ESTRATÉGIAS DE PROTEÇÃO DE DADOS E COMBATE À DESINFORMAÇÃO EM PAÍSES EMERGENTES: UM ESTUDO COMPARATIVO

DATA PROTECTION STRATEGIES AND COMBATING DISINFORMATION IN EMERGING COUNTRIES: A COMPARATIVE STUDY

Daniel David Guimarães Freire [1]

Bianca Barrocas [2]

RESUMO

O artigo explora a intersecção entre a proteção de dados pessoais e o fenômeno da desinformação em nações emergentes. Destaca os desafios que esses países enfrentam, como infraestrutura tecnológica deficiente, desigualdades socioeconômicas e baixos níveis de alfabetização digital, que comprometem a implementação eficaz de políticas de proteção de dados. Além disso, a desinformação agrava a situação ao minar a confiança nas instituições e dificultar a aplicação dessas políticas. A análise comparativa entre Brasil, Índia e África do Sul ilustra as distintas abordagens adotadas por esses países, destacando tanto os avanços quanto as lacunas existentes. O artigo propõe estratégias como a promoção da alfabetização digital, colaboração internacional e uso de tecnologias emergentes para fortalecer a proteção de dados e combater a desinformação.

Palavras-chave: Proteção de dados; Desinformação; Países emergentes; Alfabetização digital; Colaboração internacional.

ABSTRACT

The article explores the intersection between personal data protection and the phenomenon of disinformation in emerging nations. It highlights the challenges these countries face, such as poor technological infrastructure, socioeconomic inequalities, and low levels of digital literacy, which hinder the effective implementation of data protection policies. Additionally, disinformation exacerbates the situation by undermining trust in institutions and complicating the enforcement of these policies. The comparative analysis between Brazil, India, and South Africa illustrates the

[1] Mestrando e Bacharel pela Universidade Federal do Estado do Rio de Janeiro. E-mail: danieldavidgfreire@gmail.com

[2] Bacharel pela Universidade Federal do Estado do Rio de Janeiro. E-mail: barrocas.bianca@edu.unirio.br

different approaches adopted by these countries, highlighting both advances and existing gaps. The article proposes strategies such as promoting digital literacy, international collaboration, and the use of emerging technologies to strengthen data protection and combat disinformation.

Keywords: Data protection; Disinformation; Emerging countries; Digital literacy; International collaboration.

1. INTRODUÇÃO

Na era digital, a proteção de dados pessoais surge como um tema central nas políticas públicas globais. À medida que a interconectividade e a dependência de tecnologias digitais se expandem, a privacidade dos dados torna-se uma preocupação fundamental para governos, empresas e cidadãos (Bennett, 2018; Solove, 2021). A coleta, armazenamento e utilização de dados pessoais são agora práticas comuns em diversos setores da economia e da sociedade, impulsionadas pela rápida digitalização (Zuboff, 2019). Entretanto, tal transformação tecnológica nem sempre é acompanhada por uma compreensão adequada dos riscos associados à privacidade e à segurança dos dados, particularmente em países emergentes, onde fatores como infraestrutura limitada, desigualdades socioeconômicas e baixos níveis de alfabetização digital agravam os desafios (Kshetri, 2017; Bennett & Raab, 2020).

Países emergentes, caracterizados por economias em rápido crescimento e pela adoção acelerada de novas tecnologias, enfrentam dificuldades particulares na formulação e implementação de políticas eficazes de proteção de dados (Floridi, 2016; Kuner, 2020). Embora o acesso à internet e a dispositivos móveis esteja em expansão, as estruturas legais e regulatórias frequentemente não conseguem acompanhar essa evolução, resultando em lacunas significativas na proteção dos direitos dos cidadãos (González Fuster, 2014).

Paralelamente, o fenômeno da desinformação torna-se um desafio global crescente, com impactos especialmente agudos pelo mundo e em especial, países emergentes (Bradshaw & Howard, 2019). A disseminação deliberada de informações falsas ou enganosas mina os esforços de proteção de dados, manipulando a opinião

pública e enfraquecendo a confiança nas iniciativas de privacidade e segurança digital (Marwick & Lewis, 2017). E em contextos em que a confiança nas instituições é frágil e a população tem acesso limitado a fontes confiáveis de informação, esses riscos são ainda maiores (Donovan, 2020).

