

**POLÍTICAS PÚBLICAS E A REGULAMENTAÇÃO DAS REDES SOCIAIS: a
Fragilidade dos dados pessoais e como são utilizados.**

**Public Policies and Regulation of Social Media: The Vulnerability of Personal Data
and its Utilization**

Raquel de Almeida Farias

RESUMO

Este trabalho tem como objetivo analisar a fragilidade dos dados pessoais e como eles podem ser manipulados, por meio das redes sociais *Facebook* (Estados Unidos), e *TikTok* (China), esclarecendo como é feito seu processamento e controle. Abordar também, as questões políticas e econômicas por trás do interesse desses dados, demonstrando o quanto cada empresa arrecada anualmente com o desfrute dessas informações. Além disso, demonstrar também, como a lei Geral de proteção de dados determina a forma que esses dados devem ser manuseados e quais medidas o Poder público por meio da Autoridade nacional de Proteção de Dados Pessoais, tem tomado a fim de garantir a privacidade dos cidadãos brasileiros, abordando o caso recente em que a empresa *Meta* foi condenada a indenizar alguns cidadãos brasileiros devido ao vazamento de seus dados. A metodologia utilizada neste trabalho será a de revisão bibliográfica, no qual utilizará como base artigos publicados no período de 2018 á 2022, este método envolve a avaliação minuciosa de estudos anteriores, a identificação de tendências, lacunas no conhecimento e a construção de uma compreensão abrangente do estado atual do domínio de pesquisa em questão limitando-se ao tema específico da utilização dos dados e como o poder público trabalha para garantir a privacidade dos usuários, com intuito de demonstrar o quão frágil são os dados pessoais e a necessidade de atuação do poder público a fim de garantir a segurança dos usuários brasileiros.

PALAVRAS-CHAVE: *TikTok*; *Facebook*; econômico; dados pessoais; interesse; poder público brasileiro; cidadãos.

ABSTRACT

This study aims to analyze the vulnerability of personal data and how they can be manipulated through the social media platforms Facebook (United States) and TikTok (China), elucidating the processing and control mechanisms employed. It also addresses the political and economic aspects behind the interest in these data, demonstrating the annual revenue each company generates from the utilization of such information. Additionally, the study explores how the General Data Protection Law dictates the handling of these data and the measures taken by the government, through the National Data Protection Authority, to ensure the privacy of Brazilian citizens. The paper delves into a recent case where the company Meta was ordered to compensate Brazilian citizens due to a data breach. The methodology employed in this work is a literature review, relying on articles published from 2018 to 2022. This method involves a meticulous evaluation of previous studies, identification of trends, knowledge gaps, and the construction of a comprehensive understanding of the current state of research in the specific domain of data usage. The focus is on illustrating the fragility of personal data and the imperative role of government intervention in safeguarding the privacy of Brazilian users.

Keywords: TikTok; Facebook; economic; personal data; interest; Brazilian government; citizens.

1 INTRODUÇÃO

Desde os primórdios da história mundial, os dados pessoais foram desenvolvidos para que de alguma forma as grandes potências mundiais tivessem controle sobre os países menos desenvolvidos.

Tomando como exemplo o contexto da Guerra Fria em 1947, onde as maiores potências da época eram os Estados Unidos da América e a União Soviética deram início a corrida tecnológica, bélica e ideológica, com intuito de se fortalecer e dominar seus rivais, percebeu-se a necessidade de transmitir os dados de forma rápida e sem limitações territoriais.

Diante desse cenário ambas potências foram responsáveis por planejar e executar ferramentas que por meio de redes iriam mandar localizações exatas de ataques, entre outras atividades de guerra. Com o passar de alguns anos, os Estados Unidos criaram uma tecnologia eficiente, capaz de por meio de uma rede transmitir dados de uma base militar a outra, situação essa que permitiu testes civis nas universidades e que a longo prazo se tornaria a tecnologia atual de transmissão de dados.

