



PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO
MONOGRAFIA JURÍDICA

**A FRAGILIDADE DA LEGISLAÇÃO PENAL FRENTE AOS CRIMES DE FURTO
EM BANCOS DIGITAIS**
UMA ANÁLISE DAS LACUNAS NORMATIVAS E DA AUSÊNCIA DE
REGULAMENTAÇÃO ESPECÍFICA PARA CRIMES DIGITAIS NO SISTEMA PENAL
BRASILEIRO

ORIENTANDA: GABRIELLEN OLIVEIRA DA SILVA
ORIENTADORA: PROFA. MS. LARISSA JUNQUEIRA REIS BAREATO

GOIÂNIA-GO
2025

GABRIELLEN OLIVEIRA DA SILVA

**A FRAGILIDADE DA LEGISLAÇÃO PENAL FRENTE AOS CRIMES DE FURTO
EM BANCOS DIGITAIS**

UMA ANÁLISE DAS LACUNAS NORMATIVAS E DA AUSÊNCIA DE
REGULAMENTAÇÃO ESPECÍFICA PARA CRIMES DIGITAIS NO SISTEMA PENAL
BRASILEIRO

Monografia Jurídica apresentada à disciplina
Trabalho de Curso II, da Escola de Direito,
Negócios e Comunicação da Pontifícia
Universidade Católica de Goiás (PUCGOIÁS).
Profa. Ms. Orientadora Larissa Junqueira Reis
Bareato.

GOIÂNIA-GO
2025

GABRIELLEN OLIVEIRA DA SILVA

**A FRAGILIDADE DA LEGISLAÇÃO PENAL FRENTE AOS CRIMES DE FURTO
EM BANCOS DIGITAIS**

UMA ANÁLISE DAS LACUNAS NORMATIVAS E DA AUSÊNCIA DE
REGULAMENTAÇÃO ESPECÍFICA PARA CRIMES DIGITAIS NO SISTEMA PENAL
BRASILEIRO

Data da Defesa: 19 de novembro de 2025

BANCA EXAMINADORA

Orientadora: Profa. Ms. Larissa Junqueira Reis Bareato	Nota
--	------

Examinadora Convidada: Profa. Ms. Marina Rúbia	Nota
--	------

Dedico este trabalho à minha mãe, cuja força, amor e apoio incondicional me permitiram chegar até aqui. Ao meu namorado, pelo incentivo constante desde o início desta jornada, e aos meus amigos, que, como companheiros de caminhada, tornaram essa experiência mais rica e significativa.

RESUMO

O presente trabalho monográfico analisou a fragilidade da legislação penal brasileira frente aos crimes de furto em bancos digitais, por meio do exame das lacunas normativas e da ausência de regulamentação específica para os delitos cibernéticos no sistema pátrio. Para seu desenvolvimento, adotou-se a metodologia da pesquisa bibliográfica e documental, que contemplou a evolução histórica do crime de furto e o seu confronto com a realidade da era digital. Verificou-se que o conceito clássico de furto, centrado na materialidade da “coisa alheia móvel”, tornou-se conceitualmente insuficiente diante da desmaterialização dos bens e valores em contas virtuais. O estudo comprovou que a ascensão do ciberespaço proporcionou o aumento exponencial desses crimes, fenômeno analisado à luz da Teoria das Atividades Rotineiras. Evidenciou-se, ainda, que a Lei nº 14.155/2021 não supriu a necessidade de tipificação autônoma para o furto eletrônico, o que resultou em insegurança jurídica e na oscilação da jurisprudência em relação ao enquadramento penal, entre furto qualificado e estelionato eletrônico. Concluiu-se que a proteção efetiva do patrimônio digital demandou uma urgente reforma legislativa que incluísse a criação de um tipo penal específico para o furto eletrônico, garantindo maior coerência e eficácia à repressão criminal.

Palavras-chave: Legislação Penal; Furto Eletrônico; Bancos Digitais; Crimes Cibernéticos; Reforma Legislativa.

ABSTRACT

This study analyzed the weaknesses of Brazilian criminal law regarding digital bank theft by examining regulatory gaps and the lack of specific regulations for cybercrimes in the Brazilian system. The study adopted a bibliographic and documentary research methodology, which examined the historical evolution of the crime of theft and its confrontation with the reality of the digital age. It found that the classic concept of theft, centered on the materiality of "movable property," has become conceptually insufficient given the dematerialization of assets and values in virtual accounts. The study demonstrated that the rise of cyberspace has led to an exponential increase in these crimes, a phenomenon analyzed through the lens of Routine Activities Theory. It was also evident that Law No. 14,155/2021 did not address the need for a separate criminal classification for electronic theft, resulting in legal uncertainty and a shift in case law regarding the criminal classification between qualified theft and electronic fraud. It was concluded that effective protection of digital assets required urgent legislative reform that included the creation of a specific criminal category for electronic theft, ensuring greater coherence and effectiveness in criminal prosecution.

Keywords: Criminal Law; Electronic Theft; Digital Banks; Cybercrimes; Legislative Reform.

SUMÁRIO

INTRODUÇÃO	6
1. A EVOLUÇÃO HISTÓRICA DO CRIME DE FURTO E DA LEGISLAÇÃO PENAL BRASILEIRA	8
1.1 ORIGEM E DESENVOLVIMENTO DO DIREITO PENAL NO BRASIL	8
1.2 A TIPIFICAÇÃO DO CRIME DE FURTO NAS CONDIÇÕES PENAS BRASILEIRAS	9
1.3 A EVOLUÇÃO DOUTRINÁRIA E JURISPRUDENCIAL DO CONCEITO DE “FURTO”	10
1.4 O IMPACTO DAS TRANSFORMAÇÕES SOCIAIS E TECNOLÓGICAS NA CONFIGURAÇÃO DOS CRIMES PATRIMONIAIS	11
2. O NOVO MUNDO DA ERA DIGITAL	13
2.1 A TRANSFORMAÇÃO DOS CRIMES PATRIMONIAIS NO AMBIENTE VIRTUAL	13
2.1.1 A teoria das atividades rotineiras	16
2.2 A ATUAÇÃO DOS CRIMINOSOS NAS PLATAFORMAS DIGITAIS	17
2.3 AS VULNERABILIDADES DOS SISTEMAS BANCÁRIOS DIGITAIS E O AUMENTO DOS FURTOS ELETRÔNICOS	17
3. A FRAGILIDADE LEGISLATIVA E OS DESAFIOS JURÍDICOS	20
3.1 A LEI Nº 14.155/2021 E SUAS LIMITAÇÕES NA REPRESSÃO AOS CRIMES DIGITAIS	20
3.2 O CÓDIGO PENAL E A AUSÊNCIA DE TIPIFICAÇÃO ESPECÍFICA PARA OS FURTOS ELETRÔNICOS	23
3.3 A NECESSIDADE DE REFORMA LEGISLATIVA DIANTE DA EVOLUÇÃO TECNOLÓGICA	25
3.3.1 A responsabilidade dos Bancos	27
3.4 A INSEGURANÇA JURÍDICA	28
CONCLUSÃO	31
REFERÊNCIAS	33