Este artigo busca explorar a complexa relação entre a proteção de dados em países emergentes e o impacto da desinformação. A análise inclui uma visão geral dos desafios e oportunidades que esses países enfrentam na criação de políticas eficazes de proteção de dados, além de examinar como a desinformação afeta a percepção pública e a implementação dessas políticas. Estudos de caso de países como Brasil, Índia e África do Sul serão utilizados para ilustrar diferentes abordagens e desafios. Ao final, serão discutidas estratégias para combater a desinformação e fortalecer a proteção de dados, com ênfase na promoção da alfabetização digital, na colaboração internacional e no uso de tecnologias emergentes para proteger os dados dos cidadãos e promover a confiança no ambiente digital.

2. BACKGROUND HISTÓRICO DA PROTEÇÃO DE DADOS E DA DESINFORMAÇÃO

A proteção de dados surge como conceito jurídico e político de acordo com o avanço da tecnologia e a digitalização das informações. Durante as décadas de 1970 e 1980, com o aumento do uso de computadores e a criação de bases de dados eletrônicas, a preocupação com a privacidade e a segurança das informações pessoais começou a ganhar relevância (Westin, 1967; Flaherty, 1989). Certos países como a Alemanha e a Suécia foram pioneiros na criação de leis de proteção de dados, estabelecendo os primeiros marcos regulatórios para controlar o uso de dados pessoais por entidades públicas e privadas (Bennett, 1992).

Nos anos 2000, a globalização e a explosão da internet trouxeram novos desafios para a proteção de dados. A coleta e o processamento de informações pessoais se tornaram práticas comuns e a necessidade de regulamentação mais robusta tornou-se evidente (Solove, 2004). A União Europeia liderou esse movimento a partir da introdução da Diretiva de Proteção de Dados de 1995, que estabeleceu

padrões comuns para a proteção de dados em todos os Estados-membros (González Fuster, 2014). O Regulamento Geral sobre a Proteção de Dados (GDPR), adotado em 2018, representou um avanço significativo, não apenas para Europa, mas para o mundo, influenciando a criação de legislações similares em várias outras regiões, incluindo países emergentes como o Brasil, com a Lei Geral de Proteção de Dados (LGPD) (Kuner, 2020).

Com o avanço da globalização e da digitalização, os países emergentes começaram a desempenhar um papel cada vez mais significativo no cenário global. Essas nações, caracterizadas por economias em rápido crescimento e uma população jovem e conectada, experimentaram uma rápida expansão do acesso à internet e ao uso de dispositivos móveis (Kshetri, 2017). No entanto, essa rápida digitalização ocorreu frequentemente em um contexto de infraestrutura limitada e desigualdades socioeconômicas, criando desafios para a proteção de dados (Bennett & Raab, 2020).

Em muitos desses países, as leis de proteção de dados foram adotadas recentemente e ainda estão em processo de implementação. O Brasil, por exemplo, promulgou a LGPD em 2018, com a lei entrando em vigor em 2020 (Doneda & Almeida, 2021). Na Índia, a legislação de proteção de dados ainda está em desenvolvimento, refletindo o processo gradual de adaptação das políticas públicas às novas realidades digitais (Chawla & Bhandari, 2021). A África do Sul, com a implementação da Protection of Personal Information Act (POPIA), também demonstra como os países emergentes estão começando a lidar com a necessidade de regulamentar o uso de dados pessoais (Pistorius, 2017).

Esses países enfrentam desafios específicos, como a falta de capacitação institucional e a necessidade de equilibrar o desenvolvimento econômico com a proteção dos direitos dos cidadãos. A implementação dessas leis requer não apenas a criação de um marco regulatório, mas também a educação e a conscientização da população sobre a importância da privacidade e da segurança digital (Sax, 2019).

3. A EVOLUÇÃO DA DESINFORMAÇÃO E SEU IMPACTO NA SOCIEDADE

A desinformação, embora não seja um fenômeno novo, ganhou novas dimensões com a expansão das mídias digitais e das redes sociais (Wardle & Derakhshan, 2017). A capacidade de disseminar rapidamente informações falsas ou enganosas para grandes audiências transformou a desinformação em uma ferramenta poderosa para influenciar a opinião pública, manipular processos democráticos e minar a confiança nas instituições (Marwick & Lewis, 2017).

Durante eventos políticos significativos, como eleições e referendos, a desinformação tem sido utilizada para polarizar a sociedade e criar divisões profundas (Bradshaw & Howard, 2019). Além disso, durante crises de saúde pública, como a pandemia de COVID-19, a desinformação sobre vacinas e tratamentos foi amplamente disseminada, gerando confusão e colocando vidas em risco (Donovan, 2020). Em países emergentes, onde o acesso à informação confiável pode ser limitado e onde as instituições nem sempre são robustas, o impacto da desinformação pode ser particularmente devastador (Kshetri, 2017).

