LEONARDO BERNARDES LIMA GOMES

O DIREITO DE PRIVACIDADE, DE LIBERDADE DE EXPRESSÃO E SEGURANÇA NA INTERNET

CURSO DE DIREITO – UniEVANGÉLICA

2021

LEONARDO BERNARDES LIMA GOMES

O DIREITO DE PRIVACIDADE, DE LIBERDADE DE EXPRESSÃO E SEGURANÇA NA INTERNET

Monografia apresentada ao Núcleo de Trabalho de Curso da UniEvangélica, como exigência parcial para a obtenção do grau de bacharel em Direito, sob a orientação da professora M.e. Ana Paula Ferreira Russo.

ANÁPOLIS – 2021

LEONARDO BERNARDES LIMA GOMES

O DIREITO DE PRIVACIDADE, DE LIBERDADE DE EXPRESSÃO E SEGURANÇA NA INTERNET

Anápolis, ____ de _____ de 2021.

Banca Examinadora

_____

_____

RESUMO

A presente monografia tem por objetivo estudar as leis que tratam sobre a proteção de dados dos usuários na internet, utilizando a legislação vigente no Brasil e no mundo, tendo como advento, os direitos constitucionais elencados no art. 5 da Constituição Federal. Aqui será analisado as leis que versam sobre o tema no ordenamento jurídico brasileiro, bem como as legislações internacionais que trazem consequências diretas e indiretas ao Brasil e aos usuários de todo o globo.

Palavras chave: Lei Geral de Proteção de Dados, Marco Civil da Internet, Privacidade.

SUMÁRIO

INTRODUÇÃO

O presente trabalho visa analisar os impactos causados no direito à privacidade, na liberdade de expressão e principalmente na segurança dos indivíduos que se conectam diariamente na internet, com ênfase nas consequências jurídicas, tendo como parâmetro a legislação vigente no Brasil.

É sabido que a rede mundial de computadores tem se tornado cada vez mais popular no século XXI, razão pela qual o local também tem sido utilizado com frequência, por pessoas más intencionadas, que praticam diversos crimes cibernéticos, que vão desde o roubo de informações pessoais; violação a segredos industriais; mensagens privadas e até mesmo imagens íntimas.

Nesse sentido, diversos países têm buscado soluções jurídicas que visam proteger seus cidadãos dos problemas mencionados acima, criando leis que versam sobre a proteção de dados na internet.

Nessa lógica, foram criadas no Brasil as Leis Carolina Dieckmann (Lei 12.737, de 30 de novembro de 2012), o Marco Civil da Internet (Lei 12.965, de 23 de abril de 2014) e por último, a Lei Geral de Proteção de Dados (Lei 13.709, de 14 de agosto de 2018).

É de se ressaltar que as citadas leis significaram um grande avanço para o Brasil e para o mundo no ramo do direito digital, sendo que o Marco Civil da Internet foi elogiado até mesmo pelo criador da internet na qual conhecemos nos dias de hoje, Sir Tim Berners-Lee.

Tratando sobre o mesmo assunto, a União Europeia implementou no dia 25 de maio de 2018 o Regulamento Geral de Proteção de Dados (GPDR, na sigla em inglês), que tem poder de afetar qualquer empresa ou usuário que tenha relações com o bloco europeu.

A GPDR se trata de uma das leis de proteção de dados mais rígidas do mundo, criada após as denúncias feitas por Edward Snowden em 2013, no qual revelou que os Estados Unidos da América promovia espionagem em massa de diversos países e que supostamente compartilhava informações com outras nações, como o Reino Unido.

A referida lei traz diversos benefícios aos usuários da internet, como por exemplo, permitir que o indivíduo, em algumas situações, possa analisar, corrigir e até mesmo excluir informações que empresas guardam sobre ele.

Outro ponto importante se refere ao fato de que as empresas devem coletar apenas os dados necessários para o funcionamento do serviço prestado. E em caso de roubo dessas informações, comumente praticadas pelos *“hackers”*, essas empresas devem avisar os seus usuários afetados no prazo máximo de 72 horas.

Ademais, a GPDR traz diversos outros pontos que tratam sobre a proteção de dados, pontos esses que causam efeitos até mesmo no Brasil.

Nessa ótica, podemos concluir que leis que versam especificamente do direito digital são cada vez mais necessárias, uma vez que os citados problemas acima têm se tornado cada vez mais recorrentes, fazendo inúmeras vítimas todos os dias no Brasil e no mundo.

CAPÍTULO I – A HISTÓRIA DA INTERNET E SEUS EFEITOS

Desde que a internet se tornou algo popular entre as pessoas, alguns contratempos emergiram nesse meio, como a iminência de um problema a despeito da privacidade humana, questões que envolvem a liberdade de expressão e a segurança digital. Entretanto, essa tecnologia é indispensável nos dias de hoje, sendo utilizada em absolutamente todo lugar e em todos os ramos de atividades e negócios do mundo. E para adentrarmos no objetivo da presente pesquisa, precisa-se, inicialmente, discorrer acerca do surgimento da internet, aspectos históricos, alguns conceitos necessários e o impacto social causado por essa tecnologia.

1.1 O Surgimento da Internet

De acordo com Naughton (2000), a internet teve início, principalmente, em meio às disputas políticas existentes entre os Estados Unidos da América e a extinta União Soviética, entre os anos de 1945 e 1991, polarizados em capitalismo e socialismo, respectivamente.

Devido à necessidade de propagação de mensagens em altas velocidades naquela época, o Departamento de Defesa dos Estados Unidos criou uma agência federal denominada ARPA (*Advanced Research Projects Agency*), cujo objetivo seria o desenvolvimento de uma tecnologia que pudesse facilitar a troca de informações de forma rápida, além de não depender da localização geográfica do receptor e/ou emissor.

Após a criação da aludida agência, surgiu o protótipo da primeira rede de internet, chamada Arpanet (*Advanced Research Projects Agency Network*). Assim, no dia 29 de outubro de 1969, a primeira mensagem via e-mail trocada na história foi realizada entre a Universidade da Califórnia e o Instituto de Pesquisa de Stanford (NAUGHTON, 2000, p. 72).

Após o esfriamento dos ânimos relacionados à Guerra Fria, a Arpanet deixou de ser uma tecnologia restrita ao uso militar e passou a ser difundida entre os civis, principalmente após as diversas pesquisas realizadas a partir do ano de 1962 por Joseph Carl Robnett Licklider, homem contratado diretamente pela ARPA para melhorias no sistema de internet (NAUGHTON, 2000, p. 72 e SIERRA, 2018, p. 23).

Anos mais tarde, já no início da década de 90 o cientista e físico britânico Tim Berners-Lee desenvolveu um navegador web chamado *World Wide Web* (www), que em português significa Rede Mundial de Computadores, ocasionando nos anos seguintes um estouro na utilização da internet, por parte das pessoas em geral (NAUGHTON, 2000, p. 213).

Nos anos subsequentes à criação de Berners-Lee, outros navegadores e aplicativos foram desenvolvidos, como *Mozilla Firefox*, *Opera Browser*, etc; o que atraiu um número maior de pessoas e assim, a internet não parou de crescer (TODAMATÉRIA, 2018).

Nessa mesma linha, surgiram também as redes sociais como o *Facebook*, lançado no ano de 2004 e o famoso *Orkut*, lançado no mesmo ano do rival, sendo esse último extremamente popular no Brasil entre os anos de 2006 a 2011. A ideia por trás da criação das redes sociais foi amplamente difundida como “tornar o mundo menor”, visto que o usuário poderia interagir com fotos, comentários e opiniões de qualquer pessoa do planeta, podendo trocar mensagens com outras pessoas de forma praticamente instantânea, o que popularizou ainda mais a internet (TODAMATÉRIA, 2018).

No Brasil, a internet surgiu em meados dos anos 80, quando universidades brasileiras passou a compartilhar algumas informações com

universidades e centros de pesquisas norte-americanos. Já em 1982, foi criada no Brasil a Rede Nacional de Ensino e Pesquisa (RNP), cujo objetivo era construir uma estrutura nacional de rede de internet de âmbito acadêmico (RNP, 2019).

Já em 1992 a primeira rede de internet foi instalada no país e alcançou inicialmente, dez estados, além do Distrito Federal. Desde então, a internet se instalou de forma rápida no Brasil, alcançando em maio de 2020, conforme pesquisa apontada pela Agência Brasil o patamar de 134 milhões de usuários em território nacional, ou seja, cerca de 64% da população brasileira.

Outrossim, atualmente ouve-se muito acerca da chamada Internet das Coisas (do inglês *Internet of Things* (*IoT*)), o que se refere a uma revolução tecnológica que tem como objetivo conectar os itens usados no dia a dia à Rede Mundial de Computadores. Tem surgido cada vez mais equipamentos como eletrodomésticos, meios de transporte e até mesmo roupas e maçanetas conectadas à internet e a outros dispositivos, como computadores e *smartphones*.

A ideia é que cada vez mais dispositivos estejam conectados à internet, facilitando assim a vida das pessoas, sendo que o indivíduo pode programar uma cafeteira, por exemplo para preparar o café em determinado horário do dia, sendo desnecessário a presença de uma pessoa para fazer todo esse processo cotidiano. Mas essas tecnologias não estão presentes exclusivamente em eletrônicos residenciais não, pois hoje em dia existem os relógios inteligentes, comumente conhecidos como *smartwatch* e até mesmo óculos como o Google Glass que apresentam inúmeras informações em sua lente (MAGRANI, 2018, p. 20).

Todos esses equipamentos estão dentro do que se chama Internet das Coisas. Mas afinal, de onde surgiu esse termo? Inicialmente, o citado termo fora proposto por um professor e pesquisador do MIT (*Massachusetts Instituite of Technology*) chamado Kevin Ashton no ano de 1999.

De acordo com Ashton, a conexão contínua feita por usuários de todo o mundo, por meio de aparelhos conectados à internet como os já citados anteriormente, deverá causar um acumulo de dados tão grande e com tamanha

precisão que será possível otimizar e economizar recursos naturais e energéticos. Para o especialista, essa revolução será maior do que o próprio desenvolvimento da internet que conhecemos hoje (MAGRANI, 2018, p. 32).

