LEI GERAL DE PROTEÇÃO DE DADOS EM UMA REALIDADE CONECTADA

("LEI GERAL DE PROTEÇÃO DE DADOS" IN A CONNECTED REALITY)

*Ana Clara Alves Rocha**
*Andressa Alves Menezes***
*Andressa Lobato Guimarães****
*Arthur Miguel Alves do Santos*****
*Letícia Medeiros Vieira Sorrequia******

Resumo: O presente artigo visa traçar a trajetória jurídica da proteção de dados no Brasil, especialmente no campo das redes sociais, a partir de uma análise do desenvolvimento das mídias digitais, que se encontram cada vez mais enraizadas na realidade contemporânea. Assim, se discute a efetividade das normas de proteção de dados, mais especificamente a Lei Geral de Proteção de Dados Pessoais (LGPD) e seu impacto na democracia representativa e no capitalismo de vigilância, levando em conta também sua atuação no caso dos novos crimes digitais.

Palavras-Chave: Proteção de Dados. Democracia. Mídias digitais. Crimes digitais. Inteligência Artificial.

*** Graduanda da 1ª fase do curso de Direito da Universidade Estadual da Paraíba.**
Currículo lattes: https://wwws.cnpq.br/cvlattesweb/PKG_MENU.menu?f_cod=430E028D0A5C7EBB643EE-C0BBCFAC69D# ; E-mail: anaclaraar16@gmail.com

**** Graduanda da 4ª fase do curso de Direito da Universidade de Brasília.**
Currículo lattes: https://wwws.cnpq.br/cvlattesweb/PKG_MENU.menu?f_cod=E74B-D6203159B80381243826E32ADE9A# ; email: Menezes.ams20@gmail.com

***** Graduanda da 2ª fase do curso de Direito da Universidade de Brasília.**
Currículo lattes: http://lattes.cnpq.br/0158443583910315; email: dessalogui2002@gmail.com

****** Graduando da 2ª fase do curso de Direito da Universidade de Brasília.**
Currículo lattes: http://lattes.cnpq.br/4863821803772852; email: arthurmiguel.historia@gmail.com

******* Graduanda da 5ª fase do curso de Direito da Universidade de Brasília.**
Currículo lattes: https://wwws.cnpq.br/cvlattesweb/PKG_MENU.menu?f_cod=FE7F77E4DC37202E6F4C-94F91DC4A5FF# ; email: lsorrequia@gmail.com
Projeto de Extensão, Simulações Jurídicas e Pesquisa.
Coordenadoras: Julyane Lopes Moreira e Letícia Conceição Guimarães da Silva

Revista Acadêmica do Curso de Graduação em Direito da UFSC

Abstract: This paper intends on tracing the legal path of data protection in Brazil, specially on the field of social media, coming from an analysis of the development of digital media, which has been even more rooted in today's world. Therefore, it questions the data protection norms' efficiency, more specifically the "Lei Geral de Proteção de Dados Pessoais" (LGPD) and its impact on representative democracy and surveillance capitalism, also taking into account its part on facing the new digital crimes.

Keywords: Data protection. Democracy. Digital Media. Digital Crimes. Artificial Intelligence.

1. INTRODUÇÃO

O desenvolvimento tecnológico no contexto contemporâneo possibilitou um avanço no fluxo de dados. Entre esses progressos, a análise de informações por *big data*[1] e os estudos na formação de inteligências artificiais capazes de prever e influenciar o comportamento do usuário a partir de suas interações no ambiente virtual proporcionaram a renúncia da vida pessoal às tecnologias. Neste prisma, os usuários, embora tenham a percepção da exploração de suas informações por bancos de dados, não tem controle do que é feito posteriormente com as informações coletadas.

Considerando que os indivíduos fazem uso das redes sociais para se expressar virtualmente, compartilhando seus interesses e crenças sem discrição, e como esse espaço virtual se porta como uma extensão de sua individualidade, torna-se necessário adotar medidas com o fito de garantir os direitos fundamentais de personalidade, garantidores da autonomia, liberdade e da privacidade dos indivíduos. Tendo em vista o limbo jurídico do tratamento de dados e de seus limites éticos, é fulcral adequar o meio virtual às cláusulas pétreas da Constituição por meio da tutela legal dos dados pessoais.

Nesse sentido, cabe tratar sobre consentimento e acesso às informações na realidade do capitalismo de vigilância, em que o cidadão deixa de ser apenas o consumidor e passa a ser também um produto, posto que seus dados são uma moeda de troca, especialmente no contexto de propagandas e de *marketing* virtual. Além de produtos, o lucro é proveniente da comercialização de estilos de vida e ideologias, elemento que transforma a *internet* em um mecanismo de manipulação que transcende a esfera econômica, influenciando o processo político e representando uma ameaça à democracia representativa no globo.

---

[1] "Big Data é "[...] a capacidade de uma sociedade de obter informações de maneiras novas a fim de gerar ideias úteis e bens e serviços de valor significativo." (MAYER-SCHÖNBERGER; CUKIER, 2013, p.2).

Um novo elemento no contexto global que acirra o debate sobre o tratamento de dados é a pandemia da covid-19. A ampliação do uso de tecnologias para comunicação, a falta de conhecimento de muitos usuários em relação à segurança ou não das plataformas e da necessidade de uso de dados no combate à pandemia expõe a fragilidade procedimental da sociedade na defesa dos direitos fundamentais no ambiente virtual. Nesse sentido, a expansão do uso de informações no *marketing* em contexto pandêmico e da influência nos comportamentos dos internautas podem ter resultados negativos em temas fulcrais, como a solução da crise sanitária ou a segurança da saúde mental.

Portanto, a Lei Geral de Proteção de Dados Pessoais (LGPD) busca solucionar a questão referente à responsabilidade dos agentes e proteger os direitos fundamentais de personalidade diante de uma nova dimensão de criminalidade. Consoante a uma série de escândalos relacionados ao tratamento inadequado de dados que ameaçam a autonomia e a privacidade dos indivíduos, a lei visa regular e minimizar seus efeitos, removendo o Brasil gradualmente do limbo jurídico que é a internet.

2. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

2.1. ANTECEDENTES

A Lei Geral de Proteção de Dados Pessoais, promulgada no Brasil em 2018, é o resultado de diversas discussões iniciadas no século XX em diversos países a partir da ampliação do processamento de dados no meio eletrônico. Dessa maneira, o presente tópico se destina a compreender o histórico do debate e das leis que influenciaram a formação da LGPD.

De acordo Laura Schertel Mendes (2019), as primeiras normas referentes à proteção de dados pessoais foram desenvolvidas especialmente na Europa durante a década de 70 "como reação ao processamento eletrônico de dados nas Administrações Públicas e nas Empresas Privadas, bem como às ideias de centralização dos bancos de dados em gigantes bancos de dados nacionais" (MENDES, 2019, p. 37). Nesse sentido, essas legislações inovaram ao tipificar as medidas para o controle procedimental da coleta e tratamento de dados pelo Estado, fator de influência para a elaboração da LGPD, no Brasil.