INTRODUÇÃO

O presente trabalho tem como tema central a fragilidade da legislação penal brasileira frente aos crimes de furto em bancos digitais. Este tema emerge da crescente digitalização das relações sociais e financeiras, que, embora traga inegáveis benefícios, expõe o patrimônio a novas e sofisticadas formas de agressão. A rápida evolução tecnológica e a virtualização do patrimônio confrontam a concepção tradicional do Direito Penal, que ainda se apoia majoritariamente na materialidade do objeto furtado, conforme disposto no Código Penal Brasileiro de 1940.

O objetivo geral desta pesquisa é realizar uma análise crítica das lacunas normativas e da ausência de regulamentação específica para os crimes digitais de furto no sistema penal brasileiro. Busca-se, assim, demonstrar como a insuficiência legislativa e a dificuldade de enquadramento penal comprometem a repressão eficaz a esses delitos.

Deste modo, a investigação busca responder ao seguinte problema de pesquisa: Em que medida a ausência de tipificação penal autônoma para os furtos em bancos digitais e a fragilidade conceitual da Lei nº 14.155/2021 geram insegurança jurídica e comprometem a efetividade da tutela penal do patrimônio no ambiente virtual brasileiro?

Para alcançar o objetivo proposto, o trabalho adota um procedimento metodológico de natureza bibliográfica e documental. A pesquisa baseia-se na análise de doutrina especializada em Direito Penal, Processo Penal e Criminologia, contemplando autores como Rogério Greco, Guilherme de Souza Nucci, e Cezar Roberto Bitencourt. Além disso, são examinados os diplomas legais pertinentes, com destaque para o Código Penal e a Lei nº 14.155/2021, bem como a jurisprudência atual do Superior Tribunal de Justiça (STJ) sobre o tema.

O trabalho está estruturado em três capítulos principais, que desdobram o tema central, conforme o que se segue.

O Capítulo 1 trata de A Evolução Histórica do Crime de Furto e da Legislação Penal Brasileira. Inicia-se com a origem do Direito Penal no Brasil e a tipificação do crime de furto nas codificações históricas, passando pela evolução doutrinária e jurisprudencial do conceito, e finalizando com a análise do impacto das transformações sociais e tecnológicas na configuração dos crimes patrimoniais.

O Capítulo 2 aborda O Novo Mundo da Era Digital. Este segmento explora a transformação dos crimes patrimoniais no ambiente virtual, a aplicação da Teoria das Atividades Rotineiras ao contexto cibernético, a atuação dos criminosos nas plataformas digitais e as vulnerabilidades dos sistemas bancários digitais frente ao aumento dos furtos eletrônicos.

Por fim, o Capítulo 3 versa sobre A Fragilidade Legislativa e os Desafios Jurídicos. Analisa-se a Lei nº 14.155/2021 e suas limitações na repressão aos crimes digitais, a ausência de tipificação específica para os furtos eletrônicos no Código Penal, a necessidade premente de reforma legislativa diante da evolução tecnológica e, por fim, a insegurança jurídica e as dificuldades de enquadramento penal dos crimes digitais.

Ao final, a pesquisa conclui pela urgência de uma reforma legislativa que vá além da mera ampliação de penas, contemplando a criação de instrumentos processuais e técnicos compatíveis com a complexidade do mundo digital.

1. A EVOLUÇÃO HISTÓRICA DO CRIME DE FURTO E DA LEGISLAÇÃO PENAL BRASILEIRA

1.1 ORIGEM E DESENVOLVIMENTO DO DIREITO PENAL NO BRASIL

O Direito Penal, enquanto instrumento de controle social formalizado, tem suas raízes na necessidade humana de preservar a convivência e proteger bens jurídicos considerados essenciais à manutenção da ordem social. Em suas origens mais remotas, a punição era pautada pela vingança privada, o “olho por olho, dente por dente” do Código de Hamurabi, expressão de um sistema rudimentar de justiça em que a reparação do dano recaía diretamente sobre o ofensor, sem mediação estatal.

Roberto Sanches Cunha (2024, p. 60) expressa que, no período inicial da colonização portuguesa no Brasil, vigoravam as Ordenações Afonsinas, sistema jurídico de natureza religiosa e influenciado pelo direito romano, que era o mesmo aplicado em Portugal. Em 1514, esse conjunto normativo foi substituído pelas Ordenações Manuelinas, que mantiveram a estrutura anterior, porém sem a previsão objetiva de tipos e quantidades de penas, deixando essa definição ao arbítrio dos juízes. Posteriormente, essas ordenações deram lugar à compilação organizada por D. Duarte Nunes Leão, conhecida como Código de D. Sebastião ou Código Sebastião, que buscou reunir leis esparsas e de difícil compreensão pela população.

Essa compilação foi sucedida pelas Ordenações Filipinas, que prevaleceram por mais de dois séculos a partir do século XVII. De forte cunho religioso, o Código Filipino aproximava direito, moral e religião, aplicando punições severas e desumanas, especialmente contra práticas consideradas heréticas ou contrárias à fé oficial, afirma o mesmo autor.