Nesse sentido, percebe-se que os dados foram se tornando uma forma de riqueza e poder, na proporção de que os países que os possuíam ter mais poder sobre outros países. A partir desse ponto, no contexto dos dias atuais em que a sociedade se expõe em aplicativos como Instagram que em possuía 1 bilhão de usuários ativos por mês, Facebook tinha 2,6 bilhões de usuários, já o WhatsApp e o YouTube tinham 2 bilhões cada um, conforme os dados do Institut National D'Etudes Démographiques (Instituto Nacional de Estudos Demográficos) da França, se percebe a vulnerabilidade dos dados pessoais a ponto de existir a necessidade de uma regulamentação das redes sociais que no Brasil teve início com o Marco Civil da Internet em 2014.

Baseado no exposto, o problema de pesquisa que direciona esta pesquisa é: Como é realizado o tratamento de dados pelo *TikTok* e *Facebook*, qual o ganho dessas empresas com a dominação sobre os dados pessoais, e quais as medidas tomadas pelo Poder Público Brasileiro para proteger os dados pessoais dos cidadãos brasileiros, com análise do caso recente de vazamento de dados pela empresa *Meta*.

O objetivo deste trabalho é demonstrar a fragilidade dos dados pessoais e como eles podem ser manipulados. Além disso, demonstrar também quais medidas o Poder público tem tomado a fim de garantir a privacidade dos cidadãos brasileiros.

Desta forma, serão abordadas as seguintes pautas: a) a contextualização da legislação vigente (Lei Geral da Proteção de Dados) e a atuação da agência fiscalizadora das atividades empresariais que envolvem o uso de dados no Brasil (ANPD); b) a exposição da forma que os dados pessoais são utilizados pelo *Facebook* e *Tiktok*, acrescidos dos seus lucros e afins; c) demonstrar como o poder público tem atuado e qual a efetividade da sua atuação no sentido de resguardar os dados pessoais dos brasileiros.

Este trabalho irá se utilizar da metodologia de revisão bibliográfica, no qual utilizará como base artigos publicados no período de 2018 á 2022, este método envolve a avaliação minuciosa de estudos anteriores, a identificação de tendências, lacunas no conhecimento e a construção de uma compreensão abrangente do estado atual do domínio de pesquisa em questão, no qual utilizará como base artigos publicados no período de 2018 á 2022, limitando-se ao tema específico da utilização dos dados e como o poder público trabalha para garantir a privacidade dos usuários.

2 O SURGIMENTO DA LEI GERAL DE PROTEÇÃO DE DADOS E A ATUAÇÃO DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS COMO ORGÃO DE FISCALIZAÇÃO

Devido ao grande crescimento ao acesso à internet nos anos de 2016 e 2017, que segundo o IBGE, (SENADO,2020), superavam 70% nos domicílios e de 69% viatelefone celular, e com a viabilização desse meio para realização de compras e pagamentos, no ano de 2018, inspirada nas linhas específicas da regulamentação europeia, aprovado por unanimidade de forma emergencial, a Lei Geral de Proteção de Dados teve origem por meio do PL 53/2018, que alterou a Lei nº 12.965, de 23 de abril de 2014, dando início a um marco legal que regulamentou a utilização, proteção e transferências de dados pessoais no Brasil.

Essa lei, que possui aplicação tanto para empresas locais como para empresas que possuem sede no exterior, desde que a operação de tratamento seja realizada em território brasileiro, destacando que não há aplicação da mesma quando o tratamento de

dados for efetuado por pessoa física com intuito particular e não oneroso, como atividades jornalísticas e artísticas.

Possui como principal objetivo garantir a privacidade e segurança dos cidadãos brasileiros, certificando que haja anuência declarada do usuário para que seja feita a coleta e utilização de seus dados pessoais, como também determina que haja opções de correções, visualizações e remoção desses dados.

