



**CENTRO UNIVERSITÁRIO UNIFTC
CURSO DE GRADUAÇÃO EM DIREITO**

**AÇUCENA VITÓRIA QUEIROZ SANTANA
ANGELA OLIVEIRA DE SOUZA
VENICIUS CONCEIÇÃO ASSIS**

CIBERCRIMES E A ADEQUAÇÃO DA LEGISLAÇÃO BRASILEIRA

**SALVADOR
2024**



**AÇUCENA VITÓRIA QUEIROZ SANTANA
ANGELA OLIVEIRA DE SOUZA
VENICIUS CONCEIÇÃO ASSIS**

CIBERCRIMES E A ADEQUAÇÃO DA LEGISLAÇÃO BRASILEIRA

Trabalho de Conclusão de Curso
apresentado ao Departamento de Direito
do Centro Universitário UNIFTC, Unidade
Salvador, como requisito final para
obtenção do título de Bacharel em Direito.

Orientador: Prof. Dr^a. Júlia Simões Neris

**SALVADOR
2024**



**CENTRO UNIVERSITÁRIO UNIFTC
CURSO DE GRADUAÇÃO EM DIREITO**

ATA DE APROVAÇÃO

**AÇUCENA VITÓRIA QUEIROZ SANTANA
ANGELA OLIVEIRA DE SOUZA
VENICIUS CONCEIÇÃO ASSIS**

CIBERCRIMES E A ADEQUAÇÃO DA LEGISLAÇÃO BRASILEIRA

Trabalho de Conclusão de Curso
apresentado ao Departamento de Direito
do Centro Universitário UNIFTC, Unidade
Salvador, como requisito final para
obtenção do título de Bacharel em Direito.

Aprovado em: ____ de _____ de 2024.

Banca Examinadora

(Nome do orientador, sua titulação e Instituição a que pertence).

(nome do membro interno, titulação e instituição a que pertence).

(nome do membro externo, titulação e instituição a que pertence).



AGRADECIMENTOS

Primeiramente, agradecemos a Deus, fonte de nossa força e esperança, que nos concedeu saúde, coragem e sabedoria ao longo desta caminhada. Em todos os momentos desafiadores, sua presença foi essencial para que pudéssemos seguir em frente e alcançar nossos objetivos.

Agradecemos, com especial carinho, aos nossos familiares. Vocês foram nosso apoio constante, incentivando-nos a perseverar e a não desistir, mesmo diante das dificuldades. Sem o amor, paciência e compreensão de cada um de vocês, esta conquista não seria possível. Obrigado por acreditarem em nós e por estarem sempre ao nosso lado.

Gostaríamos de estender nossa gratidão à nossa orientadora, Prof^a Dr^a Júlia Simões Neris, por sua dedicação, paciência e orientação criteriosa. Agradecemos pela confiança em nosso trabalho, pela disposição em compartilhar seu conhecimento e por nos guiar com maestria durante todas as etapas do desenvolvimento deste projeto. Sua orientação foi fundamental para o nosso crescimento acadêmico e pessoal, e levaremos para a vida os ensinamentos que nos transmitiu.



SANTANA, Açucena; SOUZA, Angela; ASSIS, Venicius. **CIBERCRIMES E A ADEQUAÇÃO DA LEGISLAÇÃO BRASILEIRA**. Orientadora: Júlia Simões Neris¹. 2024. 30 páginas. Trabalho de Conclusão do Curso de Direito – Centro Universitário UNIFTC, Salvador, 2024.

CIBERCRIMES E A ADEQUAÇÃO DA LEGISLAÇÃO BRASILEIRA

CYBERCRIMES AND THE ADEQUACY OF BRAZILIAN LEGISLATION

AÇUCENA VITÓRIA QUEIROZ SANTANA²

ANGELA OLIVEIRA DE SOUZA³

VENICIUS CONCEIÇÃO ASSIS⁴

RESUMO

Este estudo analisa a eficácia da legislação brasileira no combate aos cibercrimes, considerando o avanço tecnológico e as novas ameaças digitais. Explora a evolução das leis, como o Marco Civil da Internet e a Lei Geral de Proteção de Dados, além dos desafios enfrentados pelas autoridades na investigação e punição desses crimes. Com foco na importância da educação digital, cooperação internacional e atualização contínua das leis, o trabalho propõe possíveis medidas a serem adotadas para fortalecer a cibersegurança e proteger os cidadãos no ambiente digital, através da metodologia de pesquisa de revisão crítica da literatura.

Palavras-chave: Cibercrimes, legislação brasileira, Marco Civil da Internet, Lei Geral de Proteção de Dados, investigação, educação digital, cooperação internacional, cibersegurança.

ABSTRACT

This study analyzes the effectiveness of Brazilian legislation in combating cybercrime, considering technological advances and new digital threats. It explores the evolution of laws, such as the Marco Civil da Internet and the General Data Protection Law, as well as the challenges faced by authorities in investigating and punishing these crimes. Focusing on the importance of digital education, international cooperation and continuous updating of laws, the work proposes possible measures to be adopted to strengthen cybersecurity and protect citizens in the digital environment, through the research methodology of critical literature review.

Key-words: Cybercrimes, Brazilian legislation, Marco Civil da Internet, General Data Protection Law, investigation, digital education, international cooperation, cybersecurity.

¹ Docente Orientadora do Centro Universitário UnifTC - Unidade Salvador – BA. Especialista em Direito Tributário pela Faculdade Baiana de Direito e Mestra em Direito pela Universidade Federal da Bahia. E-mail: juusneris@gmail.com

² Graduanda em Direito pelo Centro Universitário Faculdade de Tecnologia e Ciências.

³ Graduanda em Direito pelo Centro Universitário Faculdade de Tecnologia e Ciências.

⁴ Graduando em Direito pelo Centro Universitário Faculdade de Tecnologia e Ciências.

INTRODUÇÃO

O termo "cibercrimes" surgiu na França no final da década de 1990, referindo-se a atividades criminosas ocorridas em ambientes virtuais, empregando tecnologias conectadas à internet como meio de troca de informações e comunicação global (SALGADO, 2009, p. 4). O avanço tecnológico é um elemento crucial nesse contexto, pois diferentes níveis de conhecimento sobre a tecnologia podem expor as pessoas a vulnerabilidades, independentemente de idade, gênero, cor, raça ou religião; qualquer pessoa pode ser alvo de crimes virtuais. Deste modo, este trabalho explora uma questão crítica e urgente: a eficácia das leis brasileiras no combate aos cibercrimes (SIMAS, 2014).

O Código Penal brasileiro tem enfrentado grandes dificuldades para se adaptar a essa modalidade de crime, especialmente diante da rapidez dos avanços tecnológicos e do desenvolvimento contínuo da internet. Diante disso, levanta-se a questão norteadora: a legislação brasileira é suficientemente eficaz para lidar com a crescente incidência de crimes cibernéticos, considerando a evolução tecnológica e as novas modalidades de delitos que surgem a cada dia?

Este trabalho visa analisar a eficácia legislativa na responsabilização dos indivíduos que cometem crimes cibernéticos, além de propor melhorias para adequar a legislação às novas realidades trazidas pela tecnologia. Os objetivos deste estudo são analisar os fatores que contribuem para a vulnerabilidade dos usuários na internet, investigar os principais tipos de cibercrimes e o modus operandi utilizado, identificar as lacunas legais no sistema penal e avaliar a eficácia das políticas de prevenção e repressão aos crimes virtuais.

