PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO

PUC-SP

Gabriel Eduardo Jasponte Rosa

Estudo da evolução dos Crimes Virtuais: Uma Análise do Impacto da Tecnologia na Criminalidade em Consonância com a Proporcionalidade na Tutela Penal

Trabalho de Conclusão de Curso em Direito

São Paulo

2025

Gabriel Eduardo Jasponte Rosa

Estudo da evolução dos Crimes Virtuais: Uma Análise do Impacto da Tecnologia na Criminalidade em Consonância com a Proporcionalidade na Tutela Penal

Monografia apresentada ao Curso de Direito da Pontifícia Universidade Católica de São Paulo como um dos pré-requisitos para obtenção do título de Bacharel em Direito sob orientação do Prof Dr. Motauri Ciocchetti de Souza

São Paulo

2025

Resumo

O avanço das tecnologias digitais e a popularização da internet têm gerado um novo cenário de criminalidade, caracterizado pelos crimes virtuais. Este estudo analisa a evolução desses delitos, abordando suas principais modalidades, classificação e as implicações jurídicas de sua tipificação. Embora o Código Penal brasileiro tenha se adaptado parcialmente a criação de legislações específicas, como a Lei 12.735/2012 (Lei Carolina Dieckmann) e a Lei 12.965/2014 (Marco Civil da Internet) é fundamental para o enfrentamento da criminalidade digital. O trabalho destaca a importância do princípio da proporcionalidade na aplicação da legislação penal, buscando equilibrar a repressão à criminalidade com a proteção de direitos fundamentais. A pesquisa analisa os desafios enfrentados pela legislação brasileira na proteção contra crimes virtuais e propõe uma reflexão crítica sobre a resposta penal diante da expansão do ciberespaço.

Palavras-chave: crimes virtuais; direito penal; internet; legislação; proporcionalidade.

Abstract

The advancement of digital technologies and the popularization of the internet have created a new landscape of criminality characterized by virtual crimes. This study analyzes the evolution of these offenses in Brazil, addressing their main modalities, classification, and the legal implications of their typification. Although the Brazilian Penal Code has partially adapted, the creation of specific legislations, such as Law 12.735/2012 (Carolina Dieckmann Law) and Law 12.965/2014, is fundamental for combating digital criminality. The work highlights the importance of the principle of proportionality in the application of penal legislation, seeking to balance the repression of crime with the protection of fundamental rights. The research, employing a qualitative approach, examines the challenges faced by Brazilian legislation in protecting against virtual crimes and proposes a critical reflection on the effectiveness of penal responses in the face of the expansion of cyberspace.

Keywords: criminal law; internet; legislation; proportionality; virtual crimes.

AGRADECIMENTOS.

Dedico este trabalho, primeiramente, aos meus pais, que sempre acreditaram em mim e me mostraram, com seu exemplo, o valor da dedicação, da ética e do esforço diário. Ao meu irmão, pela amizade, companheirismo e incentivo em cada etapa dessa caminhada. À minha família como um todo, que esteve presente em todos os momentos, oferecendo apoio, carinho e compreensão. Dedico também aos meus amigos, que com palavras de motivação e gestos de companheirismo tornaram a jornada mais leve.

Ao meu orientador, pela dedicação, disponibilidade e orientação segura, que foram essenciais para a realização deste trabalho.

Por fim, agradeço a todos que, direta ou indiretamente, fizeram parte dessa caminhada e colaboraram para a concretização deste trabalho.

LISTA DE ABREVIATURAS E SIGLAS.

T&T – American Telephone and Telegraph Company (Companhia Americana de Telefonia e Telégrafo)

ARPANET – Advanced Research Projects Agency Network (Rede da Agência de Projetos de Pesquisa Avançada)

COACRIM – Centro de Apoio Operacional Criminal

COECIBER – Coordenadoria Estadual de Combate aos Crimes Cibernéticos

DDoS – Distributed Denial of Service (Negação de Serviço Distribuída)

LGPD – Lei Geral de Proteção de Dados

MIT – Massachusetts Institute of Technology (Instituto de Tecnologia de Massachusetts)

MPMG – Ministério Público de Minas Gerais

OCDE – Organização para a Cooperação e Desenvolvimento Econômico

SRI – Stanford Research Institute (Instituto de Pesquisa de Stanford)

STF – Supremo Tribunal Federal

UCLA – University of California, Los Angeles (Universidade da Califórnia, Los Angeles)

USP – Universidade de São Paulo

WEF – World Economic Forum (Fórum Econômico Mundial)

SUMÁRIO.

INTRODUÇÃO.

Nos últimos anos o avanço acelerado das tecnologias digitais tem transformado profundamente a maneira como nos comunicamos e interagimos com o mundo. A internet, como uma ferramenta global, criou um estágio na sociedade contemporânea, no qual surgem tanto oportunidades quanto desafios. Com a crescente digitalização de atividades cotidianas e profissionais novos tipos de crimes começaram a emergir, exigindo do Direito Penal uma adaptação constante para lidar com essas ameaças.

A cultura digital é um fenômeno em constante evolução, o que torna ainda mais complexo o entendimento e a regulamentação das práticas criminosas que se originam no ambiente virtual. O Direito Penal deve se adaptar continuamente ao avanço tecnológico, sob pena de se tornar ineficaz diante dos novos tipos de infrações. A internet, ao mesmo tempo que promove inovações, também cria um terreno fértil para atividades ilícitas. O anonimato proporcionado pelo ambiente online, aliado a tecnologias de criptografia e ocultação, contribui para a ideia de impunidade entre os infratores, que acreditam estar livres de consequências judiciais.

Embora parte desses crimes possa ser enquadrada nos tipos penais já previstos no Código Penal brasileiro, a necessidade de uma legislação mais específica tornou-se evidente. A criação de normas como a Lei 12.737/2012, conhecida como "Lei Carolina Dieckmann", foi um passo importante para enfrentar crimes virtuais, mas ainda estamos longe de uma solução definitiva. A evolução constante das tecnologias exige que o legislador acompanhe essas transformações, buscando sempre um equilíbrio entre segurança jurídica e a proteção de direitos fundamentais.

A presente pesquisa visa analisar como o Direito Penal brasileiro tem respondido aos desafios impostos pelos crimes virtuais, focando na evolução dos “Cibercrimes” junto ao princípio da proporcionalidade na aplicação da legislação penal.

CAPÍTULO 1.

INTERNET E SURGIMENTO DO CRIME VIRTUAL.

1.1 O surgimento da internet.

[1]A internet, que nos dias de hoje é uma parte muito importante da nossa vida cotidiana, se formou na década de 1960. [2]A “Arpanet” Foi criada naquele período para enviar informações entre centros de pesquisa e instalações militares com foco em específico no Pentágono. No início o objetivo era garantir uma comunicação eficaz em um âmbito de segurança nacional, especialmente durante a guerra fria.

A primeira mensagem enviada entre computadores da Universidade da Califórnia em Los Angeles (UCLA) e do Instituto de Pesquisa de Stanford (SRI) foi um Marco muito importante nesse desenvolvimento. Um simples “login” constitui essa comunicação e representou o início de uma Nova Era de conexão

Na década de 1980, a internet abriu espaço para aplicações comerciais e pessoais, isso deu um passo além do uso acadêmico e militar, que inicialmente eram o motivo de sua criação. Essa mudança foi extremamente importante já que proporcionou que empresas e indivíduos se conectassem de uma maneira mais ampla.

O Brasil fez sua entrada nesse cenário em 1988, quando a internet foi oficialmente introduzida no país. Contudo, foi em 1994 que o uso da rede foi liberado para o público em geral, permitindo que milhões de brasileiros utilizassem essa nova ferramenta de comunicação. Desde então, a internet se consolidou como um elemento essencial da sociedade, transformando a forma como as pessoas se comunicam, trabalham e consomem informações.

Hoje, a internet é o principal meio de comunicação global, com mais de 5 bilhões de usuários. Essa vasta rede não apenas facilita a comunicação instantânea, mas também democratiza o acesso à informação, mas também surgem novas formas de criminalidade.

---

[1] SILVA, Daniel Neves. "História da internet"; Brasil Escola

[2] Bello, Elena. "Conoce la historia de Internet desde su primera conexión hasta hoy." IEBSchool.

O ambiente digital, com sua natureza anônima e acessível, se tornou um terreno fértil para atividades ilícitas. Assim, é fundamental relacionar a evolução da internet com o surgimento do crime na internet se relaciona com a evolução

1.2 Surgimento do crime na internet.

[3]De acordo com Damásio de Jesus e José Antônio Milagre, já em 1939, muito antes da internet se tornar o que conhecemos atualmente, havia relatos de que Alan Turing, um matemático e cientista da computação britânico, foi recrutado pelo governo dos Estados Unidos para investigar a quebra de códigos com o objetivo de proteger informações.

Décadas de 1960-1970: Os Primórdios Técnicos.

[4]Segundo o site Arctic Wolf, o cibercrime tem raízes profundas no desenvolvimento da própria tecnologia computacional. Nos anos 1960, quando a internet ainda era um projeto militar (ARPANET), ocorreram as primeiras transgressões digitais documentadas. O evento marcante de 1962, quando Allen Scherr comprometeu os sistemas do MIT para roubar senhas usando cartões perfurados, revelou pela primeira vez como sistemas computacionais poderiam ser explorados para fins ilícitos.

