Centro Universitário de Brasília - UniCEUB

Faculdade de Ciências Jurídicas e Sociais - FAJS
Curso de Bacharelado em Direito

KALLENY DOS SANTOS TAVARES

A RESPONSABILIDADE DOS PROVEDORES NA UTILIZAÇÃO DOS DADOS PESSOAIS PARA FINS DE MARKETING

BRASÍLIA
2021

KALLENY DOS SANTOS TAVARES

A RESPONSABILIDADE DOS PROVEDORES NA UTILIZAÇÃO DOS DADOS PESSOAIS PARA FINS DE MARKETING

Artigo científico apresentado como requisito parcial para obtenção do título de Bacharel em Direito pela Faculdade de Ciências Jurídicas e Sociais - FAJS do Centro Universitário de Brasília (UniCEUB).

Orientador: Professor Paulo Rená da Silva Santarém

BRASÍLIA
2021

KALLENY DOS SANTOS TAVARES

A RESPONSABILIDADE DOS PROVEDORES NA UTILIZAÇÃO DOS DADOS PESSOAIS PARA FINS DE MARKETING

Artigo científico apresentado como requisito parcial para obtenção do título de Bacharel em Direito pela Faculdade de Ciências Jurídicas e Sociais - FAJS do Centro Universitário de Brasília (UniCEUB).

Orientador: Professor Paulo Rená da Silva Santarém

Brasília, 12 ABRIL 2021

BANCA AVALIADORA

_____

Professor(a) Orientador(a)

_____

Professor(a) Avaliador(a)

A RESPONSABILIDADE DOS PROVEDORES NA UTILIZAÇÃO DOS DADOS PESSOAIS PARA FINS DE MARKETING

Kalleny dos Santos Tavares

Resumo: O presente trabalho analisa a controvérsia sobre a utilização dos dados pessoais pelos provedores para fins de *marketing* digital. Analisa as possíveis problemáticas da padronização de consumo do usuário e o direcionamento de anúncios. Foca na proteção de dados e no direito à privacidade, à luz da doutrina e da legislação brasileira. O escopo dessa investigação é levantar informações mais precisas sobre o uso dos dados pessoais fornecidos pelos navegantes de rede e quais questões estão sendo levantadas atualmente, além do porquê da utilização indevida não poder ser abordada de maneira despretensiosa. Assim, constata-se que a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.579) prioriza a forma com que os dados pessoais estão sendo utilizados e estabelece contornos jurídicos implícitos que permitem a sua proteção.

Palavras-chave: responsabilidade civil; lei de proteção de dados; *marketing* digital; dados pessoais; marco civil da internet; provedores de aplicação; perfilização; publicidade direcionada; algoritmos.

Sumário:

1 – Introdução. 2 – As modalidades de provedores de Internet. 3 – A proteção de dados pessoais. 4 – O *marketing* na era digital. 4.1 – Os algoritmos. 4.2 – A publicidade direcionada e a perfilização. 4.3 – O App Tracking Transparency (ATT). 5 – A responsabilidade dos provedores no Brasil. 6 – Casos práticos do uso de dados pessoais para fins de *marketing* digital. 6.1 – O caso Target. 6.2 – O caso da Cambridge Analytica x Facebook. 7 – Considerações finais.

1. INTRODUÇÃO

Durante as últimas décadas houve a popularização da internet e do uso das redes sociais. Esse avanço tecnológico possibilitou que milhões de pessoas ao redor do mundo, em instantes, pudessem compartilhar informações, baixar aplicativos, enviar e-mails e postar fotos do seu dia a dia em redes sociais.

De acordo com o Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (CETIC), em 2019, o Brasil contava com 134 milhões de usuários do Internet. O dado representa cerca de 74% da população com 10 anos ou mais e demonstra aumento

significativo do uso de internet pela população brasileira em comparação aos anos anteriores (CETIC, 2020).

O universo digital tornou-se uma das principais plataformas para anúncio e venda de produtos. O acesso instantâneo possibilitou o engajamento e a customização entre o consumidor e as empresas.

Nesse contexto, diversas empresas coletam dados pessoais disponíveis na internet e os utilizam para direcionar anúncios publicitários. A problemática se agrava porque muitos usuários não têm conhecimento do quanto os seus dados pessoais estão vulneráveis no ambiente cibernético.

De acordo com Kotler (2017, np) vivemos um mundo totalmente novo e a "internet que trouxe conectividade e transparência às nossas vidas, tem sido em grande parte responsável por essas transformações". Acerca disso Kotler (2017, np) ainda complementa que:

> A conectividade nos fez questionar muitas teorias dominantes e grandes pressupostos que havíamos aprendido sobre consumidor, produto e gestão da marca. Ela diminui de forma significativa os custos de interação entre empresas, funcionários, parceiros de canal, clientes e outras partes envolvidas. Isso, por sua vez, reduz as barreiras de entrada em novos mercados, permite o desenvolvimento simultâneo de produtos e abrevia o tempo necessário para a construção da marca.

O Marco Civil da Internet (Lei Federal nº 12.965/2014) estabelece princípios, garantias e disciplina no uso da internet no Brasil. Desta maneira, essa legislação tentou trazer respostas mais claras acerca das inseguranças do usuário na era digital. Mesmo assim, ainda se faz necessário uma norma que traga, de forma mais específica, os limites do uso de dados pessoais em decorrência do desenvolvimento do modelo de negócios da economia digital.

Na Europa, a principal legislação de proteção de dados é a *General Data Protection Regulation*. O normativo foi um instrumento essencial para harmonização da proteção de dados nos países membros da União Europeia, e serviu de inspiração para a Lei de Proteção de Dados (Lei nº 13.709/18) brasileira (TALIBERTI *et al*, 2018, np). Desse universo dos dados pessoais, a proteção em relação ao ambiente *online* será o objeto desta pesquisa.

Toda interação realizada por um usuário na internet fica registrada. A maioria da população sequer chega a ler os termos e condições do uso e, cada vez mais, utilizam-se novos dispositivos que captam informações e tratam os dados com finalidade genérica ou indeterminada. Deste modo, é necessário analisar como os provedores de serviços de internet

captam e usam esses dados pessoais para fins de marketing e quais as consequências jurídicas dessas ações.

2. AS MODALIDADES DE PROVEDORES DE INTERNET

Segundo Marcel Leonardi (2005, p. 21), o provedor de serviços de internet "é a pessoa natural ou jurídica que fornece serviços relacionados ao funcionamento da Internet, ou por meio dela". O provedor de serviços de internet é um gênero do qual decorrem várias categorias, sendo algumas destas: provedor de *backbone*; provedor de acesso; provedor de correio eletrónico; provedor de hospedagem; e provedor de conteúdo.

Inicialmente, há a espécie de provedores de *backbone* que "são estruturas de rede capazes de manipular grandes volumes de informações, constituídas basicamente por roteadores de tráfego interligados por circuitos de alta velocidade". São pessoas jurídicas que disponibilizam estruturas aos provedores de acesso e hospedagem de forma onerosa e fundamental para o funcionamento da internet (LEONARDI, 2005, p. 21-22).

Em seguida o doutrinador apresenta mais uma espécie, os provedores de acesso, o qual conceitua como "a pessoa jurídica fornecedora de serviços que possibilitem o acesso de seus consumidores à Internet". Mais especificamente, aqueles que se conectam a um provedor *backbone* e revendem essa conectividade a outros indivíduos ou provedores LEONARDI, 2005, p. 23).

Esses provedores são aqueles "conectados às espinhas dorsais, estarão os provedores de acesso ou de informações, que são os efetivos prestadores de serviços aos usuários finais da Internet, que os acessam tipicamente através do serviço telefônico" (LEONARDI, 2005, p. 23). Alguns exemplos de provedores de acesso são: Net Virtua, GVT, Brasil Telecom, Tim, Claro, dentre outras.

Ademais, para ser um provedor de acesso basta apenas que possibilite a conexão à internet a seus usuários. Em outras palavras, não é necessário que forneça serviços acessórios, mesmo que sejam fornecidos pela mesma pessoa jurídica (LEONARDI, 2005, p. 24).

Desta maneira, na concepção do doutrinador, boa parte dos provedores de acesso à internet também funcionam como provedores de serviços ao oferecer um maior conjunto de funcionalidades e, por esse motivo, a separação entre ambos tende a diminuir. Apesar disso, a

diferença conceitual é de extrema importância para compreensão da responsabilidade de tais empresas em relação a sua atividade exercida.

Em seguida, há a categoria dos provedores de correio eletrônico que fornecem ao usuário nome e senha para o uso de um sistema que permite o envio e recebimento de mensagens. Destaca-se que é necessário o acesso prévio à internet (LEONARDI, 2005, p. 24).

Outra categoria são os provedores de hospedagem que promovem o "armazenamento de dados em servidores próprios de acesso remoto, possibilitando o acesso de terceiros a esses dados, de acordo com as condições estabelecidas com o contratante do serviço". Assim, há dois serviços que podem ser prestados por esses provedores (i) o armazenamento de arquivos em um servidor; e (ii) a possibilidade de acesso a tais arquivos conforme as condições previamente estabelecidas com o provedor de conteúdo (LEONARDI, 2005, p. 25).

Destaca-se que, segundo o doutrinador, esses provedores são essenciais para o funcionamento da *world wide web* e inerentes à existência dos provedores de conteúdo, pois utilizam esses serviços para veicular informações na rede. Nesse ponto, cumpre destacar que o controle do conteúdo armazenado em seus servidores é controlado, em regra, pelos provedores de conteúdo (LEONARDI, 2005, p. 26). Alguns exemplos de provedores de hospedagem são: Google Search, Bing, Yahoo! Search, dentre outros.