No contexto da proteção de dados, a desinformação tem sido usada para criar incertezas sobre a segurança das informações pessoais e para semear desconfiança em relação a novas tecnologias e regulamentações. Em muitos casos, a desinformação é disseminada por grupos com interesses próprios, que buscam manipular a percepção pública para promover agendas políticas ou comerciais (González Fuster, 2014). O combate à desinformação é, portanto, um componente chave na criação de um ambiente digital seguro e confiável, especialmente em países emergentes (Donovan, 2020).

4. PROTEÇÃO DE DADOS EM PAÍSES EMERGENTES: DESAFIOS E OPORTUNIDADES

Como mencionado, a proteção de dados pessoais tornou-se uma prioridade crescente para governos ao redor do mundo. No entanto, em países emergentes, a adoção de políticas de proteção de dados tem sido um processo complexo e, muitas vezes, fragmentado (Bennett & Raab, 2020). Isso ocorre porque muitos desses países estão simultaneamente enfrentando desafios relacionados à

infraestrutura tecnológica, desigualdades sociais e econômicas, e níveis variados de alfabetização digital (Kshetri, 2017). Como resultado, a proteção de dados em países emergentes frequentemente se desenvolve de maneira desigual, com grandes disparidades entre as regiões urbanas e rurais, bem como entre diferentes grupos socioeconômicos (Doneda & Almeida, 2021).

Além disso, a rápida digitalização em países emergentes, impulsionada pela expansão do acesso à internet e ao uso de dispositivos móveis, não foi acompanhada por um desenvolvimento paralelo de marcos regulatórios robustos (Sax, 2019). Em muitos casos, as leis de proteção de dados, quando existem, são recentes e ainda estão em processo de implementação. Isso cria um cenário em que os dados pessoais dos cidadãos estão vulneráveis a abusos, tanto por parte de empresas que operam sem a devida consideração pela privacidade quanto por agentes mal-intencionados, que exploram essas lacunas para fins ilícitos (Chawla & Bhandari, 2021).

Por outro lado, o crescimento econômico e o aumento da conectividade em países emergentes oferecem oportunidades significativas para o fortalecimento das políticas de proteção de dados. Com a expansão do comércio eletrônico, dos serviços financeiros digitais e das plataformas de mídia social, há uma demanda crescente por medidas que garantam a segurança e a privacidade dos dados dos usuários (Kuner, 2020). Governos e empresas em países emergentes estão começando a reconhecer a importância de proteger os dados como uma forma de construir confiança com os consumidores e de promover um ambiente digital seguro e próspero (González Fuster, 2014).

Os desafios enfrentados pelos países emergentes na implementação de políticas de proteção de dados são complexos e variam de acordo com o contexto local. Entre os principais desafios estão:

4.1. Infraestrutura Tecnológica Deficiente

Muitos países emergentes ainda lutam com infraestrutura tecnológica inadequada, o que dificulta a implementação eficaz de políticas de proteção de dados (Pistorius, 2017). Em áreas rurais ou em regiões com menor desenvolvimento

econômico, o acesso à internet de alta qualidade é limitado, o que impacta a capacidade de aplicar e monitorar as regulamentações de proteção de dados (Kshetri, 2017). Além disso, a falta de infraestrutura também afeta a capacidade dos governos de realizar a supervisão e a fiscalização necessárias para garantir a conformidade com as leis de proteção de dados (Bennett & Raab, 2020).

4.2. Desigualdades Socioeconômicas

As desigualdades socioeconômicas representam um obstáculo significativo para a proteção de dados em países emergentes (Doneda & Almeida, 2021). Grupos marginalizados, como as populações de baixa renda e as comunidades rurais, muitas vezes têm menor acesso à informação sobre seus direitos de privacidade e menos recursos para proteger seus dados. Isso cria uma situação em que as populações mais vulneráveis estão mais expostas a abusos de privacidade e a riscos associados ao uso indevido de seus dados pessoais (Chawla & Bhandari, 2021).

4.3. Baixos Níveis de Alfabetização Digital

A alfabetização digital é um componente crítico da proteção de dados, pois permite que os indivíduos compreendam como seus dados são coletados, usados e protegidos (Sax, 2019). Em muitos países emergentes, os níveis de alfabetização digital são baixos, o que torna a população mais suscetível a práticas de coleta de dados invasivas e a abusos por parte de empresas e governos (Kshetri, 2017). A falta de educação sobre privacidade digital também dificulta a conscientização pública sobre os riscos associados ao uso de tecnologias digitais, o que, por sua vez, afeta a eficácia das políticas de proteção de dados (Doneda & Almeida, 2021).

