A insuficiência das leis de repreensão das figuras enigmáticas:

Deficiências Legislativas que facilitam a ocorrência de crimes digitais.

Edinael Ferreira Medrado[1]
Felipe Carlos Bueno[2]
Giovana Duarte Cassimiro[3]
Gláucya Gabrielle da Silva[4]
Nicolly Victoria Pascoal[5]

https://doi.org/10.5281/zenodo.17543597

RESUMO

A insuficiência das leis de repressão aos crimes digitais permite que figuras enigmáticas, muitas vezes anônimas e não identificáveis, atuem livremente no ambiente virtual. A falta de uma legislação específica e eficaz facilita a prática de fraudes, roubos de dados e outros delitos cibernéticos, tornando a internet uma "terra sem lei". A ausência de penalidades efetivas e a dificuldade em rastrear os criminosos ampliam a sensação de insegurança da população. Diante desse cenário, torna-se urgente a criação e a atualização de normas que acompanhem os avanços tecnológicos, garantindo um ambiente digital mais protegido e reduzindo as brechas legais que favorecem essas atividades ilícitas.

Palavras-chave: A insuficiência das leis; crimes digitais; figuras enigmáticas**.**

ABSTRACT.

The insufficiency of laws to repress digital crimes allows enigmatic figures, often anonymous and unidentifiable, to act freely in the virtual environment. The lack of specific and effective legislation facilitates fraud, data theft, and other cyber offenses, turning the internet into a "lawless land." The absence of effective penalties and the difficulty in tracking criminals increase the population's sense of insecurity. Given this scenario, it is urgent to create and update regulations that keep pace with technological advances, ensuring a safer digital environment and reducing legal loopholes that enable such illicit activities.

Keyword: The insufficiency of laws; digital crimes; enigmatic figures.

[1] Concluinte curso de Direito pela Faculdade de Araraquara – FARA;
[2] Concluinte curso de Direito pela Faculdade de Araraquara – FARA;
[3] Concluinte curso de Direito pela Faculdade de Araraquara – FARA;
[4] Concluinte curso de Direito pela Faculdade de Araraquara – FARA;
[5] Concluinte curso de Direito pela Faculdade de Araraquara – FARA

INTRODUÇÃO

A evolução da tecnologia e da internet trouxe mudanças significativas para a sociedade, alterando a dinâmica dos crimes, especialmente os cibernéticos, como fraudes e roubos de dados. O aumento desses crimes destaca a urgência de uma legislação eficaz, uma vez que a falta de normas específicas deixa a população desprotegida e insegura. Esse cenário não apenas gera problemas substanciais, mas também incentiva a prática de atividades ilícitas, uma vez que as leis atuais frequentemente não abordam as nuances dos crimes digitais.

Em síntese a expressão popular "Terra sem lei", refere-se ao mundo digital, local caótico, no qual criminosos não são identificados por suas ações ilícitas, tipificada no código penal brasileiro, entretanto, os atos delituosos, classificado como crimes cibernéticos, usualmente, não enfrentam penalidades, uma vez que os criminosos não são identificáveis. Reputado que os criminosos não são identificáveis, e frequentemente assumem o papel de figuras enigmáticas, caracterizadas por sua invisibilidade.

Visto que, diante do aumento dos crimes digitais, a falta de legislação eficaz deixa a população desprotegida e insegura, gerando problemas significativos e, ainda, incentiva a prática desses crimes, já que as leis não são tão específicas. Os avanços da tecnologia, exigem leis eficazes que devem acompanhar as inovações sem deixar lacunas vagas, para garantir um ambiente seguro até mesmo na internet.

1. CRIMES CONTRA A HONRA.

O avanço da tecnologia e ascensão da chamada "era digital", crimes do cotidiano físico também passam a figurar entre os delitos que podem ser facilmente operados também no meio virtual. Os crimes contra a honra, tão comuns, estão também entre as práticas que ganharam novos contornos com o avanço da tecnologia.

Descritos no código penal, mais necessariamente nos artigos 138,139 e 140, os crimes contra a honra se dividem em três categorias: calúnia, difamação e injúria.

Entende-se calúnia (Art. 138) como atribuir de forma pública um crime a alguém, pune-se com detenção de 6 meses a 2 anos ou multa.

> Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime: Pena - detenção, de seis meses a dois anos, e multa.
> § 1º - Na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga.
> § 2º - É punível a calúnia contra os mortos. Exceção da verdade § 3º - Admite-se a prova da verdade, salvo:

> I - se, constituindo o fato imputado crime de ação privada, o ofendido não foi condenado por sentença irrecorrível;
> II - se o fato é imputado a qualquer das pessoas indicadas no nº I do art. 141;
> III - se do crime imputado, embora de ação pública, o ofendido foi absolvido por sentença irrecorrível.

A difamação é a acusação pública de um ato, embora não ilícito ou ilegal, considerado imoral pela sociedade ou grupo em que o ofendido está inserido, contra a tradição e costumes próprios do contexto em que se injuria alguém. Punível com três meses a um ano de detenção e multa

> Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação:
> Parágrafo único - A exceção da verdade somente se admite se o ofendido é funcionário público e a ofensa é relativa ao exercício de suas funções.

