UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS
FACULDADE DE DIREITO

CRIMES VIRTUAIS E OS DESAFIOS LEGAIS DO ENFRENATMENTO NO BRASIL

CAROLINA MOURA PESTANA

RIO DE JANEIRO
2024

CAROLINA MOURA PESTANA

CRIMES VIRTUAIS E OS DESAFIOS LEGAIS DO ENFRENATMENTO NO BRASIL

Projeto de Monografia apresentado à Faculdade de Direito da Universidade Federal do Rio de Janeiro, como requisito parcial para obtenção do título de Bacharel em Direito.

Orientador: Nilo César Martins Pompílio da Hora

RIO DE JANEIRO

2024

CAROLINA MOURA PESTANA

CRIMES VIRTUAIS E OS DESAFIOS LEGAIS DO ENFRENATMENTO NO BRASIL

Projeto de Monografia apresentado à Faculdade de Direito da Universidade Federal do Rio de Janeiro, como requisito parcial para obtenção do título de Bacharel em Direito, sob orientação do **Professor Dr. Nilo Cesar Martins Pompílio da Hora**.

Data da Aprovação:__/__/____.

Banca Examinadora:

_____
Orientador

_____
Membro da Banca

_____
Membro da Banca

RIO DE JANEIRO

2024

CIP - Catalogação na Publicação

P292c

Pestana, Carolina Moura
Crimes virtuais e os desafios legais do enfrentamento no Brasil / Carolina Moura Pestana. - Rio de Janeiro, 2024.
42 f.

Orientador: Nilo Cesar Martins Pompílio da Hora.
Trabalho de conclusão de curso (graduação) - Universidade Federal do Rio de Janeiro, Faculdade Nacional de Direito, Bacharel em Direito, 2024.

1. Crimes Virtuais. 2. Legislação. 3. Enfrentamento. 4. Internet. I. Pompílio da Hora, Nilo Cesar Martins , orient. II. Título.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a), sob a responsabilidade de Miguel Romeu Amorim Neto - CRB-7/6283.

RESUMO

A análise dos crimes cibernéticos é importante, considerando a internet como um meio eficaz de comunicação que oferece novas perspectivas para o Direito Penal. O presente trabalho abordar os crimes virtuais no context atual, bem como sua difícil definição e tipificação. A lém disso, o foco da pesquisa é entender as condições de investigação policial relacionadas a esses delitos, apresentar a legislação vigente e levanter os desafios para o enfrentamento do tema. Para isso, foi utilizada uma metodologia de pesquisa bibliográfica de caráter exploratório, com base no método dedutivo. O objetivo não é esgotar o tema, mas sim estimular novas discussões para estudos futuros.

Palavras-chaves: crimes; internet; leis; enfrentamento;

ABSTRACT

The analysis of cybercrimes is important, considering the internet as an effective means of communication that offers new perspectives for Criminal Law. This study addresses virtual crimes in the current context, as well as their difficult definition and classification. Furthermore, the focus of the research is to understand the conditions of police investigation related to these offenses, present the current legislation, and highlight the challenges in addressing the issue. To achieve this, an exploratory bibliographic research methodology was used, based on the deductive method. The aim is not to exhaust the topic but to stimulate new discussions for future studies.

Keywords: crimes; internet; laws; confrontation;

Sumário

Lista de Figuras

INTRODUÇÃO

Este trabalho aborda a problemática dos crimes virtuais e os desafios legais enfrentados no Brasil. Com o avanço acelerado da tecnologia, os ataques cibernéticos, as fraudes online e os crimes de ódio emergiram como uma ameaça significativa e crescente, afetando não apenas indivíduos, mas também empresas e instituições de diversas naturezas. A análise deste tema se revela de extrema importância, uma vez que permite compreender a complexidade desses delitos, suas motivações, métodos e impactos. Além disso, é crucial para a elaboração de políticas públicas e estratégias de segurança que busquem soluções eficazes e inovadoras para combater essas atividades ilícitas. Assim, o estudo dos crimes virtuais não se limita a um aspecto jurídico, mas se expande para questões sociais, econômicas e tecnológicas, demandando uma abordagem multidisciplinar que envolva colaboração entre governos, setor privado e a sociedade civil.

Além disso, é fundamental ressaltar também a urgência de um enfrentamento eficaz dessas práticas delituosas por meio da utilização de instrumentos legais adequados. Este trabalho tem como propósito fornecer uma visão geral abrangente do cenário de crimes cibernéticos no Brasil. Para tal, será abordada a importância da legislação vigente, a qual deve ser aprimorada constantemente para se adaptar aos constantes avanços tecnológicos e às novas formas de criminalidade virtual. A cooperação internacional também será uma temática central, visto que os crimes virtuais não se limitam a fronteiras geográficas, tornando-se vital a atuação conjunta de diferentes países para combater efetivamente essa problemática. Nesse sentido, será abordada a importância dos acordos bilaterais e multilaterais entre as nações, assim como a necessidade de compartilhamento de informações entre as autoridades competentes, a fim de viabilizar investigações e processos eficientes. Ademais, serão discutidos aspectos técnicos e procedimentais relevantes, com destaque para a atuação das polícias especializadas e a necessidade de capacitação constante dos agentes públicos envolvidos nesse contexto.

Por fim, ressalta-se que a compreensão e o enfrentamento adequados dos crimes virtuais são fundamentais não apenas para garantir a segurança da sociedade, mas também para assegurar o respeito aos direitos individuais dos cidadãos em um contexto digital cada vez mais complexo. À medida que as interações online se tornam uma parte intrínseca do cotidiano, a proteção contra abusos e fraudes se torna uma prioridade inadiável. Através deste estudo aprofundado, busca-se

fornecer uma base sólida que não só elucide a natureza e a extensão dos crimes virtuais, mas também identifique lacunas nas legislações existentes e proponha inovações necessárias. Espera-se, assim, contribuir para o desenvolvimento de estratégias eficazes no combate a essa modalidade delitiva, promovendo a colaboração entre diferentes setores da sociedade, incluindo governos, instituições educacionais e o setor privado. O objetivo final é viabilizar a construção de um ambiente virtual mais seguro e confiável, onde os direitos dos cidadãos sejam respeitados e protegidos, possibilitando que todos possam usufruir das vantagens da tecnologia sem receios ou vulnerabilidades.

CAPÍTULO I – CRIMES VIRTUAIS

I.1. Definição teórica e legal

"A tecnologia move o mundo" é uma frase do empresário e inventor Steve Jobs, que se refere ao impacto que a tecnologia tem na sociedade. A tecnologia tem moldado a forma como as pessoas vivem, se comunicam e se relacionam. A evolução tecnológica tem influenciado a medicina, a educação, o trabalho e a comunicação. Por consequência também vem moldando as diferentes formas de execução de práticas delituosas e vulnerabilidade das vítimas de crimes.

Uma pesquisa do Estado de Minas Gerais indica que 71% dos brasileiros já foram vítimas de golpes virtuais, sendo o Brasil, o segundo maior alvo de crimes cibernéticos na América Latina. Em 2022, o país sofreu 3.879.869 ataques digitais de identidade.

Os crimes virtuais são aqueles que ocorrem no ambiente digital, como crimes cibernéticos, fraudes eletrônicas e invasões de sistemas. Eles podem ser classificados em diversas categorias, como roubo de identidade, *phishing*, *malware* e ataques de negação de serviço. A legislação brasileira relacionada aos crimes virtuais está em constante evolução para acompanhar o avanço tecnológico e os desafios que surgem nesse contexto. Além disso, existem tratados e convenções internacionais, como a Convenção de Budapeste, que visam a cooperação entre países no combate aos crimes cibernéticos. Os impactos sociais e econômicos dos crimes virtuais são significativos, incluindo prejuízos financeiros, danos à reputação das vítimas e desconfiança no ambiente online.

O jurista e especialista em Direito Digital, Sérgio G. G. N. B. Carvalho, conceitua crimes virtuais:

> "aqueles que são cometidos por meio da internet ou de dispositivos eletrônicos, envolvendo ações ilícitas que podem incluir fraudes, invasões de sistemas, e disseminação de conteúdos ilícitos."

Tulio Lima Vianna, categoriza os crimes cibernéticos em 4 tipos: crimes cibernéticos próprios, impróprios, mistos e mediato ou indireto.

> Aos delitos em que o computador foi o instrumento para a execução do crime, mas não houve ofensa ao bem jurídico inviolabilidade da informação automatizada (dados) denominaremos Delitos Informáticos Impróprios e àqueles em que o bem jurídico afetado

> foi a inviolabilidade dos dados, chamaremos de Delitos Informáticos Próprios (VIANNA, 2001, p.36).

Os crimes cibernéticos próprios acontecem somente online. Eles estão descritos detalhadamente no Código Penal. Abrangem atos como a inserção de dados falsos em sistemas e a invasão de dispositivo informático. Também é vital discutir como se proteger online para evitar ataques futuros.

A inserção de dados falsos compromete a confiabilidade das informações online, resultando em significativos prejuízos. Esse tipo de crime, descrito no artigo 313-A do Código Penal, evidencia a facilidade com que dados podem ser alterados na ausência de boas medidas de segurança. Da mesma forma, a invasão de dispositivo informático, conforme estabelecido na Lei "Carolina Dieckmann" (art. 154-A do Código Penal), ocorre quando alguém acessa um aparelho sem autorização, visando obter ou destruir dados de forma ilegal. Essa situação ressalta a importância de proteger adequadamente nossos dispositivos eletrônicos.

Já os crimes cibernéticos impróprios são aqueles que são tipificados, no Código Penal, pois violam bens jurídicos comuns, contudo, usam o meio digital como animus operandi.

Finalmente, vale trazer os conceitos de crimes cibernéticos Misto e Mediato ou Indireto, segundo Tulio Lima Vianna.

