VULNERABILIDADE DIGITAL: DESAFIOS PARA GRUPOS DE RISCO NO ACESSO À JUSTIÇA E NA PROTEÇÃO CONTRA CRIMES CIBERNÉTICOS NO BRASIL

Matheus Portela Peruzzi[1]
Miriane Maria Willers[2]
Luciano de Almeida Lima[3]

RESUMO

Este trabalho buscou investigar a vulnerabilidade digital de grupos de risco no Brasil, com foco nas dificuldades enfrentadas para acessar a justiça e proteger-se contra crimes cibernéticos. A pesquisa procurou responder às seguintes questões: qual é o nível de segurança e privacidade assegurado aos indivíduos que utilizam a internet e dispositivos digitais? De que forma o Direito pode atuar para regulamentar e punir práticas ilícitas, garantindo maior proteção ao cidadão? A metodologia adotada foi a dedutiva. O procedimento metodológico incluiu o método monográfico devido à relevância nacional do caso estudado. A pesquisa foi explicativa e utilizou o método documental. A partir de uma revisão da literatura, analisa-se como a exclusão digital, aliada à falta de educação digital, compromete a segurança e a privacidade de indivíduos vulneráveis, tais como idosos, crianças, mulheres e pessoas de baixa renda. Os avanços legislativos, representados pelo Marco Civil da Internet e pela Lei Geral de Proteção de Dados (LGPD), embora significativos, demonstram limitações práticas em sua implementação, especialmente para aqueles que não possuem pleno acesso e compreensão das tecnologias. O estudo aponta a educação digital e políticas públicas de inclusão como estratégias fundamentais para reduzir a vulnerabilidade digital e garantir uma proteção jurídica mais abrangente e eficaz. Conclui-se que, para que a inclusão digital e o acesso à justiça sejam universais, é necessário fortalecer tanto a legislação quanto os programas de capacitação digital, promovendo uma sociedade mais justa e segura no ambiente digital.

Palavras-chave: Vulnerabilidade Digital, Grupos de Risco, Crimes Cibernéticos, Acesso à Justiça, Inclusão Digital, Proteção Jurídica.

ABSTRACT

This study investigates the digital vulnerability of at-risk groups in Brazil, focusing on the challenges they face in accessing justice and protecting

[1] Acadêmico do Curso de Direito. Universidade Regional Integrada do Alto Uruguai e das Missões. São Luiz Gonzaga, RS. E-mail: 097385@saoluiz.uri.edu.br
[2] Professora do Curso de Direito. Universidade Regional Integrada do Alto Uruguai e das Missões. São Luiz Gonzaga, RS. E-mail: profmiriane@saoluiz.uri.edu.br
[3] Professor do Curso de Direito. Universidade Regional Integrada do Alto Uruguai e das Missões. São Luiz Gonzaga, RS. E-mail: profluciano@saoluiz.uri.edu.br

themselves against cybercrimes. The research sought to address the following questions: what level of security and privacy is ensured for individuals using the internet and digital devices? How can the law contribute to regulating and punishing illicit practices, thereby providing greater protection for citizens? Through a literature review, it analyzes how digital exclusion, combined with a lack of digital literacy, compromises the security and privacy of vulnerable individuals, such as the elderly, children, women, and low-income populations. Legislative advances, represented by the Brazilian Internet Bill of Rights and the General Data Protection Law (LGPD), while significant, reveal practical limitations in their implementation, particularly for those without full access to and understanding of technology. The study highlights digital education and public inclusion policies as essential strategies to reduce digital vulnerability and ensure more comprehensive and effective legal protection. It concludes that, for digital inclusion and access to justice to be universal, both legislation and digital literacy programs must be strengthened, fostering a fairer and safer society in the digital environment.

Keywords: Digital Vulnerability, At-Risk Groups, Cyber Crimes, Access to Justice, Digital Inclusion, Legal Protection.

1. INTRODUÇÃO

Com o avanço das tecnologias digitais e a integração da internet em praticamente todos os setores da sociedade, a realidade dos relacionamentos sociais, econômicos e institucionais passou por uma transformação sem precedentes. Este cenário trouxe consigo não apenas uma maior facilidade de comunicação e acesso a informações, mas também uma série de desafios e riscos, especialmente para os grupos mais vulneráveis da sociedade. Muitas vezes, essas pessoas não têm a proteção necessária contra as ameaças cibernéticas (Almeida, 2017). Como destaca Aires (2023), a inclusão digital e o acesso à internet não aconteceram de forma igual para todos, criando uma situação de "exclusão digital" que dificulta o acesso à justiça e aos direitos fundamentais de milhões de brasileiros.

Dentre as ameaças do ambiente digital, os crimes cibernéticos ocupam uma posição de destaque e trazem desafios significativos para o sistema jurídico. Crimes como fraudes financeiras, estelionato, roubos de identidade e assédio online têm se tornado cada vez mais comuns, afetando principalmente aqueles que já enfrentam dificuldades de acesso e compreensão das tecnologias digitais. Conforme Doneda (2006), a fragilidade e exposição dos

dados pessoais na internet coloca em risco não apenas a privacidade, mas também a dignidade e segurança de indivíduos, uma vez que tais dados são frequentemente alvo de ataques cibernéticos. Nesse sentido, a vulnerabilidade digital é um fenômeno que abrange tanto questões técnicas quanto sociais, expondo grupos já marginalizados a riscos adicionais.