Na década seguinte, em 1971, o pesquisador Bob Thomas criou o Creeper, um programa experimental que se autorreplicava entre mainframes (processadores de quantidades enormes de informações e operações críticas) conectados à ARPANET. Apesar de não ser malicioso por natureza (apenas exibia a mensagem *"I'M THE CREEPER: CATCH ME IF YOU CAN - EU SOU O CREEPER: ME PEGUE SE FOR CAPAZ"*), este foi o precursor tecnológico dos futuros vírus (Programa malicioso que se replica e se espalha por sistemas). Em 1979, um programador da Apple escreveu o primeiro vírus para microcomputadores, demonstrando que a ameaça não se limitaria mais a mainframes institucionais.

---

[3] JESUS, Damásio de; MILAGRES, José Antônio. Manual de Crimes Informáticos. 1ª Edição. ed. São Paulo: Saraiva, 2016. 231 p. ISBN 978850262724-6.

[4] ARCTIC WOLF. A Decade of Cybercrime. [S.l.]: Arctic Wolf, [s.d.].

Esse acontecimento revelou falhas na segurança de sistemas compartilhados. Então, existiu uma necessidade de estimular um desenvolvimento de antivírus, protocolos básicos de segurança e necessidade de políticas de uso aceitável.

Anos 1980: O Nascimento do Cibercrime Moderno.

A década de 1980 assistiu à profissionalização da atividade cibercriminosa, coincidindo com a popularização dos computadores pessoais. Em 1981, Ian Murphy ganhou notoriedade como primeiro condenado por crime digital nos EUA, ao invadir sistemas da AT&T para alterar horários de cobrança. O caso provou que ações digitais poderiam ter repercussões legais.

Em 1983, o termo "hacker" entrou para o léxico popular, e dois anos depois surgiu o primeiro caso internacional de espionagem digital, com hackers alemães invadindo sistemas americanos para vender segredos ao serviço secreto soviético. Mas o divisor de águas foi 1988, quando o [5]Morris Worm (Tipo de malware que se replica automaticamente e se espalha por redes), [6]um malware (Software malicioso projetado para causar danos, roubar informações ou comprometer sistemas) criado acidentalmente por um estudante de Cornell, infectou 10% dos computadores conectados à internet primitiva, cerca de 6.000 máquinas, causando prejuízos milionários.

Nesta década houve os primeiros grandes debates sobre ética e regulamentação digital. Também ocorreu a adoção da Lei de Fraude e Abuso Computacional nos EUA (1986)

Anos 1990: Era da Comercialização.

A explosão da internet comercial transformou radicalmente o cenário do cibercrime. Com a popularização do e-mail e da web, os ataques deixaram de ser técnicas de nicho para se tornarem ferramentas de crime organizado. Vladimir Levin

[5] FBI. Famous Cases & Criminals. Washington, D.C.: Federal Bureau of Investigation, [s.d.].
[6] SCHNEIDER, J. The History of Malware | IBM.

marcou a década ao roubar US$10 milhões do Citibank em 1995, o primeiro grande assalto bancário digital.

O vírus Melissa (1999) estabeleceu novos paradigmas: pela primeira vez um malware combinava infecção de documentos Word com propagação automática por e-mail, causando prejuízos globais de US$80 milhões. Enquanto isso, Kevin Mitnick tornou-se o hacker mais famoso do mundo por invadir sistemas como os da Motorola e Nokia através de engenharia social (Técnica de manipulação psicológica usada para enganar pessoas e obter informações confidenciais).

Anos 2000: Sofisticação e Escala Global.

A primeira década do século XXI viu o cibercrime atingir maturidade operacional. Em 2000, o ataque DDoS (Ataque distribuído que sobrecarrega um servidor ou rede com tráfego excessivo, tornando-o inacessível) coordenado por "Mafiaboy" (um adolescente canadense) derrubou gigantes como Yahoo!, Amazon e CNN, demonstrando a vulnerabilidade da nova economia digital. Nesse mesmo ano, o worm ILOVEYOU tornou-se o primeiro ataque verdadeiramente global, infectando 10% dos computadores conectados à internet e causando prejuízos estimados em US$15 bilhões.

Em 2008, a violação da Heartland Payment Systems expôs dados de 134 milhões de cartões de crédito, revelando falhas graves na segurança de pagamentos digitais.

Esse período marcou uma profissionalização dos grupos criminosos, uma exploração de vulnerabilidades em sistemas financeiros e o início dos primeiros grandes debates sobre privacidade digital.

2010-2020: A Era Industrial do Crime Digital.

A segunda década do século marcou a transformação do cibercrime em uma verdadeira economia paralela.

O surgimento de criptomoedas facilitou o anonimato de pagamentos, catalisando o crescimento do Ransomware (malware que criptografa os dados de um computador ou rede, tornando-os inacessíveis até que um resgate seja pago.) em

forma de serviço, permitindo que desenvolvedores oferecem ferramentas de ransomware para outros criminosos, permitindo que qualquer pessoa lance ataques de sequestro de dados. O worm Stuxnet (2010), desenvolvido por governos contra instalações nucleares iranianas, mostrou o potencial destrutivo da guerra cibernética.

Megavazamentos como os da Sony (2011) e Yahoo! (2013-14, com 3 bilhões de contas) tornaram a violação de dados uma epidemia global. O ransomware WannaCry (2017) e seu sucessor NotPetya devastaram sistemas em mais de 150 países, incluindo hospitais e infraestrutura crítica.

2020s: A Nova Fronteira Digital.

A pandemia acelerou exponencialmente a transformação digital, e com ela, o cibercrime. O período é marcado por ataques de extrema ousadia como o ataque à Colonial Pipeline (2021), que paralisou o abastecimento de combustível nos EUA, levando a uma declaração presidencial de emergência.

Os grupos ransomware profissionalizados como DarkSide, REvil e LockBit operam como corporações, com equipes de suporte ao "cliente" e modelos de assinatura. Em 2023, os ataques a fornecedores de nuvem e cadeias de suprimentos digitais multiplicaram-se, explorando a interdependência dos sistemas.

Damásio de Jesus e José Antônio Milagre dizem que a crescente evolução das tecnologias nas últimas décadas tem dificultado significativamente o combate a crimes virtuais, uma vez que os criminosos se adaptam rapidamente a essas inovações, aprimorando suas habilidades e desenvolvendo novas estratégias para facilitar a prática de delitos online. Eles utilizam seus conhecimentos em informática para roubar informações de usuários comuns e até de instituições públicas, visando benefícios econômicos ou entretenimento

Esse panorama ganha ainda mais força com a pesquisa nacional do Datafolha, divulgada durante o Fórum Brasileiro de Segurança Pública e destacada na matéria [7]"Celular 'rouba' 53% mais que arma", publicada pelo UOL. Segundo o levantamento, enquanto 22% dos brasileiros com 16 anos ou mais, cerca de 37 milhões, foram

[7] ROBERTO; THAIS BILENKY. Celular “rouba” 53% mais que arma, mostra pesquisa.

vítimas de crimes patrimoniais tradicionais (roubo, assalto ou furto) em um ano, 33%, ou aproximadamente 56 milhões de pessoas, sofreram golpes digitais. Além disso, 36% da população (cerca de 61 milhões de indivíduos) receberam algum tipo de assédio digital, como telefonemas, mensagens ou chamadas suspeitas.

Esses dados ilustram com clareza o deslocamento crescente da criminalidade para o ambiente virtual e evidenciam a urgência de estudos que unam análise conceitual e prática. O que antes era visto como inofensivo e um salto tecnológico sem precedentes, se mostrou também um terreno fértil para novas formas de criminalidade, transformando a internet de uma ferramenta de progresso em um campo de batalha contra ameaças invisíveis.

1.3 Necessidade de criação de leis no Brasil.

A internet chegou ao Brasil no final da década de 1980, inicialmente restrita ao ambiente acadêmico e de pesquisa. A partir da década de 1990, a internet começou a se popularizar com a criação de provedores comerciais e a expansão da infraestrutura de telecomunicações, tornando-se mais acessível ao público em geral.

O Brasil também enfrenta essas ameaças cibernéticas e não está isento delas. A crescente incidência de crimes eletrônicos e a necessidade de um conjunto legal específico para sua regulamentação e combate são claras. Contudo, a aplicação dessas leis encontra obstáculos, uma vez que a tecnologia avança a uma velocidade superior à capacidade das legislações de se adaptarem (ALMEIDA; DE OLIVEIRA, 2022, p. 277-294).

Os primeiros indícios de crimes virtuais no Brasil podem ser rastreados até a década de 1990, quando a internet começou a se popularizar. Inicialmente, os crimes eram limitados e muitas vezes relacionados a invasões de sistemas e fraudes simples. No entanto, com o aumento do acesso à internet e a evolução das tecnologias, os criminosos começaram a explorar novas oportunidades para cometer delitos.

[8]Antes mesmo que a discussão sobre crimes virtuais ganhasse a relevância atual, o Ministério Público brasileiro já demonstrava proatividade no enfrentamento

[8] MPMG, Ministério Público do Estado de Minas Gerais. Combate aos Crimes Cibernéticos.

desse novo desafio. Um marco importante ocorreu em 2008, quando o Ministério Público de Minas Gerais inovou ao criar a Coordenadoria Estadual de Combate aos Crimes Cibernéticos (COECIBER).