Nesse sentido, tem-se cada vez mais objetos conectados à internet numa residência, como por exemplo os “assistentes pessoais” que carregam dentro de si uma software de Inteligência Artificial, sendo mais comum no Brasil, o recém chegado Amazon Alexa, que se tratam de pequenos aparelhos que recebem comandos de voz para controlar outros equipamentos conectados à internet, como por exemplo, lâmpadas inteligentes, acionamento de cortinas, eletrodomésticos e até mesmo torneiras high-tech (TECHTUDO, 2019).

Outra tecnologia que está cada vez mais avançada, dentro do conceito de Internet das Coisas, são os carros autônomos, que têm se tornado cada vez mais presente em países desenvolvidos. A Áustria, por exemplo, é comumente escolhida para diversos testes desses veículos, uma vez que as estradas bem pavimentadas e devidamente sinalizadas contribuem com a facilidade de locomoção e com os testes dessa tecnologia.

Empresas que fabricam carros como a Tesla, Volkswagen e Ford tem realizado cada vez mais pesquisas nessa área, e até mesmo empresa como a Sony, fabricante conhecida de aparelhos eletrônicos que envolvem TVs, câmeras e outros equipamentos, desenvolveu um veículo que conta com 40 sensores de movimentos em sua carroceria para identificar objetos em sua volta, visando tornar obsoleto, no futuro, a presença de uma pessoa atrás do volante (TECNOBLOG, 2021).

Tudo isso, só é possível graças à internet, que teve início em um período conturbado da história humana, voltada exclusivamente para fins militares e que atualmente, pouco mais de 50 anos depois, já se fala em aparelhos que podem desempenhar funções sem a necessidade de ter uma pessoa controlando.

1.2 Conceito de Big Data

Para melhor aprofundamento na presente monografia, devemos tratar acerca de alguns termos técnicos, como por exemplo, o Big Data.

Big Data, de forma simples, é um termo do ramo da Tecnologia da Informação (TI) que se refere a um conjunto de dados que precisam ser processados e armazenados, ou seja, trata-se de um complexo de informações obtidas por meio dos usuários de qualquer serviço que esteja conectado à Rede Mundial de Computadores.

Portanto, ao utilizar um aplicativo mensageiro, por exemplo, o indivíduo realiza um cadastro de perfil on-line, apresentando informações como nome, telefone, endereço residencial/eletrônico, dentre outros dados, e tais informações serão processadas pela empresa proprietária do serviço e armazenada num banco de dados, o que é chamado de Big Data.

Mas afinal de contas, o Big Data serve apenas para processar e armazenar dados? Na verdade não, visto que o conceito é ainda mais complexo, pois trata-se de um conjunto de técnicas utilizadas para analisar grande quantidade de dados, com o intuito de gerar resultados importantes para melhoria de serviços virtuais, pesquisas de opinião e principalmente, publicidade. (MARQUESONE, 2017, p. 5).

A publicidade é o principal alvo quando tratamos de um grande armazenamento de dados pessoais, pois ao reunir certas informações de um indivíduo, a empresa detentora desses dados podem direcionar a uma pessoa ou a um grupo de pessoas, propagandas acerca de determinado produto. Para fazer isso, as empresas utilizam até mesmo a suposta capacidade financeira do indivíduo.

Aliás, não é necessário se cadastrar em serviços *on-line* para que tais informações sejam captadas e armazenadas em um grande banco de dados, visto que os sites atualmente contam com um ferramenta simples chamada *cookie (*biscoito em tradução livre) que captam informações daquele usuário que está

utilizando um dispositivo com acesso à internet. Portanto, ao acessar um site de *e-commerce* e pesquisar por uma televisão, esse usuário será constantemente bombardeado com propagandas de televisores até que esse mude sua pesquisa.

E mais, se esse usuário estiver conectado ao seu e-mail, por exemplo, os cookies serão repassados ao provedor do serviço de endereço eletrônico e sempre que esse usuário acessar sua conta, seja via smartphone ou computadores pessoais, propagandas relacionadas ao que ele pesquisou anteriormente surgirão em sua tela novamente.

Nesse sentido, observa-se que as pessoas estão totalmente presas a esses sistemas, independente de anuência, a menos que o indivíduo decida se tornar anônimo, o que é impossível atualmente, pois o próprio governo dispõe de ferramentas que praticamente obrigam o cidadão a possui uma “vida virtual”.

Voltando a tratar do armazenamento de dados, a empresa Google, para fins de conhecimento, processa diariamente mais de 3 bilhões de pesquisas em todo o mundo, sendo que desse total, 15% são totalmente inéditas. O chamado “motor de pesquisas” da empresa rastreia no mesmo período mais de 20 bilhões de sites, o que gera um acumulo de dados tamanho que chega a ser difícil de explicar, ou seja, 100 petabytes, o que seria 100 milhões de gigabytes num único dia. Mas é assim que o buscador mais utilizado do mundo apresenta respostas das mais diversas possíveis, de forma rápida e eficiente, utilizando novas pesquisas para apresentar novos resultados, isso é Big Data (CETAX, 2020).

Para se ter uma noção, a empresa Google possui as chamadas “fazendas de dados" distribuídas pelo globo, com enormes servidores funcionando 24 horas por dia, com centenas de funcionários no controle da enorme quantidade de informações geradas diariamente no mundo todo. E só pra constar, o Google conhece muito mais sobre você do que qualquer outra pessoa, dado as informações fornecidas pelo usuário (TECMUNDO, 2016).

Outrossim, para uma utilização fluida e precisa de equipamentos incluídos no conceito de Internet das Coisas, as ferramentas de Big Data são extremamente necessárias, pois esses equipamentos estão a todo instante gerando dados e mais dados, a fim de melhorar os seus sistemas, sendo que veículos autônomos, por exemplo, estão a se comunicar com outros veículos a todo instante, visando tornar o trânsito cada vez mais seguro e diminuindo o número de congestionamentos.

1.3 Impacto Social

Anteriormente abordamos acerca do contexto histórico da internet, seu surgimento, as tecnologias que emergiram em meio ao desenvolvimento da Rede Mundial de Computadores e principalmente, sobre a presença marcante e cada vez mais necessária desse recurso no meio social.

Conforme dados já apontados nesta monografia, a internet registra cada vez mais um número maior de usuários, crescendo de forma exponencial a cada dia. O *Instagram*, por exemplo registrou 1 bilhão de usuários ativos em 2020, quando completou 10 anos de existência e, atualmente ocupa a 5ª posição como rede social mais utilizada no mundo, ficando atrás do *Facebook*, contando com 2,6 bilhões de usuários, *YouTube* e *Whatsapp* com 2 bilhões cada e *WeChat* com 1,2 bilhões (G1, 2020).

Outro ponto a ser destacado no uso das redes sociais está no fato de que cada vez mais pessoas tem conseguido ganhar dinheiro por meio delas, sendo o palco de diversos cursos acerca de Marketing Digital, cujo objetivo é a promoção de produtos e serviços *on-line* (ORGÂNICA, 2021).

Artistas, políticos e atletas de todo o mundo tem utilizado as redes sociais para apresentar seus produtos, serviços, marcas e opiniões ao público. Alguns atletas, como por exemplo o jogador de futebol brasileiro Neymar chega a cobrar até R$ 2,7 milhões por post, conforme noticiou o jornal Folha de S. Paulo. Outros artistas também aparecem na lista, como o ator Caio Castro que cobra pouco mais de 600 mil reais, ou seja, para que uma empresa utilize o perfil dessas pessoas, a

fim de divulgar o seu produto, é necessário estar disposta a pagar a quantia exigida pelo proprietário do perfil.

E isso tem se tornado cada vez mais comum, visto que a profissão chamada *digital influencer* (em tradução livre – influenciador digital) tem crescido cada vez mais.

Ou seja, a internet já vinha crescendo em um ritmo acelerado, entretanto o cenário mudou drasticamente com a chegada da pandemia da Covid-19, visto que muitas pessoas passaram a ficar mais em casa, em razão das políticas de isolamento social, culminando assim num número maior no tráfego da internet mundial. Em alguns países da Europa, como o Reino Unido, Alemanha, França e Itália, o consumo da internet registrou um crescimento de 40%, conforme noticiado pelo Portal G1, isso graças ao *home office* e às aulas *on-line*.

Aliás, a internet se mostrou ainda mais necessária no atual cenário em que vivemos, visto que a pandemia pegou muita gente de surpresa no final de 2019. Diversas empresas optaram por mandar seus funcionários para casa, visando protegê-los da doença. As instituições de ensino fizeram o mesmo com seus acadêmicos, decidindo ministrar aulas pela internet, por meio de aplicativos que antes não ouvíamos falar e hoje fazem parte do nosso cotidiano.

Empresas e pessoas tiveram que se reinventar, devendo aprender a utilizar o maravilhoso e fantástico mundo virtual. Reuniões passaram a ser feitas de forma remota, entrevistas de emprego não precisaram ser feitas de forma presencial, enfim, tudo mudou (TECNOBLOG, 2020).

Além do mais, durante a pandemia o Brasil ganhou um sistema avançado de recebimento e transferência de dinheiro via internet, o famoso PIX, apresentado pelo Banco Central em outubro de 2020, cuja finalidade é o imediato envio ou recebimento de valores, funcionando 24 horas por dia, 7 dias por semana (UOL, 2020).

Mas as mudanças, por melhores que sejam, acabam desencadeando eventos indesejados, sendo alguns já previstos e outros não. A privacidade *on-line* é algo que muito se discute atualmente, visto que o mundo está cada vez mais conectado, o que acaba por gerar conflitos entre os indivíduos. Há aplicações de golpes virtuais, exposição de pessoas, opiniões maldosas e, principalmente a propagação de *fake news*, que em tradução livre significa “notícias falsas”.

Na opinião deste acadêmico, nunca enfrentamos tantos problemas associados à internet, mesmo com os diversos avanços em termos de segurança *on-line*. O serviço PIX, por exemplo, tem sido utilizado por criminosos do Brasil inteiro para prática indiscriminada de crimes cibernéticos, devido a facilidade de transferência de valores proporcionada por esse sistema (G1, 2021).