Por fim, Leonardi (2005, p. 27) apresenta a categoria dos provedores de conteúdo que é "toda pessoa natural ou jurídica que disponibiliza na internet as informações criadas ou desenvolvidas pelos provedores de informação, utilizando para armazená-las servidores próprios ou os serviços de um provedor de hospedagem".

Devido a crescente demanda de lides envolvendo provedores de serviços de internet e a ausência de legislação específica sobre a matéria, o judiciário aplicou essa diferenciação para fins de responsabilidade civil.

A Ministra Nancy Andrighi do Superior Tribunal de Justiça proferiu o voto no julgamento do Recurso Especial nº 1.316.921/RJ no qual se discutia a possibilidade da Google remover da sua ferramenta de pesquisa resultados referente a determinada expressão (BRASIL, 2012). Assim, reconheceu a distinção dos tipos de provedores de serviços de internet proposta por Marcel Leonardi, *in verbis*:

> "Os provedores de serviços de Internet são aqueles que fornecem serviços ligados ao funcionamento dessa rede mundial de computadores, ou por meio dela. Trata-se de gênero do qual são espécies as demais categorias, como: (i) provedores de backbone (espinha dorsal), que detêm estrutura de rede capaz

> de processar grandes volumes de informação. São os responsáveis pela conectividade da Internet, oferecendo sua infraestrutura a terceiros, que repassam aos usuários finais acesso à rede; (ii) provedores de acesso, que adquirem a infraestrutura dos provedores backbone e revendem aos usuários finais, possibilitando a estes conexão com a Internet; (iii) provedores de hospedagem, que armazenam dados de terceiros, conferindo-lhes acesso remoto; (iv) provedores de informação, que produzem as informações divulgadas na Internet; e (v) provedores de conteúdo, que disponibilizam na rede os dados criados ou desenvolvidos pelos provedores de informação ou pelos próprios usuários da web" (BRASIL, 2012).

Nesse mesmo julgado, a Ministra ainda pontuou que frequentemente os provedores oferecem mais de uma modalidade de serviço de internet, todavia a diferença conceitual é de suma importância para a imputação da responsabilidade inerente a cada serviço prestado.

O mesmo entendimento foi replicado pela Ministra no REsp 1.381.610/RS no qual se discutia se quem mantém e edita blog é responsável pelo conteúdo das informações nele veiculadas e, caso seja, a razoabilidade do *quantum* indenizatório (BRASIL, 2013).

Em 23 de abril de 2014, o Marco Civil da Internet (Lei nº 12.965/14) foi sancionado e foi a primeira lei brasileira que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Segundo Pacheco (2015, p. 17):

> "[...] o denominado Marco Civil da Internet (Lei 12.965/2014), ao pretender estabelecer princípios, garantias, direitos e deveres vinculados à manifestação do pensamento, à criação, à expressão e à informação (meio ambiente cultural), por meio do uso da internet no Brasil (meio ambiente digital), procura de qualquer forma tentar organizar parâmetros jurídicos específicos no âmbito infraconstitucional destinados a tutelar o conteúdo da comunicação social e mesmo dos direitos e deveres fundamentais da pessoa humana por meio do uso de computadores no Brasil em redes interligadas visando, ao que tudo indica, destacar a importância da tutela jurídica da internet no século XXI em nosso País".

A lei federal, para diferenciar os tipos de provedores quanto à responsabilidade civil e os limites técnicos de cada um, adotou apenas dois conceitos: os provedores de conexão e os provedores de aplicações (BRASIL, 2014). De acordo com Serro (2015, p. 5), os provedores de conexão são:

> "[...] os responsáveis pela intermediação entre a operadora e o usuário do serviço contratado. Nesta modalidade de provedor, é oferecida a conexão à Internet conforme especificidades e velocidades contratadas e o acesso pode ser feito através de uma identificação de usuário e senha, por exemplo. Os

> provedores de conexão são os responsáveis por alcançar ao usuário diretamente o acesso à rede".

Já os provedores de aplicações da internet são o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet[1] e que esses provedores devem manter os registros de acesso a aplicações de internet pelo prazo de seis meses[2] (BRASIL, 2014). No Brasil, alguns exemplos dessa espécie são: Blogger (Google), Facebook, Youtube (Google) e Twitter.

De acordo com Paesani (2000, p. 74), citado por Serro (2015, p. 9), os provedores possuem diferentes tipos de responsabilidade civil de acordo com a prestação de seus serviços. Desta forma, a positivação entre a diferenciação dos tipos de provedores acarreta em uma melhor adaptação das lides levadas ao judiciário.

3. A PROTEÇÃO DE DADOS PESSOAIS

De acordo com Doneda (2021, p. 22-26), a disciplina jurídica da proteção de dados pessoais vem sendo construída há cinco décadas e os debates ocorridos em 1960 foram extremamente fundamentais para moldar essa disciplina. O primeiro normativo sobre essa matéria foi a *Lei de Proteção de Dados do Land* alemão de Hesse, escrito em 1970, que operou "uma mudança de perspectiva que trouxe consigo o desenvolvimento de um modelo normativo autônomo, o da proteção de dados pessoais". Posteriormente outras legislações nacionais surgiram na Europa.

Os marcos regulatórios europeus e seu desenvolvimento estão fortemente ligados à forma em que é dada a proteção aos dados pessoais atualmente, em outras palavras, a base dos institutos jurídicos dessa disciplina são o produto da influência mútua entre sistemas jurídicos, principalmente da Europa e também dos Estados Unidos (DONEDA, 2021, p. 23).

Essa influência ocorre por alguns fatores, sendo o principal deles o desenvolvimento econômico e tecnológico pioneiro nessas regiões, permitindo com que a problemática

---

[1] BRASIL, Lei nº 12.965/14, art. 5º: "VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; e".

[2] BRASIL, Lei nº 12.965/14, art. 15: "O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento".

envolvendo à privacidade e os dados pessoais fossem debatidas primeiramente (DONEDA, 2021, p. 23).

Um grande marco para a proteção de dados pessoais, ocorreu em 1983 no paradigmático julgamento *Volkszählungsurteil (BVerfGE 65, 1)* pelo Tribunal Constitucional Alemão (*Bundesverfassungsgericht*) que julgou insconstitucional a Lei do Censo alemã (*Volkszählunsgesetz*) e, por consequência, redefiniu os contornos do direito a proteção de dados pessoais (BRASIL, 2020).

A lei em comento permitia que o Estado alemão cruzasse informações a partir de dados coletados para mensurar estatisticamente a distribuição espacial e geográfica da população com registros públicos para a finalidade genérica para execução de atividades administrativas (BIONI, 2019, p 96).

Segundo Bioni (2019, p. 96) acerca do julgamento em comento:

> "Tal vagueza e amplitude da lei de recenseamento foi o estopim para uma série de reclamações perante o Tribunal Constitucional alemão, que declarou a sua inconstitucionalidade parcial. A Corte alemã considerou que eventual compartilhamento dos dados coletados deveria se destinar única e exclusivamente para a finalidade de recenseamento (estatística)".

Ainda segundo esse autor, o julgamento *Volkszählungsurteil* teve extrema relevância ao definir a proteção de dados pessoais como direito de personalidade autônomo destacado do direito à privacidade. Mais ainda, o *decisum* estabelece a importância do cidadão ter controle de seus dados pessoais.

O julgado ainda é utilizado para embasar fundamentos de controvérsias atuais envolvendo a proteção de dados pessoais. Como no voto do Ministro Gilmar Mendes no pedido de liminar em ação direta de inconstitucionalidade nº 6.389. O pedido tratava do caso de compartilhamento de dados por empresas de telecomunicações prestadoras de serviços telefônicos fixo e móvel com a Fundação Instituto Brasileiro de Geografia e Estatísticas para fins de suporte na situação de emergência em decorrência do coronavírus (COVID-19). No voto o Ministro pontua:

> "A partir da leitura ampliativa do artigo 2.1, em conjunto com o artigo 1.1. da Grundgesetz, o Tribunal Constitucional reconheceu a existência de um direito constitucional de personalidade que teria como objeto de proteção o poder do indivíduo de "decidir sobre a divulgação e o uso dos seus dados pessoais" („selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen"), de "decidir sobre quando e dentro de quais limites os fatos da sua vida pessoal podem ser revelados" („zu entscheiden, wann und

> innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden“) e ainda “de ter conhecimento sobre quem sabe e o que sabe sobre si, quando e em que ocasião” („wissen können, wer was wann und bei welcher Gelegenheit über sie weiß“). (FRANZIUS, op. cit., p. 259). No caso concreto, o Tribunal entendeu que o processamento automatizado dos dados possibilitado pela Lei do Censo de 1983 colocaria em risco o poder do indivíduo de decidir por si mesmo sobre se e como ele desejaria fornecer a terceiros os seus dados pessoais. A situação de risco identificada pelo Tribunal referia-se à possibilidade concreta de, por meio de sistemas automatizados, as informações fornecidas sobre profissões, residências e locais de trabalho dos cidadãos serem processadas de modo a se formar um perfil completo da personalidade” (BRASIL, 2020, p. 18-19).

