transmitidos aos canais de venda, colocando, desta forma, a privacidade dos dados digitais dos usuários em perigo.

Além do seu funcionamento, é importante, também, saber como os *cookies* são monetizados, ou seja, como eles são pagos, uma vez que, a maioria dos aplicativos, navegadores e serviços *on-lines* são teoricamente gratuitos, no sentido que não cobram o usuário para que tenha acesso a seu conteúdo. Mais uma vez, fica claro como a informação vem modificando as relações econômicas da sociedade. Anteriormente, os consumidores trocavam o produto ou serviço pretendido por dinheiro, caracterizando uma relação direta e bilateral entre o consumidor e fornecedor. Por outro lado, atualmente, os consumidores não pagam em dinheiro o uso da navegação, o pagamento é feito de maneira não ostensiva, indireta e involuntariamente, por meio do uso econômico dos seus dados digitais.

Assim, os dados são fornecidos pelos indivíduos e os anunciantes pagam aos navegadores (leiam-se navegadores como, e-mails, aplicativos, redes sociais, sites, etc.) para que a publicidade direcionada cheguem a estes indivíduos. Tendo isso em

vista, a relação econômica passou a ser plurilateral envolvendo o consumidor/usuário da web, fornecedor/web e os anunciantes. (BIONI, 2020)

Logo, o que se infere desta relação plurilateral é que o consumidor – ou, pelo menos diversas informações pessoais suas – virou, na verdade, também ele, um produto a ser comercializado, por meio do fornecimento dos seus dados. E, mais ainda, este recoloca-se como a parte hipossuficiente da relação de consumo. Desta forma, o questionamento que se faz aqui é: por que a legislação brasileira, mesmo sendo moderna e robusta em relação à proteção dos dados digitais, não consegue proteger na prática os dados digitais dos seus usuários?

Como exemplo disso, têm-se o fato ocorrido em janeiro de 2021, em que o Brasil foi alvo do maior ataque cibernético da história. Conforme matéria publicada na revista VEJA, foi descoberto pela empresa de segurança digital PSafe o vazamento de 40 milhões de CNPJs de empresas nacionais e 223 milhões de CPF's, número superior de toda população brasileira pois continha também dados de pessoas falecidas. O ocorrido foi um ataque cibernético por hackers que conseguiram estes dentre outros dados extraídos do sistema da Serasa Experian. Segundo a matéria;

Os perigos se concentram nos dados de órgãos do governo e de grandes empresas. No ano passado, o Tribunal Superior Eleitoral (TSE), o Ministério da Saúde e a Embraer, entre outros, foram alvos de invasões. Também em 2020, uma brecha simples de segurança expôs dados pessoais de clientes do banco digital Nubank. (CASTRO, 2021)

Apesar de que o Brasil conte com uma boa legislação de proteção de dados, na prática ela é ineficiente e, mais do que isso, as empresas não se preocupam em se proteger ou em protegerem os dados dos seus clientes. O jornal CNN, publicou uma matéria com executivo Marco DeMello da empresa PSafe, a mesma que identificou o mega vazamento de dados de brasileiros, em que afirma que esses casos serão cada vez mais comuns e que as empresas brasileiras são negligentes com esse assunto. De acordo com a notícia

Segundo ele, o Brasil é o segundo pior país do mundo quando o assunto é cybersegurança. E isso pode trazer grandes problemas. Nos Estados Unidos, 60% das pequenas e médias empresas que são atacadas por hackers vão à falência após seis meses, segundo dados da organização sem fins lucrativos U.S. National Cyber Security Alliance. Entre os motivos estão as perdas de documentos essenciais, perda de credibilidade e, claro, processos e multas de governos. No Brasil, a partir de agosto, a Lei Geral de Proteção de Dados

permitirá que o governo passe a multar empresas em até R\$ 50 milhões ou até 2% do faturamento bruto. É um valor que pode, de fato, acabar com as empresas, ainda mais em um momento em que vivemos. E, segundo DeMello, as empresas não se protegem porque não querem. “São medidas básicas e não muito custosas”, diz ele. “As empresas investem para criar, mas não investem o suficiente para proteger.” (JANKAVSKI, 2021)

Diante do exposto, o que fica demonstrado é que a legislação brasileira contém mecanismos para a proteção dos dados dos seus usuários, mas fica a sensação de que, na prática, as empresas e, até mesmo o governo, não aplicam os mecanismos de segurança. Dessa maneira, necessário adentrar dentro da legislação brasileira para se analisar o que acontece para que aconteça essa situação, que será a partir de agora, objeto de estudo deste trabalho.

3 A LEGISLAÇÃO BRASILEIRA EM RELAÇÃO AOS COOKIES E AO DIREITO DE PRIVACIDADE

3.1 Os direitos de personalidade – Código Civil de 2002

Antes de iniciar o estudo concreto dos direitos de privacidade digital, é necessário compreender que o direito brasileiro não possui uma legislação *una* e direta, ou seja, um código, que trate do direito de privacidade e dos *cookies* digitais sistematizados em um único diploma legal. O ordenamento jurídico brasileiro concernente a este assunto é espaçado e regula indiretamente o uso dos *cookies* através do Código Civil, da lei 13.709/18, a Lei Geral de Proteção de Dados, da Constituição Federal de 1988 e do Código do Consumidor.

Assim, inicia-se o estudo do tema através do Código Civil de 2002, em cujo Capítulo II, os artigos 11 ao 21 regulam os direitos de personalidade.

Os direitos de personalidade, ao longo da história, não tiveram uma trajetória linear e crescente, mas sim passaram por altos e baixos, sendo que se consolidaram após a segunda guerra mundial, com a solidificação do princípio da dignidade da pessoa humana e a declaração universal dos direitos humanos da Organizações das Nações Unidas.

No Brasil, o Código Civil de 1916 já reconhecia os direitos de personalidade de forma implícita, embora tal direito só apareceu de forma explícita no projeto do Código Civil do jurista baiano Orlando Gomes, em que ganharam um capítulo próprio. Assim, o atual Código Civil (2002) foi arquitetado com base no projeto do mencionado jurista em que há um capítulo próprio (Capítulo II) para o direito de personalidade que resguarda os direitos ao nome, à imagem, à liberdade, à honra, à integridade física e aos direitos autorais. (BIONI, 2020)

Segundo Nelson Rosenvald e Cristiano Farias, famosos doutrinadores civilistas brasileiros, o direito de personalidade são:

Aqueles direitos subjetivos reconhecidos à pessoa, tomada em si mesma e em suas necessárias projeções sociais. Enfim, são direitos essenciais ao desenvolvimento da pessoa humana, em que se convertem as projeções físicas, psíquicas e intelectuais do seu titular, individualizando-o de modo a

lhe emprestar segura e avançada tutela jurídica (FARIAS e ROSENVALD, 2006)

Assim, os direitos de personalidade são aqueles essenciais no que diz respeito às integridades física, psíquica, intelectual e moral de cada pessoa, o que, dentre outras coisas, confere a individualidade de cada ser, devendo, portanto, ser tutelados pelo ordenamento jurídico.

A questão para que se deve atentar é que, quando o Código Civil de 2002 foi projetado, não se falava, ainda, em dados pessoais digitais, e a problemática em que se esbarra é: os dados digitais devem ser resguardados como direitos de personalidade? Eles devem ser protegidos conforme os ditames do capítulo II do Código Civil?

Sobre o tema, de acordo com Bioni (2020, p. 57):

[...] cada vez mais, as atividades de processamento de dados têm ingerência na vida das pessoas. Hoje vivemos em uma sociedade e uma economia que se orientam e movimentam a partir desses *signos identificadores* do cidadão. Trata-se de um novo tipo de identidade e, por isso mesmo, tais *dossiês digitais* devem externar informações corretas para que seja fidedignamente projetada a identidade do titular daquelas informações. Isso acaba por justificar dogmaticamente a inserção dos dados pessoais na categoria dos direitos de personalidade, assegurando, por exemplo, que uma pessoa exija a retificação de sus dados pessoais para que a sua projeção seja precisa. Por isso, os dados pessoais não estão relacionados somente com a privacidade, transitando dentre mais de uma das espécies dos direitos da personalidade.

Logo, não resta dúvida de que os dados digitais devem possuir respaldo nos direitos de personalidade, pois aqueles são uma construção da sociedade no curso de sua evolução, e só porque foram extemporaneamente construídos, não devem ser excluídos.

Outro motivo que corrobora para que direito de personalidade resguarde os dados digitais é que o direito de personalidade garante que as informações relativas à personalidade do indivíduo sejam verídicas. Assim, atualmente, na era informacional, é de suma importância que os dados digitais das pessoas sejam verídicos uma vez que toda esfera da vida do indivíduo pode ser colocada nos meios informacionais. Importante ressaltar, dessa forma, que o direito de personalidade está

ligado à veracidade das informações, ao passo que, o direito de privacidade, como será explicitado no próximo tópico se refere ao sigilo e controle das informações.