Pensando nos problemas descritos acima que o Congresso Nacional elaboram leis, visando proteger seus cidadãos, dado o crescente número de violações de direitos que ocorrem por meio da internet. No Brasil, temos as Leis Carolina Dieckmann (Lei 12.737, de 30 de novembro de 2012), o Marco Civil da Internet (Lei 12.965, de 23 de abril de 2014) e por último, a Lei Geral de Proteção de Dados (Lei 13.709, de 14 de agosto de 2018), que serão devidamente exploradas em momento oportuno.

CAPÍTULO II – O DIREITO À PRIVACIDADE, LIBERDADE DE EXPRESSÃO E À PROTEÇÃO DE DADOS

O direito à privacidade e liberdade de expressão se encontram expressamente garantidos no artigo 5°, incisos X e IX da Constituição Federal de 1988. O direito à proteção de dados veio a ser garantido por meio da Lei Geral de Proteção de Dados, em seu artigo 17, assegurando ao titular dos dados a faculdade de se resguardar e de dispor das suas informações, de maneira que não lhe cause quaisquer danos.

2.1 Direito Fundamental à Privacidade

Antes de aprofundar no que se refere ao direito à privacidade, é necessário diferenciar os conceitos de direito e garantias fundamentais. Nas palavras do doutrinador Ruy Barbosa, direito são disposições meramente declaratórias, que apenas estabelecem sua existência legal. Quanto as garantias, essas são medidas que visam assegurar a aplicação do direito (BARBOSA, 1993).

Conforme previsto no texto constitucional, o direito à privacidade se encontra no campo dos direitos relativos à personalidade. Seu objetivo é garantir que o indivíduo possa desfrutar de uma vida íntima, sem com que haja uma conduta invasiva de outro sujeito ou do próprio Estado.

Retira-se do texto constitucional, em seu artigo 5°, inciso X, acerca do direito à privacidade - “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).

Nesse sentido, verifica-se que o legislador apresentou grande preocupação em relação à vida privada do indivíduo, dando-lhe até mesmo o direito a indenização pelos danos decorrente de tal violação.

Destaca-se que o dispositivo constitucional (art. 5°, X) aborda duas dimensões distintas: intimidade e vida privada. De acordo com parte da doutrina, a intimidade se trata do mais elevado nível de particularidade de um indivíduo, ou seja, trata-se do direito de estar a sós consigo mesmo. Já o direito à vida privada está ligado as relações que uma pessoa possui com seus amigos e familiares. Salienta que em ambos os casos, a norma garante plena proteção legal ao direito à privacidade (BARRETO, 2019).

Ademais, conforme Súmula n. 227 do STJ, o direito a intimidade não está restrito à pessoa física, podendo alcançar até mesmo a pessoa jurídica, garantindo-lhe a faculdade de sofrer dano moral. Contudo, o ordenamento jurídico precisa arrazoar acerca da existência de dois direitos constitucionais igualmente assegurados, quais sejam, o direito à privacidade e o direito a informação (STJ, 2011).

Até meados dos anos 2000, o direito à privacidade se restringia aos atos praticados pelo vizinho bisbilhoteiro, pelo colega de trabalho ou pelo familiar que não respeitava o espaço de determinado indivíduo. No entanto, com o avanço da internet, esse direito ficou cada vez mais difícil de ser exercido, visto que fora imposto maiores obstáculos ao Estado, que agora precisa executar sua tutela jurisdicional no âmbito digital.

Cabe ressaltar que exercer a tutela jurisdicional no meio digital não é uma tarefa fácil, uma vez que é extremamente trabalhoso rastrear o indivíduo que cometeu crime cibernético, visto que a velocidade na qual uma informação é difundida na rede chega ser inimaginável.

Portanto, para aprofundar no que se refere acerca da privacidade online, é necessário, inicialmente, entender quais são os principais fenômenos que contribuem para violação desse direito constitucional, e são pelo menos dois: o primeiro trata-se da estruturação de dados, que trouxe a possibilidade de armazenar informações em grandes quantidades, sem sequer pedir permissão do usuário para isso; já o segundo, compreende no aumento do uso da internet, influenciando os indivíduos a manterem perfis e informações na rede, a fim de "facilitar" a vida cotidiana.

O uso de informações pessoais sempre foi utilizado para fins comerciais, desde anotações em livros de registros, até a captação de dados inseridas pelo próprio indivíduo por meio eletrônico, no entanto, tal prática tem se tornado recorrente nos últimos 10 anos, o que permite que fornecedores de produtos e mercadorias das mais diversas possíveis, alcance um número cada vez maior de clientes e, com isso, acaba elevando o seu capital.

Cumpre ressaltar que todas as informações pessoais de um usuário são, muitas vezes, inseridas por ele próprio, de forma voluntária e gratuita. Todos esses dados são de imenso valor para empresas e órgãos governamentais de todo o mundo, o que acaba tornando verdadeira a seguinte frase dita por Andrew Lewis: *"se você não está pagando por um produto, é sinal de que o produto é você"*.

Outro ponto a ser destacado, é acerca do conflito existente entre a privacidade online é a liberdade de imprensa, algo que tem tido embates, muitas vezes calorosos, com o avanço da internet. De acordo com Philip Meyer, existem duas ações que geram o mencionado conflito, são elas: a revelação de fatos privados da vida íntima de alguém e o indevido método de reportagem (1987, p.124).

É inegável que a internet é a principal fonte de informação existente atualmente, no entanto, é também o principal meio para divulgar informações e notícias que podem trazer prejuízos à imagem e a vida de outras pessoas.

O texto constitucional, em seu artigo 220, §1°, dispõe da seguinte redação, acerca da liberdade de imprensa - "Nenhuma lei conterá dispositivo que

possa constituir embaraço à plena liberdade de informação jornalística em qualquer veículo de comunicação social, observado o disposto no art. 5º, IV, V, X, XIII e XIV" (BRASIL, 1988).

Outrossim, não se pode esquecer da Lei n. 5.250 de 9 de fevereiro de 1967, também chamada de Lei de Imprensa, na qual regula a liberdade de manifestação do pensamento e da informação. Contudo, a citada lei não trata acerca do conflito existente entre o direito à privacidade e a liberdade de imprensa, ou seja, não há dispositivo que caracteriza de maneira cristalina a violação à privacidade, trazendo apenas clareza quanto aos crimes contra a honra, os chamados direito de personalidade (calúnia, difamação, injúria e ofensa à memória dos mortos).

2.2 A Liberdade de Expressão na Internet

De início, deve-se destacar que a Constituição Federal, em seu artigo 5°, inciso IV, estabelece que é livre toda e qualquer manifestação do pensamento de grupos ou indivíduos, sendo defeso em lei, o anonimato (BRASIL, 1988).

Outrossim, cumpre dizer que o Pacto de San José da Costa Rica, em seu artigo 13, dispõe que – "toda pessoa tem direito à liberdade de pensamento e de expressão. Esse direito inclui a liberdade de procurar, receber e difundir informações e ideias de qualquer natureza, sem considerações de fronteiras, verbalmente ou por escrito, ou em forma impressa ou artística, ou por qualquer meio de sua escolha" (Pacto de San José de Costa Rica, 1969).

Ante o exposto, verifica-se que a liberdade de expressão é um direito fundamental do indivíduo inserido num Estado Democrático de Direito e, nesse contexto, a liberdade de expressão, de pensamento, opinião política, ideológica e religiosa é tão crucial quanto se alimentar.

A internet possibilitou um alcance ainda maior da liberdade de expressão, permitindo aos usuários que buscam expor suas opiniões numa rede social, por exemplo, alcançar centenas ou até mesmo, milhares de pessoas em questão de minutos e, devido à ausência de fronteiras no meio digital, usuários de outros países

podem visualizar, interagir e compartilhar praticamente qualquer conteúdo publicado na rede mundial de computadores.

No entanto, destaca-se que a liberdade de expressão possui certas limitações no Brasil, ou seja, diferentemente do que ocorre nos Estados Unidos, o indivíduo não é plenamente livre para manifestar aquilo que pensa. A Constituição, por exemplo, garante ao cidadão, o livre exercício de cultos religiosos, conforme redação do artigo 5°, inciso VI – “é inviolável a liberdade de consciência e de crença, sendo assegurado o livre exercício dos cultos religiosos e garantida, na forma da lei, a proteção aos locais de culto e a suas liturgias” (BRASIL, 1988).

Contudo, para Alexandre de Moraes, o referido dispositivo se aplica somente se “a realização de cultos religiosos não forem contrários à ordem, tranquilidade e sossego público, bem como compatíveis com os bons costumes. Dessa forma, a questão das pregações e curas religiosas devem ser analisadas de forma a não obstaculizar a liberdade religiosa garantida constitucionalmente, nem tampouco acobertar práticas ilícitas” (MORAES, 2006, p. 207).

No mesmo sentido, aplica-se quanto às liberdades políticas e ideológicas, uma vez que é vedado o fomento das massas, quanto a ideologias racistas, como o nazismo, por exemplo. Aliás, acentua-se que nos últimos anos, a rede mundial de computadores tem contribuído fortemente com a propagação de grupos voltados para o extremismo político e ideológico, pautados principalmente em teorias conspiratórias.

Um desses grupos que mais se beneficiou com o alcance da internet, é o chamado QAnon, criado em meados de 2018, em apoio ao ex-presidente americano Donald Trump. A organização teve grande participação na invasão ao Capitólio dos Estados Unidos no início de 2021, após o então presidente perder as eleições para a Casa Branca. O grupo alega lutar contra o “Estado Profundo”, afirmando ser contrário às vacinas, bem como negando a existência do coronavírus. Devido ao extremismo político propagado por essa organização, empresas como o Facebook já deletou inúmeros perfis que fazem apologia a esse tipo de informação, cujo objetivo

é incitar pessoas a praticarem diversos crimes virtuais (BBC, 2020).

Contudo, mesmo havendo questões delicadas como o surgimento de grupos extremistas, que proferem xingamentos, ataques racistas, dentre outras ações, devemos ressaltar que a internet é a melhor demonstração do que se conhece por democracia hoje em dia, pois, se existem organizações que promovem ações distintas, sejam elas boas ou ruins, significa que o indivíduo está exercendo seu direito de opinar mediante determinado assunto ou situação, ou seja, democracia.