A injúria, mais abrangente e mais cotidiana, trata-se da ofensa pessoal a alguém de forma que ofenda a sua dignidade, como num xingamento. Punível com um mês a seis de detenção e multa.

> Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro: Pena - detenção, de um a seis meses, ou multa.
> § 1º - O juiz pode deixar de aplicar a pena: I - quando o ofendido, de forma reprovável, provocou diretamente a injúria; II - no caso de retorsão imediata, que consista em outra injúria. § 2º - Se a injúria consiste em violência ou vias de fato, que, por sua natureza ou pelo meio empregado, se considerem aviltantes: Pena - detenção, de três meses a um ano, e multa, além da pena correspondente à violência. Pena - reclusão de um a três anos e multa

2. INVASÕES INFORMÁTICA

Um dos crimes cibernéticos tipificados no código penal brasileiro é a “invasão informática” que consiste na usurpação de sistemas ligados a dispositivos informáticos, previsto no art. 154- A Código Penal.

> 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.

O aumento das transgressões no mundo digital colaboraram para a criação de leis voltadas aos crimes cibernéticos, entretanto, é inegável as lacunas existentes na legislação brasileira, principalmente em relação aos criminosos anônimos, denominados como “Crackers”, que provém do inglês “to crack” e, em português traduzido para “quebrar”, são conceitos atribuído aos indivíduos que possui como objetivo a quebra de códigos de seguranças, no intuito de invadir diversos tipos de sistemas de segurança, com o propósito de causar danos e prejudicar outrem. Os criminosos virtuais, atuam de diversas maneiras, desde do acesso a

dispositivos eletrônicos de terceiros, até sistema de segurança de informações de grande relevância social.

3. EXPLORAÇÃO SEXUAL INFANTOJUVENIL DIGITAL.

A exploração sexual infantil no contexto digital representa uma das formas mais severas de violação dos direitos de crianças e adolescentes. No Brasil, onde o acesso à internet se ampliou consideravelmente, os riscos relacionados ao uso inadequado da tecnologia se tornam cada vez mais evidentes. Este crime digital é uma realidade alarmante no Brasil a Safernet (Associação Civil do Direito Privado) recebeu 71.867 novas denúncias somente em 2023 e no mundo segundo a Organização das Nações Unidas (ONU) cerca de 300 milhões de crianças foram afetadas pela exploração sexual e abuso infantil online.

A exploração sexual infantil na internet inclui práticas como **pornografia infantil, *grooming* (aliciamento), *sexting, sextortion e revenge porn***. Os criminosos se aproveitam do anonimato e da facilidade de contato com as vítimas através de redes sociais, aplicativos de mensagens e jogos online. De acordo com o Estatuto da Criança e do Adolescente (ECA), a produção, posse ou distribuição de materiais pornográficos envolvendo crianças e adolescentes é considerada crime; no entanto, a identificação e responsabilização dos infratores ainda apresentam desafios significativos no ambiente virtual.

O Estatuto da Criança e do Adolescente - ECA (Lei nº 8.069/1990) diz que:

> Art. 4º: Garante proteção integral à criança e ao adolescente, assegurando-lhes direitos fundamentais com prioridade absoluta.
> Art. 5º: Prevê a inviolabilidade da integridade física, psíquica e moral das crianças e adolescentes.
> Art. 240: Penaliza quem produz, filma ou fotografa cenas de sexo explícito ou pornográficas envolvendo menores de 18 anos.
> Art. 241-A: Criminaliza quem oferece, troca, disponibiliza ou vende material de pornografia infantil.
> Art. 241-D: Tipifica o aliciamento de crianças para fins sexuais por meio de comunicação eletrônica, como redes sociais.

Um exemplo desse problema é o *grooming*, em que os criminosos fabricam perfis falsos para conquistar a confiança de crianças e adolescentes, incentivando-os a compartilhar fotos ou vídeos íntimos. A pornografia infantil, que conta com a legislação vigente, ECA e Código Penal, continua a ser uma das principais preocupações, pois existe um mercado ilegal que trafica imagens e vídeos com menores.

Além disso, novas práticas, como a sextorsão, utilizam conteúdos íntimos para extorquir as vítimas, buscando obter vantagens financeiras ou outros benefícios, enquanto o revenge porn espalha imagens íntimas sem autorização, com o intuito de humilhar as pessoas afetadas

Nesse sentido o Código Penal Brasileiro (Decreto-Lei nº 2.848/1940) define:

> Art. 213: Define o crime de estupro, incluindo situações em que o ato é praticado por meios digitais (conforme entendimento do STJ).
> Art. 218-C: Criminaliza a divulgação de cenas de sexo explícito ou pornográficas envolvendo crianças e adolescentes, mesmo sem o consentimento das vítimas.

