

Cibercrimes: Os desafios da legislação brasileira frente a essa nova modalidade criminal

Bianca Natasha Brandão Silva ¹, Carlos Henrique Passos Mairink²

Resumo: O presente Trabalho de Conclusão de Curso analisa os principais crimes que podem ser praticados no ambiente virtual e os desafios enfrentados pelo Direito Penal brasileiro diante das novas formas de criminalidade digital. A pesquisa aborda condutas ilícitas que vão desde os crimes contra a honra e o patrimônio até aqueles que atentam contra a dignidade sexual, como a pornografia de vingança, o estupro virtual e a sextorsão. Também são examinadas práticas como o furto e o estelionato eletrônicos, a invasão de dispositivos informáticos e a disseminação de conteúdos ilícitos por meio de redes sociais. O estudo destaca a evolução legislativa brasileira, incluindo leis como a nº 12.737/2012 (Lei Carolina Dieckmann), nº 12.965/2014 (Marco Civil da Internet), nº 14.155/2021 e o Decreto presidencial 11.491/23, que adaptaram o ordenamento jurídico às demandas da era digital. Metodologicamente, adota-se uma abordagem qualitativa e descritiva, fundamentada em pesquisas bibliográficas, documentais e jurisprudenciais, buscando avaliar a eficácia da legislação penal e os mecanismos de responsabilização de pessoas físicas e jurídicas. Conclui-se que, embora o Brasil tenha avançado na criação de normas específicas e em políticas públicas de cibersegurança, como a Estratégia Nacional de Segurança Cibernética (E-Ciber) e a Política Nacional de Cibersegurança (PNCiber), ainda há desafios quanto à identificação dos autores, à cooperação internacional e à efetividade das sanções penais. O trabalho evidencia, assim, a importância da atualização contínua do Direito Penal, da conscientização social e do fortalecimento das ações preventivas e repressivas para garantir um ambiente digital mais seguro e ético.

Palavras-chave: crimes cibernéticos; direito penal; responsabilização; internet; segurança digital.

Cybercrimes: The challenges facing Brazilian legislation in the face of this new type of crime

Abstract: This undergraduate thesis analyzes the main crimes that can be committed in the virtual environment and the challenges faced by Brazilian Criminal Law in dealing with new forms of digital crime. The research addresses illegal behaviors ranging from crimes against honor and property to those that violate

¹ Aluna do Curso de Direito da Famig. Faculdade Minas Gerais.

² Revisor. Professor do Curso de Direito da Famig. Faculdade Minas Gerais

sexual dignity, such as revenge porn, virtual rape, and sextortion. It also examines practices such as electronic fraud, data theft, and unauthorized access to computer systems. The study highlights the evolution of Brazilian legislation, including Laws nº 12.737/2012 (Carolina Dieckmann Law), nº 12.965/2014 (Brazilian Internet Bill of Rights), and nº 14.155/2021, which have adapted the legal framework to digital-era demands. Methodologically, it adopts a qualitative and descriptive approach, based on bibliographic, documentary, and case-law research, to assess the effectiveness of criminal law and the mechanisms of accountability for individuals and legal entities. The findings indicate that, although Brazil has advanced in legal reforms and public cybersecurity policies—such as the National Cybersecurity Strategy (E-Ciber) and the National Cybersecurity Policy (PNCiber)—significant challenges remain regarding offender identification, international cooperation, and the enforcement of penalties. The study concludes by emphasizing the need for continuous legal adaptation, public awareness, and stronger preventive and repressive measures to ensure a safer and more ethical digital environment.

Keywords: cybercrime; criminal law; accountability; internet; digital security.

1 INTRODUÇÃO

Os avanços tecnológicos das últimas décadas remodelaram a maneira como as pessoas interagem, se comunicam e vivem seu cotidiano. Dentre essas inovações, internet consolidou-se como um dos marcos mais importantes da era digital, conectando pessoas e organizações em escala global. No entanto, o mesmo ambiente que impulsionou o desenvolvimento da comunicação e da troca de informações também se tornou propício para atos ilícitos, desafiando as restrições do direito penal tradicional e exigindo que o ordenamento jurídico brasileiro se adapte às novas realidades impostas pelo crime cibernético.

O crescimento acelerado do meio digital resultou na proliferação de inúmeros tipos de atividades criminosas que afetam não apenas o patrimônio, mas também a honra, a privacidade, a dignidade sexual e até mesmo a segurança de dados e sistemas computacionais. O anonimato e o fácil acesso à tecnologia digital conferem aos criminosos maior abrangência e sofisticação, consequentemente, dificultando a identificação e a persecução penal dos autores. Nesse contexto, novas tipologias criminosas estão surgindo, como a fraude eletrônica, estupro cibernético, pornografia de vingança e invasão de dispositivos. Esses fenômenos desafiam tanto a legislação quanto a investigação criminal.

Diante desse cenário, o presente trabalho se propõe a analisar os principais crimes que podem ser cometidos no ambiente virtual, abordando suas características, tipificação jurídica e a forma de responsabilização dos autores, sejam eles pessoas físicas ou jurídicas. O objetivo deste estudo é compreender como o ordenamento jurídico brasileiro tem respondido aos desafios impostos pela criminalidade digital, com ênfase nas inovações legislativas como a Lei nº 12.737/2012 (Lei Carolina Dieckmann), a Lei nº 14.155/2021 e o Marco Civil da Internet (Lei nº 12.965/2014). Analisa-se, ainda, o papel das políticas públicas e das estratégias nacionais de segurança cibernética na prevenção e no combate a esses crimes.

O estudo explora também a crescente ocorrência de crime cibernéticos e suas severas consequências sociais, econômicas e psicológicas que recaem sobre as vítimas e a sociedade. Da mesma forma, destaca-se a necessidade de atualização contínua do direito penal e processual penal, bem como o fortalecimento da cooperação internacional, visto que a natureza transnacional desses crimes exige uma resposta jurídica unificada.

O presente trabalho utiliza uma abordagem qualitativa descritiva, com base em estudos bibliográficos, documentos e casos reais. O objetivo é analisar de forma crítica como o direito penal brasileiro tem lidado com os novos tipos de crimes que acontecem no meio digital, assim como contribuir para o debate em torno da proteção de bens jurídicos e aprimoramento da política de segurança cibernética no Brasil.

2 CRIMES QUE PODEM SER PRATICADOS NA INTERNET

Embora seja considerada um dos maiores avanços tecnológicos da humanidade, a internet também impôs novos desafios para o campo do Direito Penal. A possibilidade de comunicação instantânea, aliado ao relativo anonimato e ao alcance global, aumentaram a incidência de práticas criminosas nesse ambiente, demandando do ordenamento jurídico brasileiro ajustes normativos e interpretativos para o enfrentamento dos crimes cibernéticos. Como destaca Nucci (2014, p.70), o Direito Penal está o tempo todo sendo desafiado a se adaptar a novas

condutas nocivas, sob pena de se tornar ineficaz na proteção de bens jurídicos relevantes, por isso quando determinado bem jurídico é entendido como relevante, merecem a tutela deste. Portanto, é inevitável que diante da gravidade dessa modalidade criminal, o Direito Penal sofra modificações para garantir a proteção desses bens jurídicos.

Nesse contexto, a doutrina estabelece que os crimes cometidos no ambiente digital podem ser classificados em duas categorias: a primeira, os propriamente ditos, aqueles que só podem ser praticados por meio da utilização de sistemas informáticos, como o acesso ilícito a dispositivos informáticos. A segunda categoria abarca os crimes informáticos impróprios, caracterizados pela utilização da internet como meio para a prática de crimes já previstos no Código Penal, como difamação, fraude e estupro, conforme classificação proposta por Sydow (2009).

Diante desse cenário, o presente capítulo dedica-se à análise dos tipos de crimes que podem ser cometidos no ambiente virtual, com foco especial em sua tipificação e nos desafios impostos ao Direito Penal brasileiro. O escopo da análise abrange condutas ilícitas de variada complexidade, desde aquelas que violam o patrimônio até aquelas mais sofisticadas, que envolvem acesso ilícito a dispositivos informáticos e interrupção de serviços telemáticos.

2.1 Crimes contra a honra

A internet aumentou a frequência de crimes contra a honra. Crimes como calúnia (art. 138, Código Penal), injúria (art. 140, Código Penal) e difamação (art. 139, Código Penal) continuam os mesmos quando acontecem online, mas acabam ganhando novas proporções e podendo causar mais danos. A facilidade de disseminação de informações, muitas vezes anonimamente, amplia a extensão dos danos causados à vítima. Silva observa que a internet transformou delitos como esses em fenômenos de massa, uma vez que o meio digital aumenta a disseminação da ofensa, dado que grande parte do mundo está conectado, com acesso à internet, potencializando o alcance dos resultados (Silva, 2020).

Assim, um comentário difamatório em rede social, ofensivo, ou a disseminação de notícia falsa podem configurar crimes contra a honra, tipificados

nos artigos 138 a 140 do Código Penal (CP), agravados pelo meio utilizado, conforme o art. 141, §2º CP, que prevê a triplicação da pena quando o delito for cometido ou divulgado por meio de qualquer tipo de rede social na rede mundial de computadores.

Apresenta-se, a seguir, um precedente judicial relevante envolvendo crime contra a honra cometido por meio da internet. A análise adiante destaca os fatos, a tipificação jurídica, a decisão judicial e a fundamentação aplicada pelo Tribunal de Justiça de São Paulo (TJSP):

EMENTA – TJSP, APELAÇÃO Nº 0062364-28.2018.8.26.0050 APELAÇÃO CRIMINAL. CALÚNIA. PUBLICAÇÃO DE VÍDEO NAS REDES SOCIAIS. Imputação falsa de crime (organização criminosa e corrupção passiva) feita contra servidor público. Crime contra a honra com majorante do art. 138, caput, do Código Penal. Uso indevido de redes sociais como meio de divulgação amplia o dano à reputação. Pena de 9 meses e 10 dias de prestação de serviços à comunidade e 14 dias-multa mantida. TJSP, 4ª Câmara de Direito Criminal, Apelação nº 0062364-28.2018.8.26.0050, julgada em 9 de novembro de 2022. (SÃO PAULO, 2022).

O caso em questão é um prático exemplo de que os operadores do direito têm compreendido o quanto o uso da internet e meios digitais têm dado novas roupagens para os crimes em geral, e a necessidade de que essas novas nuances, dada a gravidade pelo poder de alcance conferido pelas redes sociais, necessitam de repressão adequada, visando coibir o uso indevido da internet como meio de disseminação de imputações criminosas falsas.

2.2 Crimes contra o patrimônio

Os crimes contra o patrimônio representam uma parcela significativa dos delitos cometidos no ambiente digital, adaptando-se a novas ferramentas e formas de interação. A internet facilita transações financeiras e o acesso a dados pessoais, por isso tornou-se um espaço atrativo para condutas que visam à obtenção de vantagem ilícita em detrimento do patrimônio alheio. Desse modo, dentre as diversas manifestações desses delitos, a fraude eletrônica adquire especial relevância.

2.3 Fraudes eletrônicas

A fraude eletrônica abrange uma ampla gama de condutas, desde a clonagem de cartões de crédito e débito até a manipulação de sistemas bancários para desvio de fundos. A sofisticação dessas práticas exige atualizações constantes tanto nas medidas de segurança quanto na legislação penal. Segundo Nucci (2014), a fraude, em sua essência, envolve enganar a vítima para que ela entregue voluntariamente bens ou dinheiro ao infrator. Da mesma forma, a fraude também pode servir como meio de subtração sem o consentimento da vítima, inclusive por meio da manipulação fraudulenta de sistemas eletrônicos. No contexto digital, essas condutas podem ser orquestradas por meio de phishing, smishing ou vishing, técnicas que induzem o usuário a fornecer dados sensíveis, como senhas e informações bancárias, mas também privam os indivíduos de seus bens de forma dissimulada (Silva, 2021, p.10).

2.4 Furto mediante fraude eletrônica

O artigo 155 do Código Penal define o crime de furto como “subtrair, para si ou para outrem, coisa móvel alheia” (BRASIL, 1940). Tradicionalmente, esse tipo penal pressupõe a subtração clandestina ou sorrateira de bem material alheio, sem emprego de violência ou grave ameaça. Nesse sentido, a Lei nº 14.155/2021 alterou o Código Penal para tratar de forma mais rigorosa as condutas que envolvem fraude eletrônica, inserindo o § 4º-B ao artigo 155 do Código Penal, estabelecendo como furto qualificado quando o crime for praticado mediante a utilização de dispositivo eletrônico ou informático, com ou sem violação de mecanismo de segurança, para sacar recursos de conta bancária ou similar. A pena-base foi alterada para reclusão de 4 a 8 anos, mais multa. Dessa forma, a legislação passou a reconhecer expressamente o chamado furto virtual, alinhando-se à necessidade de tutela penal do patrimônio diante de condutas cada vez mais sofisticadas praticadas no ambiente digital.

Ainda sobre o furto mediante fraude eletrônica, a Lei nº 14.155/2021 instituiu o § 4º-C, que introduz majorantes específicos para esse tipo de crime, aplicando um aumento de 1/3 (um terço) a 2/3 (dois terços) quando cometido em servidores localizados no exterior, ou de 1/3 (um terço) até o dobro quando o crime

for cometido contra idosos ou pessoas vulneráveis. A promulgação desse dispositivo se mostra fundamental no enfrentamento de fraudes sofisticadas. Da mesma forma, busca maior responsabilização quando perpetradas contra vítimas em situação de vulnerabilidade elevada.