Nesse sentido, com a Independência e a Constituição de 1824, surgiu o Código Criminal do Império, pautado por princípios mais humanitários e protetivos, permitindo a individualização das penas, estabelecendo agravantes e atenuantes e prevendo tratamento específico para menores de quatorze anos. Apesar de ainda prever a pena de morte, esta foi praticamente restrita a crimes cometidos por escravizados, mantendo ainda a criminalização de ofensas à religião oficial. Após a

Proclamação da República, em 1890, foi instituído o Código Criminal Republicano, ajustado às proibições constitucionais de 1891, como a vedação à pena de morte e à prisão perpétua. Esse código implementou penas de prisão, banimento temporário e suspensão de direitos, consolidando um sistema penitenciário de caráter correcional. Entretanto, a proliferação de leis complementares e extravagantes levou, em 1932, à necessidade de compilação das normas penais, resultando na Consolidação das Leis Penais, elaborada por Vicente Piragibe (Cunha, 2024).

Com o passar dos séculos, o Estado assumiu o monopólio da jurisdição penal, consolidando o direito de punir (*jus puniendi*) como prerrogativa exclusiva do poder público. No Brasil, a estruturação do Direito Penal seguiu a tradição europeia, em especial a influência do pensamento liberal iluminista, que inspirou o Código Criminal do Império de 1830, primeiro diploma penal nacional.

Esse Código já previa o crime de furto em termos amplos, definindo-o como a subtração de coisa alheia móvel, refletindo a preocupação do legislador com a tutela do patrimônio material. Conforme destaca Cezar Roberto Bitencourt (2019, p. 47), “O Direito Penal brasileiro, desde sua formação, buscou equilibrar o rigor punitivo com os ideais humanistas, herdados do Iluminismo e da escola clássica”.

1.2 A TIPIIFICAÇÃO DO CRIME DE FURTO NAS CODIFICAÇÕES PENAIS BRASILEIRAS

O Código Criminal de 1830, em seu artigo 259, já tipificava o furto como a “subtração de coisa alheia móvel”, com previsão de penas proporcionais ao valor do bem furtado. Ainda que rudimentar, o dispositivo estabeleceu as bases do tipo penal que seria consolidado em legislações posteriores.

Com o advento do Código Penal de 1890, o legislador ampliou o rol de circunstâncias qualificadoras, reconhecendo modalidades mais graves de furto, como o praticado durante o repouso noturno ou com rompimento de obstáculo. Essa codificação também reforçou o caráter patrimonial do delito, desvinculando-o de aspectos morais e aproximando-o da concepção moderna de proteção ao bem jurídico.

Já o Código Penal de 1940, ainda em vigor, sistematizou de forma mais técnica a matéria. O crime de furto foi inserido no Título II da Parte Especial, sob o

capítulo “Dos Crimes Contra o Patrimônio”, no artigo 155, que dispõe:

“Subtrair, para si ou para outrem, coisa alheia móvel: Pena – reclusão, de um a quatro anos, e multa. ”

Segundo Rogério Greco (2020, p. 422), esse tipo penal reflete a concepção clássica do furto, baseada na materialidade do objeto: “O furto pressupõe a subtração de um bem corpóreo, tangível, que possa ser transportado ou removido do poder de seu legítimo possuidor. ” Esse conceito, embora tenha atendido às necessidades do século XX, mostra-se atualmente limitado diante das novas formas de apropriação patrimonial, em especial aquelas realizadas por meio digital, nas quais o objeto material dá lugar a dados, senhas e ativos virtuais.

1.3 A EVOLUÇÃO DOUTRINÁRIA E JURISPRUDENCIAL DO CONCEITO DE “FURTO”

A doutrina penal clássica consolidou o entendimento de que o furto é uma violação ao direito de propriedade que exige a subtração física de uma coisa alheia móvel. Damásio de Jesus (2016, p. 231) explica que “a elementar ‘subtrair’ implica a retirada da esfera de disponibilidade do titular, mediante deslocamento corpóreo do bem”.

Entretanto, a evolução tecnológica e o surgimento de novas formas de riqueza colocaram em xeque essa concepção. Com o desenvolvimento das transações eletrônicas, a noção de “coisa” passou a abarcar também bens imateriais, como valores creditados em contas digitais ou criptomoedas.

A jurisprudência brasileira, porém, ainda demonstra resistência em reconhecer plenamente o furto digital como modalidade típica autônoma, preferindo enquadrar tais condutas como fraude eletrônica (art. 171, §2º-A, do Código Penal) ou outros delitos cibernéticos. Isso revela a fragilidade conceitual e normativa do sistema penal frente às transformações digitais.

Como observa Luiz Regis Prado (2021, p. 519), “a concepção tradicional do furto, ancorada na materialidade do bem, encontra-se em evidente crise diante da desmaterialização dos valores e da virtualização do patrimônio”. Deste modo, demonstra que o conceito clássico de subtração já não é suficiente para abarcar as novas formas de lesão ao patrimônio surgidas no contexto tecnológico e digital.

1.4 O IMPACTO DAS TRANSFORMAÇÕES TECNOLÓGICAS NA CONFIGURAÇÃO DOS CRIMES PATRIMONIAIS

O Direito Penal, enquanto instrumento de controle social, acompanha a evolução das condutas humanas e das formas de agressão aos bens jurídicos tutelados. No campo dos crimes patrimoniais, essa evolução ocorre de modo progressivo, refletindo a transformação das relações econômicas e dos meios tecnológicos que sustentam as transações financeiras.

O primeiro passo dessa transformação é a mudança do próprio conceito de patrimônio. Tradicionalmente, o patrimônio estava limitado aos bens materiais, suscetíveis de apreensão física. Contudo, a economia digital trouxe a necessidade de reconhecer novos objetos de valor jurídico, como dados bancários, moedas virtuais, senhas e informações financeiras.

Segundo Cezar Roberto Bitencourt (2022, p. 145):

O conceito de patrimônio não pode mais ser entendido apenas sob a ótica material. A sociedade da informação impõe o reconhecimento de bens imateriais como expressão de riqueza, cuja violação produz efeitos tão graves quanto a subtração de bens corpóreos.