> Aos delitos complexos em que, além da proteção da inviolabilidade dos dados, a norma visar a tutela de bem jurídico diverso, denominaremos Delitos Informáticos Mistos. Por fim, nos casos em que um Delito Informático Próprio é praticado como crime-meio para a realização de um crime-fim não informático, este acaba por receber daguele a característica de informático, razão pela qual O denominaremos de Delito Informático Mediato ou Indireto.(VIANNA, 2001, p. 37)

Os delitos informáticos mistos são aqueles que envolvem a proteção da inviolabilidade dos dados, mas também visam tutelar um bem jurídico de natureza diferente. Esses crimes, resultantes do acesso não autorizado a sistemas computacionais, adquiriram a classificação de "sui generis" devido à relevância do bem jurídico protegido, que vai além da simples inviolabilidade dos dados. Por outro lado, os delitos informáticos mediatos ou indiretos são crimes não informáticos que se tornam possíveis por meio de um delito informático que serve como meio para sua realização.

Em contrapartida, os Delegados de Polícia Emerson Wendt e Higor Vinicius Nogueira Jorge, na expectativa de contribuir para a segurança virtual do Brasil, lançaram uma obra onde dividiram crimes cibernéticos como exclusivos e abertos.

> Os crimes cibernéticos exclusivos são aqueles que dependem do meio computacional para serem cometidos, como ocorre nos casos de invasão de dispositivo informático, previstos nos artigos 154-A e 154-B do Código Penal Brasileiro. Por outro lado, os crimes cibernéticos abertos podem ser realizados tanto no ambiente virtual quanto fora dele, como as violações de direitos autorais e o estelionato (WENDT, JORGE, 2012, p. 19).

Ainda no mérito de categorias e definições, Marco Aurélio Rodrigues da Costa, divide os crimes de informática entre puros, mistos e comuns.

> O crime informático puro é o que se encontra relacionado ao sistema de informática, isto é, o sujeito ativo pretende apenas corromper os dados do computador do sujeito passivo, tais como o "software" e o "hardware "e, assim, é percebido nos vírus que contaminam um computador, por exemplo. Já o crime de informática misto, diz respeito à violação do bem jurídico diferente do sistema, porém este é instrumento inerente à consumação do delito, como ocorre no caso do furto eletrônico a contas bancárias online. E, por último, o crime informático comum é aquele que está previsto na lei penal e pode ou não ocorrer com o uso do computador, a exemplo da pedofilia, do racismo e do cyberbullying. (COSTA, 1995)

Segundo Marco Aurélio Rodrigues, os conceitos e a sistematização do Direito Penal informático Brasileiro se encontra em estado "in vitro". Portanto os autores não buscam esgotá-lo ao publicar obras, mas sim contribuir para a evolução do assunto.

> Um dos temas mais difíceis entre os doutrinadores do Direito Penal de Informática é a conceituação e denominação. O conceito vem, em muitas oportunidades, de forma restritiva ou por demais abrangente. Não reflete as muitas situações em que se enquadram os crimes de informática. A denominação é, também, motivo de grande polêmica entre os estudiosos do Direito Penal de Informática, pois a cada denominação segue-se um conceito e, vice e versa. É, pois importante que se busque dissecar tais polêmicas. (COSTA, 1995)

Embora diversos autores façam diferentes conceituações e nomeclaturas sobre crimes virtuais, o objetivo aqui é demonstrar que os crimes virtuais possuem os mesmos requisitos e tipificações que os crimes cometidos fora de meios informáticos, estando ambos tipificados no código penal.

I. 2. Espécies de crimes virtuais

Os crimes virtuais são atos ilegais no ambiente digital, como fraudes, invasão de privacidade, roubo de identidade, difamação virtual, pirataria digital, vazamento de dados pessoais, etc. Eles podem ser classificados em várias categorias, como crimes de informática, pornografia infantil, ciberterrorismo, *cyberbullying*, estelionato, falsificação de documentos, lavagem de dinheiro virtual, etc. Cada tipo apresenta características distintas e diferentes impactos na sociedade. É importante destacar que, segundo Rossini, os crimes cometidos por meio de um computador, mesmo quando não conectado à internet, também são classificados como crimes virtuais.

O combate a esses crimes requer medidas de segurança digital, conscientização da população e cooperação internacional. É fundamental que governos, empresas e usuários estejam atualizados e capacitados para garantir a proteção e a privacidade de todos. Uma abordagem colaborativa permitirá criar um ambiente virtual seguro e confiável.

Os crimes virtuais são uma categoria crescente de delitos, abrangendo diversas atividades ilícitas realizadas por meio da internet ou de dispositivos digitais.

I.2.1 Invasão de dispositivo informático

Sendo caracterizado por acesso não autorizado a computadores, smartphones ou redes, a invasão de dispositivo informático é um crime previsto no artigo 154-A do Código Penal brasileiro, na Lei 12.737/2012, também conhecida como Lei Carolina Dieckmann. A lei estabelece que a pena para este crime é de reclusão de 1 a 4 anos e multa. Muitos juristas criticam essa lei pelo uso do termo dispositivo informático, em vez de dispositivo eletrônico, que seria mais abrangente. Outra critica tecida ao texto da Lei é a ausência de definição de termos técnicos e a ínfima quantidade de pena aplicada, categorizando o crime como baixo potencial ofensivo.

I.2.2 Fraude eletrônica

Envolvem enganar indivíduos ou instituições para obter benefícios financeiros, como

clonagem de cartões de crédito. Esse crime pode ser cometido por meio de diversas técnicas, como: roubo de identidade, esquemas de pirâmide, anúncios fraudulentos em redes sociais, contatos telefônicos fraudulentos, envio de correio eletrônico fraudulento.

A Lei 14.155/2021 introduziu o delito de fraude eletrônica no artigo 171, §2º-A do Código Penal. A pena para este crime é de reclusão de 4 a 8 anos e multa. Além disso, essa lei também prevê uma causa de aumento de pena de um a dois terços, caso o crime seja praticado por meio de um servidor mantido fora do território nacional.

Em sua doutrina, Rogério Greco entende no seguinte sentido:

> Desde que surgiram as relações sociais, o homem se vale da fraude para dissimular seus verdadeiros sentimentos e intenções para, de alguma forma, ocultar ou falsear a verdade, a fim de obter vantagens que, em tese, lhe seriam indevidas. (GRECO, 2014, p. 236)

Se antes os crimes todos os crimes de fraude com vantagem financeira eram tipificados como crime de estelionato, o parágrafo 2º veio com o objetivo de especificar quando as fraudes forem cometidas por meios eletrônicos ou digitais.

I.2.3 *Ransomware*

O crime de *ransomware* é uma forma de ataque cibernético em que o invasor sequestra os dados de uma vítima, geralmente por meio de criptografia, e exige um resgate para liberá-los. Nesse tipo de crime, o malware é instalado em um dispositivo, criptografando os arquivos do usuário e tornando-os inacessíveis. Após a infecção, o criminoso exibe uma mensagem exigindo pagamento, frequentemente em criptomoedas, para fornecer a chave de descriptografia. Apesar de ser popularmente conhecido como “sequestro de dados”, o crime de *Ransomware* é tipificado como extorsão (Art. 159 do CP), visto que o crime de sequestro o objeto só poderia ser um indivíduo. Já que se trata de crime formal, é considerado crime mesmo que não seja efetuado pagamento por parte da vítima.

I.2.4 Violação de direitos autorais

A violação de direitos autorais é um crime previsto no artigo 184 do Código Penal Brasileiro. A pena para esse crime pode variar de detenção de 3 meses a 1 ano ou multa, dependendo se o autor possui intuito de lucro ou não com a conduta.

Regulamentada pela Lei nº 9.610, de 19 de fevereiro de 1998, a violação de direitos autorais é caracterizada por infringir os direitos do autor ou os relacionados a ele, por exemplo: falsificações, produtos piratas, reprodução de obras ou produtos sem autorização, oferta de produtos copiados por sistemas remotos ou via cabos.

I.2.5 Pornografia infantil

Os artigos 240 e 241 do Estatuto da Criança e do Adolescente abordam a produção e a comercialização de material pornográfico. É tipificada a publicação ou divulgação de fotos ou vídeos envolvendo crianças e adolescentes, inclusive através de meios de comunicação como a internet. Aqueles que armazenam esse tipo de material em sites ou em seus computadores também cometem o mesmo crime. Para a caracterização da infração, não é relevante se usuários tiveram acesso ao conteúdo; basta que o material pornográfico exista. (BRASIL, 1990)

I.2.6 Estupro virtual

Práticas de violência sexual realizadas por meio de plataformas digitais, como redes sociais, aplicativos de mensagens ou ambientes online. Essa forma de violência pode envolver coerção, manipulação ou assédio sexual, utilizando imagens, vídeos ou mensagens para ameaçar ou intimidar a vítima. Atualmente, tramita o Projeto de Lei 3628/2020 na Comissão de Constituição e Justiça e de Cidadania, que propõe o aumento das penas do crime de estupro de vulnerável e tipifica a conduta de estupro virtual de vulnerável. Esse mesmo projeto, também propõe alterar o Código Penal e o Estatuto da Criança e do Adolescente, para aumentar as penas dos crimes de estupro de vulneráveis e de aliciamento de menores para fins sexuais. (CAMARA.LEG.BR)

CAPÍTULO II - LEGISLAÇÃO BRASILEIRA

A legislação brasileira relacionada aos crimes virtuais é abordada por diversas leis, com destaque para o Código Penal, que prevê punições para crimes como invasão de dispositivo informático e difusão de vírus e o Marco Civil da Internet estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Além disso, no âmbito internacional, o país é signatário de tratados e convenções que visam à cooperação entre nações para o combate a crimes cibernéticos, como, por exemplo, a Convenção de Budapeste. A harmonização entre legislações nacionais e a cooperação internacional são fundamentais para enfrentar a complexidade dos crimes virtuais no contexto global.

II.1 Crimes virtuais no Código Penal

No Código Penal Brasileiro, os artigos 154-A, 154-B, 266 e 298 são responsáveis por legislar sobre os temas que tratam de condutas criminosas relacionadas à invasão de dispositivos informáticos, interrupção de serviços de comunicação e falsificação de documentos, refletindo a necessidade de uma legislação adaptada às novas realidades digitais.