Esta estrutura especializada se integra ao Centro de Apoio Operacional das Promotorias Criminais (COACRIM), órgão responsável pelo suporte técnico em diversas áreas da Justiça Criminal. A COECIBER tem como objetivo central desenvolver estratégias conjuntas com os promotores de Justiça do estado, articulando ações e protocolos específicos para coibir a criminalidade digital.

Até o ano de 2012, no Brasil ainda não existia uma lei específica voltada para a tipificação de crimes virtuais. Até que em 2011, um grupo de hackers violou a intimidade da atriz Carolina Dieckman, invadiram seu computador pessoal e divulgaram suas imagens íntimas pelas redes sociais. A partir deste evento foi sancionada a Lei dos Crimes Cibernéticos (12.737/2012), conhecida como Lei Carolina Dieckmann, que tipifica atos como invadir computadores, violar dados de usuários ou “derrubar” sites. Apesar de ganhar espaço na mídia com o caso da atriz, o texto já era reivindicado pelo sistema financeiro diante do grande volume de golpes e roubos de senhas pela internet.

No mesmo ano a Lei 12.735/12 também foi sancionada, ela tipifica condutas realizadas mediante uso de sistema eletrônico, digitais ou similares que sejam praticadas contra sistemas informatizados. Essa é a lei que determina a instalação de delegacias especializadas.

Dois anos depois foi sancionado em 23 de abril de 2014, o Marco Civil da Internet, oficialmente conhecido como Lei nº 12.965. Seu debate começou em 2009 motivado pela busca por direitos e deveres claros para todos os usuários e provedores de serviços online. A lei foi impulsionada por diversos fatores, incluindo o crescimento do uso da internet, que tornou evidente a necessidade de regulamentar o uso da rede, garantindo direitos aos usuários e responsabilidades aos provedores de serviços.

CAPÍTULO 2.

CRIMES VIRTUAIS.

2.1 Conceito e Classificações.

A Constituição Federal de 1988 estabelece, no rol dos direitos e garantias fundamentais, o princípio da legalidade penal, previsto no art. 5º, inciso XXXIX, segundo o qual *"não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal*". Esse mesmo princípio é reafirmado no art. 1º do Código Penal, em vigor desde 1940: *"Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal".*

O princípio traz a ideia de que nenhuma conduta pode ser considerada criminosa, nem punida, sem que exista lei anterior que a descreva de maneira clara. Trata-se de uma garantia essencial do Estado de Direito, pois impede arbitrariedades na aplicação da lei penal.

Entretanto, a aplicação desse princípio levanta debates relevantes quando se trata de crimes virtuais. Isso porque a velocidade da transformação digital e o surgimento de novas formas de criminalidade muitas vezes antecedem a criação de tipos penais específicos, gerando lacunas legislativas e dificultando a responsabilização efetiva dos autores dessas condutas.

Não existe um consenso absoluto na doutrina jurídica sobre a definição de crime cibernético. A divergência principal reside na amplitude do conceito e no papel que a tecnologia desempenha na ação criminosa, já que a rápida evolução digital impõe constantes desafios à tipificação penal.

A Organização para a Cooperação e Desenvolvimento Econômico (OCDE) ofereceu uma definição abrangente, conceituando o crime cibernético como "*qualquer conduta ilegal, não ética ou não autorizada que envolva processamento automático de dados e/ou a transmissão de dados*" (ROSSINI, 2002b, p. 110).

[9]Doutrinadores costumam discutir sobre classificações de crimes existentes no Código Penal Brasileiro, assim, os meios utilizados para o crime, os danos

[9] GARCIA, Plínio Silva; MACADAR, Marie Anne; LUCIANO, Edimara Mezzono. A influência da injustiça organizacional na motivação para a prática dos crimes cibernéticos. Jistem usp, Brazil, vol. 15, 2018.

provocados, a natureza das ações e suas motivações são fatores adicionais para classificação do crime cibernético.

Diante das diversas discussões, prevalecem duas divisões conhecidas como: próprios e impróprios; e puros, mistos e comuns

2.1.1 Próprios e impróprios.

A complexidade surge na distinção entre duas categorias: o crime cibernético próprio e o impróprio. O crime próprio só existe no ambiente digital e, para que o criminoso seja punido, ele precisa estar claramente descrito na lei. Já o crime impróprio usa a internet como uma ferramenta para cometer delitos que já estão previstos no Código Penal, como roubo ou fraude, o que permite que o autor seja punido.

No caso de crime impróprio, um exemplo seria um golpe de phishing. O criminoso cria um e-mail falso se passando por um banco para convencer a vítima a fornecer seus dados pessoais e bancários. Em seguida, ele usa essas informações para fazer transações fraudulentas. Neste caso, o crime real não é o e-mail falso, mas sim a fraude ou o furto qualificado, crimes que já existiam antes da internet, mas que agora usam a tecnologia como meio para serem executados.

Exemplificando um tipo de conduta que acarretaria a classificação para crimes próprios, seria o cometimento do crime que traz o art.313-B, incluído no Código Penal pela lei n° 9.983, como segue: "*Art.313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente: pena- detenção, de 3 (três) meses a 2(dois) anos, e multa".*

2.1.2 Puros, mistos e comuns.

O crime cibernético puro é aquele em que a ação, por si só, já é o delito e o alvo é o próprio computador. Um exemplo é a invasão de dispositivo informático, prevista no artigo 154-A do Código Penal, onde o criminoso invade um sistema para obter ou alterar dados sem autorização.

Já o crime cibernético misto tem-se o entendimento que o mundo digital é a forma indispensável para a ação delituosa se concretizar.

Por fim, o crime cibernético comum é um crime já previsto no Código Penal, mas que utiliza a tecnologia para ser executado.

2.2 Principais modalidades.

[10]Diante dos conceitos e classificações expostos em epígrafe, é fundamental entender as principais modalidades de crimes virtuais, sendo elas:

- **Crimes contra sistemas e dados.**

Caracterizam-se pela violação da integridade, disponibilidade ou confidencialidade de informações e dispositivos. Nessa modalidade, incluem-se condutas como a invasão de dispositivos informáticos (art. 154-A do Código Penal), exemplificada pelo acesso não autorizado a bancos de dados de uma empresa para subtração de informações sigilosas. Outra prática recorrente são os ataques de negação de serviço (DoS/DDoS), nos quais agentes mal-intencionados sobrecarregam servidores, como quando um site governamental recebe requisições massivas que o tornam indisponível. Embora não haja tipificação penal específica para esses ataques, eles podem ser enquadrados em tipos já existentes, como o crime de invasão de dispositivo ou o crime de dano.

- **Crimes contra o patrimônio praticados por meio digital.**

A tecnologia é utilizada como instrumento de fraude ou apropriação indevida. Incluem-se nesse grupo golpes em plataformas de comércio eletrônico, como anúncios falsos de venda de celulares em que o pagamento é recebido, mas o produto não é entregue. A chamada “clonagem” de cartões ou contas bancárias também é prática recorrente, geralmente associada a estelionato (art. 171 do CP) ou a delitos

[10] SCHAUN, Guilherme. Uma lista com 24 crimes virtuais. JusBrasil, [s.l.]

contra o sistema financeiro, quando praticada com dispositivos ou softwares maliciosos que capturam dados financeiros.

- **Crimes contra a honra na internet.**

Calúnia, difamação e injúria também podem ser cometidas em ambiente digital, sendo amplificadas pela velocidade e pelo alcance da internet, que permitem que ofensas se espalhem rapidamente.

- **Crimes contra a propriedade intelectual.**

Consistem na violação de direitos autorais e conexos. O exemplo mais comum é a distribuição não autorizada de conteúdos protegidos, como filmes e músicas, conduta prevista no art. 184 do Código Penal.

- **Crimes contra a dignidade sexual cometidos virtualmente.**

Constituem um campo de especial gravidade, pois combinam a vulnerabilidade da vítima com a ampla capacidade de alcance e disseminação das tecnologias digitais. Nessa categoria, enquadram-se condutas em que a tecnologia é utilizada para constranger, coagir ou explorar sexualmente pessoas, independentemente de contato físico direto. Exemplos recorrentes incluem o aliciamento sexual por meio de aplicativos de mensagens e redes sociais, em que o autor, muitas vezes utilizando identidade falsa, estabelece contato com a vítima para obter favores sexuais, imagens ou vídeos íntimos. Também se destacam práticas como a sextorsão, caracterizada pela obtenção de material de cunho sexual, com ou sem consentimento inicial, seguida de ameaça de divulgação.

Outras condutas incluem abusos sexuais mediados por tecnologia, nos quais o agressor induz a vítima a realizar atos sexuais diante de câmeras, gravando ou transmitindo em tempo real. Em determinados casos, essas práticas ocorrem em contexto de exploração sexual infantil, com posterior comercialização ou compartilhamento das imagens em redes ilícitas.

Outro aspecto relevante é a difusão não autorizada de conteúdo sexual de adultos, o que inclui o chamado “revenge porn” e práticas semelhantes.

- **Crimes cibernéticos de ódio e discriminação.**

Nessa categoria, meios digitais são utilizados para incitar, promover ou praticar condutas discriminatórias contra indivíduos ou grupos, com base em características como raça, cor, etnia, religião, gênero, orientação sexual, origem nacional ou condição física e mental. A natureza global e interativa da internet potencializa a disseminação desse tipo de conteúdo, permitindo que discursos ofensivos alcancem grande número de pessoas em curto espaço de tempo.