Em seguida, o segundo passo se dá no âmbito jurisprudencial e interpretativo. Antes de qualquer reforma legal, o Poder Judiciário procura adequar as categorias existentes às novas condutas. Assim, tribunais passaram a reconhecer que transferências eletrônicas indevidas, ainda que sem contato físico com o bem, configuram subtração patrimonial, já que há a perda de disponibilidade econômica pelo titular. Nesse ponto, Rogério Greco (2023, p. 215) observa “O direito penal não pode ser prisioneiro da materialidade dos bens. O patrimônio, como bem jurídico tutelado, é valor econômico suscetível de apropriação, independentemente de sua natureza física ou digital. ”

O terceiro passo ocorre no plano legislativo, com a criação de normas que incorporam essas novas formas de ofensa. No Brasil, esse processo foi gradual: iniciou-se com a Lei nº 12.737/2012 (Lei Carolina Dieckmann), que criminalizou a invasão de dispositivos informáticos, e evoluiu com a Lei nº 14.155/2021, que aumentou as penas de furto e estelionato cometidos por meios eletrônicos. Para Nucci (2022, p. 380):

O Direito Penal brasileiro tem se movido de forma reativa, adaptando-se à medida que os novos delitos ganham destaque na sociedade. É um processo que segue a lógica de resposta à demanda social, mais do que uma previsão técnica antecipada.

O quarto passo é a consolidação doutrinária e jurisprudencial. Após a criação da norma, doutrinadores e tribunais superiores reinterpretem os tipos penais para adequá-los à nova realidade. Assim, o conceito de “coisa alheia móvel”, antes restrito a objetos tangíveis, passa a ser compreendido como qualquer valor econômico transferível, inclusive ativos digitais. Conforme destaca Bitencourt (2022, p. 146):

A jurisprudência contemporânea amplia o alcance da tutela penal para abarcar novas formas de manifestação da riqueza, sem que isso implique violação ao princípio da legalidade, mas sim atualização interpretativa necessária à efetividade do tipo penal.

Por fim, o quinto passo consiste na efetivação prática da mudança, que depende da adequação dos órgãos de persecução penal. As autoridades policiais e o Ministério Público precisam dominar técnicas de investigação digital, rastreamento de transações eletrônicas e cooperação com instituições financeiras. Greco (2023, p. 217) resume esse processo afirmando que:

A efetividade da tutela penal patrimonial no ambiente digital exige não apenas reformas legislativas, mas também a capacitação técnica dos operadores do Direito, sob pena de a norma tornar-se letra morta diante da complexidade tecnológica das condutas.

Portanto, a transformação dos crimes patrimoniais pode ser compreendida em cinco etapas interdependentes: Ampliação do conceito de patrimônio (do material ao digital); Adaptação jurisprudencial inicial; Alteração legislativa reativa; Reinterpretação doutrinária e consolidação dos entendimentos; Implementação prática e capacitação técnica.

Essas etapas revelam que o Direito Penal evolui por meio da interação entre sociedade, doutrina, jurisprudência e legislação, e não apenas pela edição de novas leis. Como sintetiza Nucci (2022, p. 381):

A evolução dos crimes patrimoniais é um reflexo inevitável das transformações sociais e tecnológicas; o Direito, embora muitas vezes reativo, deve ser capaz de traduzir essa nova realidade em parâmetros normativos coerentes e eficazes.

Dessa forma, percebe-se que as transformações tecnológicas não apenas modificam as formas de ataque ao patrimônio, mas também redefinem os contornos dogmáticos do Direito Penal contemporâneo, exigindo um contínuo processo de adaptação interpretativa e legislativa.

2. O NOVO MUNDO DA ERA DIGITAL

2.1 A TRANSFORMAÇÃO DOS CRIMES PATRIMONIAIS NO AMBIENTE VIRTUAL

O autor Gabriel Rocha dos Santos afirma em seu artigo “O Direito e a Evolução Das Relações No Mundo Digital”, quando a sociedade e as comunicações perceberam a necessidade de outrem para que pudessem realizar suas tarefas e atividades, então iniciou-se o processo de evolução e transformação das relações.

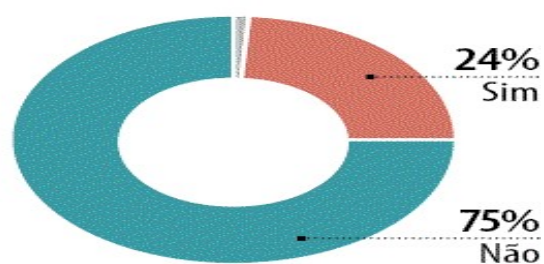
Em um minucioso processo, a internet tomou espaço no cotidiano dos indivíduos se tornando um meio essencial e não apenas agregado ao dia a dia. Ainda, Santos (2018), na mesma obra citada acima, apresenta os prós e os contras que podem ser analisados após a vinda da internet para o Brasil, conforme o que se segue:

Mas, assim como tantos conceitos melhoraram e foram atualizados, alguns pontos negativos surgiram. Alguns deles foram: a) o aumento da exposição individual involuntária; b) anonimato; c) facilidade para sofrer/cometer fraudes; d) vazamento de informações pessoais indesejadas; e) exposição a ataques hackers/terroristas; f) exposição da intimidade através de vazamento de fotos, vídeos, conversas e afins. (2018, p. 3).

Se por um lado a internet e o mundo da era digital pôde proporcionar aos cidadãos melhorias como acesso a informações diariamente por meio de jornais ou até mesmo páginas em redes sociais, ou ainda formas de se comunicar com pessoas que estão distantes, em contrapartida, é importante lembrar os pontos negativos que essa nova era trouxe para o país.

O autor, nas alíneas “c” e “d” acima, traz à tona uma preocupação: A facilidade para sofrer/cometer fraudes, além do vazamento de informações indesejadas. Deste modo, as pessoas puderam aperfeiçoar os meios pelos quais cometeriam os crimes, sendo que os delitos por meio virtual propiciaram de forma espontânea o aumento de vítimas de crimes cibernéticos, visto o natural impulsionador: o acesso à internet. Nesse mesmo sentido, a Agência Senado apresentou no mês de outubro de 2024 índice de aumento de golpes digitais atingindo a população brasileira. O órgão realizou um estudo direcionado a pessoas com mais de 16 anos, questionando os indivíduos sobre o assunto, e obtiveram o seguinte resultado, conforme gráfico a seguir:

Nos últimos 12 meses, você perdeu dinheiro por algum crime digital como clonagem de cartão, fraude na internet ou invasão de contas bancárias?



Fonte: Instituto de Pesquisa DataSenado:
www.senado.leg/datasenado – coleta de 5 a 28.6.2024

agência **senado**

A Agência acrescenta que, de acordo com a pesquisa, são mais de 40,85 milhões de pessoas que perderam dinheiro após serem vítimas de crimes cibernéticos no ano de 2024. Isso porque ainda não se sabe ao certo o prejuízo causado a estas pessoas, pois são crimes que variam entre grandes e pequenos prejuízos, que muitas vezes não são contabilizados pelas autoridades por não serem nem ao menos identificados.