Tendo em vista a introdução desses novos direitos que visam garantir a proteção dos direitos fundamentais estipulados pela constituição federal brasileira, como liberdade, privacidade e livre desenvolvimento da pessoa natural, a lei geral da proteção de dados trouxe a oportunidade de aprimoramento das políticas públicas, com a inclusão de medidas técnicas e administrativas com intuito de reduzir o risco dos proprietários dos dados. Como ressalta SABOYA et al.(2019):

diante desse caráter personalíssimo dos dados pessoais aqui já destrinchados, e pelo fato de os mesmos dados exercerem relação direta com a dignidade da pessoa humana, é justo que a proteção de dados pessoais seja elevada ao patamar da mais nobre roupagem conferida pela Constituição Federal pátria, isto é, que seja inserida na esfera tutelar dos direitos fundamentais. Pois, o mundo contemporâneo, muito mais complexo e dinâmico que o nosso texto constitucional, exige que se reconheça o direito à proteção de dados como uma das modalidades de direitos fundamentais expressamente previstas, a fim de que se garanta maior efetividade à salvaguarda desse direito e, com isso, maior combatividade às situações que representem violação a tal prerrogativa. Somente assim se poderá viabilizar uma tutela efetiva aos dados pessoais na amplitude e na relevância que o assunto requer. SABOYA et al.(2019)

Além disso, a lei possui regras especiais para que crianças e adolescentes utilizem a internet, baseadas nos princípios gerais da necessidade e da compatibilidade, que visam que o tratamento de dados deve ocorrer de acordo com as finalidades apontadas ao usuário, sem excessividade e de acordo com o contexto de seu tratamento, ou seja, se um menor de idade entrar nas redes para jogar, dele não poderá solicitar, por exemplo acesso a dados e funcionalidades que desviem do intuito do jogo.

Quaisquer dados, como telefone, endereço, email, idade, estado civil, entre outros estão tutelados por essa regulamentação, sendo vedada a prática abusiva, ilícita e discriminativa em seu tratamento, (BRASIL. Lei nº 13.709, 2018. Artigo 52, inciso II)

sob pena de multa que pode chegar à R\$50 milhões, de reais por dia, como também, impedimento parcial ou total da atividade exercida com relação ao tratamento de dados pessoais.

Frisa-se que a vigência da LGPD foi gradual, ou seja, sua implantação ocorreu de forma escalonada, tendo como início a implantação dos artigos que tratam da formação da ANPD (Autoridade Nacional de Proteção de Dados) em 28 de dezembro de 2018, em 18 de setembro de 2020, os artigos da lei com ressalva dos dispositivos que descrevem as sanções administrativas, e por último em 1 de agosto de 2021 os artigos que tratam das sanções administrativas.

Como relatado acima em 28 de dezembro de 2018, com intuito de trazer mais segurança e solidez para a aplicação da Lei Geral da Proteção de Dados, foi criada a Autoridade Nacional de Proteção de Dados, agência que possui papel fundamental de regular e fiscalizar tanto os entes privados como públicos, podendo realizar alterações e adequações pertinentes para a aplicação da LGPD.

Sua estrutura é composta conforme descreve o art.55-C, com conselho diretor, conselho nacional de proteção de dados, corregedoria, ouvidoria, órgão de assessoramento jurídico próprio, unidades administrativas e unidades especializadas, integrada por membros indicados pelo presidente da república, representantes do poder executivo, do senado federal, da câmara dos deputados, da câmara nacional de justiça, do conselho nacional do ministério público, do Comitê Gestor da Internet no Brasil, de entidades da sociedade civil com atuação na proteção de dados, de instituições (científicas, tecnológicas e de inovação, de entidades representativas do setorempresarial relacionado à proteção de dados. Nesse contexto, PINHEIRO (2020, p.98) destaca:

É muito importante que os membros do Conselho sejam experts no tema de proteção de dados pessoais e também sobre a sua aplicação nos diferentes setores da sociedade, visto que há muitas particularidades que precisarão ser consideradas na implementação da legislação e para seu contínuo aperfeiçoamento. Além disso, o Brasil precisa se manter competitivo e atraente para os investidores estrangeiros, bem como promover um ambiente que fomente inovação tecnológica. Quanto mais heterogêneo puder ser sua composição, melhor, incluindo especialistas técnicos, jurídicos, econômicos, cientistas de dados e comunicadores. PINHEIRO (2020, p.98)

É importante frisar que, como dito anteriormente, a competência das aplicações de sanções regulamentadas pela LGPD, é de total responsabilidade da ANPD, competência essa que prevalecerá, no que se tratar a proteção de dados pessoais, sobre a competência de outros órgãos governamentais.