Para cumprir esses objetivos, o trabalho está estruturado em três capítulos, que abrangem diversos tópicos teóricos, decretos de leis, tratados internacionais e desafios enfrentados pela legislação brasileira em relação aos crimes virtuais.

Para cumprir esses objetivos, o trabalho está estruturado em três capítulos, que abrangem diversos tópicos teóricos, decretos de leis, tratados internacionais e desafios enfrentados pela legislação brasileira em relação aos crimes virtuais.

O primeiro capítulo, "Cibercrimes", oferece uma visão geral dos crimes cibernéticos no Brasil, desde os primeiros registros na década de 1960, que incluíam manipulação de sistemas e sabotagem. Discute também diversas modalidades de crimes virtuais, diferenciando entre crimes virtuais próprios (aqueles praticados exclusivamente no ambiente digital) e impróprios (aqueles em que o ambiente digital facilita ou intensifica o crime).

O segundo capítulo, "Leis e Tratados Internacionais", examina a legislação brasileira aplicável aos crimes cibernéticos, incluindo aspectos como stalking virtual, vingança pornográfica e cyberbullying. Além disso, explora a Convenção de Budapeste e analisa a eficácia das leis brasileiras diante dos desafios impostos por crimes cibernéticos, destacando as limitações e avanços no enfrentamento a essas práticas.

O terceiro capítulo, "Persecução Penal", aborda os desafios na investigação e punição dos crimes cibernéticos. Este capítulo explora a necessidade de capacitação e recursos para as autoridades, a importância da conscientização e educação, e a colaboração entre setores públicos e privados. Também discute a cooperação internacional como um fator essencial para combater eficazmente os cibercrimes, dada a natureza transnacional desses delitos.

A metodologia adotada consiste em uma revisão crítica da literatura existente sobre o tema, utilizando fontes bibliográficas, documentos oficiais, relatórios governamentais e estudos de caso para embasar a análise e as conclusões deste trabalho. A sustentação teórica é fundamentada em abordagens multidisciplinares, abrangendo áreas como direito, criminologia, sociologia e psicologia. A justificativa deste estudo reside na importância de compreender e enfrentar um problema social de grande impacto e complexidade, contribuindo para a formulação de políticas públicas mais eficazes e para a proteção de qualquer cidadão brasileiro.

Ademais, a metodologia adotada consistirá em uma revisão crítica da literatura existente sobre o tema, utilizando fontes bibliográficas, documentos oficiais, relatórios governamentais e estudos de caso para embasar a análise e as conclusões deste trabalho.

MÉTODOS

Para o desenvolvimento deste estudo, foi adotada uma metodologia baseada em uma revisão crítica e sistemática da literatura disponível sobre cibercrimes e a adequação da legislação brasileira ao combate desses delitos.

Primeiramente, a pesquisa explorou fontes bibliográficas de natureza acadêmica e técnica, incluindo artigos científicos, livros especializados, legislações brasileiras e internacionais, bem como documentos oficiais e relatórios emitidos por órgãos governamentais e institutos de pesquisa. Esta revisão foi essencial para identificar as bases normativas que orientam o combate aos cibercrimes e suas limitações práticas, a partir de uma perspectiva multidisciplinar que abrange o direito penal, direito digital, criminologia, sociologia e psicologia.

Além disso, foram utilizados estudos de caso que ilustram o impacto dos cibercrimes no Brasil e os desafios das autoridades para lidar com tais delitos. A análise das legislações foi acompanhada de uma contextualização histórica que incluiu a origem e evolução de normas como o Marco Civil da Internet e a Lei Geral de Proteção de Dados, ambas fundamentais no contexto brasileiro.

Internacionalmente, o trabalho considerou também a Convenção de Budapeste, importante tratado que busca estabelecer diretrizes de cooperação internacional para o enfrentamento dos cibercrimes, promovendo um padrão mínimo de segurança digital entre países signatários. Esse método de pesquisa documental possibilitou, ainda, o mapeamento das práticas investigativas mais comuns e das dificuldades encontradas no cumprimento das leis, principalmente na obtenção e preservação de provas digitais.

Em síntese, a metodologia utilizada combinou uma revisão crítica de literatura com análise documental e de casos práticos, integrando múltiplas perspectivas sobre a eficácia da legislação brasileira e os obstáculos operacionais enfrentados por autoridades e usuários na proteção de dados e segurança digital.

Acredita-se que esse enfoque multidisciplinar e o uso de estudos de caso proporcionaram uma base sólida para que as conclusões e recomendações finais do trabalho sejam fundamentadas e contribuam para o fortalecimento das políticas de cibersegurança no Brasil.

CAPÍTULO I - CIBERCRIMES

1. CONCEITO E HISTÓRIA CIBERCRIMES NO BRASIL

O termo “cibercrime” surgiu na década de 90 durante uma reunião, em Lyon, na França, que reuniu um subgrupo das nações do G8 que é um grupo de países que se consideram democráticos e que são considerados os mais influentes e desenvolvidos economicamente do mundo. Este subgrupo analisou, discutiu e adotou este termo para descrever os crimes promovidos via aparelhos eletrônicos ou pela disseminação de informações na internet (SALGADO, 2009, p. 4).

A legislação brasileira vem se adequando ao desenvolvimento social, conforme a conduta da sociedade, respeitando direitos fundamentais, como a liberdade de expressão, o direito à informação, entre outros direitos básicos. No que diz respeito aos crimes cibernéticos, eles representam um campo de conflitos entre o direito e a internet, cuja presença se torna cada vez mais constante. Isso exige da legislação brasileira a responsabilidade de criar regulamentações (SALES, 2023. p 237).

2. PANORAMA DOS CRIMES CIBERNÉTICOS NO BRASIL

Os cibercrimes, também conhecidos como crimes digitais ou informáticos, referem-se a condutas ilícitas realizadas no ambiente virtual, utilizando tecnologias digitais como ferramentas principais. Com a crescente digitalização das atividades humanas e a ampla dependência da internet para funções cotidianas, comerciais e institucionais, os cibercrimes tornaram-se uma preocupação central para governos, empresas e cidadãos.

Em sentido estrito, a criminalidade informacional inclui crimes em que, segundo Simas (2014, p. 12), “o meio informático surge como parte integradora do tipo legal, ainda que o bem jurídico protegido não seja digital”.

Os primeiros registros de crimes cibernéticos surgiram por volta da década de 1960, quando delitos envolvendo manipulação de sistemas, sabotagem, espionagem e abuso de computadores começaram a ser notados. No entanto, foi na década de 1980 que, com as significativas transformações sociais

e econômicas trazidas pelo avanço tecnológico, esses crimes ganharam maior visibilidade (OLIVEIRA JÚNIOR, 2013).

Desde 2012, o Brasil tem enfrentado os crimes cibernéticos por meio de legislações específicas, como a Lei Carolina Dieckmann, sancionada em 30 de novembro de 2012. Essa lei tipifica crimes como invasão de computadores, violação de dados de usuários e derrubada de sites (SALES, 2023, p. 241). Ela também acrescentou ao Código Penal os artigos 154-A e 154-B, além de modificar os artigos 266 e 298, parágrafo único, especificando os crimes de falsificação de documentos particulares e de cartão por intermédio da internet (BRASIL, 2012).