O avanço da tecnologia trouxe a facilidade proporcionada aos criminosos para a prática dos crimes cibernéticos, o que aumentou exponencialmente o número de vítimas dos delitos ocorridos no ambiente virtual. Evidente o aumento mencionado anteriormente quando da análise de pesquisas realizadas no ano de 2023 e 2024, que comparam a quantidade de crimes cibernéticos ocorridos nestes anos e em anos anteriores. A Federação Brasileira de Bancos (FEBRABAN), apresentou pesquisa indicando que golpes como o 0800 ou da falsa Unidade de Resposta Audível (URA) tiveram aumento de 65,2% de 2021 para 2022, segundo o Anuário de Segurança Pública disponibilizado em 2023.

Os golpes digitais realizados por meio de ligações telefônicas fraudulentas têm se intensificado, assumindo formas cada vez mais elaboradas, como o golpe do 0800 e o da falsa Unidade de Resposta Audível (URA). No golpe do 0800, os criminosos entram em contato com a vítima se passando por instituições financeiras, utilizando números telefônicos que imitam os canais oficiais de atendimento, com o objetivo de obter dados pessoais, bancários e senhas de acesso, configurando conduta tipificada como fraude eletrônica nos termos do artigo 171, §2º, “a”, do Código Penal, incluído pela Lei nº 14.155/2021.

De modo semelhante, o golpe da falsa Unidade de Resposta Audível (URA) envolve a criação de sistemas automatizados de atendimento telefônico falsos, que

simulam o funcionamento de centrais legítimas, induzindo o usuário a fornecer informações sensíveis. Tais práticas violam não apenas a legislação penal, mas também os princípios previstos no Marco Civil da Internet (Lei nº 12.965/2014), especialmente os que tratam da proteção da privacidade, dos dados pessoais e da segurança das comunicações.

Segundo Silvana Drumond Monteiro (2007) “Os avanços das tecnologias digitais prosseguem à grande velocidade e, atualmente, há uma utilização massiva dessas novas técnicas em um ambiente denominado “Ciberespaço”. E ainda nesse sentido, tem-se o conceito de ciberespaço, de conforme a mesma autora (2007, p.1):

[...] grande máquina abstrata, porque semiótica, mas também social, onde se realizam não somente trocas simbólicas, mas transações econômicas, comerciais, novas práticas comunicacionais, relações sociais, afetivas e, sobretudo, novos agenciamentos cognitivos. É um universo virtual, plástico, fluido, carregado de devires.

Nesse toar, ainda Monteiro (2007) traz o seguinte entendimento sobre o conceito de ciberespaço:

O ciberespaço é definido como um mundo virtual porque está presente em potência, é um espaço desterritorializante. Esse mundo não é palpável, mas existe de outra forma, outra realidade. O ciberespaço existe em um local indefinido, desconhecido, cheio de devires e possibilidades. Não podemos, sequer, afirmar que o ciberespaço está presente nos computadores, tampouco nas redes, afinal, onde fica o ciberespaço? Para onde vai todo esse “mundo” quando desligamos os nossos computadores? É esse caráter fluido do ciberespaço que o torna virtual.

Após o surgimento do ciberespaço e sua difusão na realidade dos indivíduos brasileiros, passou-se a considerar a transformação dos crimes patrimoniais no ambiente virtual e a natural migração para este, visto que o ciberespaço proporciona ao crime mais possibilidades do que se possa imaginar, denominando-se desta forma, o cibercrime, instituto criado para explicar os crimes cometidos dentro do ambiente virtual.

Conforme esclarece Abreu de Sá, Costa, Silva e Negreiro (2025) sobre os crimes cibernéticos, conhecidos como cibercrimes, são delitos cometidos no ambiente virtual utilizando dispositivos que estejam conectados à internet. O roubo de dados até fraudes financeiras e disseminação de conteúdos ilegais são exemplos do cometimento dos crimes cibernéticos, e devido ao avanço tecnológico se tornaram um grave problema para a população brasileira e a legislação penal, que precisou passar por mudanças em leis específicas. Conforme os mesmos autores citados anteriormente mencionam:

No Brasil, os cibercrimes estão tipificados em leis específicas, como o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, que criminaliza a invasão de dispositivos informáticos. Além disso, outros crimes do Código Penal Brasileiro, como estelionato (art. 171), foram adaptados para contemplar modalidades digitais, especialmente após a promulgação da Lei nº 14.155/2021, que agravou penas para crimes cometidos pela internet.

Foi necessário que o Código Penal Brasileiro (CPB) sofresse alterações como forma de abranger o novo surgimento dos crimes praticados através da internet, e possibilitar a punibilidade destes.

2.1.1 A teoria das Atividades Rotineiras

A Teoria das Atividades Rotineiras é uma teoria que, segundo Camila Fernandes Bicalho (2024), foi inicialmente desenvolvida por Lawrence E. Cohen e Marcus Felson em 1979, nos Estados Unidos, e é também conhecida como “Triângulo do Crime”. Essa teoria utiliza-se de três elementos, tendo eles como os principais, para que, de forma simultânea possam convergir no tempo e no espaço, sendo eles: (i) um potencial ofensor motivado, disposto a cometer um possível crime; (ii) um alvo disponível, ou seja, uma pessoa ou objeto a ser atacado; e (iii) a ausência de um guardião capaz de proteger o alvo. Formando desta forma, o triângulo de requisitos para ocorrência da ação.

Segundo esta teoria, o foco principal deixa de ser o autor dos crimes, e passa a ser um estudo de como as vítimas se comportam no espaço-tempo para tornarem adequada a possibilidade da ação predatória. Deste modo, o autor explica que são analisados diversos fatores para que talvez respostas sejam encontradas sobre o tema. O local de moradia do criminoso, a idade da vítima, o horário em que o crime é cometido, são exemplos de fatores que estão associados a frequência dos crimes.