Em síntese, a ANPD tem de facilitar a acessibilidade aos direitos previstos na LGPD, tanto para os usuários que dispõem de seus dados, quanto aos responsáveis pelo tratamento deles a fim de garantir a segurança e a privacidade. Por via de regra, é fundamental a atuação da ANPD para que haja o cumprimento da LGPD, pois não há como ter efetividade uma lei com previsão de sanções sem um agente de fiscalização. Destaca Danilo Doneda e Laura Schertel Mendes (2018, p. 24):

Além de a Autoridade ser um ponto de referência e orientação para o cidadão, ocorre que o tratamento de dados pessoais é uma atividade complexa e que muitas vezes acontece de forma opaca, sendo realizado por entidades e corporações cujas práticas não são suficientemente transparentes – e que podem ser abusivas. A existência de uma Autoridade que atue de forma coordenada para prevenir e reprimir abusos, fiscalizando e tutelando tratamentos de dados de inteiras coletividades é fundamental para diminuir a distância abissal entre o cidadão e os entes que tratam seus dados, evitando que sejam abertas demandas individuais pelo caminho geralmente longo (e custoso) da via judicial Danilo Doneda e Laura Schertel Mendes (2018, p. 24)

Desta forma, percebe-se que a presença ativa de uma Autoridade que oriente e atue na prevenção de abusos no tratamento de dados pessoais é crucial. Essa Autoridade, ao fiscalizar e tutelar tratamentos em larga escala, reduz a distância entre cidadãos e entidades manipuladoras de dados. Além de evitar demandas individuais demoradas e custosas, essa abordagem fomenta um ambiente mais transparente e responsável, assegurando efetivamente a proteção da privacidade e dos direitos dos cidadãos.

3 ANÁLISE ACERCA DA UTILIZAÇÃO DOS DADOS PESSOAIS

Diante da contextualização trazida acerca da regulamentação de dados vigente no Brasil, se analisará como são aplicadas na prática em duas redes sociais muito importantes e utilizadas no território nacional, sendo elas o *Facebook* e o *TikTok*.

Primeiramente é importante entender a subdivisão existente no sentido de atividade realizada, pois uma empresa pode ser a controladora de dados, bem como a processadora de dados.

Como destaca BRASIL. Autoridade Nacional de Proteção de Dados.(2021 p 06):

(...) o agente de tratamento é definido para cada operação de tratamento de dados pessoais, portanto, a mesma organização poderá ser controladora e operadora, de acordo com sua atuação em diferentes operações de tratamento.

Partindo desse princípio, Pinheiro(2020) esclarece-se que uma empresa controladora de dados é aquela que possui responsabilidade de determinar como e quando os dados serão processados ou seja, ela definirá os meios e os propósitos dos dados que possui.

Já a empresa que é processadora de dados, fica responsável de realizar todo o trabalho em nome da controladora de dados, a fim de alcançar os resultados esperados no sentido de público alvo, mensuração e análise, entre outros.

Como ressalta BRASIL. Autoridade Nacional de Proteção de Dados.(2021 p 07):

O controlador é o agente responsável por tomar as principais decisões referentes ao tratamento de dados pessoais e por definir a finalidade deste tratamento. Entre essas decisões, incluem-se as instruções fornecidas a operadores contratados para a realização de um determinado tratamento de dados pessoais.

O *Facebook* como controlador de dados pessoais, conforme determina a RGPD, precisa aderir medidas para estabelecer a forma que os dados pessoais serão coletados, qual o intuito de sua utilização, bem como determinar um prazo para ficar em sua posse. Além disso, tem a obrigação de garantir que as pessoas tenham acesso aos dados sobre elas, cumprindo com o estabelecido em contrato para processar os dados legalmente e principalmente, de forma segura.

