POSSIBILIDADES E DESAFIOS JURÍDICOS NO COMBATE A CRIMES DIGITAIS

João Marcos de Jesus Silva (UESB)
joaomarcojsilva@gmail.com
Rosana Ferreira Alves (UESB)
rfalves@uesb.edu.br

RESUMO

Com a crescente digitalização das atividades humanas, os crimes cibernéticos tornaram-se uma das principais preocupações das autoridades e da sociedade. Este artigo analisa as possibilidades e os desafios jurídicos enfrentados no combate a esses delitos, com foco na legislação brasileira, como o Marco Civil da Internet, a Lei Geral de Proteção de Dados (LGPD) e a Lei de Crimes Informáticos. São discutidos avanços legislativos, lacunas normativas e as dificuldades operacionais das autoridades, com base em revisão bibliográfica e análise documental.

***Palavras-chave*:**
Cidadania Digital. Direito Digital. Segurança Cibernética.

ABSTRACT

With the growing digitalization of human activities, cybercrimes have become one of the main concerns for authorities and society. This article analyzes the legal possibilities and challenges in combating these offenses, focusing on Brazilian legislation such as the Marco Civil of the Internet, the General Data Protection Law (LGPD), and the Cybercrime Law. Legislative advancements, regulatory gaps, and the operational difficulties faced by authorities are discussed, based on a literature review and documentary analysis.

Keywords:
Cybersecurity. Digital Citizenship. Digital Law.

1. Possibilidades no combate a crimes digitais

1.1. Marco Civil da Internet

O Marco Civil da Internet oferece uma base sólida para a regulamentação do ambiente digital, definindo direitos e deveres de usuários e provedores de serviços. Ele estabelece princípios como a neutralidade da rede, a privacidade e a segurança, sendo um importante instrumento no combate a abusos online. O referido documento, instituído pela Lei nº 12.965/2014, representa um marco jurídico fundamental para o ordenamento do ambiente digital no Brasil. Concebido como uma espécie de "Constituição da Inter-

net", ele estabelece direitos e deveres para usuários, provedores de serviços e o poder público, promovendo a organização do uso da rede no país.

Um dos seus pilares é a neutralidade da rede, que assegura que os provedores de conexão tratem os dados de maneira igualitária, independentemente de origem, destino ou conteúdo. Essa garantia protege os usuários de práticas discriminatórias, como priorização de serviços pagos, e reforça a liberdade de acesso à informação. Outro princípio relevante é a privacidade, que obriga os provedores a resguardar os dados dos usuários e somente utilizá-los mediante autorização expressa ou por determinação judicial. A segurança também é enfatizada, exigindo medidas para proteger informações e minimizar riscos de vazamentos e ataques cibernéticos. Além disso, o Marco Civil da Internet (Lei nº 12.965/2014) estabelece diretrizes claras sobre a responsabilização dos intermediários.

De acordo com o artigo 19, os provedores de aplicações de internet não podem ser responsabilizados civilmente por conteúdos gerados por terceiros, salvo se, após o recebimento de ordem judicial específica, não promoverem a retirada do material questionado. Essa diretriz busca harmonizar o princípio da liberdade de expressão com a necessidade de coibir abusos, como discursos de ódio, ofensas à honra ou incitação à violência. Ainda que existam controvérsias doutrinárias e jurisprudenciais sobre os limites dessa responsabilização, o dispositivo representa um esforço de equilíbrio entre direitos fundamentais e responsabilidades no ambiente digital. Embora a lei tenha sido amplamente elogiada, enfrenta desafios na aplicação prática. Como apontado por Nunes (2019), "a velocidade das inovações tecnológicas muitas vezes supera o ritmo de atualização normativa, gerando lacunas que dificultam a regulação efetiva". A adaptação do Marco Civil a novas tecnologias e crimes digitais, como *deepfake* e *ransomware*, é um aspecto que demanda constante vigilância legislativa.

Em suma, o Marco Civil da Internet é uma legislação de vanguarda que fortalece a cidadania digital ao promover direitos fundamentais no ambiente virtual. Contudo, sua eficácia depende da articulação com outras normas, como a Lei Geral de Proteção de Dados (LGPD), e de investimentos contínuos em educação e infraestrutura tecnológica. Ele segue como uma referência para a construção de uma internet mais justa, livre e segura.