Exemplos comuns incluem a criação de páginas ou perfis destinados à propagação de ideologias racistas ou extremistas, a postagem de mensagens xenofóbicas ou homofóbicas em redes sociais e a organização de ataques coordenados contra grupos minoritários. A depender do caso concreto, essas condutas podem configurar crimes previstos na Lei 7.716/89 (crimes resultantes de preconceito) ou injúria racial (art. 140, §3º, do CP, ampliado pela Lei 14.532/23).

Por fim, é importante ressaltar que as modalidades apresentadas, ainda que abrangentes, não esgotam o rol de crimes possíveis no ambiente digital. A constante evolução da tecnologia cria oportunidades para ilícitos emergentes, como fraudes envolvendo criptoativos, utilização de “deepfakes” para manipulação de informações ou chantagem, entre outras práticas.

2.3 Dados estatístico.

Além das modalidades mais recorrentes, os dados empíricos evidenciam a real dimensão do problema. Diferentemente do senso comum, que tende a apontar os idosos como principais alvos de golpes digitais, as pesquisas demonstram outra

realidade. [11]Um levantamento do DataSenado, realizado em 2023 com quase 22 mil entrevistados, indicou que os jovens entre 16 e 29 anos representam a faixa etária mais afetada, correspondendo a 27% das vítimas. Já os idosos, com mais de 60 anos, considerados mais vulneráveis por terem ingressado no mundo digital em idade avançada, representaram apenas 16% do total. Como ressaltou o coordenador do DataSenado, Marcos Ruben de Oliveira, os resultados "*não evidenciam que os idosos sofrem mais golpes*", embora haja proporcionalmente mais jovens na população brasileira.

O mesmo estudo revelou que 24% dos brasileiros com mais de 16 anos foram vítimas de algum golpe digital, estimando-se que mais de 40 milhões de pessoas perderam dinheiro em razão de crimes virtuais. Esse cenário é confirmado pelo Anuário Brasileiro de Segurança Pública de 2024, que apontou um crescimento de 13,6% nos estelionatos digitais entre 2022 e 2023, em contraste com a redução de quase 30% nos roubos físicos a bancos e instituições financeiras. Ou seja, a criminalidade está migrando gradualmente do espaço físico para o virtual.

Os impactos econômicos também são expressivos. Apenas em 2024, as violações de dados teriam provocado prejuízos da ordem de R$ 2,3 trilhões. Esse panorama é ainda mais preocupante quando se observa o contexto regional: a América Latina figura como a região com maiores dificuldades em dar respostas a incidentes de cibersegurança, segundo a pesquisa Global Cybersecurity Outlook 2025, do Fórum Econômico Mundial (WEF). Aproximadamente 42% das organizações latino-americanas manifestaram preocupação com crimes digitais. Além disso, o levantamento evidenciou uma grave escassez de profissionais de cibersegurança, estimada em 4,8 milhões de especialistas em falta para suprir a demanda global.

Esses dados revelam não apenas a expansão quantitativa dos crimes virtuais, mas também seus reflexos sociais e econômicos, reforçando a urgência de se estudar o fenômeno sob a perspectiva jurídica e institucional.

[11] SENADO. Golpes virtuais aumentam e não fazem distinção de idade. Brasília: Senado Federal, 2025

2.4 A tipificação legal no ordenamento jurídico brasileiro.

A proteção penal sempre esteve ligada ao valor do bem jurídico em questão, se este não causa lesão ou ameaça relevante, não há necessidade de prevenção e proteção pelo ordenamento jurídico. Com o avanço da tecnologia e a presença cada vez maior da internet no dia a dia, surgiu a necessidade de criar regras de proteção, o que deu origem a um ramo em crescimento do direito focado na parte virtual.

Durante muito tempo, o Brasil não tinha leis específicas para lidar com os crimes virtuais. Até 2012, a maioria dos casos era enquadrada de forma improvisada em tipos penais já existentes, o que gerava insegurança jurídica. Essa lacuna foi parcialmente resolvida com a edição da Lei nº 12.737/2012, que incluiu no Código Penal artigos voltados diretamente aos chamados crimes cibernéticos.

O destaque da lei foi o artigo 154-A, que criminaliza a invasão de computadores, celulares e outros dispositivos, mesmo que não estejam conectados à internet, quando feita sem permissão e com o objetivo de obter, alterar ou destruir informações. O texto legal prevê pena para quem invade, mas também para quem cria ou espalha programas usados nessas práticas.

Além disso, a lei também alterou os artigos 266 e 298 do Código Penal, passando a punir de forma mais clara condutas como a interrupção de serviços de utilidade pública baseados em informática e a falsificação de cartões de crédito e débito.

[12]Segundo Harakemiv e Vieira (2014), os artigos 154-A e 154-B, presentes no título I do Código penal, não protegem apenas a honra, mas também valores como a intimidade, a vida privada, o sigilo das informações contidas em dispositivos eletrônicos e até o patrimônio do usuário que teve seus dados violados.
Em relação à autoria, qualquer pessoa pode praticar esse tipo de crime, já que se trata de um delito comum. Da mesma forma, qualquer indivíduo pode ser vítima, utilize ou não diretamente os meios digitais.

> *"No crime em questão, adicionado ao Código Penal pela Lei 12.737/12, considera-se que pode incorrer como sujeito ativo qualquer pessoa, já que o seu tipo penal não exige nenhuma*

[12] HARAKEMIW, Rafael Antônio; VIEIRA, Tiago Vidal. Crimes Cibernéticos. Anais do 2º Simpósio Sustentabilidade e Contemporaneidade nas Ciências Sociais, 2014.

> *qualidade especial do seu agente, sendo, portanto, um crime comum. Quanto ao sujeito passivo dos crimes informáticos considera-se que possa ser qualquer pessoa que utilize ou não o meio eletrônico, podendo existir mais de um indivíduo desde que tenham seus bens jurídicos ameaçados ou lesados pela mesma conduta delituosa, como por exemplo, uma série de e-mails contendo o mesmo conteúdo viral cujo objetivo é lesar quem os recebe" (HARAKEMIV; VIEIRA, 2014, p.424).*

No mesmo período, foi criada também a Lei nº 12.735/2012, voltada ao combate de crimes contra sistemas informatizados, que alterou tanto o Código Penal Militar quanto a legislação sobre práticas discriminatórias.

Pouco tempo depois, em 2014, entrou em vigor o Marco Civil da Internet (Lei nº 12.965/2014). Ele estabeleceu princípios para o uso da rede, como a liberdade de expressão e o respeito à privacidade, além de definir regras sobre guarda de dados pelos provedores e sobre o papel da administração pública na fiscalização de condutas ilegais.

CAPÍTULO 3.

O PRINCÍPIO DA PROPORCIONALIDADE.

Depois de compreender o conceito, classificações e como os crimes virtuais são tipificados no ordenamento jurídico, surge a necessidade de refletir sobre a adequação das respostas penais diante dessas condutas. É nesse contexto que se insere o princípio da proporcionalidade, funcionando como um limite e, ao mesmo tempo, como uma diretriz para o legislador e para o julgador. Ele busca assegurar que a pena seja compatível com a gravidade do delito, evitando tanto a impunidade quanto o excesso punitivo, especialmente em um cenário tão novo e dinâmico como o dos crimes virtuais.

3.1 Conceitos.

O princípio da proporcionalidade ocupa um papel central no Direito Penal, sendo considerado essencial para a preservação do Estado Democrático de Direito. Sua função é assegurar que, diante de conflitos entre direitos fundamentais, não ocorra a supressão de um deles, preservando sempre o núcleo essencial de cada direito envolvido.

[13]Segundo Chade Rezek Neto, muitos juristas entendem que a proporcionalidade se configura como um princípio de interpretação constitucional, justamente por oferecer ao intérprete um caminho para encontrar soluções práticas quando há divergências na aplicação e na proteção dos direitos fundamentais. Ele conceitua o princípio como:

> *"O princípio construtivo e fundamental, implícito e pressuposto na reunião entre Estado de Direito e Democracia, sendo sua função a de hierarquizar, em situações de conflito, os demais princípios buscando uma verdadeira idéia do Direito[...] tem grande relevância ordenando a aplicação dos princípios contidos na Constituição Federal para que haja o maior atendimento possível de certos princípios, com a mínima desatenção dos demais"*

Diante dessa perspectiva, Chade Rezek Neto ressalta que o princípio da proporcionalidade não deve ser visto apenas como uma ferramenta de interpretação constitucional. Para ele, trata-se de um verdadeiro princípio ordenador do Direito, uma

[13] Chade REZEK NETO. O Princípio da Proporcionalidade no Estado Democrático de Direito. São Paulo: Lemos & Cruz, 2004. p. 56. Idem, ibidem, p. 57.

espécie de “princípio dos princípios”, que orienta e dá fundamento à aplicação das demais normas jurídicas.

[14]E, de acordo com Dimitri Dimoulis e Leonardo Martins:

> “*A proporcionalidade deve ser entendida como elemento disciplinador do limite à competência constitucional atribuída aos órgãos estatais de restringir a área de proteção de direitos fundamentais, isto é, como resposta jurídica ao problema do vínculo do legislador aos direitos fundamentais, configurando um limite de seu poder limitador.”*

Quando se busca aplicar os princípios na prática, especialmente o da proporcionalidade no Direito Penal, é fundamental considerar a racionalidade e o respeito à dignidade humana. Isso porque o objetivo a ser alcançado só pode se realizar de forma legítima se estiver em conformidade com os princípios constitucionais.