No Brasil, o termo proteção de dados pessoais foi incorporado recentemente com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), promulgada em 18 de agosto de 2018 pelo presidente Michel Temer. Apesar disso, a problemática envolvendo proteção de dados já estava presente no debate jurídico brasileiro, isso porque, comumente era associada a discussões relacionadas à privacidade, ao direito do consumidor ou a outras liberdades individuais (DONEDA, 2021, p. 29). Essa assimilação ocorre principalmente com o direito à privacidade, nesse ponto, afirma:

> “A assimilação da proteção à privacidade pelo direito brasileiro é, de modo geral, linear com a sua progressiva consolidação como um dos direitos da personalidade pela doutrina e jurisprudência, até a sua previsão constitucional e sua menção específica no Código Civil de 2002, no art. 21. O efetivo desenvolvimento e aplicação desse direito, no entanto, não chegaram a formular um arcabouço capaz de fazer frente às novas situações e questões que surgiriam com a introdução de novas tecnologias” (DONEDA, 2021, p. 29).

Os conflitos envolvendo proteção de dados aumentaram mais ainda no final do século XX, pois, segundo Castells (2018, p. 135), citado por Ruaro *et al* (2019, p. 344), houve o surgimento de uma nova economia que tem como característica ser informacional, em rede e global. Assim, a matéria prima passou a ser os dados.

O debate sobre o direito à privacidade e a proteção de dados pessoais ganha cada vez mais espaço nos tribunais brasileiros e do mundo, afinal, é de suma importância regularizar a utilização de tratamento de dados pessoais.

Antes da Lei nº 13.709, a proteção de dados era tratada de forma transversal por outras normas, como a Constituição Federal; o Código Civil; o Código de Defesa do Consumidor; o Marco Civil da Internet; e a Lei de Acesso à Informação. Contudo, em 2018,

com grande influência do Regulamento Geral sobre a Proteção de Dados europeu, houve a positivação em lei específica. A lei europeia refletiu em diversas contribuições e norteou a Lei Geral de Proteção de Dados Pessoais no Brasil (RUARO *et al*, 2019, p. 345).

Acerca da Lei Geral de Proteção de Dados Pessoais, Garcia *et al* (2020, p. 16) afirma:

> "Inspirada na lei europeia de proteção de dados pessoais, conhecida como General Data Protection Regulation (GDPR), a LGPD tem como objetivo proteger os dados pessoais de pessoas naturais, ou seja, pessoas físicas. Este é o primeiro ponto: a LGPD nao tem como escopo os dados das empresas (pessoas jurídicas), mas sim os dados que as empresas têm das pessoas físicas, sejam elas funcionárias, terceiras, clientes, acionistas etc. - ou seja, todo mundo".

A LGPD estabelece já no artigo 5º conceitos importantes para sua compreensão[3]. A norma conceitua como dados pessoais toda informação relacionada a uma pessoa identificada

[3]BRASIL, Lei nº 13.709, art. 5º: Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento; IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico; V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento; VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); IX - agentes de tratamento: o controlador e o operador; X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração; XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo; XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada; XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados; XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado; XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro; XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados; XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco; XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional".

ou identificável, nos quais o sensíveis são os relacionados a personalidade do indivíduo e suas preferências. Já os dados anonimizados são aqueles que, por meios técnicos razoáveis e disponíveis na ocasião do tratamento, não possam ser identificados os titulares (BRASIL, 2018).

Além disso, a norma brasileira traz consigo um rol de princípios que devem ser atendidos. De acordo com Pinheiro (2020, p. 40) "a legislação visa fortalecer a proteção da privacidade do titular dos dados, a liberdade de expressão, de informação, de opinião e de comunicação, a inviolabilidade da intimidade, da honra e da imagem e o desenvolvimento econômico e tecnológico".

No que tange a aplicação material e territorial dessa norma, o artigo 3[4] dispõe que aplica-se a todos que realizam o tratamento de dados pessoais, seja pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que tenha pelo menos um desses elementos: (i) o tratamento ocorra em território nacional; (ii) a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; (iii) a coleta dos dados tenha ocorrido em território nacional (BRASIL, 2018).

No estágio atual, os dados pessoais dos cidadãos são o novo petróleo da era digital. Devido a isso, o debate sobre o direito à privacidade e a proteção de dados pessoais está ganhando cada vez um maior espaço nos tribunais brasileiros e do mundo, afinal, é de suma importância regularizar a utilização dessa disciplina.

4. O MARKETING NA ERA DIGITAL

O mundo digital gerou uma verdadeira revolução no mundo e principalmente na forma como empresas e consumidores se relacionam. De acordo com Torres (2010, p. 7), o

[4] BRASIL, Lei nº 13.709, art. 3º: "Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: I - a operação de tratamento seja realizada no território nacional; II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional. §1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta. §2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei".

marketing digital é cada vez mais importante para as empresas, isto porque o consumidor está mais conectado e utilizando a internet como meio de comunicação, relacionamento, entretenimento e informação. Assim, conceitua o *marketing* digital como:

> "[...] o conjunto de estratégias de marketing e publicidade, aplicadas a Internet, e ao novo comportamento do consumidor quando está navegando. Não se trata de um ou outra ação, mas de um conjunto coerente e eficaz de ações que criam um contato permanente da sua empresa com seus clientes. O marketing digital faz com que os consumidores conheçam seu negócios, confiem nele, e tomem a decisão de compra a seu favor".

Segundo Bioni (2019, p. 3), a sociedade vive uma nova forma de organização que tem como elemento central a informação. A ciência mercadológica segmentou os bens de consumo (*marketing)* e sua promoção (publicidade), assim, os dados pessoais dos cidadãos se tornaram fator vital para a engrenagem da economia da informação[5] (BIONI, 2019, p. 10).

O consumidor possui um papel cada vez mais ativo, ao passo que é elemento decisivo e integrante do processo de elaboração de planos de *marketing*. A metáfora do sorvete social (*prosumer*) exemplifica bem essa assertiva.

Essa metáfora surgiu em vídeo intitulado "*Social Media in Plain English*" de Lee e Sachi LeFever do Common Craft. De acordo com a narrativa apresentada por Cláudio Torres (2009, p. 22), a abstração criada ilustra uma cidade chamada Scoopville, famosa por seu sorvete. Há mais de vinte anos a empresa Big Ice Cream produzia sorvetes de excelente qualidade. Após a criação de um grupo de trabalho, foi decidido que para maximizar as vendas, seriam ofertados três sabores diferentes de sorvetes: baunilha, morango e chocolate.

Com a chegada de um novo eletrodoméstico, que possibilita que qualquer um pudesse fazer seus próprios sorvetes a custo competitivo, todos os moradores da cidade passaram a fazer seus sorvetes de acordo com suas respectivas preferências.

> "Os Smith decidiram fazer sorvete de abacaxi. John fez sorvetes de pistache. Silvia, apaixonada por conservas, inventou o sorvete de picles. E de repente, todos na cidade começaram a inventar seus próprios sorvetes, de todos os sabores imagináveis, a um custo baixo, distribuindo depois a seus amigos e parentes" (TORRES, 2009, p. 23)

[5] De acordo com Bioni (2019, p. 3), a sociedade da informação se caracteriza como a informação sendo o novo elemento estruturante que (re)organiza a sociedade e o elemento nuclear para o desenvolvimento da economia. Mais especificamente, essa nova organização social abrange como ferramentas o meio ambiente virtual, a computação eletrônica e a Internet.

Ao passar do tempo, os moradores começaram a enxergar o sorvete como algo para passar o tempo com amigos e familiares. Por outro lado, os visitantes ao chegar na cidade, se depararam com muitos sabores e tinham dificuldade em encontrar os mais populares.

Assim, John optou por colocar um papel na frente de sua loja e convidou seus clientes para dar notas, escrever impressões pessoais e indicar sorvetes. A ideia foi aderida de forma positiva e outros moradores também passaram a fazer o mesmo. Como consequência, houve uma melhora no sorvete:

> "No final, algumas coisas ficaram claras: os sorvetes melhoraram, porque os fabricantes aprendiam diretamente de seus clientes; as opiniões nos painéis funcionavam melhor que qualquer propaganda, atraindo mais clientes; e os painéis permitiam que os consumidores encontrassem exatamente os sorvetes desejados" (TORRES, 2009, p. 24).

Como dito por Torres (2010, p. 24-25), não há mais separação entre produtor e consumidor. A história ilustra bem a era das mídias sociais e a importância do feedback do consumidor, que participa diretamente das decisões de venda na economia de hoje. Para Bioni (2019, p. 12), a metáfora do sorvete social exemplifica a mudança do consumidor para uma postura mais ativa no ciclo de consumo, *in verbis*:

> "O consumidor deixa, portanto, de ter uma posição meramente passiva no ciclo do consumo. Ele passa a ter uma participação ativa, que condiciona a própria confecção, distribuição e, em última análise, a segmentação do bem de consumo, transformando-se na figura do *prosumer*. O consumidor não apenas consome (*consumption*), mas, também, produz o bem de consumo (*production*): *prosumer*" (BIONI, 2019, p. 12).

A partir desse vídeo ficou ainda mais claro que é o consumidor quem decide. Mais ainda, ficou exemplificado como as informações pessoais dos consumidores são pontos chaves para a atividade publicitária do *marketing* em geral (BIONI, 2019, p. 13).

Nesse mesmo sentido, Kotler (2017, np) discorre sobre a grande mudança do *marketing* que, inicialmente, era focado no produto, em seguida no consumidor e, por fim, no ser humano. O mercado está em constante evolução e uma nova espécie de consumidor surgiu de classe média, jovem, urbano, com conectividade fortes e mobilidade. Nesse ponto, acrescenta:

> "Eles se deslocam muito, com frequência trabalham longe de casa e vivem em ritmo acelerado. Tudo deve ser instantâneo e poupar tempo. Quando estão interessados em algo que veem na televisão, procuram em seus dispositivos móveis. Quando estão decidindo sobre uma compra em uma loja física, pesquisam preço e qualidade on-line. Sendo nativos digitais, podem

> tomar decisões de compra em qualquer lugar e a qualquer momento, envolvendo uma grande variedade de dispositivos. Apesar de versados na internet, adoram experimentar coisas fisicamente. Valorizam o alto envolvimento ao interagir com marcas. Também são bem sociais: comunicam-se e confiam uns nos outros. Na verdade, confiam mais em sua rede de amigos e na família do que nas empresas e marcas. Em suma, são altamente conectados" (KOTLER, 2017, np).