3.1. O CONCEITO DE ABANDONO DIGITAL E SEUS IMPACTOS.

O abandono digital acontece quando os pais ou responsáveis não monitoram adequadamente as atividades online de crianças e adolescentes. Embora muitos ofereçam dispositivos eletrônicos para entretenimento, deixam de supervisionar ou estabelecer limites, o que os expõe a conteúdos prejudiciais e a ações de criminosos virtuais. Essa situação se agrava pela ausência de uma cultura de educação digital, na qual as crianças seriam orientadas sobre os perigos e os limites do ambiente virtual.

TIC Kids Online Brasil (2021) mostram que 93% dos jovens brasileiros, com idades entre 9 e 17 anos, acessam a internet com frequência, muitas vezes sem a supervisão necessária. Essa realidade ressalta a importância de se implementar ferramentas de controle parental e campanhas de conscientização que ajudem as famílias a protegerem os menores.

De acordo com o psicólogo Jonathan Haidt (2024), crianças com menos de 14 anos não deveriam ter acesso a smartphones, e o uso de redes sociais deveria ser limitado a adolescentes acima de 16 anos, sempre com a supervisão dos responsáveis.

3.2. NOTÍCIAS DE EXPLORAÇÃO INFANTOJUVENIL NA INTERNET.

1. Caso de Parnaíba (Piauí): O caso em Parnaíba, no Piauí, envolve a prisão de um homem acusado de abusar sexualmente de crianças com quem mantinha vínculo, além de registrar os atos em imagens e compartilhá-las na *deep web*. As investigações foram desencadeadas após uma análise de imagens realizada por uma agência policial australiana, que detectou a origem das gravações em Parnaíba. A análise levou a Interpol a identificar a localização e iniciar a operação para prender o responsável. As imagens, agora parte de investigações internacionais, indicam o uso da internet para o tráfico de material de abuso sexual infantil, prática comum na *deep web*, onde a anonimização e a criptografia dificultam a identificação dos criminosos. (Operação Anomia — Polícia Federal / veículos de imprensa, 2022)

2. O fato de a identidade do acusado ainda não ter sido divulgada é uma estratégia comum de preservação da privacidade durante a investigação, visando garantir que o processo seja conduzido sem interferências externas. Contudo, a ocultação de identidades também levanta questões sobre o direito à informação e a transparência processual. Além disso, as investigações se expandem para procurar possíveis cúmplices e outras vítimas, uma vez que, em casos como esse, a exploração de crianças e adolescentes é frequentemente uma atividade em rede, com múltiplos envolvidos. (Constituição Federal 1988)

3. Operação Caruncho e Identidade dos Cúmplices: A Operação Caruncho, realizada pela Polícia Federal, desmantelou uma rede criminosa envolvida na produção e disseminação de material pornográfico infantil. Nessa operação, mais de 40 pessoas ainda permanecem desconhecidas, o que significa que grande parte da rede continua sem ser desmantelada. Isso mostra a complexidade das investigações, onde a tecnologia e a criptografia dificultam a identificação dos responsáveis. O grande número de cúmplices ainda não identificados também levanta um ponto importante: a responsabilidade coletiva e as dificuldades de responsabilização dos envolvidos, quando muitos atuam de forma descentralizada e escondida na internet. (Polícia Federal - PF investiga crimes de abuso sexual infantojuvenil na internet — Polícia Federal)

A vigilância parental, aliada a campanhas de educação digital, desempenha um papel crucial na proteção de crianças e adolescentes contra os perigos do ambiente virtual. Ao mesmo tempo, cabe ao Estado e à sociedade civil fortalecer as redes de proteção e implementar medidas que garantam a dignidade e segurança das futuras gerações.

Casos como os citados neste artigo ilustram a complexidade das investigações relacionadas a crimes digitais envolvendo abuso infantil. Eles destacam a necessidade urgente de uma atuação integrada entre governos, agências internacionais e plataformas digitais para proteger as vítimas e responsabilizar os criminosos. A atuação preventiva, por meio de educação digital e conscientização, também desempenha um papel essencial na redução desses crimes, além da importância de atualizações constantes nas legislações, adaptando-as às novas tecnologias e formas de abuso. Pois segundo a Constituição Federal de 1988 no Art. 227:

> Art. 227: "É dever da família, da sociedade e do Estado assegurar à criança e ao adolescente, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão."

Dessa forma, o combate à exploração sexual infantil digital exige um compromisso coletivo, que vai além das ações pontuais e se transforma em uma mobilização permanente em defesa dos direitos das crianças e adolescentes.

4. EXPOSIÇÃO DA INTIMIDADE SEXUAL

A exposição da intimidade sexual consiste na divulgação não autorizada de vídeos ou imagens íntimas de uma pessoa. Trata-se de um crime que envolve a violação da privacidade e da dignidade das vítimas, sendo um problema grave na era digital devido à velocidade com que essas informações se propagam.