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
>
> Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa.
> 1o Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
>
> 2o Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
>
> 3o Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
>
> Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
>
> 4o Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
>
> 5o Aumenta-se a pena de um terço à metade se o crime for praticado contra:
>
> I – Presidente da República, governadores e prefeitos;
>
> II – Presidente do Supremo Tribunal Federal;

> III – Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
>
> IV – dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.
>
> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.
>
> Art. 266 – Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:
> Pena – detenção, de um a três anos, e multa.
>
> 1o Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.
>
> 2o Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.

O artigo 298 do Código Penal aborda a falsificação de documentos particulares, incluindo a alteração de cartões de crédito ou débito, com penas que variam de um a cinco anos de reclusão. Essa tipificação é essencial para coibir fraudes que afetam a segurança financeira dos cidadãos.

> Art. 298 – Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro:
> Pena – reclusão, de um a cinco anos, e multa.
>
> Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito.

É importante destacar a recente tipificação do crime de fraude eletrônica, realizada em 2021, que adicionou o § 2º-A ao artigo 171 do Código Penal Brasileiro. Esse parágrafo aborda especificamente os casos em que a fraude é cometida utilizando informações fornecidas pela vítima ou por terceiros induzidos a erro através de redes sociais, chamadas telefônicas, e-mails fraudulentos ou outros meios semelhantes.

Além disso, também temos no Código Penal crimes tradicionais que podem ser cometidos tanto dentro como fora de dispositivo informático, por exemplo: crimes contra a honra (arts. 138, 139 e 140 do CP); crime de ameaça (art. 147 do CP); extorsão (art. 158 do CP); extorsão indireta (art. 160 do CP); escárnio por motivo de religião (art. 208 do CP); favorecimento da prostituição (art. 228 do CP); ato obsceno (art. 233 do CP); incitação ao crime (art. 286 do CP); apologia de

crime ou criminoso (art. 287 do CP); Apropriação indébita (art. 168 do CP); Estelionato (art. 171 do CP); Violação de direito autoral (art. 184 do CP).

II.2. Marco Civil da internet

A Lei nº 12.965/2014, também conhecida como Marco Civil da Internet, é a principal legislação que regulamenta o uso da internet no Brasil. Ele estabelece princípios, garantias, direitos e deveres para todos os usuários da rede, além de definir regras detalhadas para a atuação do Estado, das empresas e dos cidadãos na era digital. No contexto dos crimes virtuais e da segurança cibernética, o Marco Civil da Internet desempenha um papel fundamental, pois estabelece a neutralidade de rede como uma salvaguarda essencial para a transmissão de dados e informações de forma justa e imparcial. Além disso, a lei prevê a proteção da privacidade dos usuários, reforçando a importância do consentimento informado e do respeito aos direitos individuais no ambiente online.

Instituído pela Lei nº 12.965/2014, é um marco fundamental na regulamentação do uso da internet no Brasil e desempenha um papel significativo no combate aos crimes cibernéticos como por exemplo:

a) **Estabelecimento de Princípios e Direitos**: o Marco Civil consagra direitos e garantias fundamentais dos usuários da internet, como a liberdade de expressão, a privacidade e a proteção de dados pessoais. Isso proporciona uma base legal que permite aos usuários reivindicar seus direitos em caso de abusos, como invasões de privacidade e uso indevido de informações.
b) **Responsabilidade dos Provedores**: a lei estabelece a responsabilidade dos provedores de serviços de internet em relação ao conteúdo gerado por terceiros. Isso significa que os provedores devem agir de forma diligente na remoção de conteúdos que violem a lei, facilitando a identificação e a punição de práticas ilícitas, como a disseminação de conteúdos difamatórios ou prejudiciais.
c) **Proteção de Dados Pessoais**: o Marco Civil traz diretrizes para a coleta e o tratamento de dados pessoais, exigindo o consentimento explícito dos usuários. Isso é crucial para evitar abusos e garantir que informações pessoais não sejam utilizadas de forma inadequada, reduzindo o risco de crimes como roubo de identidade e fraudes.

d) **Cooperação com Autoridades**: a lei prevê mecanismos de colaboração entre provedores e autoridades policiais na investigação de crimes cibernéticos. Isso facilita a coleta de provas e a responsabilização dos infratores, permitindo uma resposta mais eficaz às práticas ilícitas.

O Marco Civil incentiva práticas de segurança da informação, promovendo a adoção de medidas para proteger dados e sistemas. Isso contribui para um ambiente digital mais seguro e resiliente contra ataques cibernéticos.

A lei também destaca a importância da educação digital, incentivando a conscientização sobre segurança online e boas práticas na utilização da internet, o que é essencial para prevenir crimes cibernéticos.

Em suma, o Marco Civil da Internet é uma ferramenta essencial no combate aos crimes cibernéticos no Brasil. Ao estabelecer direitos, responsabilidades e diretrizes claras, a lei não apenas protege os usuários, mas também cria um ambiente mais seguro e confiável para a navegação online. Sua implementação e efetividade são fundamentais para enfrentar os desafios da criminalidade digital de forma eficaz.

II.3. A lei nº 12.735/2012

A Lei nº 12.735/2012, sancionada em 30 de novembro de 2012, introduziu alterações significativas no Código Penal Brasileiro e no Código de Processo Penal, focando na tipificação de crimes cometidos por meio da internet. O principal objetivo dessa legislação é coibir a prática de delitos cibernéticos. A Lei nº 12.735/2012, também conhecida como Lei Azeredo, tipifica condutas criminosas realizadas por meio de sistemas eletrônicos ou digitais contra sistemas informatizados. Essa legislação altera o Código Penal, o Código Penal Militar e a Lei de Combate ao Racismo, incluindo disposições que obrigam a remoção imediata de mensagens racistas da internet. A criação da Lei 12.735/2012 surgiu como uma medida de emergência para preencher uma lacuna na legislação, refletindo a necessidade de um arcabouço jurídico mais robusto para enfrentar crimes cibernéticos e proteger os direitos dos cidadãos na era digital.

> Art. 4º Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.

Além do artigo que visa combater os crimes informáticos por meio de criação de setores especializados a referida lei também estabelece meios de combate para discursos racistas online, ao acrescentar o inciso II no parágrafo 3º do artigo 20 da Lei nº 7.716, que tipifica condutas racistas e discriminatórias praticas por meios informáticos.

> Art. 5º O inciso II do § 3º do art. 20 da Lei nº 7.716, de 5 de janeiro de 1989 , passa a vigorar com a seguinte redação:
>
> "Art. 20. .....
>
> .....
>
> § 3º .....
>
> .....
>
> II - a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio;

A Lei nº 12.735/2012 é um avanço na legislação brasileira sobre crimes virtuais, refletindo a necessidade de adaptação do sistema jurídico às realidades da era digital. A lei busca garantir a segurança e a privacidade dos usuários na internet, promovendo um ambiente online mais seguro.

Essa legislação é parte de um conjunto mais amplo de normas que buscam enfrentar os desafios impostos pela tecnologia e, somada a outras leis, contribui para a construção de um arcabouço jurídico mais robusto no combate à criminalidade cibernética no Brasil.

II.4. A lei nº 12.737/2012

A Lei nº 12.737/2012, também conhecida como "Lei Carolina Dieckmann", foi sancionada em 30 de novembro de 2012 e é um marco importante na legislação brasileira voltada para a proteção contra crimes cibernéticos. A lei recebeu esse nome em referência à atriz Carolina Dieckmann, cuja privacidade foi violada após o vazamento de fotos íntimas, trazendo à tona a discussão sobre a segurança digital e a privacidade na internet.

A Lei nº 12.737/2012 estabelece a tipificação criminal de delitos informáticos, alterando

o Código Penal para incluir novos artigos. O Art. 154-A tipifica a invasão de dispositivo informático, definindo como crime a violação de mecanismos de segurança para obter, alterar ou destruir dados sem autorização. A pena para essa infração varia de 3 meses a 1 ano de detenção, podendo ser aumentada em caso de prejuízo econômico ou se a invasão resultar na obtenção de informações sigilosas, que pode levar a uma pena de reclusão de 6 meses a 2 anos.

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita. (BRASIL, 1940)

O artigo 154-B do Código Penal, pós alteração da Lei 12.735/2012, determina que a ação penal para os crimes do artigo 154-A somente pode ser iniciada mediante representação, exceto nos casos em que o crime é cometido contra a administração pública ou concessionárias de serviços públicos. Além disso, a lei altera os artigos 266 e 298 do Código Penal, acrescentando penalidades para a interrupção de serviços telegráficos, telefônicos e informáticos, e equiparando cartões de crédito e débito a documentos particulares em casos de falsificação.

> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos. (BRASIL, 1940)

Adentrando em sua relevância, a Lei nº 12.737/2012 é crucial em um contexto onde a tecnologia permeia todos os aspectos da vida cotidiana. Ela reconhece e aborda os desafios relacionados à privacidade e à segurança na era digital, criando um arcabouço legal que busca proteger os cidadãos contra abusos e violações.

Além de suas implicações legais, a lei serve como um alerta sobre a importância da proteção da informação pessoal e a necessidade de uma cultura de respeito à privacidade, destacando a responsabilidade dos usuários e das empresas em manter um ambiente digital seguro.

II.5. Legislação de proteção à criança e adolescente contra crimes virtuais

Com relação ao crime cibernético de pornografia infantil, o Estatuto da Criança e do Adolescente (ECA) conta com o artigo 241 para tratar com rigor os crimes nesse âmbito.

> Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: (Incluído pela Lei nº 11.829, de 2008)
>
> Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa. (Incluído pela Lei nº 11.829, de 2008)
>
> § 1 º Nas mesmas penas incorre quem: (Incluído pela Lei nº 11.829, de 2008)
>
> I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo; (Incluído pela Lei nº 11.829, de 2008)
>
> II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo. (Incluído pela Lei nº 11.829, de 2008)
>
> Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: (Incluído pela Lei nº 11.829, de 2008)
>
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. (Incluído pela Lei nº 11.829, de 2008)

Ao analisarmos o artigo, é possível perceber a preocupação do legislador em responsabilizar também a plataforma digital ou rede social na qual os conteúdos criminosos estariam disponibilizados em caso de omissão na cooperação investigativa ou exclusão do conteúdo.