Assim, no Direito Penal, o princípio da proporcionalidade pode ser entendido como um guia constitucional de equilíbrio e adequação, que deve orientar tanto o legislador quanto o aplicador da lei na definição e imposição da pena. A sanção deve corresponder à gravidade da infração, sem ser inferior nem exceder o dano causado à vítima. Mais do que as diferentes formas de expressão, o que realmente importa é a essência desse princípio: assegurar que a punição seja justa e compatível com o fato praticado.

3.2 O equilíbrio entre repressão criminal e proteção de direitos fundamentais.

Ao tratar dos crimes virtuais, o princípio da proporcionalidade ganha especial relevância. De um lado, está o dever do Estado de reprimir condutas lesivas que se disseminam rapidamente no ambiente digital; de outro, permanece a obrigação de assegurar direitos fundamentais como a liberdade de expressão, a privacidade e a proteção de dados pessoais.

---

[14] Dimitri DIMOULIS; Leonardo MARTINS. Teoria Geral dos Direitos Fundamentais. São Paulo: Editora Revista dos Tribunais, 2007. p. 191

O grande desafio consiste em equilibrar esses dois polos: a necessidade de punir adequadamente práticas como fraudes, invasões e ofensas virtuais sem que a repressão ultrapasse os limites da razoabilidade e acabe por violar garantias constitucionais. Em outras palavras, a tutela penal deve ser eficaz contra delitos digitais, mas sempre guiada pelo respeito à dignidade humana e à preservação das liberdades individuais.

Esse equilíbrio, porém, nem sempre é fácil de alcançar. Em muitas situações, as iniciativas de combate aos crimes virtuais geram dilemas jurídicos relevantes. Medidas como o monitoramento em massa de usuários, a quebra indiscriminada de sigilo de dados ou até mesmo o bloqueio de plataformas inteiras podem ter a intenção de reprimir ilícitos, mas também carregam o risco de afetar direitos fundamentais de pessoas que não possuem qualquer ligação com a prática criminosa. Da mesma forma, a criação de novos tipos penais voltados ao ambiente digital exige cautela, para que não se criminalizem comportamentos sociais comuns nem se restrinjam liberdades como a expressão e o acesso à informação.

Um exemplo desse debate surgiu com a proposta de triplicar a pena dos crimes contra a honra cometidos pela internet, inserida na Lei nº 13.964/2019, o chamado “Pacote Anticrime”. A medida recebeu fortes críticas da doutrina penal e acabou vetada pelo então presidente Jair Bolsonaro. Para Jacqueline Valles, mestre em Direito Penal, a alteração representaria flagrante desproporcionalidade, pois a pena poderia se tornar mais severa do que em crimes praticados com violência física, como o aborto resultante de lesão.

[15]Na mesma linha, o criminalista Bruno Salles advertiu que a previsão afrontava o equilíbrio na proteção do bem jurídico, lembrando que o Código Penal só admite hipótese semelhante de triplicação em situações extremas, como na omissão de socorro seguida de morte. Já o advogado Adib Abdouni, especialista em Direito Criminal e Constitucional, ressaltou que o Código Penal já prevê o aumento da pena quando o crime for cometido por meio que facilite sua divulgação, de modo que a

[15] CONJUR. Advogados condenam pena triplicada para crimes contra a honra na web. Consultor Jurídico, São Paulo, 19 mar. 2021

proposta seria redundante e violadora dos princípios da proporcionalidade e da ofensividade.

Por outro lado, o criminalista Conrado Gontijo, doutor em Direito Penal Econômico pela USP, destacou que o verdadeiro problema não está no tamanho da pena, mas na dificuldade de investigar e identificar os autores desses delitos, defendendo que o fortalecimento da capacidade investigativa do Estado seria a medida mais eficaz e proporcional.

Ainda nesse contexto, surgiu o Projeto de Lei 4658/24, de autoria do deputado Paulo Litro (PSD-PR), que propõe o aumento de 1/3 da pena nos casos de crimes contra a honra cometidos em plataformas digitais. O argumento central é que a internet se tornou espaço tanto de comunicação legítima quanto de práticas ilícitas, como difamação e calúnia, exigindo que o ordenamento jurídico evolua para coibir tais condutas. O projeto está em análise na Comissão de Constituição e Justiça e, se aprovado, seguirá para votação no Plenário da Câmara e, posteriormente, no Senado.

[16]Por fim, merece destaque a Lei nº 14.155/21, sancionada pelo ex-presidente Jair Bolsonaro, que ampliou penas para crimes de furto, estelionato e invasão de dispositivos eletrônicos, considerando fatores como o prejuízo econômico, a idade da vítima e o uso de servidores localizados no exterior. Essa alteração elevou, por exemplo, a pena do crime de invasão de dispositivo informático de detenção de 3 meses a 1 ano para reclusão de 1 a 4 anos, demonstrando a tentativa do legislador de adequar a sanção à gravidade da conduta, em consonância com o princípio da proporcionalidade. Para Luiz Augusto D'Urso, advogado especialista em Direito Digital, as novas penas representam uma resposta penal mais equilibrada e pedagógica, sobretudo em delitos que envolvem idosos ou pessoas vulneráveis, reforçando a ideia de que a punição deve corresponder ao impacto real do delito, e não ser meramente abstrata ou excessivamente punitiva.

[16] MIGALHAS. Lei que torna crimes cometidos pela internet mais graves é sancionada. Migalhas, [s.l.].

3.3 O risco do excesso punitivo e da proteção penal insuficiente.

[17]O princípio da proporcionalidade, ao ser aplicado no Direito Penal, revela dois desdobramentos essenciais para a manutenção do equilíbrio entre a tutela de bens jurídicos relevantes e a preservação das liberdades individuais: a proibição do excesso (*Übermassverbot*) e a proibição da proteção deficiente (*Untermassverbot*). Ambos os conceitos foram inicialmente forjados na doutrina constitucional alemã, mas, com o tempo, passaram a ser utilizados também no campo penal, justamente em razão da necessidade de garantir que a função punitiva do Estado se mantenha dentro de parâmetros de racionalidade e legitimidade.

A proibição do excesso tem como finalidade impedir que o Estado, ao legislar ou aplicar o Direito Penal, ultrapasse os limites necessários para atingir o fim de proteção do bem jurídico. Isso significa que a pena ou a própria tipificação não podem ser desproporcionais em relação à gravidade da conduta. Um excesso punitivo se caracteriza quando a sanção é tão severa que acaba por violar garantias fundamentais do indivíduo, como a dignidade humana, a liberdade de expressão ou a presunção de inocência. Já a proibição da proteção deficiente se situa no polo oposto: ocorre quando o Estado deixa de legislar ou de adotar medidas adequadas para resguardar bens jurídicos fundamentais, permitindo que permaneçam vulneráveis diante de condutas socialmente lesivas.

Essa dualidade se mostra particularmente sensível quando se trata dos crimes virtuais, já que a internet trouxe novos desafios ao sistema penal. De um lado, observa-se a pressão social e política para o endurecimento das punições diante de práticas como fraudes eletrônicas, disseminação de discursos de ódio, pornografia infantil ou crimes contra a honra cometidos em redes sociais. De outro, nota-se a dificuldade do legislador em acompanhar a velocidade da evolução tecnológica, o que frequentemente gera lacunas normativas e fragilidade na tutela penal de condutas altamente danosas.

No que concerne à proibição do excesso, os riscos são evidentes. A criminalização de condutas na internet pode, em alguns casos, ser formulada de maneira imprecisa ou excessiva, afetando de forma desnecessária direitos constitucionais. Por exemplo, ao

[17] DIAS, Jean. A proibição do excesso (Übermassverbot) e a proibição de proteção deficiente (Untermassverbot) no direito penal. JusBrasil.

se prever penas demasiadamente severas para crimes de opinião ou ao ampliar, de modo genérico, o alcance de tipos penais relacionados à honra, corre o risco de restringir indevidamente a liberdade de expressão, um pilar fundamental da democracia. O excesso punitivo, nesses casos, não fortalece a tutela do bem jurídico, mas pode resultar em um efeito paralisante no uso legítimo das plataformas digitais, configurando um abuso legislativo.

Por outro lado, a proibição da proteção deficiente se revela quando o Estado deixa de estabelecer mecanismos eficazes de responsabilização para condutas que, apesar de novas, geram danos significativos à sociedade. É o caso, por exemplo, da ausência de previsão clara para determinadas modalidades de fraude eletrônica ou para crimes que envolvem a manipulação de dados pessoais sensíveis. Nessas situações, a insuficiência normativa deixa vítimas em situação de desamparo e reforça a percepção de que a internet seria um “território sem lei”. Esse déficit de tutela contraria o dever constitucional do Estado de proteger bens jurídicos fundamentais, como o patrimônio, a honra, a privacidade e, em casos mais graves, a vida.

A ausência de legislação adequada sobre determinados fenômenos sociais configuraria uma forma de proteção insuficiente. No campo dos crimes virtuais, esse raciocínio pode ser transportado de maneira clara: punir em excesso pode gerar inconstitucionalidade, enquanto punir de forma insuficiente pode significar omissão estatal inaceitável.