Entre os crimes cibernéticos, destacam-se o stalking virtual (Lei n. 14.132/2021) e a vingança pornográfica (Lei n. 13.718/2018), ambos tipificados no Código Penal Brasileiro.

Segundo Damásio de Jesus e José Antonio Milagre (2016, p. 09), o cibercrime refere-se a um “fato típico e antijurídico praticado contra a tecnologia da informação, ou seja, cometido através da informática em geral”.

Esses crimes virtuais, como a vingança pornográfica, são frequentemente cometidos por alguém que mantinha uma relação com a vítima e divulga imagens íntimas na internet, geralmente como retaliação pelo fim do relacionamento (SALES, 2023, p. 243).

A evolução tecnológica, com o surgimento de aplicativos de mensagens e videochamadas, tem facilitado a comunicação em rede em questão de segundos. Esse fácil acesso à informação e à comunicação tem sido um dos principais fatores para o crescimento dos crimes cibernéticos.

De acordo com Simas (2014, p. 14), "a evolução nas novas tecnologias impacta o fenômeno criminal, pois a tecnologia pode, por um lado, ser objeto de crimes e, por outro, suscitar e potencializar novas formas de criminalidade ou práticas de crimes antigos".

Essa evolução intensificou o combate aos crimes digitais, exigindo que a legislação brasileira se adapte, ainda que de forma gradual, à nova realidade. A última grande inovação legislativa foi o Marco Civil da Internet (BRASIL, 2014), uma lei que regulamenta o uso da internet por usuários, consumidores, empresas e provedores de redes.

Diversas modalidades de crimes cibernéticos são comuns no Brasil. Augusto Eduardo de Souza Rossini destaca algumas das mais recorrentes, como falsificação de dados, fraudes eletrônicas, crimes relacionados à pornografia infantil, além de racismo e xenofobia, crimes que se manifestam na disseminação de imagens que promovem discriminação ou violência contra indivíduos ou grupos com base em raça, religião, cor, ascendência ou origem étnica.

Esses delitos são particularmente graves porque utilizam a internet como meio de propagação, ampliando seu alcance de maneira ilimitada. Em questão de segundos, informações podem se espalhar e qualquer pessoa com acesso à internet pode ser impactada.

Conforme mencionado pela Deputada Federal Tábata Amaral, em entrevista ao Flow Podcast em 27 de setembro de 2024, "o Poder Judiciário brasileiro ainda não está preparado para lidar com questões envolvendo redes sociais, inteligência artificial, robôs ou outras tecnologias emergentes."

Portanto, é fundamental questionar o impacto da inércia das autoridades legislativas, que perpetua esse ciclo de atraso. É urgente a criação de esforços coordenados para oferecer soluções reais para combater os crimes cibernéticos, promovendo a justiça por meio de investimentos em tecnologia.

Concluindo este panorama dos crimes cibernéticos no Brasil, passaremos à definição e exemplos de crimes cibernéticos próprios e impróprios.

2.1. CRIMES (PRÓPRIOS E IMPRÓPRIOS)

Os crimes praticados no ambiente digital são conhecidos por diversas terminologias, tais como crimes virtuais, digitais, informáticos, telemáticos, de alta tecnologia, crimes computacionais, fraudes informáticas, delitos cibernéticos e crimes transnacionais. Esses delitos podem ser divididos em duas categorias principais: crimes puros (ou próprios) e crimes impuros (ou impróprios).

Os crimes puros referem-se àqueles que são cometidos exclusivamente por meios eletrônicos, onde o bem jurídico diretamente protegido é a informática. Nesse caso, a prática ilícita só pode ocorrer no ambiente digital e depende totalmente da tecnologia para sua realização.

Por outro lado, os crimes impuros ocorrem quando o computador ou a tecnologia é utilizado apenas como um instrumento para alcançar um resultado que afeta o mundo físico ou real, lesando ou ameaçando bens jurídicos que vão além da esfera informática (ALBUQUERQUE, 2000, p. 40-41).

2.1.1. CRIMES CIBERNÉTICOS PRÓPRIOS

Os crimes cibernéticos próprios são aqueles que ocorrem exclusivamente no ambiente digital, ou seja, só podem ser praticados por meio de dispositivos eletrônicos, como computadores, celulares ou outros aparelhos informatizados. Nesse tipo de crime, o objetivo é violar diretamente dados ou sistemas informatizados, sendo o bem jurídico protegido a integridade das informações digitais.

Segundo preleciona Anderson Soares Furtado Oliveira, crime cibernético próprio é aquele que:

[...] só pode ser cometido no ciberespaço, ou seja, necessariamente, deve ser realizado no ambiente do ciberespaço, para que a conduta seja concretizada, tendo um tipo penal distinto do tradicional. Ademais, tanto a ação quanto o resultado da conduta ilícita consumam-se no ciberespaço. (OLIVEIRA, 2009, p.33).

Esses crimes geralmente são cometidos por hackers que utilizam o ambiente virtual para realizar ações que não seriam possíveis fora desse contexto. Conforme explica Marco Túlio Vianna, em seu livro Fundamentos de Direito Penal Informático, "são aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados)" (VIANNA, 2003).

Esses crimes dependem exclusivamente da tecnologia para ocorrer e, portanto, não poderiam ser executados fora do ambiente digital.

2.1.2. CRIMES CIBERNÉTICOS IMPRÓPRIOS

Por outro lado, os crimes cibernéticos impróprios são aqueles que podem ocorrer tanto no ambiente digital quanto fora dele, sendo que, no caso dos crimes cibernéticos, a tecnologia é utilizada apenas como ferramenta. A diferença

é que esses crimes já são reconhecidos pelo Código Penal, mas o meio digital é utilizado para facilitar ou executar a prática ilícita.

Seguindo a linha de pensamento de Aires José Rover, sobre crimes impróprios:

São todas aquelas condutas em que o agente se utiliza do sistema de informática como mera ferramenta para a perpetração de crime comum, tipificável na lei penal. Dessa forma, o sistema de informática não é essencial à consumação do delito, que poderia ser praticado por meio de outra ferramenta. (ROVER, 2009, p.3).

Exemplos incluem crimes contra bens jurídicos comuns, como a violação da dignidade da pessoa humana, entre outros. Esses crimes são cometidos no ambiente digital, mas trazem consequências diretas para a vida real.

Assim, o patrimônio continua protegido pela lei, seja ele um objeto físico ou uma quantia de dinheiro "grafada por meio de bits". A tecnologia, nesse caso, é apenas o meio para a execução do crime. Por exemplo, a alteração de dados bancários ou a transferência ilegal de valores por meios digitais é equivalente ao furto ou roubo tradicional, mas a ação ocorre no mundo virtual, envolvendo bens imateriais, como dados e informações financeiras.

Conforme explica Rita de Cássia Lopes da Silva:

"A informação, neste caso, por se tratar de patrimônio, refere-se a bem material, apenas grafado por meio de bits, suscetível, portanto, de subtração. Assim, ações como a alteração de dados referentes ao patrimônio, como a supressão de quantia de uma conta bancária, pertencem à esfera dos crimes contra o patrimônio" (SILVA, 2003).