Além dessa geração, Laura Mendes (2019) aponta para outras quatro etapas de desenvolvimento das leis de proteção de dados. A primeira, como mencionada,

ocorreu na década de 70 com o princípio da legislação do ciberespaço. A segunda geração tratou da preservação da privacidade a partir dos direitos previstos na Constituição. A terceira defendeu o "direito à autodeterminação informativa" (MENDES, 2019, p. 40). A quarta visava promover a autonomia do indivíduo diante de seus dados pessoais. E a quinta – e atual – geração tem como objetivo responsabilizar os agentes que detêm os dados no meio virtual.

A LGPD está inserida no contexto geracional contemporâneo, o que indica um atraso do Direito brasileiro em relação às interações na *internet*. Essa característica é evidenciada pela sua falta de dispositivos e ausência de pistas interpretativas até meados dos anos 2000 (MENDES; BIONI, 2019, p. 165) que culminou com a promulgação do Marco Civil da Internet (Lei nº 12.965/2014) – importante legislação no estabelecimento de direitos e deveres para o uso da *internet* no país. Apesar do debate acerca dessa lei ter se iniciado em 2010 conforme a proposta do Ministério da Justiça, apenas em 2020 ela entrou em vigor, tendo ainda alguns de seus efeitos, especialmente os que concernem o campo da saúde, adaptados por pressão do contexto pandêmico do COVID-19 (DAMO, 2020).

Devido a esse atraso em adaptar a jurisprudência ao panorama virtual, por muito tempo, a ação constitucional de *habeas data*, apesar de ser um importante remédio constitucional, que caracteriza o garantismo da Constituição de 1988, trazendo como fator inovador o direito à defesa da personalidade, é incapaz de lidar com os desafios do intenso fluxo de informações diante de uma realidade que se tornava cada vez mais dependente da inteligência artificial e do tratamento de dados pessoais. Com a criação do Regulamento Geral de Proteção de Dados (RGPD) por parte da União Europeia (UE), fruto de uma longa jornada na área de segurança de dados, o legislativo brasileiro, que desenvolvia essa temática paulatinamente, percebeu a oportunidade de utilizar esse regulamento como um molde para um conjunto normativo próprio. Consoante ao apresentado no Tratado de Proteção de Dados Pessoais:

> No que toca ao Brasil, é imperioso citar, ainda nessa quadra, a relevância do RGPD para a elaboração da LGPD, que incorporou uma série de institutos, princípios e regras da normativa europeia. Além disso, muito embora o Brasil sequer esteja vinculado ao direito europeu em geral, nem no concernente aos direitos humanos e fundamentais, para efeitos da transferência de dados o Brasil deve atender aos parâmetros do regulamento europeu, o que por si só, dado o impacto sobre as relações comerciais entre os países europeus e o nosso, implica certa (no que importa ao ponto) simetria entre os marcos regulatórios. (BIONI; MENDES et al, 2020, p. 64)

Destarte, a LGPD demonstra o compromisso do Brasil em integrar-se nos debates do novo mundo globalizado e em inserir-se na nova realidade ESG (*environmental, social and corporate governance*) do capitalismo, em que as empresas e o governo buscam trabalhar juntos para demonstrar preocupação com a comunidade e o meio ambiente, diante da cobrança dos seus consumidores, que se tornam cada vez mais conscientes. Assim, a temática da proteção de dados se torna cada vez mais querida não só pelas instituições do Estado, que tem como dever garanti-la, mas também pelas empresas, que lucram ao apresentarem uma imagem interessada no bem-estar do seu comprador, fazendo da LGPD uma demanda do mercado e dos cidadãos.

2.2. NOVAS GARANTIAS E DIREITOS

A LGPD (Lei nº 13.709/2018) é um reconhecimento da dimensão digital dos direitos fundamentais (SARLET, 2021), e afeta todas as pessoas naturais que estão sob o véu da Constituição Federal de 1988, no art. 5º, *caput*, em que se reza "são titulares de direitos fundamentais os brasileiros e estrangeiros residentes no país", embora a lei também abranja pessoas jurídicas, o que posteriormente será explanado.

Antes de ser discorrido sobre as novas garantias e direitos, faz-se necessário destacar um ponto sobre a delimitação da aplicabilidade da Lei nº 13.709/2018 (art. 4º); o tratamento de dados deve seguir propósitos certos e funcionais, contudo, em situações em que há necessidade de liberdade de informação e expressão, a soberania, a segurança e a defesa do Estado, a LGPD não se aplica.

2.2.1. A proteção de dados da pessoa natural como direito fundamental

Para que um dado[2] seja considerado pessoal, e por consequência abarcado pela Lei nº 13.709/2018, ele deve se referir a uma pessoa natural, identificada ou identificável, ou seja, dados anonimizados são excluídos da incidência do diploma normativo. Dentro da relação trilateral (entre o titular, o objeto e o destinatário), os titulares são somente as pessoas naturais, mas isso por si só não traz uma a conexão entre direitos fundamentais e a proteção de dados, o que calha a aumentar

[2] Importante salientar que na leitura do inciso I do artigo 5º da LGPD, dado pessoal equivale ao mesmo que informação relacionada à pessoa natural, embora no campo da tecnologia e segurança da informação se conceituem termos distintos.

a clareza dessa relação é a leitura do art. 1º da Lei Geral de Proteção de Dados Pessoais quando correlacionado ao art. 5º já citado, CF/88, *in verbis*:

> Art. 1º. Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa jurídica de direito público ou privado, **com o objetivo de proteger direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural**. (Grifo nosso)

O sinal mais claro da relação desta conexão do dispositivo com a Carta Magna, de acordo com Ingo Sarlet (2021), se trata provavelmente do termo "livre desenvolvimento da personalidade da pessoa natural", afinal, de acordo com o mesmo, com "uma leitura harmônica e sistemática do texto constitucional, a CF consagrou um direito fundamental implicitamente positivado à proteção de dados pessoais" (SARLET, 2021, p. 77). Ora, se o direito já existia, que novas garantias se têm com a positivação deste? No *Tratado de Proteção de Dados Pessoais* (BIONI, 2021), essa positivação estaria dando a marca de direito autônomo, com um domínio próprio de proteção. Nesse sentido, todo e qualquer controlador que realiza o tratamento de dados deve fixar bases claras em seus contratos de permissão de uso dessas informações, para a garantia do direito fundamental à proteção de dados (BOTELHO, 2020).

Essa noção da proteção de dados como um direito tutelado constitucionalmente foi reforçada jurisprudencialmente, para além da doutrina e da legislação, pelo julgado do Supremo Tribunal Federal, do dia 24 de abril de 2020, quando a Ministra Relatora, Rosa Weber, suspendeu de maneira liminar a Medida Provisória n. 954/2020, que obrigaria empresas telefônicas a compartilhar com o Instituto Brasileiro de Geografia e Estatística (IBGE) dados que efetiva ou potencialmente levariam a identificação de pessoa natural. Sua linha de raciocínio se desdobra a partir do entendimento que, com âmbito próprio do direito à proteção de dados, auxilia-se a observação de toda a extensão dos direitos garantidos no art. 5 da Carta Magna. Desse modo, a decisão constituiu base fulcral para o reconhecimento da proteção de dados como garantia fundamental e proposição de ampliação de normas sobre o tema, como a Emenda Constitucional nº 115/2022, na qual se acresceram novos incisos para legitimação das ações protetivas de dados e delimitação de competências nessa área.