Essa vulnerabilidade digital é especialmente prejudicial para certos grupos de risco, que incluem crianças, idosos, mulheres e pessoas de baixa renda. De acordo com Moraes e Bustamante (2021), a exclusão digital e a falta de acesso a ferramentas de proteção impactam de forma desproporcional esses grupos, pois, além de estarem mais expostos a crimes virtuais, possuem menos recursos para se defender judicialmente. Tal realidade cria um ciclo de exclusão e insegurança que compromete a plena participação desses indivíduos na sociedade digital. Durante a pandemia de Covid-19, a exclusão digital se tornou ainda mais evidente, aprofundando as desigualdades e expondo vulnerabilidades estruturais que até então eram pouco visíveis.

A legislação brasileira tem buscado responder a esses desafios com marcos regulatórios, como a Lei 13.709/2018 - Lei Geral de Proteção de Dados (LGPD), que visa assegurar a privacidade e a proteção de dados pessoais dos cidadãos (Brasil, 2018). Contudo, como destaca Zanatta (2019), a aplicação prática da LGPD ainda enfrenta obstáculos significativos, uma vez que muitos dos mecanismos previstos na lei não possuem fiscalização eficiente ou ampla compreensão por parte da população. Nesse contexto, a legislação, embora necessária, se revela insuficiente para garantir uma proteção efetiva, exigindo uma estrutura mais integrada de conscientização digital e de acesso à justiça. Enquanto a União Europeia tem estabelecido padrões rigorosos de proteção de dados, o Brasil ainda está em fase inicial de implementação de políticas abrangentes para o setor digital.

O acesso à justiça é um dos princípios fundamentais de uma sociedade democrática e inclusiva. No entanto, a exclusão digital afeta diretamente o exercício desse direito, impedindo que grande parte da população se beneficie de recursos legais que estão disponíveis apenas para quem possui um mínimo de alfabetização digital. Para que o acesso à justiça se torne uma realidade

para todos, é necessário não apenas regulamentar a proteção digital, mas também implementar políticas públicas que promovam a inclusão digital de maneira sustentável. Nesse sentido, as desigualdades no acesso a tecnologias de informação representam um obstáculo não apenas jurídico, mas também social e econômico (Broadhurst & Chang, 2013).

Esta pesquisa visa abordar os principais aspectos da vulnerabilidade digital, focando nas características dos grupos de risco e nos desafios que enfrentam para acessar a justiça e garantir proteção contra crimes cibernéticos. Partindo de uma revisão da literatura abrangente e da análise de estudos recentes sobre o tema, busca-se compreender as interações entre exclusão digital e proteção jurídica no Brasil. A metodologia adotada foi a dedutiva. O procedimento metodológico incluiu o método monográfico devido à relevância nacional do caso estudado. A pesquisa foi explicativa e utilizou o método documental. A literatura indica que, embora exista uma base legislativa relevante, como o Marco Civil da Internet e a própria LGPD, ainda há uma lacuna significativa entre a teoria jurídica e a proteção prática dos direitos no ambiente digital (Conselho Nacional de Justiça, 2021; Doneda, 2006). Dessa forma, é necessário avançar não apenas na criação de normas, mas também em sua efetiva implementação e na educação digital da população.

Em suma, a presente pesquisa propõe-se a contribuir para a compreensão dos fatores que caracterizam a vulnerabilidade digital e das ferramentas de proteção jurídica disponíveis para esses grupos. Dessa forma, busca-se incentivar o desenvolvimento de políticas públicas e jurídicas que, ao integrar a inclusão digital ao acesso à justiça, promovam uma sociedade mais equitativa e segura no uso das tecnologias digitais. Como reforça Solove e Hartzog (2022), a proteção contra crimes cibernéticos só será eficaz quando integrada a um sistema de segurança que compreenda tanto o fortalecimento legislativo quanto a conscientização e educação de seus cidadãos.

2 VULNERABILIDADE DIGITAL E GRUPOS DE RISCO

A vulnerabilidade digital é um fenômeno que ganha destaque em uma sociedade cada vez mais dependente da internet e das tecnologias de informação. Trata-se de uma condição em que certos indivíduos ou grupos estão mais expostos a riscos no ambiente digital devido às limitações de acesso, conhecimento ou proteção, o que os torna alvos mais suscetíveis das práticas de crimes cibernéticos. Moraes e Bustamante (2021) apontam que essa vulnerabilidade é particularmente crítica para grupos de risco, como crianças, idosos, mulheres e pessoas de baixa renda, que, por diferentes razões, enfrentam barreiras ao uso seguro e pleno das tecnologias digitais. Esses grupos, frequentemente, não possuem os recursos necessários para se protegerem adequadamente online, o que amplia os riscos de exposição a práticas ilícitas e abusivas, dificultando o acesso à justiça ideal e à reparação dos danos sofridos.

A inclusão digital e a democratização do acesso à internet são fundamentais para reduzir as disparidades sociais e para garantir a efetiva participação de todos os indivíduos na sociedade digital. Contudo, a inclusão digital não é homogênea e muitos grupos ainda permanecem excluídos dos avanços tecnológicos, especialmente aqueles que já se encontram em situação de vulnerabilidade social. Esse fenômeno, chamado de exclusão digital, não se limita apenas ao acesso físico aos dispositivos e à internet, mas envolve também a capacidade de compreensão e de uso adequado das ferramentas digitais disponíveis. A exclusão digital, que afeta diretamente o acesso à justiça e a proteção dos direitos no ambiente digital, foi agravada pela pandemia de Covid-19, que acelerou a dependência tecnológica sem que houvesse um preparo adequado para todos (Aires 2023).