Esses crimes, sejam próprios (que ocorrem exclusivamente no ambiente digital) ou impróprios (que podem ocorrer tanto online quanto offline), trazem consequências graves para os indivíduos e o patrimônio. Suas modalidades variam desde fraudes eletrônicas até crimes mais graves, com potencial de impacto significativo.

Concluindo este capítulo que fala sobre cibercrimes, passaremos à profunda discussão no próximo capítulo sobre leis e tratados internacionais em especial que o Brasil esteja inserido, e se a legislação brasileira é suficientemente eficaz para lidar com a crescente incidência de cibercrimes.

CAPÍTULO II - LEIS E TRATADOS INTERNACIONAIS

1 . LEGISLAÇÃO BRASILEIRA APLICÁVEL AOS CRIMES CIBERNÉTICOS.

Na legislação brasileira, temos como referência algumas leis criadas para estabelecer punições aos crimes cibernéticos. Cronologicamente, começamos pela Lei Carolina Dieckmann (Lei nº 12.737/2012), a primeira lei a punir crimes cibernéticos, que inseriu no Código Penal Brasileiro o crime de invasão de computadores e dispositivos eletrônicos, independente de conexão à internet. Essa lei marcou o início do combate aos crimes virtuais.

Em 3 de novembro de 2012, foi promulgada a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, em razão de um incidente envolvendo a atriz. Em maio de 2011, um hacker invadiu seu computador pessoal, acessando 36 fotos pessoais e íntimas e exigindo a quantia de 10 mil reais para não publicá-las. A atriz recusou a extorsão, e as fotos acabaram sendo divulgadas na internet. Esse caso trouxe o tema à tona e resultou na criação da lei, que “dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências” (art. 1º), promovendo alterações no Código Penal (SALES, 2023, p. 241).

No Código Penal Brasileiro, o art. 154-A dispõe:

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. (Redação dada pela Lei nº 14.155, de 2021) (BRASIL, 2012).

Em 2012, foi promulgada a Lei nº 12.965/2014, conhecida como Marco Civil da Internet (MCI) (BRASIL, 2014). Essa lei regulamenta os direitos e deveres dos consumidores virtuais, protege a privacidade e os dados pessoais dos usuários, e promove a responsabilidade dos provedores de internet, estabelecendo garantias, regulamentações e direitos para o uso da internet no Brasil. Ela também define diretrizes para a atuação da União, dos Estados, do Distrito Federal e das capitais brasileiras (SALES, 2023, p. 238).

A Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), estabelece no art. 1º que:

“Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural” (BRASIL, 2018).

A proteção da privacidade e dos dados pessoais na internet é um dos principais objetivos da LGPD. Além de responsabilizar provedores de internet, a lei impõe responsabilidades às empresas que tratam dados pessoais, exigindo que elas formulem regras de boas práticas e de governança em privacidade (SALES, 2023, p. 246). Essa legislação foi criada em resposta à crescente incidência de crimes cibernéticos e aos problemas decorrentes do vazamento de dados pessoais. Essas leis visam tipificar atos como invasão de computadores, roubo de senhas, violação de dados de usuários e divulgação de informações privadas.

2. STALKING VIRTUAL, VINGANÇA PORNOGRÁFICA E CYBERBULLYING

Entre os crimes cibernéticos, destacam-se o stalking virtual (Lei nº 14.132/2021) e a vingança pornográfica (Lei nº 13.718/2018), ambos tipificados no Código Penal Brasileiro.

O stalking virtual, de acordo com o art. 147-A do CPB, consiste em:

“Perseguir alguém reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade” (BRASIL, 2021).

Conforme o art. 147-A do CPB, a perseguição pode ocorrer de várias maneiras, como mensagens eletrônicas, SMS, WhatsApp, Telegram ou qualquer outro aplicativo de rede social (SALES, 2023, p. 244).

A vingança pornográfica (revenge porn), prevista no art. 218-C do CPB, é definida como:

“Divulgação de cena de estupro ou de cena de estupro de vulnerável, de cena de sexo ou de pornografia”, sem o consentimento da vítima. Esse crime, agora conhecido como crime de vingança sexual, geralmente é cometido por alguém que tinha uma relação com a vítima e que divulga imagens íntimas como forma de vingança pelo fim do relacionamento (SALES, 2023, p. 243).

O Cyberbullying consiste em práticas de bullying no ambiente virtual, frequentemente se sobrepondo ao stalking, pois envolve a reiteração de ofensas e perseguições com xingamentos e ataques à honra da vítima. A identificação

dos autores desses crimes é complexa, pois eles utilizam perfis falsos em redes sociais e até técnicas para alterar o identificador de Protocolo de Internet (IP).

O cyberstalking é, portanto, o uso da tecnologia para perseguir alguém e se diferencia da perseguição “offline” (ou mero stalking) justamente no que tange o modus operandi, que engloba o uso de equipamentos tecnológicos e o ambiente digital. Além disso, o stalking e o cyberstalking podem se mesclar, havendo as duas formas concomitantemente. O stalker –indivíduo que pratica a perseguição – mostra-se onipresente na vida da sua vítima, dando demonstrações de que exerce controle sobre ela, muitas vezes não se limitando a persegui-la, mas também proferindo ameaças e buscando ofendê-la ou humilhá-la perante outras pessoas. Curiosamente o cyberstalking é cometido, muitas vezes, não por absolutos desconhecidos, mas por pessoas conhecidas, não raro por ex-parceiros como namorados, ex cônjuge, etc. (CRESPO, 2015, p. 1).

Conforme a Lei nº 14.811, de 12 de janeiro de 2024, foram instituídas medidas de proteção à criança e ao adolescente contra a violência nos estabelecimentos educacionais ou similares. Essa lei também prevê a Política Nacional de Prevenção e Combate ao Abuso e Exploração Sexual de Crianças e Adolescentes e altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) (BRASIL, 2024).

O Brasil enfrenta grandes desafios no combate aos crimes cibernéticos. As estratégias adotadas pelas autoridades públicas incluem investimentos em capacitação e tecnologia, cooperação internacional, conscientização pública e troca de informações entre setores operacionais e administrativos, visando soluções eficazes para esses casos complexos.

Concluindo esta abordagem sobre a legislação brasileira, passaremos a abordar sobre a Convenção de Budapeste, na qual o Brasil está inserido.

3. A CONVENÇÃO DE BUDAPESTE

De acordo com o Ministério da Justiça e Segurança Pública (MJSP) (2024), a Organização das Nações Unidas (ONU) tem se empenhado na criação de normas que sirvam de base para países que ainda não possuem legislação nacional específica para o combate aos cibercrimes. O texto, aprovado em 8 de

agosto de 2024, está em consonância com a Convenção de Budapeste, tratado internacional relacionado a cibercrimes, ao qual o Brasil aderiu pelo Decreto Legislativo nº 37/2021, e promulgado pelo Decreto nº 11.491/2021.

Segundo o Ministério da Justiça e Segurança Pública (2024):

“Crimes como tráfico de pessoas, contrabando de migrantes, pedofilia, estelionato e lavagem de dinheiro utilizam diversas tecnologias e a internet. O cibercrime ultrapassa as fronteiras geográficas dos países e essa convenção vai contribuir para a cooperação e a colaboração entre os países no seu enfrentamento”, avalia o secretário Nacional de Justiça, Jean Keiji Uema (MJSP, 2024).