O artigo 216-B do Código Penal aborda esse tipo de crime:

> Art. 216-B: Produzir, fotografar, filmar ou registrar, por qualquer meio, conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado sem autorização dos participantes.
> Pena: Detenção de 6 meses a 1 ano, e multa.
> Parágrafo único: Aplica-se a mesma pena a quem realiza montagem em fotografia, vídeo, áudio ou qualquer outro registro, incluindo pessoa em cena de nudez ou ato sexual ou libidinoso.

A criminalização desse tipo de conduta foi reforçada com a Lei nº 12.737/2012 (Lei Carolina Dieckmann), sancionada após a atriz Carolina Dieckmann ter suas imagens íntimas divulgadas por hackers.

4.1. NOTÍCIA SOBRE A EXPOSIÇÃO A INTIMIDADE NA INTERNET.

1. Influenciadores Sthefane Matos e Victor Igoh: Em 2020, os influenciadores Sthefane Matos e Victor Igoh tiveram um vídeo íntimo exposto após a conta do iCloud de Sthefane ser acessada por alguém que conhecia sua senha. Além de divulgar o vídeo, o invasor apagou fotos, mensagens e contatos. Apesar da gravidade do caso, até o momento, o responsável não foi punido, evidenciando as falhas na aplicação das leis e na proteção das vítimas. (UOL: Disponível em: Sthe Matos e Victor Igoh confirmam vídeo íntimo vazado na internet: que leis os defendem?)
2. Caso Carolina Dieckmann: Em 2012, a atriz teve 36 fotos íntimas vazadas na internet após ser vítima de um ataque hacker. Criminosos invadiram seu computador, roubaram os arquivos pessoais e tentaram chantageá-la, exigindo dinheiro para não divulgar as imagens. Carolina se recusou a pagar e denunciou o caso à polícia, o que gerou grande

repercussão na mídia e mobilizou o debate sobre a necessidade de leis mais rigorosas contra crimes digitais. (Brasil Paralelo: disponível em: Lei Carolina Dieckmann faz 13 anos)

5. ESTELIONATO

A palavra estelionato se origina do termo latim *"stelionatus"*, que deriva de *"stellio"*, que significa "lagarto" (Dicionário Houaiss da Língua Portuguesa, 2001). A palavra Stellio, em seu sentido figurado ou metafórico, está relacionada à ideia de fraude ou de engano, pois, o lagarto era associado e visto como um animal perspicaz e engenhoso.

Sendo um dos crimes digitais ou cibernéticos mais frequentes no cotidiano, superando até mesmo o crime de roubo, (Anuário Brasileiro de Segurança Pública, 2023) o estelionato se caracteriza pela vantagem ilegal por meio de fraudes, ocasionando prejuízo a outra, o estelionatário tem sempre a intenção e o dolo. A vítima é enganada, sendo provocada na maioria das vezes a agir pela emoção, diminuindo assim a sua capacidade de tomar decisões e de ter reações lógicas quando o agente está cometendo o delito, os criminosos utilizam da engenharia social, como por exemplo o golpe de um falso sequestro de um familiar ou de alguém próximo.

O golpe mais comum é o do WhatsApp hackeado, onde o criminoso se passa pela vítima pedindo dinheiro aos familiares, e após a consumação do crime, some sem deixar rastros, dificultando não somente a responsabilização pelo ato ilícito cometido pelo mesmo, como também a reparação do dano à vítima.

Sendo assim, no estelionato, é necessário para sua atuação, quatro elementos, quais são: Vantagem ilícita para o agente; prejuízo a vítima; uso de fraude e o nexo causal entre a fraude e o prejuízo.

A base normativa para o crime de estelionato no Brasil é o artigo 171 do Código Penal, de 1940, que assegura:

> Art. 171. Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis. (Vide Lei nº 7.209, de 1984)
> § 1º - Se o criminoso é primário, e é de pequeno valor o prejuízo, o juiz pode aplicar a pena conforme o disposto no art. 155, § 2º.
> § 2º - Nas mesmas penas incorre quem:
> Disposição de coisa alheia como própria
> I - vende, permuta, dá em pagamento, em locação ou em garantia coisa alheia como própria;
> Alienação ou oneração fraudulenta de coisa própria