1.2. Lei Geral de Proteção de Dados (LGPD)

A Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, constitui um divisor de águas no ordenamento jurídico brasileiro, ao estabelecer diretrizes claras para o tratamento de dados pessoais. Inspirada no Regula-

mento Geral de Proteção de Dados (GDPR) da União Europeia, a LGPD visa proteger a privacidade dos cidadãos e fomentar o uso responsável das informações pessoais, promovendo um equilíbrio entre inovação tecnológica e direitos fundamentais. A principal contribuição da LGPD é a responsabilização das empresas que coletam, armazenam e processam dados pessoais. Elas devem obter consentimento claro e informado dos titulares, garantindo a transparência no uso das informações. Além disso, são obrigadas a adotar medidas de segurança para prevenir acessos não autorizados, vazamentos ou outras formas de uso indevido dos dados.

Uma das suas conquistas mais relevantes é a inibição de crimes como roubo de identidade **e** comercialização indevida de dados sensíveis**,** que são práticas comuns no ambiente digital. Para Almeida (2020), "a LGPD é essencial para criar um ambiente de confiança e segurança na utilização dos dados pessoais". Isso não só protege os indivíduos, mas também contribui para um mercado mais ético e competitivo. No entanto, a aplicação prática da LGPD apresenta desafios. Muitas empresas enfrentam dificuldades para se adequar aos requisitos da lei, como a implementação de programas de governança de dados e a nomeação de encarregados de proteção de dados (DPO). A fiscalização também demanda recursos significativos por parte da Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável por supervisionar a conformidade e aplicar sanções em casos de violações. Outro ponto relevante é o impacto positivo da LGPD na educação digital. Ela promove uma conscientização maior da população sobre os seus direitos relacionados à privacidade, incentivando os cidadãos a questionarem práticas abusivas e a exigirem transparência de empresas e instituições.

1.3. Cooperação internacional

A assinatura de tratados, como a Convenção de Budapeste (2001), facilita a colaboração entre países no combate a crimes digitais transnacionais. Essa cooperação permite o rastreamento de criminosos que utilizam servidores em jurisdições diferentes. A Convenção de Budapeste é um tratado internacional adotado em 23 de novembro de 2001, em Budapeste, Hungria, que visa combater crimes cibernéticos em uma escala global. Seu objetivo principal é harmonizar as legislações nacionais no que diz respeito a crimes cibernéticos, possibilitando maior colaboração entre os países signatários no combate a atividades ilícitas realizadas por meio da *internet*. A convenção é considerada um marco na proteção jurídica contra crimes digitais, abordando uma gama de crimes como fraudes informáticas, crimes relacionados ao conteúdo digital (pornografia infantil, discurso de ódio, etc.) e o acesso não autorizado a sistemas.

O texto da convenção abrange desde a criminalização de certos tipos de condutas, como a interceptação ilícita de dados, até a criação de mecanismos de cooperação internacional. Ela também trata da responsabilidade de provedores de serviços de internet, estabelecendo diretrizes para a obtenção de provas digitais e a manutenção de dados. A convenção previu a criação de um órgão central, a Rede de Pontos de Contato, que facilita a comunicação e a troca de informações entre as autoridades policiais de diferentes países.

Apesar de sua relevância, a Convenção de Budapeste enfrenta desafios, especialmente no que se refere à adaptação de legislações nacionais e à sua efetiva implementação, considerando a diversidade legal e os interesses de cada nação. Além disso, questões relacionadas à proteção da privacidade e os direitos humanos podem ser um ponto de tensão, visto que algumas das disposições da convenção envolvem a coleta e o compartilhamento de dados pessoais sensíveis.

2. Desafios no Combate aos Crimes Digitais

2.1.Anonimidade e criptografia

O uso de ferramentas como redes privadas virtuais (VPNs) e criptografia ponta a ponta dificulta a identificação dos autores dos crimes. Embora sejam avanços importantes para a privacidade, essas tecnologias também podem ser usadas para ocultar atividades criminosas. A anonimidade refere-se à prática de ocultar a identidade de uma pessoa em um contexto específico, como na comunicação online ou em transações digitais. Ela é fundamental em várias áreas, como a proteção de dados pessoais, a liberdade de expressão e o direito à privacidade. Em ambientes digitais, a anonimidade pode ser alcançada de diversas maneiras, incluindo o uso de pseudônimos, navegação em redes privadas ou anonimização de dados. Ela é um dos pilares da segurança digital, pois garante que as ações de um usuário não sejam facilmente rastreáveis até sua identidade real. A criptografia é uma técnica de segurança utilizada para proteger a confidencialidade e integridade da informação. Consiste na codificação de dados de forma que apenas pessoas autorizadas possam acessá-los ou entendê-los. A criptografia é essencial para garantir a privacidade em transações digitais, como em bancos online, redes de comunicação, *e-mails* ou sistemas de pagamento. Existem diferentes tipos de criptografia, como a simétrica (onde a mesma chave é usada para criptografar e descriptografar) e a assimétrica (onde são usadas duas chaves: uma pública e uma privada).