Como dito, com a sociedade da informação houve um crescimento considerável do uso das funcionalidades oferecidas pela internet, principalmente os *smartphones*. Através dos dispositivos móveis é possível captar dados de maneira eficaz. De acordo com Kotler (2017, np), podem ser capturados dados abundantes que incluem: padrões de movimentos em canais off-line; faixa demográfica; atividades na mídia social; preferência por promoções e produtos; registros de transações; padrões de consulta em canais on-line e outros.

A captura de dados é instrumento essencial para o marketing na era digital. Essa captura permite saber exatamente onde o usuário está a qualquer momento e proporciona uma análise preditiva de seu comportamento (KOTLER, 2017, np). Todos os passos ficam registrados e determinam padrões e hábitos entre os milhares de usuários na rede.

4.1. Os algoritmos

Segundo Ricardo Cappra (2017), ao longo dos anos a forma a qual recebemos conteúdo mudou significativamente. Afirma que, anos atrás, havia uma verdadeira parede entre o alto escalão de empresas, dos governos e toda a sociedade. A informação estava sempre no topo da pirâmide e o resto da sociedade recebia informação via mídias tradicionais, como jornais e revistas.

Com o advento da internet, houve uma verdadeira inclusão social com relação à informação – todo mundo estava recebendo ao mesmo tempo. As informações chegam no alto escalão ao mesmo tempo que chegam em toda a sociedade. Todavia, Cappra (2017), apresenta o grande problema do advento da internet: a grande quantidade de dados. Mais especificamente, havia um grande volume, velocidade de dados e em formatos que sequer é possível observar. Para que não ocorra o caos, surgiram os algoritmos que possuem como finalidade, por exemplo, filtrar a melhor música dentro de uma variedade quase infinita de músicas.

De acordo com Cappra (2017), os algoritmos constroem uma caracterização dos usuários, baseada nos dados disponíveis acerca de cada um. A consequência disto é a criação de um novo muro, pois cada usuário se assemelha a um grupo na internet e estes grupos não interagem entre si, pois estão clusterizados.

Segundo Leonardo Pena (2018, np) a clusterização é a divisão da população em pontos de dados em vários grupos com traços semelhantes, *in verbis*:

> "Clusterização é a tarefa de dividir a população ou os pontos de dados em vários grupos, de modo que os pontos de dados nos mesmos grupos sejam mais semelhantes a outros pontos de dados no mesmo grupo do que os de outros grupos. Em palavras simples, o objetivo é segregar grupos com traços semelhantes e atribuí-los a clusters. Vamos entender isso com um exemplo. Suponha que você seja o chefe de uma loja de aluguel e queira entender as preferências de seus clientes para expandir seus negócios. É possível que você veja os detalhes de cada cliente e crie uma estratégia comercial única para cada um deles? Definitivamente não. Mas o que você pode fazer é agrupar todos os seus clientes em 10 grupos com base em seus hábitos de compra e usar uma estratégia separada para clientes em cada um desses 10 grupos. E isso é o que chamamos de clustering".

Mello (2017, p. 43) ainda acrescenta:

> "A clusterização é uma importante técnica usada para dividir elementos de dados em subconjuntos homogêneos (chamados *clusters*), dentro dos quais os elementos são mais semelhantes uns aos outros, enquanto são mais diferentes em relação aos elementos de outros grupos (STARCZEWSKI & KRZYŻAK, 2015). Johnson & Wichern (1992) afirmam que a clusterização realiza o agrupamento de itens em função das similaridades ou distâncias (dissimilaridades) entre observações"

Os algoritmos irão determinar a partir de certas informações, características e *clusters,* o que será exibido para cada usuário (CAPPRA, 2017). Estes algoritmos funcionam como uma série de regras de funcionamento, de forma exemplificada, se um usuário pesquisar o livro A, deverá ser recomendado o livro B (CAPPRA, 2020).

Se usuários diferentes pesquisarem o mesmo termo em um provedor de busca, o resultado será diferente, isso ocorre porque, o algoritmo irá seguir os padrões de comportamento de cada um para vender um determinado produto. Cada vez que um usuário faz uma nova busca há um novo direcionamento no código do algoritmo, em outras palavras, o algoritmo aprende toda vez que é realizada uma nova busca. É importante destacar que, independentemente se a busca for realizada no computador ou no *smartphone*, o usuário é identificado dentro do algoritmo (CAPPRA, 2020).

4.2. A publicidade direcionada e a perfilização

A ciência mercadológica percebeu que a comunicação em massa de certo produto era ineficaz, visto que atingia muitos consumidores que não irão consumir aquele produto. Nesse contexto, surgiu a publicidade direcionada através da internet, que com a ajuda dos algoritmos, possibilita rastrear os interesses dos usuários e correlacioná-los a anúncios publicitários (BIONI, 2019, p. 16).

A ferramenta fundamental para a publicidade direcionada é a perfilização, que é feita através de algoritmos estruturados com base nos dados. A LGPD (Lei nº 13.709) não trouxe o conceito desse termo, todavia a legislação europeia, *General Data Protection Regulation*, definiu como sendo qualquer forma de processamento automatizado de dados pessoais utilizados para avaliar aspectos pessoais acerca de uma pessoa natural, em especial para analisar ou prever aspectos relacionados a performance dessa pessoa no trabalho, situação econômica, saúde, preferências pessoais, interesses, confiabilidade, comportamento localização ou movimentos[6].

De acordo com Valeria Ferraris (2013, p. 3-4), citada por Rafael Zanatta (2019, p. 8), a perfilização pode ocorrer de forma direta ou indireta. A direta ocorre utilizando os dados observados ou providos por um grupo ou indivíduo para derivar, inferir ou predizer atributos desconhecidos ou comportamento futuro. Já a indireta ocorre quando utiliza-se dados de um grupo populacional maior e indivíduos identificados na base de atributos que surgiam da população maior, tais como sistemas que recomendam vídeos ou músicas.

Nesse sentido, as redes sociais se tornaram o maior meio para a captação desenfreada de dados. Diariamente os usuários compartilham informações acerca de suas rotinas e preferências como uma maneira de interagir socialmente e muitos sequer se atentam que seus dados estão sendo coletados para alimentar uma rede de publicidade.

Segundo Bioni (2019, p. 17), a partir da interação dos usuários, as redes sociais acumulam diversos dados pessoais. Uma vez que um usuário está *logado,* passa a fornecer

---

[6] UNIÃO EUROPÉIA, GDPR: “(4) 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;”. Disponível em: <https://gdpr-info.eu/art-4-gdpr/>.

uma variedade de informações acerca do seu perfil, o que torna a ferramenta ideal para o direcionamento de publicidade.

> "Diversos outros serviços utilizam da mesma técnica, catalogando o comportamento do usuário para, a partir daí, direcionar uma publicidade condizente ao seu perfil inferido. O usuário da rede é, portanto, a todo momento, monitorado, acumulando-se uma série de dados (comportamentais), que são aplicados para a personalização da abordagem publicitária" (BIONI, 2019, p. 17).

Ademais, ainda é possível monitorar a eficácia de um anúncio publicitário, visto que os próprios cliques podem ser mensurados. A título exemplificativo, há o mecanismo de busca do Google, que permite estabelecer correlação entre termos buscados por um usuário à publicidade direcionada, "[...] define que a contraprestação somente será devida se o potencial consumidor clicar no correspondente anúncio (Google AdWords)" (BIONI, 2019, p. 17).

Mais ainda, o Google Adwords possui uma poderosa ferramenta denominada *remarketing* que permite a exibição de anúncios estratégicos. De forma específica, a ferramenta permite a exibição de anúncios, enquanto os usuários navegam no Google ou em sites parceiros, para usuários que já interagiram em determinado site ou aplicativo para dispositivos móveis. Desta maneira, aumenta o reconhecimento de determinada marca e lembra os usuários-alvo de fazer determinada compra (GOOGLE, 2021).

Outra forma de publicidade direcionada é através da localização geográfica dos *smartphones*. Nessa forma de publicidade se leva em conta a proximidade física do possível consumidor com o bem de consumo ofertado. A *geolocation* dos usuários passou a ser um bem tão valioso que foi um dos motivos pelos quais a Google adquiriu a um valor bilionário aplicativo Waze, que captura a localização dos seus usuários, e também a razão pela qual as redes sociais permitem que os usuários marquem os lugares que frequentam (BIONI, 2019, p. 18).

Essa modalidade de publicidade direcionada através dos dispositivos móveis é denominada *mobile marketing* por Bioni (2019, p. 18), *in verbis*:

> "Não é, portanto, uma mera coincidência que surja um anúncio publicitário, cujo bem de consumo esteja bem próximo geograficamente do cidadão ao utilizar um *smartphone*. A publicidade baseada na localização do potencial consumidor é uma (nova) estratégia mercadológica.
> É o chamado *mobile marketing* que implementa uma integração entre publicidade, Internet e telefone celular, sendo mais uma ferramenta para colocar consumidores e fornecedores em contato".

Como dito, é a partir da perfilização que a publicidade direcionada é feita. A criação de perfis dos usuários da internet permite que sejam exibidos conteúdos nas redes sociais que alimentam o negócio de diversas empresas. Quanto mais tempo e mais interação o usuário possui, mais dados pessoais podem ser extraídos (OMS; TORRES, 2020, p. 2).