Um exemplo concreto dessa tensão pode ser observado no Projeto de Lei 4658/24, que prevê o aumento de pena em um terço para crimes contra a honra praticados pela internet. A proposta surge como resposta ao aumento dos casos de difamação e calúnia em plataformas digitais, mas também abre espaço para críticas no sentido de que tal medida pode representar um endurecimento desproporcional em situações que poderiam ser resolvidas por mecanismos cíveis ou administrativos, sem a necessidade de uma intervenção penal tão severa. Trata-se, portanto, de um caso típico em que o princípio da proporcionalidade deve ser invocado para evitar que o Estado, no afã de atender a demandas sociais, incorra em excesso punitivo.

No extremo oposto, a proteção deficiente é igualmente problemática. Crimes como o uso de “deepfakes” para difamar ou chantagear pessoas, o roubo de identidade digital ou mesmo ataques massivos de ransomware ainda encontram pouca ou nenhuma

previsão específica no ordenamento jurídico brasileiro. Essa ausência legislativa compromete a efetividade da proteção penal, deixando bens jurídicos relevantes expostos a condutas altamente nocivas e tecnicamente sofisticadas. A omissão estatal, nesse contexto, se traduz em descumprimento do dever constitucional de proteger direitos fundamentais em face de ameaças contemporâneas.

A importância de equilibrar esses dois polos, excesso e insuficiência não se resume a um debate teórico. Na prática, significa definir os contornos de um Direito Penal garantista e eficaz: garantista porque não admite excessos punitivos que desrespeitem a dignidade humana e os direitos fundamentais; eficaz porque não permite omissões que deixem a sociedade desprotegida diante de condutas lesivas. A proporcionalidade, nesse sentido, funciona como guia de racionalidade para o legislador e para o aplicador da lei, especialmente em áreas tão complexas e em constante transformação como os crimes virtuais.

Portanto, a análise da proibição do excesso e da proibição da proteção deficiente revela que ambos os riscos estão presentes no atual debate sobre criminalidade digital. O desafio é encontrar um ponto de equilíbrio: evitar leis penais simbólicas, criadas apenas para atender clamor social, mas também não permanecer inerte diante das novas formas de criminalidade que se desenvolvem no ambiente virtual. A proporcionalidade, aplicada nesse contexto, é o instrumento capaz de garantir que o Direito Penal continue sendo, ao mesmo tempo, uma barreira contra o autoritarismo e um mecanismo de proteção real contra condutas que violam direitos fundamentais no meio digital.

3.4 Casos Concretos: Episódio do vídeo do Felca, discussão sobre a adultização das crianças e incitação adolescentes a cometer cybercrime.

[18]Um exemplo recente que evidencia os desafios jurídicos e sociais relacionados aos crimes virtuais é o vídeo publicado pelo influenciador digital “Felca”, em agosto de 2025, no qual foram feitas denúncias sobre a chamada *adultização das*

[18] G1. Monetização, exploração de menores e redes de pedofilia: entenda denúncias feitas por Felca. G1, São Paulo, 13 ago. 2025

crianças em redes sociais. O material, que rapidamente alcançou milhões de visualizações, apontava a existência de conteúdos envolvendo menores em contextos considerados inapropriados, marcados por sexualização precoce e exploração velada. Entre os pontos levantados, destacou-se a ideia de um suposto “Algoritmo P”, que estaria favorecendo a disseminação desses conteúdos, ampliando sua visibilidade e, por consequência, potencializando os riscos de exploração infantil no ambiente digital.

A repercussão foi imediata, tanto na sociedade civil quanto em órgãos de investigação. O caso trouxe à tona a figura de influenciadores específicos, como Hytalo Santos, que já era alvo de apurações pelo Ministério Público da Paraíba por suspeitas de exploração de menores, e cuja atuação passou a ser alvo de medidas judiciais, incluindo mandados de busca e apreensão. Além disso, a gravidade das denúncias impulsionou debates no Congresso Nacional, gerando a Lei 15.211, sancionada pelo presidente Luiz Inácio Lula da Silva, que busca coibir casos de violações graves contra menores de 18 anos no ambiente virtual.

Do ponto de vista jurídico, esse episódio representa um marco contemporâneo no debate sobre a criminalidade virtual, na medida em que expõe não apenas condutas já tipificadas, como crimes de exploração sexual infantil, mas também zonas de incerteza jurídica em torno da chamada *adultização*. Esse fenômeno não encontra definição precisa na legislação brasileira, o que gera dificuldades na atuação do Ministério Público, da polícia e do Judiciário. Por um lado, há a necessidade de proteger de forma efetiva os direitos fundamentais da criança e do adolescente, em especial sua dignidade e integridade. Por outro, existe o risco de excessos punitivos, caso se estabeleçam interpretações amplas demais, capazes de criminalizar condutas culturais, sociais ou artísticas que não configuram exploração.

Nesse sentido, o caso Felca ilustra com clareza a aplicação do princípio da proporcionalidade. Ele demonstra a tensão entre a liberdade de expressão, tanto dos criadores de conteúdo quanto das próprias famílias, e a proteção da infância contra abusos. Ao mesmo tempo em que se exige uma resposta firme contra práticas de exploração ou incentivo à sexualização precoce, é imprescindível evitar que medidas legais e administrativas avancem sobre esferas legítimas de expressão ou convivência social.

Além disso, o episódio evidencia a relevância de se discutir a responsabilidade das plataformas digitais. A possível influência de algoritmos que priorizam determinados conteúdos aponta para a necessidade de maior transparência e regulamentação do funcionamento desses mecanismos, de modo a impedir que interesses comerciais se sobreponham à proteção da infância. Essa questão conecta-se à responsabilidade civil e penal dos provedores, tema já sensível no nosso ordenamento jurídico, especialmente sob o Marco Civil da Internet e das normas do Estatuto da Criança e do Adolescente.

[19]Além do episódio do influenciador Felca, outros casos recentes evidenciam a gravidade do problema da criminalidade virtual envolvendo crianças e adolescentes. Reportagem exibida pelo programa *Profissão Repórter* em maio de 2025 mostrou como jovens têm sido vítimas ou até acusados de praticar crimes cibernéticos em redes sociais e plataformas de jogos online.

Entre os casos acompanhados, destacou-se a investigação de uma adolescente de 14 anos em São Paulo, apontada como integrante de um grupo suspeito de atear fogo contra um homem em situação de rua no Rio de Janeiro, ato transmitido ao vivo por uma rede social. Além disso, a jovem foi vinculada a outras práticas graves, como incentivo à automutilação, estupro virtual, maus-tratos a animais e divulgação de conteúdos violentos.

A matéria também trouxe relatos de adolescentes processados na Vara da Infância e Juventude por armazenar e comercializar imagens de pornografia infantil ou incentivar a automutilação em grupos do Discord. Segundo a juíza Vanessa Cavalieri, esses jovens muitas vezes apresentam dificuldades de adaptação social e encontram nas redes uma forma de pertencimento, o que os leva a uma escalada de condutas ilícitas em busca de status dentro das comunidades virtuais.

Outro ponto abordado foi o surgimento dos chamados “justiceiros digitais”, como o caso de um jovem de 21 anos que se autodenomina “Mistério” e criou uma equipe informal de investigação para denunciar crimes cibernéticos. Embora essa atuação tenha resultado em denúncias encaminhadas às autoridades, especialistas alertam

---

19

G1. Incentivo à automutilação, estupro virtual: conteúdos violentos; como crianças e jovens têm sido vítimas ou acusadas de crimes na internet. *Profissão Repórter*, São Paulo, 21 mai. 2025.

para os riscos legais e de segurança pessoal envolvidos quando indivíduos assumem funções típicas do Estado.

Os casos evidenciam a urgência de o Direito acompanhar a velocidade das transformações tecnológicas, garantindo tanto a proteção eficaz contra condutas lesivas quanto a preservação das liberdades fundamentais, em equilíbrio com os valores constitucionais.

CONSIDERAÇÕES FINAIS.

O estudo realizado ao longo deste trabalho teve como objetivo analisar a evolução, a classificação e as principais modalidades dos crimes virtuais, bem como refletir sobre a tutela penal a partir do princípio da proporcionalidade. O percurso desenvolvido buscou demonstrar como a internet, ao mesmo tempo em que ampliou as possibilidades de interação, comunicação e desenvolvimento social, também se tornou um espaço fértil para práticas delitivas que desafiam o direito penal tradicional.

Desde o surgimento da rede mundial de computadores, o Brasil se deparou com a necessidade de repensar suas estruturas jurídicas. A criação de novas formas de criminalidade que vão desde fraudes eletrônicas e invasões de dispositivos até crimes contra a honra praticados em redes sociais, evidenciou a insuficiência das normas já existentes para lidar com condutas digitais. Tal cenário levou à elaboração de legislações específicas, como o Marco Civil da Internet e a Lei Carolina Dieckmann, que representaram importantes avanços, mas que não esgotaram a complexidade do tema.

Ao longo da pesquisa, buscou-se não apenas apresentar a evolução histórica e normativa, mas também oferecer uma classificação sistemática dos crimes virtuais. Essa divisão entre crimes próprios e impróprios, bem como entre crimes puros, mistos e comuns, revelou-se essencial para compreender a natureza peculiar dessas infrações. A tipificação penal, em muitos casos, depende da adaptação de tipos tradicionais a um novo ambiente tecnológico, o que gera constantes debates sobre a suficiência e adequação das respostas legislativas.