Importante destacar ainda o que diz os autores Cláudio Beato, Betânia Peixoto e Mônica Andrade (2004, p. 76) sobre o assunto, quando ainda nesse sentido afirmam que entre os principais fatores de risco de vitimização dos indivíduos incluem: exposição, proximidade com o agressor, capacidade de proteção, atratividade das vítimas e a natureza dos crimes. Observa-se que é uma análise minuciosa sobre como o comportamento da vítima pode ser um fator importante a analisar quando do

aumento de crimes no ambiente virtual.

Desta forma, entende-se que, em que pese a Teoria das Atividades Rotineiras ter sido criada para analisar a perspectiva dos fatores influenciados pela vítima para o acontecimento dos crimes, é notório o seu cabimento no ambiente cibernético, quanto aos crimes ocorridos no ambiente virtual. Isso porque se repete, dentro deste ambiente, as características dos fatores analisados na teoria, sendo eles (i) indivíduos motivados a cometer crimes, (ii) alvos disponíveis para serem atacados e (iii) uma ausência de guardiões capazes de proteger esses alvos.

2.2 A ATUAÇÃO DOS CRIMINOSOS NAS PLATAFORMAS DIGITAIS

Segundo o que Abreu de Sá, Costa, Silva e Negreiro (2025) esclarece, o estelionato virtual, o roubo de identidade, ataques de ransomware, phishing, hacking de contas bancárias e a exploração sexual online estão entre os crimes cibernéticos mais comuns. Há um aprimoramento frequente nos métodos utilizados pelos criminosos, que possuem à sua disposição ferramentas de alto nível tecnológico disposto por meio da internet.

Nesse toar, Oliveira (2025) afirma que “É de se imaginar que a existência de um local “seguro” onde é possível trafegar de forma anônima e de difícil localização se tornou atrativo para práticas criminosas”. A frase do artigo “Criminalidade Digital: Desafios Legais no enfrentamento”, permite pressupor a facilidade em cometer crimes utilizando apenas um dispositivo com internet. Ainda, segundo o autor, “Os impactos de tais infrações são vastos e, por muita das vezes, irreversíveis na vida da vítima, podendo causar danos econômicos, psicológicos e sociais”.

Os crimes cibernéticos envolvem um cenário ideal aos seus praticantes, prevalecendo a impunidade e o anonimato na execução de tais atos. Com a dificuldade na identificação e rastreamento de usuários que utilizam a internet, o autor do artigo referido acima destaca os principais crimes envoltos a essa problemática, sendo visados entre os crimes mais preocupantes neste cenário, o ato de bloquear por completo o acesso a dados ou sistemas operacionais vigentes em uma empresa, afim de propor uma quantia considerável de dinheiro ou, em muitos casos, de criptomoedas (dificuldade no rastreamento) para devolver o acesso ao seu verdadeiro dono, tal crime é chamado de “Ransomware”.

2.3 AS VULNERABILIDADES DOS SISTEMAS BANCÁRIOS DIGITAIS E O AUMENTO DOS FURTOS ELETRÔNICOS

As vulnerabilidades dos sistemas bancários digitais são múltiplas e, como destacam Sanches e outros doutrinadores penalistas, esses sistemas frequentemente apresentam falhas de segurança que podem ser exploradas por criminosos para a prática de ilícitos.

Segundo Sanches (2018), a "dependência crescente de tecnologias digitais e a implementação de sistemas bancários virtuais criaram novas formas de delitos, com especial destaque para os furtos eletrônicos, que exploram brechas de segurança no ambiente online". Essa afirmação está diretamente relacionada ao aumento do número de fraudes e furtos em contas bancárias, que resultam em danos financeiros significativos tanto para as instituições financeiras quanto para os próprios clientes.

Em sua obra, Sanches (2018) também pontua que a insegurança dos sistemas bancários digitais não está limitada apenas a falhas técnicas. Muitas vezes, o comportamento negligente por parte dos próprios usuários, como o uso de senhas fracas e a falta de precauções em ambientes online, contribui para o aumento dos furtos eletrônicos. A vulnerabilidade dos sistemas bancários é, assim, um fenômeno multifacetado, no qual fatores tecnológicos e comportamentais se combinam para criar um ambiente propício à ação de criminosos.

A doutrinadora Ana Silva (2020) também ressalta que a evolução dos métodos de fraude eletrônica tem sido uma resposta direta à inadequação de certos mecanismos de proteção nos sistemas bancários. Para ela, a ausência de protocolos mais rigorosos, como a autenticação multifatorial e a criptografia avançada, configura um terreno fértil para os fraudadores. Silva (2020) argumenta que, embora existam diversas medidas de segurança, a adaptação dos criminosos a essas tecnologias é extremamente rápida, o que cria um ciclo contínuo de vulnerabilidades e inovações no campo da criminalidade.

A crescente sofisticação das técnicas de fraudes digitais tem levado os bancos a investir cada vez mais em tecnologias de segurança, como a biometria digital, sistemas de monitoramento em tempo real e inteligência artificial para detecção de atividades suspeitas. Contudo, conforme alertam Sanches e outros estudiosos,

"embora essas tecnologias tenham sido um avanço significativo, a evolução constante dos métodos fraudulentos exige uma atualização contínua das estratégias de proteção" (Sanches, 2018).

O aumento dos furtos eletrônicos, agravado pela vulnerabilidade dos sistemas bancários digitais, revela a necessidade urgente de um diálogo entre a tecnologia, o direito penal e as instituições financeiras para a criação de mecanismos mais eficazes de prevenção e combate aos crimes cibernéticos. A atuação proativa dos bancos, juntamente com a atualização da legislação penal, pode ser a chave para reduzir a incidência desses delitos.

3. A FRAGILIDADE LEGISLATIVA E OS DESAFIOS JURÍDICOS

3.1 A LEI Nº 14.155/2021 E SUAS LIMITAÇÕES NA REPRESSÃO AOS CRIMES DIGITAIS

A consolidação dos bancos digitais e das transações financeiras por meios eletrônicos transformou profundamente a dinâmica das relações econômicas e, consequentemente, a configuração dos delitos contra o patrimônio. A criminalidade cibernética evolui em ritmo acelerado, e o ordenamento jurídico brasileiro tem se mostrado insuficiente para oferecer respostas proporcionais à complexidade desses novos delitos. Nesse contexto, a promulgação da Lei nº 14.155, de 27 de maio de 2021, representou um avanço legislativo ao atualizar o Código Penal e o Código de Processo Penal para lidar com crimes cometidos por meios eletrônicos. Contudo, apesar de seu mérito, a referida lei evidencia a persistência de lacunas normativas e desafios jurídicos que comprometem a repressão efetiva aos crimes digitais, sobretudo aos furtos e fraudes praticados em ambientes bancários virtuais.