Somado ao ECA, a Lei Nº 13.185, de 2015, aborda de forma eficaz a questão do bullying na internet, reconhecendo a necessidade de proteção e prevenção desse fenômeno, especialmente no ambiente digital. Essa legislação estabelece diretrizes para a criação de políticas públicas voltadas à promoção de um ambiente seguro e saudável nas relações entre crianças e adolescentes.

A lei define o bullying como "a prática de violência física ou psicológica, intencional e repetitiva, que ocorre sem a provocação do ofendido". Nesse contexto, a legislação também enfatiza a importância de ações educativas que promovam a conscientização sobre os efeitos negativos do bullying, buscando prevenir e combater suas manifestações, inclusive nas redes sociais.

Além disso, a lei determina a criação de programas de formação para educadores, familiares e a comunidade, visando a identificação e enfrentamento do bullying, assim como a

proteção das vítimas. Com isso, a Lei Nº 13.185 representa um avanço significativo no combate ao bullying, reconhecendo as particularidades do ambiente virtual e a necessidade de uma abordagem integrada para a sua prevenção.

II.6. Lei 14.132/2021 e Lei 14.811/2024

A legislação brasileira tem avançado para se adequar às novas formas de interação que a tecnologia oferece. As redes sociais se tornaram extremamente populares, facilitando e aproximando as relações interpessoais. O contato entre as pessoas nunca foi tão acessível, permitindo interações de praticamente qualquer lugar e possibilitando acompanhar a rotina de outros. Nesse contexto, destaca-se a Lei 14.132/2021, que criminalizou uma das condutas mais relevantes nas redes: o cyberstalking. Antes de nos debruçarmos sobre o cyberstalking e seu conceito, é necessário compreender ao conceito da mesma conduta, porém no meio físico, denominada como stalking.

Stalking é um termo em inglês derivado do verbo "*to stalk*", que significa perseguir, vigiar ou espionar. As motivações para essa prática podem ser variadas, sendo uma das mais comuns, por exemplo, o término de um relacionamento amoroso, em que uma das partes não aceita a decisão da outra e começa a violar sua integridade, inicialmente de forma psicológica, geralmente de maneira repetitiva e insistente. Isso pode evoluir para situações mais graves, como ameaças à integridade física ou até à vida da pessoa.

Assim, surge então o conceito de cyberstalking, trazendo uma adaptação da conduta anteriormente conhecida para o mundo virtual. No cyberstalking, o agente utiliza dos meios virtuais para perturbar a vítima de forma indesejável. Segundo Auriney Brito (2013):

> [...] a exemplo do que ocorreu com o bullying, o stalking ganhou uma ferramenta que facilitou o serviço do perseguidor (stalker), e potencializou os danos causados às vítimas. Emails, tweets, visitas de perfil e até as famosas “cutucadas” podem servir de exemplos de novos meios de execução proporcionados pelo uso da internet, passando com isso a denominar-se Cyberstalking. (BRITO, 2013, p. 84)

Nesse contexto, em 2021, a Lei 14.132 modificou o Código Penal Brasileiro, incluindo a definição de stalking e cyberstalking, conforme a seguinte redação:

> Art. 147-A. 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. Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa.

A Lei Nº 14.132/2021, que alterou o Código Penal, representa um avanço significativo ao reconhecer a complexidade do crime de *stalking*, incluindo suas manifestações no ambiente digital. A criação de mecanismos que acompanhem a rápida evolução dessas práticas é fundamental para garantir que a legislação continue a proteger as vítimas de perseguição, independentemente do meio utilizado pelos agressores. Assim, reformas legislativas que visem adaptar o cenário jurídico são sempre bem-vindas, pois, à medida que novas formas de crimes emergem, o Direito, como ferramenta para promover justiça e defender interesses coletivos, deve estar preparado para lidar com essas mudanças.

Além do *cyberstalking*, outro crime foi adicionado ao Código Penal em 2024, o *cyberbullying*. Sancionada pelo Presidente da República em Janeiro, a Lei 14.811/2024 foi aprovada pelo Senado em dezembro de 2023. (senado.leg.br)

Cyberbullying é uma forma de bullying que ocorre no ambiente digital, utilizando tecnologias como redes sociais, aplicativos de mensagens, e-mails e outras plataformas online. Assim como o *bullying* tradicional, o *cyberbullying* envolve comportamentos hostis, mas se diferencia por sua capacidade de alcançar as vítimas em qualquer lugar e a qualquer hora.

A Lei 14.811/2024 também inclui na lista de crimes hediondos condutas como: sequestro e cárcere privado contra menores de 18 anos, indução ou auxílio ao suicídio ou automutilação usando a internet e o tráfico de crianças ou adolescentes.

II.7. Convenção de Budapeste

Em 2021, o Brasil aderiu à Convenção de Budapeste sobre os Crimes Cibernéticos, celebrada em novembro de 2001, cujo objetivo primordial é a cooperação internacional para combater o cibercrime. A Convenção de Budapeste sobre o Cibercrime é um tratado internacional que estabelece normas para combater crimes cibernéticos e promover a cooperação entre países. O Brasil promulgou a convenção em 2023, através do Decreto nº 11.491, e assumiu novas obrigações internacionais no combate a este tipo de crime.

Essa convenção aborda principalmente as violações de direitos autorais, fraudes relacionadas ao acesso à internet por meio de computadores, pornografia infantil e infrações à segurança de redes. De acordo com seu preâmbulo, a Convenção enfatiza a importância de estabelecer "uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adoção de legislação adequada e da melhoria da cooperação internacional", além de reconhecer " a necessidade de uma cooperação entre os Estados e a indústria privada".

Os novos instrumentos de cooperação jurídica internacional previstos na Convenção são três: a tipificação dos cibercrimes, a responsabilidade penal das pessoas jurídicas e a cooperação jurídica internacional para a obtenção de provas digitais e possui potencial para amparar na criação de políticas públicas e criminais voltadas para o tema. (ibccrim)

CAPÍTULO III - DESAFIOS E ENFRENTAMENTO

No capítulo de desafios legais do enfrentamento, será destacada a relevância da jurisprudência e precedentes relevantes para embasar a atuação legal contra os crimes virtuais. Além disso, é fundamental abordar as limitações e lacunas existentes na legislação brasileira no que diz respeito à criminalização e punição efetiva dos crimes cibernéticos. A identificação e análise desses desafios legais são essenciais para o desenvolvimento de estratégias mais eficazes e abrangentes de enfrentamento dos crimes virtuais no Brasil.

III.1. Estatísticas e tendências recentes

Segundo dados de outubro deste ano do DataSenado, os crimes virtuais vêm aumentando significativamente no Brasil, chegando a atingir 24% da população do país com mais 16 anos nos últimos 12 meses, que corresponde a um total de 40,85 milhões de pessoas lesadas. Essas estatísticas indicam a urgência de medidas efetivas para enfrentar o problema dos crimes virtuais no país.

Conforme uma pesquisa do Datafolha em parceria com o FBSP (Fórum Brasileiro de

Segurança Pública), o Brasil registra mais de 4.600 tentativas de golpes financeiros a cada hora, realizadas por meio de aplicativos de mensagens e ligações telefônicas. O levantamento realizado entre 11 e 17 de junho de 2024 contou com a participação de 2.508 pessoas de todas as regiões do país.

Figura 1: Gráfico demonstrando o número de tentativas de golpes por celular por hora. Fonte: Poder 360

Durante a pandemia de Covid-19 e o período de isolamento social, houve um aumento significativo no uso de computadores, celulares e tablets. O trabalho e os estudos remotos se tornaram soluções para manter o distanciamento social. Segundo a Agência Nacional de Telecomunicações (Anatel), o uso da internet no Brasil cresceu entre 40% e 50% durante a quarentena.

Os números alarmantes de crimes virtuais pós pandemia da Covid-19 se deu devido a migração dos crimes tradicionais para o meio informático. É possível observer uma mudança significativa no modus operandi de criminosos no Brasil pós pandemia, como evidencia a publicação de Lima e Bueno (2023) no fórum segurança, conforme gráfico publicado pelos autores analisando dados públicos oficias.

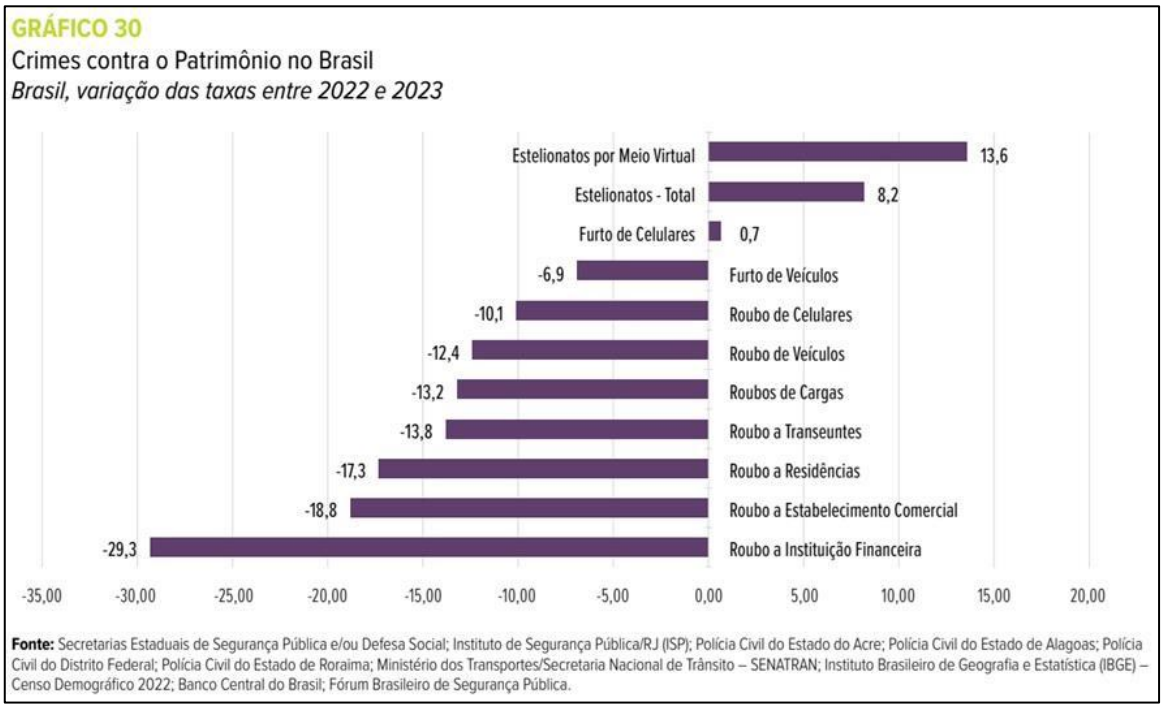

Figura 2: Gráfico da proporção de crimes cometidos contra o patrimônio entre 2022 e 2023. Fonte: Fórum Segurança