Outro ponto fundamental desenvolvido foi a análise do princípio da proporcionalidade na tutela penal dos crimes virtuais. Esse princípio é de extrema importância, pois estabelece um limite entre duas tendências igualmente preocupantes: o risco do excesso punitivo, que pode comprometer direitos fundamentais como a liberdade de expressão e a privacidade, e o risco da proteção insuficiente, que deixaria a sociedade vulnerável diante de ataques cada vez mais sofisticados no ambiente digital. Encontrar esse equilíbrio é um dos maiores desafios do direito penal contemporâneo.

As considerações finais têm a função de retomar o caminho percorrido, refletir sobre a fragilidade inicial do ordenamento jurídico brasileiro e as conquistas diante dos crimes virtuais e indicar perspectivas para o futuro. Trata-se de reconhecer que o

fenômeno é dinâmico, em constante transformação, e que exige do direito não apenas atualização legislativa, mas também diálogo interdisciplinar, cooperação internacional e políticas públicas eficazes.

Apesar dos avanços alcançados com a criação de leis específicas para enfrentar os crimes virtuais, como o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, ainda existem limitações significativas na resposta normativa brasileira. Essas legislações representaram marcos importantes: de um lado, o Marco Civil estabeleceu princípios e garantias para o uso da internet no Brasil, como a proteção da privacidade e a responsabilidade dos provedores; de outro, a Lei Carolina Dieckmann tipificou condutas como a invasão de dispositivos eletrônicos. Contudo, tais avanços não foram suficientes para abranger a totalidade das novas formas de criminalidade digital.

Uma das maiores dificuldades consiste na rapidez com que a tecnologia evolui. O direito, por sua própria natureza, é marcado por certa rigidez normativa, enquanto os crimes virtuais se sofisticam em ritmo acelerado. Golpes financeiros baseados em engenharia social, disseminação massiva de desinformação e ataques cibernéticos de grande escala são exemplos de fenômenos recentes que desafiam constantemente o legislador. Nesse sentido, há um descompasso entre a realidade fática e a capacidade normativa de resposta, o que gera insegurança tanto para os operadores do direito quanto para os cidadãos.

A dificuldade de tipificação é algo que merece destaque. Muitos crimes virtuais não se enquadram de forma clara nas figuras já previstas pelo Código Penal, obrigando o intérprete a recorrer à analogia ou a adaptações interpretativas. Isso cria riscos tanto de impunidade quanto de excesso punitivo.

Além disso, o caráter transnacional da internet amplia os desafios de aplicação da lei penal. Uma conduta pode ser praticada por um agente localizado em outro país, utilizando servidores espalhados pelo mundo, e afetar vítimas em território brasileiro. Nessas hipóteses, a legislação nacional mostra-se insuficiente se não houver mecanismos efetivos de cooperação internacional. Embora o Brasil participe de tratados e convenções, ainda há entraves burocráticos e limitações técnicas que dificultam a investigação e a punição de crimes cibernéticos que ultrapassam fronteiras.

Não se pode deixar de mencionar os desafios de natureza probatória. A volatilidade dos dados digitais, que podem ser facilmente apagados, alterados ou criptografados, impõe ao Estado uma necessidade constante de investimento em tecnologia e capacitação de agentes públicos. Sem uma estrutura adequada, a persecução penal torna-se ineficaz, contribuindo para a sensação de impunidade e estimulando a continuidade das práticas criminosas no ambiente virtual.

O enfrentamento dos crimes virtuais não pode se restringir ao plano normativo interno. Como já destacado, a internet é um ambiente sem fronteiras rígidas, e isso exige um esforço coordenado entre diferentes países para a construção de respostas eficazes. A cooperação internacional, nesse contexto, torna-se um elemento indispensável. Convenções multilaterais, como a [20]Convenção de Budapeste sobre Cibercrime, estabelecem diretrizes importantes para a harmonização legislativa e para a criação de mecanismos de assistência mútua entre Estados. Embora o Brasil ainda não seja signatário desse tratado, a adesão a instrumentos semelhantes pode fortalecer a capacidade de investigação e punição de crimes transnacionais.

A cooperação internacional, no entanto, não se limita a acordos formais entre Estados. É necessário investir em redes de colaboração técnica, em que autoridades policiais e judiciárias compartilhem informações de maneira célere e segura. A velocidade é um fator crucial no contexto digital, e atrasos burocráticos podem inviabilizar investigações que dependem da preservação de registros eletrônicos. Assim, mais do que tratados, o fortalecimento de canais diretos de comunicação entre instituições se mostra fundamental.

Outro aspecto essencial é o papel das políticas públicas voltadas para a prevenção e conscientização. Embora a repressão penal seja necessária, ela não é suficiente para conter o avanço dos crimes virtuais. O fortalecimento da chamada cidadania digital, com campanhas educativas, programas escolares e iniciativas de inclusão tecnológica, é indispensável para que os cidadãos compreendam seus direitos e saibam como se proteger no ambiente virtual. A prevenção, nesse caso, tem uma dupla função: reduzir a vulnerabilidade das potenciais vítimas e diminuir a oportunidade de ação para os agentes criminosos.

---

[20] TARDIN, P.; TARDIN, P. CRIMES CIBERNÉTICOS E O TRATADO INTERNACIONAL DE BUDAPESTE - Dois Níveis.

Nesse sentido, políticas públicas de segurança digital devem caminhar lado a lado com políticas educacionais. O incentivo à alfabetização digital crítica pode ser uma das medidas mais eficazes contra golpes, fraudes e disseminação de desinformação. A população que conhece os riscos da internet e domina ferramentas básicas de proteção, como verificação de fontes, uso de senhas fortes e reconhecimento de tentativas de phishing, torna-se menos suscetível às práticas criminosas.

É preciso reconhecer que o combate aos crimes virtuais não depende apenas do Estado. O setor privado, especialmente as grandes empresas de tecnologia e provedores de serviços digitais, desempenha papel relevante nesse processo. No próprio caso felca, mencionado acima, ficou evidente como os algoritmos e as práticas de moderação de conteúdo das plataformas podem influenciar diretamente a exposição de crianças e adolescentes a riscos, o que reforça a necessidade de atribuir às empresas uma parcela de responsabilidade pela prevenção e contenção desses danos. Esses agentes possuem acesso direto às informações e recursos técnicos que podem auxiliar na identificação e interrupção de práticas criminosas, razão pela qual sua atuação diligente é indispensável. A responsabilidade compartilhada entre Estado, empresas e cidadãos é, portanto, uma condição necessária para que a tutela penal e as políticas públicas alcancem maior efetividade.

Cabe destacar que a construção de uma cultura de segurança digital é um desafio de longo prazo. Assim como ocorreu com outros direitos fundamentais, como a proteção ambiental ou os direitos do consumidor, é preciso que a sociedade assimile gradualmente a importância da proteção no espaço virtual. Somente com essa mudança cultural, combinada a esforços legislativos, cooperação internacional e políticas públicas sólidas, será possível reduzir os impactos dos crimes virtuais e garantir que a internet continue sendo um espaço de liberdade, inovação e desenvolvimento social.

Um dos pontos que se destacam no estudo dos crimes virtuais é a necessidade de constante interpretação jurisprudencial. Como a legislação muitas vezes não acompanha a velocidade das inovações tecnológicas, o Poder Judiciário acaba assumindo papel central na definição de parâmetros e limites para a responsabilização penal e civil no ambiente digital.

Nesse cenário, ganha relevo o debate em torno do artigo 19 do Marco Civil da Internet, que estabelece que os provedores de aplicações de internet somente podem ser responsabilizados civilmente por danos decorrentes de conteúdos gerados por terceiros se, após ordem judicial específica, não tomarem providências para tornar indisponível o conteúdo apontado como infringente. O dispositivo, ao ser criado, buscou equilibrar a liberdade de expressão com a proteção contra abusos, evitando que plataformas fossem obrigadas a atuar como censores privados.

Ocorre que, em face da multiplicação de conteúdos criminosos em redes sociais, como notícias falsas, discursos de ódio e incitação à violência, esse dispositivo passou a ser objeto de questionamento perante o STF (Supremo Tribunal Federal). A Corte vem sendo chamada a decidir se a regra do artigo 19 deve ser interpretada de forma mais flexível, ampliando a responsabilidade das plataformas em determinadas situações. É um debate que toca diretamente no princípio da proporcionalidade: de um lado, está a proteção da liberdade de expressão e o receio de um excesso punitivo que possa sufocar o debate público; de outro, está a necessidade de proteger vítimas e a sociedade contra danos reais e imediatos causados pela disseminação de conteúdos ilícitos.

Essa discussão ilustra, de forma concreta, a tensão entre repressão criminal e proteção de direitos fundamentais, já explorada neste trabalho. Se por um lado a ausência de mecanismos eficazes pode levar à proteção insuficiente diante de crimes digitais, por outro, a imposição de obrigações desproporcionais às plataformas pode gerar efeitos colaterais negativos, como a restrição excessiva do fluxo de informações legítimas. Assim, a jurisprudência tem buscado construir um caminho intermediário, reconhecendo a importância da responsabilização, mas também preservando o núcleo essencial da liberdade de expressão.

