

**FACULDADE DE ADMINISTRAÇÃO, NEGÓCIOS E SAÚDE DE SERGIPE -
FANESE
CURSO DE DIREITO**

ANDREY ANDRADE SOUZA

CRIMES CIBERNÉTICOS: SEUS REFLEXOS NO MUNDO JURÍDICO BRASILEIRO

ARACAJU/SE
2025

S826c

SOUZA, Andrey Andrade

Crimes cibernéticos : seus reflexos no mundo jurídico brasileiro / Andrey Andrade Souza. - Aracaju, 2025.
18f.

Trabalho de Conclusão de Curso (Artigo)
Faculdade de Administração, Negócios e Saúde de Sergipe. Coordenação de Direito.

Orientador(a): Prof. Esp. Anderson Teinassis
C. Santos Santana

1. Direito 2. Cibercrime 3. Tecnologia
4. Patrimônio I. Título

CDU 34 (045)

Elaborada pela Bibliotecária Edla de Fatima S. Evangelista CRB-5/1029

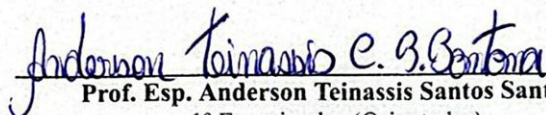
ANDREY ANDRADE SOUZA

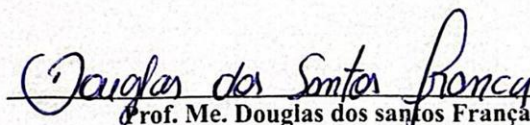
**CRIMES CIBERNÉTICOS: SEUS REFLEXOS NO MUNDO JURÍDICO
BRASILEIRO.**

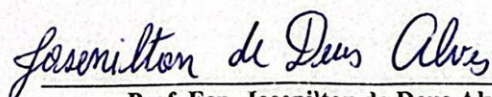
Artigo Científico apresentado à Faculdade de Administração e Negócios de Sergipe - FANESE,
como requisito parcial e elemento obrigatório para a obtenção do grau bacharel em Direito no
período de 2025.2.

Aprovado (a) com média:

10,0


Prof. Esp. Anderson Teinassis Santos Santana
1º Examinador (Orientador)


Prof. Me. Douglas dos Santos França
2º Examinador


Prof. Esp. Josenilton de Deus Alves
3º Examinador

Aracaju, 05 de dezembro de 2025

RESUMO

O presente artigo discute os crimes cibernéticos direcionados à lesão patrimonial, tendo como contexto a expansão da internet e a crescente interação social por intermédio dos meios digitais. A questão fulcral é entender de que maneira o comportamento dos usuários no ambiente digital proporciona práticas ilícitas e quais mecanismos legais podem ser competentes para enfrentar tais condutas. O objetivo do estudo é delinear as principais modalidades de crimes patrimoniais digitais, analisar suas formas de execução, verificar seus impactos na sociedade e observar a efetividade do aparato normativo brasileiro. A pesquisa adota o método quantitativo e qualitativo, de caráter bibliográfico, estatístico e documental, apoiando-se em autores como Araújo (2023), Castells (2002), Nucci (2025) e Masson (2015). Os resultados do trabalho indicam que, embora o ordenamento jurídico disponha de instrumentos como o Marco Civil da Internet e a Lei Geral de Proteção de Dados, há a necessidade da constante atualização normativa, bem como da maior integração entre o mundo jurídico, as tecnologias e as políticas de prevenção de crimes. Destarte, percebe-se que, por meio de respostas jurídicas consistentes, estratégias de segurança no domínio digital e aprimoramento legislativo, será possível combater e reduzir o avanço da criminalidade patrimonial no meio virtual.

Palavras-chave: Cibercrime. Tecnologia. Patrimônio.

^{1*}Artigo apresentado à banca examinadora do curso de Direito da Faculdade de Administração e Negócios de Sergipe, em Dezembro de 2025, como critério parcial e obrigatório para a obtenção do título de Bacharel em Direito. Orientador: Prof. Esp. Anderson Teinassis C. S. Santana.

INTRODUÇÃO

O cenário contemporâneo vivencia uma transformação sem precedentes, impulsionada pela expansão da internet. O crescente número de usuários está diretamente associado à popularização dos dispositivos móveis e ao avanço da infraestrutura de conectividade, elementos que possibilitam maior acessibilidade e inclusão digital.

A internet consolidou-se como o principal sistema de interação de caráter mundial, onde os consumidores são atraídos por informações, lazer, possibilidade de relacionamentos, entre outras formas de interação fornecidas pelo meio digital. Apesar de, por um lado, a conectividade global ter ampliado o acesso a informações e comunicações, também favoreceu o surgimento e a evolução de condutas ilícitas no ambiente virtual, afetando diversas pessoas, vítimas dessas novas práticas criminosas (Araújo, 2023).

Conforme uma matéria da CNN, assinada por João Nakamura (2024), “o Brasil é vice-campeão em ataques cibernéticos, com 1.379 golpes por minutos”, aponta Panorama de Ameaças para a América Latina 2024. A ocorrência dos crimes cibernéticos surge nesse contexto como uma das mais complexas questões da atualidade, desafiando tanto a atuação das autoridades policiais, quanto à eficácia do ordenamento jurídico vigente.

Entre as diversas modalidades de crimes virtuais, aquelas que atentam contra o patrimônio, merecem atenção especial, haja vista o crescimento expressivo de golpes, fraudes e furtos digitais, que ocasionam prejuízos significativos a pessoas físicas, jurídicas e instituições financeiras.

Essa problemática faz surgir indagações sobre: De que forma o comportamento dos usuários no ambiente virtual, contribui para o aumento dos crimes contra o patrimônio? Quais são as principais modalidades de crimes cibernéticos, que causam prejuízos patrimoniais a pessoas e instituições? Quais mecanismos legais e normativos, o ordenamento jurídico brasileiro dispõe para mitigar tais práticas e proteger as vítimas?