Portanto, os dados digitais também devem estar tutelados pelo direito de personalidade haja vista a existência de dados digitais públicos e podem necessitar de correção e revisão.

3.2 O direito de privacidade

Como já mencionado, o direito à privacidade é resguardado pela Constituição Federal de 1988 em seu art. 5º, que dispõe sobre os direitos e garantias fundamentais. Este direito é assegurado a todos cidadãos, em decorrência da universalidade dos direitos fundamentais. Ele está contido no inciso X do referido artigo, que diz:

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. (BRASIL, 1988)

Inicialmente, é importante traçar uma breve diferença entre os conceitos de “intimidade” e de “vida privada”, trazidos por este inciso da Constituição. Segundo Alexandre de Moraes (2003, p. 62) os conceitos constitucionais de intimidade e vida privada apresentam grande interligação, porém podem ser diferenciados por meio da menor amplitude do primeiro, que se encontra no âmbito de incidência do segundo. Assim, a intimidade versa sobre as relações subjetivas e de trato íntimo dos indivíduos, como por exemplo, as relações familiares, do meio social, de amizade e amorosas. Já a vida privada envolve as demais relações humanas, este é o conceito mais abrangente, enquanto o primeiro mais delimitado, são, por exemplo, as relações profissionais, comerciais, escolar, etc.

Pois bem, para compreender o conceito de privacidade atual, é necessário entender sua origem, além de que seu significado contemporâneo será fruto da mudança histórica, que envolve a mudança na tecnologia, na economia, na política, no Estado e na sociedade como um todo.

Os autores do início do século XIX, relacionavam o direito de privacidade às ideias de proteção da vida privada, à inviolabilidade da propriedade e honra. No fim do século XIX, os primeiros autores que iniciaram a modificação desta visão do direito de privacidade foram Warren e Brandeis (WARREN; BRANDEIS; DONEDA, 2006, p. 137) que escreveram o famoso artigo “The Right to Privacy”, que é um dos mais citados e relevantes da história norte-americana sobre o tema. Nele, os autores traduziram o cotidiano da época, vendo como os jornais, a fotografia e outras novas tecnologias da época invadiam a vida privada e doméstica das pessoas. Ao escreverem sobre o direito de privacidade, relacionaram sua proteção à inviolabilidade da personalidade, afastando-se da ideia anteriormente dominante, que relacionava a proteção da vida privada à propriedade privada.

Já no século XX, com as transformações do Estado, das relações pessoais e com o desenvolvimento tecnológico, o sentido deste direito foi, consequentemente, modificado. Assim, a doutrina entende como privacidade a aversão a qualquer intromissão não consentida na vida privada (DONEDA, 2006), como se lê em Miranda:

o direito à privacidade permite que o indivíduo mantenha o domínio daquilo que se relacione consigo mesmo, como o corpo, casa, propriedade, pensamentos, sentimentos e tenha liberdade para escolher que parte deste domínio deseja permitir que outras pessoas tenham acesso. (MIRANDA, apud DONEDA, 2006)

O direito de privacidade no século XX traduzia-se no poder individual de escolher dentro dos seus assuntos subjetivos o que poderia ser compartilhado ou não com os demais. É o direito de se ter resguardado qualquer assunto que não seja de interesse público, o qual se encontra resguardado na atual Constituição Federal e que prevê o direito de indenização pelo dano material ou moral decorrente de sua violação.

Já na atual era informacional este conceito vem se mostrando obsoleto, sendo que, para Laura Schertel Mendes (2014, p. 32):

A disciplina da proteção de dados pessoais emerge no âmbito da sociedade de informação, como uma possibilidade de tutelar a personalidade do indivíduo, contra os potenciais riscos a serem causados pelo tratamento de dados pessoais. **A sua função não é a de proteger os dados *per se*, mas a pessoa que é titular desses dados.** (GRIFO NOSSO)

O autor Bruno Bioni explicita seu posicionamento, primeiramente, fazendo a reflexão que o direito à privacidade tem sido historicamente articulado com base na dicotomia entre as esferas públicas e privadas, conforme se lê (LAFER, Celso. Apud.: BIONI, Bruno, 2020, p. 91):

É nesse sentido que se compreende a privacidade como o direito de ser deixado só, (BULOS) estar a salvo de interferências alheias, do segredo ou sigilo que são direitos calibrados pela dicotomia das esferas pública e privada. A pessoa tem o direito de retrair aspectos de sua vida do domínio público (DOTTI) (BIONI, 2020, p. 92)

Logo, vemos que o direito à privacidade, desde os seus primórdios até a sua concepção atual, tem o condão final de proteger o que é privado, relativo à pessoa humana, do que circula na esfera pública. A exemplo disso, a casa, a correspondência e as comunicações dos indivíduos são claras hipóteses de espaços da vida privada que angariaram dispositivos constitucionais autônomos para tutelar sua inviolabilidade. O que é público e privado delimita o conteúdo do direito de privacidade e, segundo Bioni (2020, p. 93), sua lógica se centra na liberdade negativa do indivíduo não sofrer interferências alheias indevidas.

Para se compreender a ideia do referido autor, é necessário, porém, explicitar a diferença entre a liberdade negativa e a positiva. O estudo destes conceitos é de cunho primordialmente filosófico, mas também perpassa por economia, direito, ciência política e outras ciências sociais.

Sobre o assunto, o historiador e filósofo Isaiah Berlin foi referência no estudo da distinção entre a liberdade positiva e negativa em sua obra “Dois conceitos de liberdade”, de acordo com os pesquisadores Marcos Antônio Soares e Tiago Brene (SOARES e BRENE, 2014). Em suma, a diferença entre elas repousa na ideia de que a liberdade negativa é caracterizada pela ausência de algo, como a ausência de interferência; enquanto a liberdade positiva tem como característica a presença de algo, como a presença de uma ação, da autodeterminação. Nas palavras do filósofo, entende-se a liberdade negativa nos seguintes termos:

Sou livre na medida em que ninguém ou nenhum grupo interfere com minhas atividades. A liberdade política neste sentido, é simplesmente a área em que posso agir sem sofrer limitações de terceiros. (BERLIN. Apud.: MENDROT, 2016).

Já em relação à liberdade positiva, o mesmo autor ensina que:

O que torna plausível esse tipo de linguagem é o reconhecimento de que é possível, e às vezes justificável, coagir os indivíduos em nome de algum objetivo (digamos justiça ou bem-estar público) que eles mesmos buscariam se fossem mais esclarecidos. Isso torna mais fácil aceitar que estou coagindo outros em seu próprio benefício, e não em meu interesse. (Ibidem)

Assim, resumidamente, para o autor, a liberdade negativa equivaleria “estar livre de” enquanto a liberdade positiva seria “estar livre para”. Tais considerações foram feitas, pois, para Bioni, o direito de privacidade que está pautado na dicotomia da esfera pública e privada, é balizado como uma liberdade negativa. É “um direito estático à espera de que o seu titular delimite quais fatos da sua vida deveriam ser excluídos do domínio público”. (BIONI, 2020, p. 93)

No entanto, com a evolução tecnológica em ritmos exponenciais e o enorme fluxo de informações pessoais, a necessidade de proteção de dados pessoais está modificando os elementos do direito de privacidade, aprofundando seus postulados e tocando em certos pontos centrais dos interesses em questão. Segundo o já referido autor, esta modificação é tão pertinente que:

Consistiria em uma proteção dinâmica e em uma liberdade positiva do controle sobre as informações pessoais. A esfera privada não seria algo já posto à espera de uma violação, mas um espaço a ser construído *a posteriori* e dinamicamente mediante o controle das informações pessoais. Haveria, por isso, uma mudança qualitativa representada pela transposição do eixo antes focado no trinômio “pessoa – informação – sigilo” ao eixo agora composto por quatro elementos “pessoa – informação – circulação – controle”. [...] Deveria haver um intercâmbio entre as tutelas estáticas e dinâmica do direito à privacidade. (BIONI, 2020, p. 94)

Deste modo, o que se observa é que, na sociedade da informação, o direito de privacidade está ultrapassando o seu âmbito de origem e, novamente, passando por uma modificação.

Assim, o que se percebe é que a modificação do direito de privacidade não o afasta de seu conceito original, mas adiciona uma nova extensão ao seu significado. Tal modificação pode ser vista até mesmo nas novas nomenclaturas como, proteção de dados pessoais, privacidade informacional, autodeterminação informativa e outros nomes. A sua transformação envolve também a mudança do paradigma do direito de privacidade, afastando-se da noção de ser um direito estático, baseado na liberdade

negativa dos indivíduos - ou seja, a espera que seja violado para agir -, para um direito dinâmico, assentado na liberdade positiva dos seus titulares, de modo que, assim, eles deveriam encontra-se empoderados o suficiente para terem a aptidão para os controlar.