O autor Auriney Uchôa Brito cita a crescente dos crimes virtuais:

> Alguns fatores como a intensificação dos relacionamentos via internet, a produção em série de computadores, a popularização do comércio eletrônico (e-commerce) e o aumento de transações bancárias, estão diretamente ligados ao aumento de ocorrências de crimes conhecidos, mas que praticadas pela internet ao surgimento de novos valores e logicamente à novas condutas delitivas. (Brito, 2009, p.14)

O aumento das denúncias de discurso de ódio na internet também levanta preocupações sobre a intolerância política na era digital. Em 2022, os crimes de discriminação online cresceram 67% em comparação ao ano anterior, com a xenofobia registrando um aumento impressionante de 874%. Essa é a terceira vez consecutiva que essa tendência é notada durante anos eleitorais, de acordo com o gráfico obtido pela SaferNet, organização que acompanha crimes cibernéticos. (ESTADÃO, 2022)

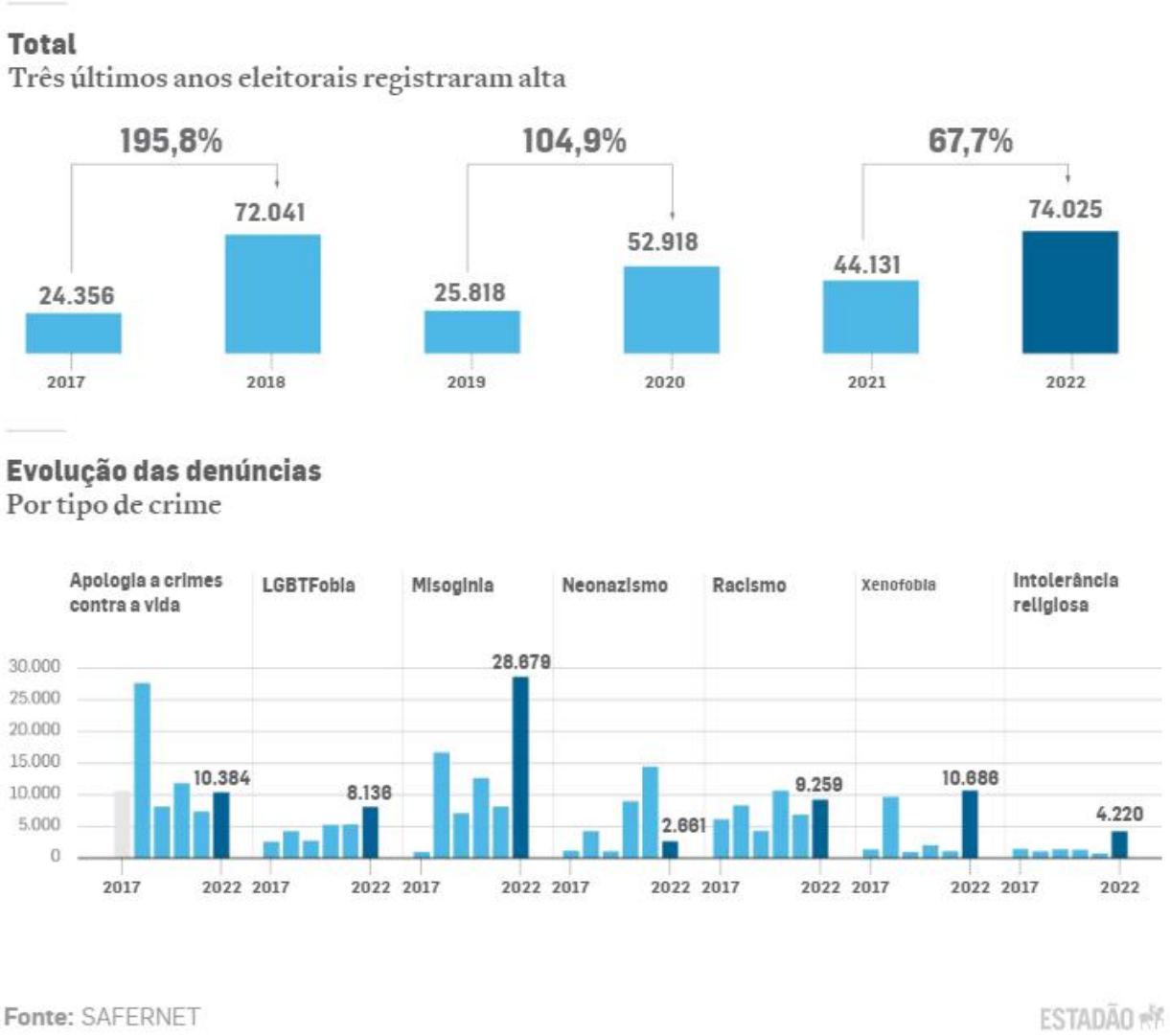

Figura 3: Gráfico com o percentual de crimes nos últimos três anos eleitorais em comparação com o ano anterior e evolução das denúncias por tipo de crime. Fonte: Estadão

Além de golpes financeiros, invasões informáticas e crimes de ódio, a pornografia infantil é outro crime que também registrou aumento considerável no Brasil nos últimos anos. Como, por exemplo, o estado da Paraíba, onde o número de operações da Polícia Federal contra abuso infantil na internet cresceu mais de dez vezes entre 2022 e 2024, segundo dados levantado pela Rádio CBN.

Outra face do problema é a criança ou adolescente deixado sem supervisão na internet, que acaba exercendo o papel de autor dos crimes, seja em sala de jogos ou redes socias e até mesmo em fóruns clandestinos. Essa situação tem sido tão comum que levantou-se a possibiliade de responsabilização dos pais, conceituando o fenomeno como “abandodo digital”, através de

publicação na revista do Instituto Brasileiro de Direito de Família (IBDFAM).

III.2. Desafios na aplicação da legislação

Apesar de diversas leis relacionadas ao tema terem sido discutidas até aqui, o crime digital avança junto com o mundo digital, que têm se desenvolvido a passos largos, o que acaba acarretando diversos problemas que dificultam o enfrentamento de crimes no âmbito virtual, como por exemplo a dificulade de investigação para descoberta de autoria delitiva e coleta de evidências digitais. Com a possibiliade de apagar dados online e uso de mecanismos que mascaram perfis falsos e endereços de IP, muitos criminosos se escoram na falta de equipamentos e profissionais competentes fornecidos aos orgãos encarregados das investigações. Outro problema atual é a jurisdição, visto que crimes informáticos comumente transpassam fronteiras o que levanta dúvidas sobre competência e a extradição e punição de criminosos.

A evolução tecnológica rápida é mais um desafio para os legisladores. A velocidade com que a tecnologia avança faz com que as legislações existentes se tornem rapidamente obsoletas. Novas formas de crimes cibernéticos, como fraudes, phishing e ransomware, surgem constantemente, exigindo que as leis sejam constantemente atualizadas e adaptadas. Essa necessidade de adaptação contínua pode ser um entrave para os legisladores, que muitas vezes lutam para acompanhar as inovações, correndo risco de criarem leis que ja nascem desatualizadas.

Além disso, a ausência de cooperação internacional também acarreta em uma grande lacuna nesse enfrentamento. A colaboração internacional é fundamental para a investigação e o processamento de crimes cibernéticos que transcendem fronteiras nacionais. Em um mundo cada vez mais interconectado, em que as atividades criminosas digitais podem ser praticadas em um país e impactar cidadãos de outro, a cooperação entre nações torna-se uma necessidade cada vez mais urgente. No entanto, essa colaboração enfrenta uma série de obstáculos, tanto políticos quanto jurídicos.

Desafios políticos e ideológicos podem surgir devido a diferenças nas prioridades e nas agendas de segurança nacional de cada país. Além disso, questões de soberania e a hesitação em compartilhar informações sensíveis podem criar barreiras significativas. No âmbito jurídico, as disparidades nas legislações nacionais sobre crimes cibernéticos, proteção de dados e direitos

individuais complicam ainda mais o processo de colaboração.

III.3. Tecnologias e ferramentas para combate aos crimes virtuais

A criptografia se destaca como uma das principais tecnologias para o combate aos crimes virtuais, oferecendo mecanismos de proteção de dados e comunicações, dificultando a ação de criminosos cibernéticos. Além disso, a segurança da informação é fundamental para prevenir ataques e garantir a integridade dos sistemas, o que pode ser feito por meio de firewalls, antivírus e outros softwares especializados. A utilização de inteligência artificial e big data também tem se mostrado eficaz na identificação de padrões de comportamento suspeito e na prevenção de fraudes cibernéticas, ampliando o leque de ferramentas disponíveis para o enfrentamento dos crimes virtuais.

III.3.1. Criptografia e Segurança da Informação

A criptografia desempenha um papel fundamental na proteção de informações sensíveis e na prevenção de crimes virtuais. Com o aumento das ameaças cibernéticas, a segurança da informação se torna uma prioridade para empresas e governos. A utilização de algoritmos criptográficos fortes ajuda a proteger dados confidenciais durante a transmissão e armazenamento, dificultando o acesso não autorizado. Além disso, a implementação de protocolos de segurança, contribui para a autenticação e integridade das comunicações online, tornando mais difícil para os criminosos virtuais interceptar e manipular informações.