Nessa perspectiva, as mudanças sociais advindas da inserção massiva das tecnologias digitais na vida cotidiana são de extrema relevância na discussão. Nesse cenário, este trabalho estudou as diferentes modalidades de crimes cibernéticos que acarretam lesão patrimonial, observando suas características, formas de execução e a negatividade dos efeitos. Além disso, analisou o alicerce jurídico brasileiro, inclusive, outros instrumentos normativos e medidas de prevenção, a fim de avaliar a efetividade das respostas legais no combate a esse tipo de criminalidade.

A metodologia adotada no artigo é de natureza teórica, quantitativa e qualitativa, baseada em pesquisa bibliográfica, estatística e documental, que recorreu à Araujo (2023), no que afeto ao tema das inovações tecnológicas ligadas à realidade virtual com a delimitação teórica e prática dos crimes virtuais e a Castells (2002), a partir da sua contextualização social e tecnológica (base interdisciplinar). Em relação à sustentação jurídica no âmbito penal, a pesquisa se baseou em Nucci (2025), mediante a sua conceituação de crime no geral e de crimes em espécie, e Masson (2015) com sua contribuição relacionada à base teórica sobre os crimes que lesam o patrimônio. Além dessa investigação, o trabalho perquiriu, a partir do artigo científico de autoria de Sena, Oliveira e Santos (2023), que forneceram dados relacionados às formas de combate e repressão aos crimes cibernéticos.

Esse estudo não decorre apenas da necessidade de compreender a relação entre as tecnologias e crimes, mas, ao mesmo tempo, consiste em frisar a importância do aprimoramento jurídico e a solução de lacunas do direito digital, que são essenciais para fortalecer a segurança no ambiente virtual. Afinal, da mesma forma que as inovações tecnológicas se expandem, as práticas criminosas não ficam para trás, exigindo que o mundo jurídico acompanhe esse movimento com rapidez e precisão.

O IMPACTO DAS TECNOLOGIAS DIGITAIS NO COMPORTAMENTO HUMANO

CONTEXTO HISTÓRICO DA INTERNET

A internet, nomenclatura de amplo conhecimento, é o resultado de evolução tecnológica, estratégia militar e a imprescindível cooperação científica. Sua origem deu-se na década de 1960, período em que a Agência de Projetos de Pesquisa Avançada (ARPA) do Departamento de Defesa dos Estados Unidos, desenvolveu a primeira rede de computadores ARPANET, seu acesso era feito pelos centros de pesquisa, mas também ocorreu o início das interações entre cientistas com a ajuda desse aparato tecnológico (Castells, 2002).

De acordo com o artigo “Tecnologias de informação e comunicação”, escrito por Liliane Silva (2010), a ARPANET funcionava via chaveamento de pacotes, onde havia a propagação de dados em redes de computadores com a divisão em pacotes menores, composto por fragmento de dados, o endereço do destinatário e informações que possibilitavam o reagrupamento da mensagem original. Complementa a autora:

Em 29 de Outubro de 1969 ocorreu a transmissão do que pode ser considerado o primeiro E-mail da história. O texto desse primeiro e-mail seria "LOGIN",

correspondente pretendia o Professor Leonard Kleinrock da Universidade da Califórnia em Los Angeles, mas o computador no Stanford Research Institute, que recebia a mensagem, parou de funcionar após receber a letra "O" (Silva, 2010, p. 6).

A internet, rede global de computadores, é caracterizada pela comunicação mediante protocolos padronizados, esse poder de comunicação proporciona o acesso a informações e serviços entre dispositivos conectados, diversificando e ampliando as interações entre as pessoas no meio social. Manuel Castells afirma que:

Em fins da década de 1990, o poder de comunicação da Internet, juntamente com os novos progressos em telecomunicação e computação provocaram mais uma grande mudança tecnológica, dos microcomputadores e dos *mainframes* descentralizados e autônomos à computação universal por meio da interconexão de dispositivos de processamento de dados, existentes em diversos formatos. Nesse novo sistema tecnológico o poder de computação é distribuído numa rede montada ao redor de servidores da *web* que usam os mesmos protocolos da Internet, e equipados com capacidade de acesso a servidores em megacomputadores, em geral diferenciados entre servidores de bases de dados e servidores de aplicativos (Castells, 2002, p.89).

A INTERNET NO BRASIL

No Brasil, a internet iniciou sua caminhada em 1988. Graças a uma conexão entre um computador do Laboratório Nacional de Computação Científica, da Universidade Federal do Rio de Janeiro (UFRJ) e a rede da Universidade de Maryland, nos Estados Unidos da América. No mesmo ano do surgimento da internet no Brasil, a Fundação de Amparo à Pesquisa do Estado de São Paulo (Fapesp) teve contato com a internet, promovendo a criação do Alternex, provedor que facilitou o acesso das universidades à internet (Silva, [s.d.]).

O Ministério de Ciência e Tecnologia (MCT) criou em 1989, a Rede Nacional de Pesquisa (RNP), com o objetivo de possibilitar o amplo acesso à nova tecnologia no país. Porém, até o ano de 1995, a atuação da RNP esteve limitada à comunidade escolar e de pesquisa brasileira. A disponibilização da internet para o público e para fins de comércio, somente ocorreu entre os anos de 1994 e 1995, fazendo com que a estrutura da RNP deixasse de ser restrita aos acadêmicos, proporcionando assim, a sua utilização para tratativas comerciais. Ainda em 1995, foi criado o Comitê Gestor da Internet (CGI), com o propósito de debater sobre segurança e desenvolvimento da internet, esse Comitê é representado pela sociedade, empresas e academia, tendo atuação na promoção de estudos e sugestões acerca da segurança na internet (Silva, [s.d.]).