2.5 Estelionato mediante fraude eletrônica

A figura típica do estelionato, previsto no artigo 171 do Código Penal, caracteriza-se pela obtenção de vantagem ilícita em prejuízo de outrem, induzindo ou mantendo a vítima em erro por meio de ardil, engano ou qualquer outro meio fraudulento. No ambiente virtual, essa conduta permanece essencialmente a mesma, mas o meio empregado é a fraude eletrônica, realizada por meio da internet ou de dispositivos digitais. O estelionato virtual apresenta variedade de formas, dentre as quais se destacam: os golpes em plataformas de comércio, ataques de *phishing* e links que coletam dados bancários, clonagem de perfis em mídias sociais para solicitar valores a conhecidos, falsas centrais de atendimento bancário ou mensagens em aplicativos de comunicação. É importante ressaltar que, em todas essas situações, a vítima, induzida em erro, realiza voluntariamente um ato de disposição patrimonial.

Com a promulgação da Lei nº 14.155/2021, o estelionato mediante de fraude eletrônica passou a receber tratamento mais severo. A lei introduziu qualificadoras e majorantes específicas no artigo 171 do Código Penal, acrescentando novos parágrafos e incisos, aumentando a pena para 4 a 8 anos de reclusão e multa quando a fraude envolver a utilização de dispositivos eletrônicos ou de informática, incluindo servidores localizados no exterior.

O estelionato virtual é um dos crimes mais comuns no Brasil atualmente, perpetrado em larga escala por meio de golpes digitais. É o que mostra o resultado do Anuário Brasileiro de Segurança Pública de 2025, que contabilizou um aumento de 17,0% nos casos de estelionato por meio eletrônico entre os anos de 2023 e 2024. Sua relevância prática está ligada à necessidade de conscientização pública, fortalecimento da segurança cibernética, treinamento das autoridades investigativas para rastrear e prevenir tais práticas, assim como reduzir a

impunidade, constatações essas reafirmadas por Renato Sérgio de Lima Diretor, Presidente do Fórum Brasileiro de Segurança Pública e Professor da FGV EAESP, no mesmo anuário. (Lima, 2025, p.107).

2.5.1 Distinção entre furto e estelionato virtuais

É crucial distinguir entre furto por meio de fraude eletrônica (artigo 155, § 4º, II do CP e Estelionato virtual (artigo 171, § 2º-A do CP). Enquanto no estelionato virtual a vítima consente com a transferência de bens em decorrência de erro ou engano empregado pelo autor, no furto virtual ocorre subtração sem o consentimento da vítima, isso, por meio de manipulação de sistemas eletrônicos. Isto posto, o critério de distinção é o método de execução, uma vez que, no estelionato virtual, a vítima é induzida a entregar voluntariamente um bem, no furto virtual, o autor invade sistemas, manipula dados ou explora vulnerabilidades para extrair valores ou bens sem o conhecimento da vítima.

Sobre o tema, a Ministra Laurita Vaz, do Superior Tribunal de Justiça, enquanto relatora do Conflito de Competência nº 67.343 - GO (2006/0166153-0), em seu voto distinguiu os tipos da seguinte forma:

EMENTA. CONFLITO NEGATIVO DE COMPETÊNCIA. PENAL E PROCESSO PENAL. FRAUDE ELETRÔNICA NA INTERNET. TRANSFERÊNCIA DE NUMERÁRIO DE CONTA DA CAIXA ECONÔMICA FEDERAL. FURTO MEDIANTE FRAUDE QUE NÃO SE CONFUNDE COM ESTELIONATO. CONSUMAÇÃO. SUBTRAÇÃO DO BEM. APLICAÇÃO DO ART. 70 DO CPP. COMPETÊNCIA DA JUSTIÇA FEDERAL PARANAENSE.

O furto mediante fraude não se confunde com o estelionato. A distinção se faz primordialmente com a análise do elemento comum da fraude que, no furto, é utilizada pelo agente com o fim de burlar a vigilância da vítima que, desatenta, tem seu bem subtraído, sem que se aperceba; no estelionato, a fraude é usada como meio de obter o consentimento da vítima que, iludida, entrega voluntariamente o bem ao agente.

Hipótese em que o agente se valeu de fraude eletrônica para a retirada de mais de dois mil e quinhentos reais de conta bancária, por meio da "Internet Banking" da Caixa Econômica Federal, o que ocorreu, por certo, sem qualquer tipo de consentimento da vítima, o Banco. A fraude, de fato, foi usada para burlar o sistema de proteção e de vigilância do Banco sobre os valores mantidos sob sua guarda. Configuração do crime de furto qualificado por fraude, e não estelionato. (BRASIL, 2007).

Portanto, a invasão de contas bancárias, sem consentimento da vítima, vem sendo caracteriza furto mediante fraude eletrônica. Por outro lado, quando o alvo enganado é uma pessoa física, titular do bem, e esse de alguma forma consente, mesmo que sem perceber, ocorre o estelionato. Sem a cooperação da pessoa física, entende-se que se amolda melhor ao tipo penal do furto mediante fraude.

2.6 Crimes contra dignidade sexual

Crimes sexuais podem ser entendidos como ações que violem a liberdade sexual de determinado indivíduo, visto que, segundo Machado, Aragão e Alencastro (2023) “é relevante o entendimento de que a intimidação ou a violência a liberdade sexual alheia são entendidos como crimes sexuais, executados desta maneira contra a vontade da vítima”. Nesse sentido, pode-se inferir que crimes sexuais vituais virtuais são aqueles cometidos via internet ou dispositivos eletrônicos que violam a liberdade ou a dignidade sexual da vítima.

Embora ocorram em um ambiente digital, eles têm consequências concretas e graves no mundo real, incluindo traumas psicológicos e sociais. Esses crimes representam uma das formas mais graves de violência digital, afetando diretamente a dignidade sexual e a integridade psicológica das vítimas.

A legislação brasileira tem sido alvo de algumas reformulações com a finalidade de alcançar a punibilidade das ações virtuais contra a dignidade sexual. Por meio da Lei Nº 13.718/2018, houve algumas mudanças como adição artigo 218-C e 216-B ao Código Penal. O primeiro institui como crime a conduta de divulgar cena de estupro, sexo ou nudez sem consentimento, de forma a desestimular e inibir a pornografia de vingança. O segundo passou a tipificar o registro não autorizado de intimidade sexual, passando a considerar crime a ação de “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” (BRASIL, 2018). A criação deste último artigo tem como um dos seus objetivos punir filmagens clandestinas divulgadas em redes sociais.

A legislação brasileira avançou na criminalização desses comportamentos, mas ainda enfrenta obstáculos legais e desafios investigativos que serão ainda

discutidos neste estudo. Por ora, este tópico se propõe a analisar os principais crimes sexuais cometidos no ambiente virtual, abordando suas características, e a legislação aplicável no Brasil.

2.7 Sextorsão

O Código Penal brasileiro não possui um tipo penal específico para a “sextorsão”. O termo “sextorsão” é resultado da junção da palavra “sexo” e da palavra “extorsão”.

Conforme artigo 158 do CP, a extorsão consiste em “constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar de fazer alguma coisa” (BRASIL, 1940). A sextorsão portanto, é um termo utilizado pela doutrina para se referir a situações em que o agente, valendo-se de conteúdo íntimo da vítima, ameaça-lhe de divulgação com o objetivo de obter alguma vantagem indevida.

Apesar de não haver tipificação penal específica, os operadores da lei tem se valido de outros tipos penais que podem ser aplicados aos casos. É o que diz Rogério Sanches apud Silva (2022).

[...] Prática cada vez mais comum é a denominada sextorsão, em que o agente constrange outra pessoa se valendo de imagens ou vídeos de teor erótico que de alguma forma a envolvam. No caso, emprega-se grave ameaça consistente na promessa de divulgação do material caso a vítima se recuse a atender à exigência. A depender das circunstâncias, vislumbramos três figuras criminosas às quais a conduta pode subsumir: a) se o agente simplesmente constrange a não fazer o que a lei permite, ou fazer o que ela não manda, há o crime em estudo; b) se constrange a vítima com intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixe de fazer alguma coisa, há a extorsão; c) se constrange a vítima à prática de atividade sexual, há estupro. (SANCHES apud SILVA, 2022, p.121).

Vale ressaltar que, conforme o entendimento do Des. Edson Ulisses De Melo, no julgamento do HC 202039482/SE, em que o acusado usava do *modus operandi* de a criar de perfis falsos em redes sociais com objetivo de conseguir fotos íntimas das vítimas e passar a exigir a prática de atos sexuais das vítimas, a referida conduta se amoldaria ao que a doutrina denominaria como sextorsão. Entendendo por vez

ser cabível, como no caso concreto, o concurso material entre outros tipos penais incluído os previstos no artigo 158 CP, extorsão, e o artigo 241-B do Estatuto da Criança e do Adolescente (ECA), que dispõem sobre o crime de adquirir, possuir ou armazenar registros de qualquer forma que contenham cena de sexo explícito envolvendo criança ou adolescente. Esta figura como uma amostra de como o judiciário tem se posicionado diante das ardilosasidades que cercam dos crimes cibernéticos.

2.8 Estupro virtual

Inicia-se esta seção explanando que Código Penal Brasileiro, no artigo 213, tipifica o crime de estupro, definindo-o como o ato de “constranger alguém, mediante violência ou grave ameaça, a ter conjunção carnal ou a praticar ou permitir que com ele se pratique outro ato libidinoso” (BRASIL, 1940). Dessa forma, com o avanço das tecnologias digitais, surgiu a necessidade de reinterpretar esse dispositivo conforme às novas realidades. Portanto, culminando no entendimento jurisprudencial do chamado 'estupro virtual'. O presente tópico analisa como o Superior Tribunal de Justiça consolidou essa interpretação, destacando os fundamentos legais e práticos do entendimento.

A interpretação tradicional quanto a esse delito presumia contato físico direto entre autor e vítima, no entanto, a realidade digital modificou essa compreensão. Assim, o estupro virtual se configura quando o agente, utilizando de grave ameaça exercida por meios digitais, constrange a vítima a praticar atos libidinosos em si mesma ou a expor sua intimidade através de transmissões online, fotografias ou vídeos. Neste viés, é oportuno que seja trazido entendimento do Relator Joel Ilan Paciornik, no julgamento do RHC 70.976/MS, o qual conclui que a dignidade sexual não se ofende somente com lesões de natureza física. O posicionamento de Rogério Sanches apud Silva (2022), não é diferente, segundo ele:

[...] De acordo com a maioria da doutrina, não há necessidade de contato físico entre o autor e a vítima, cometendo o crime o agente que, para satisfazer a sua lascívia, ordena que a vítima explore seu próprio corpo (masturbando-se), somente para contemplação (tampouco há que se imaginar a vítima desnuda para a caracterização do crime – RT 429/380). (Sanches apud Silva, 2022, p.123).

Embora não haja contato físico entre agressor e vítima, as ações, núcleos do tipo penal de estupro se mostram presentes, logo há clara violação da dignidade sexual e constrangimento forçado. Ademais, a moderna interpretação do art. 213 do CP tem como bem jurídico a ser tutelado a liberdade e a dignidade sexual, e não apenas a integridade física. Dessa forma, a conduta de constranger alguém a praticar atos libidinosos, ainda que a distância, fere diretamente esses bens jurídicos e deve ser punida na forma do estupro.

2.8.1 Deep fakes

O progresso das tecnologias digitais também favoreceu a criação e manipulação de conteúdos audiovisuais de forma maliciosa. Por consequência, essas condutas impeliram a criação de normas penais específicas para proteger a privacidade e a liberdade sexual dos indivíduos. Para tanto, a Lei nº 13.772/2018 introduziu o artigo 216-B no Código Penal, estabelecendo como crime a conduta de tirar fotografias, vídeos, gravações de áudio ou qualquer gravação que revele a intimidade sexual de uma pessoa sem o seu consentimento, punível com pena de reclusão de seis meses a um ano, além de multa. Esse dispositivo também tipifica como fato punível a edição digital de arquivos, como a inserção da imagem de uma pessoa em cenas de nudez ou atos sexuais (*deepfakes*). Assim, esse tipo de conduta criminosa é um violento atentado à privacidade e à dignidade sexual no ambiente digital, podendo ensejar em consequências irreparáveis à vítima. É perceptível, portanto, o caráter essencial da expressa garantia da responsabilização criminal.

2.8.2 Pornografia de vingança (revenge porn)

Pornografia de vingança é a divulgação não consensual de imagens ou vídeos de nudez ou atos sexuais, frequentemente praticada por ex-parceiros com o objetivo de humilhar a vítima ou se vingar. Com o fim de punir e combater essa prática, a Lei nº 13.718/2018 incluiu o artigo 218-C no Código Penal, prevendo pena de prisão de um a cinco anos para quem oferecer, transmitir, disseminar ou vender vídeos íntimos sem consentimento da vítima. O parágrafo primeiro aumenta a pena quando o delito é cometido por pessoa que tem ou teve relação íntima com a vítima ou com intenção de vingança. Essa qualificação legal protege a dignidade sexual e a privacidade das vítimas, além de consistir em uma resposta legislativa

imprescindível ante ao crescente fenômeno nas mídias sociais, que facilita o compartilhamento rápido e massivo de conteúdo íntimo.