Como processador de dados, de acordo com as diretrizes disponibilizadas pela plataforma, o *Facebook*, atua nos seguintes seguimentos: Públicos personalizados de arquivo de dados, onde utiliza os dados disponibilizados por uma empresa credenciada, a fim de selecionar um público alvo para campanhas publicitárias; Mensuração e análise, que possui o intuito de levantar em números, o desempenho e alcance das publicidades e como o público alcançado reagiu ao anúncio; *Workplace* do *Facebook*, é a função que abre espaço para que os colaboradores de empresas possam interagir entre si usando as ferramentas da plataforma.

Já a atuação do *Tiktok* como controlador de dados, segundo a *BANGBOO* se dá por meio do tipo de conteúdo buscado pelo usuário e tempo de uso da plataforma, informação essa que é revertida em vídeos que sejam compatíveis com as preferências dos usuários. Além disso, quando o usuário se utiliza de outra rede social para fazer login na plataforma, a mesma possui liberdade para coletar informações de terceiros TIKTOK, (2021):

[...] as preferências que você define (como a escolha do idioma), as fotografias e os vídeos que você envia ou cria e os comentários que você faz ("Conteúdo do Usuário"). Nós coletamos o Conteúdo de Usuário através de pré-carregamento no momento da criação, importação ou envio, independentemente de você optar por salvar ou enviar esse Conteúdo de Usuário, a fim de recomendar opções de áudio e fornecer outras recomendações personalizadas. [...] Coletamos certas informações sobre o dispositivo que você usa para acessar a Plataforma, tais como seu endereço IP, agente de usuário, operadora móvel, configurações de fuso horário, identificadores para fins publicitários, modelo de seu dispositivo, o sistema do dispositivo, tipo de rede, IDs do dispositivo, sua resolução de tela e sistema operacional, nomes e tipos de aplicativos e arquivos, padrões ou ritmos de teclas, estado da bateria, configurações de áudio e dispositivos de áudio conectados. Com sua permissão, podemos também coletar dados precisos de localização (como GPS). TIKTOK, (2021)

Ressalta-se ainda, que o TikTok compartilha os dados pessoais com seus parceiros a fim de fazer a destinação correta das publicidades, frisando:

Compartilhamos seus dados com os seguintes terceiros selecionados: Parceiros de Negócios. Se você optar por se registrar para usar a Plataforma usando os detalhes da sua conta de redes sociais (por exemplo, Facebook, Twitter, Instagram, Google), você nos fornecerá ou permitirá que sua rede social nos forneça seu número de telefone, endereço de e-mail, nome de usuário e perfil público. Da mesma forma, compartilharemos certas informações com a rede social relevante. [...] Provedores de pagamento. Se você optar por comprar Moedas ou realizar outras transações relacionadas a pagamentos, compartilharemos os dados com o provedor de pagamento relevante para facilitar essa transação. [...] Provedores de serviço. Fornecemos informações e conteúdo a provedores de serviços que suportam nossos negócios [...] Provedores de análise. Utilizamos provedores de análise para nos ajudar na otimização e melhoria da Plataforma. Nossos fornecedores de análises terceirizados também nos ajudam a veicular anúncios segmentados. [...]

Anunciantes e redes de publicidade. Compartilhamos informações com anunciantes e empresas de medição de terceiros para mostrar quantos e quais usuários da Plataforma visualizaram ou clicaram em um anúncio. [...] Nosso Grupo Corporativo. Também podemos compartilhar suas informações com outros membros, subsidiárias ou afiliadas do nosso grupo corporativo, para fornecer a Plataforma, incluindo a melhoria e otimização da Plataforma, impedindo o uso ilegal e dando suporte aos usuários. [...] Aplicação da Lei. Compartilharemos suas informações com agências de aplicação da lei, autoridades públicas ou outras organizações se for legalmente exigido. (TIKTOK,(2021)

Com acesso ao endereço de IP, localização e dispositivo, o Tiktok pode também identificar falas, objetos, escritas e dados mais sensíveis nos vídeos publicados pelos usuários. Outrossim, a plataforma pode obter acesso ao conteúdo de conversas por mensagens, bem como analisar o conteúdo das mensagens, o que no Brasil não é regulamentado especificamente.