A inicialização da internet no Brasil não apenas promoveu a democratização do acesso à informação, mas também impulsionou o desenvolvimento de novas comunicações e negócios. Esse aparato tecnológico refletiu diretamente na valorização da rede virtual como

parte essencial da vida cotidiana. Todavia, a popularização da internet trouxe grandes desafios, como a inclusão digital e a segurança da informação, impasses que perduram há anos e ainda são amplamente debatidos.

Paralelamente, o contínuo avanço tecnológico passou a exigir uma adaptação constante do ordenamento jurídico, evidenciando a necessidade de regulamentações específicas para o ambiente digital. Logo, a emergência da legislação voltada à proteção de dados, à prevenção de crimes cibernéticos e à responsabilidade nas relações virtuais tornou-se indispensável, diante dos novos riscos sociais e econômicos que acompanham a expansão da internet.

Assim sendo, conclui-se que a expansão da internet exigiu o desenvolvimento de instrumentos regulatórios, aptos a conciliar liberdade de expressão e inovação tecnológica com a proteção de direitos fundamentais. O Marco Civil da Internet (Lei nº 12.965/2014) consagrou princípios como a neutralidade da rede, a proteção da privacidade e a preservação de registros de acesso, estabelecendo a base normativa da internet no país brasileiro (Brasil, 2014).

Posteriormente, a Lei nº 13.709/2018 (Brasil, 2018), titulada como Lei Geral de Proteção de Dados (LGPD), passou a disciplinar de forma ampliada o tratamento de dados pessoais, impondo obrigações aos agentes de tratamento e reconhecendo a autodeterminação informativa como direito fundamental consolidado pelo Supremo Tribunal Federal na (ADI 6.387), onde ficou decidido sobre a ampliação da responsabilidade das plataformas digitais, por divulgação de conteúdos ilegais no espaço virtual, sem a necessidade prévia de ordem judicial (STF, ADI 6.387, Rel. Min. Rosa Weber, 2020).

Portanto, mesmo com a internet proporcionando novas oportunidades, ficou nítido o oferecimento de vulnerabilidades que necessitam de atenção na devida gestão. Dessa forma, é perceptível que o contato com internet no Brasil é frisado por suas potencialidades e dificuldades, influenciando diretamente nos hábitos da sociedade.

A DEPENDÊNCIA TECNOLÓGICA E SUAS CONSEQUÊNCIAS JURÍDICAS

O comportamento do homem diante das tecnologias digitais vivencia inúmeras alterações no dia a dia de casa, trabalho e demais vínculos sociais, essas mudanças geram impactos na vida pessoal e profissional de cada indivíduo, sendo assim um tema amplo e complexo, que abrange diversos setores do conhecimento, como o direito, a psicologia, a sociologia, dentre outras áreas.

A tecnologia acompanha os seres humanos desde suas origens, sendo responsável por impulsionar o desenvolvimento que possibilitou alcançar a modernidade atual. Esse avanço se reflete em diferentes áreas, como informática, engenharia, comunicação e medicina. Entretanto, mesmo sendo agentes dessa evolução, os indivíduos ainda enfrentam dificuldades em lidar plenamente com seus sentimentos e emoções, em razão das transformações comportamentais que ela provoca (Prado, [s.d.]).

Entre as alterações de comportamento, vale a pena ressaltar a ascensão desenfreada da criminalidade no âmbito virtual, consequência das diversas formas de estabelecer ilegalidades no mundo tecnológico, facilitando assim, o aumento considerável da prática anônima de crimes. O ambiente digital, mesmo sendo um facilitador da vida humana na modernidade, é um criador de vulnerabilidades, pelo fato das pessoas estarem interligadas e com dependência tecnológica (Brito, 2013 *apud* Silveira, 2025). Não é à toa, que o resultado dessa submissão, compromete a autonomia do pensamento humano, resultando no comprometimento da personalidade individual, tornando as pessoas reféns da nova realidade digital (Silveira, 2025).

Inclusive, as mídias digitais, têm influência na prática da prostituição, tráfico, contrabando e demais outras condutas ilegais. Embora seja uma ferramenta que possibilita a comodidade, e se destaca como um potencial gerador de desenvolvimento econômico, também proporciona um espaço desprotegido e sujeito à exploração criminosa, ensejando na criação de novos meios de execução de crimes já existentes, e possibilitando o aparecimento de atuações ilícitas inéditas (Silveira, 2025).

A crescente inclusão digital retrata a atual realidade, que tem a população frequentemente sujeita a esse avanço, sem que haja, por vezes, a orientação cabível. Sendo perceptível, o aumento de interações virtuais, como relacionamentos digitais, e o comércio eletrônico, modalidade essa que fez surgir um alerta sobre o aumento de transações bancárias e financeiras de forma online, afetando consideravelmente o setor econômico-financeiro, diante das vulnerabilidades características do mundo tecnológico (Brito, 2013 *apud* Silveira, 2025).

A pesquisa do Instituto DataSenado, divulgada em 2024, demonstrou que os golpes no ambiente digital, atingiram mais de 40,85 milhões de pessoas, nos 12 meses entre os anos de 2023 e 2024, esse é o número alarmante de indivíduos que sofreram algum crime cibernético, como por exemplo, fraude de internet, invasão de conta bancária ou clonagem de cartão (Agência Senado, 2024). Lamentavelmente, na maioria das vezes, os crimes digitais são consumados com a ajuda da própria vítima do evento ilícito, evidenciando a interligação da

falta de informação e a vulnerabilidade dos usuários, possibilitando a concretização de crimes e potencializando as barreiras no combate a essas práticas delituosas (Silveira, 2025).

A presença das tecnologias digitais na vida cotidiana tem acarretado transformações profundas no comportamento humano, impactando o âmbito pessoal e profissional. O avanço tecnológico proporciona facilidades e oportunidades de desenvolvimento, mas também gera novos desafios para a sociedade. Essa realidade comprova que o homem, no papel criador e beneficiário das tecnologias, encontra-se, concomitantemente, vulnerável aos impactos que tais ferramentas produzem em suas relações sociais, e, sobretudo, na seara da segurança, pois é notório o aparecimento de diferentes atuações ilegais, que se aproveitam das fragilidades dos sistemas digitais conectados à internet.