Esse contexto de exclusão digital acarreta um aumento na exposição a crimes cibernéticos e práticas abusivas, o que torna os grupos vulneráveis alvos frequentes de ações ilícitas na internet. O impacto da fragilidade dos dados pessoais no ambiente digital compromete a dignidade e a segurança dos indivíduos. A privacidade e a proteção de dados são direitos essenciais, especialmente para aqueles que não possuem conhecimento adequado para controlar suas informações no ambiente online. Como consequência, a falta de

proteção digital leva à criação de um ciclo de vulnerabilidade, onde a exclusão e a falta de recursos para defesa se combinam para agravar as consequências de incidentes cibernéticos para esses grupos (Doneda 2006).

Estudos como o de Almeida (2017) reforçam a importância de uma abordagem que vá além do acesso à tecnologia, defendendo que é essencial promover a educação digital como forma de capacitar esses grupos para um uso mais seguro e consciente da internet. Almeida argumenta que o direito à privacidade e à segurança digital deve ser acessível a todos e que, para garantir esse direito, é fundamental que os indivíduos compreendam os riscos e as práticas de segurança online. Ao discutir os desafios enfrentados por países da Ásia no combate aos crimes cibernéticos, é visível uma perspectiva comparativa, ressaltando que o enfrentamento da vulnerabilidade digital exige uma combinação de políticas de proteção e conscientização pública, algo que também se aplica ao contexto brasileiro.

Para Moraes e Bustamante (2021), a vulnerabilidade digital representa uma ameaça direta ao acesso à justiça, pois impede que grupos de risco, que frequentemente já possuem dificuldades no acesso a serviços básicos, consigam recorrer ao sistema jurídico de forma plena e eficaz. Essas dificuldades são reforçadas pela falta de mecanismos de defesa e pelo desconhecimento de direitos e ferramentas digitais. A ausência de uma educação digital adequada limita ainda mais a capacidade de defesa desses indivíduos, tornando-os alvos fáceis para práticas de exploração, seja em termos de abuso financeiro, roubo de dados ou assédio online. A alfabetização digital é um passo essencial para a proteção desses indivíduos, sendo uma forma de reduzir a dependência de terceiros e aumentar a capacidade de identificação e prevenção de situações de risco.

Outro aspecto relevante é a forma como o sistema jurídico brasileiro responde às demandas impostas pela vulnerabilidade digital. Embora a LGPD e o Marco Civil da Internet, Lei 12.965/2014, representem avanços importantes para a proteção dos direitos digitais, esses instrumentos ainda encontram barreiras em sua aplicação prática. As proteções oferecidas pela LGPD são limitadas, uma vez que dependem não apenas de uma fiscalização efetiva,

mas também da compreensão dos cidadãos sobre seus próprios direitos digitais, o que frequentemente não ocorre entre os grupos mais vulneráveis. A proteção digital não deve se limitar a questões legais, mas deve englobar iniciativas educacionais e políticas públicas que promovam uma inclusão digital significativa (Zanatta 2019).

Portanto, a vulnerabilidade digital não é apenas um problema técnico, mas uma questão profundamente ligada à exclusão social e à desigualdade no acesso a direitos fundamentais. Esse conceito engloba não só a falta de recursos, mas também a ausência de conhecimento e de suporte institucional adequado para que os grupos vulneráveis possam se defender e se proteger no ambiente digital. O acesso limitado a tecnologias e a carência de uma educação digital eficaz expõem esses grupos a riscos contínuos e profundos, perpetuando a desigualdade e a injustiça. A partir dessa análise, é necessário explorar formas de reduzir essas vulnerabilidades, promovendo uma discussão sobre a importância de políticas inclusivas e de uma legislação que vá além da proteção formal, para garantir uma real segurança e equidade no uso das tecnologias digitais (Doneda, 2006).

2.1 Crimes Cibernéticos e Seus Impactos nos Grupos Vulneráveis

Os crimes cibernéticos configuram um dos principais desafios enfrentados pelos grupos vulneráveis na era digital. Com o avanço da internet e das tecnologias de informação, tais crimes se tornaram não apenas mais comuns, mas também mais complexos e difíceis de combater. Esses crimes incluem desde fraudes e roubos de identidade até assédio virtual e manipulação de dados, afetando especialmente aqueles que não possuem acesso a recursos adequados para defesa no ambiente digital. O ambiente digital, com todas as suas vantagens, expõe indivíduos a práticas ilícitas que exploram a falta de conhecimento e as limitações de proteção, criando barreiras para que grupos vulneráveis possam se proteger efetivamente (Solove e Hartzog 2022).

Broadhurst e Chang (2013) observam que os crimes cibernéticos são caracterizados por sua natureza transnacional e pelo fato de que muitas vezes

são praticados por indivíduos ou grupos que exploram lacunas nos sistemas de proteção e monitoramento. O impacto desses crimes é particularmente prejudicial para os indivíduos que já se encontram em situação de vulnerabilidade, pois, além de não disporem de uma rede de proteção digital sólida, são frequentemente desconhecedores dos direitos e dos mecanismos de denúncia e reparação. Esses crimes, que incluem desde o *phishing* e roubo de informações financeiras até o cyberbullying e a exposição de dados pessoais, não apenas violam a privacidade, mas também a integridade emocional e financeira dos indivíduos afetados.