2.2.2. A justificativa da proteção de dados da pessoa jurídica

A LGPD incide até mesmo nas pessoas jurídicas e em entes sem personalidade jurídica, mas por razões que se diferem de outros ordenamentos, à exemplo do Ale-

mão, que, por força de orientação fixada pelo Tribunal Constitucional Federal, assegura a proteção de dados igualmente às pessoas jurídicas quanto às naturais. No Brasil, a proteção ocorre, pois as informações armazenadas desses entes jurídicos podem afetar direitos e interesses de terceiros, ou seja, de pessoas naturais (SARLET, 2021).

Assim, o remédio constitucional do *habeas data* é efetivamente materializado na Lei Geral de Proteção de Dados, fazendo dessa norma infraconstitucional uma garantia irrenunciável da população brasileira diante das novas dificuldades jurídicas do mundo conectado. A proteção da pessoa jurídica se dá como extensão desse direito ao mercado e à burocracia estatal, reafirmando o compromisso com a proteção da personalidade dentro de todos os âmbitos em que o tratamento de dados é relevante ao sujeito.

2.3 IMPORTÂNCIA DA SEGURANÇA NO TRATAMENTO DE DADOS

Em um contexto onde a produção de dados se dá de maneira elevada, até mesmo superando a economia mundial, o fenômeno do *Big data* destaca-se pelo ultra processamento de dados, pela quantidade e variedade de informações armazenadas em bancos de dados por todo o globo. Em contrapartida, a consciência dos indivíduos quanto ao recolhimento e uso de seus dados não acompanha essa enorme produção informacional, não sendo possível ao usuário ter o controle de todas as informações concedidas e o valor agregado a tal recolhimento, assim "[...] os dados se tornaram matéria-prima dos negócios, um recurso econômico vital, usado para criar uma nova forma de valor econômico" (MAYER-SCHÖN- BERGER; CUKIER, 2013, p. 4).

Logo se infere que contemporaneamente a economia é movida a dados, onde os chamados Mercados de Atenção tentam atrair o máximo do nosso tempo dentro do aplicativo, para que assim possam coletar mais dados pessoais e mais recursos que posteriormente serão usados para traçar personalidades e manipulá-las. A exploração dos dados pessoais são mais problemáticos do que a simples violação da privacidade, mas oferecem também riscos aos direitos de personalidade, como a individualidade, autonomia e ainda a própria democracia.

Segundo Schertel (2019), os dados pessoais são projeções diretas da personalidade, tendo assim a capacidade de modelar a representação da pessoa na sociedade e de violar os seus direitos fundamentais. Nesse ínterim, tem-se a necessidade, cada vez mais latente, vide à expansão comunicacional e memorial

advinda da internet, do controle das informações pessoais divulgadas no meio virtual e suas implicações posteriores na vida da pessoa em questão. Nesse ínterim, propostas como o direito ao esquecimento, admitidas em outras normas jurídicas internacionais, vêm sendo suscitadas no sentido de evitar que notícias de cunho privado e sem pertinência ao público sejam disseminadas livremente nos meios midiáticos e possam causar constrangimento no indivíduo ao qual a notícia trata.

Outrossim, ao considerarmos a enorme coleta de dados e a possibilidade de exposição indevida de conteúdos de terceiros na internet, é cabível pensar na ocorrência de casos extremos, onde há implicações na honra, privacidade, imagem e ferimento dos direitos de personalidade da vítima, podendo dessa maneira assumir a aplicação do entendimento do direito ao esquecimento. Em contraponto, os princípios da liberdade de expressão e o princípio democrático observam a possibilidade do ferimento do direito à informação e assim o entendimento do STF é de que tal paradigma não é cabível no ordenamento jurídico brasileiro.

Seguindo o debate acerca da possibilidade de um uso seguro do espaço digital por parte dos indivíduos, temos o sancionamento da LGPD como uma das medidas estabelecidas pelo Estado brasileiro a fim de nortear os direitos dos usuários e os deveres dos agentes. É importante salientar as noções vigentes no art. 6º da LGPD que diz respeito a como "as atividades de tratamento de dados pessoais deverão observar a boa-fé" (BRASIL, 2018) e princípios como a finalidade, em que o tratamento dos dados deverá ser realizado para propósitos legítimos, específicos e informados ao titular dos dados, a prevenção, a fim de precaver ocorrência de danos relacionados ao tratamento dos dados, e ainda o princípio da necessidade, em que há a limitação do tratamento de dados ao mínimo necessário para o que se é proposto.

No art. 11, § 3º, trata-se do uso compartilhado de dados pessoais específicos entre controladores a fim de obter vantagem econômica e de como esta comunicação poderá ser vedada pelo poder público. Ainda, o art. 13, §2º, afirma que é de responsabilidade do órgão de pesquisa a segurança das informações, não permitindo a transferência destes a terceiros.

Com essas constatações, a LGPD ressalta a importância da segurança no tratamento de dados, além da minimização dos prejuízos e prevenção em casos de vazamentos, uma vez que, os dados são matérias-primas para as tomadas de decisões no mundo. Sendo assim, urge o comprometimento dos agentes de tratamento aos titulares de informações, buscando a harmonização entre a economia e os direitos fundamentais do usuário.

> A informação passa a ser considerada como fator de produção em um contexto em que os dados são produzidos em uma velocidade vertiginosa, exigindo-se uma gestão da informação, a saber, o método utilizado por uma organização qualquer para planejamento, coleta, organização, utilização, controle, disseminação e descarte de suas informações de maneira eficiente (HINTZ-BERGEN et. al., 2018, p. 56).

3. PUBLICIDADE EM UM MUNDO CONECTADO

3.1. INTELIGÊNCIA ARTIFICIAL E A COLETA DE DADOS

O fluxo de informações resultante das novas tecnologias altera diversos campos da vida social no século XXI, inclusive a área jurídica em suas normas e procedimentos para proteger os direitos dos cidadãos no meio digital. Nesse prisma, deve-se analisar o modo pelo qual os dados são reunidos e de que maneira sua coleta e análise se relacionam às legislações de proteção vigentes, em especial, a LGPD.

As novas empresas disruptivas, que modificam o modelo paradigmático de áreas como a socialização, transporte e hospedagens (a exemplo de *Facebook*, *Uber* e *Airbnb*), percebem na obtenção de informações do usuário um potencial de lucro ainda pouco explorado e, por isso, desenvolvem diferentes ferramentas para acessar os dados pessoais de seus clientes. Em vista disso, os dados são alcançados por instrumentos de *web tracking, social tracking* e *location tracking* (OLIVEIRA; SILVA, 2018), ou seja, dados obtidos na *Web* a partir de um "conjunto de expedientes tecnológicos de alta complexidade, como aplicações de *javascript*, técnicas de *browser fingerprinting* e os *cookies* de navegador" (OLIVEIRA; SILVA, 2018, p. 311), fornecidos para as redes sociais ou para os navegadores de GPS.