Então, é imprescindível que o meio social se adapte a essa nova realidade com uma postura crítica e preventiva, aliada à busca ativa pela regulação normativa, para que seja possível usufruir dos avanços tecnológicos, sem se tornar refém das vulnerabilidades digitais. Sob esse olhar, observa-se que o percurso histórico da internet, o desenvolvimento jurídico e as transformações sociais por ela geradas, configuram faces de um mesmo fenômeno normativo e civilizatório. Portanto, refere-se a um processo em constante construção, no qual, a tecnologia, a sociedade e o Direito, evoluem de forma interdependente, revelando a necessidade de equilíbrio entre inovação, proteção e responsabilidade coletiva no ambiente digital.

CRIMES CIBERNÉTICOS E O SEU POTENCIAL LESIVO PATRIMONIAL

A CONSTRUÇÃO TEÓRICO-JURÍDICA DO CRIME

Antes de iniciar de fato a discussão sobre a lesividade patrimonial, ocasionada pelos crimes cibernéticos, é essencial entender o passo a passo do tema em questão. O Código Penal Brasileiro (CPB), não conceitua explicitamente a palavra crime, o regulamento vigente diz no art. 1º, que: “Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal.” (Brasil, 1940). Então, para que a ação seja enquadrada como crime, há a necessidade da anterioridade da lei. Contudo, é indispensável o entendimento dogmático sobre o que seria a literalidade da expressão crime. Assim, o doutrinador Guilherme de Souza Nucci, afirma que:

Inicialmente, cumpre salientar que o conceito de crime é artificial, ou seja, independe de fatores naturais, constatados por um juízo de percepção sensorial, uma

vez que se torna impossível classificar uma conduta, ontologicamente, como criminosa.

Em verdade, é a sociedade a criadora inaugural do crime, qualificativo que reserva às condutas ilícitas mais gravosas e merecedoras de maior rigor punitivo. Após, cabe ao legislador transformar esse intento em figura típica, criando a lei que permitirá a aplicação do anseio social aos casos concretos (Nucci, 2025, p. 111).

A partir desse esclarecimento introdutório, faz-se necessário compreender os três aspectos ligados ao significado de crime, que são os conceitos material, formal e analítico. Sob a óptica material, o crime é compreendido a partir da reprovação social de determinadas condutas, ou seja, da convicção coletiva de que certos comportamentos podem ou devem ser impedidos e sancionados (Nucci, 2025). Para ilustrar, sem considerar a existência de lei específica, podemos imaginar uma situação na qual determinada pessoa invade um dispositivo informático de outra, e acaba divulgando dados, ou até mesmo transferindo valores sem o devido consentimento, a sociedade, ao analisar a situação, enxergaria o ato como grave e passível de punição legal.

Avançando para o contexto formal, tem-se a positivação dessa reprovação social, isto é, a transformação da desaprovação coletiva em norma jurídica com sanção definida (Nucci, 2025). Tendo como base o caso hipotético anterior, a invasão de dispositivos informáticos somente é reconhecida como crime, porque o legislador, interpretando essa necessidade de proteção, editou a Lei específica nº 12.737/2012 (Brasil, 2012), conhecida como Lei Carolina Dieckmann e posteriormente alterou o CPB, por intermédio da Lei nº 14.155/2021 (Brasil, 2021) que agravou as penas dos crimes relacionados à violação de dispositivos informáticos.

Por fim, sob o prisma analítico, busca-se uma compreensão mais aprofundada e estruturada desse conceito, analisando o aspecto técnico-jurídico. A definição de crime nesse momento parte da teoria tripartida, uma atuação típica (descrita em lei), antijurídica (contrária ao ordenamento jurídico, e sem estar amparada por alguma causa de justificação) e culpável (onde será feito o juízo de reprovabilidade social da conduta do agente) (Nucci, 2025).

Para exemplificar, considere-se o caso de um criminoso que cria um perfil falso em determinada rede social, objetivando ludibriar outras pessoas e aplicar golpes financeiros, esse ato ilegal é tipificado como Estelionato eletrônico, previsto no Art. 171, §2º-A, do CPB (incluído pela Lei nº 14.155/2021). No caso em questão, não há justificativa legal, sendo o ato antijurídico e culpável, pois o autor age consciente do caráter ilícito da sua ação, estando capaz de responder penalmente.

CRIMES DE LESÃO PATRIMONIAL

Após a exposição geral referente à conceituação de crime, será discutido nesse momento sobre a parte especial do Direito Penal, enfatizando os principais delitos patrimoniais que afetam pessoas ou instituições. O CPB destina o Título II, da Parte Especial, ao enquadramento das posturas tipificadas como crimes, nocivos ao patrimônio.

Os delitos contra o patrimônio são configurados como infrações penais que violam ou colocam em risco bens, interesses ou direitos de natureza econômica, no âmbito público ou privado. A essência do elemento patrimonial é o seu valor econômico, passível de ser expresso em dinheiro. Além disso, também é patrimônio, aqueles bens que, embora sem valor comercial, possuem utilidade ou valor moral para o seu titular. Após o crivo legislativo, será possível enquadrar ou não determinada atitude como crime, em desfavor dos bens de pessoa física ou jurídica, tendo o patrimônio como elemento fundamental de proteção (Masson, 2015).

Dentre as infrações de lesão patrimonial, o furto, o roubo, o dano e o estelionato são destaque entre as ações ilegais. O furto, tipificado no artigo 155 do CPB, trata-se da subtração de coisa móvel alheia, para benefício próprio ou de outra pessoa. Sendo assim, um delito que possui como objeto jurídico o patrimônio pessoal de propriedade ou posse legítima. No crime de roubo, previsto no artigo 157 do CPB, há também a subtração de coisa móvel alheia, em benefício próprio ou de terceiros, com a presença da grave ameaça ou violência contra pessoa, ponto que difere do crime tipificado como furto. A integridade física, patrimonial e a liberdade individual são os objetos jurídicos do roubo (Nucci, 2025).