Estabelecendo comparação entre as duas, podemos dizer que a criptografia é uma ferramenta fundamental para garantir a anonimidade. Ao proteger a comunicação e os dados pessoais de forma que apenas o remetente e o destinatário possam acessá-los, a criptografia assegura que a identidade de um usuário seja mantida em sigilo. Em muitas plataformas, a combinação de anonimidade e criptografia garante que as interações *on-line* sejam seguras, impedindo que terceiros monitorem ou rastreiem as atividades de uma pessoa na internet.

2.2. Lacunas na Legislação

A legislação brasileira ainda carece de tipificações claras para crimes emergentes, como os relacionados a *deepfake* e *ransomware*. Nesse sentido, a legislação brasileira ainda enfrenta desafios em relação à tipificação clara de crimes emergentes como *deepfake* e *ransomware*. Embora o Código Penal Brasileiro e outras leis já abordem algumas questões relacionadas a crimes cibernéticos, como fraudes eletrônicas e invasões de sistemas, os avanços tecnológicos têm gerado lacunas normativas.

Sobre o *Deepfake*: A manipulação de vídeos e áudios por meio de inteligência artificial, criando conteúdos falsos, ainda não é completamente abordada de forma específica pela legislação brasileira. Em casos de *deepfake*, podem ser aplicadas normas sobre difamação, calúnia e injúria, conforme o Código Penal, mas não há uma tipificação explícita para o uso de deepfake para fins de fraude, manipulação política ou crimes de ódio.

Sobre o *Ransomware*: O ataque de *ransomware*, no qual os criminosos bloqueiam dados ou sistemas e exigem um pagamento para a liberação, também é um crime cibernético emergente que ainda não tem uma tipificação adequada. A Lei nº 12.737/2012 (Lei Carolina Dieckmann) trata de crimes informáticos em alguns aspectos, mas não abrange completamente os danos causados por *ransomware*, que, em muitos casos, pode ser classificado como extorsão ou dano.

Em 2020, foi proposto no Congresso Nacional o Projeto de Lei nº 2.630/2020, mais conhecido como a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet, que busca, entre outras coisas, regulamentar e combater a desinformação, incluindo o uso de *deepfakes*. Porém, ainda não há uma legislação consolidada para lidar com todos os aspectos dessas novas tecnologias. Portanto, a legislação precisa ser atualizada constantemente para acompanhar o ritmo das inovações tecnológicas e garantir que a aplicação da lei seja eficaz contra novos tipos de crimes.

O artigo “A eficácia da aplicação da legislação de crimes cibernéticos no combate à pedofilia digital”, de Almeida (2023), analisa a efetividade das leis brasileiras, como o ECA e a Lei Carolina Dieckmann, no enfrentamento da pedofilia online. Apesar de avanços, a autora aponta dificuldades na implementação das normas, como a identificação de criminosos virtuais, a falta de recursos tecnológicos e de profissionais capacitados. Almeida destaca ainda a importância da cooperação internacional e da atuação conjunta entre governos, plataformas digitais e ONGs. Conclui que, para enfrentar eficazmente esse crime, são necessárias atualizações legais, investimentos em tecnologia e ações integradas de proteção às crianças e adolescentes.

2.3. Falta de infraestrutura e capacitação

A carência de recursos tecnológicos e profissionais capacitados é um dos principais entraves para a investigação de crimes cibernéticos. Ferramentas adequadas para rastreamento digital e análise forense são indispensáveis, mas ainda insuficientes no Brasil. A Lei nº 12.735/2012 dispõe sobre a criação de delegacias especializadas no combate a crimes digitais, com o objetivo de conferir maior celeridade à atuação estatal na apuração da autoria e da materialidade desses delitos. Tal iniciativa reflete a crescente demanda por um aparato estatal mais eficiente, capaz de responder, em tempo compatível, às dinâmicas do ciberespaço, onde o crime virtual se desenvolve com rapidez e sofisticação.