4.4. Desafios Regulatórios e de Implementação

Em muitos países emergentes, as estruturas legais para a proteção de dados ainda estão em desenvolvimento. Leis recentes, como a Lei Geral de Proteção

de Dados (LGPD) no Brasil, são passos importantes na direção certa, mas a implementação eficaz dessas leis é frequentemente prejudicada por desafios institucionais e regulatórios (Pistorius, 2017). A falta de recursos, a burocracia, e a falta de capacitação em agências reguladoras são alguns dos obstáculos que dificultam a aplicação dessas políticas (Bennett & Raab, 2020).

5. OPORTUNIDADES PARA O FORTALECIMENTO DAS POLÍTICAS DE PROTEÇÃO DE DADOS

Apesar dos desafios, há várias oportunidades para o fortalecimento das políticas de proteção de dados em países emergentes. Abaixo estão algumas das principais oportunidades identificadas:

5.1. Crescimento do Comércio Eletrônico e Serviços Digitais

O crescimento do comércio eletrônico e dos serviços digitais em países emergentes cria uma demanda crescente por políticas de proteção de dados (Kuner, 2020). Empresas que operam nesses mercados reconhecem a necessidade de proteger os dados dos consumidores como uma forma de construir confiança e garantir a sustentabilidade de seus negócios. Isso abre uma janela de oportunidade para o desenvolvimento de políticas públicas que incentivem as melhores práticas de proteção de dados e que promovam a conformidade com as regulamentações internacionais (González Fuster, 2014).

5.2. Colaboração Internacional e Regional

A colaboração internacional e regional pode ser uma ferramenta poderosa para fortalecer as políticas de proteção de dados em países emergentes (Bennett & Raab, 2020). Organizações internacionais, como a União Europeia e as Nações Unidas, têm promovido iniciativas para apoiar países em desenvolvimento na criação e implementação de leis de proteção de dados (Kuner, 2020). Além disso, a

cooperação regional, como a Aliança Latino-Americana de Proteção de Dados, pode ajudar a harmonizar as regulamentações e promover a troca de melhores práticas entre os países (Doneda & Almeida, 2021).

5.3. Uso de Tecnologias Emergentes

As tecnologias emergentes, como a inteligência artificial e o blockchain, oferecem novas oportunidades para a proteção de dados (Sax, 2019). Essas tecnologias podem ser usadas para criar sistemas mais seguros e transparentes de gerenciamento de dados, permitindo que os indivíduos tenham maior controle sobre suas informações pessoais. Além disso, o uso de tecnologias avançadas pode ajudar a superar alguns dos desafios de infraestrutura e a melhorar a eficácia das políticas de proteção de dados em países emergentes (Pistorius, 2017).

5.4. Conscientização e Educação Pública

A promoção da conscientização e da educação pública sobre a proteção de dados é fundamental para o fortalecimento das políticas nessa área (Bennett & Raab, 2020). Campanhas educativas que informem os cidadãos sobre seus direitos de privacidade e sobre como proteger seus dados pessoais podem ajudar a reduzir a vulnerabilidade a abusos e a aumentar a demanda por práticas responsáveis de proteção de dados (Chawla & Bhandari, 2021). Além disso, a inclusão da educação digital nos currículos escolares pode preparar as futuras gerações para navegar no ambiente digital com maior segurança e responsabilidade (Sax, 2019).

6. ANÁLISE COMPARATIVA DE POLÍTICAS DE PROTEÇÃO DE DADOS EM PAÍSES EMERGENTES

Na era digital, a proteção de dados pessoais surge como uma prioridade global, especialmente em países emergentes, onde o crescimento econômico e a adoção rápida de tecnologias digitais geram demanda por políticas robustas e

eficazes para garantir a segurança das informações pessoais (Bennett & Raab, 2020; Zuboff, 2019). No entanto, os desafios enfrentados por essas nações são complexos e multifacetados, tendo em vista as disparidades econômicas, sociais e tecnológicas que influenciam a implementação e a eficácia dessas políticas (Kshetri, 2017; Sax, 2019).