No caso da ação ilícita de destruir, inutilizar ou deteriorar coisa alheia, há o enquadramento como dano no artigo 163 do CPB. Nesse crime, quem sofre a agressão do agente é a coisa, uma das particularidades desse delito, trata-se da sabotagem informática por vírus, quando compromete, consideravelmente, o funcionamento ou destrói algum programa da máquina computacional (Nucci, 2025).

O estelionato, tipificado no artigo 171 do CPB, trata-se da obtenção de vantagem ilícita, para si próprio ou terceiro, gerando prejuízo alheio, através do induzimento ou mantendo alguma pessoa em erro por meio fraudulento. Esse crime pode ser praticado de diversas maneiras, sendo a prevista no caput do artigo, a mais ampla. Nessa modalidade, o agente busca obter vantagem ilícita, seja um benefício, ganho ou lucro, ao induzir ou manter alguém em erro. Frequentemente, a vítima, por engano, colabora involuntariamente com a ação delituosa, sem perceber que está sendo lesada. A palavra induzir, no sentido literal da lei, significa persuadir ou levar ao erro, enquanto manter, seria conservar a vítima na situação

enganosa. Assim, a vantagem indevida decorre tanto do engano provocado diretamente pelo agente, quanto da omissão que permite à vítima permanecer equivocada (Nucci, 2025).

O §2º-A (Brasil, 1940) do respectivo artigo, acrescenta a possibilidade de qualificação do crime de estelionato, quando cometido mediante fraude eletrônica. A pena prevista é de reclusão de quatro a oito anos, além de multa, quando o delito é realizado mediante o uso de informações obtidas da própria vítima ou de terceiro enganado por meio de redes sociais, ligações telefônicas, e-mails fraudulentos ou outros artifícios semelhantes. Nucci (2025) destaca que a ampliação do dispositivo legal, introduzida pela Lei nº 14.155/2021, teve como objetivo, abranger as novas formas de fraude decorrentes do avanço tecnológico, reconhecendo a multiplicidade de mecanismos eletrônicos e informáticos, utilizados para ludibriar as pessoas no ambiente digital.

A evolução das tecnologias, além dos benefícios, também proporciona a possibilidade do cometimento de crimes por intermédio dos novos aparatos digitais. O estelionato digital, previsto no artigo 171-A do CPB, é o exemplo da atuação impactante do mundo tecnológico na vida dos brasileiros. Nucci ressalta que:

Há diversos modos de se concretizar este estelionato. Organizar (reunir pessoas para atingir um objetivo, compondo uma estrutura previamente iniciada, aproximar coisas ou pessoas para uma finalidade), gerir (administrar, comandar ou dirigir), distribuir (repartir algo entre várias pessoas, dividir em partes), intermediar (servir de contato entre partes, entremear) são os verbos constitutivos da conduta típica, cujo objeto pode ser carteira (setores ou partes de instituições financeiras, conjunto de aplicações para obtenção de lucro, apontamentos financeiros) ou operação (prática de um conjunto de atos aptos a atingir uma meta).

(...)

Cuida-se de tipo penal voltado a punir o estelionato digital ou o criptoestelionato, razão pela qual envolve a obtenção de uma vantagem ilícita (qualquer benefício, ganho ou lucro auferido de modo indevido, ou seja, contrário às regras do ordenamento jurídico), que, neste caso, é uma vantagem de natureza econômica, pois se cuida de crime patrimonial (Nucci, 2025, pp.705 e 706).

CRIMES CIBERNÉTICOS

A Central Nacional de Denúncias de Crimes Cibernéticos divulgou, no ano de 2020, um estudo demonstrativo da ascensão dos crimes cometidos com a ajuda da internet, onde foi apresentado o número de 156.692 denúncias relacionadas aos delitos no âmbito virtual (Garrett, 2021 *apud* Pinheiro, 2022).

Embora seja crescente a prática de crimes com o uso da internet, ainda não há a uma definição fixa sobre o que seria os crimes cibernéticos ou cibercrimes, pois existem diversas condutas que se enquadram nesse tipo de ilegalidade (Pinheiro, 2022). Dentre as definições, alguns estudiosos do tema explicam, por exemplo, que: “crime informático é um fenômeno

inerente às transformações tecnológicas que a sociedade experimenta e que influenciaram diretamente no direito penal” (Damásio e Milagre, 2016, p. 48 *apud* Araújo, 2023). Isso permite compreender a expressão “crime informático” como um gênero, do qual os crimes cibernéticos e telemáticos são espécies. Cláudio Rodrigues Araújo, ao citar Viana e Machado (2014), no seu livro, destaca que:

(...) a conceituação de delito informático pode ter trilhado como uma conduta típica e ilícita, que constitui crime ou contravenção, doloso ou de culpa, comissiva ou de omissão, por prática por pessoa física ou jurídica, com a utilização da informática no ambiente de rede ou fora dele, ofendendo de forma direta ou não a segurança informática, que possui por elementos a integridade, disponibilidade e confidencialidade.

Os chamados delitos informáticos, (...), aborda crimes e contravenções penais, o que alcança não apenas as condutas com prática no contexto da internet, mas total conduta na qual existe relacionamento com sistemas informáticos. Isto é, uma fraude na qual o computador tem utilização como ferramenta de crime, fora da internet, também seria alcançada pelo que teve denominação delitos informáticos. Mas, delito informático é gênero, de onde delito telemático é espécie, dada a peculiaridade de ocorrência no e partindo inter-relacionamento perante os computadores em rede telemática utilizados na prática delitiva (Viana e Machado, 2014 *apud* Araújo, 2023, p. 20).