Os *Cookies* de navegador são os elementos mais utilizados na *Web* para adquirir conhecimento sobre o comportamento do consumidor pelas empresas. Nesse sentido, esse arquivo é inserido no computador pelo site e possibilita a identificação e monitoramento do sujeito em sua navegação. Apesar de teoricamente ser possível bloquear seu uso, ferramentas como *supercookies* e *evercookies* evitam que o controle humano sobre as informações adquiridas pelo computador seja efetivo. (OLIVEIRA; SILVA, 2018).

Os dados pessoais são classificados de 4 formas (OLIVEIRA; SILVA, 2018): dados providos, em que o próprio usuário cede informações às plataformas; dados observados, caracterizados pela análise comportamental do indivíduo a partir de cookies, sensores e outras mídias como câmera e som; dados derivados, resultan-

tes da reunião de informações de um grupo em um agrupamento específico para classificação de perfis; dados inferidos, decorrentes de análises probabilísticas que tentam prever o comportamento individual.

Destarte, a obtenção e o tratamento de dados pessoais, muitas vezes com uso de inteligências artificiais, podem ocasionar descumprimento de normas fundamentais, caso não haja procedimentos que respeitem a ética e a legalidade (MENDES; DONEDA; SOUZA; ANDRADE, 2018). Nesse contexto, o desenvolvimento de "uma verdadeira agenda relativa aos princípios éticos da inteligência artificial e das decisões automatizadas amparadas no uso de algoritmos" (MENDES; DONEDA; SOUZA; ANDRADE, 2018, p. 6) é basilar para conter possíveis danos à autonomia, economia e privacidade (OLIVEIRA; SILVA, 2018).

Outro elemento importante na discussão sobre a obtenção de dados pessoais é o modo de lidar com informações de crianças e adolescentes. Sob essa perspectiva, os nativos digitais, embora estejam desde o início da vida em uma sociedade informatizada, são os mais vulneráveis na obtenção de dados pessoais, fato que ameaça as determinações do Estatuto da Criança e do Adolescente (ECA) e da Constituição Federal (BOTELHO, 2020). Com a finalidade de preservar o princípio do melhor interesse desse grupo, a LGPD determina, em seção específica (Capítulo 2, Seção III) sobre os procedimentos adequados e "parâmetros técnicos de segurança [...] trazendo todas as consequências ao controlador do seu descumprimento" (BOTELHO, 2020, p. 227).

3.2. AS BOLHAS DAS REDES SOCIAIS E A PROPAGANDA

A última década foi marcada por um advento das redes sociais, que cada vez mais interfere no cotidiano da população. Nesse sentido, bem como na vida real são criados ambientes e grupos sociais de maior contato por possuírem interesses e pensamentos semelhantes, na internet, são criadas as bolhas informacionais. Nessas "bolhas", o conjunto de informações e opiniões condizem com as do usuário – independente de serem factuais ou não – em que o acesso é facilitado pelos sites a fim de manter o internauta de forma que se sinta confortável em seu meio virtual e, consequentemente, utilize as redes de forma contínua.

As bolhas das redes sociais se tratam de um fenômeno que se aplica a todos os usuários das redes sociais a partir da adaptação contínua de um algoritmo matemático criado exclusivamente para aquele indivíduo e que visa apresentá-lo

os conteúdos que são mais prováveis de serem consumidos por ele. O interesse econômico por trás desse algoritmo, entretanto, é o que faz com que, por vezes, ele seja tão perverso.

O conhecimento da personalidade virtual do usuário – tendo sido traçada pelo algoritmo a partir dos seus gostos, interesses e pensamentos com que compactua – permite que empresas façam propagandas de forma muito mais eficaz, já que atingem diretamente seu provável comprador. Dados empíricos demonstram o uso de mecanismos em sites e dispositivos tecnológicos, como os *cookies* e as assistentes virtuais, para monitorar os internautas e alimentar bases de perfis para publicidade sem que o indivíduo tenha sequer consciência de que faça parte de uma cadeia produtiva (OLIVEIRA; SILVA, 2018).

Dessa forma, as bolhas informacionais se tornam áreas virtuais de coleta de dados, o que torna imprescindível a intervenção de medidas que garantam o consentimento do usuário e a regulação dos dados extraídos, vide a criação da Lei Geral de Proteção de Dados Pessoais. Porém, o tópico da proteção de dados extrapola em muitos sentidos o que é previsto pela lei, tendo em vista a dificuldade de se controlar a eficácia, já que se trata de um meio não físico em que as ações tomam proporções globais rapidamente. Assim, apesar da LGPD ter alcançado importantes conquistas como a necessidade de autorização do consumidor para o uso de seus dados e a possibilidade desse exigir acesso a todas as informações que as indústrias e órgãos governamentais possuem acerca dele, ainda não é possível se falar efetivamente de consentimento por parte do internauta, já que o acesso a seus dados ainda ocorre de maneira muito velada, mesmo que necessite de uma autorização explícita dele.

Destarte, o espaço virtual se torna ideal para empresas e organizações político-ideológicas, já que, pelo acesso facilitado aos dados dos usuários, motiva o consumo excessivo e a alienação do cliente. Em suma, como apresentado no documentário O Dilema das Redes (NETFLIX, 2020), os usuários tornam-se produto para os verdadeiros consumidores: as empresas anunciantes das plataformas e *data centers* que buscam traçar o perfil e moldar as opiniões políticas do indivíduo.

3.3. A DEMOCRACIA E A PROTEÇÃO DE DADOS

O conturbado contexto político contemporâneo inclui, entre os agentes do desgaste do processo democrático, o tratamento inadequado de dados como potencial limitador da autonomia e liberdade. Nessa perspectiva, é fulcral relacionar

o uso das redes sociais e acontecimentos recentes na política nacional e internacional com o objetivo de compreender os mecanismos utilizados para abalar os fundamentos da democracia.

A obra O Dilema das Redes (NETFLIX, 2020) descreve o funcionamento do tratamento de dados por grandes empresas como *Google* e *Facebook* com o fito de demonstrar o efeito bumerangue e seu potencial de ocasionar prejuízos no contexto individual e/ou coletivo dos usuários. Segundo os ex-funcionários das empresas de tecnologia entrevistados no filme, o efeito bumerangue consiste em captar os dados do indivíduo, traçar um perfil do consumidor e, posteriormente, enviar mensagens e anúncios que moldem seu comportamento de modo a manter a pessoa conectada o maior tempo possível.

Dessarte, o tratamento inadequado de dados pessoais com fins financeiros, para além de violar os direitos do titular, ocasiona fenômenos negativos tanto no âmbito individual como coletivo. A partir dessa análise, o desenvolvimento de distúrbios psíquicos como depressão e ansiedade, inclusive em crianças e adolescentes, podem ser apontados como grandes prejuízos individuais decorrentes das redes sociais e, em um contexto político, a polarização ideológica e favorecimento de extremismos têm entre seus fatores de influência a estrutura atual dos aplicativos virtuais de interação como *YouTube*, *WhatsApp*, entre outros.