6.1. Brasil e a Lei Geral de Proteção de Dados (LGPD)

O Brasil, como um dos principais países emergentes, introduziu a Lei Geral de Proteção de Dados (LGPD) em 2018, com a lei entrando em vigor em 2020. A LGPD foi inspirada pelo Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia, buscando criar um ambiente regulatório que proteja os direitos dos cidadãos enquanto promove o desenvolvimento econômico digital (Doneda & Almeida, 2021). No entanto, a implementação da LGPD enfrenta desafios significativos, como a falta de infraestrutura tecnológica adequada e a necessidade de capacitação das instituições responsáveis pela fiscalização e aplicação da lei (Sax, 2019). Além disso, o Brasil enfrenta desigualdades regionais e socioeconômicas que afetam a uniformidade na aplicação da lei, especialmente em áreas rurais e entre populações vulneráveis (Kshetri, 2017).

6.2. Índia e sua Abordagem em Evolução

A Índia, outro país emergente de destaque, está em processo de desenvolvimento de sua legislação de proteção de dados. O projeto de lei de proteção de dados pessoais, que ainda está sendo discutido, reflete os esforços do país para equilibrar a proteção dos direitos dos cidadãos com o crescimento de sua economia digital (Nair, & Shaikh, 2022). A Índia enfrenta desafios semelhantes aos do Brasil, incluindo desigualdades socioeconômicas e níveis variados de alfabetização digital, que impactam a eficácia das políticas de proteção de dados (Bennett & Raab, 2020). A infraestrutura tecnológica desigual e a falta de capacitação institucional também são

obstáculos importantes que a Índia precisa superar para garantir a proteção adequada dos dados pessoais de seus cidadãos (Kshetri, 2017; Sax, 2019).

6.3. África do Sul e a Protection of Personal Information Act (POPIA)

Na África do Sul, a Protection of Personal Information Act (POPIA), implementada em 2020, representa um passo importante na proteção de dados no continente africano. A POPIA é fruto de inspiração em normas internacionais e tem como propósito proteger os direitos de privacidade dos cidadãos sul-africanos, enquanto promove a confiança no ambiente digital (Koornhof et al. 2018). No entanto, a África do Sul enfrenta desafios significativos na implementação da POPIA, devido a infraestrutura tecnológica limitada e a necessidade de capacitação das autoridades reguladoras (Bennett & Raab, 2020). Além disso, as disparidades econômicas e sociais exacerbam as dificuldades na aplicação uniforme da lei em todo o país (Doneda & Almeida, 2021).

6.4. Comparação e Análise Crítica

Em que pese o Brasil, a Índia e a África do Sul tenham adotado abordagens diferentes para a proteção de dados, todos enfrentam desafios semelhantes, como a infraestrutura deficiente, as desigualdades socioeconômicas e os baixos níveis de alfabetização digital (Sax, 2019; Kshetri, 2017). Essas nações também compartilham a necessidade de equilibrar o desenvolvimento econômico com a proteção dos direitos dos cidadãos, criando políticas que sejam ao mesmo tempo eficazes e adaptáveis às realidades locais (Nair, & Shaikh, 2022; Doneda & Almeida, 2021). A comparação dessas abordagens revela a importância da cooperação internacional e da troca de melhores práticas para superar os desafios comuns e fortalecer a proteção de dados em países emergentes (Kuner, 2020).

7. ESTRATÉGIAS PARA COMBATER A DESINFORMAÇÃO E FORTALECER A PROTEÇÃO DE DADOS

A desinformação, caracterizada pela disseminação deliberada de informações falsas ou enganosas, tornou-se um desafio global, com impactos especialmente graves em países emergentes (Bradshaw & Howard, 2019; Marwick & Lewis, 2017). Isto pois a desinformação não apenas compromete a confiança pública nas instituições, mas também enfraquece os esforços de proteção de dados, criando incertezas sobre a segurança das informações pessoais e dificultando a implementação de políticas públicas eficazes para seu combate.

7.1. Promoção da Alfabetização Digital

Uma das estratégias mais eficazes para combater a desinformação é a promoção da alfabetização digital, capacitando os cidadãos a identificar e avaliar criticamente as informações que consomem. Em países emergentes, onde os níveis de alfabetização digital são frequentemente baixos, a educação pública sobre o uso seguro e responsável das tecnologias digitais é essencial para reduzir a vulnerabilidade à desinformação (Kshetri, 2017). Além disso, a integração de disciplinas relacionadas à ética da informação nos currículos educacionais pode fomentar uma compreensão mais profunda dos impactos sociais e políticos da desinformação, desde o início do contato com estas tecnologias, que vem acontecendo cada vez mais cedo. Programas educacionais focados na privacidade digital e na proteção de dados podem aumentar a conscientização sobre os riscos associados à desinformação e fortalecer a resiliência da população contra tentativas de manipulação (Bennett & Raab, 2020).