A Convenção de Budapeste, aprovada pelo Congresso Nacional por meio do Decreto Legislativo nº 37/2021 e promulgada pelo Decreto nº 11.491/2023, orienta os países aderentes a adotar medidas legislativas e outras providências necessárias para tipificar como crimes condutas virtuais que causem danos patrimoniais e morais, incluindo: (art. 2º) acesso ilegal a qualquer tipo de computador, (art. 3º) interceptação ilícita, (art. 4º) violação de dados, (art. 5) interferência em sistemas e (art. 6) uso indevido de dispositivos (BRASIL, 2023).

A Convenção ainda relacionou os tipos de crimes em títulos distintos:

- a) Título I: crimes relacionados com computadores, crimes que atentam a confiabilidade, a integridade e disponibilidade de sistemas e dados informatizados (Arts. 2º ao 6º);
- b) Título II: outros crimes relacionados com computadores (Arts. 7º e 8º);
- c) Título III: crimes relacionados ao conteúdo, como produção ou distribuição ilícita de pornografia infantil (Art. 9º);
- d) Título IV: crimes relacionados com a violação de direitos autorais e conexos (Art. 10º); e
- e) Título V: disposições acerca da tentativa, auxílio e cumplicidade, sanções e medidas (Arts 11 ao 13). Decreto nº 11.491/2023 (BRASIL, 2023).

Conforme ilustrado na pesquisa acima, a Convenção de Budapeste tem grande relevância internacional no combate aos cibercrimes. Essa importância decorre da falta de cooperação internacional entre os países, e o tratado foi criado para auxiliar na tipificação penal desses crimes, tanto em países subdesenvolvidos quanto em desenvolvidos. Embora não seja necessário que as nações copiem exatamente as legislações de outros países integrantes, elas devem se adequar à realidade de uma internet sem fronteiras territoriais, onde a circulação de informações ocorre entre países sem necessidade de presença física.

O Estado não desaparece, porém. É apenas redimensionado na Era da Informação. Prolifera sob a forma de governos locais e regionais que se espalham pelo mundo com seus projetos, formam eleitorados e negociam com governos nacionais, empresas multinacionais e órgãos internacionais. (...) O que os governos locais e regionais não têm em termos de poder e recursos é compensado pela flexibilidade e atuação em redes. (CASTELLS, 2007).

Diante do exposto, sobre a Convenção de Budapeste, passa-se a discutir a eficácia das leis brasileiras e se elas são realmente suficientes para o combate aos cibercrimes.

4. EFICÁCIA DAS LEIS BRASILEIRAS DIANTE DOS CIBERCRIMES

As leis brasileiras enfrentam dificuldades nas investigações criminais para identificar os autores dos cibercrimes. Apesar da colaboração entre diferentes setores e o aprimoramento ao longo dos anos, as instituições competentes, como o Ministério Público, a Polícia e o Judiciário, encontram desafios significativos (SIQUEIRA, 2017, p. 122).

Por conta dessas tais dificuldades, a população brasileira tem se sentido vulnerável aos crimes virtuais, pois a vulnerabilidade de qualquer cidadão é muito clara, qualquer pessoa hoje em dia é exposta facilmente na internet e a identificação do criminoso, muitas das vezes não chega a êxito, trazendo consigo uma sensação de impunidade.

A dificuldade de punição desses criminosos não se deve à falta de tipificação penal. Conforme discutido, existem leis específicas para punir esses agentes. A principal dificuldade está na ausência de pessoal qualificado e de tecnologia avançada para identificar com precisão os autores dos crimes.

Segundo Preleciona Siqueira, (2017, p.122), “Seria possível a identificação do criminoso obtendo o seu endereço de IP, login e senha do aparelho utilizado para a prática do crime, porém, os criminosos utilizam endereços falsos, dificultando o trabalho investigativo dos policiais.”

Conforme indica Barreto e Brasil (2016) , a Lei do Marco Civil da Internet (MCI) foi criada para complementar lacunas no sistema jurídico brasileiro em relação aos crimes virtuais. Nas primeiras linhas, a lei destaca como objetivo principal estabelecer fundamentos, conceitos e diretrizes para o uso da internet. O MCI busca, entre outras finalidades, enumerar os direitos dos usuários, supervisionar conflitos polêmicos, assegurar a atuação do Poder Público diante

de crimes virtuais e garantir o acesso à internet de forma íntegra, tanto individual quanto coletiva, com todos protegidos e amparados pela lei.

Segundo a Constituição Federal de 1988:

Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação (BRASIL, 1988).

Conforme mencionado, o Marco Civil da Internet, juntamente com a Lei Carolina Dieckmann, a Lei de Cyberbullying e a Lei de Proteção de Dados, têm como base o art. 5º da Constituição Federal de 1988. Todas essas normas visam proteger a vida, a liberdade, a igualdade, a segurança, a intimidade e outros direitos fundamentais. Contudo, mesmo com a tipificação de crimes e as punições previstas, a sensação de vulnerabilidade persiste, pois a ausência de identificação dos autores dos crimes ainda representa um grande desafio para as instituições governamentais.

Assim, o combate aos crimes virtuais exige uma ação contínua e integrada entre o sistema jurídico, as instituições públicas e a sociedade. Conclui-se que, segundo Barreto e Brasil (2016, p. 15): a eficácia legislativa não alcança resultados significativos devido à dificuldade em identificar a autoria dos delitos.

Para avaliar a eficácia das leis brasileiras no combate aos cibercrimes, é necessário primeiro compreender o que torna uma legislação eficaz. Essa análise não precisa se limitar ao direito penal aplicado a crimes digitais; ao contrário, podemos buscar fundamentos em fases processuais, na doutrina jurídica e em áreas complementares do Direito, como o direito civil e o administrativo, para construir uma visão mais abrangente sobre a efetividade legislativa.

Rogério Montai de Lima, por exemplo, destaca a importância da fase da sentença para assegurar a eficácia do exercício do direito de ação. Ele defende que, para alcançar um mínimo de eficácia processual, é fundamental dar atenção a essa fase crucial. A palavra “sentença” aparece 144 vezes no Código de Processo Penal, 203 vezes no Código de Processo Civil e 12 vezes na

Constituição Federal de 1988, o que ressalta sua relevância para o processo jurídico (LIMA, 2013, p. 25).

Aury Lopes Jr. traz uma crítica contundente ao cenário do processo penal brasileiro, descrevendo-o como um "ciclo vicioso e autofágico". Segundo ele, o direito penal no Brasil tornou-se excessivamente abrangente, sendo utilizado como solução para uma ampla gama de problemas que poderiam ser resolvidos em outras esferas, como a administrativa. Essa tendência leva a um acúmulo de processos nas varas criminais e tribunais, comprometendo o funcionamento do sistema de justiça penal (LOPES, 2022, p. 95). Lopes também destaca que muitas condutas irrelevantes ou que poderiam ser resolvidas fora da esfera penal acabam gerando *notitia-criminis* desnecessárias, o que sobrecarrega o sistema.

Crespo (2011) observa que, em um contexto no qual leis penais são criadas frequentemente para atender a novas demandas, é preciso sensibilidade e cautela para avaliar a real necessidade de novas tipificações criminais. Ele argumenta que, diante dos desafios da Sociedade da Informação, é importante priorizar políticas sociais e soluções amigáveis por meio do direito civil e administrativo, deixando o direito penal como última alternativa (*ultima ratio*). Isso evita que o direito penal seja banalizado, reservando-o para situações em que outras formas de resolução não são eficazes.