II - vende, permuta, dá em pagamento ou em garantia coisa própria inalienável, gravada de ônus ou litigiosa, ou imóvel que prometeu vender a terceiro, mediante pagamento em prestações, silenciando sobre qualquer dessas circunstâncias;
Defraudação de penhor
III - defrauda, mediante alienação não consentida pelo credor ou por outro modo, a garantia pignoratícia, quando tem a posse do objeto empenhado;
Fraude na entrega de coisa
IV - defrauda substância, qualidade ou quantidade de coisa que deve entregar a alguém;
Fraude para recebimento de indenização ou valor de seguro
V - destrói, total ou parcialmente, ou oculta coisa própria, ou lesa o próprio corpo ou a saúde, ou agrava as consequências da lesão ou doença, com o intuito de haver indenização ou valor de seguro;
Fraude no pagamento por meio de cheque
VI - emite cheque, sem suficiente provisão de fundos em poder do sacado, ou lhe frustra o pagamento.
Fraude eletrônica
§ 2º-A - A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo. (Incluído pela Lei nº 14.155, de 2021)
§ 2º-B - A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional. (Incluído pela Lei nº 14.155, de 2021)
§ 3º - A pena aumenta-se de um terço, se o crime é cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência. Estelionato contra idoso ou vulnerável (Redação dada pela Lei nº 14.155, de 2021)
§ 4º - A pena aumenta-se de 1/3 (um terço) ao dobro, se o crime é cometido contra idoso ou vulnerável, considerada a relevância do resultado gravoso. (Redação dada pela Lei nº 14.155, de 2021)
§ 5º - Somente se procede mediante representação, salvo se a vítima for: (Incluído pela Lei nº 13.964, de 2019)
I - a Administração Pública, direta ou indireta; (Incluído pela Lei nº 13.964, de 2019)
II - criança ou adolescente; (Incluído pela Lei nº 13.964, de 2019)
III - pessoa com deficiência mental; ou (Incluído pela Lei nº 13.964, de 2019) IV - maior de 70 (setenta) anos de idade ou incapaz. (Incluído pela Lei nº 13.964, de 2019)
Art. 171-A. Organizar, gerir, ofertar ou distribuir carteiras ou intermediar operações que envolvam ativos virtuais, valores mobiliários ou quaisquer ativos financeiros com o fim de obter vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil ou qualquer outro meio fraudulento. (Incluído pela Lei nº 14.478, de 2022) Pena - reclusão, de 4 (quatro) a 8 (oito) anos, e multa. (Incluído pela Lei nº 14.478, de 2022)

5.1. NOTÍCIAS SOBRE O CRIME DE ESTELIONATO

1. Polícia investiga empresa de veículos acusada de estelionato em BH**:** Polícia civil de MG investiga empresa de veículos acusada de praticar estelionato contra os clientes. Entre as denúncias, a empresa basicamente recebia veículos consignados para terceiros e não repassava os valores para os proprietários. A loja fechou com dezenas de transações em aberto e sem a quitação das dívidas existentes, os novos compradores e vendedores saiam prejudicados. (CNN Brasil, 2025: disponível em: **:**

https://www.cnnbrasil.com.br/nacional/sudeste/mg/policia-investiga-empresa-de-veiculos-acusada-de-estelionato-em-bh/)

2. Quadrilha de estelionato é presa em "escritório do crime" no litoral de SP**:** A Polícia Civil prendeu sete pessoas em flagrante em Guarujá, São Paulo, por estelionato e organização criminosa. O grupo operava em um "escritório do crime" voltado a aplicar golpes telefônicos e pela internet. Entre as práticas identificadas estavam *phishing,* falsificação de documentos, falso telemarketing e fraudes relacionadas a internet banking. A operação revelou a estrutura organizada para captar informações sigilosas e enganar vítimas, reforçando os perigos das fraudes digitais e a importância de estratégias para combatê-las. (**Fonte:** G1, 2023. Disponível em: **https://g1.globo.com/sp/santos-regiao/noticia/2023/11/07/policia-prende-sete-pessoas-em-escritorio-do-crime-em-guaruja-sp.ghtml**)

6. AS DEFICIÊNCIAS LEGISLATIVAS

6.1. CRIMES CONTRA A HONRA - MUNDO DIGITAL.

Vivendo num mundo eminentemente digital, ofensas ao ordenamento jurídico passam também a figurar em âmbitos não previstos originalmente na letra da lei.

Em 2014, a União Europeia sancionou a lei do "Direito ao Esquecimento", que garante que links de sites que contenham informações desatualizadas ou que não condizem com a realidade possam ser removidos se um dos indivíduos citados nos referidos textos apresentem o pedido de retirada do conteúdo. Em 2021, o tema foi debatido entre os magistrados do Supremo Tribunal Federal, porém, foi julgado inconstitucional e, portanto, inaplicável ao Brasil.

Mas enquanto no velho mundo se discute a remoção de um conteúdo após sua queixa, no Brasil, ainda pouco habituado à prevenção destes crimes, uma das principais dificuldades ainda está no combate rápido das ofensas propagadas digitalmente.

Em 5 de maio de 2014, Fabiane Maria de Jesus, moradora da cidade de Guarujá no litoral de SP foi espancada e morta em decorrência de um linchamento que sofreu, após ser confundida com uma suposta 'feiticeira' que faria sacrifícios rituais com crianças. A notícia, comprovadamente falsa, havia circulado no Facebook nos dias anteriores, contendo um suposto retrato falado.

Quase 11 anos depois, segundo matéria divulgada no site G1, em matéria de 2022, a defesa de Fabiane e sua família tenta, ainda sem sucesso, uma indenização por parte da rede social que não providenciou a retirada do conteúdo na altura.