Diante disso, sustenta-se que a proteção dos dados pessoais não deve mais ser pautada pela dicotomia entre a esfera pública e privada já que uma informação pública isolada, que inicialmente não causaria problemas em ser divulgadas ou exposta (em linguagem técnica, dados brutos), quando associada a outras podem expor dados sobre a personalidade do usuário (em linguagem técnica, dados processados).

Dessa forma, para Bioni:

O direito à proteção dos dados pessoais deve ser alocado como uma nova espécie do rol aberto dos direitos da personalidade, dando elasticidade à cláusula geral da tutela da pessoa humana. Caso contrário, corre-se o risco de ele não se desprender das amarras conceituais e da dinâmica do direito à privacidade e, em última análise, inviabilizar uma normatização própria para regular o fluxo informacional como fator promocional da pessoa humana. (BIONI, 2020, p. 96)

Pelo exposto, não se trata de mais um direito à privacidade, mas sim, que a proteção dos dados pessoais deve ser entendida como uma extensão do direito à privacidade, com todas as consequências de suas peculiaridades, para se ter autonomia própria e não ser atrelado a uma categoria específica e já existente, como o direito de privacidade.

3.3 O código de defesa do consumidor (lei nº 8.078/90)

O Código de Defesa do Consumidor foi a primeira lei brasileira que tratou mais, detidamente da proteção da privacidade e os dados pessoais dos consumidores. Tal proteção está descrita no art. 43 do referido código, na seção sobre “Dos Bancos de Dados e Cadastros de Consumidores”, integralmente reproduzido a seguir:

Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.

§ 1º Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.

§ 2º A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.

§ 3º O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.

§ 4º Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.

§ 5º Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.

§ 6º Todas as informações de que trata o caput deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor. (GRIFO NOSSO) (BRASIL. **Leis Ordinárias de 1990**. Brasília: Casa Civil, Subchefia para Assuntos Jurídicos, 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm>. Acesso em: 02 fev. 2021)

O que vemos no artigo acima é a proteção ao consumidor em seu direito de informação sobre dados pessoais disponibilizados, além dos direitos à informação correta, a sua retificação caso haja alguma informação errada e de sua disponibilização de maneira acessível, clara e de fácil compreensão.

O que se percebe é o que o mencionado artigo tem a função de dar acesso, retificação e cancelamento aos dados pessoais, incorporando os princípios da transparência, qualidade (exatidão da informação) e limitação temporal, que gravitam em torno da figura do consumidor, para que ele, na condição de titular dos dados pessoais, exerça controle sobre suas informações pessoais. (BIONI, 2020)

Dessa forma, o Código de Defesa do Consumidor (CDC), alcança todo e qualquer dado pessoal do consumidor. No entanto, ele ainda regulamentou de forma genérica e superficial, se assemelhando ao direito de personalidade e ficando a cargo

de outra lei especificar como será o manejo dos dados dos consumidores no âmbito digital.

Diante desta carência legislativa para disciplinar de fato sobre os dados digitais pessoais, o legislador brasileiro verificou a necessidade de uma lei que regulamentasse tal tema, e, assim, surgiu a Lei de Proteção de Dados Pessoais, que será objeto do próximo tópico deste trabalho.

3.4 A lei de proteção de dados pessoais – LGPD (lei nº 13.709/2018)

A Lei de Proteção de Dados Pessoais (LGPD) foi sancionada em agosto de 2018 e alterada pela lei nº 13.853 de 2019, sendo que, dentre das várias alterações, modificou-se a data de vigência da mesma, que passou a ter pleno vigor apenas em agosto de 2020. Ela teve origem no Projeto de Lei nº 53 de 2018, que foi aprovado por unanimidade e em regime de urgência pelo Plenário do Senado. Esta lei é considerada um marco legal que regulamenta o uso, a proteção e a transferência de dados pessoais dos usuários da internet no Brasil.

Antes da LGPD, o Marco Civil da Internet (MCI - Lei nº 12.965/2014) instituiu os princípios, garantias, direitos e deveres para o uso da Internet no Brasil, ficando conhecido como a “Constituição da Internet”. O MCI instituiu, ainda, os crimes cibernéticos e, também, dispõe sobre a proteção da privacidade e dos dados pessoais. No entanto, quanto ao tratamento de dados pessoais, essa lei se mostrou vaga, uma vez que não dispôs sobre o seu uso, destino e comercialização e com isso surgiu a LGPD, que tem como objetivo o tratamento de dados pessoais. Segundo Cíntia Rosa Pereira de Lima e Lívia Froner Moreno Ramiro, pode-se dizer que:

LGPD representa um avanço na tutela dos dados pessoais, pois centralizou o tema, coordenando o sistema protetivo de dados pessoais em sistemas, direitos e obrigações específicos; contudo não exclui outros, como o Código de Defesa do Consumidor.

Neste mesmo sentido é a opinião do autor Bruno Ricardo Bioni para quem “até a aprovação da LGPD, o Brasil contava somente com leis setoriais de proteção de dados. Era uma verdadeira “colcha de retalhos” que não cobria setores importantes

da economia, dentre aqueles cobertos, não havia uniformidade em seu regramento. ” (BIONI, 2020, p. 104)

Os direitos elencados na LGPD estão, em sua maioria, nos artigos 17 a 22 e decorrem da autodeterminação informacional, que é o direito de controlar as informações que lhe dizem respeito ao usuário. Dessa maneira, o consentimento possui um papel fundamental para a consolidação do direito à autodeterminação informacional, pois o consentimento informado e inequívoco, prescrito no art. 7º, I, LGPD, é um dos pilares do sistema protetivo dos dados pessoais. (LIMA e RAMIRO, 2019)

Segundo o art. 5º, XII, da LGPD, o consentimento é a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada (BRASIL, 2019).

Assim, toda informação e utilização de dados deve ter o consentimento com o efetivo conhecimento do titular dos dados e, desse modo, ter real conhecimento dos termos e condições de uso e expressamente concordar com eles.

Além do consentimento, que é uma das principais bases legais para o tratamento de dados, a LGPD também apresenta, todavia, as situações elencadas nos incisos do art. 7º, em que o consentimento é dispensado para o tratamento de dados pessoais, excluído o inciso I que dispõe sobre o consentimento do titular. As situações em que são dispensadas o consentimento são, principalmente, para o funcionamento da administração pública e cumprimento de obrigação legal ou regulatória pelo controlador, presentes nos incisos II, III e IV. Aquelas situações para atender o exercício regular de direitos dos indivíduos, como:

V - Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. (BRASIL, 2019)

Está igualmente dispensado o consentimento quando envolver questões relacionadas à proteção a vida, a incolumidade física e para tutela da saúde, sendo este último ponto, privativamente aos profissionais de saúde e autoridades sanitárias.

Por fim, conforme o inciso IX, “quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais”. (BRASIL, 2019)

Essas hipóteses são previstas para o tratamento de dados pessoais, os quais conforme visto no item “1.3” do capítulo 1, são os dados que são capazes de identificar o indivíduo e determiná-lo. A LGPD é mais rigorosa quanto ao tratamento de dados pessoais sensíveis, que são aqueles que versam sobre as características subjetivas dos usuários. O tratamento destes dados só poderá ser realizado mediante o consentimento do titular, de forma específica, destacada e para finalidades específicas ou, no caso de uso sem o consentimento, nas hipóteses dos incisos II, III, IV, VI, VII e VIII do art. 7º e para:

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. (BRASIL, 2019)

Assim, o que se infere a partir da redação da LGPD, principalmente com o inciso I do art. 7º e do art. 11º, é a permissão para a transação de dados pessoais, desde que haja o consentimento expresso do seu titular. Corroboram essa ideia, o § 5º do art. 7 e o art. 8º deixando claro que:

§ 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores **deverá obter consentimento específico do titular para esse fim**, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei. [...]

Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. (GRIFO NOSSO)

Por outro lado, os dados pessoais sensíveis podem ser compartilhados desde que seus titulares consintam de forma explícita e destacada para finalidades específicas. O que ocorre é que, no §3º do artigo 11, o compartilhamento destes dados com objetivo de obter vantagem econômica (*cookies*) poderá ser objeto de vedação

ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências. (BRASIL, 2019)

Diante do exposto, o que se percebe é que a LGPD permite o tratamento de dados pessoais e dados pessoais sensíveis, desde que haja o consentimento. Além disso, poderá ser vedada ou objeto de regulamentação a venda dos dados sensíveis, que são os *cookies* digitais.