Nesse cenário, o comparecimento de Francis Haugen no Senado com a finalidade de denunciar condutas do *Facebook* com as informações obtidas de seus usuários demonstram a falta de ética e responsabilidade no tratamento de dados por empresas de tecnologia (SEISDEDOS, 2020). Os documentos internos da empresa exibidos pela ex-funcionária explicitam a intenção dos algoritmos de gerar discórdia entre os cidadãos, o desenvolvimento dos instrumentos de ampliação de vícios na plataforma e a conivência dos diretores com o crescimento de problemas psíquicos entre adolescentes, além da omissão no combate ao crime organizado por meio do site.

O potencial adverso desse tratamento inadequado de dados é explorado a partir das seguintes circunstâncias: divulgação facilitada de informações sem a devida verificabilidade, força de empresas tecnológicas que determinam os conteúdos absorvidos pelos usuários, utilização de robôs e perfis falsos capazes de realizar disparos em massa, fator de subversão da esfera pública (FRAZÃO, 2021).

Na discussão sobre a interferência das empresas disruptivas na democracia, é fundamental compreender alguns pressupostos da ativa participação popular. Ana

Frazão (2021) demonstra 5 pontos que configuram o processo político democrático na pós-modernidade. Primeiramente, a plena garantia de liberdade e igualdade são pressupostos universais na construção de um ambiente público participativo. Outro fator essencial é o livre acesso à informação, demanda do desenvolvimento fundamentado de opiniões que serão utilizadas em discussões sobre a relação entre o poder e a sociedade. A influência do poder, que determina as ações do poder público na formação de políticas para atendimento dos cidadãos, é outra determinação clássica do modelo político.

Além desses pressupostos determinados no histórico tradicional da democracia, o século XXI estabelece outras áreas na defesa deste regime. A relevância da comunicação na sociedade tecnológica hodierna, elemento que insere os agentes da mídia como novos atores no jogo da influência política e persuasão, demanda maiores estudos interdisciplinares sobre sua força na contemporaneidade.

Visto que o ambiente digital por ora se estrutura de forma anárquica, alguns agentes interessados em explorar o poder da desinformação e distorção de informações criam uma esfera pública artificial e que se mostra eficiente para pautar a discussão pública e para mudar crenças e opiniões de pessoas.

Nesse sentido, as mudanças promovidas pelo meio digital no debate público são evidentes, deixando cada vez mais difícil entender qual a informação é verdadeira e qual informação é falsa, além de, pela viabilidade de participação de robôs e perfis falsos nas discussões, o debate público pode se tornar completamente distorcido, pela falta de acesso à informação de quem participa e a quais são os interesses defendidos.

O novo fluxo informacional tem facilitado a expansão do chamado mercado da dúvida, onde até mesmo assuntos científicos e fatos outrora já confirmados por meio de evidências contundentes são revogados, gerando a sensação de que tudo é controverso, levando ao descrédito da ciência, a falta de consenso entre a população e afetando a democracia.

Quanto ao mercado da dúvida, se torna evidente que, este processo de expansão e ampliação no fluxo informacional só pode ser interpretado como inclusivo na superfície, o que se nota é que internamente a comunicação e o debate público têm sido conduzidos por grandes agentes políticos económicos, se valendo de minorias que defendem seus interesses cegamente, mesmo que às custas da normalização do absurdo.

A autora Ana Frazão (2021) trata de como Hannah Arendt conduz uma explanação fidedigna da relação entre persuasão e propaganda em sua obra As Origens do Totalitarismo (2013). Nesta, a jurista demonstra como, pela perda de laços sociais e de perspectiva social comunitária, os indivíduos ficam suscetíveis a serem cooptados por movimentos nacionalistas, visto que esses lhe oferecem um senso significado e pertencimento. Dessa maneira, a propaganda fora utilizada para fazer com que apenas a visão do líder importasse para pessoa e que o pensamento analítico e político do indivíduo fosse neutralizado, por meio de estratégias como: a desconsideração da verdade (onde toda informação e evidência que contraria a visão do líder é incorreta) e a negação da história, que é distorcida para caber na ideologia, a propagação de mentiras e narrativas falsas.

A realidade do capitalismo de vigilância nos demonstra como os governos e os *players* econômicos criam um *one way mirror*, onde tais agentes sabem tudo dos cidadãos ao passo que estes nada sabem dos primeiros. Assim, surge no mercado a figura dos *gatekeepers*, agentes que exercem todas as formas de controle de informação no network que criam. Dessa forma, a arquitetura da plataforma é programada para o convencimento do seu usuário para o consumo de informações que sejam mais lucrativas a eles, ainda que aparente se tratar de uma relação mútua entre as redes e seus usuários. Dessarte, torna-se evidente que é falaciosa a interpretação de que existem plataformas abertas e neutras.

É nesse pano de fundo que conseguimos analisar as *fake news*. O que torna as *fake news* potencialmente perigosas não são suas mentiras em si, posto que essas se apresentaram durante todo o percurso da história, mas sim as inúmeras variáveis somadas na contemporaneidade que potencializam a sua disseminação e os seus efeitos, como: a expressiva utilização da *internet*, o protagonismo de plataformas que se tornam gestores de conteúdo, a existência de aplicativos de comunicação que podem ser utilizados para disseminar tais informações, e a possibilidade de anonimização dos indivíduos que fazem uso das plataformas.

A propaganda política que outrora era feita de maneira ampla e indiscriminada, é, agora, na sociedade de informação, customizada, e possui um poder de penetração muito maior; é por tal motivo que o fenômeno das *fake news* se dá de maneira tão expressiva e se relaciona com negócios de extração de dados pessoais.

Por fim, a necessidade da compreensão dos dados pessoais como uma informação de influência nos cenários políticos e econômicos configura a necessidade de leis e regulamentações sobre o tema que impeçam a impunidade de empresas que ameaçam o indivíduo e a democracia.

> Uma boa governança de dados que proteja os titulares e evite a utilização abusiva e indevida é portanto fundamental para assegurar o debate em busca dos melhores argumentos e das soluções mais adequadas evitando que a discussão pública seja pautada pelas mentiras que foram mais bem divulgadas ou que tiveram mais financiamento (FRAZÃO, 2021, p. 760)

4. CRIMES DIGITAIS

4.1. CONTEXTO PANDÊMICO E CRIMES DIGITAIS

O contexto contemporâneo global tem como marco de alteração paradigmática as mudanças, conjunturais ou estruturais, decorrentes da pandemia da covid-19. Nesse sentido, o texto de Nagli (2020) indica pontos relevantes no novo comportamento dos cidadãos e instituições em relação às tecnologias. As medidas de distanciamento social promovidas por diversos governos forçaram o uso de ferramentas virtuais para a interação e integração, instrumentos ainda recentes e, por isso, com falhas que ameaçam a preservação de direitos fundamentais.

O aplicativo *Zoom* é um indicativo da vulnerabilidade de *softwares* a ataques cibernéticos no contexto pandêmico. Sua crescente popularidade nas fases iniciais de espalhamento do vírus, a falta de familiaridade por parte dos usuários em sua utilização e carência de segurança da plataforma resultou em diversos "ataques noticiados pela grande mídia" (NAGLI, 2020, p. 2). Destarte, esse e outros serviços de reuniões virtuais precisaram desenvolver diferentes artifícios como "implementação em larga escala de autenticação de dois fatores; preparar as aplicações internas para uso remoto" (NAGLI, 2020, p. 6) com a finalidade de evitar novos escândalos relacionados à violação de privacidade.