Em suma, "[...] quanto mais tempo e mais interações dos titulares, maior a capacidade das empresas extrair dados pessoais de forma massiva e perfilizar o usuário de forma mais precisa". Dessa forma, o processo de perfilização fica mais meticuloso e os "[...] anúncios oferecidos e os conteúdos priorizados conseguem ser cada vez mais compatíveis com a personalidade e características psico-sociais dos indivíduos" (OMS; TORRES, 2020, p. 2).

A maioria dos serviços dos grandes provedores de serviços de internet possuem lucros que chegam a casa dos bilhões, mesmo oferecendo quase todas as suas funcionalidades de forma gratuita. Assim, surge um questionamento, como tais empresas possuem recordes de receita? A resposta é simples: anúncios.

A frase "*não existe almoço grátis*" originada pelo escritor norte americano Robert Heinlein ilustra bem a dinâmica entre os provedores de serviços de internet e os usuários. Afinal, tudo tem um preço.

Segundo Bioni (2019, p. 21), em um modelo de negócios tradicional, o consumidor irá pagar em troca uma quantia pecuniária. Ao passo que, nesse novo modelo de negócio, os usuários pagam cedendo seus dados pessoais em troca de publicidade direcionada. "Dessa forma, tal relação torna-se plurilateral, uma vez que ela envolve, necessariamente, os anunciantes de conteúdo publicitário, para haver retorno financeiro nesse modelo de negócio".

Como exposto por Panek (2019, p. 28), toda essa publicidade ocorre às custas da busca e armazenamento desenfreado de dados pessoais dos usuários, *in verbis*:

> "[...] a busca e armazenamento de informações acontecem de maneira arbitrária, desenfreada e intrusiva, objetivando coletar o máximo de volume de dados, para distribuir, vender e revender a outras empresas, criando uma rede de atores que tem à sua disposição dados pessoais privados de terceiros".

Como visto, o usuário se torna um produto comercializável, ao passo que, seus dados são o ponto chave da operação econômica em questão (BIONI, 2019, p. 22). Nesse sentido, Pinheiro (2020, p. 29) acrescenta que "[...] a informação passou a ser a principal moeda de troca utilizada pelos usuários para ter acesso a determinados bens, serviços ou conveniências".

4.3. O *App Tracking Transparency* (ATT)

A partir de 2021 a Apple irá implementar o *App Tracking Transparency (ATT)* como uma das atualizações do sistema iOS 14.5, iPadOS 14.5 e tvOS 14.5, de acordo com o o site oficial da empresa (*https://developer.apple.com/documentation/apptrackingtransparency*). A medida busca trazer maior transparência ao rastreamento feito por aplicativos, ao passo que irá notificar o usuário sempre que um aplicativo quiser rastrear seus dados pessoais em sites ou aplicativos de outras empresas, tanto para fins de publicidade, como de venda de suas informações (APPLE, 2021).

Através da estrutura do *App Tracking Transparency* o usuário irá precisar dar permissão para rastreá-lo ou acessar o identificador de publicidade do dispositivo (*Identifier For Advertising* - IDFA)[7]. Dessa forma, considera-se rastreamento todo ato de vincular dados do usuário ou dispositivo coletado de seu aplicativo com os dados dos usuários ou dispositivos coletados de aplicativos, sites ou propriedades off-line de outras empresas para publicidade direcionada ou fins de publicidade. Mais que isso, o termo rastreamento também está ligado com o compartilhamento de dados do usuário ou dispositivos com *data brokers*[8] (APPLE, 2021).

Como forma alternativa, a Apple disponibilizou a ferramenta *SKadNetwork*, que ajuda os anunciantes a medirem o sucesso das campanhas de anúncios, mantendo a privacidade do usuário. Nesta ferramenta, o usuário não precisa dar permissão (APPLE, 2021). Ademais, a empresa irá remover aplicativos de sua loja que possuam mecanismos de incentivo ou que apenas funcionem caso o usuário permita o rastreamento (CABRERA, 2021, np).

Por outro lado, as novas medidas de transparência adotada pela empresa receberam diversas críticas da indústria do *marketing* digital, principalmente acerca da alternativa apresentada pelo *SKadNetwork*, por não possuir o acesso a dados suficientes para traçar o perfil dos usuários. A estrutura do *App Tracking Transparency* modifica a capacidade e a forma em que os anunciantes oferecem publicidade direcionada. A indústria do marketing

[7]O *Identifier For Advertising* - IDFA é um ID exclusivo para dispositivos iOS que permite que as empresas rastreiem dados e façam o direcionamento de anúncios (APPLE, 2019, np).
[8]Segundo Peirano (2019, p. 2018), citado por Pyles (2020, np), os "*data brokers* são empresas especializadas na compra e venda de dados pessoais" que buscam reunir todos os dados pessoais dos usuários.

digital teme que os usuários não aceitem o rastreamento e afirmam que haverá a drástica diminuição de acesso aos dados (CABRERA, 2021, np).

De acordo com Cabrera (2021, np), o Facebook prevê que essa mudança irá reduzir em 50% o mercado de publicidade digital. Mais ainda, afirma que a mudança feita pela Apple pode alterar a natureza gratuita da internet. O *App Tracking Transparency* reformulou as regras de publicidade digital e ainda não é possível saber as consequências práticas dessa mudança.

5. A RESPONSABILIDADE DOS PROVEDORES NO BRASIL

A forma com que a internet e outros sistemas funcionam não torna necessário saber a identidade do usuário para submetê-lo a uma publicidade direcionada – é apenas necessário que seja atribuído um identificador eletrônico. A título exemplificativo há o chamado protocolo de endereço IP quando um computador está conectado à internet (BIONI, 2019, p. 75).

Na mesma linha, os usuários de *smartphones* possuem identificadores de publicidade. Assim, os usuários que usam o sistema android possuem o Android Advertising ID (AAID); já os que usam o sistema iOS possuem o Identifier For Advertising (IDFA).

Os identificadores de publicidade funcionam como um rastreador e permitem individualizar os usuários na internet para fins publicitários. Mais especificamente, possibilitam associar aos identificadores hábitos, histórico de navegação, localização geográfica, dentre outros e criam uma impressão digital com o perfil dos usuários. Assim, mesmo que não estejam associados a um nome, possuem a capacidade de identificar os usuários (CABRERA, 2021, np).

Em contrapartida, há discursos, inclusive de membros de grandes empresas do ramo da internet, que afirmam que a possibilidade de fornecer publicidade direcionada não está ligada com a possibilidade de associar esses identificadores ao nome de pessoas, *in verbis*:

> "Certa vez, um engenheiro do Google teria dito que eles não coletam informações associadas aos nomes das pessoas, pois isso geraria desinformação – "ruído" nas palavras dele. Em outra oportunidade, o então chefe de assuntos de privacidade do Facebook, Erin Egan, afirmou paradoxalmente que, apesar de a rede social fornecer publicidade com base na identidade dos seus usuários, isso não significaria que eles sejam pessoas identificáveis. Em uma série de reportagens sobre a técnica de "Privacy Differential" da Apple, a revista *Wired* é provocativa ao dizer,

> paradoxalmente, que essa técnica “coleta dados sobre você”, mas não muito “bem sobre você” (BIONI, 2019, p. 75).

Assim, surge um questionamento: quais as consequências jurídicas para os agentes que elaboram perfis comportamentais dos indivíduos a partir dos dados coletados na internet?

Como adiantado, a Lei Geral de Proteção de Dados foi incorporada recentemente no ordenamento jurídico brasileiro e teve grande influência do Regulamento Geral sobre a Proteção de Dados europeu. Rememorando, o artigo quinto da legislação brasileira conceitua como dados pessoais toda informação relacionada a uma pessoa identificada ou identificável, nos quais os sensíveis são os relacionados à personalidade do indivíduo e suas preferências (BRASIL, 2018).

Já o dado anonimizado não será considerado dado pessoal e é todo “dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento”. Ocorre que, o §2º do art. 12 estabelece uma exceção, ao dispor que os dados anonimizados “poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada” (BRASIL, 2018).

Ao prever que dados anonimizados podem ser considerados dados pessoais, caso sejam utilizados para formação de perfil comportamental de determinada pessoa natural, é possível inferir que a racionalidade da LGPD está nas consequências que as atividades de tratamento de dados podem acarretar sobre um determinado sujeito. Ademais, os termos “determina pessoa” e "identificada" presentes nesse dispositivo corroboram esse ponto, logo que “devem ser compreendidas com relação aos desdobramentos que o tratamento de dados pode ter sobre um indivíduo” (BIONI, 2019, p. 77).

A norma brasileira adota o conceito expansionista em relação ao dado pessoal, assim equivale a uma informação que, direta ou indiretamente, identifica um sujeito. Essa definição abraça, portanto, mesmo as informações que têm o potencial de identificar alguém, ainda que de maneira remota (BIONI, 2019, p. 64). Vale destacar que a própria noção de anonimização é nebulosa e não possui critérios claros para as ciências da computação (MARTINS *et al,* 2020, np).

Mais adiante, a LGPD estabelece as possibilidades em que poderá ser realizado tratamentos de dados pessoais[9], estes devem observar os princípios (i) da boa-fé; (ii) da finalidade, ao serem realizados apenas para propósitos legítimos específicos, explícitos e informados ao titular; (iii) da adequação, sendo necessário a compatibilidade do tratamento com as finalidades informadas ao titular; (iv) do livro acesso; (v) da qualidade dos dados; (vi) da transparência; (vii) da segurança; (viii) da prevenção; (ix) da não discriminação; e (x) da responsabilização e prestação de contas[10] (BRASIL, 2018).