Decisões que tratam de crimes contra a honra praticados em redes sociais, de vazamento de dados sensíveis ou de fraudes eletrônicas têm enfatizado a necessidade de uma resposta penal adequada e guiam o direito penal em um terreno de incerteza jurídica, mas sempre proporcional à gravidade da conduta e ao bem jurídico tutelado. Essa postura jurisprudencial evidencia que o direito penal, no contexto digital, deve ser utilizado com cautela: não como solução para todos os problemas da internet, mas como instrumento de proteção em situações que efetivamente exigem repressão estatal.

O desafio está, portanto, em consolidar uma jurisprudência coerente, que consiga dialogar com a evolução tecnológica e com as demandas sociais sem se afastar dos princípios constitucionais. O princípio da proporcionalidade, nesse sentido, atua como verdadeiro fio condutor, orientando a interpretação judicial e impedindo que o direito penal se torne tanto um mecanismo ineficaz quanto um instrumento de excessos punitivos.

Diante de todo o percurso traçado neste trabalho, percebe-se que os crimes virtuais representam um dos maiores desafios contemporâneos para o Direito Penal. O ambiente digital, marcado pela rapidez, pelo anonimato e pela ausência de barreiras geográficas, cria um terreno fértil para condutas ilícitas que, muitas vezes, ultrapassam a capacidade de resposta dos mecanismos tradicionais.

O estudo demonstrou que a legislação brasileira tem avançado de forma gradual e significativa. A edição de diplomas como a Lei Carolina Dieckmann, o Marco Civil da Internet e a LGPD (Lei Geral de Proteção de Dados) evidencia a tentativa do legislador em acompanhar as transformações da sociedade digital. No entanto, também ficou claro que serão necessários maiores avanços para dar conta da complexidade da cibercriminalidade, sendo necessárias constantes revisões, interpretações jurisprudenciais e, sobretudo, a implementação de políticas públicas de conscientização e prevenção.

A análise do princípio da proporcionalidade foi essencial nesse cenário. Afinal, a resposta penal não pode se pautar apenas pela repressão, sob pena de gerar excesso punitivo, tampouco pode se omitir diante das novas formas de criminalidade, sob risco de proteção insuficiente. O equilíbrio entre esses polos deve orientar tanto a elaboração de leis quanto a atuação dos tribunais e das autoridades responsáveis pela investigação.

Portanto, conclui-se que a trajetória do enfrentamento aos crimes virtuais é contínua e desafiadora. O Direito Penal, como última ratio, deve estar sempre atento para atuar com rigor e proporcionalidade, garantindo que os bens jurídicos mais relevantes sejam protegidos, mas sem perder de vista os direitos fundamentais que sustentam a democracia. O futuro desse campo jurídico dependerá da capacidade de equilibrar repressão, prevenção e liberdade, em uma dinâmica que acompanhará, inevitavelmente, o ritmo acelerado da evolução tecnológica.

REFERÊNCIAS.

ALMEIDA, Haian de Assis Lopes; DE OLIVEIRA, Tamar Ramos. CRIMES VIRTUAIS: O AVANÇO DOS CRIMES ELETRÔNICOS E A EVOLUÇÃO DAS LEIS ESPECÍFICAS NO BRASIL. Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 8, n. 11, p. 277-294, 2022.

ARCTIC WOLF. A Decade of Cybercrime. [S.l.]: Arctic Wolf, [s.d.]. Disponível em: https://arcticwolf.com/resources/blog/decade-of-cybercrime/. Acesso em: 15 jul. 2025.

Bello, Elena. "Conoce la historia de Internet desde su primera conexión hasta hoy." IEBSchool. Disponível em: https://www.iebschool.com/hub/historia-de-internet-innovacion/. Acesso em: 9 jul. 2025.

CÂMARA DOS DEPUTADOS. Projeto aumenta pena para crimes praticados no meio digital. Agência Câmara Notícias, Brasília, 07 abr. 2025. Disponível em: https://www.camara.leg.br/noticias/1139965-projeto-aumenta-pena-para-crimes-praticados-no-meio-digital/ Acesso em: 1 set. 2025.

Chade REZEK NETO. O Princípio da Proporcionalidade no Estado Democrático de Direito. São Paulo: Lemos & Cruz, 2004. p. 56. Idem, ibidem, p. 57.

CONJUR. Advogados condenam pena triplicada para crimes contra a honra na web. Consultor Jurídico, São Paulo, 19 mar. 2021. Disponível em: https://www.conjur.com.br/2021-mar-19/advogados-condenam-pena-triplicada-crimes-honra-web/. Acesso em: 1 set. 2025.

DIAS, Jean. A proibição do excesso (Übermassverbot) e a proibição de proteção deficiente (Untermassverbot) no direito penal. JusBrasil, 11 abr. 2025. Disponível em:

https://www.jusbrasil.com.br/artigos/a-proibicao-do-excesso-ubermassverbot-e-a-proibicao-de-protecao-deficiente-untermassverbot-no-direito-penal/429256367 Acesso em: 15 set. 2025.

Dimitri DIMOULIS; Leonardo MARTINS. Teoria Geral dos Direitos Fundamentais. São Paulo: Editora Revista dos Tribunais, 2007. p. 191

FBI. Famous Cases & Criminals. Washington, D.C.: Federal Bureau of Investigation, [s.d.]. Disponível em: https://www.fbi.gov/history/famous-cases/. Acesso em: 15 jul. 2025.

G1. Incentivo à automutilação, estupro virtual: conteúdos violentos; como crianças e jovens têm sido vítimas ou acusadas de crimes na internet. *Profissão Repórter*, São Paulo, 21 mai. 2025. Disponível em: https://g1.globo.com/profissao-reporter/noticia/2025/05/21/incentivo-a-automutilacao-estupro-virtual-conteudos-violentos-como-criancas-e-jovens-tem-sido-vitimas-ou-acusadas-de-crimes-na-internet.ghtml Acesso em: 29 set. 2025.

G1. Monetização, exploração de menores e redes de pedofilia: entenda denúncias feitas por Felca. G1, São Paulo, 13 ago. 2025. Disponível em: https://g1.globo.com/sp/sao-paulo/noticia/2025/08/13/monetizacao-exploracao-de-menores-e-redes-de-pedofilia-entenda-denuncias-feitas-por-felca.ghtml Acesso em: 20 set. 2025.

GARCIA, Plínio Silva; MACADAR, Marie Anne; LUCIANO, Edimara Mezzono. A influência da injustiça organizacional na motivação para a prática dos crimes cibernéticos. Jistem usp, Brazil, vol. 15, 2018. Disponível em: http://www.scielo.br/pdf/jistm/v15/1807-1775-jistm-15-e201815002.pdf

HARAKEMIW, Rafael Antônio; VIEIRA, Tiago Vidal. Crimes Cibernéticos. Anais do 2º Simpósio Sustentabilidade e Contemporaneidade nas Ciências Sociais, 2014. Disponível em: https://themaetscientia.fag.edu.br/index.php/ASSCCS/article/view/194/280.

JESUS, Damásio de; MILAGRES, José Antônio. Manual de Crimes Informáticos. 1ª Edição. ed. São Paulo: Saraiva, 2016. 231 p. ISBN 978850262724-6.

MIGALHAS. Lei que torna crimes cometidos pela internet mais graves é sancionada. Migalhas, [s.l.]. Disponível em: https://www.migalhas.com.br/quentes/346274/lei-que-torna-crimes-cometidos-pela-internet-mais-graves-e-sancionada Acesso em: 1 set. 2025.

MPMG, Ministério Público do Estado de Minas Gerais. Combate aos Crimes Cibernéticos. Disponível em: https://www.mpmg.mp.br/portal/menu/areas-de-atuacao/criminal/crimes-ciberneticos/ Acesso em: 09 jun. 2025.

ROBERTO; THAIS BILENKY. Celular “rouba” 53% mais que arma, mostra pesquisa. Disponível em: https://noticias.uol.com.br/colunas/a-hora/2025/08/15/celular-rouba-53-mais-que-arma-mostra-pesquisa.htm. Acesso em: 20 ago. 2025.

ROSSINI, Augusto Eduardo de Souza. Brevíssimas considerações sobre delitos informáticos. São Paulo: ESMP, jul. 2002. p. 140 (Caderno Jurídico, ano 02, n. 04).

SCHAUN, Guilherme. Uma lista com 24 crimes virtuais. JusBrasil, [s.l.]. Disponível em: https://www.jusbrasil.com.br/artigos/uma-lista-com-24-crimes-virtuais/686948017

SCHNEIDER, J. The History of Malware | IBM. Disponível em: https://www.ibm.com/think/topics/malware-history. Acesso em: 14 jul. 2025.

SENADO. Golpes virtuais aumentam e não fazem distinção de idade. Brasília: Senado Federal, 2025. Disponível em: https://www12.senado.leg.br/noticias/infomaterias/2025/04/golpes-virtuais-aumentam-e-nao-fazem-distincao-de-idade

SILVA, Daniel Neves. "História da internet"; Brasil Escola. Disponível em: https://brasilescola.uol.com.br/informatica/internet.htm. Acesso em: 15 jun. 2025.

TARDIN, P.; TARDIN, P. CRIMES CIBERNÉTICOS E O TRATADO INTERNACIONAL DE BUDAPESTE - Dois Níveis. Disponível em: https://www.doisniveis.com/direito-internacional/crimes-ciberneticos-e-o-tratado-internacional-de-budapeste/. Acesso em: 14 ago. 2025.