No mais, não se pode deixar de citar, novamente, as palavras de Alexandre de Moraes, ao discorrer acerca do casamento entre liberdade de expressão e democracia:

> A liberdade de expressão constitui um dos fundamentos essenciais de uma sociedade democrática e compreende não somente as informações consideradas como inofensivas, indiferentes ou favoráveis, mas também as que possam causar transtornos, resistência, inquietar pessoas, pois a Democracia somente existe baseada na consagração do pluralismo de ideias e pensamentos, da tolerância de opiniões e do espírito aberto ao diálogo (MORAES, 2006, p. 207).

Aliás, destaca-se que a história é repleta de lutas em prol da democracia e, consequentemente, em prol da liberdade de expressão. Por esse motivo que a liberdade do indivíduo em se expressar, em dividir a sua opinião política e ideológica é considerado um direito fundamental, portanto, um direito inalienável. Em alguns países de cunho socialista, a exemplo de Cuba, a liberdade de se expressar contra o governo é totalmente proibida, tendo os governantes derrubado a internet do país, a fim de dirimir o alcance daqueles contrários às políticas ali implementadas (FOLHA DE S. PAULO, 2021).

Voltando a tratar do Brasil, cumpre dizer que a Constituição Federal, assegura ao indivíduo que teve os seus direitos violados, além da indenização pelo dano sofrido, seja ele: material, moral ou de imagem; o chamado direito de resposta (CF, art. 5°, V).

Para Barros Filho, a prerrogativa de oferecer resposta a uma agressão veiculada pelos meios de comunicação tem, para os doutrinadores, a mesma

natureza jurídica da legítima defesa. Assim, face a uma agressão injusta, pode o agredido reagir. Imediatamente e com meios proporcionais à agressão, garantidos pela legislação de imprensa (BARROS FILHO, 2006).

Portanto, o direito de resposta se equipara ao instituto da legítima defesa, doutrinariamente falando. Entretanto, o processo para que o indivíduo que teve o seu direito violado exerça o seu condão de resposta é extremamente difícil, uma vez que a rede mundial de computadores não possui, em diversas situações, meios de imprensa que possam ser acionados a fim de garantir o respectivo direito. Em muitos casos, blogs hospedados em outros países, cujo conteúdo é feito por um usuário anônimo e que não pode ser rastreado, seja pelas barreiras impostas pelo caráter transnacional da internet ou até mesmo por programas de computador que visam dificultar esse tipo de identificação, muitas pessoas têm o seu direito de resposta sendo jogados no lixo.

Destaca-se também que, devido ao compartilhamento de conteúdo em massa, torna-se praticamente impossível para o lesionado exercer a sua defesa, ante o dano causado.

Com base no que fora exposto neste item, perfaz necessário mencionar o que fora dito por Alexandre Daoun, quanto ao avanço da internet - “os benefícios da modernidade e celeridade alcançados com a rede mundial trazem, na mesma proporção, a prática de ilícitos penais que vêm confundindo não só as vítimas como também os responsáveis pela persecução penal” (DAOUN, 2007).

2.3 A Finalidade das Informações Coletadas

Conforme já tratado neste capítulo, a rede mundial de computadores traz inúmeros benefícios aos usuários de todo o mundo, contudo, há alguns pontos negativos, principalmente no que concerne à coleta e comercialização de dados pessoais.

De início, destaca-se que informação sempre foi e, muito provavelmente, sempre será objeto de cobiça de entidade privadas e governamentais, dado a

importância que os dados coletados possuem. Entretanto, a coleta de dados não é algo novo, como muitos acreditam, uma vez que tal objetivo não se iniciou com a internet, sendo apenas impulsionado por essa.

É de comum conhecimento que diversos estabelecimentos comerciais, como pequenas mercearias de bairro das décadas de 80 e 90, possuíam livros de registros debaixo de balcões, contendo as informações de seus clientes, como o nome completo, endereço, telefone, se era um bom pagador ou não, ou seja, a coleta de dados já era existente e considerada uma prática comum entre os comerciantes. Contudo, a internet elevou esse patamar, principalmente o comércio on-line, popularmente conhecido como *e-commerce*.

Portanto, conforme já apontado, viver em sociedade atualmente, significa estar conectado e, estar conectado implica em dispor dados pessoais a terceiros e, o grande cerne da questão se baseia na finalidade que tais dados possuem. Viver uma vida conectada é absolutamente normal hoje em dia, uma vez que as pessoas carregam seus aparelhos celulares para todos os lados, contendo perfis em diversas redes sociais, aplicativos mensageiros e até mesmo, aplicativos de banco, que permite fazer pagamentos, transferências e recebimentos de dinheiro em tempo real, de forma imediata. Tudo isso gera informações de cunho pessoal, e tais dados se encontram dentro do campo protetivo da privacidade, sendo assim, digno de proteção.

Muitas vezes, a coleta de dados independe da permissão do usuário e, a exemplo disso, existe a ferramenta chamada *cookies* (biscoito – em tradução livre), que são pequenos arquivos criados por sites visitados e que são salvos no computador do usuário, por meio do navegador. Esses arquivos contêm informações que servem para identificar o visitante, seja para personalizar a página de acordo com o perfil ou para facilitar o transporte de dados entre as páginas de um mesmo site. *Cookies* são também comumente relacionados a casos de violação de privacidade na web (TECHTUDO, 2018).

De acordo com Reinaldo Themoteo, os *cookies* são um dos grandes responsáveis pelo chamado “rastro digital”, onde empresas armazenam uma enorme

quantidade de dados dos usuários que acessam a rede mundial de computadores todos os dias, sendo perfis e postagens, armazena também data e horário de conexão, dispositivos utilizados, informações acerca da rede utilizada na conexão, quantidade de cliques realizados, quais as informações publicitárias estavam amostra no momento de interação com o site ou aplicativo e, se tratando do *Facebook*, a coleta de informações vai além, incorporando ao arquivo digital que possuímos nessas empresas, dados como conversas, imagens, áudios, usuário que interagiram com determinada publicação, buscas realizadas, enfim, uma série de informações são obtidas a cada instante (THEMOTEO, 2015, p. 117).

Outrossim, empresas como a *Google* possuem informações acerca do usuário que muitos sequer sonham e, a exemplos disso, destaca-se que a empresa armazena todo o histórico de localização geoespacial do indivíduo, ou seja, onde quer que esse indivíduo tenha ido, portando o seu aparelho celular, a *Google* possui esse conhecimento, incluindo até mesmo a data, horário e o tempo que esse passou em determinado local, e sim, isso é extremamente assustador. Ademais, a mesma empresa armazena o históricos de pesquisas em seu buscador, histórico de visualização de vídeos no aplicativo *YouTube*, histórico de compras *on-line* a partir do *Gmail* e, o histórico de todos os sites acessados por meio do seu navegador *Google Chrome* (TECHTUDO, 2019).

Mas afinal, qual a razão de coletar tamanha quantidade de informações de usuários de todo o mundo? As empresas que fazem essa coleta geram fluxos financeiros? Pois os gastos para armazenar tantos dados devem ser exorbitantes. E sim, realmente a quantidade de informações armazenadas são absurdas, exigindo assim, enormes estrutura para armazenamento de dados, como as chamadas “fazendas de servidores” que a Google possui nos Estados Unidos e em outros países (TECMUNDO, 2016).

Todos esses dados são utilizados, principalmente para o que se entende no ramo da internet como “publicidade dirigida”, conforme bem colocado por Fabrício Germano Alves, que trata sobre a publicidade comportamental, isto é, a prática que consiste em direcionar anúncios publicitários específicos para determinados consumidores, de acordo com o seu comportamento *on-line* anterior, ou seja, é

destinada a um grupo, classe ou categoria de consumidores de acordo com uma base de dados a respeito dos mesmos elaborada a partir de interesses previamente demonstrados. Deste modo, os fornecedores conseguem cada vez mais alinhar seus anúncios publicitários em relação aos supostos interesses de seus destinatários. De fato, a prática em questão consiste em uma espécie de segmentação de mercado fundamentada em um critério comportamental (ALVES, 2016, p. 214).

Contudo, destaca-se que não são todos os sites que possuem a capacidade de coletar as informações de seus usuários, fazendo com que esse recorram às empresas que fazem essa captação. E acredite, atualmente existe um mercado mundial para compra e venda de informações acerca de indivíduos que acessam a rede mundial de computadores, movimentando mais de US$ 200 bilhões de dólares por ano, em todo o globo. Nesse sentido, os agentes que fazem a ponte entre as empresas que coletam dados e as que querem compra-los, são conhecidos no mercado internacional como *data brokers*, que em tradução livre, significa “corretores de dados” (REVISTA CONSTRUÇÃO, 2017).

Muitas dessas empresas são desconhecidas pela grande maioria das pessoas, dado que o único objetivo é coletar, vender ou comprar informações, não sendo necessário ser promovida ao público em geral. Portanto, esse é o principal destino dos dados coletados, visto que, conforme já fora dito neste capítulo, informação é algo extremamente valioso e muito disputado no mercado global.

CAPÍTULO III – PROBLEMAS SOCIAIS DO MUNDO DIGITAL

Tendo como base as inúmeras ocorrências acerca de problemas relacionados à internet, surgiu-se a necessidade de criar leis que visam a proteção dos usuários conectados à rede mundial de computadores. No Brasil, as principais legislações são: a Lei Carolina Dieckmann (Lei n. 12.737, de 30 de novembro de 2012), o Marco Civil da Internet (Lei n. 12.965, de 23 de abril de 2014) e a Lei Geral de Proteção de Dados (Lei n. 13.709, de 14 de agosto de 2018).

3.1 Legislações Nacionais e Internacionais Acerca da Proteção de Dados

Conforme já fora narrado, a rede mundial de computadores trouxe enormes benefícios aos cidadãos de todo o mundo, com avanços significativos em diversas áreas, o que possibilitou a troca de informações e conhecimento em larga escala. Contudo, a medida em que tais benefícios foram propiciados, alguns infortúnios foram surgindo, como as questões envolvendo a privacidade online, a liberdade de expressão e a segurança digital.