Em outras palavras, a LGPD permite a utilização de *cookies* - desde que consentida - e a sua venda ficará a cargo de lei complementar, ou regulamentação por parte da autoridade nacional que é a Autoridade Nacional de Proteção de Dados (ANPD), regulamentada no Capítulo IX da lei em comento. No entanto, ainda não foi editada a lei complementar para vedar a comercialização de *cookies* e nem objeto de regulamentação por parte da ANPD. Logo, a comercialização dos dados sensíveis, ainda não é proibida no Brasil.

Tal contexto, deixa uma lacuna, com base na qual os *cookies* podem ser utilizados, desde que haja consentimento expresso do usuário e também vendidos. O que se verifica, na prática, é que os meios informacionais impõem aos indivíduos que autorizem o uso de *cookies*, em uma relação que se assemelha um contrato de adesão: ou se autoriza o uso econômico dos *cookies*, ou não se pode acessar o site.

Outro aspecto importante a se ressaltar é que não há transparência em como essas ferramentas serão utilizadas, não sendo respeitados os princípios da qualidade dos dados, transparência e segurança, presentes nos incisos V, VI e VII, respectivamente, do art. 6º e claramente violando o direito de privacidade, que é um dos fundamentos (art. 2º, I) da LGPD.

Além do mais, efetivamente, os titulares dos dados não possuem controle sobre seus dados pessoais, pois meramente o consentimento para sua utilização, não é capaz de impedir sua utilização como *cookies* e, também, em muitas das vezes, as políticas de privacidade não são claras e não são passíveis de questionamento, cabendo ao indivíduo aceitar completamente com esta política de privacidade ou não poderá navegar nesta plataforma, assemelhando-se, como referido acima, a um contrato consumerista de adesão.

Desse modo, a prática do compartilhamento de dados com objetivo de obter vantagem econômica necessita urgentemente de regulamentação, haja vista que apenas o consentimento do usuário não basta para evitar violações. Tão relevante quanto o consentimento do usuário, é assegurar que o fluxo das informações dos dados não seja prejudicial, infringindo o direito de personalidade, e que o titular dos dados possua a efetiva liberdade de escolha ao uso dos seus dados pessoais.

Á vista disso, passa-se ao próximo capítulo do trabalho que analisará como a legislação brasileira está sendo aplicada na prática por tribunais, quanto à violação do direito de privacidade diante ao tratamento de dados pessoais, uma vez que as bases teóricas foram expostas neste capítulo.

4 COMO A VIOLAÇÃO DO DIREITO DE PRIVACIDADE ESTÁ SENDO TRATADO NA PRÁTICA PELA LGPD E PELOS TRIBUNAIS

4.1 As sanções previstas na LGPD e como são realizadas

A partir das discussões já desenvolvidas ao longo deste texto, percebe-se que a Lei Geral de Proteção de Dados conta com vários fundamentos (Art. 2º) e princípios (Art. 6º) para as atividades de tratamento de dados pessoais, dentre eles, os fundamentos mais pertinentes ao estudo do presente trabalho são: o respeito à privacidade, a autodeterminação informativa, a inviolabilidade da intimidade, da honra e da imagem. No artigo 6º da LGPD estão elencados os princípios, que deverão ser observados de acordo com a boa-fé, quais sejam: o princípio da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas. Caso estes princípios e fundamentos não sejam seguidos, o controlador ou operador de dados incorre em violação aos direitos dos seus usuários e deve ser responsabilizado.

A LGPD prevê, na Seção III do seu texto, a responsabilidade e o ressarcimento de danos, quando o controlador dos dados pessoais causar dano patrimonial em decorrência de violação à lei, sendo que seu artigo 42 estabelece:

O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo (BRASIL, 2019).

Na lei em estudo, há somente três hipóteses que eximem os agentes de tratamento de dados da sua responsabilidade, a saber: (i) quando não realizaram o tratamento de dados pessoais que lhes é atribuído; (ii) quando, embora, tenham realizado o tratamento de dados que lhe são atribuídos, não houve violação à legislação de proteção de dados; ou (iii) quando o dano é decorrente de culpa exclusiva do titular ou de terceiro (BRASIL, 2019). Em outras palavras, quando controladores de dados pessoais não observarem o que está disposto nesta lei e causarem dano ao titular, deverão ser responsabilizados e, caso a responsabilidade

não seja ressarcida espontaneamente, deverá ser iniciada uma demanda judicial, que será objeto do estudo mais a frente deste capítulo.

Além da responsabilidade e ressarcimento de danos, que deverá ser feita ao titular dos dados pessoais em caso de violação da legislação de proteção de dados, os agentes de tratamento de dados ficam sujeitos, também, às sanções administrativas elencadas nos incisos do art. 52 aplicáveis pela Autoridade Nacional de Proteção de Dados. Estas sanções somente serão aplicadas após um procedimento administrativo que, evidentemente, assegure a ampla defesa. Antes de iniciar o estudo das sanções em si previstas na Lei, é preciso explanar sobre a Autoridade Nacional de Proteção de Dados que irá aplicar as sanções, e que, também, é responsável pela aplicação prática da LGPD.

Vale mencionar que, no momento de sua promulgação, em 2018, a LGPD sofreu vários vetos do então presidente, Michel Temer, especialmente no tocante aos artigos que criavam e organizavam a Autoridade Nacional de Proteção de Dados (ANPD) e também o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. Com isto, foi editada a medida provisória 869/2018, que destaca a efetiva criação da Autoridade Nacional de Proteção de Dados, como órgão de natureza jurídica transitória ligado à Presidência da República. A MP 869/2018 foi aprovada pelo Senado Federal em maio de 2019 e, após algumas reestruturações, foi convertida na Lei 13.853/2019, que mantém a atual redação da LGPD. Com essas alterações, criou-se, então, a ANPD.

Dessarte, a Autoridade Nacional de Proteção de Dados foi criada como um órgão da administração pública federal integrante da Presidência da República, que possui as seguintes características:

§ 1º A natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República. § 2º A avaliação quanto à transformação de que dispõe o § 1º deste artigo deverá ocorrer em até 2 (dois) anos da data da entrada em vigor da estrutura regimental da ANPD. (BRASIL, 2019). ´

Além disso, a ANPD possui autonomia técnica e decisória, por força do art. 55-B, é responsável por cuidar da proteção dos dados pessoais, por orientar,

regulamentar e fiscalizar o cumprimento da legislação. Trata-se, portanto, do órgão central interpretativo da LGPD e de estabelecimento de normas e diretrizes para sua implementação. Criada em 2020, até o momento, suas maiores ações, foram em relação a sua estruturação de funcionamento, com a aprovação do Decreto nº 10.474/2020, que aprovou sua estrutura regimental e de cargos e a apresentação do primeiro planejamento estratégico, para os anos de 2021 a 2023.

Neste planejamento estratégico, a ANPD lista três objetivos para serem alcançados até 2023, são eles: “Promover o fortalecimento da cultura de proteção de dados pessoais”, “Estabelecer ambiente normativo eficaz para a proteção de dados pessoais” e “Aprimorar as condições para o cumprimento das competências legais”. Tem-se abaixo as tabelas divulgadas pela ANPD, em seu planejamento estratégico, das ações estratégicas vinculadas a cada objetivo estabelecido:

Figura 1 - Ações estratégicas vinculadas ao objetivo estratégico 1

Ação	Responsável	Horizonte temporal
Detectar infrações à LGPD	Coordenação-Geral de Fiscalização	Médio prazo – até 2 anos
Promover eventos de capacitação e oficinas sobre temas de Proteção de Dados Pessoais	Coordenação-Geral de Relações Institucionais	Curto prazo – até 12 meses
Promover o diálogo com entidades governamentais e não-governamentais, incluindo organismos internacionais e outras autoridades de Proteção de Dados Pessoais	Coordenação-Geral de Relações Institucionais	Curto prazo – até 12 meses
Elaborar guias e recomendações sobre Proteção de Dados	Coordenação-Geral de Normatização Coordenação-Geral de Pesquisa e Tecnologia	Médio prazo – até 2 anos

Fonte: Planejamento Estratégico da ANPD 2021-2023, 2021.

Ações estratégicas relacionadas ao objetivo “Promover o fortalecimento da cultura de proteção de dados pessoais”.

Figura 2 - Ações estratégicas vinculadas ao objetivo estratégico 2

Ação	Responsável	Horizonte temporal
Implementar um fluxo para o sistema de incidentes e reclamações	Coordenação-Geral de Normatização	Curto prazo – até 6 meses
Elaborar agenda regulatória bianual	Coordenação-Geral de Normatização	Curto prazo – até 6 meses
Regulamentar temas da agenda regulatória	Coordenação-Geral de Normatização	Curto prazo – até 2 anos

Fonte: Planejamento Estratégico da ANPD 2021-2023, 2021.

Ações estratégicas relacionadas ao objetivo “Estabelecer ambiente normativo eficaz para a proteção de dados pessoais”.