Desta forma, considerando a autonomia das plataformas, verifica-se como é possível os dados pessoais serem controlados e como a privacidade dos usuários é comprometida diante toda exploração realizada com seus dados, exemplo disso, é o caso recente de vazamento de dados da empresa *Meta*, dona do *Facebook*, que se analisará adiante.

4 EXAME DO CASO DE VAZAMENTO DE DADOS DO FACEBOOK

Como relatado anteriormente, será examinado um caso recente no Brasil onde a empresa *Meta*, proprietária o *Facebook*, foi condenada a indenizar vários usuários brasileiros pelo vazamento de dados ocorrido.

Por meio de uma ação civil coletiva, autos: 0812915-60.2021.8.10.0001; na comarca da Ilha de São Luís, no Maranhão, com autoria do Instituto Nacional, foi possível constatar que o fato ocorreu em 2021, onde a empresa permitiu com que dados como número de telefone, e-mail, nome, data de nascimento e local de trabalho, de

aproximadamente 533 (quinhentos e trinta e três) milhões de usuários, de 106 países, destes, 8.064,916 (oito milhões sessenta e quatro mil novecentos e dezesseis) usuários brasileiros.

Na sentença foi reconhecida a violação dos direitos da personalidade, do respeito a privacidade e da autodeterminação informativa, tendo em vista que a empresa como controladora e processadora de dados não cumpriu com sua obrigação de garantir a segurança dos dados e a destinação correta em relação a sua utilização, bem como ao seu descarte.

Diante dessa violação, foi estabelecida uma condenação por danos morais coletivos no montante de R\$ 72.000.000,00 (setenta e dois milhões de reais), a ser destinada ao Fundo Estadual de Direitos Difusos. adicionalmente, o pagamento de uma indenização por danos morais individuais no valor de R\$ 500,00 (quinhentos reais) aos usuários diretamente afetados pelo vazamento de dados pessoais.

O vazamento de dados promovido pelo *Facebook* evidencia não apenas falhas significativas nos protocolos de segurança, mas também revela uma preocupante falta de ética na gestão de informações sensíveis. Ao expor dados pessoais de milhões de usuários, a plataforma compromete a confiança depositada por seus usuários, levantando questões sérias sobre a responsabilidade corporativa.

Esse incidente não é apenas uma violação da privacidade, mas também uma traição da confiança que os usuários depositaram na plataforma para proteger suas informações pessoais.

As consequências desse vazamento reverberam além do imediato, deixando cicatrizes profundas na relação entre empresas de tecnologia e usuários, destacando a necessidade urgente de medidas mais rigorosas e éticas na gestão de dados.

Ressalta-se que não é apenas uma questão de segurança cibernética; é uma ameaça à sociedade e à democracia, como afirma CALLEJÓN, (2020 p.35) :

Por outro lado, este modelo, construído para a negociação publicitária, mediante utilização massiva de dados pessoais e a configuração de perfis através de algoritmos, começou a ser utilizado posteriormente na propaganda política. Sua aplicação a este âmbito provocou novas lesões a direitos, ao utilizar tais perfis psicológicos para elaborar e difundir propaganda subliminar particularizada. Esta propaganda se encaixa num

contexto de radicalização, fragmentação do espaço público, produção de bolhas, desinformação e falsificação de notícias, a fim de potencializar sua eficácia. CALLEJÓN, (2020 p.35)

Percebe-se que quando informações pessoais são exploradas indevidamente, seja para fins publicitários, políticos ou outros, a integridade do processo democrático é comprometida. A manipulação de dados sociais pode influenciar comportamentos, moldar opiniões e distorcer o panorama político. Nesse contexto, ressalta-se SILVEIRA, 2019, p. 57

A modulação da opinião pública nas redes digitais é realizada principalmente pelo controle da visualização de conteúdo. As plataformas de relacionamento social online, em geral, não produzem conteúdos, mas direcionam, organizam e disseminam as produções de seus usuários, ou seja, utilizam técnicas de modulação. A modulação não seria possível sem um sistema que sempre mantém algumas aberturas e impõe certos limites. A modulação, em geral, é invisível para os viventes, por isso trata-se de um tipo de manipulação da opinião bem mais perigosa SILVEIRA,(2019, p. 57).