Apesar da LGPD não ter abordado o conceito de perfilização, essa legislação permite a "inferência de um certo conceito interpretativo de perfilização enquanto processo automatizado de tratamento de dados que objetiva a análise e predição de comportamentos pessoais, profissionais, de consumo e de crédito". Nesse sentido, a lei usa terminologias cambiantes como "formação de perfil comportamental" (art. 12, §2º) e "definição de perfil de aspectos da personalidade" (art. 20, *caput*) (ZANATTA, 2019, p. 7).

---

[9] BRASIL, Lei nº 13.709, art. 7º: "O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular; II - para o cumprimento de obrigação legal ou regulatória pelo controlador; III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; 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 Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;-VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; 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; ou X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente".

[10] BRASIL, Lei nº 13.709, art. 6º: "As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas".

A categorização dos usuários a partir de dados pessoais repercute diretamente na tomada de inúmeras decisões. Isso ocorre porque, em uma sociedade e economia movida por dados, tudo é baseado no perfil elaborado para cada indivíduo, desde ato de consumo com base no histórico de compras ao conteúdo acessado na internet (BIONI, 2019, p. 87). Assim, como dito anteriormente, dois indivíduos podem pesquisar o mesmo termo em um provedor de busca, mas irão obter resultados completamente diferentes baseado no padrão de comportamento de cada um.

O Regulamento Geral sobre a Proteção de Dados europeu "prevê a possibilidade de oposição ao tratamento de dados para finalidades de *marketing* direto (art. 21) e a não sujeição do titular dos dados às decisões automatizadas como o profiling (art. 20)" (LIMA, 2020, p. 254). Ocorre que, a LGPD adotou um caminho divergente, e "é menos restritiva com relação à perfilização do ponto de vista de (i) ausência de um conceito jurídico expresso e (ii) ausência de uma norma geral proibitiva ao profiling, como ocorre na União Europeia" (ZANATTA, 2019, p. 20).

A norma brasileira predispõe que "se a perfilização acontecer, o titular dos dados pessoais passa a dispor de um conjunto de direitos". Já na hipótese de dados anonimizados, caso sejam "utilizados para a formação de perfil comportamental de determinada pessoa natural, se identificada [...], a legislação equipara o nível de proteção jurídica aos garantidos aos dados pessoais" (ZANATTA, 2019, p. 20).

Além disso, o art. 20 dispõe sobre a "definição de perfil de aspectos da personalidade" (BRASIL, 2018). Mais especificamente, o artigo estabelece que:

> "Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. §1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial. §2º Em caso de não oferecimento de informações de que trata o §1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais. § 3º (VETADO)".

O artigo em comento aborda o direito de revisão de decisões tomadas com base em tratamento automatizado de dados pessoais. Vale destacar que o primeiro parágrafo deste

artigo permite a solicitação de informações “a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada” (BRASIL, 2018).

Ocorre que, conforme Frazão (2018, np), a LGPD não aborda de forma clara o que seria (i) uma decisão totalmente automatizada; (ii) quais decisões automatizada afetam a esfera jurídica dos titulares de dados; (iii) “qual é o grau de transparência e explicação que será exigível em situações assim”.

De forma conclusiva, Zanatta (2019, p. 22-23) discorre que a partir da perfilização de dados pessoais e dados anonimizados é possível inferir algo sobre um indivíduo, assim, implicaria três obrigações de naturezas distintas: informacional; antidiscriminatória; e dialógica. *In verbis*:

> “(i) informacional, relacionada à obrigação de dar ciência da existência do perfil e garantir sua máxima transparência, (ii) antidiscriminatória, relacionada à obrigação de não utilizar parâmetros de raça, gênero e orientação religiosa como determinantes na construção do perfil, e (iii) dialógica, relacionada à obrigação de se engajar em um “processo dialógico” com as pessoas afetadas, garantindo a explicação de como a perfilização funciona, sua importância para determinados fins e de como decisões são tomadas”.

Feita essa análise, resta claro que “a conjugação dessas diversas variáveis evidencia que a proteção dos dados pessoais tangencia o próprio rumo da vida das pessoas [...] Desde a celebração de contratos e o ato do consumo à – até mesmo – busca pelo acesso à informação” (BIONI, 2019, p. 87).

Apesar da LGPD não ter trazido o conceito de perfilização, estabelece contornos jurídicos implícitos em poucos artigos que permitem, ainda que minimamente, a sua proteção. Assim, os dados anonimizados são considerados dados pessoais (art. 12, §2º) e é possível solicitar o direito à revisão de decisões tomadas unicamente com base em tratamento automatizado (art. 20, *caput*).

Portanto, tendo em vista a recente vigência da lei no cenário nacional, não há ainda jurisprudência consolidada sobre essa disciplina. Em âmbito internacional, entretanto, já há casos de grande repercussão e que têm sido usados para estudo acerca dessa temática.

6. CASOS PRÁTICOS DO USO DE DADOS PESSOAIS PARA FINS DE MARKETING DIGITAL

Com base no que já foi mencionado, o dado pessoal é o novo *commodity* da era da sociedade da informação. Há pouco tempo sequer havia norma brasileira que tutelasse o direito à proteção de dados pessoais e ainda há muitas incertezas acerca dos desdobramentos jurídicos na prática dessa nova legislação. A positivação desse direito e o crescente número de debates sobre o tema trouxe maior destaque a casos práticos de usos de dados, e dois deles serão abordados a seguir: o caso Target e o caso Cambridge Analytica.

6.1. O caso Target

O caso da empresa varejista americana Target é bastante relevante para a compreensão da forma como as empresas realizam o monitoramento do comportamento do consumidor e como isso embasa o comportamento da empresa. O caso ganhou repercussão quando, pelos resultados das estatísticas captadas no comportamento de uma consumidora adolescente, foi possível saber da gravidez da jovem antes mesmo dos membros da sua própria família. Em 2012, Charles Duhigg publicou um artigo no New York Time intitulado "*How Companies Learn Your Secrets*"[11] com contribuições do cientista de dados da Target com mestrado em estatística e economia, Andrew Pole.

Na gravidez as consumidoras consomem uma infinidade de produtos, assim, essa empresa "conseguiu verificar que tal perfil de consumidoras adquiria uma determinada lista de produtos. Isso permitiu não só prever o estado de gravidez, mas, também, o período de gestação para, daí, lhes direcionar produtos de acordo com a respectiva fase da gravidez" (BIONI, 2019, p. 36).

Durante décadas a Target já coletava informações em cada indivíduo que frequentava regularmente o estabelecimento e, sempre que possível, designava internamente um *Guest ID number*[12] para manter o monitoramento de tudo que o consumidor adquire, assim como suas informações pessoais, tais como: idade, estado civil, endereço, distância da sua residência até a loja, o valor do salário estimado, entre outras. Nesse sentido, a companhia podia também monitorar informações sobre seu histórico no trabalho, etnia, as revistas que estava lendo, o ano em que comprou sua casa, onde cursou faculdade, preferências políticas e quais assuntos

[11] "Como as companhias sabem os nossos segredos" (tradução nossa).
[12] "ID de identificação de convidado" (tradução nossa).

são discutidos online. Para tratar esses dados e analisá-los, havia um setor designado para isso, chamado *Target's Guest Marketing Analytics* (DUHIGG, 2012, np).

A empresa varejista coletou esses dados para análise, pois tinham ciência da importância dos hábitos para a determinação das decisões diárias dos consumidores. Assim, o cientista de dados Andrew Pole tinha como função expandir as vendas da empresa através de insights acerca dos hábitos dos consumidores. Deveria identificar momentos únicos na vida dos consumidores quando seus hábitos de compras se tornam flexíveis e o anúncio ou cupom certo os faria começar a gastar de novas maneiras (DUHIGG, 2012, np).

A maioria dos consumidores não prestava atenção ao comprar os produtos que eram adquiridos habitualmente, o que tornava mais dificultoso o trabalho dos profissionais de *marketing*, pois havia menos chances de persuadir o comprador a mudar o local onde comprava por cupons e promoções. Apenas quando os consumidores estavam passando por um grande acontecimento na vida, como em um gravidez, seus hábitos de compras se tornaram flexíveis (DUHIGG, 2012, np).

Com base nisso, o cientista de dados da empresa varejista identificou vinte e cinco produtos que, analisados de forma conjunta, detectam consumidoras grávidas (DUHIGG, 2012, np). "Dessa forma, os algoritmos dos bancos de dados foram programados para estabelecer tal correlação, segmentando, dentre as milhares de consumidoras, aquelas com tal perfil para fins de ação publicitária" (BIONI, 2019, p. 36).

A técnica funciona de forma tão eficiente que um pai solicitou uma audiência com o gerente da Target na cidade de Minneapolis. Para justificar o encontro, o homem alegava que sua filha, que ainda estava no ensino médio da escola, estaria sendo encorajada a engravidar, pois havia recebido e-mails da Target com promoções de roupa de criança e berços (DUHIGG, 2012, np).

Após alguns dias o gerente ligou para expressar suas desculpas em nome do Target e foi surpreendido com a notícia de que o homem havia tomado conhecimento posteriormente que sua filha estava grávida. Pouco tempo depois a empresa chegou a conclusão de que o modelo introduzido por Pole poderia ter diversas consequências negativas no que diz respeito às relações públicas, em outras palavras, nem todas as mulheres se sentiam confortáveis ao receber tais anúncios e muitos se sentem vigiadas pela empresa (DUHIGG, 2012, np).