Figura 3 - Ações estratégicas vinculadas ao objetivo estratégico 3

Ação	Responsável	Horizonte temporal
Estabelecer a estrutura definitiva da ANPD	Coordenação-Geral de Administração	Médio prazo – até 5 anos
Apresentar estudos sobre a transformação da natureza jurídica da ANPD, nos termos da LGPD	Secretaria-Geral	Médio prazo – até 2 anos
Obter orçamento e promover a sua execução orçamentária anual	Coordenação-Geral de Administração	Curto prazo – até 12 meses
Ampliar o corpo de servidores públicos da ANPD	Secretaria-Geral e Coordenação-Geral de Administração	Médio prazo – 2 anos

Fonte: Planejamento Estratégico da ANPD 2021-2023, 2021.

Ações estratégicas relacionadas ao objetivo “Aprimorar as condições para o cumprimento das competências legais”.

Apesar de estar toda estruturada, com objetivos e plano de ações bem delimitados, a ANPD somente atuará como órgão fiscalizador e penalizador a partir de agosto de 2021, em decorrência da *vacatio legis* da LGPD. Dessa forma, este órgão ainda não atua na prática como um órgão fiscalizador da LGPD, atuando até agosto somente como um órgão consultivo, informativo e regulamentador. O órgão será também um canal entre a comunidade e a administração pública, em que a sociedade poderá enviar as suas perguntas, sugestões e denúncias.

Além da ANPD, há também o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, que já está em vigor, e se trata de um órgão consultivo da ANPD, considerado, segundo a lei, prestador de serviço público relevante não remunerado. Diferentemente da ANPD, sua composição é feita por pessoas do Governo, Administração Pública e também da sociedade civil e de instituições e entidades relacionadas à tecnologia e ciência.

Sendo assim, somente a partir de agosto de 2021 a ANPD aplicará sanções a quem violar a legislação. As penalidades previstas na LGPD estão dispostas nos incisos do seu art. 52 e variam de acordo com o caso, dependendo da gravidade e natureza das infrações e dos direitos pessoais afetados, a boa-fé do infrator, a

condição econômica, a cooperação e a reincidência do infrator, o grau do dano e os demais incisos do §1º do art. 52. As sanções serão aplicadas apenas após processo administrativo, que fará a análise da ocorrência.

Vale mencionar que as sanções aplicadas são: advertência, com indicação de prazo para adoção de medidas corretivas; multa simples de 2% do valor do faturamento da empresa no último exercício, limitada ao valor de R\$ 50.000,00 (cinquenta mil reais); multa diária, com o limite igual da multa simples; bloqueio ou exclusão dos dados envolvidos na ocorrência; suspensão ou proibição do acesso ao tratamento de dados pessoais; e, finalmente, a publicação da infração devidamente apurada (BRASIL, 2018).

Tais sanções serão aplicadas pela ANPD e não substituem a aplicação de sanções administrativas, cíveis, penais ou em legislação específica. Essas sanções deverão ser aplicadas em *ultima ratio*, uma vez que o escopo da LGPD, e, por conseguinte de seus órgãos, é a regulamentação e instrução da sociedade e dos agentes de tratamento de dados.

Sendo assim, vê-se que a LGPD disciplinou, de forma consistente e assertiva, a prática do tratamento de dados, com diretrizes e sanções específicas no caso de violação. No entanto, não regulamentou o tratamento de dados com a finalidade de obtenção de vantagem econômica, que são os *cookies*, conforme disposto no §3º do Art. 11, o que poderá ser objeto de proibição ou regulamentação pela ANPD.

Com isso, uma vez que este órgão ainda não está em pleno vigor, não há como realizar uma análise completa da eficácia da referida lei, mas a expectativa é que, a partir de agosto de 2021, sua eficácia seja de grande cumprimento, já que está bem regulamentada e com órgãos estruturados, além do grande tempo de *vacatio legis* (de dois anos) para que as empresas possam se adequar às novas normas.

Feita a análise das previsões sobre aplicação da lei de proteção de dados, passa-se, assim, ao estudo de como o poder judiciário brasileiro está tratando o tema.

4.2 Como a violação aos direitos de privacidade estão sendo julgados pelos tribunais brasileiros.

O fito do presente tópico é pesquisar como a legislação brasileira está sendo aplicada na prática, no que tange os *cookies* e ao direito à privacidade. Feito a análise da legislação, é importante analisar como o poder judiciário está tratando o respectivo tema.

Inicialmente, é preciso recapitular que a LGPD é a lei específica que regulamenta o tratamento de dados digitais no Brasil, mesmo que o ordenamento jurídico brasileiro já conte com vários dispositivos esparsos que tratam do tema, como visto no capítulo 2 deste trabalho. Neste sentido, reforça-se que a LGPD foi sancionada em agosto de 2018 e, com as alterações da Lei 13.853/2019, entrará plenamente em vigor em 1º agosto de 2021. Em outras palavras, até a finalização do presente trabalho de conclusão de curso, a lei não está em plena vigência.

Dito isso, foi iniciada a análise da jurisprudência nos tribunais brasileiros através dos sites dos tribunais estaduais e federais, dos sites especializados em consultas jurisprudenciais, repositórios de jurisprudência de importantes tribunais brasileiros – a saber, Superior Tribunal de Justiça, Tribunal de Justiça do Estado de Minas Gerais, Tribunal de Justiça do Estado de São Paulo, Tribunal Regional do Trabalho da 3ª Região -, além dos sites do Portal da Privacidade e da Associação Nacional dos Profissionais de Privacidade de Dados¹. Neste último, há uma aba em

¹A seguir, listamos os sites efetivamente consultados como base de dados para a pesquisa em estudo:

- ANPPD. Portal das Violações – LGPD. Disponível em: <<https://anppd.org/violacoes>>. Acesso em 15 de mai. de 2021;
- PP. Portal da Privacidade. Disponível em <<https://www.portaldaprivacidade.com.br/category/jurisprudencia/>> Acesso em 15 de mai. de 2021.
- STJ. Superior Tribunal de Justiça. Disponível em <<https://www.stj.jus.br/sites/portalp/Leis-e-normas/lei-geral-de-protecao-de-dados-pessoais-lgpd>> Acesso em 15 de mai. de 2021.
- TRT. Tribunal Regional do Trabalho, 3ª Região – MG. Disponível em <<https://portal.trt3.jus.br/internet>>. Acesso em 15 de mai. de 2021.
- TJMG. Tribunal de Justiça de Minas Gerais. Disponível em <<https://www5.tjmg.jus.br/jurisprudencia/pesquisaPalavrasEspelhoAcordao.do?palavras=Lei+13.709&totalLinhas=1&pesquisarPor=ementa&pesquisaTesauro=true&orderByData=1&pesquisaPalavras=Pesquisar>> Acesso em 15 de Mai. de 2021.
- TJSP. Tribunal de Justiça de São Paulo. Disponível em <<https://esaj.tjsp.jus.br/cjsg/consultaCompleta.do>> Acesso em 15 de mai. de 2021.
- JUSBRASIL. Lei nº 13.709/16. Disponível em <<https://www.jusbrasil.com.br/jurisprudencia/busca?q=lei+13.709>>. Acesso em 15 de mai. de 2021

que contém todas as decisões do judiciário pertinente as violações da LGPD e, consequentemente, ao direito de privacidade.

No entanto, foi constatado que não há, até o presente momento, decisões colegiadas sobre o assunto em segunda instância, somente decisões de primeira instância, que ainda não transitaram em julgado, ou decisões monocráticas e interlocutórias. Isso se deve pela novidade do tema, cuja lei até mesmo não está ainda em pleno vigor.

Analizando as decisões disponíveis no site da Associação Nacional dos Profissionais de Privacidade de Dados, onde há todas as decisões judiciais relacionadas à LGPD², vê-se que há até mesmo uma decisão neste sentido, onde o magistrado decidiu indeferir o pedido de tutela provisória de urgência, pois há investigações e apurações em andamento. A referida decisão trata-se de uma Ação Civil Pública, ajuizada pelo Instituto Brasileiro de Defesa da Proteção de Dados Pessoais, *Compliance* e Segurança da Informação Sigilo, em face da Serasa S.A e da União Federal, com pedido liminar para que a ré Serasa comunique todos os titulares que tiveram os dados expostos sobre o incidente ocorrido e que realizasse em suas redes sociais quais os planos para solucionar os eventuais riscos que o vazamento de dados pudesse trazer, além de que a União Federal realizasse auditoria sobre o vazamento. Na decisão o magistrado indefere sob o fundamento que:

Contudo, os fatos narrados pela autora ainda estão sob investigação criminal pela Polícia Federal e sob apuração administrativa pela Autoridade Nacional de Proteção de Dados, de modo a se apurar os controladores responsáveis pelos vazamentos dos dados e quais os titulares dos dados, cujas conclusões ainda não ocorreram diante da alta complexidade das investigações e apurações. **Assim, somente após as comprovações necessárias será possível determinar o cumprimento do dever legal de comunicação aos titulares acerca do incidente de vazamento de dados.**

Outrossim, o mesmo ocorre com a realização de auditoria pela ANPD, que somente poderá ocorrer após o conhecimento do controlador responsável pelo vazamento dos dados, mediante a instauração de processo administrativo que assegure o contraditório e ampla defesa, nos termos do art. 55, da Lei nº 13709/2018 (GRIFO NOSSO) (TRF3, Decisão – Indeferimento de pedido liminar, Processo nº 5002936-86.2021.4.03.6100)

² ANPPD. Portal das violações – LGPD. Disponível em: <<https://anppd.org/violacoes>> Acesso em: 15 mai. de 2021.