Nesse sentido, tendo em vista a atuação do judiciário no caso citado, percebe-se o quão importante e necessário é a atuação do poder público para assegurar os direitos dos brasileiros no sentido de resguardar a privacidade, os direitos da personalidade e da autodeterminação informativa, visando assim prevenir abusos e vazamentos que possam comprometer a privacidade e a segurança dos cidadãos.

Com a aplicação da LGPD, fiscaliza-se e se impõe penalidades dissuasivas que funcionam como barreiras contra práticas inadequadas por parte de organizações e empresas. Além disso, a implementação efetiva da LGPD não apenas resguarda a privacidade dos cidadãos, mas também fortalece a confiança na utilização de serviços digitais.

Ao garantir que as informações pessoais estejam protegidas e tratadas de forma ética, a legislação fomenta uma relação mais transparente e confiável entre consumidores e empresas, além de criar um ambiente regulatório que responsabiliza aqueles que manipulam dados pessoais, o governo contribui para a construção de uma sociedade digital mais segura e resiliente.

Com essa atuação há um estímulo à inovação responsável. Ao estabelecer diretrizes claras e equilibradas, o governo incentiva o desenvolvimento de tecnologias e práticas empresariais que respeitem a privacidade e a integridade dos dados. Esse equilíbrio promove um ecossistema digital no qual a inovação coexiste harmoniosamente com a proteção dos direitos individuais, construindo assim uma base sólida para o progresso tecnológico sustentável e ético.

4 CONSIDERAÇÕES FINAIS

Em consideração ao exposto, observamos que a evolução histórica dos dados pessoais, desde os primórdios até os dias atuais, destaca o papel fundamental dessas informações como fonte de riqueza e poder. O contexto da Guerra Fria exemplifica como a tecnologia de transmissão de dados, inicialmente desenvolvida para fins militares, moldou o cenário contemporâneo.

A legislação brasileira, notadamente a Lei Geral de Proteção de Dados (LGPD), representa um marco significativo na proteção da privacidade dos cidadãos, estabelecendo direitos e responsabilidades para o tratamento adequado dos dados pessoais. A criação da Autoridade Nacional de Proteção de Dados (ANPD) fortalece a supervisão e fiscalização, reduzindo a distância entre cidadãos e entidades manipuladoras de dados.

A análise do tratamento de dados pelo Facebook e TikTok revela a complexidade envolvida, com essas plataformas atuando como controladoras e processadoras, impactando diretamente a privacidade dos usuários. O recente caso de vazamento de dados pelo Facebook, resultando em condenação e indenização, destaca a importância das regulamentações e da atuação judicial para assegurar responsabilidade e ética na gestão de informações sensíveis.

Ressaltando, portanto, a importância de medidas rigorosas e éticas na gestão de dados, não apenas como uma questão de segurança cibernética, mas como uma salvaguarda essencial para a democracia.

REFERÊNCIAS

BANGBOO. "O TikTok é seguro? Veja como funciona a coleta de dados do app!" Disponível em: <https://www.bangboo.com.br/o-tiktok-e-seguro-conheca-as-permissoes-do-aplicativo-para-coleta-de-dados>. Acesso em : 02 dez. 2023.

BRASIL. Autoridade Nacional de Proteção de Dados. Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais. Brasília: mai. 2021. Disponível em: . Acesso em: 03 dez 2023. p. 06.