A Lei nº 14.155/2021 alterou dispositivos do Código Penal, agravando as penas para o crime de invasão de dispositivo informático (art. 154-A), criando qualificadoras para o furto (art. 155) e o estelionato (art. 171) quando praticados por meio eletrônico ou utilizando informações fornecidas pela própria vítima. Também introduziu ajustes no Código de Processo Penal quanto à competência para julgamento de delitos praticados por meios digitais. A intenção do legislador foi clara: atualizar o sistema penal frente ao avanço tecnológico e à crescente incidência de crimes cometidos em ambiente virtual. Entretanto, a mera atualização textual da norma não foi acompanhada de uma estrutura processual e probatória capaz de garantir a efetiva aplicação das novas disposições legais.

Como observa Sanches (2024, p. 60), em sua obra:

A introdução de qualificadoras para crimes tradicionais como furto e estelionato, quando cometidos por meio eletrônico, representa um esforço legislativo de adaptação, mas que não é suficiente se não houver uma redefinição do próprio conceito de 'bem jurídico' e uma definição precisa dos novos tipos de crimes". O autor destaca que a adaptação do Código Penal à realidade digital exige mais do que um simples acréscimo de qualificadoras; é necessário revisar a própria concepção de patrimônio e de "coisa móvel" no contexto do ambiente virtual.

A fragilidade da lei começa por sua imprecisão conceitual. Termos como “dispositivo informático”, “meio eletrônico” ou “uso de informações fornecidas pela vítima” não possuem definição técnica precisa, abrindo espaço para interpretações divergentes e insegurança jurídica. Sanches (2024, p. 62) já havia alertado que

A falta de clareza nos conceitos e a definição vaga de ‘meio eletrônico’ e ‘dispositivo informático’ cria um cenário de insegurança, em que a interpretação judicial e a aplicação da norma ficam a cargo da discricionariedade dos tribunais, o que pode levar a soluções inconsistentes e injustas.

Essa imprecisão resulta em sobreposição de tipos penais, gerando dúvidas sobre o enquadramento de condutas que, na prática, podem se confundir entre furto qualificado, estelionato eletrônico ou invasão de dispositivo informático. Como coloca Sanches (2024, p. 64), “a imprecisão normativa impede a identificação de um tipo penal claro, o que favorece a incerteza jurídica e a multiplicidade de soluções judiciais para um mesmo comportamento criminoso”.

Tal ambiguidade prejudica a uniformidade da jurisprudência e dificulta a persecução penal, pois cada caso acaba sendo interpretado de maneira distinta pelos tribunais. Em sua análise, Sanches (2024, p. 65) complementa que

A incerteza que permeia a definição e a aplicação de tipos penais digitais reflete a necessidade urgente de uma revisão mais profunda do direito penal, que considere não só a tipificação dos novos delitos, mas também a criação de uma estrutura probatória adaptada às peculiaridades do ambiente digital.

Além disso, a lei foca essencialmente no aumento de penas, mas não enfrenta as questões estruturais que permeiam a criminalidade digital. O aumento da sanção penal não tem se mostrado um mecanismo eficaz de prevenção, especialmente quando a probabilidade de punição é baixa em razão da complexidade probatória. Os crimes digitais, por sua natureza, deixam rastros técnicos que exigem conhecimento especializado para sua coleta e preservação. A falta de protocolos claros sobre cadeia de custódia e a escassez de peritos capacitados nas comarcas brasileiras tornam a instrução processual vulnerável e frequentemente ineficaz. Essa deficiência é agravada pela ausência de legislação específica que regule a produção e a valoração da prova digital no processo penal, o que pode comprometer o devido processo legal e a ampla defesa.

Outro aspecto crítico é a questão da cooperação internacional. Muitos delitos cibernéticos envolvem servidores, agentes ou intermediários localizados fora do território nacional, exigindo medidas de cooperação jurídica que são lentas e

burocráticas. A Lei nº 14.155/2021 não estabeleceu instrumentos mais ágeis para viabilizar o intercâmbio de informações com provedores estrangeiros, o que limita a atuação das autoridades brasileiras. Assim, enquanto a tecnologia avança em tempo real, o sistema penal continua preso a mecanismos de cooperação que demoram meses ou até anos para produzir resultados.

Os tribunais têm enfrentado desafios práticos decorrentes dessas lacunas. O Superior Tribunal de Justiça, em recentes julgados, vem reconhecendo a dificuldade de responsabilização penal e civil em fraudes praticadas via aplicativos e bancos digitais. Em diversos casos, a Corte entendeu que a instituição financeira não pode ser automaticamente responsabilizada quando a fraude decorre do fornecimento voluntário de dados pela vítima, como senhas ou códigos de acesso (STJ, AgInt no AREsp 2.201.694/SP).

Por outro lado, também há decisões que afirmam a responsabilidade objetiva dos bancos em razão do risco inerente à atividade econômica, especialmente quando há falhas de segurança nos sistemas (STJ, REsp 1.899.383/DF). Essa oscilação jurisprudencial evidencia a falta de uniformidade interpretativa e demonstra como a ausência de regulamentação específica contribui para decisões contraditórias.

A fragilidade legislativa se manifesta ainda na ausência de mecanismos eficazes de prevenção e responsabilização administrativa. A lei não prevê obrigações específicas para as plataformas digitais e instituições financeiras quanto à adoção de padrões mínimos de segurança cibernética. Essa omissão transfere para o usuário final o ônus da autoproteção, contrariando princípios como o da vulnerabilidade do consumidor e o da confiança legítima. Doutrinadores como Nucci (2022) e Greco (2023) alertam que o direito penal, isoladamente, não consegue conter a criminalidade digital se não estiver integrado a políticas públicas de segurança da informação e à regulação administrativa do setor financeiro digital.