A legislação brasileira não prevê que as plataformas digitais que propaguem conteúdos que podem ser potencialmente ofensivos ou, como no caso de Fabiane, fatalmente danosos, respondam por permitir o uso de suas respectivas plataformas para a disseminação de conteúdo difamatório ou ofensivo. Denota-se, portanto, o atraso legal brasileiro no que tange a prevenção destes casos, tanto mais, porém, na punição e reparação destes.

É mister ao país, que graças ao apogeu tecnológico torna-se cada vez mais digitalmente integrado, espelhar-se em exemplos eficientes do âmbito externo, embora sempre aplicando as mesmas soluções de forma não conflitante com sua própria realidade.

Muitos podem questionar se esse realmente seria um caso de urgência no país, que enfrenta problemáticas crônicas nos mais diferentes setores da sociedade. Porém, o adiamento da ação pode necessariamente implicar na não-ação, retardando o progresso da legislação e da segurança dos cidadãos, enquanto amplia-se a cada vez mais o acesso à replicação destes crimes.

Mas, ainda que haja outros setores carentes de atenção na sociedade brasileira, não se pode negar a nítida desconsideração do princípio da dignidade, inerente a todo ser humano, que não se faz respeitar dada a omissão do país em produzir ou enrijecer as leis já vigentes sobre. Não se pode esperar que casos como os de Fabiane se repitam em nossas cidades e outras famílias passem mais de uma década sem indenização ou reparação. Casos como o de Fabiane terminaram com seu lamentável assassinato, mas, quantos outros brasileiros não tiveram também sua respectiva dignidade manchada, impactando negativamente de forma direta suas vidas? Não é, pois, a dignidade da pessoa humana um dos fundamentos da República, conforme o ART. 1º, inciso III de nossa Carta Magna? Que se exija a boa aplicação dos princípios constitucionais que conduzem a nação e se conscientize a população sobre os seus direitos de defesa da dignidade pessoal, a fim de salvaguardar a vivência digna de todos os brasileiros.

6.2. INVASÃO INFORMÁTICA - DEFICIÊNCIA LEGISLATIVA - AUSÊNCIA DE LEIS ESPECÍFICAS.

A legislação deve ser objetiva, sem desvios, clara e extremamente detalhada, já que a sua função é regular a convivência em sociedade. Portanto, a presença de leis específicas é

indiscutível, pois são essenciais para regulamentar áreas concretas e garantir a aplicação adequada de normas em situações particulares, porém, infelizmente, os regulamentos relacionados com a área digital que estão em vigor, foram elaborados de maneira apressada, sem atenção aos detalhes e à execução cuidadosa, direcionando o foco para caso do cotidiano, negligenciando casos complexos com alto grau de periculosidade, como a invasão de sistema Aeros.

Recentemente, apontado pela *InfoSecurity Magazine*, "os sistemas de comunicação e entretenimento a bordo das aeronaves, conectados a redes externas, podem ser alvos para hackers, comprometendo a segurança e o controle de voo" (InfoSecurity Magazine, 2022).

As invasões informáticas, embora pouco comentadas, têm grande importância na vida dos cidadãos devido às suas implicações ilícitas, e pela falta de punibilidade para os infratores que efetuam ataques cibernéticos na aviação. Os avanços tecnológicos, modificaram de maneira positiva, o sistema aeronáutico se transformando em um sistema de alta tecnologia, movido por software, hardware especializado, redes de comunicação e bancos de dados para gerenciar e processar informações. Entretanto, quando o sistema aeronáutico sofre qualquer tipo de exploração na vulnerabilidade digital, inúmeras pessoas que utilizam o transporte aéreo para se locomover estão expostas a risco à sua segurança.

A matéria "É possível hackear um avião?", publicada no **UOL** em 27 de agosto de 2018, retrata os riscos de ataques cibernéticos em aeronaves e discute a vulnerabilidade das tecnologias usadas em aviões, especialmente os sistemas de navegação e comunicação. Logo, é evidente que a segurança no sistema aeronáutico possui aspectos fundamentais que exigem regulamentos específicos para evitar calamidades futuras, logo, a ausência de leis específicas que trate da segurança cibernética nas aeronaves é um dos exemplos das lacunas existentes em relação ao conjunto de normas que regulam o mundo digital.

6.3. EXPLORAÇÃO SEXAL INFANTOJUVENIL DIGITAL RESPONSABILIDADE DOS PROVEDORES.

No Brasil, o Marco Civil da Internet e outras legislações, como a Lei Geral de Proteção de Dados (LGPD) e, estabelecem diretrizes importantes para a proteção de dados e a responsabilização de provedores.

A Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018) diz que:

> Art. 14: Estabelece que o tratamento de dados pessoais de crianças deve ser realizado com o consentimento específico de pais ou responsáveis, assegurando o "melhor interesse da criança.

E Marco Civil da Internet (Lei nº 12.965/2014) no mesmo sentido assegura:

> Art. 7º: Garante a proteção à privacidade e aos dados pessoais de todos os usuários da internet.
> Art. 29: Reafirma o controle parental, permitindo que os responsáveis bloqueiem ou limitem o acesso a conteúdos prejudiciais.