Logo, percebe-se que a decisão em comento corrobora a constatação que a legislação ainda é limitada devido a novidade do tema e pela legislação específica (LGPD) ainda não está em plena vigência, uma vez que a mesma prevê um órgão próprio para fiscalização, apuração e aplicação de sanções em caso de ilícitos em relação aos dados pessoais, mas só realizará estas funções a partir de agosto de 2021. Assim, esta decisão foi correta em indeferir a liminar haja vista que os procedimentos administrativos deverão ocorrer primeiramente.

Por outro lado, pode-se verificar, de acordo com as decisões de primeira instância disponibilizadas no site da ANPPD, as sentenças judiciais, já a partir de 2019, estão sendo fundamentadas pelas LGPD, principalmente para fins de condenações por danos morais por violação do direito de privacidade e obrigação de fazer, ou não fazer, em disponibilizar ou não disponibilizar os dados digitais dos titulares por parte do controlador dos dados. No entanto, em relação aos *cookies* digitais, ainda não foi possível encontrar nenhuma decisão do poder judiciário.

Com isso, foi feita a análise das decisões que possuem como objeto violação à Lei de Proteção de Dados, que estão sendo tomadas em primeira instância, uma vez que, conforme mencionado anteriormente, não há, ainda, jurisprudência de tribunais superiores sobre o assunto. Como já mencionado, a pesquisa foi feita por meio do site da ANPPD, pois este possui todas as decisões que tratam do tema da violação a privacidade de dados. Ressalte-se que, o critério de escolha para análise das decisões foi o temporal, sendo analisadas as decisões tomadas a partir de 2021 até maio do mesmo ano, quando se concluiu este trabalho.

Com base neste critério, constam nove decisões, embora, entre elas não constem nenhuma especificamente sobre a afronta ao direito de privacidade em relação aos *cookies* digitais. Ainda assim, estão surgindo as discussões em relação ao direito de privacidade com base na LGPD e a violação deste direito. O litígio mais comum entre essas decisões é a proteção ao direito de privacidade em relação aos dados pessoais, que são divulgados pelos réus, resguardado pelos incisos I, II, IV e VI do art. 2º da lei em comento, e a inobservância do art. 6 da mesma lei, que trata dos princípios a serem observados pelos controladores dos dados.

Observado o critério posto, veem-se que as decisões que estão sendo tomadas pendem no sentido de proteger o direito de privacidade dos indivíduos, tanto

individual, como coletivamente, de pessoas físicas e também jurídicas. Assim, foi, por exemplo, o entendimento do juiz da 7ª vara cível de São José do Rio Preto, São Paulo, que condenou a ré, SERASA EXPERIAN S.A., em uma ação condenatória em obrigação de fazer combinada com indenização por danos morais, em que o autor demonstra que a ré manteve em seus cadastros e possibilitou a venda a terceiros o acesso de seus números telefônicos, sem prévia comunicação, ferindo gravemente o tratamento adequado dos dados pessoais, conforme a LGPD. Conforme a decisão:

[...] O nome do autor foi incluído no cadastro de inadimplentes, em anotação decorrente de pendência financeira e não voluntariamente, como sustenta a ré. E é bem verdade que o disposto no art. 7º, inciso X, da Lei 13.709/18, a LGPD, permite o tratamento de dados pessoais para proteção ao crédito, de forma involuntária, sem consentimento do interessado. No entanto, tal argumentação não se harmoniza com o propalado consentimento do autor para divulgação de seus telefones.

Ademais, referido permissivo legal não exime a requerida de dar o tratamento adequado aos dados pessoais, em conformidade com a finalidade e o contexto em que utilizados, princípio da LGPD, insculpido no seu art. 6º, inciso II. A divulgação de números de telefones pessoais do consumidor não se mostra adequada, nem necessária, para proteção ou análise de crédito, quando o dado não é voluntariamente disponibilizado. Portanto, tal divulgação vulnerou sim direitos personalíssimos do autor, promovendo acesso indiscriminado, por meio dos números de telefones, que sabidamente é fonte de aborrecimentos e abusos nas relações entre credores e devedores, como meio de cobrança. Desse modo, o autor faz jus à indenização pleiteada, de R\$ 4.000,00, com correção monetária desta data e juros legais da citação. Concluindo, a ação é procedente para que a ré se abstenha, em definitivo, de divulgar números de telefones do autor, bem como para que pague a indenização acima fixada. Posto isso, julgo procedentes os pedidos. (BRASIL. Tribunal de Justiça de São Paulo, 7ª vara cível. **Sentença**. Autor: Sérgio Pereira Martins Junior. Réu: Serasa S/A. Juiz: Luiz Fernando Cardoso Dal Poz. São José do Rio Preto, 15 abr. 2021)

Foi neste sentido também, de proteger os dados individuais da pessoa física, a decisão da Juíza da 9ª vara cível de Brasília:

De fato, a matéria jornalística publicou os dados bancários e expôs cópias dos contracheques dos Embargantes, violando-lhes manifestamente os direitos à privacidade e à proteção de dados pessoais. E isto porque se de um lado a divulgação dos rendimentos dos autores e as informações acerca dos desdobramentos do acordo entabulado na justiça do trabalho são de interesse público e ligados a aspectos profissionais dos autores, de outro os dados bancários e a revelação das cópias dos contracheques são informações excessiva e desnecessária para a matéria.

Com efeito, admitir que tais dados possam ser divulgados seria colocar em risco a privacidade e a segurança pessoal dos Embargantes, o que é terminantemente vedado tanto pela Constituição Federal, em seu art. 5º, X, como pela Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018, art. 2º, I, II e IV).

[...]

Forte em tais razões, JULGO PARCIALMENTE PROCEDENTES os pedidos para, confirmando a tutela antecipada (ID nº 71627664), condenar a primeira

ré a: a) obrigação de remover da notícia divulgada pela primeira ré “trechos que divulgam os dados pessoais confidenciais dos autores, quais sejam, os dados bancários e cópia dos contracheques; b) pagar aos autores danos morais, os quais arbitro em R\$ 10.000,00 para cada autor, acrescido de correção monetária e juros de mora a partir da publicação da presente. (BRASIL. Tribunal de Justiça do Distrito Federal e Territórios, 9º vara cível. Procedimento Comum Cível. **Sentença**, Processo nº 0728278-97.2020.8.07.0001. Autor: Paulo Sergio Pereira, Aldair Roberta de Oliveira e Alair Roberto de Oliveira. Réu: Metrôpoles mídia e comunicação LTDA, Jamal Jorge Bittar, Manoela Simão de Alcantara Araújo. Juíza: Grace Correa Pereira Maia. Brasília, 12 fev. de 2021)

Dessa forma, o que se observa é que as sentenças de primeiro piso estão indo na direção de resguardar o direito de privacidade dos indivíduos que possuem os dados pessoais expostos, com a condenação de indenização por danos morais e obrigação de fazer, quando necessário retirar os dados expostos, ou não fazer quando os controladores dos dados devem abster de fornecer os dados.