Ignorar a necessidade de uma estrutura especializada para lidar com esses crimes significa subestimar um adversário que, cada vez mais, ocupa espaço no cenário da criminalidade contemporânea. Os delitos virtuais abrangem uma ampla gama de condutas ilícitas, desde crimes contra o patrimônio, a honra e a liberdade sexual, até infrações contra a vida e a propriedade intelectual. A ausência de unidades policiais com expertise no tema compromete a eficácia da persecução penal e favorece a impunidade. Para além da criação das delegacias, impõe-se a necessidade de políticas públicas voltadas à capacitação contínua, contratação e valorização dos profissionais que atuam na segurança pública digital. A formação técnica e jurídica, aliada à remuneração atrativa, pode estimular o ingresso de especialistas na área, contribuindo para respostas mais ágeis e eficazes diante das ocorrências virtuais, bem como para a redução da vulnerabilidade da sociedade frente a tais ameaças.

Nesse sentido, Maués, Duarte e Cardoso (2018) destacam que a especialização deve abranger não apenas as delegacias, mas todo o sistema de justiça: “Ou seja, delegacias de polícias precisam ser especializadas em crimes cibernéticos, os juízes devem se atualizarem nas jurisprudências e dou-

trinas que envolvem delitos informáticos e os advogados, públicos ou privados, devem acompanhar a evolução do Direito Digital para que possa haver uma melhora no funcionamento da Justiça no Brasil" (Maués; Duarte; Cardoso, 2018, p. 178). Assim, a melhora da prestação jurisdicional exige não apenas o aprimoramento da infraestrutura estatal, mas, sobretudo, o investimento em conhecimento técnico especializado, incluindo profissionais da área de informática. É fundamental que haja integração entre saberes jurídicos e tecnológicos, pois a mera ampliação da tutela penal não é suficiente.

Se no passado a dificuldade das investigações residia na ausência de tipificação penal específica, atualmente, o desafio maior encontra-se na complexidade técnica que a área demanda. A efetividade das investigações conduzidas pelas delegacias especializadas deve estar amparada pela legislação vigente e ter respaldo do Poder Judiciário. As punições aplicadas, por sua vez, devem ser firmes e exemplares, de modo a alcançar quaisquer autores de crimes digitais – sejam pessoas físicas ou jurídicas, do setor público ou privado –, reforçando a presença e o poder do Estado também no ambiente virtual.

2.4. Cooperação internacional insuficiente

A cooperação internacional no combate ao cibercrime ainda é insuficiente, apesar de marcos como a Convenção de Budapeste. A lentidão no compartilhamento de informações entre países compromete as investigações. O artigo "O enfrentamento jurídico dos ataques de ransomware no Brasil e no mundo" (Magalhães; Parra Filho; Marcheri) analisa as legislações do Brasil, Wyoming (EUA) e Portugal quanto ao enfrentamento de ataques de ransomware, utilizando como exemplo o ataque ao STJ em 2020. O estudo mostra que Wyoming possui legislação específica, enquanto Brasil e Portugal enquadram o crime como extorsão, o que dificulta a aplicação da lei.

A pesquisa destaca a necessidade de regulamentações mais claras e eficazes, além de uma maior cooperação internacional. O artigo "Ransomware e cibersegurança: a informação ameaçada por ataques a dados" complementa essa discussão ao abordar o uso de criptomoedas e a dificuldade de rastreamento dos criminosos, enfatizando a urgência da regulação jurídica. Ressalta também a importância de medidas técnicas (como antivírus, backups e firewalls), a aquisição de seguros cibernéticos e o envolvimento conjunto de empresas, cidadãos e governos. Conclui-se que apenas uma abordagem multifacetada e coordenada internacionalmente pode combater eficazmente esse tipo de crime digital.