BRASIL. Autoridade Nacional de Proteção de Dados. Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais. Brasília: mai. 2021. Disponível em: . Acesso em: 03 dez 2023. p. 07

CALLEJÓN, Francisco Balaguer. Redes sociais, companhias tecnologicas e democracia. Catedrático de Direito Constitucional na Universidade de Granada, Espanha: Editora, 2020.

DANTAS, Luizmar Peixoto(A SEGURANÇA DA INFORMAÇÃO COMO FERRAMENTA PRÁTICA DE PROTEÇÃO DOS DADOS PESSOAIS E A LEI GERAL DE PROTEÇÃO DE DADOS(LGPD)Artigo Científico(Graduação em Direito), Universidade Federal de Goiás, Goiás, GO, 2022

DONEDA, Danilo; MENDES, Laura Schertel. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da Proteção de Dados no Brasil. Revista de Direito do Consumidor, São Paulo, v. 120, p. 555-587, 2018.

Disponívelem:

https://www.academia.edu/42740879/Comentário_à_nova_Lei_de_Proteção_de_Dados_lei_13.709_2018_o_novo_paradigma_da_proteção_de_dados_no_brasil?auto=download> Acesso em :03 dez 2023.

FACEBOOK, Meta. JO que é o Regulamento Geral sobre a Proteção de Dados (RGPD)?. META, 2023. Disponível em: <https://pt-br.facebook.com/business/gdpr>. Acesso em: 06 out. 2023.

FINANÇAS, O Globo. Lucro da dona do TikTok salta 79% e supera rivais Alibaba e Tencent. O GLOBO, 2023. Disponível em: <https://oglobo.globo.com/economia/financas/noticia/2023/04/lucro-da-dona-do-tiktok-salta-79percent-e-supera-rivais-alibaba-e-tencent.ghtml>. Acesso em: 06 out. 2023

LIMA, Monique. A marca de rede social mais valiosa do mundo: TikTok é a marca de

rede social mais valiosa do mundo em 202 Leia mais em: <https://forbes.com.br/forbes-money/2023/01/tiktok-e-a-marca-de-rede-social-mais-valiosas-do-mundo-em-2023/>.
forbes, 2023. Disponível em: TikTok é a marca de rede social mais valiosa do mundo em 2020

Disponível em: <https://forbes.com.br/forbes-money/2023/01/tiktok-e-a-marca-de-rede-social-mais-valiosas-do-mundo-em-2023/>. Acesso em: 06 out. 2023.

LONCOMILLA, Gina Viviane Mardones. TikTok e a presença do capital chinês na indústria fonográfica ocidental: um olhar pela economia política da internet. 1. ed. Intercom – Sociedade Brasileira de Estudos Interdisciplinares da Comunicação: Virtual, 2020.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. LGPD: Lei Geral de Proteção de Dados comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2020. E-book.

PINHEIRO, Patricia Peck; Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD) 2. ed. – São Paulo : Saraiva Educação, 2020

PRIMIÉRI, Vitória de Castro. (REDES SOCIAIS E A REGULAMENTAÇÃO ESTATAL). Artigo Científico (Graduação em Direito), Faculdade de Direito, Universidade São Judas Tadeu, São Paulo, SP, 2022

SENADO FEDERAL. Lei Geral de Proteção de Dados entra em vigor. Notícias, Brasília, 18 set. 2020.

Disponível em: <https://www12.senado.leg.br/noticias/materias/2020/09/18/lei-geral-de-protecao-de-dados-entra-em-vigor>. Acesso em: 02 dez. 2023.

SILVEIRA, Sergio Amadeu da. Democracia e os Códigos Invisíveis. São Paulo: Sesc, 2019.

TIKTOK. Política de Privacidade. 2 jun. 2021. Disponível em:

<<https://www.tiktok.com/legal/privacy-policy-row?lang=pt-BR>>. Acesso em: 02 dez 2023.

TRIBUNAL DE JUSTIÇA DO MARANHÃO, ação civil pública Disponível em: [Consulta pública · Tribunal de Justiça do Estado do Maranhão - 1º Grau \(tjma.jus.br\)](https://www.tjma.jus.br)
Acesso em: 10 dez 2023.