A análise da eficácia das leis brasileiras no enfrentamento dos cibercrimes revela que, apesar de avanços legislativos, ainda há desafios significativos para garantir uma resposta penal adequada. A seguir, serão discutidas as principais dificuldades na persecução penal dos cibercrimes, incluindo os métodos investigativos e a colaboração entre as instituições responsáveis, que são essenciais para uma resposta eficaz a essa modalidade de crime.

CAPÍTULO III - PERSECUÇÃO PENAL

1. DESAFIOS NA INVESTIGAÇÃO E PUNIÇÃO DOS CRIMES CIBERNÉTICOS

No Brasil, a punição efetiva dos crimes cibernéticos enfrenta uma série de desafios, que vão desde a falta de recursos técnicos e legais até a necessidade de cooperação internacional. Conforme expresso na pesquisa desenvolvida, a punição efetiva desses crimes exige uma abordagem holística, que envolva capacitação, recursos, legislação adequada, cooperação internacional, conscientização e colaboração entre setores. Esse contexto demanda do Estado uma nova postura institucional para enfrentar a complexidade do ambiente digital (SALGADO, 2009, p. 7).

Somente por meio de ações conjuntas e do fortalecimento das estruturas existentes será possível combater a impunidade e proteger a sociedade dos crimes cibernéticos. Esses crimes, praticados no ambiente virtual, representam um desafio tanto para o direito penal quanto para os órgãos de investigação, exigindo a adaptação dos instrumentos jurídicos e o desenvolvimento de estratégias específicas para seu enfrentamento (SALGADO, 2009, p. 7).

Esses crimes abrangem uma ampla gama de atividades, e os principais desafios encontrados na investigação e punição dos crimes cibernéticos.

2. CAPACITAÇÃO E RECURSOS

A investigação de crimes virtuais exige conhecimentos técnicos especializados em informática e tecnologia da informação. Os profissionais envolvidos devem ser devidamente capacitados para lidar com as particularidades do ambiente digital, utilizando ferramentas apropriadas para a coleta e análise de evidências digitais. Esse processo demanda, ainda, um investimento contínuo em tecnologias, infraestrutura e ferramentas específicas que possam apoiar, de forma eficaz, as investigações.

Conforme Cassanti (2014, p. 26), “a luta contra os crimes virtuais não terá qualquer possibilidade de êxito se aqueles que tentam vencê-la não compreenderem primeiro a sua essência”. Destaca-se que é essencial que as pessoas conheçam o perigo, saibam identificar para não serem vítimas.

Uma das maiores problemáticas no tocante à punição dos crimes praticados em meio ambiente digital diz respeito às provas sobre a materialidade delitiva e aos indícios de autoria que fornecem o mínimo viabilidade (justa causa) à propositura de uma ação penal. Nesse sentido, os óbices encontrados ao longo da investigação criminal, bem como do eventual processo penal, vão desde a identificação de um possível autor e sua localização (identificar o IP – protocolo de Internet – que identifica a máquina de onde partiu a conduta – o que não significa, necessariamente, identificar o sujeito criminoso), passando pela validade e licitude das provas colhidas e, por fim, as dificuldades de rastreamento das condutas quando praticadas através da denominada deep web (FIORILLO, 2016, p. 68).

De acordo com Salgado (2009, p. 5), o primeiro passo para compreender o processo de investigação de crimes cibernéticos é estabelecer duas fases de investigação: a fase técnica e a fase de campo. Na fase técnica, são executadas e analisadas tarefas e informações com o objetivo principal de localizar o computador ou dispositivo utilizado para cometer o crime.

De acordo com Salgado:

Em suma, podemos citar dois. Primeiro, a identificação do criminoso a partir dos rastros deixados por ele na rede (quebra judicial de sigilo de dados telemáticos até se chegar ao local de onde partiu a conexão ligada à conduta ilícita, sendo, após uma prévia verificação, requerida a expedição de mandado de busca e apreensão para perícia no equipamento) e, por fim, a interceptação telemática de dados em tempo real (SALGADO, 2009, p. 5).

Após identificar e localizar o dispositivo usado para o acesso criminoso à internet, ocorre a chamada fase de campo. Nessa etapa, os agentes policiais deslocaram-se até o local para realizar diligências e obter um reconhecimento operacional mais detalhado.

3. CONSCIENTIZAÇÃO E EDUCAÇÃO.

A conscientização e a adoção de práticas de segurança online são fundamentais para navegar com segurança no mundo digital, a prevenção é a chave para uma experiência online segura e protegida. A educação para a segurança na internet é uma ferramenta essencial para capacitar os usuários a aproveitarem as oportunidades que o mundo digital oferece, ao mesmo tempo em que se protegem de seus riscos. “É necessário manter-se informado e atualizado, com cursos, palestras e artigos, pois a Internet está em constante mudança e atualização” (SALGADO, 2009, p. 10).

E é fundamental que os usuários estejam conscientes dos perigos e possam adotar medidas preventivas para se protegerem contra os crimes cibernéticos.

Sendo assim, fica evidente que a educação digital desempenha um papel crucial no combate os crimes cibernéticos. O Ministério Público, em parceria com o Governo, desempenha um papel central nesse esforço, trabalhando não apenas na repressão, mas também na conscientização da população como parte essencial da prevenção desses delitos (SALGADO, 2009, p. 4).

5. COLABORAÇÃO ENTRE SETORES

Segundo Salgado (2009, p. 6) uma parceria entre o governo, provedores de internet e empresas digitais é essencial para combater os cibercrimes de maneira eficaz. Uma abordagem colaborativa permite o desenvolvimento de políticas robustas e o fortalecimento das capacidades necessárias para enfrentar essa ameaça crescente. A criação de grupos de trabalho multidisciplinares, que compartilhem informações e experiências, é uma estratégia eficaz para formar equipes capazes de alcançar resultados de forma mais ágil e eficiente.

“Hoje possuímos todos os agentes envolvidos no combate à criminalidade cibernética, peritos e técnicos de informática, agentes policiais, delegados, membros do Ministério Público e até juízes, mais treinados e informados, entre outros fatores, graças aos cursos que buscamos desenvolver, trazendo inclusive profissionais treinados de outros países. Outro fator importante é a colaboração entre os órgãos, que vem se intensificando com o compartilhamento de técnicas e informações para o aperfeiçoamento de todos e com o trabalho em equipe, resultando em operações e forças-tarefas bem-sucedidas na área de combate aos crimes cibernéticos, com destaque para o combate à pornografia infantil pela rede [...]” (SALGADO, 2009, p. 6).

Desde modo, se torna indispensável a colaboração entre setores, o compartilhamento de informações e cruzamentos de dados entre os setores governamentais que podem contribuir para a investigação e identificação dos autores, sendo uma ferramenta plenamente indispensável. Diante do exposto, passamos a dissertar sobre a cooperação internacional.

6. COOPERAÇÃO INTERNACIONAL

A cooperação internacional, nos dias de hoje se tornou plenamente capaz através de convenções internacionais e cooperação entre países desenvolvidos e subdesenvolvidos, pois todos estão vulneráveis a cibercrimes. Portanto a possibilidade de rastreamento de autores dos delitos e prevenção é possível, mas ainda é um grande desafio para as autoridades.