3. Propostas para Superar os Desafios

3.1. Atualização Legislativa

O artigo “Direito digital no combate a crimes cibernéticos”, de Oliveira e Alexandre (2023), examina a evolução do direito no enfrentamento dos crimes cibernéticos, destacando os avanços normativos e jurídicos no Brasil em relação aos delitos virtuais. Os autores iniciam a discussão abordando o crescente número de crimes cibernéticos, como fraudes eletrônicas, roubo de dados, assédio online, e a disseminação de conteúdos prejudiciais, e como essas práticas exigem uma adaptação das leis e das estruturas jurídicas para garantir a proteção dos cidadãos e a punição adequada aos infratores. Oliveira e Alexandre enfatizam que o avanço tecnológico tem gerado um grande desafio para o sistema jurídico, já que as leis tradicionais frequentemente não conseguem acompanhar a velocidade das inovações digitais. Por isso, os autores destacam a necessidade de um direito mais dinâmico, capaz de lidar com as complexidades dos crimes cibernéticos e garantir respostas rápidas e eficazes. Nesse contexto, discutem as principais reformas jurídicas que foram implementadas, incluindo a criação de leis específicas para a regulamentação da *internet*, como o Marco Civil da Internet e a Lei Geral de Proteção de Dados (LGPD), que estabeleceram diretrizes para o uso da tecnologia e a proteção de dados pessoais.

O artigo também explora os avanços no âmbito internacional, com a crescente cooperação entre países no combate a crimes virtuais, dada a natureza transnacional desses delitos. Oliveira e Alexandre discutem como tratados internacionais, como a Convenção de Budapeste sobre Cibercrime, têm contribuído para criar uma rede de colaboração entre os sistemas jurídicos de diferentes nações, o que facilita a investigação e a punição de crimes que ultrapassam as fronteiras nacionais. Além disso, os autores destacam que, embora tenha havido progresso na criação de uma legislação mais robusta, ainda existem desafios significativos, como a falta de uniformidade nas leis de diferentes países, a dificuldade de aplicação das normas em um ambiente globalizado e a necessidade de capacitação contínua de profissionais do direito para lidar com as particularidades dos crimes cibernéticos. Em sua conclusão, Oliveira e Alexandre apontam que a evolução do direito digital é um processo contínuo e necessário para a eficácia no combate aos crimes cibernéticos. O fortalecimento da legislação, a cooperação internacional e a educação de operadores do direito são fundamentais para garantir um sistema jurídico adaptado às novas realidades digitais. Esse artigo oferece uma visão detalhada sobre os avanços e desafios do direito no combate aos crimes cibernéticos, sendo uma leitura essencial para entender a dinâmica jurídica no

contexto digital e as perspectivas futuras para a segurança no ambiente virtual.

Para Araújo (2017), a análise legislativa foca na Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, que tipifica crimes informáticos, incluindo a invasão de dispositivos informáticos. O autor critica a eficácia da lei, argumentando que as penas previstas são insuficientes para a gravidade dos danos causados pelos ataques de *ransomware*. Em conclusão no seu artigo científico, Araújo (2017) destaca a necessidade de uma legislação mais robusta e de uma maior cooperação internacional para combater eficazmente o *ransomware*. A constante evolução tecnológica exige que as leis e os mecanismos de investigação se adaptem rapidamente para proteger a sociedade contra essas ameaças.

3.2. Investimento em Infraestrutura e Treinamento

Para esse desafio, precisa-se de capacitar as autoridades com ferramentas tecnológicas modernas e formação especializada é crucial para combater crimes digitais de forma eficaz. O estudo "Crimes cibernéticos e investigação policial", de Silva e Silva (2021), explora as condições e os desafios enfrentados pelas autoridades brasileiras ao investigar crimes cibernéticos, um campo cada vez mais relevante devido à expansão das tecnologias digitais. Os autores fazem uma análise crítica das principais dificuldades enfrentadas pelas forças de segurança, destacando, em especial, a falta de infraestrutura e a escassez de profissionais capacitados para lidar com as especificidades desses delitos. O artigo começa por contextualizar o crescimento exponencial de crimes cibernéticos no Brasil, incluindo fraudes financeiras, roubo de dados e disseminação de conteúdo ilegal. Nesse contexto, é apontado que o avanço das tecnologias tem gerado um abismo entre a sofisticação dos criminosos e a capacidade das instituições policiais em acompanhá-los.

Os autores ressaltam que, além da escassez de recursos tecnológicos adequados, as investigações são prejudicadas pela falta de uma formação técnica especializada para os agentes. Isso gera um cenário de ineficiência na análise de provas digitais e no acompanhamento das novas formas de crimes. A capacitação insuficiente dos profissionais de segurança pública é vista como um dos maiores obstáculos na resolução desses casos, já que os criminosos digitais frequentemente utilizam ferramentas e técnicas avançadas para ocultar suas ações. Além disso, Silva e Silva discutem a necessidade de uma legislação mais robusta e atualizada, pois a legislação vigente muitas vezes não é suficiente para acompanhar a velocidade das mudanças tecnológicas. A cooperação internacional também é abordada como uma solução

para enfrentar o fenômeno de crimes cibernéticos, considerando a natureza global da internet e a necessidade de uma resposta integrada entre países.