É igualmente importante que as políticas governamentais incentivem a colaboração entre setores privados, públicos e organizações não-governamentais para ampliar o alcance dessas iniciativas educacionais. O investimento em campanhas de conscientização pública, usando múltiplos canais de comunicação, também pode contribuir significativamente para a disseminação de práticas seguras no ambiente digital. Além disso, parcerias internacionais podem ser estabelecidas para compartilhar recursos e melhores práticas em alfabetização digital, aumentando a eficácia das estratégias de combate à desinformação em um contexto global.

7.2. Colaboração Internacional e Regional

A cooperação internacional e regional é crucial para o combate à desinformação, especialmente em países emergentes, onde os recursos e a infraestrutura podem ser limitados (Kuner, 2020). Organizações internacionais, como a União Europeia, têm promovido iniciativas para apoiar a luta contra a desinformação, incluindo a criação de redes de verificação de fatos e a promoção de normas globais de proteção de dados (Doneda & Almeida, 2021). Além disso, essas organizações têm investido em capacitação técnica e tecnológica para ajudar países emergentes a desenvolverem suas próprias capacidades de combate à desinformação.

A colaboração entre países emergentes e organizações internacionais pode ajudar a harmonizar as regulamentações, promover a troca de melhores práticas e fortalecer a capacidade de resposta a campanhas de desinformação (Bennett & Raab, 2020). Além disso, a criação de parcerias entre governos, setor privado e sociedade civil em nível regional pode facilitar a coordenação de esforços para combater a disseminação de desinformação. É importante também que essas colaborações incentivem o desenvolvimento de tecnologias de inteligência artificial e análise de dados para a detecção precoce de campanhas de desinformação. A cooperação em pesquisa e desenvolvimento de novas ferramentas tecnológicas pode proporcionar aos países emergentes os recursos necessários para responder de maneira mais eficaz a esses desafios. Finalmente, a implementação de políticas comuns e a criação de marcos regulatórios compartilhados podem garantir uma abordagem mais coesa e eficaz no combate à desinformação em um cenário global interconectado.

7.3. Uso de Tecnologias Emergentes

As tecnologias emergentes, como a inteligência artificial e o blockchain, oferecem novas ferramentas para combater a desinformação e fortalecer a proteção de dados (Sax, 2019). A inteligência artificial pode ser utilizada de múltiplas formas

para identificar e mitigar a disseminação de informações falsas, enquanto o blockchain pode garantir a transparência e a segurança no processamento de dados (Koornhof et al. 2018). A aplicação dessas tecnologias em países emergentes, no entanto, requer investimentos em infraestrutura e capacitação, bem como a adaptação das soluções tecnológicas às realidades locais, muitas vezes precárias (Kshetri, 2017).

7.4. Conscientização Pública e Participação Cidadã

A conscientização pública e a participação cidadã são elementos-chave na luta contra a desinformação e na promoção da proteção de dados (Dan et al., 2021). Campanhas de conscientização que informem os cidadãos sobre seus direitos de privacidade e os riscos da desinformação podem fortalecer a confiança no ambiente digital e incentivar a adesão às práticas de proteção de dados (Marwick & Lewis, 2017). Além disso, a participação ativa da sociedade civil na criação e implementação de políticas públicas pode garantir que as soluções desenvolvidas sejam inclusivas e eficazes (González Fuster, 2014).

A educação contínua sobre o uso consciente das tecnologias digitais e a importância da privacidade é igualmente essencial, uma vez que contribui para uma população mais informada e preparada para lidar com os desafios da era digital. A promoção de um debate público transparente sobre as implicações éticas e sociais da desinformação e da privacidade de dados pode incentivar uma cultura de vigilância crítica e engajamento social. As plataformas digitais, por sua vez, têm a responsabilidade de facilitar essa conscientização, oferecendo informações acessíveis e ferramentas que permitam aos usuários protegerem sua privacidade e identificar conteúdos enganosos. A colaboração entre governo, sociedade civil e setor privado é vital para criar um ambiente digital mais seguro e confiável.

Além disso, é necessário que as políticas de proteção de dados e combate à desinformação sejam continuamente adaptadas às novas realidades tecnológicas e às necessidades da sociedade, garantindo que a proteção dos direitos dos cidadãos esteja sempre em foco. Finalmente, a conscientização e a participação cidadã não

apenas fortalecem a resiliência contra a desinformação, mas também promovem uma cidadania digital mais ativa e consciente.