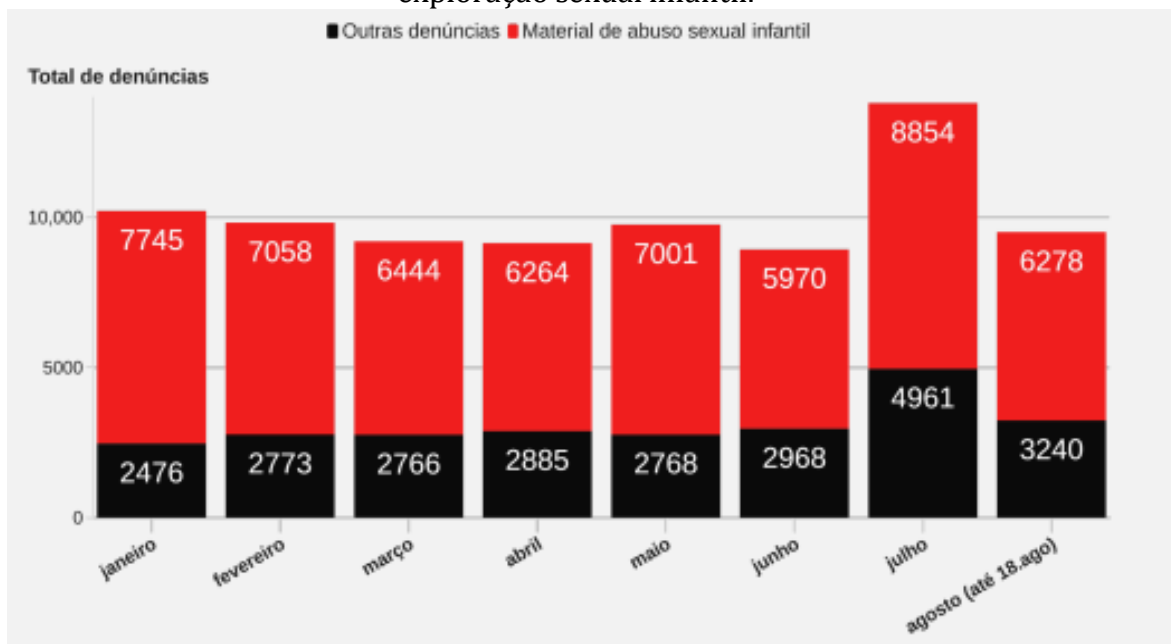
2.9 Pornografia infantil

A pornografia infantil constitui grave violação dos direitos fundamentais da criança e do adolescente. O Estatuto da Criança e do Adolescente (ECA), nos artigos 240 a 241-E, e a Lei nº 11.829/2008, estabelecem as condutas relacionadas à produção, posse, distribuição e comercialização de material pornográfico envolvendo menores, sobretudo no ambiente digital.

De acordo com o artigo 241-A do ECA, a divulgação de pornografia infantil configura crime formal, de forma que a simples disponibilização ou transmissão de imagens ou vídeos de cenas sexuais de crianças e adolescentes, passa a ser punível com pena de três a seis anos de reclusão, mais multa. O artigo 241-C, em semelhança ao artigo 216-B do Código Penal, passa a abarcar de forma específica as situações de simulação e montagens digitais, determinando como punível, com pena de um a três anos de reclusão, a criação de imagens ou vídeos falsos com menores, como *deepfakes*. Isso garante proteção mesmo sem contato físico, ampliando a tutela da dignidade infantil. Já o artigo 241-D, é direcionado a prática criminosa de *grooming*. De acordo com o Centro Internet Segura o termo *grooming* pode ser tratado como sinônimo de aliciamento online. Refere-se à aproximação de crianças com fins sexuais por meio de aplicativos, redes sociais ou jogos online. A lei pune a tentativa de contato com finalidade libidinosa, antecipando a tutela penal para prevenir abusos mais graves.

Os dados da SaferNet Brasil, organização dedicada à defesa e promoção dos direitos humanos na internet, demonstram a magnitude e vulnerabilidade do ambiente virtual, evidenciando ser fundamental normas eficazes para proteger menores de exploração e violência sexual digital. De acordo com a SaferNet, em 2025 aproximadamente 64% das denúncias recebidas estariam relacionadas a conteúdos digitais de abuso e exploração sexual de crianças e adolescentes, o que representaria o número alarmante de 7 em cada 10 denúncias recebidas.

Figura 1 Quase 7 em cada 10 denúncias à SaferNet Brasil em 2025 são de abuso e exploração sexual infantil.



Fonte 1 Central de Denúncias de Crimes Cibernéticos da SaferNet Brasil.

Convém mencionar ainda que, além do artigo 241-D do ECA, que visa atacar o aliciamento online de crianças e adolescentes, a Câmara dos Deputados, em agosto de 2025 aprovou o Projeto de Lei 2628/2022, o qual dispõe de forma mais específica e rigorosa sobre a proteção de crianças e adolescentes em ambientes digitais. O referido projeto de lei ainda se encontra em fase de tramitação, mas representa uma reação do Poder Legislativo frente o cenário de evidência dos crimes de abuso e exploração sexual infantis.

2.10 Invasão de dispositivo informático

A Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, representou um marco histórico no direito penal brasileiro, pois tipificou a conduta de invasão de dispositivo informático, inserindo o art. 154-A no Código Penal. O nome da lei faz referência ao caso da atriz brasileira Carolina Dieckmann, a qual teve imagens pessoais íntimas extraídas ilegalmente de seu computador e divulgadas sem autorização.

O art. 154-A do Código Penal estabelece que é punível a conduta de acessar dispositivo informático de outrem, conectado ou não à rede de computadores, usando de violação indevida de mecanismo de segurança e com o objetivo de obter,

adulterar ou destruir dados ou informações sem autorização do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita (BRASIL, 1940). A pena prevista é de reclusão de 1 a 4 anos, além de multa. O delito é considerado formal, consumando-se com a mera invasão, ainda que não haja efetiva subtração ou divulgação dos dados.

Ademais, o legislador inseriu o referido tipo penal entre os crimes contra a inviolabilidade dos segredos, o que evidencia a intenção do bem jurídico imediato protegido. De modo complementar, conforme entendimentos doutrinários, essa evolução legislativa não apenas visou proteger a inviolabilidade dos segredos, mas também a intimidade, segurança informática, assim como a privacidade em seu sentido amplo.

3 AUTORES E VÍTIMAS DOS CRIMES CIBERNÉTICOS

O crescente fenômeno do crime cibernético impõe novos desafios não apenas ao Direito Penal, mas também a todo o sistema jurídico, exigindo atualizações constantes para definir e responsabilizar esses comportamentos. Este capítulo tem como objetivo analisar criticamente os sujeitos ativos e passivos do crime cibernético, destacando a evolução ao longo do tempo, as consequências jurídicas e o que os números mais recentes mostram.

3.1 Autores dos crimes cibernéticos

Conforme a doutrina brasileira majoritária, o sujeito ativo de um crime é aquele que realiza a conduta descrita no tipo penal, ou que possui o domínio final do fato. De acordo com Damásio de Jesus (2011, p. 207), “é quem pratica o fato descrito na norma penal incriminadora”. No contexto de crimes cibernéticos, pode-se concluir que o autor é o indivíduo que, utilizando recursos informáticos, pratica infração penal.

Destaca-se que a maior parte desses crimes o sujeito ativo é comum, ou seja, não necessita de uma qualidade especial. Isso significa que qualquer pessoa com acesso à internet pode se tornar um autor de crime cibernético, assim, os agentes variam de simples usuários comuns de redes sociais a indivíduos com habilidades técnicas capazes de invadir bancos de dados e burlar sistemas de segurança.

De acordo com a teoria extensiva da autoria, o sujeito ativo do crime não se limita aquele que pratica a conduta criminosa de maneira complexa ou apurada. Também responde como autor aquele que, ainda que de maneira simples, produz de forma eficaz o resultado previsto no tipo penal. Por essa concepção, no ambiente digital, o simples ato de clicar em “compartilhar” uma fotografia íntima sem o consentimento, ou de propagar uma notícia falsa ofensiva, já configura autoria. Assim, qualquer usuário comum também se torna responsável pelo aumento dos cibercrimes, mostrando que a criminalidade digital afeta todas as camadas da sociedade.

Ainda assim, mesmo diante da constatação de que qualquer pessoa comum pode ser um autor de crime cibernético, alguns perfis se destacam, muitas vezes marcados por elevado conhecimento técnico e capacidade de manipulação de sistemas digitais. Conforme Tarcisio Teixeira (2014, p.379-381), é possível classificar alguns perfis de agentes: os *hackers* – especialistas em informática capazes de invadir sistemas, podendo agir para o bem ou para o mal; os *crackers* – usam suas habilidades exclusivamente para fins criminosos; os *insiders* – empregados ou colaboradores que usam o acesso privilegiado para fins ilícitos; os *phreakers* – fraudadores especializados em meios de comunicação, como telefonia; e os *pammers* – responsáveis pelo envio massivo de mensagens eletrônicas não solicitadas.

Esses tipos de agentes, por vezes, invadem dispositivos informáticos e se utilizam de softwares para captar dados, segundo David Silva Ramalho (2013, p. 203), o *keylogger*, software cujo nome resulta da junção das palavras *keystroke* (tecla) e *logging* (registro), consiste em um programa malicioso capaz de registrar e transmitir informações sobre todas as teclas digitadas pelo usuário, possibilitando o acesso a senhas, dados bancários e demais informações sensíveis, o que evidencia o seu uso frequente em práticas criminosas digitais. O autor, geralmente com conhecimentos avançados em programação e segurança da informação, invade o sistema da vítima e instala o software sem que ela perceba. Esse tipo de conduta configura o crime previsto no art. 154-A do Código Penal, invasão de dispositivo informático, introduzido pela Lei nº 12.737/2012 (Lei Carolina Dieckmann).

No que diz respeito aos crimes sexuais, de acordo com Moraes (2017):

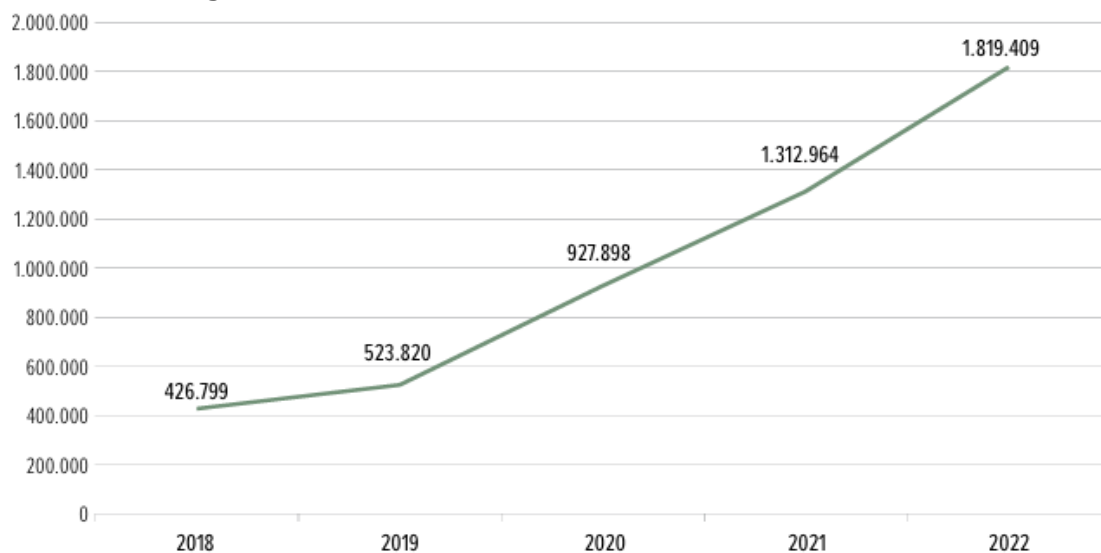
[...]a rede mundial de computadores se tornou plataforma para a realização de crimes sexuais ou de conotação sexual, principalmente no que concerne a vítimas com personalidade em formação, como crianças e adolescentes. A propósito, infelizmente a internet é o terreno quase perfeito à prática de crimes contra a liberdade e a autodeterminação sexual de menores, que são constrangidos a praticar atos libidinosos através da web [...]

Nesta mesma esteira estão os delitos sexuais cometidos contra crianças e adolescentes, que acontecem em suas mais diversas formas como aliciamento, pornografia infantil e exposição não autorizada de imagens. Assim, em meio a essa diversidade de ocorrências, o perfil do autor varia, podendo ser identificados personas como as dos: aliciadores, indivíduos que, em chats ou redes sociais, estabelecem contato para seduzir ou preparar encontros presenciais, também conhecido como *grooming* (Ellovitch, 2023), consumidores de pornografia infantil, usuários que baixam, compartilham ou mantêm em seus dispositivos arquivos com cenas envolvendo menores, não havendo um perfil específico de indivíduo que consomem esse tipo de conteúdo, conforme afirma André Abreu Magalhães (2015), perito da Polícia Federal em entrevista concedida ao canal de notícia da Câmara dos Deputados. Desse modo, os difusores de conteúdo íntimo, adolescentes ou adultos, compartilham imagens de parceiros ou colegas, muitas vezes sem perceber a gravidade jurídica da conduta. Como forma de repressão as estas condutas, em 2018, por meio da Lei 13.718, foi inserido ao Código Penal o artigo 218-C, o qual se destinou a criminalizar a conduta de divulgar e compartilhar cenas de nudez sem o consentimento das vítimas.

Em relação às fraudes eletrônicas, um dos principais tipos de crimes cibernéticos envolvendo o patrimônio, por vezes, é verificado nas condutas conhecimento técnico avançado, como hackear sistemas ou criar sites falsos. De igual modo, também são praticados por indivíduos com conhecimento técnico limitado, que simplesmente replicam padrões preestabelecidos, como o envio de mensagens via WhatsApp solicitando transferências de dinheiro, ocasião em que o autor finge ser parente ou amigo das vítimas.

Conforme dados do Anuário de Segurança Pública de 2023, entre 2018 e 2022 os crimes de estelionato registrados pelas Polícias Civil cresceram 326,3%, os números que eram de 426.799 casos em 2018, passaram para 1.819.409 em 2022.

Figura 2 Ocorrências de Estelionato Brasil, 2018 – 2022.