6.2. O caso da Cambridge Analytica x Facebook

O caso ficou conhecido através de uma investigação conjunta do *The New York Times* e *The Observe* de Londres. A empresa Cambridge Analytica (CA) atua no ramo de *marketing* digital e tem seu modelo de negócios baseado "no uso de dados pessoais para analisar o comportamento de seus titulares ou de um grupo de pessoas com o objetivo de descobrir seus interesses, gostos e preferências". A Cambridge Analytica tem como foco a "alteração de comportamento por meio do uso de dados ("*data-driven behavior change*")", apesar de não ser uma novidade no ramo da publicidade, "nunca havia sido implementada com a magnitude, precisão e eficácia da CA" (MONTEIRO, 2018, np).

Dessa maneira, a empresa coletou informações dos perfis de usuários do Facebook de mais de 50 milhões de indivíduos sem sua permissão e foi considerado um dos maiores vazamentos de dados da história dessa rede social. Através dessas informações a empresa explorou a atividade de mídia social privada de grande parte do eleitorado americano, o que possibilitou o desenvolvimento de técnicas para trabalhar na campanha do ex-presidente Trump em 2016 (ROSENBERG *et al*, 2018, np).

A construção de perfis dos eleitores americanos não poderia ser feita da maneira tradicional, analisando registros de votações e históricos de compras. Para prever as crenças políticas e o comportamento eleitoral, era necessário ter acesso a traços psicológicos. Com base nisso, a empresa desenvolveu uma técnica de mapear traços de personalidade com base no que os eleitores americanos postam no Facebook (ROSENBERG *et al*, 2018, np).

Os dados foram coletados através de um teste de personalidade vinculado à plataforma da rede social. Ao responder o teste e baixar um aplicativo, era retirado informações privadas de seus perfis e de seus amigos — atividade que o Facebook permitia na época. Segundo alguns pesquisadores, a técnica era tão precisa que poderia revelar mais sobre um indivíduo do que seus pais ou parceiros românticos (ROSENBERG *et al*, 2018, np).

Em vídeo elaborado em 2018 pelo jornal BBC Brasil (disponível em: https://www.bbc.com/portuguese/geral-43705839), é exemplificado a forma com que a empresa utilizou os dados na campanha presidencial de Donald Trump:

> "A Cambridge Analytica ofereceu seus serviços à campanha presidencial de Donald Trump em 2016. Um exemplo de como os dados podem ter sido usados na campanha: a Cambridge Analytica saberia dizer quais pessoas no Facebook teriam o perfil adequado para receber anúncios divulgando bandeiras específicas do candidato. Esse anúncios seriam 'moldados',

> levando em conta os medos, necessidades e emoções das pessoas. Uma das bandeiras de Trump era a defesa do porte de armas. Um internauta de perfil 'aventureiro' pode ter recebido mensagens de que a liberdade tinha de se protegida de ameaças externas; o 'guardião', de que armas são essenciais para proteger as pessoas; e a 'executiva', sobre a proteção de sua família e do futuro. Mas essa avalanche de dados e mensagens pode fazer alguém ganhar uma eleição? É quase impossível provar isso. Ninguém consegue rastrear, em retrospecto, quem votou em quem por causa de um anúncio. Há muitas variáveis. Agora, o mundo todo sabe como os dados de usuários no Facebook foram usados para tentar manipular eleições".

O caso botou em pauta a possibilidade de alterar o resultado de uma eleição por meio de anúncios direcionados. O vazamento dos dados em questão trouxe "uma série de transtornos ao criador e dono do Facebook, Mark Zuckerberg, acarretando sua intimação para prestar esclarecimentos ao Congresso Nacional dos Estados Unidos" (SILVA et al, 2019, p. 4).

7. CONSIDERAÇÕES FINAIS

O presente artigo científico analisou a responsabilidade civil dos provedores ao tratarem dados pessoais para fins de *marketing* digital, com foco na prática de perfilização. A pesquisa abordou as possíveis problemáticas da padronização de consumo do usuário e o direcionamento de anúncios, a partir das reflexões doutrinárias de Ricardo Bioni e Rafael Zanatta.

A partir da exposição histórica da positivação do direito à proteção de dados pessoais, em especial no Brasil, foi possível verificar que essa disciplina ganha cada vez mais destaque nos tribunais brasileiros. O combustível para o crescimento constante desses debates se mostrou a nova modalidade de economia que tem como característica central a informação.

Diante da revolução ocasionada pelo mundo digital, o consumidor passou a ser elemento decisivo do processo de elaboração de planos de *marketing*. A captura de dados agora é instrumento essencial para publicidade direcionada através da internet. A ferramenta fundamental para essa modalidade de publicidade é a perfilização, feita por meio de algoritmos.

A partir desse cenário, o usuário se torna um produto comercializável, ao passo que, o ambiente supostamente "gratuito" da internet, tem como contraprestação os dados pessoais dos indivíduos. Os grandes provedores de serviços de internet possuem lucros bilionários a

partir da venda de anúncios em suas plataformas. Todo o *marketing* direcionado ocorre às custas da busca e armazenamento desenfreado de dados pessoais dos usuários.

Com base na análise dos casos Target e Cambridge Analytica nota-se que o tema proteção de dados não é recente e justamente por isso houve necessidade de legislar sobre a temática. Além deste ponto, é importante também salientar que a perfilização de dados, especialmente dados sensíveis, atinge tanto a esfera pública (como, por exemplo, a respeito da influência nas eleições presidenciais nos Estados Unidos), como também a esfera pessoal (como explanado no caso Target).

O foco principal do artigo foi levantar informações mais precisas sobre o uso de dados pessoais fornecidos pelos usuários e como estas questões estão sendo levantadas atualmente, e o porquê da utilização indevida não poder ser abordada de maneira despretensiosa.

Após a análise da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.579) e da doutrina, é concluído que, a legislação brasileira abarca de forma precária as consequências jurídicas para os agentes que elaboram perfis comportamentais dos indivíduos a partir dos dados coletados na internet. A partir da leitura da norma em comento, em casos que haja a prática de perfilização (i) o usuário terá o direito à revisão de decisões tomadas unicamente com base em tratamento automatizado (art. 20, *caput*); e (ii) os dados anonimizados poderão ser considerados como dados pessoais (art. 12, §2º).

REFERÊNCIAS BIBLIOGRÁFICAS

APPLE. **App Tracking Transparency**. 2021. Disponível em: <https://developer.apple.com/documentation/apptrackingtransparency>. Acesso em: 27 mar. 2021.

APPLE. **Developer Forums: Does this app use the Advertising Identifier (IDFA)?** 2019. Disponível em: <https://developer.apple.com/forums/thread/103552>. Acesso em: 27 mar. 2021.

APPLE. **iOS14**. 2021. Disponível em: <https://www.apple.com/br/ios/ios-14/>. Acesso em: 27 mar. 2021.

APPLE. **SKAdNetwork**. 2021. Disponível em: <https://developer.apple.com/documentation/storekit/skadnetwork>. Acesso em: 27 mar. 2021.

APPLE. **User Privacy and Data Use**. 2021. Disponível em: <https://developer.apple.com/app-store/user-privacy-and-data-use/>. Acesso em: 27 mar. 2021.

BBC. Como os dados de milhões de usuários do Facebook foram usados na campanha de Trump. **BBC Brasil.** 09 abr. 2018. Disponível em: <https://www.bbc.com/portuguese/geral-43705839>. Acesso em: 6 abr. 2021.

BIONI, B. R. **Proteção de Dados Pessoais - A Função e os Limites do Consentimento.** Rio de Janeiro: Forense, 2019. 2, rev., atual., reformul.. Epub. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788530988777/>. Acesso em: 20 jun. 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 28 mar. 2021

BRASIL. **Lei n. 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 20 fev. 2021.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 20 fev. 2021.

BRASIL. Superior Tribunal de Justiça. Civil e consumidor. Internet. Relação de consumo. Incidência do CDC. Gratuidade do serviço. Indiferença. Provedor de pesquisa. Filtragem prévia das buscas. Desnecessidade. Restrição dos resultados. Não-cabimento. Conteúdo público. Direito à informação. REsp nº 1.316.921. Google Brasil Internet LTDA e Maria da Graça Xuxa Meneghel. Relatora: Nancy Andrighi. DJ 29/06/2012. Disponível em: <https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1161904&num_registro=201103079096&data=20120629&peticao_numero=-1&formato=PDF>. Acesso em: 23.03.2021.

BRASIL. Superior Tribunal de Justiça. Direito civil. Internet. Blogs. Natureza da atividade. Inserção de matéria ofensiva. Responsabilidade de que mantém e edita o blog. Existência. Enunciado nº 221 da súmula/stj. Aplicabilidade. REsp nº 1.381.610/RS. Paulo Henrique dos Santos Amorim e Lasier Costa Martins. Relatora: Nancy Andrighi. DJ 12/09/2013. Disponível em: <https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1260240&num_registro=201300613536&data=20130912&peticao_numero=-1&formato=PDF>. Acesso em: 23.03.2021.

BRASIL. Superior Tribunal de Justiça. Medida cautelar em ação direta de inconstitucionalidade. Referendo. Medida provisória n. 954/2020. Emergência de saúde pública de importância internacional decorrente do novo coronavírus (covid-19). Compartilhamento de dados dos usuários do serviço telefônico fixo comutado e do serviço móvel pessoal, pelas empresas prestadoras, com o instituto brasileiro de geografia e estatística. *Fumus boni juris*. *Periculum in mora*. Deferimento. ADI 6389. MC-REF/DF. Partido Socialista Brasileiro e Presidente da República. Relatora: Min. Rosa Weber. DJ

12/11/2020. Disponível em: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754358482&prcID=5895168#>. Acesso em: 23.03.2021.