No contexto dos crimes virtuais, os aspectos éticos e de privacidade desempenham um papel crucial, especialmente quando se trata de encontrar o equilíbrio entre a segurança cibernética e a proteção dos dados pessoais. Questões éticas surgem ao lidar com a vigilância online, uso de informações pessoais e tecnologias invasivas. Além disso, a proteção da privacidade dos indivíduos afetados por crimes virtuais é essencial para garantir a confiança na justiça e no sistema legal. Portanto, é fundamental abordar essas questões dentro de um quadro legal que leve em consideração os direitos individuais e a segurança da sociedade como um todo.

A criptografia, pode ser vista como um dos mecanismos utilizados para segurança da

informação, como forma de garantir a tripla proteção – confidencialidade, autenticidade e integridade.

Conhecida como a ciência ou arte de codificar mensagens, a criptografia é hoje um dos principais mecanismos de segurança que permite aos usuários de meios eletrônicos minimizar os riscos da Internet, protegendo suas comunicações, dados bancários e informações empresariais.

No entanto, essa técnica de codificação, que deveria garantir a segurança dos usuários, também tem sido utilizada para facilitar a prática de crimes e encobrir suas ações, fazendo com que a criptografia seja vista como uma ameaça em si. Ao dificultar a detecção e a punição de atividades indesejadas, a privacidade pode criar obstáculos a determinadas investigações e, em alguns casos, tornar inviável a aplicação de normas legais.

Conforme reportagem do Portal G1, entre 2015 e 2016, o WhatsApp teve suas operações suspensas três vezes no Brasil em um período de apenas oito meses, ficando paralisado por alguns dias ou horas devido a decisões judiciais. Com isso, surgiu a Ação Direta de Inconstitucionalidade (ADI) nº 5527 que requer a declaração de inconstitucionalidade dos incisos III e IV do art. 12 da Lei n° 12.965/14 (Marco Civil da Internet), sobre sanções como “suspensão” e “proibição” de serviços em caso de descumprimento da legislação brasileira.

A relatora da ADI, Ministra Rosa Weber, em seu voto fez forte defesa do elemento da criptografia e destacou sua importância nas passagens:

> Seria um inadmissível contrassenso, e mesmo retrocesso, tornar ilegal ou limitar dessa maneira o uso de criptografia. Relatório do National Research Council (Conselho Nacional de Pesquisa) dos EUA apontava, já em 1996, que os “esforços para controlar a criptografia seriam ineficazes, e seus custos excederiam qualquer benefício imaginável”.
> Além disso, a difusão da criptografia também tem garantido a segurança da comunicação de grupos de direitos humanos e indivíduos que se mobilizam contra regimes opressivos ao redor do mundo. (WEBER, 2020)

Assim sendo, proibir o uso da criptografia também parece infringir o princípio da inimputabilidade da rede, conforme estabelecido no Marco Civil da Internet, que afirma que a luta contra crimes na Internet deve focar nos responsáveis diretos, e não nos meios de acesso e transporte, com o objetivo de preservar a liberdade, a privacidade e os direitos humanos dos

usuários.

III.3.2. Conflitos entre segurança, privacidade e liberdade

Os conflitos entre segurança e privacidade surgem devido à necessidade de acesso a informações pessoais para investigação e prevenção de delitos, enquanto se respeitam os direitos individuais dos cidadãos. Essa tensão se reflete na discussão sobre a legalidade da coleta e acesso a dados pessoais, levantando questões éticas e jurídicas sobre a proteção da privacidade dos usuários. A legislação brasileira busca equilibrar esses aspectos, mas ainda enfrenta desafios na definição de limites claros e na regulação do uso de dados para fins de segurança cibernética, destacando a importância de um debate amplo e aprofundado sobre o tema.

As tecnologias emergentes, como inteligência artificial e big data, complicam ainda mais essa dinâmica. Elas permitem a análise de grandes volumes de dados, mas também levantam preocupações sobre como essas ferramentas são utilizadas em nome da segurança, potencialmente prejudicando a privacidade.

A liberdade é um princípio essencial em sociedades democráticas, permitindo que indivíduos se manifestem e compartilhem ideias. No entanto, a proteção de direitos humanos deve ser utilizada como para censurar conteúdos considerados ameaçadores ou prejudiciais. Isso levanta questões sobre onde traçar a linha entre a proteção da sociedade e a limitação da liberdade individual online. Esse debate foi acendido de forma mais contundente no Brasil recentemente, devido à uma tentativa de golpe de estado, que teve como liderança perfis famosos online e que culminou na suspensão temporária da rede social “X” no país.

A respeito disso, Bernardo Golçalves Fernandes, entende:

> Nesses termos, para a doutrina dominante, falar em direito de expressão ou de pensamento não é falar em direito absoluto de dizer tudo aquilo ou fazer tudo aquilo que se quer. De modo lógico-implícito a proteção constitucional não se estende à ação violenta. Nesse sentido, para a corrente majoritária de viés axiológico, a liberdade de manifestação é limitada por outros direitos e garantias fundamentais como a vida, a integridade física, a liberdade de locomoção. Assim sendo, embora haja liberdade de manifestação, essa não pode ser usada para manifestação que venham a desenvolver atividades ou práticas ilícitas (antissemitismo, apologia ao crime etc...) (FERNANDES, 2011, p. 279).

Assim sendo, a liberdade de expressão é uma garantia assegurada pela Constituição Federal de 1988, conforme os artigos 5º, incisos IV e XIV, e o artigo 220. Esses dispositivos garantem, respectivamente, a livre manifestação do pensamento, o acesso à informação e a criação e circulação de ideias, com ressalvas sobre anonimato, sigilo e outras garantias previstas na própria Constituição. (BRASIL, 1988)

III.3.3. Cooperação das plataformas digitais com âmbito global

Plataformas digitais tem mostrado resistencia em moderar conteúdos criminosos nas redes e em cooperar com investigações criminais. Recentemente, dirversos casos vieram a tona, como o aplicativo de mensagens Telegram, alvo de críticas por permitir a disseminação de conteúdos extremistas, desinformação e discursos de ódio. Em resposta, alguns governos na Europa têm pressionado a plataforma a tomar medidas mais rigorosas contra esse tipo de conteúdo. A situação se intensificou com o aumento das preocupações sobre segurança e privacidade, especialmente após eventos como atentados terroristas, onde plataformas de mensagens foram utilizadas para organizar ações. O criador do aplicativo de mensagens, Pavel Durov, chegou a ser preso na França, em agosto de 2024, como parte de uma investigação judicial em andamento (CNNBRASIL, 2024)

O discurso de ódio, com conteúdo criminoso, pode gerar lucro para plataformas digitais de diversas maneiras. Primeiramente, conteúdos polêmicos, incluindo discursos de ódio, tendem a provocar reações intensas, comentários e compartilhamentos. Esse aumento no engajamento resulta em mais tempo que os usuários passam nas plataformas, atraindo assim mais anunciantes dispostos a investir em publicidade.

Além disso, postagens que despertam emoções como raiva ou indignação geralmente recebem mais cliques e visualizações. As plataformas monetizam essas interações por meio da exibição de anúncios, gerando receita significativa. Os algoritmos de recomendação utilizados pelas plataformas muitas vezes priorizam conteúdos que mantêm os usuários engajados, o que pode levar a uma maior exposição a conteúdos extremos ou de ódio, perpetuando um ciclo em que essas postagens são continuamente promovidas.

A formação de comunidades online em torno do discurso de ódio também desempenha um papel importante. Essas comunidades atraem membros novos e engajados, gerando mais interações

e conteúdo, o que aumenta ainda mais o tráfego e a receita publicitária. Além disso, a moderação eficaz de conteúdos prejudiciais pode ser custosa e complexa. Quando as plataformas optam por uma moderação mais branda ou demorada, isso permite que conteúdos de ódio permaneçam visíveis por mais tempo, resultando em mais interação e, consequentemente, mais lucro.

Outro caso que evidencia a recusa da plataforma em fornecer dados de criminosos virtuais foi recente e midiático. Em 26 de janeiro de 2021, um usuário da plataforma Twitch, identificado como “abacate12345qaw”, fez comentários racistas durante uma transmissão do programa “Marca Página” no canal Omelete. As declarações foram vistas no chat da transmissão. Durante as investigações, a Amazon forneceu informações que revelaram que o IP do usuário era de Lisboa, Portugal, e o e-mail cadastrado foi identificado. O Tribunal de Justiça de São Paulo determinou que a empresa Google entregasse os dados do usuário, contudo, a empresa entrou com um mandado de Segurança no TRF3 e requereram a anulação da decisão de primeiro grau. A empresa alegou que o endereço eletrônico requisitado era acessado no Espaço Econômico Europeu (EEE), sob a custódia de dados da Google Ireland, constituída segundo as leis irlandesas e sujeita ao Regulamento Geral sobre a Proteção de Dados da União Europeia. Alegando também que era equivocada a premissa de que o Marco Civil da Internet autorizaria a requisição direta de dados. (TRF3.JUS.BR)

Por fim, foi mantida a decisão em primeiro grau e estabelecida multa diária de 5mil por dia para caso de descumprimento da decisão. O desembargador Hélio Nogueira, relator do caso, ressaltou o entendimento do STF sobre o assunto.

> “O Supremo declarou também a constitucionalidade da requisição direta de dados de provedores de aplicações de internet sediados no exterior, por parte do Judiciário brasileiro, com base no artigo 11 do Marco Civil da Internet e no artigo 18 da Convenção de Budapeste sobre Crime Cibernético, por força dos princípios da soberania e da independência nacional”. (TRF3.JUS.BR, 2024)

Para mitigar esses problemas, é necessário um esforço conjunto de plataformas de redes sociais, governos e sociedade civil para promover uma cultura de responsabilidade e respeito online, além de desenvolver tecnologias que possam identificar e limitar a disseminação de conteúdos de ódio de forma mais eficaz.