Fonte 2 Secretarias Estaduais de Segurança Pública e/ou Defesa Social; Fórum Brasileiro de Segurança Pública.

Vale acrescentar que, não se pode ignorar a participação de pessoas jurídicas da discussão em torno da autoria de crimes cibernéticos. O Supremo Tribunal Federal, no julgamento do RE 548.181/PR, admitiu a responsabilidade penal de pessoas jurídicas em crimes ambientais. Da mesma forma, Cestari, Naspolini e Fuller (2023, p.299), compreendem a viabilidade dessa lógica para certos delitos informáticos, sobretudo os relacionados à proteção de dados pessoais, desde que instituídos por lei ordinária. A publicação do Decreto presidencial 11.491/23, o qual consagrou a adesão do Brasil à Convenção de Budapeste é um exemplo forte de entendimento de que pessoas jurídicas podem ser responsabilizadas pelo cometimento de crimes cibernéticos, já que em seu artigo 12, estipula que as partes signatárias devem adotar medidas legislativas para assegurar que esse tipo de agente cometa os crimes tipificados pela mesma Convenção.

3.2 Vítimas dos crimes cibernéticos

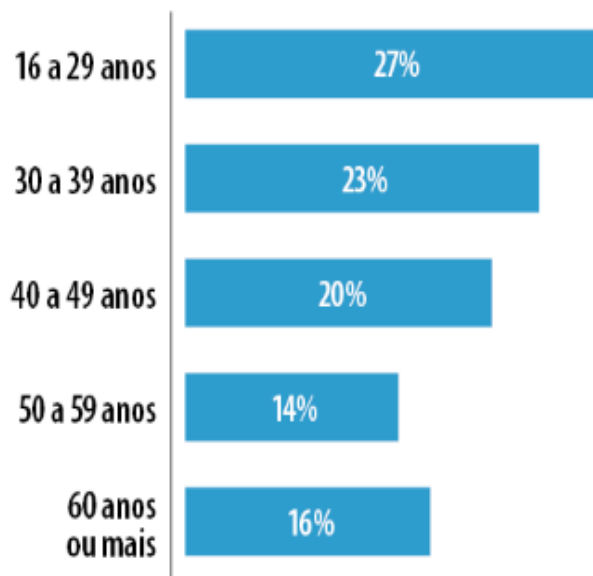
No Direito Penal, conforme interpretação doutrinária, a vítima é o sujeito passivo do delito, ou seja, o titular do bem jurídico lesado ou exposto a perigo. Desse

modo, em se tratando dos crimes cibernéticos, vítima pode ser tanto pessoa física quanto pessoa jurídica, a depender do bem jurídico protegido. Rogério Sanches (2015, p. 150) define como sujeito passivo “a pessoa ou ente que sofre as consequências da infração penal. Pode figurar como sujeito passivo qualquer pessoa física ou jurídica, ou mesmo ente indeterminado, destituído de personalidade jurídica (ex: coletividade, família, etc.), caso em que o crime é chamado pela doutrina de vago.”

A esse respeito, para Rogério Greco (2015, p. 236), o sujeito passivo pode ser considerado formal ou materialmente. Em suas lições, ensina que o sujeito formal será o Estado, toda vez que um regramento legal é desobedecido. De outro modo, o sujeito material, é o titular do bem jurídico tutelado sobre quem recairá a conduta criminosa, que, em alguns casos, também pode ser o Estado. Por conseguinte, nas infrações digitais, a vítima pode variar entre um indivíduo, uma empresa ou até mesmo a coletividade. Assim, pessoas físicas são vítimas de estelionatos eletrônicos, fraudes bancárias, crimes contra a honra e pornografia. Já as coletividades, são impactadas por crimes de ódio, fake news e invasões a sistemas de dados. As instituições empresariais são alvos de ataques de *ransomware*, espionagem industrial e vazamento de dados, da mesma forma, o próprio Estado pode ser vítima de crimes de sabotagem digital e espionagem.

Assim como os autores, as vítimas dos crimes cibernéticos também aumentaram em número e em variedade ao longo do tempo. Em relação às pessoas físicas, uma pesquisa nacional realizada pelo Instituto DataSenado em 2024 sobre os crimes digitais contra o patrimônio apurou que 24 % da população com mais de 16 anos sofreu algum tipo de golpe digital nos 12 meses anteriores, o que representa aproximadamente 40,85 milhões de vítimas. Essa pesquisa apurou não haver um perfil socioeconômico claro: variáveis como renda, escolaridade, gênero e raça distribuem-se de maneira semelhante às da população geral. “A pesquisa não evidencia que os idosos sofrem mais golpes”, afirmou Marcos Ruben de Oliveira (2025), coordenador do Instituto DataSenado. O gráfico a seguir evidencia os números da pesquisa por faixa etária.

Figura 3 População que perdeu dinheiro por algum crime como clonagem de cartão, fraude na internet ou invasão de contas bancárias por faixa etária.



Fonte 3- Instituto de pesquisa DataSenado.

Em segunda análise, certos grupos enfrentam riscos específicos em relação a alguns tipos de crimes. As mulheres, por exemplo, tornaram-se alvo de violência cibernética sob formas como pornografia de vingança, divulgação não autorizada de conteúdos audiovisuais íntimos por ex-parceiros, e assédio sexual on-line. Desde 2018, a legislação brasileira passou a prever punição específica para quem divulga cenas de nudez ou sexo de alguém sem consentimento, o artigo 218-C do CP, introduzido pela Lei 13.718/2018, face à recorrência de casos contra a honra e privacidade das vítimas.

De acordo com matéria jornalística publicada pela CNN Brasil, dados do Instituto de Segurança Pública (ISP) do Rio de Janeiro, em pesquisa realizada entre 2018 e 2024 demonstraram um aumento de 1.252 % em crimes sexuais praticados via internet. Esse relatório demonstrou que mulheres são as principais vítimas, e muitos agressores são ex-companheiros. Essa pesquisa aponta que 86,6% das vítimas de divulgação de cenas com conteúdos sexuais na internet são mulheres.

A Ministra do STJ, Nancy Andrighi, em decisão proferida em 2018, Recurso Especial Nº 1.679.465 /SP, destacou que a "exposição pornográfica não consentida", entre as quais a "pornografia de vingança", configura uma grave violação aos

direitos de personalidade, e deve ser reconhecida como uma forma de violência de gênero, exigindo resposta penal e reparatória eficaz.

Ainda sobre o mesmo teor, o Tribunal de Justiça do Distrito Federal e dos Territórios, em 2020 ao julgar Apelação Criminal 0000712-30.2019.8.07.0009 (Acórdão nº 1231584), confirmou que a divulgação de imagens e vídeos íntimos de ex-namorada em rede social, sem o consentimento dela, configura crime previsto no artigo 218-C do Código Penal. Além da configuração penal, a decisão reconheceu o ato como violação aos direitos da personalidade. Nesta ocasião, o ex-namorado foi condenado penalmente e condenado a pagar indenização por danos morais de R\$ 2.000,00.

De igual modo, outro grupo especialmente vulnerável no ambiente virtual são as crianças e adolescentes. Pois, conforme dito anteriormente, a internet facilita a ação de predadores sexuais, resultando em crimes como aliciamento de menores, produção e disseminação de pornografia infantil e o chamado “estupro virtual”. Tais condutas configuram crimes gravíssimos, tipificados como estupro de vulnerável, previsto no artigo 217-A, do CP ou exploração sexual infanto-juvenil artigos 240 e 241 do ECA.

De acordo com relatório divulgado pela SaferNet Brasil, organização de referência no monitoramento de crimes digitais no país, o ano de 2023 registrou 71.867 novas denúncias de imagens de abuso e exploração sexual infantil na internet. Um crescimento de 77,13% em relação a 2022.

Acerca do tema, em 2023, a Terceira Seção do STJ, em julgamento de temas repetitivos, decidiu que os crimes previstos nos artigos. 241-A, divulgar, e 241-B, possuir ou armazenar, do ECA são autônomos, com condutas distintas. Isso permite o reconhecimento de concurso material, ou seja, as penas podem ser somadas quando coexistem as duas condutas. Esse precedente qualificado uniformiza a interpretação no Brasil e reforça que armazenar imagens, mesmo que não se divulgue, é conduta punível e não mera preparação ou fase de execução de outro delito.

Por fim, vale citar que empresas, governos e instituições também são vítimas frequentes de crimes cibernéticos. Segundo Rogério Sanches, como dito no início desta seção, a vítima de um crime não se restringe à pessoa natural. Logo, pessoas jurídicas também podem figurar como sujeito passivo quando o bem jurídico protegido é compatível com sua natureza, como é o caso da inviolabilidade de seus sistemas informatizados. Para o fim da proteção contra violação de sistemas de pessoas físicas, o artigo 154-A do CP é um dos dispositivos legais também aplicado para esses casos.

Diante desse panorama, ataques a dados corporativos e infraestruturas críticas é uma realidade preocupante. A título de exemplo, em julho de 2025, um ataque cibernético contra a C&M Software, empresa responsável por interligar instituições financeiras ao SPB/Pix, permitiu o acesso indevido a contas reserva mantidas no Banco Central. O valor desviado estimado oscilou entre R\$ 541 milhões e R\$ 800 milhões, com algumas fontes indicando um prejuízo potencial de até R\$ 1 bilhão. Nessa ocasião, um operador de TI foi preso pela Polícia Civil de São Paulo como principal suspeito de facilitar o ataque.

Isto posto, percebe-se que os autores de cibercrimes não são apenas os hackers altamente técnicos, mas também usuários comuns. Da mesma forma, as vítimas dos crimes cibernéticos não se restringem a indivíduos em sua esfera privada, mas englobam também instituições e até mesmo a coletividade quando serviços essenciais são afetados. Considerando o entendimento majoritário reafirmado por Rogério Sanches, de que pessoas físicas ou jurídicas podem ser consideradas vítimas, desde que a conduta delitiva recaia sobre bens jurídicos inerentes à cada uma delas, no contexto digital, conclui-se que estão ligados tanto a honra e a intimidade da pessoa física quanto os dados estratégicos e segredos industriais das pessoas jurídicas. Portanto, é evidente que o perfil das vítimas se diversificou, acompanhando a expansão da internet e o avanço das formas de criminalidade virtual.

4 DA RESPONSABILIZAÇÃO POR CRIMES CIBERNÉTICOS

Vistos alguns dos tipos penais que podem ser classificados como crimes cibernéticos, sejam eles em sua modalidade própria ou imprópria, o presente capítulo se destinará a discorrer sobre os mecanismos legais que têm sido editados ao longo do tempo no ordenamento jurídico brasileiro para que condutas criminais desse tipo pudessem ser responsabilizadas. Assim como, serão trazidas à tona as discussões em torno das responsabilidades que podem recair sobre as pessoas físicas e jurídicas envolvidas nos contextos de crimes cibernéticos.

4.1 Mecanismos legais

Com o intuito de garantir a segurança dos usuários da rede mundial de internet, ao longo dos tempos foram editadas leis que alteraram o Código Penal Brasileiro, assim como reestruturaram a aplicação do direito penal no que tange ao assunto.

Em 2012 foi sancionada a Lei 12.737/2012, conhecida como Lei Carolina Dieckmann, nome da atriz brasileira que, em 2011, teve seu computador invadido por um hacker o qual acessou suas fotos íntimas e passou a extorqui-la exigindo determinada quantia em dinheiro como forma de garantia de que as imagens não seriam disseminadas na internet. Houve a recusa da vítima em promover o pagamento da quantia exigida pelo autor, o que culminou na divulgação das fotos. O caso ganhou repercussão e serviu como catalisador para as discussões jurídicas em torno do tema, contribuindo para que, no ano seguinte, fosse sancionada a Lei 12.737/2012, que alterou a redação dos artigos 266 e 298, e editou os artigos 154-A e 154 B do CP.

O Art 154-A trouxe a tipificação da conduta de “invasão de dispositivo informático”, que passou a punir a invasão de sistema alheio para obter, adulterar ou destruir dados. O Artigo 266, em sua nova redação trouxe a penalização para aqueles que interromperem, impedirem ou dificultarem o restabelecimento de serviço telemático ou de informação de utilidade pública. Já o artigo 298, sofreu a adição do parágrafo único, o qual equiparou o cartão de crédito de débito a

documento particular de modo que a tipificação de falsificação de documento particular passasse também a alcançar estes dois últimos objetos desde então.

Ainda em 2012, fora sancionada a Lei 12.735/2012, esta passou a tipificar as condutas realizadas mediante sistema eletrônico e afins, praticadas contra sistemas informatizados e similares. Ademais, determinou a mobilização dos órgãos de polícia judiciária em prol do combate à ação delituosa em rede computadores, dispositivo de comunicação ou sistema informatizado (BRASIL, 2012).

Convém trazer à baila, o Marco Civil da Internet como uma das ferramentas mais expressivas para regulamentação das ações da sociedade quando em uso do ambiente virtual. Por meio da lei 12.965/2014, foram instituídos princípios, garantias, direitos e deveres para o uso da internet no Brasil. Foram princípios estipulados para orientar a interpretação e aplicação da lei: a garantia da liberdade de expressão, comunicação e manifestação do pensamento; a proteção da privacidade e dos dados pessoais; a preservação e garantia da neutralidade da rede; a estabilidade, segurança e funcionalidade da internet; a responsabilização dos agentes pelos atos praticados; a preservação da natureza participativa da rede; e a liberdade dos modelos de negócios online, desde que respeitem os demais princípios (BRASIL, 2014).