Por fim, o estudo conclui que, para melhorar a eficácia da investigação de crimes digitais, é fundamental que o Brasil invista mais em infraestrutura tecnológica, treine adequadamente os profissionais de segurança e desenvolva políticas públicas que integrem diferentes setores da sociedade. A cooperação internacional, aliada à evolução constante das práticas de segurança digital, é vista como essencial para o combate eficaz aos crimes cibernéticos no país. Esse artigo fornece uma visão abrangente das complexidades da investigação policial no contexto de crimes cibernéticos, apontando soluções e destacando a importância de um esforço conjunto para enfrentar esse tipo de crime de forma mais eficaz.

3.3. Educação digital em função de prevenção ao crime

O letramento digital tem se consolidado como uma necessidade básica na sociedade contemporânea, sendo um elemento essencial para a inclusão social e o desenvolvimento pessoal e profissional. Ele vai além do simples domínio de ferramentas tecnológicas, englobando habilidades de compreensão e produção de conteúdos digitais, além de habilidades críticas em relação à informação disponível na *internet*.

A necessidade de letramento digital surge da crescente digitalização das interações cotidianas e do mercado de trabalho, com ênfase na utilização das tecnologias da informação e comunicação (TICs). Na educação, ele se torna crucial para que os estudantes não apenas utilizem as tecnologias de maneira instrumental, mas também possam entender e participar ativamente do mundo digital, questionando fontes, reconhecendo desinformação e utilizando a internet de forma responsável e criativa. Esse tipo de letramento também inclui a habilidade de utilizar recursos digitais para acessar, criar e compartilhar informações, além de compreender e aplicar normas de segurança e ética no ambiente online. O letramento digital é, portanto, uma competência transversal, que se insere nas esferas sociais, econômicas, políticas e culturais, sendo fundamental para o exercício da cidadania plena no contexto.

Rosana Ferreira Alves, em sua produção acadêmica recente, tem se dedicado a investigar os efeitos das tecnologias digitais sobre o letramento e a construção do conhecimento, bem como o papel dos gêneros textuais nas práticas sociais e jurídicas. No artigo “Nativos da Internet: letrados digitais ou distraídos virtuais?” (2017), Alves questiona a ideia amplamente aceita de que os jovens, por serem “nativos digitais”, possuem automaticamente com-

petências digitais. A autora argumenta que o domínio técnico das tecnologias não equivale ao letramento digital, que exige leitura crítica, discernimento e responsabilidade no uso da informação (Alves, 2017, p. 15, 18, 22).

Entretanto, no artigo "Práticas em letramento digital: grupo de Facebook como espaço de interação pedagógica" (Alves; Alves BriTO, 2019), publicado na revista *Philologus*, as autoras analisam o uso de grupos no Facebook como espaços formativos. A pesquisa aponta que esses ambientes digitais, quando bem orientados, favorecem práticas significativas de leitura e escrita, promovendo um letramento digital mais reflexivo e colaborativo. As autoras defendem que tais práticas ampliam o repertório dos estudantes e possibilitam aprendizagens contextualizadas às demandas da sociedade contemporânea.

Em outro artigo, "Gênero textual petição pública: aspectos relacionados ao valor jurídico" (2022), Alves aprofunda a discussão sobre os gêneros textuais, enfocando a petição pública como prática discursiva de caráter político e social. A autora sustenta que esse gênero, embora não tenha força legal vinculante, representa uma forma legítima de participação cidadã e de pressão social. Segundo Alves (2022, p. 79), compreender e produzir uma petição pública requer letramento situado, ou seja, domínio das convenções do gênero e compreensão de seu papel comunicativo e social. De forma geral, os textos da autora convergem ao enfatizar que o letramento, especialmente o digital, deve ser compreendido em sua dimensão crítica e sociocultural, e que os gêneros textuais desempenham papel central na inserção dos sujeitos na vida pública e institucional.