III.4. Investimento e capacitação e especialização profissional

O ambiente digital está em constante mudança, com novas tecnologias e plataformas surgindo regularmente. Essa evolução rápida frequentemente deixa os profissionais da segurança pública sem o treinamento atualizado necessário para acompanhar essas transformações. Como resultado, muitos agentes podem se sentir despreparados para lidar com as complexidades dos crimes cibernéticos.

A investigação de crimes cibernéticos exige conhecimentos específicos em áreas como análise de dados, forense digital e legislação sobre privacidade e proteção de dados. No entanto, a escassez de especialistas nessa área representa um desafio significativo, dificultando a capacidade de resposta das autoridades. Sem o conhecimento adequado, as investigações podem se tornar menos eficazes, comprometendo a segurança pública.

Além disso, muitas instituições enfrentam limitações orçamentárias e de pessoal, o que impacta negativamente a formação e a atualização de suas equipes. Sem um investimento adequado, é difícil garantir que os agentes tenham o suporte necessário para enfrentar os desafios que surgem no ambiente digital. Essa falta de especialiação não apenas prejudica a eficácia das investigações, mas também pode comprometer a segurança da sociedade como um todo.

A Magna Carta, em seu artigo 144, parágrafo 4º, estabelece que as polícias civis, sob a direção de Delegados de Polícia de carreira, são responsáveis pelas funções de polícia judiciária e pela investigação de crimes, exceto nas áreas de competência da Polícia Federal e das polícias militares.

Sobre isso, Carolina Borges Rocha, destacou:

> Estudiosos sobre o tema ainda afirmam que uma alteração no Código Penal não é conditio sine qua non para que se possa combater e coibir de forma eficaz os cibercrimes. O professor de Direito Penal da Faculdade Federal de Minas Gerais e Mestre em Ciências Penais pela UFMG Túlio Lima Vianna assevera que o nosso ordenamento não necessita de lei regulamentadoras e sim, um aparato técnico e específico nas investigações forenses por parte das polícias quanto a estes delitos e uma ação conjunta entre os diversos entes que corporificam o Poder Judiciário e o Ministério Público (ROCHA, 2013, p.8).

Pelo mesmo caminho, temos o entendimento do autor Fabrízio Rosa (2002):

> É imperioso frisar, por derradeiro, que nenhum combate sério aos “Crimes de Informática” se esgota no processo tipificador. Sem a cooperação internacional, sem a melhoria do

> aparelhamento policial e judicial e sem o aperfeiçoamento profissional dos que operam nessas áreas, a simples existência de uma adequada tipificação não tem o menor significado prático e não basta para tutelar a sociedade contra tão lesiva atividade criminosa. Resta concluir, portanto, que o controle dos "Crimes de Informática" deve merecer uma atenção especial. Temos, pois, como uma observação realmente consistente na ciência penal e que como tal deveria ser levada em maior conta pelo legislador, o fato de que tanto um excesso de tutela penal quanto seus defeitos podem prejudicar que se atinja o objetivo teleológico do sistema.(ROSA 2002, p. 72)

Um exemplo na questão de especialiação de agentes para combate desses crimes foi dado pelo Ministério Público Federal (MPF), que estabeleceu um Grupo de Atuação Especial voltado para o combate a crimes cibernéticos. O novo grupo, chamado GACCTI (Grupo de Atuação em Crimes Cibernéticos e Tecnologias de Informação), terá como objetivo investigar e processar delitos relacionados à internet e às tecnologias digitais, além de promover ações educativas e de conscientização sobre a segurança cibernética. A criação desse grupo, conforme consta na própria página do MPF, reforça o compromisso do Órgão em enfrentar os desafios trazidos pela evolução tecnológica e proteger a sociedade contra crimes virtuais.

Outra iniciativa recente foi a promoção de um treinamento para procuradores no Brasil, sobre o combate a crimes cibernéticos, promovido pelo Conselho da Europa. O objetivo da capacitação é fornecer novas competências práticas para a investigação de delitos cometidos na internet. Apesar do treinamento ter abrangido somente um grupo de 19 profissionais, a ideia é que esses membros participantes atuem como replicadores do aprendizado em suas instituições (MPF, 2024).

III.5. Enfrentamento pela educação e conscientização

A educação e conscientização sobre crimes virtuais são fundamentais para combater os crimes virtuais. Programas de educação digital e cidadania devem ser implementados nas escolas e comunidades, com o objetivo de orientar crianças, adolescentes e adultos sobre os riscos e consequências das atividades ilegais na internet. Além disso, é necessário promover campanhas de conscientização para alertar a população sobre a importância de manter a segurança cibernética e a proteção de dados pessoais. Através da educação, as pessoas podem se tornar mais conscientes e preparadas para enfrentar os desafios dos crimes virtuais no Brasil.

O projeto Segurança em Foco do Ministério Público, em sua 18ª edição, que aconteceu em maio de 2024, teve como tema o combate à cibercriminalidade, e como destaque no combate foi levantada a questão de ações preventivas por meio de campanha que impactem à população, como afirma notícia no site oficial do Conselho Nacional do Ministério Público (CNMP). Ou seja, tão importante quanto os investimentos para a frente repressiva, é essencial ações preventivas por meio de conscientização. (CNMP, 2024)

Uma das estratégias usadas por infratores e estelionatários é o uso de pessoas influentes na mídia para divulgar oportunidades de investimentos e possibilidade de renda extra, que segundo dados faz as maiores vítimas nas classes sociais menos favorecidas economicamente.

O Fortune Tiger, popularmente conhecido como “tigrinho” no Brasil, é um jogo de cassino online, do tipo caça-níquel, promovido por influenciadores e que promete grandes ganhos em dinheiro. O objetivo é formar combinações de três figuras iguais nas fileiras exibidas. Considerados jogos de azar pela Lei de Contravenções Penais, esses games diferem dos sites de apostas regulamentados, onde os jogadores apostam em resultados de eventos esportivos. Segundo o Departamento Estadual de Investigações Criminais (Deic), a divulgação de jogos de azar pode levar a acusações de crimes contra as relações de consumo, economia popular, propaganda enganosa, sonegação fiscal e estelionato. (G1.COM, 2024)

Em matéria ao site de notícia de notícia G1, explicou o advogado Gabriel Righeti.

> Os jogos de azar geralmente estão ligados ao estelionato, que nada mais é do que um golpe. Nesse caso, influenciadores divulgam uma oferta ou promessa de ganho fácil de dinheiro em um lapso temporal muito curto, induzindo as pessoas a um ganho irreal, cuja chance é muito baixa. (RIGHETI, 2024)

A operação "Integration", que apura crimes de lavagem de dinheiro e jogos ilegais contra as casas de aposta esportiva, que usavam influenciadores para driblar a lei e promover jogos de azar. De acordo com o secretário de Defesa Social de Pernambuco, Alessandro Carvalho, empresas investigadas atuavam no jogo do bicho e migraram para o ramo de apostas online. (G1.COM)
Segundo afirma o secretário:

> É feita toda uma história de que o jogo vai levar você a ter um patrimônio, um carro, uma mansão, um barco, quando isso não é realidade. Aquela pessoa que tem um carro, uma mansão, um barco, não foi jogando [que ganhou]. Foi sendo patrocinada para vender uma

> ilusão e levar pessoas a jogar, muitas vezes, de forma compulsiva e perder tudo que têm. (CARVALHO, 2024, ONLINE)

Por isso, é essencial promover a conscientização sobre os riscos associados aos jogos de azar e os efeitos prejudiciais que podem ter na vida das pessoas. É importante lembrar que o jogo de azar não deve ser praticado como uma maneira de gerar renda ou resolver problemas financeiros.

Os programas de educação digital e cidadania têm se mostrado fundamentais no enfrentamento dos crimes virtuais no Brasil, pois fornecem aos cidadãos as ferramentas necessárias para se protegerem online. Esses programas abordam temas como segurança de dados, identificação de golpes e fraudes, direitos e deveres dos usuários da internet, além de promoverem a consciência sobre a responsabilidade no uso da tecnologia. Através de parcerias entre órgãos governamentais, empresas e instituições de ensino, essas iniciativas contribuem para a formação de uma sociedade mais informada e engajada na prevenção e combate aos crimes virtuais, promovendo a cidadania digital e a segurança online.

CONCLUSÃO

Diante do exposto, conclui-se que os crimes virtuais representam um desafio cada vez mais complexo e impactante para a sociedade brasileira. Este trabalho evidenciou a necessidade de atualização e aprimoramento da legislação nacional, bem como a importância de instrumentos de cooperação internacional para enfrentar esse fenômeno. Além disso, a conscientização da população e a implementação de programas de educação digital se revelaram fundamentais para a prevenção e combate a esses crimes. Com base nas análises dos dados, recomenda-se a criação de políticas públicas mais eficazes e a promoção do debate sobre ética e privacidade no contexto dos avanços tecnológicos e o investimento em profissionais capacitados e equipamentos adequados para instruir as investigações, visando a proteção efetiva dos cidadãos e a garantia de um ambiente virtual mais seguro e ético para todos.

As principais contribuições deste trabalho incluem uma análise abrangente da legislação brasileira relacionada aos crimes virtuais, que abrange desde normas penais até diretrizes de proteção de dados e privacidade. Essa análise permite a identificação de lacunas e desafios legais

enfrentados no Brasil, revelando não apenas as limitações da legislação atual, mas também as dificuldades práticas na sua aplicação. Além disso, os resultados ressaltam a importância dos acordos e tratados de cooperação internacional, que se mostram cruciais para a investigação e punição eficaz desses crimes, uma vez que muitos delitos cibernéticos transcendem fronteiras e requerem uma abordagem colaborativa entre diferentes jurisdições. O estudo também destaca a necessidade premente de programas de educação digital e conscientização, visando empoderar os cidadãos com conhecimentos e ferramentas para se protegerem no ambiente virtual. Essa abordagem integral é fundamental para enfrentar o problema de forma eficaz e ética, promovendo uma cultura de segurança digital que envolve não apenas a legislação, mas também a formação e a responsabilidade social de todos os envolvidos. Assim, o trabalho se propõe a ser um ponto de partida para discussões mais amplas sobre políticas públicas e iniciativas que busquem garantir um ambiente online mais seguro e respeitoso para todos os usuários.