Entre esses princípios, atenção especial deve ser dada a responsabilização dos agentes pelos atos praticados, núcleo da discussão deste capítulo. A busca pela garantia da responsabilização tem se mostrado um grande desafio para os operadores da lei, dadas as dificuldades de coleta de evidências digitais, a grande variedade de técnicas de anonimato praticadas pelos autores e a determinação dos limites de responsabilização dos envolvidos.

Nesse sentido:

A investigação e a punição de crimes virtuais também apresentam desafios únicos. A natureza global da internet muitas vezes dificulta a identificação de criminosos e a cooperação internacional é necessária para combater eficazmente esses delitos. Além disso, as leis e regulamentações relacionadas aos crimes virtuais variam amplamente de país para país, tornando a aplicação da lei uma tarefa complexa. (Lopes & Lopes, 2023, p. 467)

Ressalta-se que a Convenção de Budapeste tem como um de seus objetivos promover essa cooperação internacional necessária para atingir a face da transnacionalidade dos crimes cibernéticos, a qual Lopes & Lopes (2023) citou. Diante desta necessidade, a convenção buscou viabilizar a harmonização das legislações de cada país dedicando o Capítulo II à tipificação de condutas que devem estar presentes nas legislações nacionais, sendo elas: o acesso ilegal, a interceptação ilícita de comunicações, a violação de dados, a interferência em sistemas, o uso indevido de aparelhagem, a falsificação e a fraude informática, assim como a pornografia infantil, a violação de direitos autorais e correlatos, e a tentativa, auxílio ou instigação à prática dos crimes anteriormente citados.

Os procedimentos processuais também foram alcançados pela convenção. A Seção 2 buscou padronizar algumas medidas que devem ser perseguidas para que as investigações e processos criminais se tornem cada vez mais eficazes diante da realidade da era digital. Uma dessas medidas é a ordem de exibição, prevista no artigo 18, a qual prevê que devem ser instituídos mecanismos que permitam às autoridades competentes ordenar a qualquer pessoa que resida em seu território a disponibilizar os dados, controlados ou detidos por ela, que estejam armazenados em sistema ou qualquer meio de armazenamento de computador. Desta forma, a autoridade competente poderá determinar que qualquer pessoa, física ou jurídica, forneça as informações especificadas sem necessidade de busca ou apreensão física, que também é assegurada no artigo 19 da mesma norma, dando mais celeridade ao procedimento.

Percebe-se, portanto, que os desafios da responsabilização ultrapassam a necessidade de apenas tipificar as condutas. Tem se mostrado cada vez mais importante voltar os olhos para a implementação de engenharias de identificação das autorias, cooperação internacional de esforços, para que as legislações até então editadas atinjam a suas eficácias pretendidas, sejam elas regular, coibir ou punir.

4.2 Da responsabilização da pessoa física

No que tange à responsabilidade penal, Fernando Capez (2019) ensina que essa se trata do dever de responder penalmente, quando presentes condições como

a subjetividade, ou seja, a culpa ou o dolo, a imputabilidade e a culpabilidade. Seguindo uma linha de pensamento muito parecida, Nucci (2012) traz em seus escritos que a “responsabilidade penal significa a possibilidade de se atribuir a alguém a prática de um fato típico e ilícito, desde que seja imputável, tenha consciência potencial da ilicitude do fato e lhe fosse exigível conduta diversa” (Nucci, 2012, p. 321).

Convém salientar que a doutrina majoritária entende que a responsabilização penal exige a subjetividade, ou seja, dolo ou culpa, exceto quando se tratar de situações específicas constitucionalmente previstas, onde a responsabilidade penal será objetiva.

A responsabilidade penal, no direito brasileiro, é subjetiva. Exige-se dolo ou culpa para que o agente seja punido, sendo inadmissível a responsabilidade objetiva em matéria penal, salvo na hipótese constitucionalmente admitida da pessoa jurídica em crimes ambientais. (Nucci, 2020, p. 206).

Nesse sentido, pode-se inferir que todo aquele indivíduo que realizar as condutas típicas como, por exemplo as elencadas entre os artigos 154-A e 154 B do CP, podem ser passíveis de punição, desde que presente a conduta que efetivamente contrarie a legislação e o elemento da culpabilidade.

Todavia, como tratado anteriormente, um dos desafios atualmente enfrentados pela justiça, no que se refere à punição efetiva dos autores de crimes cibernéticos, está na dificuldade de identificação destes, já que, em sua grande maioria, os autores buscam se revestir do anonimato em redes e da não rastreabilidade de IP (*Internet Protocol*), endereço do dispositivo utilizado no fluxo de troca de dados pela internet, para encobrir a autoria. Assim, mesmo com os dispositivos legais já existentes, a realidade que ainda vigora é a da impunidade.

4.3 Da responsabilização da pessoa jurídica

Diante da realidade de impunidade que ainda vigora sobre a temática e necessidade de reparar danos que recorrentemente tem ultrapassado os limites pessoais e alcançado a coletividade, muito tem se questionado sobre a responsabilidade penal das pessoas jurídicas pela prática de crimes cibernéticos.

Em abril de 2023, o Brasil promulgou o Decreto nº 11.491/2023, o qual teve como finalidade tornar lei o acordo firmado na Convenção de Budapeste para o Crime Cibernético em 2001. A Convenção buscou estabelecer formas de cooperação internacional, tratando da criminalização de condutas, da harmonização das legislações, assim como a fomentação de medidas para facilitar a descoberta, a investigação e o julgamentos dessas infrações penais.

A Convenção, destinou seu artigo 12 à responsabilização penal das pessoas jurídicas, determinando que seja assegurado a responsabilidade dessas por crimes tipificados com base na convenção, quando praticados em seus benefícios por qualquer pessoas em posição de direção, tendo o indivíduo agido de forma individual ou como integrante da própria pessoa jurídica. Vale ressaltar que, atualmente, no Brasil, a responsabilidade penal da Pessoa Jurídica só é prevista nos casos de crimes ambientais, conforme artigo 225, § 3º da Constituição Federal de 1988.

Eládio Lecey (2001), em seus estudos sobre a responsabilidade penal em crimes de direito ambiental diz que:

A complexidade dos interesses em jogo na estrutura das pessoas jurídicas pode levar à irresponsabilidade organizada dos indivíduos (...). A diluição da responsabilidade não raro é buscada deliberadamente, com a utilização de mecanismos colegiados de decisão. (Lecey apud Costa e Buzetti , 2024, p.127).

De forma comparativa, a referida reflexão do autor se molda perfeitamente à questão da responsabilidade das pessoas jurídicas quanto aos cibercrimes, em função de se tornar cada vez mais perceptível que, quanto mais os indivíduos seguem setorizando suas responsabilidades dentro das estruturas complexas que as pessoas jurídicas carregam, se recobrem dessa complexidade para minimizar os impactos que uma eventual punição pode causar. Quanto mais esses atores se sentem longe da possibilidade de responsabilização, menor é a preocupação em lidar com as problemáticas que o ambiente virtual carrega.

Convém salientar que, em se tratando de responsabilidade penal ambiental, parte considerável da base dessa responsabilização oriunda do entendimento de que crimes ambientais devem ser entendidos como crimes de perigo, ou seja,

“dispensa a efetiva lesão, configurando-se com a simples exposição do bem jurídico a perigo” (CUNHA, 2015, p. 162). A Lei 9.605/1998, Lei de Crimes Ambientais possuem tipos penais que visam tutelar o meio ambiente por um viés preventivo, atuando antes que o dano se concretize. Sobre a temática, o relator do Recurso especial nº 1.439.150-RS (2014/0047232-9), Ministro Rogério Schetti Cruz, ao julgar recurso sobre crime ambiental previsto no art. 56, caput, Lei 9.605/1998, que prevê como crime o transporte irregular de produto ou substância tóxica, nociva à saúde pública ou ao meio ambiente, expressou:

EMENTA RECURSO ESPECIAL. CRIME AMBIENTAL. TRANSPORTE DE PRODUTOS TÓXICOS, NOCIVOS OU PERIGOSOS. ART. 56, CAPUT, DA LEI N. 9.605/1998. LEI PENAL EM BRANCO. RESOLUÇÃO DA ANTT N. 420/2004. NORMA DE INTEGRAÇÃO. BEM JURÍDICO TUTELADO. MEIO AMBIENTE E INCOLUMIDADE PÚBLICA. CRIME DE PERIGO ABSTRATO. PERÍCIA. PRESCINDIBILIDADE. RECURSO ESPECIAL CONHECIDO E PROVIDO. (...)2. Por outro lado, a conduta ilícita prevista no art. 56, caput, da Lei n. 9.605/1998 é de perigo abstrato. Não é exigível, pois, para o aperfeiçoamento do crime, a ocorrência de lesão ou de perigo de dano concreto na conduta de quem produz, processa, embala, importa, exporta, comercializa, fornece, transporta, armazena, guarda, tem em depósito ou usa produto ou substância tóxica, perigosa ou nociva à saúde humana ou ao meio ambiente, em desacordo com as exigências estabelecidas em leis ou nos seus regulamentos. 3. Embora seja legítimo aspirar a um Direito Penal de mínima intervenção, não pode a dogmática penal descurar de seu objetivo de proteger bens jurídicos de reconhecido relevo, assim entendidos, na Documento: 1644265 - Inteiro Teor do Acórdão - Site certificado - DJe: 16/10/2017 Página 1 de 4 dicção de Claus Roxin, como “interesses humanos necessitados de proteção penal”, qual a proteção ao meio ambiente e à incolumidade pública. Não se pode, assim, esperar a concretização de danos, ou exigir a demonstração de riscos concretos para a punição de condutas que representam potencial produção de danos ao ecossistema e, por consequência, a pessoas indeterminadas. (BRASIL, 2017).

Nessa perspectiva, pode-se, a título de comparação, imaginar que um vazamento de dados de uma infraestrutura crítica, como de serviços financeiros e energia, teria consequências tão nocivas quanto um vazamento de substância tóxica no meio ambiente, atingindo não apenas a individualidade de cada pessoa vítima, mas também uma sociedade em sua coletividade, tornando-se imperioso a adoção de uma postura mais interventiva sobre o tema. Os direitos ambientais fazem parte dos direitos fundamentais de terceira geração, que se fizeram essenciais diante das

profundas alterações sociais geradas pelo desenvolvimento tecnológico e científico (LENZA, 2018). Na esteira deste desenvolvimento também veio a infeliz potencialização de crimes pelo ambiente virtual, ofendendo direitos que essa terceira geração destinou-se a garantir. O caráter transnacional e coletivo desses crimes, pressupõe uma abordagem de combate nas mesmas proporções, tornando analogia entre direito ambiental e o direito cibernético, no que se refere a responsabilidade penal da pessoa jurídica, um caminho com expressivo potencial de sucesso.

O crime de perigo, no caso do referido julgado, se enquadra no que a doutrina diz como abstrato, dispensando a comprovação de que ocorreu o perigo de forma efetiva, considerando o simples acontecimento da conduta para que o crime se configure. Por outro lado, o crime de perigo concreto exige a comprovação do risco, que de acordo com a Rogério Sanches (2015, p.162) pode ser individual ou coletivo, sendo que no primeiro a exposição ao risco será sofrida por um grupo quantificado de pessoas ou apenas uma; enquanto na segunda, a exposição ao risco será sofrida por um número indeterminado de pessoas.

Quando se trata de incidentes de segurança, eventos em que há uma violação da segurança dos dados (Susskind, 2024), os mais sensíveis são os que envolvem vazamento de dados pessoais, pois a exposição desses dados deixam os seus titulares mais propensos a se tornarem vítimas de crimes cibernéticos como fraudes e extorsões. A Lei Geral de Proteção de Dados (Lei 13.709/2018), não prevê tipificação penal para o vazamento de dados, apenas sanções de natureza administrativa e civil, limitando a sanção penal apenas aos casos em que o vazamento de dados esteja associado à outros tipos penais já existentes. Uma das dificuldades na responsabilização de penal das pessoas jurídicas nesses casos, passa não só pela ausência de tipo penal específico que permita essa punição, mas também pela dificuldade de entender em qual momento essa responsabilidade se configuraria, se na mera exposição de dados, como acontece nos crimes de perigo, cita-se os ambientais como exemplo, ou na efetiva configuração do dano, que desaguaria nos outros tipos penais já existentes no ordenamento jurídico brasileiro, como os crimes contra a honra, a moral, a privacidade. É cristalino, ante o exposto,

que o caminho e as bases do direito ambiental, facilmente vem servindo e tendem a permanecer como um guia promissor para o movimento de reestruturação do Direito Penal frente aos desafios que os crimes cibernéticos criaram.

A necessidade de adaptação jurídica é latente, já que as ferramentas legais têm se mostrado limitadas. Até mesmo os mecanismos de responsabilidade civil das pessoas jurídicas vêm sendo alvo de novas intervenções. A título de exemplo, o artigo 19 do Marco Civil da Internet, Lei 12.965/2014, que determina que provedores de aplicação são civilmente responsáveis por danos decorrentes de conteúdo de terceiros foi alvo de discussão no Recurso Extraordinário (RE) 1037396 e 1057258. Em junho de 2025, o Supremo Tribunal Federal (STF), julgou parcialmente inconstitucional a regra do artigo 19. O entendimento da maioria foi de que a referida norma “já não é suficiente para proteger direitos fundamentais e a democracia”. O texto da lei diz:

Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário. (BRASIL, Lei 12.965 23 de abril de 2014).

A regra, portanto, seria: a plataforma apenas teria o dever de remover o conteúdo gerado por terceiro quando houvesse ordem judicial, exceto se estivesse relacionada a ações contrárias às regras da provedora de aplicações, ou em situações excepcionalmente previstas na legislação, como é o caso da pornografia infantil.