Nesse sentido, diversos países se movimentaram para criar leis que visam trazer proteção aos usuários da internet. A União Européia, por exemplo, implementou no dia 25 de maio de 2018 o Regulamento Geral de Proteção de Dados (GPDR, na sigla em inglês), que tem poder de afetar qualquer empresa ou usuário que tenha relações com o bloco europeu.

A GPDR é uma das leis de proteção de dados mais rígidas do mundo, e fora criada após as denúncias feitas pelo ex-agente da Agência Central de Inteligência (CIA – sigla em inglês) Edward Snowden em 2013, no qual revelou que os Estados Unidos da América promovia espionagem em massa de diversos países e que supostamente compartilhava informações com outras nações, como o Reino Unido (G1, 2013).

A lei de proteção de dados da União Européia traz diversas prerrogativas aos usuários da internet, como por exemplo, permitir que o indivíduo, em algumas situações, possa analisar, corrigir e até mesmo excluir informações que empresas guardam sobre ele. Ademais, a coleta de dados pessoais do usuário só podem ser feitas mediante consentimento explicito, além de dispor de linguagem acessível e simplificada, acerca da políticas de proteção de dados daquela empresa, bem como dos órgãos governamentais (JUSBRASIL, 2018).

Outro ponto importante se refere ao fato de que as empresas devem coletar apenas os dados necessários para o funcionamento do serviço prestado. E em caso de roubo dessas informações, comumente praticadas pelos *“hackers”*, essas empresas devem avisar os seus usuários afetados no prazo máximo de 72 horas, sob pena de multa no importe de 20 milhões de euros, ou 4% do volume global de negócios da empresa.

Destaca-se que a referida lei traz implicações diretas e indiretas a diversos países do mundo, incluindo o Brasil, visto que a lei é aplicada a qualquer empresa que venha a armazenar e manipular dados advindos do velho continente, e que tenha ligações com o bloco econômico, o que incluí principalmente, instituições financeiras sediadas fora da Europa.

A GPDR dispõe que alguns países podem ser enquadrados no que chamam de “Porto Seguro”, ou seja, são nações que possuem tratamento de dados equivalente ao praticado na Europa, podendo esses países manipular e armazenar dados advindos dos cidadãos europeus.

Lado outro, cumpre mencionar que a GPDR trouxe maior proteção aos dados de crianças e adolescentes, cuja finalidade é evitar a exposição exagerada de menores de idade na internet. A idade para utilização de aplicativos de rede sociais pode variar entre países do bloco. Contudo, visando se adequar, o Facebook estabeleceu que a idade mínima para que um indivíduo possa fazer uso do seu ecossistema de redes sociais passasse a ser de 16 anos em toda a Europa.

No Brasil, as legislações vigentes são relativamente mais antigas, se comparado a GPDR da União Européia, pouco fora tratado e aprofundado acerca da proteção de dados dos usuários. Conforme já mencionado, em 2012 entrou em vigor a primeira lei que tratou diretamente de crimes cibernéticos, bem como tipificou o crime de *hacker*, cuja penalidade é aplicada em razão da invasão de dispositivos eletrônicos, no qual o objetivo do invasor é obter informações pessoais de outrem, o que claramente é uma grave violação da privacidade alheia (BRASIL, 2012).

A Lei 12.737/2012 é popularmente conhecida como Lei Carolina Dieckmann, em razão de ter sido proposta após a divulgação de 36 fotos da atriz em situação de nudez na internet, em maio de 2012. Carolina recebeu ameaças de extorsão para que pagasse 10 mil reais para não ter as fotos publicadas na rede. Após denúncia feita pela mesma, a Polícia Civil constatou que cibercriminosos invadiram a caixa de e-mail de Carolina, por meio de um programa malicioso (malware), o que permitiu o acesso dos criminosos em seu dispositivo, que por sua vez efetuaram a cópia dos arquivos contendo fotos íntimas da atriz (G1, 2013).

Com base no infortúnio enfrentado pela atriz, foi adicionado ao Código Penal o artigo 154-A, que dispõe da seguinte redação:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:

> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

Outrossim, dado que a referida lei busca a proteção da vida privada do indivíduo, os parágrafos § 3° e § 4° do mesmo artigo, dispõe que:

> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
>
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
>
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.

Destaca-se que a Lei 12.737/2012 não tem como objetivo, apenas a proteção à pessoa física, mas alcança também a pessoa jurídica, uma vez que o § 3° traz em sua redação, questões que envolvem segredos comerciais e industriais, dado os vazamentos de projetos desenvolvidos no ramo empresarial, que acabam custando caro no “mercado negro”, embora ainda não haja uma legislação específica que aborde o tema (TERRA, 2021).

Portanto, a Lei Carolina Dieckmann foi a primeira legislação em território nacional, a abordar o tema da privacidade na internet, inserindo no ordenamento jurídico a tipificação do crime de *hacking*, termo em inglês, utilizado para identificar atividades que visam o acesso ilegal de dispositivos conectados ou não à rede e, em alguns casos, no roubo de informações pessoais do indivíduo.

Contudo, a necessidade de leis mais abrangentes e que visam maior proteção aos usuários persistiu, principalmente após as divulgações feitas por Edward Snowden no ano de 2013, conforme já fora narrado anteriormente. Sendo assim, a então Presidente da República, Dilma Rousseff, sancionou em abril de

2014 a Lei 12.965, popularmente conhecida como Marco Civil da Internet, cujo objetivo se baseia em estabelecer princípios, garantias, direitos e deveres para o uso da internet no Brasil (G1, 2014).

O Marco Civil da Internet foi uma dos maiores avanços jurídicos do Brasil, e principalmente, no que se refere aos direitos do indivíduo, ante a rede mundial de computadores, algo que fora destacado por Sir Tim Berners-Lee, apontado como o criador da internet na qual conhecemos hoje. Em suas palavras, Tim afirmou que se o Marco Civil for aprovado, sem maiores adiamentos ou modificações, este seria possivelmente o melhor presente de aniversário para os usuários de internet do Brasil e do mundo. Eu espero que, aprovando esta lei, o Brasil fixe sua orgulhosa reputação como um líder mundial em democracia e progresso social e ajude a inaugurar uma nova era, uma onde os direitos dos cidadãos em todos os países do mundo são protegidos por leis de direito digitais (WORLD WIDE WEB FOUNDATION, 2014).

O principal objetivo da citada lei, é garantir plena proteção aos direitos já tratados anteriormente neste trabalho, sendo garantido, primeiramente, pela Constituição Federal, são eles: o direito à privacidade, à liberdade de expressão e a proteção dos dados pessoais, já sendo discriminados no artigo 3°, incisos II e III. Todavia, a lei pouco tratou acerca da proteção de dados, conforme asseverou Teixeira (2016).

A liberdade de expressão fora bem pontuada em seu artigo 2° e seus incisos, destacando a pluralidade e a diversidade de ideias, bem como na finalidade social da internet.

Logo em seguida, o Marco Civil da Internet, em seu artigo 7°, é garantido pelo menos 3 importantes direitos relacionados a privacidade, são eles: a inviolabilidade da intimidade e da vida privada; a inviolabilidade e sigilo do fluxo de suas comunicações pela internet; e a inviolabilidade e sigilo de suas comunicações

privadas armazenadas. Deve-se destacar que esses dois últimos direitos podem ser quebrados por ordem judicial. Desse modo, Teixeira (2016, p. 69) assevera que:

> Assim como nas questões fiscais, bancárias, etc. o fluxo das comunicações pela internet são sigilosas e invioláveis. Nestes casos, apenas por ordem judicial, conforme a legislação a ser editada, poderá decretar a quebra do sigilo das comunicações eletrônicas estabelecidas pela internet.

Nesse sentido, cumpre ressaltar que o direito à privacidade não é absoluto, uma vez que, dentro do devido processo legal, direitos como o sigilo de comunicação via internet podem ser quebrados. Não obstante, o artigo 7°, incisos VII, VIII, IX e X, aborda também, direitos relacionados ao tratamento de dados no Brasil, contudo, reitera-se que não houve o devido aprofundamento neste quesito, vindo a ser tratado posteriormente por meio da Lei 13.709/2018.

E, conforme já narrado neste trabalho, o legislador demonstrou enorme preocupação na elaboração do Marco Civil da Internet, uma vez que o objetivo principal foi, mais uma vez, reiterar o direito à privacidade e à liberdade de expressão que o cidadão, usuário da rede mundial de computadores tem à sua disposição. O artigo 8°, traz em seu caput essa afirmação, ao dizer que “a garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet” (Brasil, 2014).

Nesse sentido, com base no artigo supra, asseverou a Academia Brasileira de Direito do Estado – ABDET (2015, p. 10):

> Os provedores responsáveis deverão proteger os registros, dados pessoais e as comunicações privadas dos usuários, cuja finalidade é a preservação da intimidade, da privacidade, da honra e da imagem dos usuários, sendo que a divulgação de tais informações se dará apenas através de ordem judicial, ressalvada a possibilidade das autoridades administrativas obterem os dados cadastrais, na forma da lei

Ademais, destaca-se que no mesmo artigo, em seu parágrafo único, restou estabelecido que qualquer contrato firmado entre um prestador de serviços ligados à internet e um usuário, não podem dispor de cláusulas que violem o caput, tampouco os incisos I e II, no qual dispõem da seguinte redação:

> Art. 8° (...)
>
> I - impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet; ou
>
> II - em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil.

Quanto à quebra do sigilo de comunicações, autorizada mediante ordem judicial, o artigo 22 traz pontos extremamente relevantes que devem ser observados, para que tal quebra possa der deliberada, uma vez que não se trata de mera requisição de informações pessoais, conforme se extrai do parágrafo único e seus incisos, bem como da determinação expressa no artigo 23, na qual dispõe que o juiz deverá tomar todas as providências necessárias, a fim de garantir o sigilo dos dados recebidos (BRASIL, 2014).