BRITO, D. M. de O. **Marketing compliance, proteção e gestão de dados pessoais: implementação do regulamento geral de proteção de dados**. 2018. Disponivel em: < https://iconline.ipleiria.pt/bitstream/10400.8/3692/1/Relat%c3%b3rioEst%c3%a1gio.MarketingRelacional.DanielaBrito.2160121.pdf> Acesso em: 20 jun. 2020.

CABRERA, Carolina Botero. Apple agita el modelo de la publicidad dirigida. **El Espectador.** 5 mar. 2021. Disponível em: <https://www.elespectador.com/opinion/apple-agita-el-modelo-de-la-publicidad-dirigida/>. Acesso em: 02 abr. 2021.

CADWALLADR, C.; CONFESSORE, N.; ROSEBERG, M. **How Trump Consultants Exploited the Facebook Data of Millions.** 2018. Disponível em: <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>. Acesso em: 29 jun. 2020.

CETIC.BR. Três em cada quatro brasileiros já utilizam a Internet, aponta pesquisa TIC Domicílios 2019. 26 mai. 2020. Disponível em: <https://cetic.br/pt/noticia/tres-em-cada-quatro-brasileiros-ja-utilizam-a-internet-aponta-pesquisa-tic-domicilios-2019/>. Acesso em: 7 abr. 2021.

DONEDA, Danilo. Panorama histórico da Proteção de Dados Pessoais. In: DONEDA, Danilo *et al* (Coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. E-book. Pp. 22-39. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788530992200/cfi/6/10!/4/2/4@0:0>. Acesso em: 01 mar. 2021.

DUHIGG, C. **How Companies Learn Your Secrets**. 2012. Disponível em: <https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html>. Acesso em: 20 jun. 2020.

ENTENDA OS ALGORITMOS E OS DADOS COM RICARDO CAPPRA. Entrevistado: Ricardo Cappra. Entrevistador: Ivan Moré. [S. l.]: CLAV. 5 out. 2020. Podcast. Disponível em: <https://open.spotify.com/episode/3uSOi6Cx3WWANEvVblRnhz?si=8j6t-va2QLW5xl8GDgqekA>. Acesso em: 22 mar. 2021.

FRAZÃO, Ana. Controvérsias sobre direito à explicação e à oposição diante de decisões automatizadas: série analisa as repercussões para a atividade empresarial. **Jota.** 12 dez. 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/controversias-sobre-direito-a-explicacao-e-a-oposicao-diante-de-decisoes-automatizadas-12122018>. Acesso em: 6 abr. 2021.

GALEGALE, G.P. **Internet das coisas aplicada a negócios: um estudo bibliométrico.** São Paulo, v. 13, n. 3, p. 423-438. 2016. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1807-17752016000300423&lng=en&nrm=iso>. Acesso em: 8 jun. 2020.

GOOGLE. **Ajuda do Google Ads**. Sobre o remarketing. 2021. Disponível em: <https://support.google.com/google-ads/answer/2453998?hl=pt-BR>. Acesso em: 27 mar. 2021.

KOTLER, Philip. **Marketing 4.0**: do tradicional ao digital. Rio de Janeiro: Sextante, 2017. Disponível em: <http://professor.pucgoias.edu.br/SiteDocente/admin/arquivosUpload/17352/material/Marketing-4-0-Do-tradicional-ao-digital%20(1).pdf>. Acesso em: 1 abr. 2021.

LEONARDI, Marcel. **Responsabilidade civil dos provedores de serviços de internet**. São Paulo: Juarez de Oliveira, 2005.

LIMA, Cíntia Rosa Pereira de (Coord.). **Comentários à Lei Geral de Proteção de Dados: lei n. 13.709/2018, com alteração da lei n. 13.853/2019.** São Paulo: Almedina, 2020. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788584935796/cfi/4!/4/4@0.00:16.2>. Acesso em: 6 abr. 2021.

MARTINS, Guilherme Magalhães. A pandemia da covid-19, o "profiling" e a Lei Geral de Proteção de Dados. **Migalhas.** São Paulo, 28 abr. 2020. Disponível em: <https://www.migalhas.com.br/depeso/325618/a-pandemia-da-covid-19--o--profiling--e-a-lei-geral-de-protecao-de-dados>. Acesso em: 5 abr. 2021.

MELLO, Paula Lunardi de. **Sistemáticas de agrupamento de países com base em indicadores de desempenho**. 2017. 84 f. Dissertação (Mestrado) - Curso de Engenharia de Produção, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2017. Disponível em: <https://www.lume.ufrgs.br/bitstream/handle/10183/158359/001021609.pdf?sequence=1>. Acesso em: 20 mar. 2021.

MONTEIRO, Renato Leite. Cambridge Analytica e a nova era Snowden na proteção de dados pessoais. **El País.** 20 mar. 2018. Disponível em: <https://brasil.elpais.com/brasil/2018/03/20/tecnologia/1521582374_496225.html>. Acesso em: 7 abr. 2021.

Pacheco, F.C.A. **O Marco civil da internet e o meio ambiente digital na sociedade da informação - Comentários à Lei n. 12.965/2014, 1ª edição.** Editora Saraiva, 2015. 9788502627741. Epub. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788502627741/>. Acesso em: 24 Mar 2021.

PANEK, Lin Cristina Tung. **Lei geral de proteção de dados n. 13.709/2018**: uma análise dos principais aspectos e do conceito privacidade na sociedade informacional. 2019. 33 f. Monografia (Especialização) - Curso de Direito, Universidade Federal do Paraná, Curitiba, 2019. Disponível em: <https://acervodigital.ufpr.br/bitstream/handle/1884/68114/TCC%20FINAL%20-%20lgpd.pdf?sequence=1&isAllowed=y>. Acesso em: 29 mar. 2021.

PENA, Leonardo. Introdução A Clusterização E Os Diferentes Métodos. **Portal Data Science.** 3 dez. 2018. Disponível em: <https://portaldatascience.com/introducao-a-clusterizacao-e-os-diferentes-metodos/>. Acesso em: 20 mar. 2021.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais**: comentários à lei n. 13.709/2018 (lgpd). 2. ed. São Paulo: Saraiva, 2020. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788553613625/cfi/3!/4/4@0.00:0.00>. Acesso em: 28 mar. 2021.

PYLES, Victor. Os data brokers e a comercialização dos dados pessoais. **Empório do Direito**, São Paulo, 2020. Disponível em: <https://emporiododireito.com.br/leitura/os-data-brokers-e-a-comercializacao-dos-dados-pessoais>.Acesso em: 04 abr. 2021.

ROSENBERG, Matthew *et al*. How Trump Consultants Exploited the Facebook Data of Millions. **The New York Times.** 17 mar. 2018. Disponível em: <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>. Acesso em: 7 abr. 2021.

RUARO, Regina Linden; GLITZ, Gabriela Panfolfo Coelho. Panorama geral da lei geral de proteção de dados pessoais no brasil e a inspiração no regulamento geral de proteção de dados pessoais europeu. **Repats**, Brasília, v. 6, n. 2, p. 340-356, jun-dez 2019. Disponível em: <https://portalrevistas.ucb.br/index.php/REPATS/article/view/11545/pdf>. Acesso em: 24 mar. 2021.

SERRO, B. M. **Da responsabilidade civil dos provedores de aplicações frente à Lei n. 12.965/2014: análise doutrinária e jurisprudencial.** UFMS, 2015. Disponível em: <http://coral.ufsm.br/congressodireito/anais/2015/6-3.pdf>. Acesso em: 27 jun. 2020.

SILVA, R. L; EHRHARDT, F. F.; JÚNIOR, A. A. W. **Sociedade em rede: caso cambridge analytica e a lei n. 13.709/2018 uma análise do seu potencial de proteção de dados dos usuários.** UFRS, 2019. Disponivel em: < https://www.ufsm.br/cursos/pos-graduacao/santa-maria/ppgd/wp-content/uploads/sites/563/2019/09/5.17.pdf> Acesso em: 20 jun. 2020.

TALIBERTI, Camila *et al*. Entra em vigor o Regulamento Geral de Proteção de Dados da União Europeia. **Migalhas.** São Paulo, jun. 2018. Disponível em: <https://www.migalhas.com.br/depeso/281042/entra-em-vigor-o-regulamento-geral-de-protecao-de-dados-da-uniao-europeia>. Acesso em: 06 fev. 2021.

TORRES, Cláudio. **A Bíblia do marketing digital**: tudo o que você queria saber sobre marketing e publicidade na internet e não tinha a quem perguntar. São Paulo: Novatec, 2009.
TORRES, Cláudio. **Guia Prático de Marketing na Internet para Pequenas Empresas**. São Paulo: Createspace Independent Pub, 2010. Disponível em: <https://www.faneesp.edu.br/site/documentos/Marketing_Internet.pdf>. Acesso em: 1 abr. 2021.

UNIÃO EUROPEIA. Parlamento e Conselho. Regulamento (EU) 2016/679, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, [*s. l.*], L 119/1, 4 maio 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT>. Acesso em: 22 mar. 2021.

ZANATTA, Rafael. Perfilização, Discriminação e Direitos: do código de defesa do consumidor à lei geral de proteção de dados pessoais. **Researchgate**, 2019. Disponível em: <https://www.researchgate.net/publication/331287708_Perfilizacao_Discriminacao_e_Direitos _do_Codigo_de_Defesa_do_Consumidor_a_Lei_Geral_de_Protecao_de_Dados_Pessoais>. Acesso em: 02 abr. 2021.