A vulnerabilidade digital se agrava nos casos de roubo de dados e exposição indevida de informações, especialmente em uma era onde a privacidade e o controle sobre os próprios dados se tornaram itens valiosos. Muitos desses crimes são facilitados pela falta de conhecimento sobre segurança digital e proteção de dados, fazendo com que as vítimas, na maioria das vezes, nem sequer tenham consciência de que estão em risco até que já sejam afetadas. A ausência de medidas preventivas e educativas adequadas para o uso seguro da internet agrava ainda mais os danos sofridos por grupos vulneráveis, uma vez que muitos não têm conhecimento sobre práticas de segurança, como o uso de senhas fortes ou a verificação de sites antes de realizar transações online (Doneda 2006).

Estudos demonstram que a exposição à crimes cibernéticos causam impactos significativos na vida das vítimas, incluindo traumas psicológicos, dificuldades financeiras e estigma social. Segundo Gonzaga (2020), o aumento das atividades online durante a pandemia de Covid-19 resultou em uma ampliação da vulnerabilidade a esses crimes, especialmente entre idosos e crianças, que tiveram que se adaptar rapidamente a uma nova realidade digital, sem o devido suporte educacional ou de segurança. A adaptação abrupta ao ambiente digital expôs ainda mais aqueles que já se encontravam em situação de exclusão tecnológica, como os indivíduos de baixa renda e com menos escolaridade. Devido a essa exposição adicional ampliou-se o alcance dos criminosos cibernéticos, que se aproveitaram de vulnerabilidades específicas de grupos que têm menos chances de adotar práticas de defesa.

Em relação aos crimes de assédio virtual, Barelli e Silva (2022) destacam que mulheres e adolescentes são as principais vítimas, com casos de perseguição e cyberbullying que podem ter consequências devastadoras para a saúde mental e o bem-estar social. Muitos casos, as vítimas não conseguem ou não sabem como buscar ajuda, seja por medo de represálias ou por desconhecimento dos canais de apoio disponíveis. A resposta jurídica e social a esses crimes ainda é insuficiente, especialmente em relação ao suporte psicológico e ao acompanhamento dos casos. A nossa legislação brasileira, embora avançada em alguns aspectos, como a Lei Maria da Penha e a própria LGPD, ainda apresenta lacunas significativas no tratamento de crimes que ocorrem exclusivamente no ambiente digital, deixando muitas vítimas sem proteção efetiva.

A respeito das fraudes financeiras, a fragilidade dos sistemas de segurança digital faz com que os consumidores sejam especialmente vulneráveis a esquemas de *phishing* e fraudes bancárias. Esses crimes não só afetam a segurança econômica das vítimas, mas também retraem a confiança no sistema bancário digital, criando um ciclo de insegurança que desestimula o uso de tecnologias financeiras. A atualização dos sistemas de segurança seria a resposta a esse tipo de crime tanto quanto uma maior capacitação dos indivíduos sobre as ameaças cibernéticas. As instituições financeiras devem adotar uma postura mais proativa, oferecendo orientação e educação sobre práticas seguras para todos os seus clientes, especialmente aqueles que têm menos experiência no ambiente online (Solove e Hartzog 2022).

Para que os grupos vulneráveis consigam se defender contra os crimes cibernéticos, é essencial que o sistema jurídico seja mais inclusivo e adaptado às demandas digitais. O aprimoramento das leis de proteção e dos mecanismos de denúncia, aliado a uma política pública de educação digital, é o caminho para a construção de uma sociedade mais resiliente e preparada para enfrentar os desafios impostos pelo ambiente digital. Para alcançar uma proteção eficiente, o Brasil deve adotar medidas comparáveis às da União Europeia, que garantem um nível mais elevado de segurança e proteção de dados pessoais. Pois, a legislação brasileira deve avançar para cobrir lacunas

que atualmente deixam muitos grupos em situação de exposição contínua e sem acesso a recursos adequados de defesa (Tavares 2016).

Os crimes cibernéticos representam uma ameaça constante e agravada pela exclusão digital e pela falta de proteção e educação. Os grupos vulneráveis, estão em uma situação particularmente delicada, uma vez que possuem menos recursos para se protegerem de práticas ilícitas na internet. O impacto desses crimes vai além das perdas financeiras, afetando também a privacidade, a saúde mental e a confiança desses indivíduos no ambiente digital. A análise desses efeitos, é evidenciado a necessidade de uma abordagem mais integrada e inclusiva para combater a vulnerabilidade digital, através de políticas públicas, educação e fortalecimento das leis de proteção (Zanatta, 2019).

2.2 Acesso à Justiça e Exclusão Digital

O acesso à justiça é um direito fundamental garantido pela Constituição Federal, mas, no contexto digital, torna-se um desafio adicional para os grupos vulneráveis que sofrem com a exclusão digital. Consistindo na limitação de acesso, seja por falta de dispositivos tecnológicos, conhecimento ou conectividade, ela afeta diretamente o exercício de direitos básicos, incluindo o direito à justiça. Ela não é meramente uma questão de tecnologia, mas de direitos humanos, pois impede que milhões de brasileiros, especialmente aqueles em situação de vulnerabilidade social, acessem plenamente os serviços judiciais e defendam seus interesses em uma sociedade que se digitaliza rapidamente (Aires 2023).