Ocorre que, apesar da incontestável importância de se prevê essa responsabilidade de responsabilização, a necessidade de judicialização para obtenção de uma ordem legal que determine a remoção do conteúdo ofensivo ou ilegal, mostrou-se insuficiente enquanto resposta prática contra os crimes contra a honra, por exemplo, os quais necessitam ter seus efeitos danosos causados pela publicação cessados o mais rápido possível.

Nesse último caso, o STF, em relação ao Recurso Extraordinário 1037396, também tema de repercussão geral nº 987, decidiu pelo:

Reconhecimento da inconstitucionalidade parcial e progressiva do art. 19 do MCI 1. O art. 19 da Lei nº 12.965/2014 (Marco Civil da Internet), que exige ordem judicial específica para a responsabilização civil de provedor de aplicações de internet por danos decorrentes de conteúdo gerado por terceiros, é parcialmente inconstitucional. Há um estado de omissão parcial que decorre do fato de que a regra geral do art. 19 não confere proteção suficiente a bens jurídicos constitucionais de alta relevância (proteção de direitos fundamentais e da democracia). Interpretação do art. 19 do MCI 2. Enquanto não sobrevier nova legislação, o art. 19 do MCI deve ser interpretado de forma que os provedores de aplicação de internet estão sujeitos à responsabilização civil, ressalvada a aplicação das disposições específicas da legislação eleitoral e os atos normativos expedidos pelo TSE. 3. O provedor de aplicações de internet será responsabilizado civilmente, nos termos do art. 21 do MCI, pelos danos decorrentes de conteúdos gerados por terceiros em casos de crime ou atos ilícitos, sem prejuízo do dever de remoção do conteúdo. Aplica-se a mesma regra nos casos de contas denunciadas como inautênticas. 3.1. Nas hipóteses de crime contra a honra aplica-se o art. 19 do MCI, sem prejuízo da possibilidade de remoção por notificação extrajudicial. [...] (STJ, 2025).

A promulgação do decreto nº 11.491/2023, pelo Brasil, assim como a interpretação comparativa ao que já foi estruturado dentro do Direito Ambiental de decisões como a do STF em relação ao artigo 19 da 12.965/2014, reforçam que a tendência é de que a responsabilização das pessoas jurídicas, em algum percentual, é um dos caminhos que necessitam ser explorados em busca da garantia de não violação de direitos à honra, à privacidade, à infância segura, e outros, dentro do ambiente virtual.

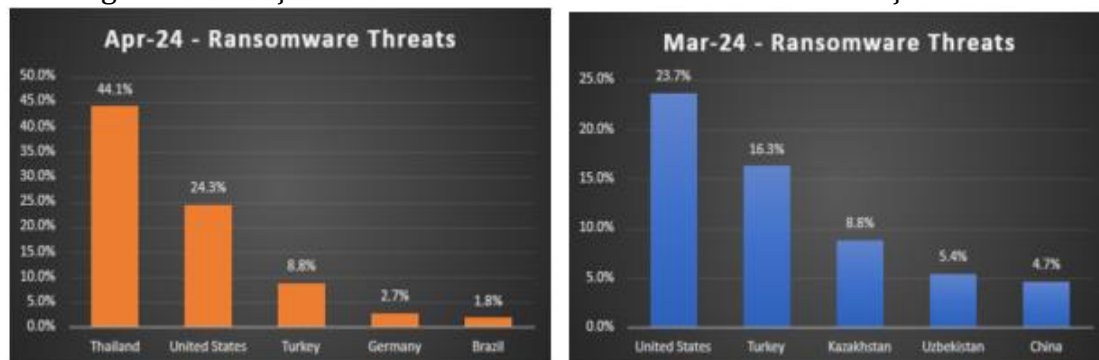
5 AÇÕES DE COMBATE A CIBERCRIMES

Um estudo desenvolvido pela Trend Micro, empresa de soluções em cibersegurança, mostrou que em 2024 os ataques cibernéticos seguiram um tendência de alta, se comparado ao mesmo período do ano anterior. Dados da empresa dão conta de que ações de malware corresponderam a mais de 2 milhões e 300 mil ataques de janeiro a abril de 2024, tendo como principais alvos os setores: governamental, educacional, industrial, de saúde e tecnologia. (TRENDMICRO, 2024)

Em relação ao *ransomware*, tipo de malware destinado a capturar dados confidenciais e exigir valores pecuniários para reaver o acesso a esses dados, o

Brasil ocupou a lista dos cinco países mais atacados por essa modalidade, com 3,5 milhões de ataques registrados até meados de abril de 2024. (TRENDMICRO, 2024).

Figura 4 Ameaças de Ransomware nos meses de abril e março de 2024.



Fonte 4: Relatório da Trend Micro.

Apesar de ser um número muito alto, o mesmo estudo demonstrou que os ataques de *ransomware* tem diminuído, demonstrando que o perfil de ação tem se modificado. De acordo com Rayanne Nunes, diretora de Tecnologia da Trend Micro Brasil, foram registrados menos ataques massivos e mais ações exclusivas, voltadas especialmente para empresas de tecnologias, o governo, saúde serviços financeiros e o setor industrial.

Um exemplo da mudança constante da forma como esses ataques acontecem, são casos de *phishing*, onde os criminosos se passam por entidades confiáveis para obter dados pessoais e confidenciais. De acordo com o referido relatório, foram detectados quase 3 milhões e meio de arquivos maliciosos enviados em formato de spam, nos quatro primeiros meses de 2024. Destes arquivos, os com extensão .PDF foram muito explorados, só em abril foram mais de 1,5 milhão.

Os números apresentados pelo relatório permitem ter uma dimensão do quão amplo é o universo de atuação dos cibercrimes. Diante da imensidão de modalidades e da variedade de agentes afetados por eles, torna-se quase que impossível pensar em uma ação de combate única, uma fórmula pronta para lidar com essas questões.

Os estudos explorados até aqui, tem reforçado veementemente a necessidade de adoção de várias frentes de combate, que compreendem o âmbito individual das pessoas físicas e jurídicas enquanto usuários da rede mundial de internet, o

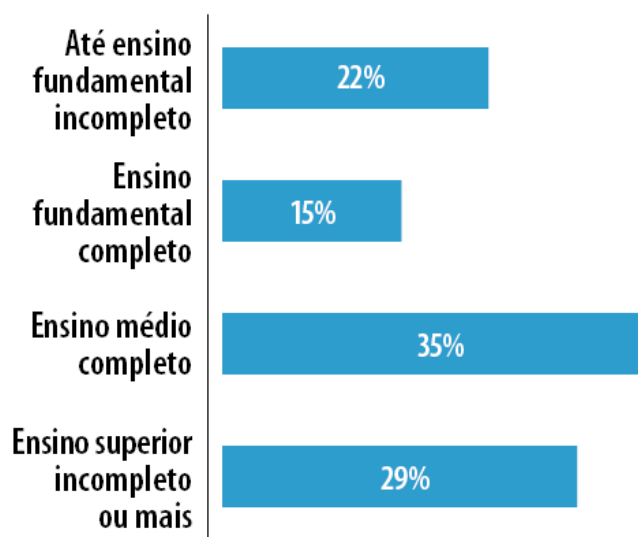
governamental e corporativo, enquanto garantidores de um espaço virtual seguro e as ações de cooperação internacional. Ante o exposto, põe-se a discorrer sobre as ações que têm sido adotadas e quais podem ser implementadas em busca do combate aos cibercrimes.

5.1 Ações no âmbito individual

Como visto até aqui, as modalidades de cibercrimes possuem como alvo inúmeros agentes, empresas privadas, órgãos governamentais, instituições financeiras e também a pessoas física. Possuem também como um dos principais fatores de sua vastidão o uso da rede mundial de internet. Dados do Instituto Brasileiro de Geografia e Estatística (IBGE) dão conta de que, no Brasil, em 2024, a Internet era utilizada em 93,6% dos domicílios particulares, algo que corresponde a 74,9 milhões de domicílios.

O considerável número de pessoas interagindo no espaço virtual e a internet como terreno fértil para atuação de cibercriminosos fez acender um alerta sobre como a postura preventiva do indivíduo deve ser considerada como um dos fatores cruciais no enfretamento a este tipo de delito. A falta de conscientização em relação a segurança cibernética resulta em um aumento da vulnerabilidade. No entanto, fato interessante é que não se pode afirmar que essa falta de conhecimento está necessariamente ligada a baixa escolaridade. Os seguintes dados do Instituto de Pesquisa Data Senado mostram a porcentagem de população que perdeu dinheiro por clonagem de cartão, fraude na internet ou invasão de contas bancárias por escolaridade:

Figura 5 População que perdeu dinheiro por algum crime digital como clonagem de cartão, fraude na internet ou invasão de contas bancárias por escolaridade.



Fonte 5 Instituto de Pesquisa DataSenando.

Os resultados evidenciam que a desinformação sobre os crimes cibernéticos alcança as mais diversas pessoas e seus níveis de escolaridade, buscando explorar em cada uma delas as suas respectivas vulnerabilidades. Visto isso, percebe-se que um ponto de partida importantíssimo contra esses delitos é o investimento constante em políticas de conscientização sobre cibersegurança para o público comum, orientando-os sobre a necessidade de adoção de hábitos seguros como implementação de senhas fortes em seus dispositivos e sistemas, assim como redobrada cautela na interação com links que lhes são apresentados.

Diante desta constatação, o Ministério Público de Minas Gerais –MPMG nos últimos anos, tem implementado o projeto “Chegando Junto”, o qual se destina à emitir anúncios institucionais direcionados em plataformas de busca enquanto os cidadãos realizam pesquisas sensíveis. A intensão com esse anúncios é alertar o usuário dos riscos de prejuízos financeiros quando interagem com determinados tipos de serviços disponíveis no ambiente virtual. Iniciativa parecida também vem sendo adotada pelo Ministério Público do Piauí- MPPI por meio do “Alerta Digital”, projeto por meio do qual a é feito acompanhamento sistemático dos boletins de ocorrência com a finalidade de detectar os golpes e fraudes mais frequentes e posteriormente difundir alertas à população.

A interação das pessoas no ambiente virtual é uma realidade, porventura, também uma necessidade, logo na multidisciplinariedade de ações de combate

precisam estar presentes não só as de repressão por meio dos dispositivos legais, mas também as de prevenção, que precisam ser difundidas ao usuário final.

5.2 Ações no âmbito e corporativo e governamental

A relação de consumo nos últimos tempos foi modificada pelo advento da internet, e cada dia mais empresas tem se utilizado desse recurso para interagir com o público alvo dos seus serviços. Essa interação com as plataformas das referidas empresas, quase sempre vem precedidas da necessidade de um cadastro se usuário, o qual necessita ceder algumas informações pessoais que serão armazenados nos bancos de dados destas empresas. Em outros casos o próprio serviço oferecido, como os de trocas de mensagens, trazem no próprio bojo a prática de partilha de informações pessoais, geralmente armazenados nos bancos de dados dessa prestadora de serviço. Outrora as redes sociais disponibilizadas por essas empresas também têm sido utilizadas para produção de conteúdo de terceiros. Assim sendo, é notório que, não só o próprio indivíduo é responsável pelas informações que divide no ambiente virtual, como também aquele que se destina a propiciar o ambiente de troca e a armazenar as informações cedidas por esses usuários, assunto amplamente explorado quando este estudo se dispôs a tratar da responsabilização por crimes cibernéticos.

Enquanto responsáveis pelos ambientes de interação virtual, essas corporações tem se deparado com os dilemas oriundos o uso dos mecanismos de moderação utilizados atualmente como ferramentas de combate a alguns crimes digitais. Conforme Cruz (2024) “a atividade de moderação de conteúdo caracteriza-se quando a plataforma formula, edita, publica e aplica normas sobre o que pode ou não ser realizado por seus usuários”.

Em alguns momentos, o uso de alguns mecanismos de moderação, estabelecidos inclusive pelo Marco Civil da Internet, foram alvos de Medida Provisória, sob a justificativa de que poderiam estar ferindo a liberdade de expressão dos usuários. A Medida Provisória Nº 1.068, de 06 de setembro de 2021, vedava provedores de redes sociais usar mecanismos de moderação de conteúdo que implicassem censura de ordem, política, ideológica, científica, artística ou

religiosa. A medida provisória foi devolvida ao Congresso Nacional, sendo considerada inconstitucional, dado que seu conteúdo provocava significativas modificações no Marco Civil da Internet, editando novas regras de moderação, tendendo para uma maior garantia dos usuários e uma maior dificuldades para remoção e suspensão de conteúdos ilegais. A necessidade de indicação de justa causa e motivação para o então cancelamento e suspensão de contas e perfis seria um desses dificultadores.

Na busca por um melhor aperfeiçoamento das ações de moderação, a utilização de Inteligência Artificial (IA) tem se mostrado uma aposta para garantir que elas sejam executadas com maior rapidez e em maior escala, duas características cruciais diante do grande volume de postagens que são geradas e da capacidade de disseminação em pouquíssimo tempo. Sobre esse uso da inteligência artificial para moderação, Cruz (2024) destaca:

O campo da IA soma-se nesse esforço na medida em que torna possível “ensinar” computadores a reconhecerem padrões e sinais típicos em conteúdos postados por usuários, entrando em cena quando falamos, por exemplo, das tarefas de detecção, priorização e análise de conteúdos que violam o conjunto de regras das plataformas. (CRUZ,2024).

Percebe-se que a tendência é de que as ações governamentais, legislativas ou programáticas, e corporativas se inclinem para uma margem mais restritiva, observados os limites da garantia da liberdade de expressão, como forma de garantir um ambiente virtual cada vez mais seguro. É inegável que, uma postura nesse sentido acenda alertas em torno de um temor à censura, a final a listagem do que pode ou não ser postado, traz consigo uma sensação de limitação. Mas o que seria do papel do legislador, do gestor público, dos operadores das leis, se não de conciliar esses limites? Importante salientar que no cerne desta discussão está uma crescente nas ações criminosas que usam desse mesmo espaço de virtual para praticar a violação de direitos tão fundamentais quanta à liberdade de expressão.