Outro ponto a ser destacado, refere-se ao tratamento de dados em solo nacional, nos moldes do que ocorre na União Européia, por meio da já citada lei GPDR. O artigo 11 destaca que “em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros” (BRASIL, 2014).

Portanto, a fim de que possa ser observado o devido cumprimento ou não da legislação, os provedores de conexão deverão dispor de ferramentas que permita

que o Poder Público exerça o múnus da fiscalização, podendo assim trazer maior segurança aos usuários.

Outrossim, o Marco Civil da Internet trouxe ao ordenamento jurídico brasileiro, o chamado “Controle Parental”, permitindo aos pais e/ou responsáveis por menores de idade, a prerrogativa de controlar o que seus filhos podem ou não acessar. A ferramenta é bastante conhecida em aparelhos celulares, *tablets* e *video games*, visto que tais dispositivos são, em muitos casos, destinados à crianças e adolescentes. Vejamos a redação do artigo 29 da lei:

> Art. 29. O usuário terá a opção de livre escolha na utilização de programa de computador em seu terminal para exercício do controle parental de conteúdo entendido por ele como impróprio a seus filhos menores, desde que respeitados os princípios desta Lei e da Lei nº 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente.

Por último, o tratamento de dados é regulamentado principalmente pela Lei 13.709/2018, conhecida por Lei Geral de Proteção de Dados (LGPD), que será devidamente abordada no tópico seguinte.

3.2 Tratamento de Dados Coletados no Brasil e no Mundo

Conforme já fora demonstrado no tópico anterior, o tratamento de dados em grande parte do mundo, segue o que se encontra disposto na GPDR, da União Européia, dado o imenso número de países que possui relações comerciais com o bloco europeu. No que se refere à maior potência mundial, os Estados Unidos da América, por mais incrível que possa parecer, esse país não possui uma legislação específica e aprofundada que trate acerca desse tema.

Contudo, cumpre mencionar que isso não significa que a nação mais poderosa do mundo não possua leis que tratem do tema, pois as legislações

americanas apenas regulamentam o uso de determinados tipos de dados ou regulamentam alguns setores, como o de saúde, telecomunicações e financeiro. Destaca-se que, como nos Estados Unidos, os estados da federação possuem autonomia de criar suas próprias leis, e alguns acabam dispondo de códigos mais abrangentes do que outros, como é o caso da Califórnia, que possui leis mais rígidas, quando o assunto é privacidade.

Para melhor elucidação, as legislações federais presentes nos Estados Unidos são: *Driver's Privacy Protection Act* (DPPA), que define uma série de regras que os departamentos estaduais de veículos devem seguir, ao manipular dados dos cidadãos; *Children's Online Privacy Protection Act* (COPPA), que regulamenta a coleta de dados de crianças e adolescentes; a *Fair Credit Reporting Act* (FCRA), que trata acerca da manipulação de dados coletados por meio do comercio digital, dentre outras leis menores (GATEFY, 2021).

Quanto ao tratamento de dados no Brasil, esse veio a ser regulamentado pela Lei 13.709/2018, na qual recebeu o título de Lei Geral de Proteção de Dados, entrando em vigor no dia 14 de agosto de 2020, e tendo sido sancionada 24 meses antes, pelo então Presidente da República, Michel Temer. A legislação possui ao todo 65 artigos, que foram amplamente discutidos, tendo inclusive, a participação da sociedade na elaboração da lei (BRASIL, 2018).

A referida lei, surgiu da necessidade de regulamentar a forma na qual empresas que se utilizam da tecnologia associada à internet, coletam, manipulam e armazenam os dados fornecidos pelos usuários da rede mundial de computadores. Conforme já tratado no primeiro capitulo deste trabalho, os dados gerados pelos usuários são de extrema relevância para as grandes corporações, uma vez que são utilizados das mais diversas formas possíveis, gerando lucros cada vez maiores. Ademais, a maioria dessas empresas, são comandadas pelos homens mais ricos do planeta. Bioni (2018), ao tratar sobre o assunto, asseverou:

> Com a inteligência gerada pela ciência mercadológica, especialmente quanto a 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.

Outro ponto a ser lembrado, refere-se a publicidade direcionada, onde cada usuário possui o seu *"profiling"*, que pode ser traduzido como perfil, onde são geradas classificações e segmentações das preferências, das tendências ideológicas e até mesmo do histórico de compras dos usuários, algo que é muito bem explorado pelas empresas de tecnologia, visto que o lucro dessas gigantes são baseados, principalmente, em publicidade. Dessa forma, Bioni (2018) vai além, ao dizer que:

> Os dados pessoais de um indivíduo formam um perfil a seu respeito para a tomada de inúmeras decisões. […]. Na famosa expressão de Eli Pariser, há uma bolha que, como um filtro invisível, direciona desde a própria interação do usuário com outras pessoas em uma rede social até o acesso e a busca por informação na rede. Doutrina-se a pessoa com um conteúdo e uma informação que giram em torno dos interesses inferidos por intermédio dos seus dados, formando-se uma bolha que impossibilita o contato com informações diferentes […].

Sendo assim, conforme apontado por Bioni acima, até mesmo a informação que chega ao usuário pode ser direcionada, o que acaba levantando a questão da liberdade de informar e de ser informado, visto que se o usuário não pode controlar uma notícia que chega a ele, por exemplo, conclui-se que esse pode estar inserido numa "bolha social". A coleta de dados ocasiona esse tipo de situação, uma vez que o profiling do titular direciona de forma específica, conteúdos que serão exibidos de acordo com aquele perfil, e essas informações podem ser de cunho publicitário, notícias, conteúdo político-ideológico, dentre outros.

Mas nem só de prejuízo vive esse modelo, visto que os maiores beneficiários dessa empreitada são as grandes empresas no ramo da tecnologia e publicidade, uma vez que os custos para direcionar propagandas àqueles que

realmente possuem interesse no produto, são menores, dado que ela será focada em determinado público, não sendo difundida de forma ampla (PONTICELLI, 2018).

Bioni (2018) e Toscano (2017), afirmam que esse modelo atual explica o fato de que a grande maioria dos conteúdos disponíveis na rede mundial de computadores são “gratuitos”, fugindo do padrão tradicional de consumo onde uma prestação pecuniária é trocada por um serviço ou produto. Aqui, o produto é o usuário, e a sua contraprestação pelos serviços disponibilizados é o fornecimento de seus dados.

Voltando a tratar acerca da Lei Geral de Proteção de Dados, observa-se que o primeiro artigo aborda exatamente aquilo que já fora tratado nesta monografia, qual seja, a proteção dos direitos fundamentais de liberdade e de privacidade.

Logo adiante, o artigo 2°, inciso I, destaca como primeiro fundamento desta legislação, o “respeito à privacidade”, em seguida, por meio do inciso III, ressalta “a liberdade de expressão, de informação, de comunicação e opinião” e “a inviolabilidade da intimidade, da honra e da imagem”, em seu inciso IV. Nota-se que em apenas um artigo, fora abrangido os principais direitos individuais, concernentes à privacidade e à liberdade.

Quanto ao artigo 5° da Lei Geral de Proteção de Dados, verifica-se que o legislador demonstrou clara preocupação no que são considerados dados e quais são os seus tipos, a fim de que a tutela jurisdicional, referente a tais informações, seja devidamente prestada por parte do Estado.

Cumpre destacar que o artigo citado prevê uma distinção entre “dados pessoais” e “dados pessoais sensíveis”, contudo, as características elencadas em cada um possui caráter amplo. Nesse sentido, Bioni (2018), informa que “os dados sensíveis são uma espécie de dados pessoais que compreendem uma tipologia diferente em razão de o seu conteúdo oferecer uma especial vulnerabilidade:

discriminação”. Por tais motivos, a legislação supra busca trazer maior proteção a esses tipos de dados.

Logo em seguida, o inciso X do artigo 5°, traz em sua redação, o que vem a ser o significado de “tratamento de dados”, nos termos da lei, vejamos:

> 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;

Outrossim, é sabido que a LGPD veio para proteger pessoas físicas e jurídicas, contudo, dando continuidade na análise do artigo 5°, nota-se que a lei trouxe as definições das pessoas envolvidas nessa relação, quais sejam, os titulares, os controladores, operadores, encarregados e os chamados “agentes de tratamento de dados”, vejamos:

> 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;

Assim sendo, ao colocarmos no campo prático, podemos concluir que os usuários de uma rede social, por exemplo, são os titulares dos dados, enquanto a empresa proprietária da plataforma é a controladora, tendo como funcionários os operadores e encarregados de dados, que seriam os agentes de tratamento descrito no inciso IX do artigo 5°.

Um dado de extrema relevância trazido por Bioni (2018), refere-se ao uso da palavra “consentimento”, que aparece 35 vezes ao decorrer dos 65 artigos da lei. O termo foi invocado pela primeira vez no inciso XII do artigo 5° da LGPD, ao deixar expresso o que vem a ser o consentimento, por parte do usuário, vejamos:

> XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

Não obstante ao dado levantado por Bioni (2018), esse ainda afirma que o instituto do consentimento possui um centro gravitacional no indivíduo, que:

> [...] grande parte dos princípios tem todo o seu centro gravitacional no indivíduo: a) de um lado, princípios clássicos, como a transparência, a especificação de propósitos, de acesso e qualidade de dados por meio do quais o titular do dado deve ser munido com informações claras e completas sobre o tratamento de seus dados e, ainda, ter acesso a eles para, eventualmente, corrigi-los; b) de outro lado, princípios mais “modernos”, como adequação e necessidade, em que o tratamento dos dados deve corresponder às legítimas expectativas do seu titular. Isso deve ser perquirido de acordo com a finalidade especificada para o tratamento dos dados, assegurando-se que os dados sejam pertinentes, proporcionais e não excessivos.

Até aqui, foi discutido os direitos tutelados pela Lei Geral de Proteção de Dados, bem como acerca do que vem a ser dados pessoais, passando ainda pelos titulares de tais informações. Nesse sentido, resta tratar a respeito do tratamento dos dados coletados no Brasil, visto que esse é o principal ponto trazido pela referida lei.

O artigo 6° da LGPD traz as observações que deverão ser feitas pelos agentes de tratamento de dados, tendo como princípio base a boa-fé (BRASIL, 2018).