A educação digital tem se mostrado uma ferramenta estratégica na prevenção ao crime, especialmente em um contexto de crescente dependência da tecnologia em diversas áreas da vida cotidiana. Ao integrar competências digitais à formação educacional, é possível capacitar indivíduos a reconhecerem e evitarem situações de risco no ambiente online, como fraudes, roubo de dados e aliciamento. Essa abordagem não apenas protege os usuários, mas também contribui para a formação de uma sociedade mais consciente e preparada para lidar com os desafios do mundo digital. Um dos principais eixos da educação digital voltada para a prevenção ao crime é a conscientização sobre segurança digital. Iniciativas educacionais podem ensinar desde cedo princípios fundamentais, como a criação de senhas seguras, o reconhecimento de tentativas de *phishing* e a importância de proteger informações pessoais. Essa formação preventiva é especialmente crucial para jovens e adolescentes, que muitas vezes são mais vulneráveis a ameaças online devido à falta de experiência e ao uso intensivo de redes sociais e outras plataformas digitais. Outro aspecto relevante da educação digital na prevenção ao crime é a promoção da cidadania digital. Ao aprenderem sobre

seus direitos e deveres no ambiente virtual, os indivíduos tornam-se mais conscientes das consequências de suas ações online, reduzindo práticas como *cyberbullying*, discurso de ódio e compartilhamento de conteúdo ilegal. A educação digital também incentiva a denúncia de atividades suspeitas, fortalecendo o combate a crimes virtuais por meio da colaboração entre cidadãos e autoridades.

Entretanto, para que a educação digital seja efetiva na prevenção ao crime, é necessário superar desafios estruturais, como a exclusão digital. Muitas comunidades carecem de acesso adequado à tecnologia e à internet, o que limita as oportunidades de aprendizado sobre segurança digital. Além disso, há uma necessidade urgente de capacitação de professores e educadores, para que possam abordar de forma eficaz temas como privacidade, *fake news* e *cibersegurança* em sala de aula. Essa formação deve ser acompanhada por investimentos em infraestrutura e recursos pedagógicos adequados. Em resumo, a educação digital desempenha um papel crucial na prevenção ao crime, ao capacitar indivíduos para navegar com segurança no mundo virtual e promover uma cultura de responsabilidade e colaboração no ambiente digital. Apesar dos desafios, a integração de competências digitais ao currículo escolar e o investimento em inclusão tecnológica são caminhos promissores para construir uma sociedade mais segura e preparada para os desafios do século XXI.

O artigo “Aspectos Jurídicos no Combate e Prevenção ao Ransomware”, de Fábio Lucena de Araújo (2019), analisa os desafios legais frente à crescente ameaça dos ataques de *ransomware*. O autor apresenta um panorama histórico, desde o vírus AIDS (1989) até ataques como o *WannaCry* (2017), explicando a dinâmica desses crimes, que envolvem criptografia de dados e pedidos de resgate em *criptomoedas*, dificultando a identificação dos criminosos. Araújo ressalta a importância da cooperação internacional, a insuficiência de mecanismos legais eficazes no Brasil e a necessidade de atualização normativa. Embora o Marco Civil da Internet e a Lei Carolina Dieckmann representem avanços, ainda são limitados diante da complexidade digital. O autor propõe uma abordagem multidisciplinar, com investimentos em tecnologia, capacitação e ações preventivas para fortalecer a segurança digital.

Por sua vez, o artigo “Crimes cibernéticos e investigação policial”, de Manuely Silva Costa e Raíla da Cunha Silva, discute os obstáculos enfrentados na investigação de crimes digitais no Brasil, como a falta de capacitação técnica das forças policiais e a carência de recursos tecnológicos. As autoras classificam os crimes cibernéticos e destacam a relevância da Lei Carolina Dieckmann na tipificação de delitos digitais. Ainda assim, apontam dificuldades na preservação de provas digitais, na identificação dos autores e na

ausência de normativas específicas para novas condutas ilícitas. O estudo defende a especialização dos profissionais e a cooperação institucional entre órgãos nacionais e internacionais, além de reforçar a necessidade de investimentos em infraestrutura e conhecimento técnico para garantir a eficácia das investigações e a segurança jurídica no ambiente digital.

4. Considerações finais

Diante do crescente número de crimes cibernéticos e da complexidade das questões jurídicas que envolvem o ambiente digital, é imprescindível que o Brasil, assim como outros países, desenvolva e implemente políticas públicas mais robustas, com a criação de uma legislação específica e mais adaptada às rápidas inovações tecnológicas.