Entre as possibilidades de cooperação temos: o pedido de assistência jurídica (trata-se do intercâmbio de informações entre países estrangeiros, consistentes na coleta de provas para investigações policiais ou instrução de processos judiciais em tramitação), dentre outras previstas na legislação vigente (p. ex., a carta rogatória) ou em tratados internacionais dos quais o Brasil faça parte (FIORILLO, 2016, p.97).

Cibercrimes frequentemente envolvem diversas jurisdições, o que dificulta a aplicação da lei devido às variações nas legislações de cada país estrangeiro, tornando a cooperação internacional indispensável e essencial para efetivação de sua eficácia, sua crescente complexidade e sofisticação tornou a cooperação necessária e fundamental para assegurar a eficácia das respostas legais e das ações policiais.

“Há casos em que se faz necessária a interceptação telemática, porém, ainda enfrentamos certas dificuldades na sua implementação devido à alegação de algumas empresas de apenas se submeterem, neste caso, à legislação do local de sua matriz, geralmente EUA, mesmo após deferimento de ordem judicial” (SALGADO, 2009, p. 4).

Contudo, apesar da convenção internacionalmente conhecida como “Convenção Budapeste” ter um objetivo de atingir a cooperação internacional entre os países, a adesão não obriga a nenhum país a aderir a lei de outro país. Apenas trás noções básicas de cooperação e orientações de como elaborar leis e agilidade com facilidade em compartilhamento rápido e eficiente de provas eletrônicas entre os países, de forma que todos os países que entre nesse tratado, tenha objetivos em comum de resolver conflitos jurisdicionais que atinjam o mundo virtual, pois os crimes virtuais que “desconhece os limites impostos por fronteiras” (FIORILLO, 2016, p. 7).

“A Convenção busca harmonizar elementos relativos ao Direito Penal substantivo dos países subscritores, bem como definir poderes e ações que facilitem a persecução penal, além de procurar estabelecer um regime rápido e eficaz de cooperação internacional” CRESPO (2011, p.31).

Segundo o coordenador-geral André Zaca Furquim, do Ministério da Justiça e Segurança Pública (MJSP, 2023), a expectativa é que essa convenção aumente o número de pedidos de cooperação jurídica internacional, uma vez que investigações no Brasil frequentemente precisam de acesso a provas eletrônicas localizadas em outros países. a implementação completa promulgada pelo Brasil, Decreto nº 11.491/2023, ajudará na modernização de políticas e regulamentos sobre cibercrimes, aprimorando a coleta e a preservação de provas digitais.

Segundo o Ministério da Justiça e Segurança Pública (2024), a ONU fez uma nova proposta de melhoria da convenção para ampliação de instrumentos utilizados na cooperação internacional sobre o combate aos cibercrimes.

O novo instrumento deverá servir também como base normativa aos países que não têm legislação nacional. O texto aprovado alerta que as nações estão preocupadas com a utilização de sistemas de tecnologias de informação e comunicação pelos criminosos e que isso impacta na rapidez de práticas de crimes como: organizado transnacional, terrorismo, contrabando de migrantes, produção ilícita armas de fogo, peças e munições e tráfico de pessoas, de drogas e de bens culturais. A proposta de convenção contra crimes cibernéticos inclui recursos para “aprimorar a cooperação internacional, os esforços de aplicação da lei, a assistência técnica e a capacitação” para o enfrentamento dos delitos (MJSP, 2024).

A busca por aprimorar a investigação criminal não é uma preocupação exclusiva do Brasil, mas uma prioridade global. Existe uma necessidade crescente de fortalecer as investigações de delitos virtuais para que esses crimes não permaneçam impunes, visto que o ambiente digital pode ser o ponto de partida para práticas criminosas de grande escala, muitas vezes inesperadas pela sociedade. Um exemplo é o uso de inteligência artificial, que pode ser empregada em diversos tipos de delitos, desde infrações menores até crimes hediondos e, potencialmente, crimes contra a humanidade.

Dessa forma, é de extrema importância que o Poder Legislativo e o Poder Judiciário invistam em projetos de lei e tecnologias avançadas, capazes de promover a cooperação internacional no combate aos cibercrimes, assegurando um ambiente virtual mais seguro e saudável para todos.

RESULTADOS

Os resultados obtidos neste estudo indicam que a legislação brasileira, embora tenha evoluído para incluir leis voltadas aos crimes digitais, ainda apresenta falhas na aplicação e efetividade quando confrontada com a complexidade dos cibercrimes.

A análise revelou que leis como o Marco Civil da Internet, a Lei Geral de Proteção de Dados (LGPD) e a Lei Carolina Dieckmann são avanços importantes para regulamentar o uso da internet e proteger os dados pessoais. No entanto, tais normas, na prática, ainda carecem de medidas eficientes de fiscalização e aplicação devido à limitada capacidade de investigação digital e à falta de recursos tecnológicos em diversos órgãos competentes.

A pesquisa destacou a importância da Convenção de Budapeste, um tratado internacional ao qual o Brasil aderiu com o intuito de facilitar a colaboração entre países na investigação e repressão aos cibercrimes. Ainda assim, as limitações para a colaboração efetiva com países que possuem legislações diferentes sobre privacidade e proteção de dados representam um obstáculo significativo, resultando em dificuldades na identificação e punição de criminosos cibernéticos.

Outro aspecto importante dos resultados foi a constatação de que a população brasileira ainda possui uma percepção limitada sobre os riscos do ambiente digital.

Entretanto, apesar das campanhas existentes, a pesquisa apontou uma carência de abordagens mais acessíveis e contínuas, que levem informação de qualidade a todas as camadas da sociedade, incluindo grupos mais vulneráveis, como crianças e idosos.

Em conclusão, os resultados da pesquisa ressaltam que, embora o Brasil tenha dado passos significativos no desenvolvimento de uma estrutura legal para combater cibercrimes, o sucesso dessas medidas ainda é limitado pela falta de recursos, de especialização das autoridades e da população, e pela necessidade de uma maior integração com o contexto internacional.

CONSIDERAÇÕES FINAIS

Os cibercrimes são uma ameaça crescente e presente no nosso cotidiano, e a verdade é que o sistema jurídico brasileiro ainda não está totalmente preparado para lidar com a complexidade e a velocidade com que esses crimes evoluem. Este trabalho demonstrou que, apesar de avanços como o Marco Civil da Internet, Lei Geral de Proteção de Dados e Lei de Cibercrimes, ainda há falhas significativas que dificultam o combate eficaz aos crimes digitais.

Para enfrentar esses desafios, o Brasil precisa investir mais em capacitação e tecnologia. Uma solução prática seria a criação de uma força-tarefa nacional dedicada exclusivamente à cibersegurança, com peritos qualificados e tecnologias avançadas para investigar e identificar criminosos digitais. Além disso, é essencial fortalecer a cooperação com outros países, especialmente aqueles que já possuem experiência consolidada no combate a esses crimes, permitindo que possamos agir sobre delitos que atravessam fronteiras e envolvem múltiplas jurisdições.

A conscientização também é fundamental. A sociedade precisa entender os riscos do ambiente digital e aprender a se proteger. Campanhas educativas, em escolas e empresas, podem ser um grande passo para ajudar a população a adotar práticas seguras e a identificar ameaças com mais facilidade.