Cumpre ressaltar que a Lei Geral de Proteção de Dados, dispõe que deverá haver uma finalidade para o tratamento dos dados em território nacional, bem como deverá ser feito de forma adequada ao contexto no qual os dados estão inseridos. Ademais, com base no inciso III, os dados deverão ser tratados de forma limitada, devendo ser observado o mínimo necessário para a realização de suas finalidades (BRASIL, 2018).

Outro ponto a ser destacado, refere-se ao princípio do livre acesso garantido aos titulares dos dados, devendo a consulta ser feita de forma simplificada e gratuita, não podendo o agente de tratamento impor quaisquer empecilhos ao titular, conforme inciso IV, o que naturalmente incorre no inciso VI, no qual trata acerca do princípio da transparência de dados (BRASIL, 2018).

Dando seguimento, o artigo seguinte afirma que os dados coletados só poderão ser alvos de manipulação, mediante as hipóteses descritas em seus incisos, vejamos:

> 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.

Novamente, destaca-se o consentimento do titular, quanto ao fornecimento dos dados. Outrossim, o inciso III da LGPD garante a administração pública, o direito de tratar e compartilhar dados dos cidadãos, necessários a execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres (BRASIL, 2018).

Ademais, tendo em vista que muitos estudos são realizados por diversas instituições, incluindo universidades, o inciso IV trouxe previsão legal, quanto ao uso de dados pessoais na elaboração de pesquisas que envolvem a sociedade civil, desde que os dados pessoais estejam em condição de anonimato, sempre que possível (BRASIL, 2018).

Voltando a tratar do princípio do livre acesso, o artigo 9° da LGPD traz uma série de observações acerca desse direito garantido ao titular dos dados.

Todavia, mesmo com tantas garantias previstas na Lei Geral de Proteção de Dados, ainda ocorre no Brasil inúmeros vazamentos de dados, sendo alguns mais danosos do que outros. Um dos mais recentes vazou quase 400 mil chaves Pix, que estavam sob a guarda e a responsabilidade do Banco do Estado do Sergipe, o que acaba facilitando a aplicação de golpes por parte de pessoas mal intencionadas (CNN, 2021).

Nesse sentido, a LGPD traz em seu capítulo VII, alguns institutos fundamentais relacionados à efetiva aplicação da tutela jurisdicional do Estado, quanto a proteção dos dados pessoais dos cidadãos residentes no Brasil. Os artigos 46 e seguintes tratam acerca da segurança e do sigilo dos dados coletados.

Com base na lei, o artigo 46 afirma que os agentes de tratamento deverão adotar medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição e perda. Já o artigo 47 prevê que, independentemente de quem manipula os dados armazenados, obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término (BRASIL, 2018).

Em caso de vazamento de dados, o artigo 48 da LGPD destaca que o controlador deverá comunicar a autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, devendo ser feita em prazo razoável, além de mencionar, no mínimo, a descrição da natureza dos dados pessoais afetados, bem como as informações sobre os titulares envolvidos e os riscos relacionados ao incidente (BRASIL, 2018).

Por último, destaca-se que os dados coletados não ficarão necessariamente armazenados para sempre, uma vez que, no caso de uma instituição financeira, por exemplo, o titular dos dados pode encerrar o seu vínculo com a empresa, o que não perfaz mais necessário o armazenamento dessas

informações pessoais. Sendo assim, os artigos 15 e 16 dispõem acerca do término do tratamento de dados, vejamos:

Portanto, nos termos da lei, após alcançada a finalidade, os dados armazenados deixam de ser necessários, devendo o controlador eliminá-los, observando os limites técnicos das atividades vinculadas ao titular (BRASIL, 2018).

3.3 Desafios do Mundo Conectado

Conforme fora exposto ao decorrer de toda monografia, os avanços da rede mundial de computadores trouxeram e ainda trazem inúmeros benefícios à sociedade como um todo. Todavia, a medida em que o desenvolvimento de novas tecnologias, sejam elas físicas, podendo ser tocadas ou virtuais, perfaz necessário o acompanhamento por parte do Estado, a fim de que sejam garantidos os direitos fundamentais aos usuários da internet, como o direito à privacidade e à liberdade de expressão, garantidos no artigo 5°, incisos X e IX da Constituição Federal (BRASIL, 1988).

Quanto aos desafios a serem enfrentados por outras nações, como os Estados Unidos da América que, conforme mencionado anteriormente, não possui legislação específica acerca da Proteção de Dados, já se encontra em discussão no congresso do país, uma lei federal que alcance de forma unitária todo o solo norte-americano (GATEFY, 2021).

Atualmente, se discute bastante quanto a criação de softwares que garantam maior segurança, ante o vazamento de dados pessoais. Empresas como Google, Microsoft e Facebook buscam avanços na área de segurança digital, tendo em vista o crescente número de ataques cibernéticos em todo o globo (TECMUNDO, 2020).

Outro ponto comumente levantado, se pauta em relação à influência das redes sociais e da internet como um todo em eleições políticas de diversos países. O caso, possivelmente mais famoso desse tipo de poder de redes como o Facebook, foi o da assessoria britânica Cambridge Analytica, que trabalhou para a campanha eleitoral do ex-presidente americano Donald Trump.

A empresa admitiu que utilizou um aplicativo para coletar informações privadas de 87 milhões de norte-americanos, sem autorização ou conhecimento por parte dos usuários. À época, conforme noticiado pelo G1 (2019), jornais como o The New York Times e o The Guardian afirmaram que os dados coletados foram usados sem o consentimento dos cidadãos pela Cambridge Analytica. A empresa de análise de dados acessou esse grande volume de informações após um teste psicológico que circulou na rede social. Os dados recolhidos não eram apenas os de usuários que fizeram o teste, mas também os de seus amigos.

Assim sendo, toda informação coletada foi utilizada para influenciar na campanha eleitoral do então presidente dos Estados Unidos da América. O escândalo foi tamanho que, a consultoria fechou as portas e o Facebook enfrenta diversos problemas judiciais. Ademais, a empresa teve de mudar a sua política de privacidade, e de segurança on-line a fim de que programas de computadores como o que fora utilizado pela Cambridge Analytica, não venham coletar dados pessoais como havia ocorrido (G1, 2019).

Portanto, os principais desafios atualmente, é garantir a privacidade, a liberdade de expressão e a segurança virtual dos usuários de todo o mundo, bem como buscar a garantia do direito de informar e de ser informado. Outrossim, busca-se evitar com que dados caiam nas mãos de empresas como a citada acima, dirimindo a influência em pesquisas eleitorais, a fim de que seja garantido o pleno exercício da democracia. A internet é uma das ferramentas mais fascinantes já criada pelo homem, tendo aberto inúmeras portas para diversos usuários de todo o globo.

CONCLUSÃO

De início, destaca-se que o presente trabalho monográfico teve como principal objetivo, a análise da legislação vigente no Brasil, tendo como advento, os direitos constitucionais dos cidadãos, quais sejam: o direito à privacidade, à liberdade de expressão e na segurança de cada indivíduo.

O exame aqui realizado, permitiu maior compreensão acerca da resposta do Poder Legislativo, em relação ao avanço da internet no Brasil, tendo elaborado as Leis Carolina Dieckmann (Lei 12.737, de 30 de novembro de 2012), o Marco Civil da Internet (Lei 12.965, de 23 de abril de 2014), e a Lei Geral de Proteção de Dados (Lei 13.709, de 14 de agosto de 2018).

Ademais, fora destacado os pontos da GPDR, lei de proteção de dados da União Européia, que trazem consequências diretas e indiretas ao Brasil e demais países que possuem relações como o bloco europeu.

Destaca-se que o objetivo desta monografia fora a busca quanto à proteção e garantia dos direitos constitucionais aqui mencionados, uma vez que, conforme já tratado, o avanço da rede mundial de computadores trouxe inúmeros benefícios aos usuários de todo o globo, ao mesmo passo em que desafios foram surgindo, tendo como principal direito a ser tutelado, o da privacidade.

Nesse sentido, verifica-se que que ainda existem obstáculos a serem superados, devendo as autoridades de cada país monitorar as novas ferramentas

que surgem todos os dias, cujo objetivo é ferir a liberdade alheia, causando-lhe prejuízos.

REFERÊNCIAS BIBLIOGRÁFICAS

ACADEMIA BRASILEIRA DE DIREITO DO ESTADO – ABDET. **Comentários ao Marco Civil da Internet.** Disponível em: <http://abdet.com.br/site/wp-content/uploads/2015/02/MCIABDET..pdf>. Acesso em: 5 de outubro de 2021.

AGÊNCIA BRASIL. **Brasil tem 134 milhões de usuário de internet, aponta pesquisa.** Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2020-05/brasil-tem-134-milhoes-de-usuarios-de-internet-aponta-pesquisa>. Acesso em: 24 de maio de 2021.

ALVES, Fabrício Germano. **Análise da possibilidade de regulação da publicidade comportamental pelo microssistema consumerista**. Brasília: Revista de Direito, Globalização e Responsabilidade nas Relações de Consumo, 2016.

BARROS FILHO, Clóvis de. ***Liberdade de imprensa: da utopia à tirania*.** Revista da ESPM, vol. 12, ano 11, edição n. 5. São Paulo: ESPM. DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006.

BBC. **QAnon: como e por que grupos ligados a teoria da conspiração estão se multiplicando na América Latina.** Disponível em <https://www.bbc.com/portuguese/internacional-53980307>. Acesso em: 31 de agosto de 2021.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoas –** A Função e os Limites do Consentimento. São Paulo: Editora Forense, 2018.

BRASIL, LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012. **Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências,** Brasília, DF, 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 1 de outubro de 2021.

BRASIL, LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. **Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet),** Brasília, DF, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-_2018/2018/Lei/L13709.htm> Acesso em: 12 de outubro de 2021.

BRASIL. **Constituição da República Federativa do Brasil de 1988,** Brasília, DF, 1988. Disponível em:

<http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 1 de outubro de 2021.

BRASIL. LEI Nº 12.965, DE 23 DE ABRIL DE 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**, Brasília, DF, abril 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 4 de outubro de 2021.