7.5. Implementação de Políticas Públicas Robustas

Finalmente, a implementação de políticas públicas robustas é essencial para enfrentar a desinformação e fortalecer a proteção de dados (Bennett & Raab, 2020). Em países emergentes, onde as estruturas legais podem ser recentes e ainda em desenvolvimento, é crucial garantir que as leis de proteção de dados sejam aplicadas de forma consistente e eficaz (Nair, & Shaikh, 2022). Isso inclui a criação de órgãos reguladores capacitados e independentes, a alocação de recursos suficientes para a fiscalização e a promoção da cooperação entre diferentes níveis de governo e a sociedade civil (Koornhof et al. 2018).

8. CONCLUSÃO

Ao longo deste estudo, exploramos de maneira abrangente a complexa intersecção entre a proteção de dados pessoais e o fenômeno da desinformação em países emergentes. A era digital, marcada pela rápida expansão da conectividade e pela omnipresença das tecnologias da informação, trouxe à tona desafios sem precedentes para a salvaguarda da privacidade e da integridade das informações pessoais (Bennett, 2018; Solove, 2021). Países emergentes, caracterizados por economias em acelerado desenvolvimento e pela adoção intensa de inovações tecnológicas, encontram-se na encruzilhada entre o aproveitamento das oportunidades proporcionadas pela digitalização e a necessidade imperativa de proteger os direitos de seus cidadãos (Floridi, 2016; Kuner, 2020).

A análise histórica evidenciou que, embora a preocupação com a proteção de dados tenha raízes que remontam às décadas de 1970 e 1980, é na contemporaneidade que tais questões adquirem maior urgência, sobretudo diante da capacidade nunca antes vista de coleta, armazenamento e processamento massivo de dados pessoais (Westin, 1967; Flaherty, 1989). Neste contexto, marcos

regulatórios como o GDPR na União Europeia serviram de modelo para legislações em países como o Brasil, com a LGPD, refletindo um movimento global de reconhecimento da importância da privacidade digital (González Fuster, 2014; Doneda & Almeida, 2021).

No entanto, a implementação eficaz de tais políticas enfrenta obstáculos significativos em países emergentes. Desafios estruturais, como infraestrutura tecnológica deficiente, desigualdades socioeconômicas e baixos níveis de alfabetização digital, comprometem a capacidade desses países de aplicar e fiscalizar as regulamentações de proteção de dados. Além disso, a proliferação da desinformação, potencializada pelas redes sociais e pela rápida disseminação de conteúdos digitais, agrava a situação, minando a confiança pública nas instituições e dificultando a implementação de políticas de privacidade (Marwick & Lewis, 2017; Dan et al., 2021).

Estudos de caso envolvendo o Brasil, a Índia e a África do Sul ilustraram abordagens distintas na formulação e execução de políticas de proteção de dados, revelando tanto avanços quanto lacunas significativas. Enquanto o Brasil avançou com a LGPD e estabeleceu a Autoridade Nacional de Proteção de Dados, a Índia ainda se encontra em processo de consolidação de sua legislação, e a África do Sul enfrenta desafios na operacionalização da POPIA (Nair, & Shaikh, 2022; Koornhof et al. 2018).

Frente a este cenário, estratégias multifacetadas emergem como essenciais para enfrentar os desafios. A promoção da alfabetização digital destaca-se como uma ferramenta vital para capacitar os cidadãos a navegarem no ambiente digital com discernimento, identificando e resistindo à desinformação (Sax, 2019). A colaboração internacional e regional também se mostra fundamental, permitindo a harmonização de normas e a troca de melhores práticas, enquanto o aproveitamento de tecnologias emergentes, como a inteligência artificial e o blockchain, oferece novos caminhos para fortalecer a segurança e a transparência no tratamento de dados (Kuner, 2020; Bennett & Raab, 2020).

Adicionalmente, a conscientização pública e a participação cidadã emergem como pilares para a construção de um ambiente digital saudável.

Campanhas educativas e a inclusão da sociedade civil no processo de elaboração de políticas asseguram que as soluções sejam inclusivas e adaptadas às realidades regionais. Por fim, a implementação de políticas públicas consistentes e estruturadas, apoiadas por órgãos reguladores capacitados e com os recursos adequados, é imperativa para garantir a eficácia das medidas de proteção de dados e para combater a desinformação de maneira proativa (Donovan, 2020; Nair, & Shaikh, 2022).