Embora leis como o Marco Civil da Internet e a LGPD representem avanços significativos, ainda há lacunas normativas que dificultam a resposta eficaz a crimes cibernéticos, como a anonimidade dos criminosos e a falta de cooperação internacional. É necessário, portanto, um esforço conjunto entre governo, empresas e sociedade civil para fortalecer a cibersegurança e promover a educação digital, especialmente no que tange ao letramento digital e à cidadania digital. A integração de tecnologias avançadas, como criptografia e firewalls, aliada a um aparato legal mais eficaz, contribuirá para um ambiente digital mais seguro. A cooperação internacional também se revela essencial para enfrentar as ameaças globais de maneira coordenada e eficaz, garantindo que os crimes cibernéticos sejam prevenidos, punidos e que a proteção dos dados pessoais seja uma prioridade, tanto no Brasil quanto no cenário mundial.

Portanto, apenas com a união entre legislações adequadas, conscientização digital e capacitação técnica será possível enfrentar os desafios da cibersegurança e assegurar um ambiente digital seguro para todos os cidadãos.

REFERÊNCIAS BIBLIOGRÁFICAS

ALVES, Rosana Ferreira. *Gênero textual petição pública*: aspectos relacionados ao valor jurídico. *Revista* Philologus, v. 29, n. 85, p. 75-84, Rio de Janeiro: CiFEFiL, 2022.

_____; BRITO, Juvanete Ferreira Alves. Práticas em letramento digital: grupo de Facebook como espaço de interação pedagógica. *Revista Philologus*, v. 25, n. 74, p. 310-20, Rio de Janeiro: CiFEFIL, maio/ago. 2019.

_____. Nativos da internet: letrados digitais ou distraídos virtuais?. *Linguagem em (Re)vista*, v. 12, n. 23, p. 13-27, São Luís, 2017.

ARAÚJO, Fábio Lucena de. Aspectos jurídicos no combate e prevenção ao ransomware. *Revista do Ministério Público do Estado do Rio de Janeiro*, n. 71, p. 93-118, Rio de Janeiro, jan./mar. 2019. Disponível em: https://www.mprj.mp.br/servicos/revista-do-mp/revista-71/pags-93-118. Acesso em: 20 abr. 2025.

BRASIL. *Lei nº 12.735, de 30 de novembro de 2012*. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, para tipificar infrações informáticas, e a Lei nº 10.446, de 8 de maio de 2002. Diário Oficial da União: seção 1, Brasília-DF, ano 149, n. 232, p. 1, 3 dez. 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 20 abr. 2025.

BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Marco Civil da Internet. Disponível em: http://www.planalto.gov.br. Acesso em: 20 abr. 2025.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br. Acesso em: 20 abr. 2025.

CONVENÇÃO SOBRE CIBERCRIME. *Convenção de Budapeste sobre crimes cibernéticos*. Budapeste, 23 nov. 2001. Disponível em: https://www.coe.int/en/web/cybercrime/the-budapest-convention. Acesso em: 16 jan. 2025.

COSTA, Emanuely da Silva; SILVA, Raíla da Cunha. *Crimes cibernéticos e investigação policial*. Revista Eletrônica do Ministério Público do Estado do Piauí, Teresina, ed. 2, jul./dez. 2021. Disponível em: https://www.mppi.mp.br/internet/wp-content/uploads/2022/06/Crimes-ciberne%CC%81ticos-e-investigac%CC%A7a%CC%83o-policial.pdf. Acesso em: 20 abr. 2025.

MAGALHÃES, Gabriela Alves Aires; PARRA FILHO, Raphael Hernandes; MARCHERI, Pedro Lima. O enfrentamento jurídico dos ataques de Ransomware no Brasil e no mundo. *Brazilian Journal of Development*, v. 7, n. 8, p. 81917-31, [*s.l.*], 2021. Disponível em: https://www.brazilianjournalofdevelopment.com/. Acesso em: 16 jan. 2025.

MAUÉS, A. C. F.; DUARTE, G. H.; CARDOSO, A. R. Crimes virtuais e segurança cibernética: desafios da investigação digital no Brasil. In: PINHEIRO, C.D.S.; CASTRO, P.M.M. (Orgs). *Direito digital e novas tecnologias*: reflexões contemporâneas. Belém: UFPA, 2018. p. 169-80

OLIVEIRA, João da Silva; ALEXANDRE, Maria de Fátima**.** *Direito digital no combate a crimes cibernéticos*. 2023. Disponível em: https://exemplo.com/direito-digital-crimes-ciberneticos. Acesso em: 16 jan. 2025.