Os principais métodos no sequestro de dados utilizam *web tracking, social tracking e location tracking* (descritos no tópico 3.1) a partir de debilidades dos sistemas vigentes. Nessa perspectiva, a distância dos funcionários das redes corporativas, tradicionalmente caracterizadas por profissionais de segurança que visam evitar invasões às redes empresariais, e a falta de familiaridade destes indivíduos em relação ao ambiente virtual torna-os suscetíveis a ciberataques de diversos tipos, incluindo exploração de seus dados por empresas de publicidade e *data centers*. Dessa maneira, mecanismos simples de engenharia social, "usando de manipulação e trabalhando com os medos do usuário tentando obter informações" (NAGLI, 2020, p. 4) podem ser instrumentos capazes de gerar golpes e promover o tratamento inadequado de dados pessoais.

Nessa conjuntura, a obra Privacidade Hackeada (NETFLIX, 2019) expõe a falta de controle que a população tem de seus próprios dados. Desse modo, o documentário evidencia a monetização de dados dos usuários pelas plataformas a partir de vendas para *data centers* como a *Cambridge Analytica*, descrita no documentário como grupo ligado ao Projeto Álamo, definido como uma reunião de dados de diversos eleitores americanos que, a partir de ferramentas de análise por big data, foram utilizados para influenciar a percepção da população em relação à campanha presidencial de Donald Trump em 2016.

As discussões relacionadas ao tratamento de dados pessoais (descritas nos tópicos 2.1 e 2.2) forçaram empresas e governos a atualizarem seus procedimentos na análise de dados. Nesse contexto, é representativo que a LGPD determine em seu artigo 5º, inciso V, a titularidade dos dados à "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento" (BRASIL, 2018). Dessa forma, confere maior controle dos cidadãos em relação aos seus direitos de personalidade.

Contudo, a pandemia da covid-19 estabeleceu um novo dilema para o uso de dados pessoais: como utilizar os dados disponíveis para o combate à pandemia sem incorrer em violação de direitos fundamentais e crimes digitais? O relatório Privacidade e pandemia: recomendações para o uso legítimo de dados no combate à covid-19 (BIONI; ZANATTA; MONTEIRO; RIELLI, 2020) indica aspectos primordiais no tratamento responsável de dados. Dessa forma, "gestores públicos precisam apresentar evidências científicas que sustentem a importância da aplicação de certa técnica de análise de dados" (BIONI; ZANATTA; MONTEIRO; RIELLI, 2020, p. 15) e devem estabelecer o tempo de tratamento e ferramentas para proteção de direitos fundamentais.

Portanto, a proteção de dados pessoais e a prevenção de crimes digitais demandam estudos sobre as ferramentas de *software* e educação de cidadãos sobre a importância da proteção de seus dados, especialmente no contexto pandêmico, caracterizado por uso de tecnologias e fluxo de informações inéditas. Além disso, as empresas de tecnologia têm necessidade de se adaptar às novas legislações e não utilizar a pandemia como facilitadora de recepção de dados para tratamento inadequado ou venda dessas informações para organizações que buscam controlar em diversos aspectos o comportamento dos cidadãos, implicando, no fator econômico, em mudanças no padrão de consumo e, no sentido político, incentivo à formação de bolhas e polarizações que gerem benefícios aos agentes e empresas de tratamento.

4.2. EFICÁCIA AO COMBATE DOS CRIMES DIGITAIS

A Lei Geral de Proteção de Dados surge para evitar abusos dentro da mencionada realidade, em que os dados se tornam fator primordial do mercado. Porém, é fundamental discutir, a partir da LGPD, a efetividade no combate dos crimes digitais e o estabelecimento de autoridades competentes pelo *enforcement* dentro desse contexto ainda tão estranho à legislação brasileira.

Para tanto, chama-se atenção ao caso ocorrido em janeiro de 2021 – após a vigência da LGPD – em que os dados registrados em sites do governo de duzentos e vinte e três milhões de brasileiros (ou seja, dados de toda a população e de pessoas já falecidas) foram vazados por dois *hackers.* Entre esses dados estavam CPFs, CNPJs, nomes, endereços, dados de veículos, renda, benefícios do INSS, programas sociais, escolaridade, sexo e data de nascimento. Os dados vazados poderiam potencialmente ser usados para a aplicação de golpes, como o saque indevido do Fundo de Garantia do Tempo de Serviço, ou tentativas de obter vantagens financeiras por meio do envio de contas e serviços falsos ao e-mail ou telefone dos que tiveram seus dados vazados[3].

Desse modo, é evidente que a lei não tem poder de induzir eficácia, entretanto, a dificuldade de se lidar com o crime da divulgação indevida de uma quantidade expressiva de dados como essa, ainda mais após a criação de uma norma cuja função é regular o acesso, revela o desarranjo da Autoridade Nacional de Proteção de Dados (ANPD) e dos órgãos governamentais da Administração Pública. É necessário ressaltar que anteriormente à ANPD, outros órgãos públicos eram responsáveis pela fiscalização e aplicação de sanções vinculadas a proteção de dados, explicando assim a variedade de normas no ordenamento jurídico quanto ao tratamento de dados, tornando-se necessário a definição de um papel para cada entidade pública (BIONI; *et.al*, 2020, p. 581).

Apesar de conter diversas medidas de prevenção e proteger o cidadão, a LGPD ainda apresenta descrição e sanções insuficientes para o julgamento e para a procedência jurídica de casos como o do mega vazamento de dados, o que reduz significativamente a eficácia da lei. Essa insuficiência se torna ainda mais complexa em casos menores do que esse, em que a aplicação de sanções e a identificação das causas e dos culpados é mais simples, como o caso da construtora de São Paulo processada por divulgação de dados de clientes e isentada pelo Tribunal de

---

[3] G1. *Megavazamento de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber.* **G1**, São Paulo, 28 jan. 2021. Disponível em: Megavazamento de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber | Tecnologia | G1 (globo.com) Acesso em: 14 de set. 2021.

Justiça de São Paulo, já que não haveria meio legal para comprovar que realmente fora a construtora que divulgou as informações[4].

Outrossim, com a criação da Lei Geral de Proteção de Dados Pessoais, foi consolidada a perspectiva da ampliação do *internet banking*, ou seja, o acesso aos serviços bancários pela *internet*, o que permitiu o surgimento de facilitações como a criação de cartões de crédito e débito virtuais, além das transferências instantâneas realizadas através do Pix, um meio eletrônico de realização de pagamentos instantâneos por bancos virtuais. Porém, o crime tem se mostrado mais ágil do que a legislação e a lei mais uma vez falha em regular propriamente a execução dessa nova realidade. O próprio Pix tem sido amplamente utilizado para golpes por ser um meio rápido e irreversível de se realizar pagamentos[5]. Além de que, ao obter acesso aos dados pessoais de um indivíduo, um possível criminoso terá acesso facilitado à conta bancária dele já que grande parte das transações hoje em dia são feitas virtualmente. Assim, o âmbito financeiro também se demonstra exposto devido à insuficiência da legislação.