BRASIL. LEI Nº 12.965, DE 23 DE ABRIL DE 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**, Brasília, DF, abril 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 11 de outubro de 2021.

CETAX. **Big Data: o que é, conceito e definição.** Disponível em: <https://www.cetax.com.br/blog/big-data/>. Acesso em: 18 de maio de 2021.

CNN. **Banco Central comunica o 1° vazamento de dados cadastrais do Pix**. Disponível em: <https://www.cnnbrasil.com.br/business/banco-central-comunica-1o-vazamento-de-dados-cadastrais-do-pix/>. Acesso em: 19 de outubro de 2021.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006.

ECONOMIA UOL. **PIX: o que é e como funciona o novo sistema de pagamentos feitos pelo BC.** Disponível em: <https://economia.uol.com.br/guia-de-economia/oque-e-pix-tudo-sobre-o-novo-sistema-de-pagamentos.htm>. Acesso em: 29 de maio de 2021.

FOLHA DE S. PAULO. **Cuba derruba internet para evitar novos protestos organizados por redes sociais.** Disponível em < https://www1.folha.uol.com.br/mundo/2021/07/cuba-derruba-internet-para-evitarnovos-protestos-organizados-por-redes-sociais.shtml>. Acesso em: 1 de setembro de 2021.

FOLHA DE S. PAULO. **Neymar cobra R$ 2,7 milhões por post no Instagram, e Caio Castro R$ 617 mil; veja lista.** Disponível em: <https://f5.folha.uol.com.br/celebridades/2020/03/neymar-cobra-r-3-milhoes-por-postno-instagram-e-caio-castro-r-600-mil-veja-lista.shtml>. Acesso em: 8 de maio de 2021.

G1. **Cambridge Analytica se declara culpada em caso de uso de dados do Facebook.** Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2019/01/09/cambridge-analytica-se-declara-culpada-por-uso-de-dados-do-facebook.ghtml>. Acesso em: 19 de outubro de 2021.

G1. **Dilma sanciona o Marco Civil da Internet na abertura da NETMundial.** Disponível em: <http://g1.globo.com/tecnologia/noticia/2014/04/netmundial-inicia-com-obrigado-snowden-e-defesa-da-internet-livre.html>. Acesso em: 11 de outubro de 2021.

G1. **Entenda o caso de Edward Snowden, que revelou espionagem dos EUA**. Disponível em <http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html>. Acesso em: 29 de setembro de 2021.

G1. **Golpes no PIX: Febraban dá dicas para evitar cair nos principais.** Disponível em: <https://g1.globo.com/economia/pix/noticia/2021/02/24/golpes-no-pix-febrabanda-dicas-para-evitar-cair-nos-principais.ghtml>. Acesso em: 6 de maio de 2021.

G1. **Instagram faz 10 anos como uma das maiores redes sociais do mundo e de olho no TikTok, para não envelhecer.** Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2020/10/06/instagram-faz-10anoscomo-uma-das-maiores-redes-sociais-do-mundo-e-de-olho-no-tiktok-para-naoenvelhecer.ghtml>. Acesso em: 19 de maio de 2021.

G1. **Lei 'Carolina Dieckmann', que pune invasão de PCs entra em vigor.** Disponível em: <http://g1.globo.com/tecnologia/noticia/2013/04/lei-carolina-dieckmann-que-pune-invasao-de-pcs-passa-valer-amanha.html>. Acesso em: 9 de outubro de 2021.

G1. **Pandemia aumenta o uso de internet no planeta.** Disponível em: <https://g1.globo.com/pr/parana/especial-publicitario/novadc/check-in-tech-novadc/noticia/2020/11/30/pandemia-aumenta-o-uso-de-internet-no-planeta.ghtml>. Acesso em: 8 de maio de 2021.

GATEFY. **Como funcionam as leis de proteção de dados nos Estados Unidos.** Disponível em: <https://gatefy.com/pt-br/blog/como-funcionam-leis-protecao-dados-estados-unidos/>. Acesso em: 11 de outubro de 2021.

JUSBRASIL. **Lei da União Europeia que protege dados pessoais entra em vigor e atinge todo o mundo; entenda.** Disponível em: <https://examedaoab.jusbrasil.com.br/noticias/582408026/lei-da-uniao-europeia-que-protege-dados-pessoais-entra-em-vigor-e-atinge-todo-o-mundo-entenda>. Acesso em: 9 de outubro de 2021.

MAGRANI, Eduardo. **A Internet das Coisas.** Rio de Janeiro: FGV Editora, 2018.
MARQUESONE, Rosangela. **Big Data – Técnicas e Tecnologias para extração de valor de dados.** São Paulo: Editora Casa do Código, 2016.

MEYER, Philip. (1987). ***A Ética no Jornalismo***. Rio: Ed. Forense Universitária. BARRETO, Alex Muniz. ***Curso de Direito Constitucional.*** 3ª ed. Lemes/SP: EDIJUR, 2019.

MORAES, Alexandre. ***Constituição do Brasil interpretada e legislação constitucional***. 6ª ed. São Paulo: Atlas, 2006.

ORGÂNICA. **Marketing Digital em 2021: o que é e como funciona**. Disponível em: <https://www.organicadigital.com/blog/afinal-como-funciona-o-marketing-digital/>. Acesso em: 16 de maio de 2021.

Organização dos Estados Americanos, **Convenção Americana de Direitos Humanos** ("Pacto de San José de Costa Rica"), 1969.

PONTICELLI, Murilo Meneghel. **O direito fundamental à privacidade no âmbito da rede mundial de computadores com o advento da lei geral de proteção de dados**. Universidade do Sul de Santa Catarina. Tubarão – SC, 2018.

REVISTA CONSTRUÇÃO. **Na indústria dos dados pessoais o produto é você**. Disponível em <http://revistaconstrucao.org/economia-digital/na-industria-dos-dadospessoais-o-produto-e-voce/>. Acesso em 5 de setembro de 2021.

RNP. **Nossa história**. Disponível em: < https://www.rnp.br/sobre/nossa-historia >. Acesso em: 24 de maio de 2021.

SILVA, Gabriela Massa Bezerra da; DAOLIO, Raquel Pinton Geraldino. **A importância da internet como ferramenta estratégica para o negócio da empresa.** Revista Gestão em Foco, Amparo-SP, ed. 9, p. 132-137, 2017.

TECHTUDO. **Amazon Echo Dot.** Disponível em: <https://www.techtudo.com.br/tudo-sobre/amazon-echo-dot.html>. Acesso em: 22 de maio de 2021.

TECHTUDO. **O que são cookies? Entenda os dados que os sites guardam sobre você.** Disponível em <https://www.techtudo.com.br/noticias/2018/10/o-quesao-cookies-entenda-os-dados-que-os-sites-guardam-sobre-voce.ghtml>. Acesso em: 2 de setembro de 2021.

TECHTUDO. **Seis coisas que o Google sabe sobre você – e como apagar**. Disponível em: <https://www.techtudo.com.br/listas/2019/06/seis-coisas-que-ogoogle-sabe-sobre-voce-e-como-apagar.ghtml>. Acesso em: 2 de setembro de 2021.

TECMUNDO. **Conheça a estrutura monstruosa utilizada pela Google para seus**

servidores. Disponível em: <https://www.tecmundo.com.br/google/104430-conhecaestrutura-monstruosa-utilizada-google-servidores.htm>. Acesso em: 18 de maio de 2021.

TECMUNDO. **Conheça a estrutura monstruosa utilizada pela Google para seus servidores.** Disponível em <https://www.tecmundo.com.br/google/104430-conhecaestrutura-monstruosa-utilizada-google-servidores.htm>. Acesso em 2 de setembro de 2021.

TECMUNDO. **Privacidade de dados: o que CEOs de grandes empresas tem a dizer**. Disponível em: <https://www.tecmundo.com.br/mercado/149750-privacidade-dados-ceos-grandes-empresas-tem-dizer.htm>. Acesso em: 19 de outubro de 2021.

TECNOBLOG. **Sem busão: as entrevistas de emprego online na pandemia**. Disponível em: <https://tecnoblog.net/362814/sem-busao-as-entrevistas-deemprego-online-na-pandemia/>. Acesso em: 8 de maio de 2021.

TECNOBLOG. **Sony está testando carro elétrico Vision-S em estradas da Europa.** Disponível em: <https://tecnoblog.net/401410/sony-esta-testando-carroeletrico-vision-s-em-estradas-da-europa/>. Acesso em: 16 de maio de 2021.

TEIXEIRA, Tarcísio. **Marco Civil da Internet Comentado.** São Paulo: Almedina Brasil, 2016.

TERRA. **Ministros do STJ participam de evento que discute a importância de legislação específica para proteger segredos de negócio.** Disponível em: <https://www.terra.com.br/noticias/dino/ministros-do-stj-participam-de-evento-que-discute-importancia-de-legislacao-especifica-para-proteger-segredo-de negocio,e04e54bc1ab7926ba81f803035893139oaxrlh4k.html>. Acesso em: 11 de outubro de 2021.

THEMOTEO, Reinaldo J. **Internet e sociedade.** Rio de Janeiro: Fundação Konrad Adenauer, 2015.

TODAMATÉRIA. **História da Internet**. Disponível em: < https://www.todamateria.com.br/historia-da-internet/>. Acesso em: 24 de maio de 2021.

TODAMATÉRIA. **Redes Sociais**. Disponível em: <https://www.todamateria.com.br/redes-sociais/>. Acesso em: 24 de maio de 2021.

TORRES, Claudio, 2009. **A Bíblia do marketing digital: tudo o que você queira saber sobre marketing e publicidade na internet e não tenha a quem perguntar.** São Paulo: Novatec Editora, 2009.

TOSCANO, Marcos. **Na indústria dos dados pessoais o produto é você**. Rio de Janeiro: Revista Construção, 2017.

WORLD WIDE WEB FOUNDATION. **Marco Civil: Statement of Support from Sir Tim Berners-Lee.** Disponível em: <https://webfoundation.org/2014/03/marco-civil-statement-of-support-from-sir-tim-berners-lee/>. Acesso em: 4 de outubro de 2021.