Os doutrinadores, especialistas no direito penal, produzem as formas de classificar os delitos cometidos nos meios digitais, pois existem condutas ilegais que são exauridas no próprio ambiente virtual, e têm aquelas que a internet é o instrumento meio para o cometimento de algum crime fim. Diante disso, há duas formas de classificação, no primeiro momento, qualifica como crimes puros, mistos ou comuns, já no segundo instante são previstos os crimes próprios e impróprios (Pinheiro, 2022).

Na primeira forma de classificação, encontram-se os crimes puros, onde a finalidade é alcançar e violar o sistema computacional, nessa prática, os *crackers* (indivíduo com conhecimento computacional avançado) trabalham burlando os sistemas de informática. Já nos crimes mistos, o objetivo não é atingir o computador, mas sim os dados e recursos da vítima. Nesse enquadramento, a internet é dedicada à prática de ilicitudes, como por exemplo, delitos em desfavor do patrimônio. Por fim, quando se tratar dos crimes comuns, a internet será o meio de consumação de algum crime já tipificado no CPB, onde temos como amostra, o crime de racismo (Araújo, 2023).

No momento seguinte, há a divisão dos crimes próprios, praticados estritamente através de computadores, onde a violação do ambiente informático é onde se consoma o crime, necessitando de leis específicas para tratar do assunto (Pinheiro, 2022). No Brasil, ainda há uma carência de dispositivos para destrinchar essas condutas ilegais, ocorridas no mundo computacional. No caso dos crimes de invasão de algum computador, não era previsto

nenhuma legislação, porém, a Lei nº 12.737/2012 tipificou o crime de invasão de dispositivo informático, normativa introduzida no art. 154-A do CPB (Justiniano, 2016 *apud* Pinheiro 2022).

No caso dos crimes impróprios, há uma ação delituosa comum, tipificada e consolidada no ordenamento jurídico brasileiro, na qual o meio virtual funciona apenas como um dos instrumentos de execução, havendo somente uma alteração de ordem instrumental. Diante disso, delitos como o furto, previsto no artigo 155 do CPB, podem ser praticados tanto de forma presencial quanto virtualmente, sem que haja necessidade de tipificação específica. A mesma linha de pensamento se aplica a crimes como estelionato e pedofilia, nos quais o uso da internet serve apenas como veículo para a prática de infrações, já tuteladas pela legislação penal (Justiniano, 2016 *apud* Pinheiro 2022).

Perante o exposto, ficou explícito que os crimes cibernéticos não se caracterizam como um acontecimento isolado, pois é perceptível uma extensão de atuação da criminalidade tradicional adaptada ao ambiente virtual. Graças à ausência de uniformidade conceitual e à contínua evolução tecnológica, mostra-se necessário uma análise das ferramentas jurídicas, aptas a contemplar condutas exclusivas no espaço virtual, acrescentando aquelas que a internet é apenas um meio de execução de alguma ilegalidade.

INSTRUMENTOS JURÍDICOS NO COMBATE AOS CRIMES CIBERNÉTICOS PATRIMONIAIS

O Anuário Brasileiro de Segurança Pública 2023 retratou que os crimes de estelionato por meio eletrônico, chegaram a um quantitativo de 200.322 ocorrências em 2022, demonstrando a ascensão de 65,2% quando comparado com os registros de casos em 2021, ano que ocorreu a tipificação do crime anteriormente citado (Lima; Bueno, 2023). Ademais, os autores dessa análise das novas configurações dos crimes patrimoniais no Brasil, complementam que:

Embora no Brasil a tipificação de fraude eletrônica seja recente, o crescimento dos crimes de estelionato (que não diferencia aqueles em meio eletrônico dos demais) ocorreu de modo exponencial durante a pandemia de Covid-19, saltando de 426.799 ocorrências no ano de 2018 para 1.819.409 em 2022. Um crescimento da ordem de 300% desafia a lógica de trabalho de qualquer organização (...) (Lima; Bueno, 2023, p. 96).

A partir disso, é imprescindível a análise das leis existentes e capazes de abarcar essas atitudes ilícitas. A Lei nº 12.737/2012 (Brasil, 2012), conhecida como Lei Carolina Dieckmann, foi o “pontapé” legislativo para que houvesse a punição de crimes virtuais, e se

deu a partir da repercussão em razão da exposição de fotos íntimas da atriz, através da internet. A normativa trouxe atualizações para o CPB, tipificando algumas ações como a de invasão de dispositivo informático (Sena; Oliveira; Santos, 2023).

Posteriormente, surgiu a Lei nº 12.965/2014 (Brasil, 2014), o marco civil da internet, responsável por regulamentar o uso da internet no Brasil, estabelecendo princípios, direitos e deveres para que o ambiente digital seja transparente e seguro. No ano de 2020, entrou em vigor a Lei nº 13.709/2018 (Brasil, 2018), a LGPD, que dispõe sobre o tratamento dos dados pessoais, nos meios físicos e virtuais, além de fornecer ferramentas essenciais para o estudo do Direito Digital.

No artigo “Crimes contra o patrimônio na internet: Golpes financeiros e a atuação estatal na aplicação da lei penal”, os autores discorrem que a LGPD, no cenário contemporâneo, reside na promoção de práticas que reforçam a segurança jurídica no tratamento e compartilhamento de informações no meio digital. Inclusive, a norma contribui para a proteção dos direitos e garantias constitucionais, ao mesmo tempo em que fomenta a adoção de medidas preventivas voltadas à redução e ao combate de crimes virtuais (Sena; Oliveira; Santos, 2023).

Em 2021, a Lei 14.155/2021 (Brasil, 2021), alterou o Código Penal e Processual Penal com a finalidade de repreender com rigidez os crimes virtuais, essa mudança promoveu o endurecimento das penas e qualificadoras relacionadas aos crimes cibernéticos de invasão a dispositivo informático, fraude eletrônica e estelionato contra idoso ou vulnerável no ambiente digital. Isso fez com que as penas, a depender da conduta, possam variar de 1 a 8 anos, sendo possível ultrapassar 13 anos quando aplicável a majoração (Sena; Oliveira; Santos, 2023).