Conforme Moraes e Bustamante (2021), a exclusão digital cria barreiras adicionais para indivíduos vulneráveis que têm menor familiaridade com as tecnologias e enfrentam obstáculos para participar ativamente dos processos judiciais digitais. A falta de acesso aos serviços de justiça digital não só compromete a defesa dos direitos desses indivíduos, mas também perpetua um ciclo de exclusão, uma vez que os grupos vulneráveis, por estarem à margem da inclusão digital, acabam desassistidos e sem mecanismos de

reparação. Restando em uma desigualdade no acesso à justiça, pois limita a capacidade desses indivíduos de acessar serviços públicos e informações essenciais, dificultando ainda mais o exercício da cidadania plena.

A exclusão digital é particularmente problemática em um contexto onde o uso da internet e das tecnologias de informação se expande em diversas esferas sociais, incluindo o sistema de justiça. Com a pandemia de Covid-19, muitos processos judiciais passaram a ser realizados de forma remota, excluindo aqueles que não possuem meios para acessar esses serviços online. Essa situação foi especialmente crítica para os idosos, tanto na visão de advogados, servidores, até partes do processo, que, além de estarem mais isolados durante a pandemia, muitas vezes enfrentam dificuldades para lidar com plataformas digitais. Em vez de diminuir as desigualdades, a digitalização do sistema judiciário pode, na verdade, agravá-las, a menos que sejam adotadas políticas de inclusão digital que possibilitem o acesso de todos os cidadãos (Gonzaga 2020).

A exclusão digital não se resume à falta de acesso físico à internet, mas também à ausência de capacitação para o uso de ferramentas digitais de forma adequada e segura. Para isso a alfabetização digital é essencial para que os indivíduos possam exercer seus direitos no ambiente online, incluindo o acesso à justiça. Pois sem a compreensão adequada das ferramentas digitais, os grupos vulneráveis são colocados em uma situação de desvantagem, pois não conseguem acessar ou entender os recursos e serviços jurídicos disponibilizados online. Além disso, a falta de conhecimento sobre privacidade e proteção de dados é um fator que coloca esses indivíduos em risco adicional, pois a ausência de medidas de segurança digital pode levar à exposição de informações pessoais, comprometendo ainda mais sua integridade e segurança no ambiente digital (Doneda 2006).

Em muitos casos, a exclusão digital impede que esses indivíduos tenham acesso aos próprios direitos e à proteção contra abusos no ambiente online. O princípio do acesso à justiça deve ser amplamente garantido, mas, para isso, é preciso que o sistema jurídico reconheça e responda às desigualdades digitais existentes. E além de regulamentar a proteção contra

crimes cibernéticos, o sistema jurídico deve adotar uma postura mais inclusiva, implementando medidas que ampliem o acesso dos grupos vulneráveis aos serviços digitais. Corroborando essa perspectiva, o acesso à justiça não deve ser um privilégio apenas dos que têm acesso à internet e às tecnologias digitais, mas sim um direito garantido a todos, independentemente de sua situação socioeconômica (Aires 2023).

A exclusão digital tem implicações diretas para a proteção jurídica de indivíduos que são vítimas de crimes cibernéticos, mas que, devido à falta de acesso e conhecimento, não conseguem buscar a reparação necessária. Uma sociedade onde a maior parte das interações e dos crimes ocorre no ambiente digital, é fundamental que o sistema de justiça seja acessível a todos. Sem uma rede de apoio que ofereça suporte jurídico acessível e inclusivo, os indivíduos vulneráveis são colocados em uma posição de desvantagem contínua, pois não têm os recursos necessários para recorrer judicialmente em casos de abusos digitais, na maioria das vezes. (Solove e Hartzog 2022).

A digitalização do sistema jurídico no Brasil tem sido impulsionada pela necessidade de modernização e eficiência, mas, essa transição precisa considerar as barreiras que os grupos vulneráveis enfrentam para acessar o ambiente digital. O direito à privacidade e segurança digital deve ser parte integrante das políticas de inclusão, de forma que o acesso à justiça seja acompanhado por uma proteção completa e por mecanismos de segurança acessíveis a todos (Broadhurst e Chang 2013).

Para mitigar os efeitos da exclusão digital, Zanatta (2019) argumenta que é essencial que o Brasil desenvolva políticas de capacitação digital, de modo a garantir que todos os cidadãos, especialmente os de grupos vulneráveis, tenham o conhecimento necessário para acessar os serviços de justiça. A LGPD, embora ofereça importantes salvaguardas para a privacidade, precisa ser complementada por iniciativas de inclusão digital para que seu potencial seja totalmente alcançado. Dessa forma, a exclusão digital não se torna um impeditivo para o exercício dos direitos, mas sim um desafio superado por políticas que garantem o acesso amplo e igualitário.

Assim, o acesso à justiça e a inclusão digital devem ser tratados como questões interdependentes em uma sociedade que caminha para uma digitalização crescente. A exclusão digital não deve ser vista apenas como uma falta de acesso, mas como uma barreira ao exercício de direitos fundamentais e ao pleno desenvolvimento social e jurídico. (Gonzaga, 2020).