Entretanto, ao contrário de nações como os Estados Unidos, onde as empresas são obrigadas a reportar casos de exploração sexual infantil encontrados em suas plataformas, as legislações brasileiras ainda não estabelecem de forma clara a responsabilidade dos provedores em monitorar e relatar práticas criminosas.

Especialistas defendem que a implementação de uma legislação mais rigorosa, inspirada em exemplos internacionais, poderia exigir que plataformas como redes sociais e serviços de hospedagem utilizem algoritmos mais eficazes para detectar e bloquear conteúdos ilegais. Embora tenha havido progressos na legislação, persistem significativos obstáculos no combate à exploração sexual infantil. A falta de uma uniformização nacional para a identificação e registro de crimes sexuais torna difícil a formulação de políticas públicas efetivas.

Além disso, a insuficiência de formação contínua para profissionais que trabalham com crianças e adolescentes compromete a eficácia da rede de proteção. A cooperação internacional se revela essencial. Atos de cibercrime, como a pornografia infantil e o tráfico de menores, frequentemente se conectam a redes globais, o que demanda a colaboração entre diferentes governos e instituições para a identificação e penalização dos perpetradores. Essa revisão na legislação seria um passo significativo no enfrentamento da exploração sexual infantil no meio digital.

6.4. EXPOSIÇÃO DA INTIMIDADE SEXUAL - RESPONSABILIZAÇÃO DOS PARTICIPANTES.

Embora a legislação atual seja crucial para a criminalização dessa ação, ela não possui mecanismos mais sólidos para assegurar a responsabilização dos participantes. A identificação dos responsáveis pelo delito e a eliminação imediata do material divulgado ainda encontram obstáculos técnicos e burocráticos, especialmente levando em conta a diversidade de plataformas online e a privacidade oferecida por algumas tecnologias. Ademais, as penalidades estabelecidas no artigo 216-B, que vão de seis meses a um ano de prisão, juntamente com a

imposição de multa, têm recebido críticas por não terem um caráter suficientemente repressivo ou dissuasivo para prevenir a ocorrência deste delito. Por exemplo, não existe uma determinação legal explícita que force essas empresas a eliminarem o material rapidamente ou a implementar mecanismos que compliquem sua distribuição.

Também é delicado preservar a identidade das vítimas. Apesar de a lei proibir a divulgação de informações pessoais em processos judiciais ligados a delitos íntimos, na realidade, muitas vítimas ainda passam por constrangimentos, o que desencoraja a procura por justiça. Assim, a insuficiência legislativa na luta contra a exposição da intimidade sexual demanda um esforço constante de melhoria.

6.5. ESTELIONATO - DEFICIÊNCIA LEGISLATIVA.

O estelionato, como a maioria dos crimes digitais, carece de atenção em relação às suas deficiências legislativas contra o acompanhamento do avanço da tecnologia e a velocidade em que as informações se propagam, além do que, criminosos a utilizam de forma ilícita a fim de cometer delitos. Tanto no âmbito digital da prevenção quanto da punição em si, é perceptível a dificuldade de se chegar ao autor do crime, sendo um ponto extremamente negativo, devido a facilidade que o agente tem de se camuflar entre o crime e a lei, evidenciando uma vulnerabilidade transparente no sistema penal brasileiro em contrapartida às mídias sociais.

Embora haja leis específicas, como por exemplo, a Lei Geral de Proteção de Dados (LGPD), que são importantes no combate ao crime cibernético, elas por si só não alcançam todas as lacunas presentes nesse cenário, uma vez que, não supre a necessidade de uma regulamentação mais severa, concreta e adequada para casos específicos como esses de âmbito virtual. (Portal jurídico com conteúdo produzido por advogados e juristas. Disponível em: **https://www.migalhas.com.br/coluna/crimes-ciberneticos/388916/crimes-ciberneticos-e-as-lacunas-na-legislacao**)

A legislação tradicional frequentemente se mostra ineficiente no combate de crimes digitais, demonstrando a urgência de medidas que se adaptem ao avanço tecnológico, de meios que responsabilizem os criminosos e que a vítima tenha seu dano reparado de maneira ágil e efetiva.

CONCLUSÃO

Conclui-se que, embora o Brasil tenha avançado no desenvolvimento de legislações voltadas à proteção digital, como o Marco Civil da Internet e a Lei Geral de Proteção de Dados (LGPD). ainda existem brechas que comprometem a eficácia no combate aos crimes cibernéticos. A pesquisa destaca a necessidade urgente de reformulação e aprimoramento do arcabouço legal brasileiro, visando garantir maior proteção à sociedade e ao Estado frente ao avanço tecnológico e ao crescimento de práticas ilícitas no ambiente digital.

A análise das lacunas legais, aliada à promoção de uma conscientização pública sobre os riscos do crime digital, demonstra que uma atuação legislativa mais sólida deve ser acompanhada pela formação de profissionais capacitados para lidar com essas infrações. A implementação de leis mais abrangentes, a capacitação de operadores do direito e especialistas em segurança cibernética, e o engajamento social em torno do tema são passos cruciais para mitigar os danos causados por criminosos digitais e assegurar uma resposta eficaz do Estado a essas ameaças.