Em suma, a trajetória para fortalecer a proteção de dados em países emergentes é complexa e repleta de desafios. Contudo, com o compromisso contínuo de governos, instituições e cidadãos, aliado à adoção de estratégias integradas e colaborativas, é possível construir um futuro digital que respeite e proteja os direitos individuais, promovendo simultaneamente o desenvolvimento econômico e social. A luta contra a desinformação e pela proteção de dados não é apenas uma questão técnica ou legal, mas um imperativo ético e democrático na era da informação.

REFERÊNCIAS

BENNETT, C. J. **The Privacy Advocates**: Resisting the Spread of Surveillance. MIT Press, 2018.

BENNETT, C. J.; RAAB, C. D. **The Governance of Privacy**: Policy Instruments in Global Perspective. MIT Press, 2020.

BRADSHAW, S.; HOWARD, P. N. **The Global Disinformation Order:** 2019 Global Inventory of Organised Social Media Manipulation. Oxford Internet Institute, 2019.

CHAWLA, A.; BHANDARI, V. India's Data Protection Legislation: History, Challenges, and the Way Forward. **India Review**, v. 20, n. 1, p. 32-50, 2021.

DAN, V. et al. Visual Mis- and Disinformation, Social Media, and Democracy. **Journalism & Mass Communication Quarterly**, v. 98, n. 3, p. 641-664, 2021.

DONEDA, D.; ALMEIDA, V. Proteção de Dados Pessoais: A Função e os Limites da Regulação no Brasil. **Revista de Direito Administrativo**, 2021.

DONOVAN, J. Social Media and the Information Environment. **Journal of Democracy**, v. 31, n. 4, p. 75-89, 2020.

FLAHERTY, D. H. **Protecting Privacy in Surveillance Societies**: The Federal Republic of Germany, Sweden, France, Canada, and the United States. UNC Press Books, 2014.

FLORIDI, L. **The Fourth Revolution**: How the Infosphere is Reshaping Human Reality. OUP Oxford, 2014.

FLORIDI, L. **The Fourth Revolution**: How the Infosphere is Reshaping Human Reality. Oxford University Press, 2016.

GONZÁLEZ FUSTER, G. **The Emergence of Personal Data Protection as a Fundamental Right of the EU**. Springer, 2014.

KOORNHOF, P.; PISTORIUS, T. Convergence between Competition and Data Protection Law: A South African Perspective. **International Data Privacy Law**, v. 8, n. 3, p. 277-283, 2018.

KSHETRI, N. **Big Data's Big Potential in Developing Economies: Impact on Agriculture, Health and Environmental Security**. CABI, 2016.

KSHETRI, N. Big Data's Role in Expanding Access to Financial Services in China. **International Journal of Information Management**, v. 37, n. 2, p. 84-88, 2017.

KUNER, C. **Transborder Data Flows and Data Privacy Law**. Oxford University Press, 2013.

MARWICK, A. E.; LEWIS, R. **Media Manipulation and Disinformation Online.** Data & Society Research Institute, 2017.

MECABÔ, A. Proteção de Dados Pessoais: A Função e os Limites do Consentimento, de Bruno Bioni. **Revista de Direito Civil Contemporâneo-RDCC**, v. 28, p. 427-443, 2021.

NAIR, N. V.; SHAIKH, A. U. Privacy and Data Protection Laws: An Overview. **IUP Law Review**, v. 12, n. 2, 2022.

PISTORIUS, C. Protection of Personal Information Act (POPIA): Implications for South Africa. **South African Journal of Information Management**, v. 19, n. 1, p. 1-10, 2017.

ROSEN, J. Why Privacy Matters. **The Wilson Quarterly (1976-),** v. 24, n. 4, p. 32-38, 2000.

SAX, M. et al**. Between Empowerment and Manipulation:** The Ethics and Regulation of For-Profit Health Apps, 2021.

SAX, M. E. Digital Literacy and the Future of Privacy Protection in Emerging Markets. **Journal of Information Policy**, v. 9, p. 271-292, 2019.

SOLOVE, D. J. **The Digital Person**: Technology and Privacy in the Information Age. NYU Press, 2004.

SOLOVE, D. J. **Understanding Privacy.** Harvard University Press, 2010.

WARDLE, C.; DERAKHSHAN, H. **Information Disorder**: Toward an Interdisciplinary Framework for Research and Policy Making. Council of Europe, 2017.

WESTIN, A. F. **Privacy and Freedom**. Atheneum, 1967.

ZUBOFF, S. **The Age of Surveillance Capitalism**: The Fight for a Human Future at the New Frontier of Power. PublicAffairs, 2019.