2.3 Mecanismos Jurídicos e Políticas Públicas para a Proteção Digital

O crescimento dos crimes cibernéticos e da exclusão digital evidenciou a necessidade de uma legislação robusta e de políticas públicas eficazes que possam proteger os direitos dos cidadãos no ambiente digital. No Brasil, a implementação do Marco Civil da Internet (Lei nº 12.965/2014) e da Lei Geral de Proteção de Dados (LGPD) (Lei nº 13.709/2018) foram marcos importantes para regulamentar o uso da internet e a proteção dos dados pessoais. No entanto, apesar dos avanços, esses mecanismos ainda apresentam limitações significativas em termos de fiscalização e aplicabilidade, especialmente para grupos vulneráveis que enfrentam dificuldades para compreender e usufruir plenamente dessas proteções jurídicas (Zanatta 2019).

O Marco Civil da Internet é frequentemente citado como um dos primeiros passos para a regulamentação do ambiente digital no Brasil, estabelecendo diretrizes para a neutralidade da rede, a privacidade e a liberdade de expressão dos usuários. Ele representa uma conquista significativa para os direitos digitais no país, mas ainda carece de mecanismos que garantam que suas disposições sejam aplicadas de maneira eficaz para todos os cidadãos, incluindo aqueles em situação de vulnerabilidade digital. Pois, sem políticas públicas que promovam o acesso universal à internet e o conhecimento sobre os direitos digitais, o Marco Civil corre o risco de se tornar uma legislação ineficaz para as pessoas que mais necessitam de proteção (Vieira 2018).

A LGPD, por sua vez, busca assegurar a privacidade e a segurança dos dados pessoais dos usuários, um aspecto essencial para reduzir a exposição dos indivíduos a práticas abusivas e criminosas no ambiente digital.

Comparando a LGPD com o Regulamento Geral de Proteção de Dados da União Europeia (GDPR), a LGPD possui um potencial considerável para garantir a privacidade dos dados no Brasil, mas ainda depende de uma de uma fiscalização que seja acessível a todos. Enquanto a GDPR tem servido de referência para políticas de privacidade no mundo todo, a LGPD enfrenta desafios específicos, como a falta de conscientização da população sobre seus direitos e a ausência de um órgão regulador suficientemente estruturado para garantir sua aplicação efetiva (Tavares 2016).

Além das leis específicas, os crimes cibernéticos no Brasil são combatidos com base no Código Penal Brasileiro, que foi adaptado para incluir disposições sobre invasão de dispositivos, roubo de identidade e fraudes digitais, conforme pode se observar na Lei Carolina Dieckmann, Lei 12.737/2012, contudo o Código Penal abarque crimes digitais, ele não atende completamente à complexidade do ambiente virtual, especialmente em um cenário onde a tecnologia e as práticas ilícitas evoluem rapidamente. O Brasil precisa de uma legislação mais moderna e adaptada às novas realidades digitais, uma vez que os dispositivos legais atuais ainda se mostram insuficientes para prevenir e combater eficazmente os crimes cibernéticos (Barelli e Silva 2022).

Conforme pode se observar, a lei 12.737/2012 acrescentou o artigo 154-A no Código Penal:

> **Invasão de dispositivo informático**
>
> Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput
> § 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido
> Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa

> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra
> I - Presidente da República, governadores e prefeitos
> II - Presidente do Supremo Tribunal Federal
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal;
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal (BRASIL, 1940, s.p.).

A necessidade de políticas públicas específicas para promover a inclusão digital e a conscientização sobre segurança cibernética é outro aspecto essencial para a proteção dos grupos vulneráveis. Sem uma base educacional sólida sobre os direitos e os riscos digitais, os cidadãos, especialmente aqueles menos familiarizados com a tecnologia, permanecem expostos a práticas abusivas. O Estado deve investir em programas de educação digital para capacitar esses grupos e, assim, reduzir sua exposição aos riscos associados ao ambiente digital. Essa capacitação não só contribuiria para a proteção dos dados pessoais, mas também promove uma maior autonomia e segurança para os indivíduos no uso das ferramentas digitais (Almeida 2017).

Broadhurst e Chang (2013) destacam que, em outros contextos, como na Ásia, políticas públicas de inclusão digital e proteção de dados são implementadas com o objetivo de garantir que todos os cidadãos possam usufruir de uma navegação segura e informada na internet. Eles sugerem que o Brasil pode se beneficiar de exemplos internacionais ao desenvolver suas políticas públicas, incorporando práticas que já foram testadas e adaptadas a diferentes realidades culturais e sociais. Essa perspectiva de comparação internacional deve ser compreendida como um direito humano essencial, e que políticas públicas eficazes são indispensáveis para garantir que essa proteção atinja a todos, independentemente de sua situação econômica ou social.

Além das proteções legais e dos esforços de inclusão digital, o apoio institucional desempenha um papel crucial na mitigação dos riscos para os grupos vulneráveis. O sistema de justiça precisa estar preparado para lidar com

a especificidade dos crimes cibernéticos e para atender as demandas de uma sociedade digitalizada. O poder judiciário, para isso, deve investir em infraestrutura e capacitação digital, tanto para seus funcionários quanto para os usuários, a fim de reduzir esses impactos. Nesse sentido, a capacitação do sistema judicial seria uma resposta proativa às limitações atuais, permitindo que o judiciário compreenda e responda melhor aos desafios impostos pelos crimes cibernéticos (Moraes e Bustamante 2021).