Mesmo com a carência de algumas previsões legais, aplicáveis, a casos delituosos no mundo digital, a justiça brasileira busca combater e punir criminosos que se aproveitam do meio virtual para o cometimento de ilegalidades. O autor da obra “Crimes Virtuais”, aponta que:

A maior parte dos magistrados considera que aproximadamente 95% dos delitos cometidos de forma eletrônica já possuem tipificação no Código Penal, por caracterizar crimes comuns com prática partindo da internet (...). Para esses 5%, a internet não é uma área nova de atuação, mas somente um novo caminho para realizar delitos já com prática no mundo real, e basta somente que as leis tenham adaptação para os crimes virtuais. E é isso que a justiça vem fazendo, adaptando e empregando diversos dispositivos no Código Penal para combater o crime digital (OLIVEIRA et al., 2017 *apud* Araújo, 2023, pp. 24 e 25).

Devido à inovação de condutas ilícitas no âmbito virtual e à prática de crimes já conhecidos, mas agora com o uso do artifício da internet, não se mostra tarefa simples enquadrar as ocorrências nas legislações existentes. Em face do exposto, o Superior Tribunal de Justiça (STJ) é corriqueiramente provocado para analisar e decidir sobre a interpretação de normas infraconstitucionais, relacionadas aos crimes cometidos nas redes digitais. Ademais, a Terceira Seção do STJ consolidou a ideia de que a subtração de quantias de conta bancária, através de transferência eletrônica fraudulenta, caracteriza o crime de furto, tipificado no Art. 155, §4º, inciso II, do CPB (STJ, 2018).

Outro ponto, que importa salientar, seria a discussão habitual sobre o juízo de competência para a solução de casos de furto no ciberespaço. O STJ firmou o entendimento que a competência é estabelecida pelo local onde o bem foi subtraído da vítima. Em um dos casos concretos de conflito de competência (CC 145.576), onde ocorreu um furto mediante transferência eletrônica de contas-correntes da agência bancária de Barueri (SP) com valores enviados para Imperatriz (MA), o tribunal superior decidiu que a competência para julgar o caso seria na cidade paulista, pois as vítimas do ilícito eram dessa região (STJ, 2018).

Portanto, mesmo com a vigência de leis e entendimentos jurisprudenciais, direcionados ao enfrentamento dos crimes cibernéticos contra o patrimônio, ainda se evidencia uma sensível insuficiência normativa. Tal fragilidade revela-se na dificuldade do texto legal em acompanhar com celeridade, a dinâmica complexa das transformações tecnológicas e sociais da atualidade. Isso demonstra como é primordial a revisão e modernização contínua do Código Penal Brasileiro, em consonância com o aprimoramento das legislações específicas, com a finalidade de assegurar uma tutela penal efetiva, que contemple as novas formas de lesão à honra, à moral e ao patrimônio, consolidando um sistema jurídico mais eficaz, preventivo e capaz de responder aos desafios da era digital.

CONSIDERAÇÕES FINAIS

O artigo científico teve como propósito, examinar os reflexos provocados pelos crimes cibernéticos no ordenamento jurídico brasileiro, com especial atenção àqueles que atentam contra o patrimônio. Partindo da constatação de que a sociedade atual se encontra profundamente imersa na era digital, observou-se que a interconexão proporcionada pelas tecnologias da informação, potencializou a comunicação e o compartilhamento de dados em escala global. Porém, esse avanço engendrou um cenário de vulnerabilidade crescente, devido

à instantaneidade e a ausência de fronteiras, o que favoreceu o surgimento de novas formas de criminalidade, que desafiam os mecanismos tradicionais de prevenção e repressão penal.

Constatou-se, ao longo do estudo, que a dependência tecnológica do meio social, ampliou substancialmente as possibilidades de ocorrência de delitos patrimoniais praticados por meio eletrônico, como fraudes, estelionatos digitais, invasões de dispositivos informáticos e outros ataques voltados à subtração de dados e valores. Diante dessas atividades criminosas, tornou-se necessário o entendimento jurisprudencial e a intervenção do legislador, que, a partir da promulgação da Lei nº 12.737/2012 e, posteriormente, da Lei nº 14.155/2021, tipificou condutas antes não previstas e conferiu maior rigor punitivo às ações ilegais que se valem dos meios eletrônicos.

Apesar dos avanços legislativos e jurisprudenciais, verificou-se que o arcabouço jurídico brasileiro enfrenta entraves significativos, em virtude da agilidade e novos *modus operandi* dos criminosos. A mutabilidade dos meios digitais, aliada à atuação transnacional dos malfeitores, impõe à dogmática penal e ao processo de persecução criminal, o desafio constante de adaptação. Tal realidade torna evidente que o enfrentamento ao cibercrime não pode restringir-se à mera criação de tipos penais, exigindo assim, uma abordagem sistêmica que una atualização legislativa contínua, interpretação jurisprudencial dinâmica e cooperação institucional entre órgãos públicos e privados.

Por fim, ressalta-se que a temática abordada mantém-se em constante evolução, exigindo novas pesquisas e reflexões. As pretensões futuras de investigação deverão concentrar-se na avaliação das lacunas ainda existentes na legislação brasileira, na efetividade das políticas de prevenção e na cooperação internacional no combate aos delitos cibernéticos. A partir disso, o foco é contribuir para o fortalecimento de um Direito Penal Digital, que seja, ao mesmo tempo, eficiente, proporcional e compatível com os valores constitucionais do Estado Democrático de Direito.

REFERÊNCIAS

Agência Senado. **Golpes digitais atingem 24% da população brasileira, revela DataSenado.** Senado Notícias, Brasília, DF, 1 out. 2024. Disponível em: <https://www12.senado.leg.br/noticias/materias/2024/10/01/golpes-digitaais-atingem-24-da-populacao-brasileira-revela-datasenado>. Acesso em: 18 set. 2025.