Contudo, as normas contidas na lei têm dificuldades em sua plena efetivação, posto que as regulamentações da norma são ainda incipientes (LACERDA,2021). Entre as principais lacunas jurídicas, a formação paulatina da Autoridade Nacional de Proteção de Dados é o elemento fundamental para a eficácia parcial da LGPD no contexto hodierno. A lei credita essa organização como "o órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional" (art. 5º, inc. XIX), desse modo, seu progresso atual para constituição própria é insuficiente na defesa das relações no meio virtual.

Dessa forma, a proteção de dados pessoais possui relevância muito grande para a prevenção de uma série de crimes, desde aspectos menos notáveis como o acesso indevido a informações pessoais a casos mais graves como o vazamento de imagens íntimas e o prejuízo financeiro. Sob a óptica das mídias virtuais, que foi posta em foco neste artigo, é notável que o banco de dados por ela coletado é suficiente para uma percepção profunda da realidade do usuário, o que torna funda-

---

[4] VIAPIANA, Tábata. *TJ-SP reforma sentença e isenta construtora por vazamento de dados de clientes.* In: **Consultor Jurídico:** Conjur. São Paulo, 1 set. 2021. Disponível em:

https://www.conjur.com.br/2021-set-01/tj-sp-reforma-sentenca-isenta-construtora-vazamento-dados . Acesso em: 11 set. 2021.

[5] LOUREIRO, R. *PIX vira isca e criminosos criam mais de 5 mil golpes digitais em um mês.* **Exame.** , São Paulo, 13 nov. 2020. Disponível em:

https://exame.com/tecnologia/pix-vira-isca-e-criminosos-criam-mais-de-5-mil-golpes-digitais-em-um-mes/ Acesso em: 16 de out. 2021.

mental a proteção da jurisprudência para garantir essa liberdade individual. Sendo a constitucionalização do direito à proteção dos dados pessoais muito recente, o arcabouço jurisprudencial e doutrinário ainda é escasso para a adequação da lei ao contexto de constantes mudanças da atualidade, o que caracteriza as normas existentes como excessivamente abertas diante da necessidade de especificações à contemporaneidade. Nesse prisma, a legislação carece de elaboração, em especial a LGPD, que se faz deficiente em sua função de conduzir o tratamento de dados, já que pouco é descrito para que haja eficácia no combate aos crimes digitais propiciados pelo novo âmbito virtual.

5. CONSIDERAÇÕES FINAIS

O presente artigo visou demonstrar que os dados adquiriram novo valor financeiro como capital político na realidade conectada e tem potencial de prejudicar elementos fundamentais à sociedade, como a democracia e os direitos de personalidade, se não corretamente regulados. Nesse sentido, a LGPD se apresentou como uma inédita moldagem do paradigma da proteção de dados, já prevista pelo Artigo 5 da Constituição Federal, porém, até então, sem procedimentos claros na legislação. Desse modo, a promulgação de normas como a Emenda Constitucional nº 115/2022, importante marco na constitucionalização dos direitos de proteção de dados pessoais, são resultantes da intensa influência da Lei Geral de Proteção de Dados Pessoais na legislação nacional.

Assim, no âmbito da comunicação, o artigo expôs as fragilidades da proteção à privacidade no meio virtual, especialmente no uso dos dados pessoais para personalização da publicidade. Dessa forma, o tratamento inadequado dos dados possibilita maior acesso de grandes agentes econômicos e mesmo de grupos ideológicos extremistas aos usuários da *internet* que são submetidos às limitações de suas bolhas informacionais. Em virtude disso, o uso indevido de dados pessoais constitui uma ameaça ao Estado Democrático de Direito ao possibilitar que representantes de organizações políticas moldem o comportamento do usufrutuário direcionando o debate público.

Nessa perspectiva, os acontecimentos relacionados ao tratamento de dados dos estadunidenses pela *Cambridge Analytica*, especialmente durante a eleição de Donald Trump e o referendo pela saída da Inglaterra da União Europeia – o Brexit –, representam a ação direta de redes sociais, como o *Facebook*, e, consequentemente de poderosos agentes financeiros e portadores de grandes fortunas,

Revista Acadêmica do Curso de Graduação em Direito da UFSC

no Estado mediante o vazamento e o controle dos dados sem consentimento dos internautas.

Dessarte, provoca-se uma discussão acerca do papel do usuário no processo de tratamento de dados, especialmente quanto ao direito à informação, que pode ser percebido no uso de ferramentas como os *cookies* e outros instrumentos de *webtracking* que, teoricamente, deveriam alertar a ele que seus dados estão sendo utilizados a fim de obter sua autorização. Além de que, mecanismos mais complexos da atualidade, como o *supercookies* e *evercookies* tornam o controle do titular nulo ao armazenar suas informações indefinidamente.

Ademais, o texto explicitou as deficiências da LGPD no combate aos crimes digitais relacionados ao manuseio indevido dos dados. Nesse prisma, a falta de regulamentação sobre o funcionamento da Agência Nacional de Proteção de Dados (ANPD) e a insuficiência da lei em sua aplicação ao longo do processo litigioso tornam sua efetividade parcial. Logo, a norma mencionada permanece incapaz de solucionar o problema da ineptidão do usuário diante do controle de suas informações no ambiente digital, bem como as possíveis implicações penais dos crimes a ela relacionados por não ser tão englobante e consolidada quanto seria preciso.

Por fim, assim como tem sido feito em outros países, como o Reino Unido e os Estados Unidos, o esforço pela proteção dos dados ainda é uma discussão muito recente no meio jurídico, apesar de ser uma questão já suscitada desde o fim do século passado. Em vista disso, as novas legislações, como a LGPD e a Emenda Constitucional nº 115/2022, por mais importantes que sejam, são apenas marcos no âmbito temático da proteção de dados que ainda precisa de muitos avanços para garantir o direito de personalidade dos indivíduos e o resguardo de sua cidadania no meio virtual.

REFERÊNCIAS

ARENDT, Hannah. *Origens do totalitarismo: Antissemitismo, imperialismo, totalitarismo.* Tradução de Roberto Raposo. São Paulo: Companhia das Letras, 2013.

BARBOSA, J. S. .; SILVA, D. B. e .; OLIVEIRA, D. C. de; JESUS, D. C. de .; MIRANDA, W. F. de . Data protection and information security in the pandemic COVID-19: national context. *Research, Society and Development,* [S. l.], v. 10, n. 2, p. e40510212557, 2021. DOI: 10.33448/rsd-v10i2.12557.

BOTELHO, M. C. A LGPD e a proteção ao tratamento de dados pessoais de crianças e adolescentes. *Revista Direitos Sociais e Políticas Públicas* UNIFAFIBE, v. 8, n. 2, 2020.

BOTELHO, Marcos. A proteção de dados pessoais enquanto direito fundamental: considerações sobre a lei geral de proteção de dados pessoais. *Argumenta Journal Law*, Jacarezinho – PR, Brasil, n. 32, 2020, p. 191-207.

BRASIL. Constituição (1988). *Emenda constitucional nº 115*, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 1 mai. 2022.

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). Diário Oficial da União: seção 1, Brasília, DF, ano 155, n. 157, p. 59-64, 15 ago. 2018.