Assim, espera-se que o presente estudo contribua para o fortalecimento do debate acadêmico e jurídico sobre cibersegurança e que impulsione iniciativas legislativas, institucionais e sociais voltadas a uma maior proteção no ambiente digital. Dessa forma, a pesquisa busca colaborar com a construção de um sistema jurídico e social mais seguro, alinhado às demandas e desafios impostos pelo cenário digital contemporâneo.

REFERÊNCIAS.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Código Penal.** Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 27 jan. 2025.

CONJUR. **Responsabilidade dos provedores de internet no combate à exploração sexual infantil.** Disponível em: https://www.conjur.com.br/2024-out-27/responsabilidade-dos-provedores-de-internet-no-combate-a-exploracao-sexual-infantil/. Acesso em: 28 dez. 2024.

CNN BRASIL**. Polícia investiga empresa de veículos acusada de estelionato em BH.** Disponível em: https://www.cnnbrasil.com.br/nacional/sudeste/mg/policia-investiga-empresa-de-veiculos-acusada-de-estelionato-em-bh/. Acesso em: 29 jan. 2025**.**

CONRAD, Camila; AZEREDO, Paula Prestes**. Crimes virtuais contra crianças e adolescentes e medidas de prevenção.** Editora: **Viseu.**

FIGUEIREDO, Karina Correia**. Abuso e exploração sexual infantojuvenil na Internet:** uma análise do fluxo e da percepção dos policiais civis acerca do enfrentamento no Pará. 2020. Dissertação (Mestrado em Segurança Pública) – Programa de Pós-Graduação em Segurança Pública, Universidade Federal do Pará, Belém, 2020.

FOLHA DE S. PAULO**. Como prevenir o abuso sexual infantojuvenil na internet.** Disponível em: https://www1.folha.uol.com.br/seminariosfolha/2024/11/como-prevenir-o-abuso-sexual-infantojuvenil-na-internet.shtml. Acesso em: 17 jan. 2025.
G1 SANTOS**. Oito anos após mulher ser espancada até a morte em SP, fake news segue fazendo vítimas como turista queimado vivo no México. Por G1 Santos.** Disponível em: https://g1.globo.com/sp/santos-regiao/noticia/2022/06/15/oito-anos-apos-mulher-ser-espancada-ate-a-morte-em-sp-fake-news-segue-fazendo-vitimas-como-o-turista-queimado-vivo-no-mexico.ghtml. Acesso em: 27 jan. 2025.

G1 SANTOS E REGIÃO**. Polícia Civil prende quadrilha em flagrante por estelionato em escritório do crime no litoral de SP.** Disponível em: https://g1.globo.com/sp/santos-regiao/noticia/2024/10/11/policia-civil-prende-quadrilha-em-flagrante-por-estelionato-em-escritorio-do-crime-no-litoral-de-sp.ghtml. Acesso em: 28 jan. 2025.

HAIDT, Jonathan; LUKIANOFF, Greg. **A Geração Ansiosa: como o bom senso e a liberdade de expressão podem combater a intolerância e o medo nas universidades.** Tradução de George Schlesinger. São Paulo: Três Estrelas, 2019.

NAÇÕES UNIDAS. ONU **Plano global para proteger crianças da violência sexual e do tráfico na internet.** Disponível em: https://news.un.org/pt/story/2024/10/1839006. Acesso em: 20 out. 2024.

O'FLAHERTY, K. **In-Flight Cyber-Attacks.** Disponível em: https://www.infosecurity-magazine.com/magazine-features/in-flight-cyberattacks/. Acesso em: 29 jan. 2025.
RODRIGUES, Eliete Matias. Desafios no combate à exploração sexual de crianças e adolescentes. Editora: Dialética. Cidade: São Paulo. Ano: 2021.

SAFERNET**. SaferNet recebe recorde histórico de novas denúncias de imagens de abuso e exploração sexual.** Disponível em: https://new.safernet.org.br/content/safernet-recebe-recorde-historico-de-novas-denuncias-de-imagens-de-abuso-e-exploracao-sexual. Acesso em: 20 out. 2024.

SUPREMO TRIBUNAL FEDERAL**. STF conclui que direito ao esquecimento é incompatível com a Constituição Federal.** Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=460414&ori=1. Acesso em: 27 jan. 2025.

TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAPÁ**. Crimes contra a honra em redes sociais: juiz Diego Moura orienta a população a como proceder nesses casos.** Disponível em: https://www.tjap.jus.br/portal/noticias/crimes-contra-a-honra-em-redes-sociais-juiz-diego-moura-orienta-a-populacao-a-como-proceder-nesses-casos.html. Acesso em: 27 jan. 2025.

VICENTE, J. P. **EUA dizem que é uma questão de tempo até um avião ser hackeado; entenda.** Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2018/08/27/e-possivel-hackear-um-aviao.htm. Acesso em: 29 jan. 2025.