Araújo, Cláudio Rodrigues. **Crimes virtuais.** Belo Horizonte: Editora Expert, 2023. ISBN 978-65-6006-018-0. Disponível em: <https://experteditora.com.br/wp-content/uploads/2023/07/Crimes-virtuais.pdf>. Acesso em: 11 ago. 2025.

Brasil. Decreto-Lei n.º 2.848, de 7 de dezembro de 1940. **Código Penal.** Diário Oficial da União: seção 1, Brasília, DF, 7 dez. 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm. Acesso em: 24 ago. 2025.

Brasil. Lei n.º 12.737, de 30 de novembro de 2012. **Dispõe sobre a tipificação criminal de delitos informáticos;** altera o Decreto-Lei n.º 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, 3 dez. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 19 set. 2025.

Brasil. Lei n.º 12.965, de 23 de abril de 2014. **Marco Civil da Internet:** estabelece princípios, garantias, direitos e deveres para uso da Internet no Brasil. Diário Oficial da União: seção 1, Brasília, DF, 23 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 15 set. 2025.

Brasil. Lei n.º 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD):** dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, e altera a Lei n.º 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 15 set. 2025.

Brasil. Supremo Tribunal Federal. **ADI 6.387-DF.** Min. rel. Rosa Weber. Publicado em 24 de abril de 2020. Disponível em: <https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629>. Acesso em: 15 set. 2025.

Brasil. **Lei nº 14.155, de 27 de maio de 2021.** Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 – Código de Processo Penal, para aperfeiçoar a tipificação penal e o tratamento processual dos crimes de violação de dispositivo informático, de furto e de estelionato, cometidos mediante uso de dispositivo eletrônico ou informático, conectados ou não à rede de computadores. Diário Oficial da União: seção 1, Brasília, DF, 28 maio 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm. Acesso em: 19 set. 2025.

Brito, Auriney. **Direito penal informático.** São Paulo: Saraiva, 2013.

Castells, Manuel. **A Sociedade em Rede.** São Paulo: Paz e Terra, 2002.

Lima, Renato Sérgio de; Bueno, Samira. **As novas configurações dos crimes patrimoniais no Brasil**. In: FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. 17º Anuário Brasileiro de Segurança Pública. São Paulo: Fórum Brasileiro de Segurança Pública, p. 90-97, 2023. Disponível em: <https://forumseguranca.org.br/wp-content/uploads/2023/07/anuario-2023.pdf>. Acesso em: 28 set. 2025.

Masson, Cleber. **Direito Penal Esquematizado: parte especial – vol. 2. 9. ed., rev., atual. e ampl.** São Paulo: Método; Rio de Janeiro: Forense, 2015. ISBN 978-8530960162. Disponível em: <https://2014direitounic.wordpress.com/wp-content/uploads/2016/02/cleber-masson-direito-penal-esquematizado-vol-2-20152.pdf>. Acesso em: 01 set. 2025.

Nakamura, João. **Brasil é vice-campeão em ataques cibernéticos, com 1.379 golpes por minuto, aponta estudo**. CNN Brasil, São Paulo, 30 out. 2024. Disponível em: <https://www.cnnbrasil.com.br/economia/negocios/brasil-e-vice-campeao-em-ataques-ciberneticos-com-1-379-golpes-por-minuto-aponta-estudo/>. Acesso em: 15 set. 2025.

Nucci, Guilherme de S. **Manual de Direito Penal - Volume Único - 21ª Edição 2025. 21. ed.** Rio de Janeiro: Forense, 2025. *E-book*. ISBN 9788530996468. Disponível em: <https://app.minhabiblioteca.com.br/reader/books/9788530996468/>. Acesso em: 24 ago. 2025.

Pinheiro, Bruno Victor de Arruda. **As novas disposições sobre os crimes cibernéticos**. Jusbrasil, 2022. Disponível em: <https://www.jusbrasil.com.br/artigos/as-novas-disposicoes-sobre-os-crimes-ciberneticos/1518500029>. Acesso em: 08 set. 2025.

Prado, Marina Silveira. **A influência da tecnologia no comportamento humano**. Saúde News. Disponível em: <https://revistasaudenews.com.br/post/919/a-influencia-da-tecnologia-no-comportamento-humano>. Acesso em: 18 ago. 2025.

Sena, Larissa dos Santos; Oliveira, Deivid Lopes de; Santos, Fábio da Silva. **Crimes contra o patrimônio na internet: golpes financeiros e a atuação estatal na aplicação da lei penal**. [s.l.]: [s.n.], 2023. Disponível em: <https://unifan.net.br/wp-content/uploads/2023/02/CRIMES-CONTRA-O-PATRIMONIO-NA-INTERNET-GOLPES-FINANCEIROS-E-A-ATUACAO-ESTATAL-NA-APLICACAO-DA-LEI-PENAL.pdf>. Acesso em: 29 set. 2025.

Silva, Liliane. **Tecnologias de informação e comunicação**, 2010. Disponível em: <https://pt.slideshare.net/lilianesilva14/a-internet>. Acesso em: 11 ago. 2025.

Silva, Daniel Neves. **"História da internet"**; Brasil Escola. Disponível em: <https://brasilecola.uol.com.br/informatica/internet.htm>. Acesso em: 17 ago. 2025.

Silveira, Fabrício da. **Anonimato e delinquência digital: O impacto da internet no comportamento criminoso**, 2025. Disponível em: <https://www.jusbrasil.com.br/artigos/anonimato-e-delinquencia-digital-o-impacto-da-internet-no-comportamento-criminoso/3920256630>. Acesso em: 22 ago. 2025.

SUPERIOR TRIBUNAL DE JUSTIÇA (STJ). **Crimes pela internet, novos desafios para a jurisprudência**. 17 jun. 2018. Disponível em: https://www.stj.jus.br/sites/portallp/Paginas/Comunicacao/Noticias-antigas/2018/2018-06-17_06-57_Crimes-pela-internet-novos-desafios-para-a-jurisprudencia.aspx. Acesso em: 30 set. 2025.