BRASIL. *Lei nº 10.474, de 26 de agosto de 2020.* Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados e remaneja e transforma cargos em comissão e funções de confiança. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10474.htm#:~:text=DECRETO%20N%C2%BA%2010.474%2C%20DE%2026%20DE%20AGOSTO%20DE%202020&text=Aprova%20a%20Estrutura%20Regimental%20e,comiss%C3%A3o%20e%20fun%C3%A7%C3%B5es%20de%20confian%C3%A7a. Acesso em: 16 de out. 2021.

BIONI, B. *et al. Tratado de proteção de dados pessoais.* 1. ed. Brasília: Forense, 2020.

BIONI, Bruno; ZANATTA, Rafael; MONTEIRO, Renato; RIELLI, Mariana. *Privacidade e pandemia: recomendações para o uso legítimo de dados no combate à COVID-19. Conciliando o combate à COVID-19 com o uso legítimo de dados pessoais e o respeito aos direitos fundamentais.* São Paulo: Data Privacy Brasil, 2020. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2020/04/relatorio_privacidade_e_pandemia_final.pdf . Acesso em: 16 de out. 2021.

CRISTINA, C; LIMA, S. *Tudo que você precisa saber sobre as sanções da LGPD*. In: ADVOCATTA - Empresa Júnior de Pesquisas em Direito. Advocatta. Brasília, 21 ago. 2021. Disponível em: https://advocatta.org/tudo-que-voce-precisa-saber-sobre-as-sancoes-da-lgdp/. Acesso em: 10 set. 2021.

DAMO, Salvatori Paola. Migalhas. *Pandemia do novo coronavírus à luz da Lei Geral de Proteção de Dados.* Disponível em: https://www.migalhas.com.br/depeso/324507/pandemia-do-novo-coronavirus-a-luz-da-lei-geral-de-protecao-de-dados Acesso em: 16 de out. 2021.

FRAZÃO, Ana. *Proteção de dados e democracia:* A ameaça da manipulação informacional e digital. In: Denise de Souza; Fernando Antonio. (Org.). A Lei Geral de Proteção de Dados - Aspectos Práticos e Teóricos Relevantes no Setor Público e Privado. 1ed.: Thomson Reuters - Revista dos Tribunais, 2021, v. 1, p. 739-762.

G1. *Megavazamento de dados de 223 milhões de brasileiros:* o que se sabe e o que falta saber. G1, São Paulo, 28 jan. 2021. Disponível em: Megavazamento de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber | Tecnologia | G1 (globo.com) Acesso em: 14 de set. 2021.

HINTZBERGEN, Jule et. al. *Fundamentos de segurança da informação: com base na ISSO 27001 e na ISSO 27002*. Rio de Janeiro: Brasport, 2018.

Jornal do Joca. *Bolha informacional e discurso de ódio.* Disponível em: https://www.jornaljoca.com.br/wp-content/uploads/2020/08/Eixo_MidiasSociais_aula3.pdf Acesso em: 16 de out. 2021.

LACERDA, Natália. *Um estudo sobre a ANPD e sua importância para a eficácia da LGPD.* In: JusBrasil. Brasília-DF, 20 jul. 2021. Disponível em: https://webcache.googleusercontent.com/search?q=cache:lHql7MrW2XsJ:https://nataliablacerda.jusbrasil.com.br/artigos/834170035/um-estudo-sobre-a-anpd-e-sua-importancia-para-a-eficacia-da-lgpd+&cd=1&hl=pt-BR&ct=clnk&gl=br . Acesso em: 16 de out. 2021.

LOUREIRO, R. *PIX vira isca e criminosos criam mais de 5 mil golpes digitais em um mês.* Exame. , São Paulo, 13 nov. 2020. Disponível em: https://exame.com/tecnologia/pix-vira-isca-e-criminosos-criam-mais-de-5-mil-golpes-digitais-em-um-mes/ Acesso em: 16 de out. 2021.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. *Big data*: como extrair volume, variedade, velocidade e valor da avalanche de informação cotidiana. Rio de Janeiro: Elsevier, 2013.

MENDES, Laura Schertel. *A Lei Geral de Proteção de Dados Pessoais:* um modelo de aplicação em três níveis. Caderno Especial LGPD. p. 35-56. 2° ed. São Paulo: Thomson Reuters - Revista dos Tribunais, 2019, v.1, p. 35-56.

MENDES, L. S. ; BIONI, B. R. *O Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral de Proteção de Dados Brasileira*: mapeando convergências na direção de um nível de equivalência. São Paulo: RT, vol. 124. ano 28. p. 157-180. jul. - ago. 2019.

MENDES, Laura Schertel Ferreira; DONEDA, Danilo; SOUZA, Carlos Affonso Pereira de; ANDRADE, Norberto Nuno Gomes de. *Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal.* Pensar-Revista de Ciências Jurídicas, v. 23, n. 4, 2018, p. 18.

NAGLI, Luiz Sérgio Dutra. *PANDEMIA NA PANDEMIA:* A ESCALADA DE ATAQUES CIBERNÉTICOS PÓS COVID 19. In: Anais do Congresso Transformação Digital 2020, São Paulo. Fundação Getulio Vargas.

NETFLIX. *O dilema das redes.* Estados Unidos: NETFLIX, 2020. 1 documentário (1h 34min). Disponível em: https://www.netflix.com/search?q=dilema%20das%20redes Acesso em: 12 de set. 2021.

OLIVEIRA, Caroline Lujan de; OLIVEIRA, Antonieta Ferreira Machado de, WATANABE Carolina Yukari Veludo. *Utilização de dados pessoais pelas empresas:* LGPD e o comportamento do consumidor com o macro modelo APCO. Brazilian Journal of Development. Curitiba, v.7, n. 6, p. 63580 - 63591, jun. 2021. Disponível em: https://doi.org/10.34117/bjdv7n6-641 Acesso em: 28 set. 2021

OLIVEIRA, J. V. ; SILVA, L. A. *Cookies de navegador e história da internet*: Desafios à lei brasileira de proteção de dados individuais. São Paulo: UNESP, a.22, n.36, 2018. Disponível em: 2767-Texto do artigo-10305-1-10-20191031.pdf

PEIXOTO, F. H. *Direito e inteligência artificial:* referenciais básicos. Brasília: DR. IA. , 2020.

PRIVACIDADE HACKEADA. Direção: Karim Amer, Jehane Noujaim. Produção de Judy Korin, Pedro Kos, Geralyn Dreyfous, Karim Amer. Estados Unidos: Netflix, 2020.

SEISDEDOS, *A informante que levou o facebook à sua pior crise existencial*. El País, Washington, 2021. Disponível em: https://brasil.elpais.com/tecnologia/2021-10-10/a-informante-que-levou-o-facebook-a-sua-pior-crise-existencial.html. Acesso em 11 out. 2021.

VIAPIANA, Tábata. *TJ-SP reforma sentença e isenta construtora por vazamento de dados de clientes*. In: Consultor Jurídico: Conjur. São Paulo, 1 set. 2021. Disponível em: https://www.conjur.com.br/2021-set-01/tj-sp-reforma-sentenca-isenta-construtora-vazamento-dados . Acesso em: 11 set. 2021.