Para o futuro, é crucial que o Brasil responda com leis atualizadas para combater os crimes virtuais, levando em consideração as rápidas mudanças tecnológicas e os novos tipos de ameaças. Além disso, é fundamental investir em treinamento e capacitação das equipes responsáveis pela aplicação da lei, a fim de garantir uma resposta eficaz e especializada. Uma maior cooperação internacional também é essencial, com o estabelecimento de acordos e tratados que facilitem a troca de informações e a colaboração entre países na investigação e punição dos criminosos virtuais. Por fim, a conscientização pública sobre segurança cibernética e práticas seguras na internet deve ser promovida de forma constante, por meio de programas de educação digital e cidadania, visando a prevenção e proteção contra os crimes virtuais.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 23 ago.

2024. BRASIL. **Decreto-Lei n° 3.689, de 03 de outubro de 1941**. Institui o Código de Processo Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decretolei/del3689.htm. Acesso em: 26 maio.

2021. BRASIL. **Decreto-Lei no 2.848, de 7 de dezembro de 1940** (Código Penal). Disponível em: http://www.planalto.gov.br/ccivil_03/decretolei/del2848compilado.htm. Acesso em: 23 Abr.

2021. **BRASIL. Lei n° 12735, de 30 de novembro de 2012**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 4 Mar.

2021. BRASIL. **Lei n° 12737, de 30 de novembro de 2012**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 25 Fev.

2024. BRASIL. **Lei n° 12965, de 23 de abril de 2014**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 19 Fev.

BRASIL. **Estatuto da Criança e do Adolescente**. Lei 8.069/90. São Paulo, Atlas, 1991.Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069compilado.htm

2024. BRASIL. **Lei n° 13. 709, de 14 de agosto de 2018**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 26 maio.

2024. BRASIL. **Lei n° 8.069, de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Planalto.gov.br. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 12 Out. 2024.

2024.https://**g1.globo.com**/pb/paraiba/noticia/2024/10/12/numero-de-operacoes-da-pf-contra-abuso-infantil-na-internet-cresce-mais-de-10x-entre-2022-e-2024-na-paraiba.ghtml

2024.https://**www.mpf.mp.br**/pgr/noticias-pgr2/2024/mpf-cria-grupo-de-atuacao-especial-para-combateacrimescibernеticos#:~:text=O%20Minist%C3%A9rio%20P%C3%BAblico%20Federal%20criou,Tecnologias%20de%20Informa%C3%A7%C3%A3o%20(Gaccti).

2024.https://**ibdfam.org.br**/noticias/11431/Crimes+virtuais+que+envolvem+crian%C3%A7as+acendem+alerta+sobre+abandono+digital%3B+pais+podem+ser+responsabilizados%3F

2024.https://**oglobo.globo.com**/brasil/noticia/2024/07/18/golpes-virtuais-crescem-no-brasil-enquanto-roubos-presenciais-diminuem.ghtml

LOPES JÚNIOR, Aury. **Direito processual penal**. 14. ed. – São Paulo: Saraiva Educação, 2019.

ROSA, Fabrízio. **Crimes de Informática**. 2.ed. Campinas: BookSeller, 2006.

COSTA, Marco Aurélio Rodrigues. **Crimes de informática**. Disponível em: Revista Eletrônica Jus.com.br https://jus.com.br/artigos/1826/crimes-de-informatica

VIANNA, Tulio Lima 2003.**Do acesso não autorizado a sistemas computacionais**. Disponível em: https://repositorio.ufmg.br/bitstream/1843/BUOS-96MPWG/1/disserta__o_t_lio_lima_vianna.pdf Acesso em: 24/08/2024.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos**: Ameaças e procedimentos de investigação. 2ª edição, Brasport. Publicado em: abril de 2017.

GRECO, Rogério. **Curso de Direito Penal: parte especial** / Volume II: introdução à teoria geral da parte especial: crimes contra a pessoa. 5 ed., Rio de Janeiro: Impetus, 2008.

FERNANDES, Bernardo Gonçalves. **Curso de direito constitucional**. 3.ed. Rio de Janeiro: Lumen Juris, 2011.

ROCHA, Carolina Borges. **A evolução criminológica do Direito Penal**: Aspectos gerais sobre os crimes cibernéticos e a Lei 12. 737/2012. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 18, n. 3706, 24 ago. 2013. Disponível em: https://jus.com.br/artigos/25120. Acesso em: 24 out. 2024.

BRITO, Auriney Uchôa de. **O bem jurídico-penal dos delitos informáticos**. Boletim Publicação Oficial do Instituto Brasileiro de Ciências Criminais, n° 199, junho/2009.

G1 NOTÍCIAS. **Bets contratavam influenciadores para driblar lei e promover jogos de azar, diz secretário sobre operação que prendeu deolane bezerra.** Pernanbuco, 2024. Disponível em: https://g1.globo.com/pe/pernambuco/noticia/2024/09/06/bets-contratavam-influenciadores-para-driblar-lei-e-promover-jogos-de-azar-diz-secretario-sobre-operacao-que-prendeu-deolane-bezerra-video.ghtml Acesso em: outubro de 2024.

CNN BRASIL**. Telegram tem se tornado canal para movimentos extremistas**. Disponível em: https://www.cnnbrasil.com.br/internacional/analise-telegram-tem-se-tornado-canal-para-movimentos-extremistas/ Acesso em: setembro de 2024.

PODER 360. **Brasil tem mais de 4.600 tentativas por hora de golpe por telefone**. Seçao Segurança Pública. Disponível em: https://www.poder360.com.br/seguranca-publica/brasil-tem-mais-de-4-600-tentativas-por-hora-de-golpe-por-telefone/ Acesso setembro de 2024.

ALCADIPANI, RAFAEL; LIMA, RENATO SÉRGIO DE; BUENO, SAMIRA. **Estelionatos crescem e já superam os roubos e fortalecem o crime organizado no Brasil**. Fórum Segurança. Disponível em: https://fontesegura.forumseguranca.org.br/estelionatos-crescem-ja-superam-os-roubos-e-fortalecem-o-crime-organizado-no-brasil/#_ftn1 Acesso em: setembro 2024.

MURATA, Ana Maria Lumi Kamimura; TORRES, Paula Ritzmann. **A Convenção de Budapeste sobre os crimes cibernéticos foi promulgada, e agora?** BOLETIM IBCCRIM, julho de 2023. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/575/108 Acesso em outubro de 2024.

SENADO NOTÍCIAS. **É sancionada Lei que inclui bullying e cyberbullying no Código Penal**. Disponível em: https://www12.senado.leg.br/radio/1/noticia/2024/01/15/e-sancionada-lei-que-

inclui-bullying-e-cyberbullying-no-codigo-penal#:~:text=A%20Lei%2014.811%2F2024%2C%20sancionada,e%20a%20indu%C3%A7%C3%A3o%20%C3%A0%20automutila%C3%A7%C3%A3o Acesso em: outubro de 2024.

ESTADÃO. **Alta de 67% do discurso de ódio nas redes sociais acende alerta sobre extremismo**. Secçao Política. Disponível em https://www.estadao.com.br/politica/alta-de-67-do-discurso-de-odio-nas-redes-sociais-acende-alerta-sobre-extremismo/ Acesso em: outubro de 2024.

UOL NOTÍCIAS**. Jogo do tigrinho é parte da migração do crime para o mundo virtual**. Disponível em: https://noticias.uol.com.br/cotidiano/ultimas-noticias/2024/06/24/analise-jogo-do-tigrinho-e-parte-da-migracao-do-crime-para-o-mundo-virtual.htm Acesso em: outubro de 2024.

G1.GLOBO**. Quais são os crimes cometidos por quem divulga o jogo do tigrinho.** São Paulo. Disponível em: https://g1.globo.com/sp/vale-do-paraiba-regiao/noticia/2024/06/18/quais-sao-os-crimes-cometidos-por-quem-divulga-o-jogo-do-tigrinho.ghtml Acesso em outubro de 2024.

CAMARA.LEG. **Projeto de Lei 3628/2020**. Site da Câmara dos Deputados. Atividade Legislativa. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2256711 Acesso em: outubro de 2024.

MPF. **Procuradores participam de capacitação sobre combate a crimes cibernéticos promovida pelo conselho da Europa.** Disponível em: https://www.mpf.mp.br/pgr/noticias-pgr2/2024/procuradores-participam-de-capacitacao-sobre-combate-a-crimes-ciberneticos-promovida-pelo-conselho-da-europa Acesso em: outubro de 2024.

SENADO.LEG. **Golpes digitais atingem 24% da população brasileira revela DataSenado.** Senado Notícias. Disponível em: https://www12.senado.leg.br/noticias/materias/2024/10/01/golpes-digitais-atingem-24-da-populacao-brasileira-revela-datasenado Acesso em: outubro de 2024.

TRF3. **Google Brasil deve fornecer dados telemáticos para apuração de crime de racismo**. Site da Justiça Federal da 3ª Região. Disponível em: https://web.trf3.jus.br/noticias-sjsp/Noticiar/ExibirNoticia/1371-google-brasil-deve-fornecer-dados-telematicos-para Acesso em: outubro de 2024.

G1.GLOBO. **Whatsapp já foi bloqueado judicialmente por decisão judicial em 2015 e 2016 no Brasil**. Disponível em: https://g1.globo.com/tecnologia/noticia/2022/03/18/whatsapp-ja-foi-bloqueado-por-decisao-judicial-em-2015-e-2016-no-brasil.ghtml Acesso em: outubro de 2024.

WEBER, Rosa. **Acão Direta de Inconstitucionalidade 5527**. Noticias STF. Disponível em: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI5527voto.pdf Acesso em: outubro de 2024.