Verifica-se, que os direitos de privacidade coletivos também estão sendo objeto de discussão e proteção por parte do judiciário. Foi nesse sentido a sentença proferida pelo Juíza da 37ª vara cível de São Paulo na Ação Civil Pública ingressada pelo Instituto Brasileiro de Defesa do Consumidor em face da Concessionária da Linha 4 do Metrô de São Paulo S/A. A parte autora requereu que a ré cessasse a coleta e tratamento de imagens e dados biométricos sem prévio consentimento dos usuários deste serviço e a indenização de R\$ 100.000.000,00 por danos coletivos. Na decisão a Juíza acolheu parcialmente o pedido da parte autora, determinando que a ré se abstenha de captar qualquer dado pessoal através de câmeras ou outros dispositivos sem prévio conhecimento dos consumidores. Além disso, caso adote novamente, tais práticas deverá obter o consentimento prévio dos usuários e a condenação de indenização por danos morais coletivos em R\$ 100.000,00 revertidos para o Fundo de Defesa de Direitos Difusos. Conforme o julgamento:

Trata-se de ação civil pública proposta pelo Instituto Brasileiro de Defesa do Consumidor (IDEC) e Defensoria Pública em face da empresa Concessionária da Linha 4 do Metrô de São Paulo S.A. (Via Quatro), em que se discute a prática de coleta, utilização e armazenamento de dados pessoais de usuários pela plataforma digital implantada pela empresa ré nas estações da Linha 4 Amarela, sem prévio consentimento dos consumidores, e, consequentemente, a ocorrência de danos morais e danos coletivos. Pretendem os autores a condenação da ré (i) a não utilizar dados biométricos ou qualquer outro tipo de identificação dos consumidores e usuários do transporte público, sem consentimento do usuário; (ii) ao pagamento de indenização pela utilização indevida da imagem dos consumidores e (iii) indenização por danos coletivos em valor não inferior a R\$100.000.000,00. A

ré, por sua vez, defende a legalidade da utilização do equipamento em questão, argumentando que não há coleta ou armazenamento de dados pessoais no sistema, mas tão somente a detecção facial para fins estatísticos, de modo que os dados gerados não identificam especificamente o passageiro. Ocorre, porém, que tal limitação do sistema de apenas se utilizar das imagens dos usuários para fins estatísticos, sem efetiva captação, gravação ou identificação não está demonstrada nos autos, ônus que incumbia à ré, na forma do artigo 373, II do Código de Processo Civil. Diante do fato incontroverso de que havia equipamentos de gravação de imagens dos usuários para fins publicitários e estatísticos nas estações administradas pela ré, cabia a essa na qualidade de concessionária de serviço público, demonstrar cabalmente que o sistema não armazena dados pessoais dos usuários da plataforma, tampouco realiza o reconhecimento facial pelo equipamento instalado, a ausência de gravação ou filmagem dos usuários e a real destinação dada ao material obtido, se o caso, o que não ocorreu.

[...]

Ante o exposto, JULGO PROCEDENTES EM PARTE os pedidos, com resolução do mérito, na forma do artigo 487, I do Código de Processo Civil, para (i) determinar que a requerida se abstenha de captar as imagens, sons e quaisquer outros dados pessoais dos consumidores usuários, através das câmeras ou outros dispositivos envolvendo os equipamentos instalados na Linha 4 Amarela do metrô, sem consentimento prévio do consumidor, confirmando a liminar anteriormente concedida pela decisão de fls. 327/332; (ii) determinar à requerida que, caso deseje readotar as práticas tratadas nos autos, deverá obter o consentimento prévio dos usuários mediante informação clara e específica sobre a captação e tratamento dos dados, com adoção das ferramentas pertinentes; e (iii) condenar a requerida ao pagamento de indenização por danos morais coletivos no valor de R\$100.000,00, corrigida segundo a tabela prática do Egrégio Tribunal de Justiça de São Paulo, desde a data da publicação da sentença, e com juros de mora de 1% ao mês, incidentes a partir da citação, por se tratar de ilícito contratual, na forma do artigo 405, do Código Civil, a ser revertido para o Fundo de Defesa de Direitos Difusos FDD, criado na forma do artigo 13 da Lei nº 7.347/85. (TJSP, Sentença, Processo nº 1090663-42.2018.8.26.0100)

As referidas sentenças demonstram a tendência das decisões que estão sendo empreendidas pelo Judiciário brasileiro no sentido de resguardar não somente o direito de privacidade individuais, mas também coletivos, conforme disciplinado pela Lei 13.709/2018.

Isto posto, o que se conclui é que o tema em questão ainda não possui decisões jurisprudenciais e uniformidade no cenário jurídico brasileiro por se tratar de um assunto muito recente, necessitando de mais tempo para que tal análise seja feita. Todavia, as decisões de primeira instância estão sendo julgadas afim de proteger os direitos resguardados pela Lei Geral de Proteção de Dados, especificamente na proteção do direito de privacidade, a inviolabilidade da intimidade, da honra e da imagem, elencados, respectivamente, nos incisos I e IV do art. 2º da mencionada lei, que são os direitos mais violados em se tratando de violação do direito de privacidade.

Com isso, após a pesquisa, análise e estudo do presente trabalho de curso, constata-se que o direito de privacidade que é violado pelos *cookies* digitais, ainda é precariamente protegido pelas instituições do direito brasileiro, pois a LGPD não regulamenta amplamente os *cookies*, disciplinando que poderão ser objeto de vedação ou regulamentação por parte da ANPD, conforme o §3º do art. 11. No entanto, este tema até o momento não foi pauta de discussão pela ANPD. Além disso, após análise das decisões judiciais disponíveis sobre o tema não há, ainda, nenhuma que trate e condene a prática de mercantilização dos dados pessoais dos usuários dos meios informacionais sem o prévio consentimento.

Dessa maneira, o que acontece, na maioria das vezes, os meios informacionais divulgam a sua política de privacidade, em que dispõem sobre o tratamento de dados e a sua venda e requerem o consentimento dos usuários. Os usuários, por desconhecimento, por ignorância ao tema, por negligência ou até mesmo por não terem outra opção, pois não é exequível ao usuário contestar ou não aceitar trechos das políticas, aceitam tais propostas, tornando-se ciente que seus dados pessoais poderão ser comercializados ou trocados com outros controladores.

Assim, conclui-se que a legislação brasileira possui bons dispositivos legais para resguardar o direito de privacidade no tocante o tratamento de dados conforme a Lei 13.709/2018 e as decisões judiciais também caminham no sentido de proteger tal direito. Isto, representa um grande avanço à proteção do direito de privacidade. Mas ao passo dos *cookies*, a LGPD foi omissa e não há, até o momento, decisões judiciais a proteger o direito de privacidade, especificamente ferido por eles. Diante do exposto, a hipótese inicial do trabalho de que a legislação brasileira é frágil no tocante aos *cookies* e direito de privacidade se confirma. No entanto, não se pode lograr êxito integral com esta confirmação pois a tendência, com a regulamentação da ANPD e sua vigência em agosto de 2021, é que o tratamento de dados através dos *cookies* sejam objeto de vedação ou regulamentação mais específica, ou que tal ação seja reprimida pelo o judiciário brasileiro uma vez que as decisões estão sendo a favor da proteção dos direitos de privacidade.

5 CONSIDERAÇÕES FINAIS

O desenvolvimento do presente estudo possibilitou a análise da legislação brasileira e o reconhecimento da fragilidade prática atual da proteção ao direito de privacidade no tocante aos *cookies* digitais, uma vez que sequer a lei que trata da matéria possui eficácia em sua integralidade. Após esta pesquisa, verificou-se que o ordenamento jurídico brasileiro conta com várias leis que ditam sobre o direito de privacidade no tocante aos dados digitais. Porém, em 2018, foi regulamentada a lei 13.709, que trata especificamente sobre o tratamento dos dados digitais e, até o momento, ainda não está em pleno vigor, o que acontecerá em agosto de 2021, em decorrência do seu período de *vacatio legis* de dois anos.

Assim, a partir do estudo realizado, o que foi constatado é que ordenamento jurídico brasileiro conta com um dispositivo constitucional e muitos dispositivos infraconstitucionais para a proteção do direito de privacidade, como o Código Civil, o Código de Defesa do Consumidor e o Marco Civil da Internet. No entanto, estes dispositivos ainda não foram capazes de disciplinar a privacidade em relação aos dados digitais pessoais e, para isso, foi regulamentada a Lei 13.709/18, conhecida como Lei Geral de Proteção de Dados Pessoais.

Em decorrência do ínfimo tempo de regulamentação da lei especial e, até mesmo, por ainda não estar em plena vigência, a conclusão final do presente estudo restou prejudicada. Para se chegar a uma conclusão mais assertiva da hipótese, é necessário aguardar que a LGPD esteja em pleno vigor e que o seu órgão fiscalizador, a ANPD, esteja funcionando, além de que as decisões judiciais tomem forma e uniformidade.

Com isto, os objetivos foram cumpridos parcialmente, mas a hipótese apresentada não pode ser confirmada totalmente pelos motivos expostos nesta conclusão.

A despeito disso, sustenta-se que as justificativas deste trabalho ainda justificam sua razão de ser, pois, a partir de sua leitura, vê-se que a LGPD é uma legislação inovadora e possui diversos mecanismos e um órgão específico, que trabalhará para a sua aderência, despertando boas expectativas ao resguardo do

direito de privacidade. Ademais, é necessário que seja difundida uma cultura de conscientização e educação na sociedade, podendo ficar a cargo da ANPD, uma vez que ela é o órgão normativo, consultivo e coordenador da LGPD e possui em suas próprias competências, a promoção do conhecimento na população, sobre o tratamento de dados, visto que, a proteção dos dados e, conseqüentemente, o direito de privacidade vai além do consentimento informado pelo usuário.