Assim, os mecanismos jurídicos e as políticas públicas para a proteção digital representam uma área crucial e em desenvolvimento no Brasil. A aplicação de leis como a LGPD e o Marco Civil da Internet devem ser revistas para uma melhor eficácia em sua aplicação prática. Pois a exclusão digital e a falta de educação sobre segurança e privacidade no ambiente online impedem que muitos cidadãos se beneficiem dos avanços da legislação digital. (Zanatta 2019).

2.4 Educação Digital e Conscientização para a Inclusão Segura

A educação digital e a conscientização são elementos fundamentais para a proteção de grupos vulneráveis no ambiente digital. Em um contexto onde o uso das tecnologias se expande rapidamente, a falta de capacitação digital pode agravar as desigualdades sociais, deixando muitos indivíduos expostos a riscos como crimes cibernéticos e violação de privacidade. Almeida (2017) argumenta que, para que o ambiente digital seja realmente inclusivo, é essencial que o Estado invista em programas de alfabetização digital, capacitando os indivíduos a compreenderem seus direitos e a utilizarem as ferramentas tecnológicas de maneira segura. Pois sem uma base sólida de educação digital, muitos cidadãos permanecem alheios às práticas de segurança básicas e desconhecem os recursos de proteção de dados que poderiam auxiliá-los na prevenção de abusos.

De acordo com Gonzaga (2020), a pandemia de Covid-19 acelerou o processo de digitalização e trouxe à tona a necessidade urgente de uma educação digital inclusiva, especialmente para aqueles que tiveram que se

adaptar rapidamente ao uso de tecnologias sem o devido preparo. Essa necessidade é ainda mais premente para os grupos vulneráveis, como idosos, mulheres e crianças, que, ao serem lançados de maneira abrupta no mundo digital, sem orientação ou suporte adequado, se tornaram alvos fáceis de práticas criminosas. E para mitigar os riscos digitais, é crucial que programas educacionais incluam não apenas habilidades técnicas, mas também informações sobre privacidade, segurança e ética no uso da internet, promovendo uma cultura de responsabilidade digital que alcance todos os cidadãos.

A inclusão digital não deve ser vista apenas como uma questão de acesso a dispositivos ou internet, mas também como uma questão de cidadania. A educação digital é uma ferramenta poderosa para a proteção dos direitos fundamentais e que, sem ela, grupos vulneráveis permanecem marginalizados, sem condições de exercer plenamente seus direitos no ambiente digital. A conscientização sobre práticas seguras na internet deve ser incentivada desde as fases iniciais da educação formal, de modo a construir uma geração mais preparada para lidar com os desafios e riscos da era digital (Moraes e Bustamante 2021).

A falta de conscientização digital é uma das principais causas da exposição excessiva de informações pessoais e da vulnerabilidade a ataques cibernéticos. Muitos dos problemas enfrentados pelos grupos vulneráveis poderiam ser mitigados se esses indivíduos tivessem acesso a uma educação digital voltada para a segurança. Pois sem o devido conhecimento sobre medidas de proteção, como o uso de senhas seguras, a verificação de fontes de informação e o reconhecimento de fraudes, esses grupos ficam mais suscetíveis a golpes e abusos. Além disso, a educação digital deve ser promovida de maneira contínua, especialmente em um contexto onde as tecnologias e as ameaças cibernéticas evoluem constantemente, exigindo uma atualização permanente dos conhecimentos e das práticas de segurança (Barelli e Silva 2022).

A proteção dos dados pessoais é um dos aspectos mais sensíveis na atualidade, e a educação digital precisa incluir uma compreensão aprofundada

sobre os direitos de privacidade e a importância do controle sobre as próprias informações. A falta de conhecimento sobre privacidade digital não apenas facilita práticas abusivas por parte de terceiros, mas também compromete a autonomia dos indivíduos, que, ao não dominarem os conceitos de proteção de dados, ficam mais expostos a situações de vulnerabilidade. Educar sobre privacidade é uma medida preventiva essencial, pois permite que os indivíduos façam escolhas informadas sobre o que compartilham online e sobre como proteger suas informações pessoais (Doneda 2006).

Em nível global, Broadhurst e Chang (2013) observam que a educação digital é uma prioridade em muitos países da Ásia, onde programas de conscientização são promovidos para proteger os cidadãos dos crimes cibernéticos. Em países com políticas de educação digital abrangentes, as taxas de vulnerabilidade a crimes cibernéticos entre os grupos de risco são menores, pois os indivíduos são capazes de identificar potenciais ameaças e buscar soluções de forma autônoma.

A conscientização digital deve ser acompanhada de uma abordagem prática, que inclua a criação de centros de apoio e a oferta de recursos acessíveis para que os cidadãos possam aprender e aplicar práticas de segurança. Centros de apoio poderiam oferecer capacitações gratuitas e programas de conscientização, ajudando a disseminar o conhecimento sobre proteção digital e fortalecendo a autonomia dos indivíduos para navegar de forma segura no ambiente online (Aires 2023).

O sistema de proteção de dados da União Europeia serve de modelo não apenas para as políticas de privacidade, mas também para as práticas de educação digital. Em países onde a educação digital é vista como uma prioridade, as taxas de crimes cibernéticos são menores e os cidadãos têm uma compreensão mais clara de seus direitos e deveres no ambiente digital, o que contribui para uma sociedade digital mais segura e equitativa (Tavares 2016).