Este trabalho reforça que a atualização constante da legislação, combinada com políticas de prevenção, educação digital e capacitação das autoridades, é essencial para que o Brasil enfrente os desafios dos cibercrimes de forma responsável e eficiente. Esse aprimoramento precisa contar com debates que envolvam especialistas em cibersegurança, profissionais do Direito e representantes da sociedade civil, com o objetivo de construir uma regulamentação que proteja os cidadãos e responda com agilidade às complexidades do mundo digital.

Espera-se que as análises e propostas apresentadas neste estudo possam contribuir para a formulação de políticas públicas mais robustas e eficazes. É responsabilidade do Estado, das instituições e da sociedade civil trabalharem juntos para garantir que o Brasil esteja preparado para enfrentar as ameaças do ciberespaço, promovendo a proteção e o bem-estar de cada cidadão no ambiente digital.

REFERÊNCIAS

ALBUQUERQUE, Roberto Chacon de. **A Criminalidade Informática**. São Paulo: Editora Juarez de Oliveira, 200.

BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silveira. **Manual de Investigação Cibernético à luz do Marco Civil da internet**. Rio de Janeiro: Bransport, 2016.

BRASIL. **Decreto nº 11.491, de 21 de setembro de 2023**. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11491.htm. Acesso em: 19 out. 2024.

BRASIL. Ministério da Justiça e Segurança Pública. **ONU aprova proposta que poderá reforçar o enfrentamento a crimes cibernéticos**. Agência Gov, 2024. Disponível em: <https://www.gov.br/mj/pt-br/assuntos/noticias/onu-aprova-proposta-que-podera-reforcar-o-enfrentamento-a-crimes-ciberneticos>. Acesso em: 25 de out. 2024.

BRASIL. Ministério da Justiça e Segurança Pública. **A Convenção de Budapeste é promulgada no Brasil**. Brasília: Ministério da Justiça e Segurança Pública, 2023. Disponível em: <https://www.gov.br/mj/pt-br/assuntos/noticias/convencao-de-budapeste-e-promulgada-no-brasil>. Acesso em: 2 nov. 2024.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, 5 de outubro de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acessado: 26 set. 2024

BRASIL. **DECRETO-LEI nº LEI Nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. [S. I.], 2012.

BRASIL. **LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012 nº LEI Nº 12.965, de 23 de abril de 2014**. Dispõe sobre Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. [S. I.], 2014.

BRASIL. **Lei nº 14.811, de 7 de janeiro de 2024**. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2024/lei/l14811.htm. Acesso em: 19 out. 2024.

CRESPO, Marcelo. **Algumas reflexões sobre o cyberstalking**. Disponível em: <https://canalcienciascriminais.com.br/algumas-reflexoes-sobre-o-cyberstalking/>. Acesso em: 25 out. 2024.

CRESPO, Marcelo Xavier de F. **Crimes digitais**. Rio de Janeiro: Saraiva Jur, 2011. E-book. p.34. Disponível em:

<https://integrada.minhabiblioteca.com.br/reader/books/9788502136663/>. Acesso em: 30 out. 2024.

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004, p. 110.

OLIVEIRA JÚNIOR, João Batista Caldeira de. **A Internet e os “novos” crimes virtuais**. 2001. Jus.com.br. Disponível em: <https://jus.com.br/artigos/2097/a-internet-e-os-novos-crimes-virtuais>. Acessado em: 09/10/2024.

SIMAS, Diana Viveiros de. **O cibercrime**. 2014. 168f. Dissertação (Mestrado em Ciências Jurídico Forenses). Universidade Lusófona de Humanidades e Tecnologias. Lisboa. 2014.

CASTELLS, Manuel. **Fim do Milênio**. 4. ed. Tradução de Klauss Brandini Gerhardt e Roneide Venancio Majer. São Paulo: Paz e Terra, 2007. (A Era da Informação: economia, sociedade e cultura; v. 3).

CARNEIRO, Adenele Garcia. **Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação**. 2012. Âmbito Jurídico. Disponível em: <https://ambitojuridico.com.br/edicoes/revista-99/crimes-virtuais-elementos-para-uma-reflexao-sobre-o-problema-na-tipificacao/#:~:text=Na%20d%C3%A9cada%20de%2070%20a,%C3%A0%20necessidade%20de%20se%20despender>. Acessado em: 09/10/2024.

VIANA, Marco Túlio apud CARNEIRO, Adenele Garcia. **Fundamentos de direito penal informático. Do acesso não autorizado a sistemas computacionais**. Rio de Janeiro: Forense, 2003. Disponível em: . Acessado em: 09/10/2024.

SALES, Fernando. **DIREITO DIGITAL: E AS RELAÇÕES JURÍDICAS PRIVADAS NA INTERNET**. 2ª. ed. Leme - São Paulo: MIZUNO, 2023.

SILVA, Rita de Cássia Lopes da. **Direito penal e sistema informático**, 2003. Disponível em: Acessado em: 09/10/2024.

FLOW. Táбата Amaral - **Corrida à Prefeitura de São Paulo 2024**. Entrevistada: Táбата Amaral. Entrevistador: Igor 3k. 27 set. 2024. Podcast. Disponível em: <https://www.youtube.com/watch?v=8fUBPX9Ez4I&t=0s>. Acesso em: 22 out. 2024.

SALGADO, Daniel de Resende. Pense antes de postar. **Revista Fato Típico, Goiânia**, ano I, n. 2, jul./set. 2009. Disponível em: <https://www.mpf.mp.br/go/institucional/publicacoes/fato-tipico/fato-tipico-nr-2.pdf>. Acesso em: 23 out. 2024.

PINHEIRO, Bruno Victor Arruda. **As novas disposições sobre os crimes cibernéticos: uma análise acerca das leis 14.132 e 14.155/2021**. Revista Jus Navigandi, Teresina, ano 27, n. 6899, 22 mai. 2022. Disponível em: <https://jus.com.br/artigos/98006>. Acesso em: 22 out. 2024.

CASSANTI, Moisés de Oliveira. **Crimes virtuais, vítimas reais**. Rio de Janeiro: Brasport, 2014. TEIXEIRA, T. Direito Digital e Processo Eletrônico. 7. ed. São Paulo: Saraiva, 2023. E-book.

SIQUEIRA, Marcela Scheuer et al. **Crimes virtuais e a legislação brasileira**. (Re)Pensando o Direito – Rev. do Curso de Graduação em Direito da Faculdade CNEC Santo Ângelo. v. 7, n. 13 (2017).

OLIVEIRA, Anderson Soares Furtado. **Crime por Meios Eletrônicos**. Brasília: Universidade Gama Filho, 2009.

ROVER, Aires José. **Crimes de informática**. <Disponível em: <http://www.infojur.ufsc.br/aires/arquivos/CRIMES%20DE%20INFORMATICA%20public.pdf>>. Acesso em 30 de outubro de 2024.

LIMA, Rogério Montai. **Guia Prático da Sentença Penal condenatória e Roteiro Para o Procedimento no Tribunal do Júri**. Rio de Janeiro: Editora Método, 2013, p. 25.

FIORILLO, Celso Antônio P.; CONTE, Christiany P. **Crimes no meio ambiente digital**. 2ª edição. Rio de Janeiro: Saraiva Jur, 2016. E-book. pág.97. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788547204198/>. Acesso em: 02 nov. 2024.