Por todo o exposto, o tema da presente pesquisa evidentemente não se exaure com este trabalho e ainda está em aberto, em decorrência da novidade do tema, o que gera ainda abertura para outras pesquisas e aguarda-se muito debate sobre o assunto, além da possibilidade de revisitar a questão em estudos acadêmicos futuros e mais aprofundados.

5- REFERÊNCIAS

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 2. ed. Rio de Janeiro: Forense, 2020.

BRASIL. **Constituição da República Federativa de 1988**. Brasília. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm> Acesso em: 09 nov. 2020

BRASIL. **Leis ordinárias de 1990**. Brasília: Casa Civil, Subchefia para Assuntos Jurídicos, 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm> Acesso em: 02 fev. 2021

BRASIL. **Leis ordinárias de 2002**. Brasília: Casa Civil, Subchefia para Assuntos Jurídicos, 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm> Acesso em: 15 dez. 2020

BRASIL. **Leis ordinárias de 2018**. Brasília: Casa Civil, Subchefia para Assuntos Jurídicos, 2018. Disponível em: <<http://www.planalto.gov.br/ccivil03/ato20152018/2018/lei/L13709.htm>> Acesso em: 09 nov. 2020

BRASIL. **Planejamento Estratégico ANPD 2021-2023**. Brasília, 2021. Disponível em: <<https://www.gov.br/anpd/pt-br/documentos-e-imagens/planejamento-estrategico/planejamento-estrategico-2021-2023.pdf>> Acesso em: 10 abr. 2021

BRASIL. Tribunal de Justiça de São Paulo. Procedimento Comum Cível. **Sentença em Ação Condenatória em Obrigação de Fazer combinada com Indenização por Danos Morais**, da 7ª vara cível do Tribunal de Justiça de São Paulo. Autor: Sérgio Pereira Martins Junior. Réu: Serasa S/A. Juiz: Luiz Fernando Cardoso Dal Poz. São José do Rio Preto, 15 abr. 2021. Disponível em: <<https://esaj.tjsp.jus.br/pastadigital/abrirDocumentoEdt.do?nuProcesso=1030767-27.2020.8.26.0576&cdProcesso=G0000GLMP0000&cdForo=576&baseIndice=INDDS&nmAlias=PG5SJRP&tpOrigem=2&fOrigem=P&cdServico=190101&acessibilidade=false&ticket=7%2B1pM0KjkD8ToeFBIZkMBwnusAlbAwRw%2F457agFUiTreBxdKdyk%2FYfy%2FDhiHd%2BmJO9mN6m3p2ktOLGt8Blm7BeOiCmnwD082Bhwt7VI69S2iUEcHmbHPc5dZDXQxN9dhSSa%2FaaSwdKVZgUo3VY5mVJXav8l0xllxnkJKU8XBAhT1vZtkMsMoTCfZC2FQSIsd0raz0XiJ8ObWrkC7Di%2Bz4EL81nfhQe%2FCT7M>>

ZM4YD4xJAiwSG8E4VI2hXBpD4DGoZBRcr3B2VjNyFT8loyDcfiVzfeXyiKktZpGxBKXxfzJHYCKXRsolc6YEYA0VyBsTqorR9Oxt52Xz5Hz3qZOn5%2FgsC%2FPiHOcKnMJLjDFTzcbZxApbm6pIPGdePyqw0d%2Bk0> . Acesso em: 15 mai. 2021

BRASIL. Tribunal de Justiça do Distrito Federal e Territórios, 9º vara cível. Procedimento Comum Cível. **Sentença**, Processo nº 0728278-97.2020.8.07.0001. Autor: Paulo Sergio Pereira, Aldair Roberta de Oliveira e Alair Roberto de Oliveira. Réu: Metrôpoles mídia e comunicação LTDA, Jamal Jorge Bittar, Manoela Simão de Alcantara Araújo. Juíza: Grace Correa Pereira Maia. Brasília, 12 fev. de 2021. Disponível em: <<https://pje.tjdft.jus.br/consultapublica/ConsultaPublica/DetalheProcessoConsultaPublica/documentoSemLoginHTML.seam?ca=1ed4d703e37f8ce7f8ea6c63ca68d4d637d2d1b090f32d4ff3b54d2059529e9596493c07e109bbbef31b3c718181f2d3f4e7e64a2993552e&idProcessoDoc=83017167>>. Acesso em: 15 mai. 2021

BRASIL. Tribunal Regional Federal, Região 3. Ação Civil Pública, Direito Administrativo e outras matérias de Direito Público. **Decisão, Indeferimento da liminar**. Autor: Instituto Brasileiro de Defesa da Proteção de Dados Pessoais, Compliance e Segurança da Informação Sigilo. Réu: Serasa S.A., AGU União Federal e União Federal. Juiz: José Henrique Prescendo. São Paulo, 16 de mar.de 2021. Disponível em: <<https://pje1g.trf3.jus.br/pje/ConsultaPublica/DetalheProcessoConsultaPublica/documentoSemLoginHTML.seam?ca=de1048a39c322356a960112c891e894d4c03e1131bd9e5db75d69a1f45734335672ce3b1cecd428c273b4081b6df67d4c95d33de5d8beb2&idProcessoDoc=47303791>> Acesso em: 15 mai. 2021.

CASTRO, Luiz Felipe. **Maior vazamento de dados pessoais do país expõe riscos da era digital**. VEJA, 17 fev. 2021. Disponível em: <<https://veja.abril.com.br/tecnologia/maior-vazamento-de-dados-pessoais-do-pais-expoe-riscos-da-era-digital/>> Acesso em: 24 fev. 2021.

DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**. Rio de Janeiro: Renovar, 2006.

FARIAS, Cristiano Chaves; ROSENVALD, Nelson. **Direito civil. Teoria Geral**. 4. ed. Rio de Janeiro: Lumen Juris, 2006.

JANKAVSKI, André. **Vazamento de dados: empresas não se protegem porque não querem, diz CEO da PSafe**. CNN Brasil Business, São Paulo, 13 mar. 2021. Disponível em; <<https://www.cnnbrasil.com.br/business/2021/03/13/vazamento-de-dados-empresas-nao-se-protegem-porque-nao-querem-diz-ceo-da-psafe>> Acesso em: 15 mar. 2021.

LIMA, Cíntia Rosa Pereira de (Org.). **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2020.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: Linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. Série IDP: linha pesquisa acadêmica.

MENDROT, Jeferson Bruno. **As Liberdades de Isaiah Berlin**. 2016. Disponível em < <https://brunomendrot.jusbrasil.com.br/artigos/372589171/as-liberdades-de-isaiah-berlin>> Acesso em: 13 abr. 2021.

MICHAELIS, dicionário. Disponível em: <www.michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/dado/>. Acesso em 9 nov. 2020

MORAES, Alexandre de. **Direito Constitucional**. 13. ed. São Paulo: Atlas, 2003. Disponível em: < https://jornalistaslivres.org/wp-content/uploads/2017/02/DIREITO_CONSTITUCIONAL-1.pdf > Acesso em: 12 abr. 2021.

NETO, Mário Furlaneto; CARMO, Júlio César Lourenço do; SCARMANHÃ, Bruna de Oliveira da Silva Guesso. **Cookies: Vulnerabilidade do direito à privacidade nos meios digitais no âmbito da legislação brasileira**. Revista Jurídica Luso Brasileira, Vol. 4, 2018, nº 4. Disponível em: <https://www.cidp.pt/revistas/rjlb/2018/4/2018_04_1491_1517.pdf> Acesso em: 11 nov. 2020

PORTAL DAS VIOLAÇÕES - LGPD. Associação Nacional dos Profissionais de Privacidade de Dados. Disponível em: <<https://anppd.org/violacoes>> Acesso em: 9 abr. 2021.

REINALDO FILHO, Demócrito (coord.). **Direito da Informática – temas polêmicos**. 1ª Ed. Bauru, SP: Edipro, 2002.

SANTOS, Leon. Revolução 4.0: Quarta Revolução Industrial já está em vigor e deve mudar a realidade que conhecemos. **Revista Brasileira de Administração**, nº 132, p. 24-27, set./out. 2019.

SOARES, Marcos Antônio Striquer; BRENE, Tiago. **Análise dos Objetivos Fundamentais da República Federativa do Brasil à Luz dos Estudos de Isaiah Berlin**. 2014. Disponível em: < <http://direitoestadosociedade.jur.puc-rio.br/media/45artigo7.pdf>> Acesso em 12 abr. 2021.

T1E2 - Fundamentos de TI - Diferença entre Dados e Informação. 2019. Disponível em: <<https://www.youtube.com/watch?v=JluwPr6iPmg&feature=youtu.be>> Acesso em: 08 nov. 2020.