A educação digital, portanto, é uma medida preventiva indispensável para a construção de uma cultura de segurança e responsabilidade no uso das tecnologias. A qual deve implantada para que seja realizada a criação de

políticas públicas voltadas para a inclusão digital e a conscientização sobre segurança cibernética são essenciais para que todos os cidadãos possam se proteger de forma autônoma, especialmente os grupos vulneráveis, que, sem o devido apoio, permanecem expostos a uma série de riscos no ambiente digital. (Moraes & Bustamante, 2021).

Diante disso, é possível perceber que embora haja leis sancionadas, na prática, elas, no momento atual, são ineficazes para conter a pratica de crimes cibernéticos e auxiliar os grupos vulneráveis na resolução de conflitos digitais, impostos no dia a dia.

3 CONSIDERAÇÕES FINAIS

A partir do exposto, torna-se evidente que, o acesso à justiça e a proteção jurídica contra crimes cibernéticos revelou importantes aspectos sobre os desafios enfrentados por pessoas em situação de vulnerabilidade no ambiente digital. A partir de uma análise abrangente da literatura e das políticas existentes, constatou-se que, apesar dos avanços legislativos promovidos pelo Marco Civil da Internet e pela LGPD, a proteção digital no Brasil ainda apresenta lacunas significativas, especialmente no que diz respeito à inclusão e educação digital para grupos mais vulneráveis.

A exclusão digital foi identificada como uma barreira central que limita o acesso à justiça e a segurança digital desses indivíduos. Os dados indicaram que a falta de infraestrutura, conhecimento técnico e apoio educacional impede que muitos cidadãos, sobretudo aqueles de baixa renda, idosos, crianças e mulheres, compreendam e utilizem plenamente as ferramentas tecnológicas de maneira segura e autônoma.

Além disso, os crimes cibernéticos, como roubo de identidade, fraudes e assédio virtual, demonstraram ser uma ameaça constante para esses grupos de risco. Ressaltando que, sem uma educação digital sólida e sem a conscientização sobre os direitos de proteção de dados e segurança digital, esses indivíduos permanecem em uma posição de desvantagem, tornando-se alvos fáceis para práticas abusivas. Esses crimes, muitas vezes direcionados a

pessoas com menor domínio do ambiente digital, reforçam a necessidade de políticas públicas focadas não apenas na regulamentação do ambiente virtual, mas também na capacitação e educação contínua para o uso seguro da internet.

Portanto, conclui-se que uma abordagem integrada, que combine educação digital, políticas públicas inclusivas e uma legislação robusta, é essencial para reduzir a vulnerabilidade digital dos grupos de risco e promover um ambiente digital mais seguro e acessível.

REFERÊNCIAS BIBLIOGRÁFICAS

ALMEIDA, Vanessa Aparecida Fagundes **Privacidade e os direitos dos usuários na internet***.* São Paulo: Novatec Editora, 2017.

AIRES, Ana Sylvia Cardoso **Acesso à Justiça, exclusão digital e a inteligência artificial no Poder Judiciário do Brasil: desafios e perspectivas**. Revista do Tribunal Regional Federal da 1ª Região*, 2023.* Disponível em: https://revista.trf1.jus.br. Acesso em: 10 nov. 2024.

BARELLI, Edson Fernandes; SILVA, Sérgio Nogueira da. **Os desafios da vulnerabilidade digital diante do acesso à Justiça e seus principais aspectos durante a pandemia da Covid-19**. Consultor Jurídico, 2022. Disponível em: https://www.conjur.com.br. Acesso em: 10 nov. 2024.

BRASIL. Lei Nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 29 mai. 2024

BRASIL, **Decreto-Lei 2.848, de 07 de dezembro de 1940**. Código Penal. Diário Oficial da União, Rio de Janeiro. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 29 mai. 2024

BROADHURST, Roderic; CHANG, Lai Yee Ching **Cybercrime in Asia: trends and challenges**. In: HEBENTON, B.; SHOU, S. Y.; LIU, J. (Eds.). Asian Handbook of Criminology*.* Springer, 2013.

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

GONZAGA, Alexandre de Almeida **O acesso à justiça pelos grupos vulneráveis em tempos de pandemia do novo coronavírus (covid-19).**

Revista Humanidades e Inovação, 2020, v. 7, n. 19. Disponível em: https://revista.unitins.br. Acesso em: 10 nov. 2024.

MORAES, Ana Luiza Pereira; BUSTAMANTE, André Pessoa. **Uma reflexão sobre o acesso à justiça e os meios digitais. Revista Temática Permanente da Comissão de Mediação e Métodos Consensuais** *OAB RJ*, 2021. Disponível em: https://revistaeletronica.oabrj.org.br. Acesso em: 10 nov. 2024.

SOLOVE, Daniel Joshua; HARTZOG, W. Breached!: **Why Data Security Law Fails and How to Improve it**. Oxford: Oxford University Press, 2022.

TAVARES, Marcelo Carvalho. **A proteção dos dados pessoais na internet: uma análise comparativa entre Brasil e União Europeia**. Revista de Direito Comparado, 2016, v. 10, n. 1.

VIEIRA, Marco Aurélio. **A vulnerabilidade digital e os desafios para a proteção dos direitos fundamentais**. Revista de Direito Público, 2018, v. 14, n. 2.

ZANATTA, Rafael Francisco. **A Lei Geral de Proteção de Dados e os desafios para a proteção da privacidade no Brasil**. Revista de Direito Administrativo, 2019, v. 275.