5.3 Estratégia nacional de cibersegurança

Sobre uma outra ótica, ao longo desta pesquisa percebe-se que o setor corporativo, que compreende esse conjunto de organizações e empresas destinadas

a prestação de serviços, públicos ou privados, também são alvos recorrentes dos autores de cibercrimes, que por meios das mais diversas engenharias criminosas buscam se aproveitar de seus bancos de dados, perfis e ambientes de interação. Por ser assim, é imprescindível a adoção de estratégias nacionais de cibersegurança. No que tange ao assunto, é salutar entender o que seria a segurança cibernética.

De acordo com Silva e Maleta, a segurança cibernética:

Diz respeito à proteção e garantia de utilização de ativos de informação estratégicos, especialmente vinculados às infraestruturas críticas da informação, como redes de comunicação e computadores, bem como à interação com órgãos públicos e privados envolvidos no funcionamento destas infraestruturas. (Silva e Maleta, 2021, p.2).

Basicamente diz respeito a atividades que visem assegurar a utilização de dados, documentos, serviços, de uma forma segura, assim como combater eventuais ameaças que estes possam sofrer, encampando um conjunto de esforços que tenham tanto propósitos preventivos, quanto repressivos.

A sanção de normas como a Lei Carolina Dieckmann (Lei nº 12.737/2012), o Marco Civil da Internet (Lei nº 12.965/2014), a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), a Convenção de Budapeste podem ser consideradas como ações de combate a crimes cibernéticos, assim como um início da caminhada em busca da segurança cibernética. Todavia a criação de direitos, diretrizes por si só não têm se mostrado suficientes para um efetivo combate a essas condutas delituosas. A implementação de órgãos e mão de obra especializada agindo de forma coordenada, tem se mostrado uma necessidade para o alcance de melhores resultados. Buscando se adequar a essa realidade, algumas normas vêm sendo editadas. Entre elas estão a Estratégia Nacional de Segurança Cibernética (E-Ciber), instituída pelo Decreto nº 10.222/2020, ora revogado, a Política Nacional de Cibersegurança (PNCiber), por meio do Decreto Presidencial Nº 11.856/2023.

A E-Ciber de 2020, tinha como algumas de suas ações estratégicas a adoção de um modelo centralizado de governança em âmbito nacional, tendo como um dos objetivos a coordenação de diversos atores ligados à segurança cibernética. Em 2025, por meio do Decreto nº 12.573/2025, a E-Ciber ganhou uma nova roupagem,

passando a vigorar com uma política mais atualizada e abrangente. Essa atualização da E-Ciber é consequência da Política Nacional de Cibersegurança (Decreto Nº 11.856), que por meio do seu artigo 5º instituiu o Comitê Nacional de Cibersegurança (CNCiber). A mesma norma, estabeleceu como competência do CNCiber “propor atualizações para a PNCiber, a Estratégia Nacional de Cibersegurança e o Plano Nacional de Cibersegurança.” (BRASIL,2023).

Sobre as medidas acima relacionadas, ainda não é possível dimensionar em termos quantitativos os seus resultados, elas são recentes e fazem parte de um planejamento que está em execução, mas é inquestionável o seu enorme valor para o progresso da segurança cibernética no país. Nota-se que as crescentes discursões entorno das ações do Estado e da sociedade para garantir a ordem e a paz social no ambiente virtual; a edição de novos dispositivos legais; a tentativa de cooperação entre agentes nacionais e internacionais em busca da prevenção e mitigação das vulnerabilidades de sistemas digitais, vêm acontecendo, seja em grande ou pequena escala, e, mesmo diante dos inúmeros obstáculos presentes na caminhada rumo ao combate aos cibercrimes, passos significativos têm sido dados.

6 CONCLUSÃO

Este estudo permitiu compreender a dimensão e a complexidade dos crimes cibernéticos no contexto jurídico brasileiro, destacando que os avanços tecnológicos, ao mesmo tempo em que trazem inúmeros benefícios à sociedade, também facilitam comportamentos ilícitos que desafiam as estruturas tradicionais do Direito Penal. O ambiente digital tornou-se um ambiente propício para crimes que afetam bens jurídicos fundamentais, como a propriedade, a honra, a privacidade e a dignidade sexual, exigindo do Estado e dos operadores do direito a constante atualização de suas normas e interpretações.

Constata-se que o ordenamento jurídico brasileiro sofreu mudanças significativas nas últimas décadas. Leis como a Lei nº 12.737/2012 (Lei Carolina Dieckmann), a Lei nº 12.965/2014 (Fundamentos dos Direitos Civis na Internet), a Lei nº 13.718/2018 e a Lei nº 14.155/2021 representam importantes avanços na tipificação de condutas e na proteção de bens jurídicos afetados no ciberespaço.

As recentes interpretações de inconstitucionalidade parcial do artigo 19 do Marco Civil da Internet demonstram a importância da responsabilização das empresas de plataformas digitais por publicações de terceiros, bem como a possibilidade de a notificação extrajudicial para remoção de conteúdo ser uma alternativa célere para lidar com situações de crimes contra a honra, que, quanto mais se prolongam no tempo, mais se agravam. Tornou-se evidente a mudança de entendimento quanto à possibilidade de responsabilização penal das pessoas jurídicas pela prática de crimes cibernéticos, tendo como precedente relevante a já existente responsabilidade penal de pessoas jurídicas por crimes ambientais. Considerando que muitos dos crimes ambientais decorrem não apenas de condutas individuais, mas também de decisões corporativas, e que todas essas condutas precisam ser alcançadas pela legislação como forma de garantir a proteção do meio ambiente físico, mostra-se coerente ampliar essa lógica aos crimes cibernéticos, responsabilizando a pessoa jurídica por eventuais ações ou omissões que contribuam para a ocorrência desses delitos. No entanto, apesar desses avanços legislativos, ainda persistem desafios para responsabilizar efetivamente os autores, coletar evidências digitais e garantir a cooperação internacional necessária ao enfrentamento do crime transnacional.

Também foi possível reconhecer que os cibercriminosos incluem não apenas profissionais altamente qualificados, como hackers e crackers, mas também usuários comuns que, muitas vezes sem perceber a gravidade de suas ações, se envolvem em atividades ilícitas, como disseminação de notícias falsas, publicação de imagens íntimas e fraudes cibernéticas. As vítimas incluem pessoas físicas e jurídicas, bem como a própria sociedade, que sofre com ataques a sistemas públicos, bancos de dados e infraestrutura crítica.

O estudo também destacou o papel crucial da segurança cibernética e das políticas públicas preventivas no combate aos crimes digitais. O desenvolvimento da Estratégia Nacional de Segurança Cibernética (E-Ciber) e da Política Nacional de Segurança Cibernética (PNCiber) demonstra os esforços do governo brasileiro para desenvolver medidas coordenadas de proteção e resposta a incidentes cibernéticos. No entanto, essas ferramentas devem ser acompanhadas de investimentos em

capacitação técnica, campanhas de conscientização pública e mecanismos de cooperação entre os setores público e privado.

Assim, pode-se concluir que o combate ao crime cibernético requer uma abordagem interdisciplinar e abrangente, que inclua não apenas o aprimoramento da legislação penal, mas também o fortalecimento dos órgãos de investigação, bem como o aumento da alfabetização digital. Somente por meio da articulação da legislação, da tecnologia e da conscientização pública será possível criar um ambiente virtual mais seguro e ético, capaz de garantir a proteção efetiva dos direitos fundamentais na era digital.

REFERÊNCIAS

BARRA, Helena. **Crimes sexuais cometidos pela internet crescem mais de 1.250% no RJ**. CNN Brasil, 02 ago. 2025. Disponível em: <<https://www.cnnbrasil.com.br/nacional/sudeste/rj/crimes-sexuais-cometidos-pela-internet-crescem-mais-de-1-250-no-rj/>>. Acesso em: 16 ago. 2025

BRASIL. **Decreto Nº 10.222, De 5 De Fevereiro De 2020**. Aprova a Estratégia Nacional de Segurança Cibernética. Brasília, DF: Diário Oficial da União, 2020. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm>. Acesso em: 25 set. 2025.

BRASIL. **Decreto Nº 11.491, de 12 de abril de 2023**: Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. Diário Oficial da União: seção 1, Brasília, DF, p. 2, 13 abr. 2023. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11491.html>. Acessado em: 19 de set. 2025.

BRASIL. **DECRETO Nº 11.856 De 26 De Dezembro De 2023**. Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. Brasília, DF: Diário Oficial da União, 2023. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm#:~:text=DECRETO%20N%C2%BA%2011.856%2C%20DE%2026,%E2%80%9Ca%E2%80%9D%2C%20da%20Constitui%C3%A7%C3%A3o%2C>. Acessado em: 28 set. 2025.

BRASIL. **Decreto Nº 12.573, De 4 De Agosto De 2025**. Institui a Estratégia Nacional de Cibersegurança. Brasília, DF: Diário Oficial da União, 2025. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/D12573.htm>. Acesso: 28 set. 2025.

BRASIL. **Lei Nº 13.718, De 24 De Setembro De 2018**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tipificar os crimes de importunação sexual e de divulgação de cena de estupro, tornar pública incondicionada a natureza da ação penal dos crimes contra a liberdade sexual e dos crimes sexuais contra vulnerável, estabelecer causas de aumento de pena para esses crimes e definir como causas de aumento de pena o estupro coletivo e o estupro corretivo; e revoga dispositivo do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais). Brasília, DF: Diário Oficial da União, 2018. Disponível: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13718.htm>. Acesso em: 06 set. 2025.

BRASIL. **Medida Provisória Nº 1.068, De 6 De Setembro De 2021**. Altera a Lei nº 12.965, de 23 de abril de 2014, e a Lei nº 9.610, de 19 de fevereiro de 1998, para dispor sobre o uso de redes sociais. Brasília, DF: Diário Oficial da União, 2021.

Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/Mpv/mpv1068.htm>. Acesso em: 27 set. 2025

BRASIL. **Projeto De Lei 2628 De 2022**. Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais. Brasília, DF: 2024. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2837130&filename=PL%202628/2022>. Acesso em: 09 set. 2025.

BRASIL. Superior Tribunal de Justiça (STJ). **Conflito de Competência nº 67.343 – GO (2006/0166153-0)**. Relator: Ministro Arnaldo Esteves Lima. Brasília, DF, 16 ago. 2006. Disponível em: <<https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ATC?seq=2895611&tipo=91&nreg=200601661530&SeqCgrmaSessao=&CodOrgaoJgdr=&dt=20071211&formato=PDF&salvar=false>>. Acesso em: 06 set. 2025.

BRASIL. Superior Tribunal de Justiça. **Recurso em Habeas Corpus nº 70.976 – MS**, de 02 de agosto de 2016. Relator Ministro Joel Ilan Paciornik. Disponível em: <<https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ATC?seq=62595006&tipo=5&nreg=201601218385&SeqCgrmaSessao=&CodOrgaoJgdr=&dt=20160810&formato=PDF&salvar=false>>. Acesso em: 09 set. 2025.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 1.679.465 - SP (2016/0204216-5)**. Relatoria: Ministra Nancy Andrighi. Recorrido: Ministério Público Do Estado De São Paulo. Recorrente: GOOGLE Brasil Internet LTDA. Brasília, DF, julgado em 13 de mar. de 2018. Disponível em: <<https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ATC?seq=81305102&tipo=0&nreg=&Se=>>>. Acesso em: 16 ago. 2025

BRASIL. Superior Tribunal de Justiça. **Recurso Extraordinário nº 1037396- SP**. Relator: Ministro Dias Toffoli. Recorrido: Lourdes Pavioto Correa. Recorrente: Facebook Servicos Online Do Brasil LTDA. Brasília, DF, julgado em 01mar. De 2018. Disponível em: <<https://jurisprudencia.stf.jus.br/pages/search/repercussao-geral9662/false>>. Acessado em: 19 set. 2025.

BRASIL. TRIBUNAL DE JUSTIÇA DE SÃO PAULO-TJSP. **Apelação Criminal nº 0062364-28.2018.8.26.0050, 4ª Câmara de Direito Criminal**. Apelante: Marco Antonio Rosa Ferreira. Apelado: Ministério Público do Estado de São Paulo. Relatora: Des. Fátima Vilas Boas Cruz. São Paulo, 07 de novembro 2022. Disponível em: <<https://www.tjsp.jus.br/Noticias/Noticia?codigoNoticia=86113>>. Acesso em: 04 set. 2025.

BRASIL. Tribunal de Justiça de Sergipe. **Habeas Corpus nº 202000329659, de 15 de dezembro de 2020**. Relator: Des. Edson Ulisses De Melo. Disponível em: <https://www.tjse.jus.br/tjnet/jurisprudencia/relatorio.wsp?tmp_numprocesso=202000329659&tmp_numacordao=202039482&tmp.expressao=sexo%20expl%C3%ADcito>. Acesso em: 08 set. 2025.

CAPEZ, Fernando. **Curso de Direito Penal – Parte Geral**. 23. ed. São Paulo: Saraiva, 2019.

CENTRO INTERNET SEGURA. **Quero saber: Grooming / Aliciamento online.**

Centro Internet segura. Disponível em:

<<https://www.internetsegura.pt/grooming>. Acesso em: 09 set. 2025.

CESTARI, Ricardo Yunes. NASPOLINI, Samyra Haydêe Dal Farra. FULLER, Greice Patricia. **Responsabilidade penal das pessoas jurídicas nos crimes**

informáticos: requisitos fáticos e normativos. Direito & Paz, São Paulo, Ano XVII, n. 49, p. 282-302, 2º Semestre, 2023. Disponível em: <

<https://revista.unisal.br/lo/index.php/direitoepaz/article/view/1718/713>>.

Acesso em: 15 ago. 2025.

CORRÊA, Isadora Donza; NETO, João Araújo Monteiro. A adesão do Brasil à Convenção de Budapeste e o enfrentamento do Cibercrime: entre a Cooperação Internacional e a expansão do Direito Penal. **Direito & TI**, [S. l.], v. 1, n. 16, p. 32–60, 2023. DOI: 10.63451/ti.v1i16.155. Disponível em:

<<https://direitoeti.com.br/direitoeti/article/view/155>>. Acesso em: 19 set. 2025.

COSTA, Rafael de Oliveira. BUZETTI, Bruno Starcke. Novos horizontes na responsabilidade penal das pessoas jurídicas pela prática de crimes cibernéticos.

Revista Jurídica da Escola Superior do Ministério Público de São Paulo, São Paulo, v. 26, p.125-154, 2025. Disponível em:

<https://www.tce.rj.gov.br/bnportal/m/en/search/62757?exp=%22BUZETTI,%20Bruno%20Starcke%22%2Fautor&exp_default=>. Acesso em: 19 set. 2025.

CUNHA, Rogério Sanches. **Manual de Direito Penal: parte geral**. 3. ed. Salvador: JusPODIVM, 2015.

DA SILVA, Gilsimar Pinheiro . **Crimes Digitais: Evolução dos crimes e a**

aplicação do direito. Universidade 2021. Potiguar: Artigo científico. Disponível em: <46 <https://repositorio.animaeducacao.com.br/bitstreams/65597262-4fec-4790-8267-65d7f57bb5ed/download>>. Acessado em: 06 set. 2025.

DA SILVA, Ludmila Rodrigues. Os crimes virtuais sob a luz da Legislação Brasileira.

RECIMA21 - Revista Científica Multidisciplinar - ISSN 2675-6218, [S. l.], v. 5, n. 6, p. e565363, 2024. DOI: 10.47820/recima21.v5i6.5363. Disponível em:

<<https://recima21.com.br/recima21/article/view/5363>>. Acesso em: 18 set. 2025.

DA SILVA, Mariana Almeida. **A internet como ambiente facilitador à violência de gênero: cyberstalking, sextorsão e revenge porn.** Revista do Ministério

Público do Estado do Rio de Janeiro nº 86, out./dez. 2022. Disponível em :

<https://www.mprj.mp.br/documents/20184/3600511/Mariana+Almeida+da+Silva_RMP-86.pdf>. Acesso em: 08 set. 2025.

DCIBER. **Relatório da Trend Micro coloca o Brasil entre os cinco países mais atacados por ransomware em abril.** Disponível em:

<<https://dciber.org/relatorio-da-trend-micro-coloca-o-brasil-entre-os-cinco-paises-mais-atacados-por-ransomware-em-abril/>>. Acesso em: 27 set. 2025.

DISTRITO FEDERAL. **Apelação Criminal 000071230.2019.8.07.0009**. Acórdão 1231584, 00007123020198070009. Relator: Des^a. Nilsoni De Freitas Custodio, 3^a Turma Criminal, Tribunal De Justiça Do Distrito Federal E Dos Territórios. Brasília, DF, julgado em 13 fev. de 2020, publicado no PJe: 2/3/2020. Disponível em: <<https://pesquisajuris.tjdft.jus.br/IndexadorAcordaos-web/sistj>>. Acesso em: 16 ago. 2025.

ELLOVITCH, Mauro da Fonseca. **Grooming, assédio sexual a crianças e adolescentes em meio cibernético**. Consultor Jurídico, 01 set. 2023. Disponível: <<https://www.conjur.com.br/2023-set-01/mauro-ellovitch-grooming-artigo-241-eca/>>. Acesso em: 15 ago. 2025.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **17º Anuário Brasileiro de Segurança Pública**. São Paulo: Fórum Brasileiro de Segurança Pública, 2023. Disponível em: <<https://forumseguranca.org.br/wp-content/uploads/2023/07/anuario-2023.pdf>>. Acesso em: 15 ago. 2025.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **19º Anuário Brasileiro de Segurança Pública**. São Paulo: Fórum Brasileiro de Segurança Pública, 2025. Disponível em: <<https://publicacoes.forumseguranca.org.br/handle/123456789/279>>. Acesso em: 06 set. 2025.

JESUS, Damásio de. **Direito Penal Parte Geral**. Volume 1: Parte geral. 32.ed. São Paulo: Saraiva, 2011.

JÚNIOR, Janary. **Governo edita medida provisória que limita remoção de conteúdos de redes sociais**. Disponível em: <<http://camara.leg.br/noticias/803707-governo-edita-medida-provisoria-que-limita-remocao-de-conteudos-de-redes-sociais>>. Acesso em: 27 set. 2025

KOETZ, Eduardo. **10 caminhos para o combate de Ciber Crimes no Brasil**. Disponível em: <<https://advbox.com.br/blog/caminhos-para-o-combate-de-ciber-crimes-o-brasil/#:~:text=Conscientiza%C3%A7%C3%A3o%20e%20educa%C3%A7%C3%A3o,cultura%20de%20seguran%C3%A7a%20cibern%C3%A9tica%20robusta.>>. Acesso em: 25 set. 2025.

LENZA, Pedro. **Direito constitucional esquematizado**. Pedro Lenza. – 19. ed. rev., atual. e ampl. – São Paulo: Saraiva, 2015.

LOPES, Marciano Pereira; LOPES, José Augusto Bezerra. Crimes Virtuais No Ordenamento Jurídico Brasileiro. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, [S. l.], v. 9, n. 8, p. 462–472, 2023. DOI: 10.51891/rease.v9i8.10850. Disponível em: <<https://periodicorease.pro.br/rease/article/view/10850>>. Acesso em: 19 set. 2025.

MOLINA, Ton. **STF define parâmetros para responsabilização de plataformas por conteúdo de terceiros**. STF, Brasília, 26 de junho de 2025. Disponível em: <[https://noticias.stf.jus.br/postsnoticias/stf-define-parametros-para-responsabilizacao-de-plataformas-por-conteudos-de-terceiros/#:~:text=STF%20define%20par%C3%A2metros%20para%20responsabiliza%C3%A7%C3%A3o%20de%20plataformas%20por%20conte%C3%BAdos%20de%20terceiros&text=O%20Supremo%20Tribunal%20Federal%20\(STF,relatado%20pelo%20ministro%20Luiz%20Fux](https://noticias.stf.jus.br/postsnoticias/stf-define-parametros-para-responsabilizacao-de-plataformas-por-conteudos-de-terceiros/#:~:text=STF%20define%20par%C3%A2metros%20para%20responsabiliza%C3%A7%C3%A3o%20de%20plataformas%20por%20conte%C3%BAdos%20de%20terceiros&text=O%20Supremo%20Tribunal%20Federal%20(STF,relatado%20pelo%20ministro%20Luiz%20Fux)>. Acessado em: 19 de set. 2025.

LOSCHI, Marília. **Internet chega a 74,9 milhões de domicílios do país em 2024**. Estatísticas Sociais. Disponível em: <<https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/44031-internet-chega-a-74-9-milhoes-de-domicilios-do-pais-em-2024>>. Acesso em: 27 set. 2025.

MACHADO, Gabriély de Carvalho. DE ARAGÃO, Juliana Medina. DE ALENCASTRO, Maria Fernanda Borges Daniel. **Crimes sexuais, Direito Penal e Vitimologia**. 2023. Disponível em: <<https://www.jusbrasil.com.br/artigos/crimes-sexuais-direito-penal-e-vitimologia/1744633609>>. Acesso em: 06 set. 2025.

MAIA, Elijonas. **Ataque hacker desviou R\$ 541 milhões “em massa”, diz polícia**. CNN Brasil, 04 jul. 2025. Disponível em: <<https://www.cnnbrasil.com.br/nacional/sudeste/sp/ataque-hacker-desviou-r-541-milhoes-em-massa-diz-policia/>>. Acesso em: 16 ago. 2025.

MELO, Luiza. Golpes virtuais aumentam e não fazem distinção de idade. **Agência Senado**. Disponível em: <<https://www12.senado.leg.br/noticias/infomaterias/2025/04/golpes-virtuais->>>. Acesso em: 27 set. 2025.

MORAES, Geórgia. **Não há perfil definido de consumidor de pornografia infantil, diz perito**. Agência Câmara de Notícias, Brasília, 15 set. 2015. Disponível: <<https://www.camara.leg.br/noticias/470187-nao-ha-perfil-definido-de-consumidor-de-pornografia-infantil-diz-perito>>. Acesso em: 15 ago. 2025.

NUCCI, Guilherme de Souza. **Código Penal Comentado**. 20. ed. Rio de Janeiro: Forense, 2020.

NUCCI, Guilherme de Souza. **Manual de Direito Penal – Parte Geral**. 8. ed. São Paulo: Revista dos Tribunais, 2012.

NUCCI, Guilherme de Souza. **Manual de Direito Penal**. 10^a. ed. Rio de Janeiro: Forense, 2014. p. 692. Disponível: <<https://direitouniversitarioblog.wordpress.com/wp->

content/uploads/2017/02/manual-do-direito-penal-guilherme-nucci.pdf >. Acesso em: 04 set. 2025.

NUCCI, Guilherme de Souza. **Manual de direito penal: parte geral, parte especial**. 7. ed., rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2011. 1151 p. ISBN 978-85-203-3876-6. Disponível em: <<https://pt.scribd.com/document/214956750/Manual-de-Direito-Penal-Nucci-7%C2%AA-Edicao-2011>>. Acesso em: 04 set. 2025.

PEIXOTO, Camila Martins de Mello. Responsabilidade Penal Nos Crimes Virtuais. **Adelpha Repositório Digital**, 2022. Disponível em: <<https://dspace.mackenzie.br/items/a13a0d6f-1522-410f-a1d3-c77e9558bbb8>>. Acesso em 09 de out. 2025.

RAMALHO, David Silva. **O uso de malware como meio de obtenção de prova em Processo Penal**. Disponível em: <https://www.concorrenca.pt/sites/default/files/imported-magazines/CR16_-_David_Silva_Ramalho.pdf>. Acesso em: 15 ago. 2025.

SAFER NET. **Nota Técnica 02/2025**. SaferNet, Salvador, 2025. Disponível em: <https://arquivos.safernet.org.br/notas/Nota+Tecnica+02_2025+%5BSaferNet+Brasil%5D.pdf>. Acesso em: 09 set. 2025.

SAFERNET. **Safernet recebe recorde histórico de novas denúncias de imagens de abuso e exploração sexual infantil na internet**. Safer Net, 06 fev. 2024. Disponível em: <<https://new.safernet.org.br/content/safernet-recebe-recorde-historico-de-novas-denuncias-de-imagens-de-abuso-e-exploracao-sexual>>. Acesso em: 16 ago. 2025.

SEGINFO. **Brasil lança nova Estratégia Nacional de Cibersegurança (e-Ciber)**. Disponível em: <<https://seginfo.com.br/2025/08/13/brasil-lanca-nova-estrategia-nacional-de-ciberseguranca-e-ciber/>>. Acesso em: 28 set. 2025.

SENADO, Agência. Senadores pedem rejeição da MP que limita remoção de conteúdos de redes sociais. **Senado Notícias**. Disponível em: <<https://www12.senado.leg.br/noticias/materias/2021/09/14/08/senadores-pedem-rejeicao-da-mp-que-limita-remocao-de-conteudos-de-redes-sociais>>. Acesso em: 27 set. 2025.

SILVA, Ana Luísa Diniz; MALETTA, Giselle Villela. Cibersegurança e Ciberdefesa: uma nova abordagem da segurança nacional brasileira. **Revista Brasileira de Inteligência Artificial e Direito** | ISSN 2675-3156 Anais da III Mostra de Reviews, Cases e Insights do III Seminário de IA e Direito, 2021. Disponível em: <<https://rbiad.com.br/index.php/rbiad/article/download/32/71/343>>. Acesso em: 27 set. 2025.

SILVA, Karoline Rodrigues. **A Influência dos Meios Eletrônicos na Criminalidade de Massa**. 2020. Disponível em: <<https://www.jusbrasil.com.br/artigos/a-influencia-dos-meios-eletronicos-na-criminalidade-de-massa/797854492>>. Acesso em: 04 set. 2025.

STJ. **Posse e distribuição de pornografia infantil são crimes autônomos, e penas podem ser somadas.** 07 ago.2023. Disponível: <<https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2023/07082023-Posse-e-distribuicao-de-pornografia-infantil-sao-crimes-autonomos--e-penas-podem-ser-somadas.aspx>>. Acesso em: 16 ago. 2025.

SUSSKIND, Rafael. **Incidente de segurança da informação:** entenda e saiba como proceder. Disponível em: < <https://dpoexpert.com.br/incidente-de-seguranca-da-informacao/>>. Acesso em: 22 out. 2025.

SYDOW, Spencer Toth. **Delitos informáticos próprios: uma abordagem sob a perspectiva vitimodogmática.** 2009. 282 f. Dissertação (Mestrado em Direito Penal) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2009. Disponível em: < https://www.teses.usp.br/teses/disponiveis/2/2136/tde-15062011-161113/publico/Dissertacao_Mestrado_versao_parcial_formatada_padroes.pdf>. Acesso em: 04 set. 2025.

TEIXEIRA, Tarcísio. **Curso de direito e processo eletrônico: doutrina, jurisprudência e prática.** 2 ed. atual. São Paulo: Editora Saraiva, 2014.