Do ponto de vista processual, há igualmente obstáculos à efetividade das investigações. A ausência de varas especializadas em crimes cibernéticos e a falta de uniformização de procedimentos para busca e apreensão de dados eletrônicos dificultam a persecução penal. Medidas cautelares como o bloqueio de valores desviados de contas digitais ou a quebra de sigilo telemático ainda dependem de instrumentos genéricos do Código de Processo Penal, sem diretrizes claras sobre prazos, limites técnicos e preservação de dados. Essa lacuna torna as investigações

lentas e ineficientes, muitas vezes inviabilizando a recuperação de valores subtraídos das vítimas.

A repressão penal aos furtos e fraudes em bancos digitais, portanto, encontra-se presa entre dois polos de ineficácia: de um lado, um ordenamento que tipifica a conduta, mas não fornece meios técnicos para sua apuração; de outro, um sistema financeiro digital que opera em velocidade muito superior à capacidade de resposta das instituições de controle. O resultado é a sensação generalizada de impunidade, que fragiliza a confiança do cidadão nas instituições e mina o próprio propósito do direito penal enquanto instrumento de tutela dos bens jurídicos essenciais.

Em síntese, a Lei nº 14.155/2021 representa um avanço formal, mas não material. Sua eficácia depende da construção de um arcabouço complementar que envolva o aprimoramento da prova digital, a criação de varas e delegacias especializadas, o fortalecimento da cooperação internacional e a regulamentação da responsabilidade das plataformas financeiras. Sem essas medidas, a legislação continuará sendo um instrumento simbólico de combate à criminalidade digital, incapaz de produzir resultados concretos. A modernização do direito penal, portanto, não pode se limitar à atualização dos tipos penais; deve também contemplar a criação de instrumentos processuais e técnicos compatíveis com a complexidade do mundo digital, sob pena de perpetuar a fragilidade legislativa diante da sofisticação crescente dos crimes eletrônicos.

3.2 A AUSÊNCIA DE TIPIIFICAÇÃO ESPECÍFICA PARA OS FURTOS ELETRÔNICOS

Embora o Código Penal brasileiro, em seu artigo 155, preveja o crime de furto, sua estrutura normativa permanece voltada a condutas materiais e tangíveis, próprias de uma realidade pré-digital. O texto legal exige, como elemento objetivo, a “subtração de coisa alheia móvel”, o que pressupõe a transferência física da posse ou detenção de um bem. No entanto, nas operações eletrônicas, a subtração patrimonial ocorre de forma intangível, por meio da manipulação de dados, senhas, sistemas bancários ou transações automatizadas. Essa desconexão entre o tipo penal e a realidade tecnológica evidencia uma lacuna interpretativa que compromete a aplicação efetiva da norma penal.

A Lei nº 14.155/2021 buscou, em certa medida, suprir essa deficiência ao introduzir o §4º-B ao artigo 155 do Código Penal, qualificando o furto praticado mediante fraude eletrônica. Todavia, tal dispositivo não cria um novo tipo penal autônomo, mas apenas agrava a pena quando a subtração é cometida por meio eletrônico ou com o uso de informações fornecidas pela vítima. O legislador optou por uma solução intermediária, mantendo a tipificação tradicional do furto e apenas reconhecendo a modalidade eletrônica como qualificadora. Essa escolha, embora pragmática, não resolve os dilemas conceituais que envolvem a materialidade do delito e a natureza do bem jurídico subtraído no ambiente virtual.

A ausência de um tipo penal específico para o furto eletrônico cria dificuldades tanto para a persecução penal quanto para a interpretação judicial. Sanches (2024, p. 60) afirma o que se segue sobre o tema:

A crescente utilização de meios digitais para a prática de crimes exige uma reinterpretação das figuras típicas já previstas no Código Penal, pois a natureza virtual do crime demanda uma análise mais detalhada das novas formas de materialização do dano.

A jurisprudência ainda oscila entre enquadrar tais condutas como furto qualificado, estelionato eletrônico ou até mesmo invasão de dispositivo informático, dependendo da técnica utilizada pelo agente e do grau de participação da vítima. Essa falta de uniformidade gera insegurança jurídica e abre espaço para a impunidade. Doutrinadores como Bitencourt (2022) e Greco (2023) sustentam que, diante da crescente virtualização da economia, o direito penal precisa reformular sua concepção de “coisa móvel”, reconhecendo que o patrimônio digital é tão suscetível de lesão quanto o patrimônio físico.

A insuficiência do Código Penal, não decorre apenas de sua antiguidade, mas da ausência de atualização conceitual compatível com as novas formas de manifestação do patrimônio. A doutrina moderna já reconhece o valor econômico dos dados, senhas e informações digitais, que podem ser apropriados, transferidos ou comercializados. Ignorar essa dimensão imaterial do patrimônio equivale a negar proteção penal a uma parcela significativa das riquezas contemporâneas. Assim, a falta de tipificação específica dos furtos eletrônicos representa não apenas uma lacuna técnica, mas também um problema de política criminal que compromete a efetividade do sistema de justiça.

3.3 A NECESSIDADE DE REFORMA LEGISLATIVA DIANTE DA EVOLUÇÃO TECNOLÓGICA

A evolução tecnológica impõe uma dinâmica de constante atualização ao ordenamento jurídico, especialmente ao direito penal, cuja função é proteger bens jurídicos fundamentais frente a novas formas de violação. O Código Penal de 1940 foi elaborado em um contexto social, econômico e tecnológico completamente distinto do atual, no qual as infrações eram predominantemente materiais e localizadas. A digitalização das relações humanas e financeiras, no entanto, alterou profundamente essa lógica, exigindo do legislador um esforço de adaptação que, até o momento, tem ocorrido de maneira fragmentada e reativa.

A edição da Lei nº 14.155/2021 é exemplo de uma resposta legislativa pontual a um fenômeno amplo. Embora tenha representado um avanço, sua abrangência é limitada e não constitui uma reforma estrutural do sistema penal digital. Faltam instrumentos normativos que contemplem as especificidades das novas tecnologias, como o uso de inteligência artificial, criptomoedas, sistemas automatizados de pagamento e transações em blockchain. Os sistemas automatizados de pagamento consistem em estruturas digitais capazes de processar e liquidar transferências de valores com mínima intervenção humana, permitindo maior agilidade, redução de erros e menor custo operacional. Quando integrados à tecnologia blockchain, sendo um registro distribuído, imutável e auditável, esses sistemas possibilitam a realização de transações de forma segura, transparente e descentralizada. Além disso, por meio de *smart contracts* (contrato inteligente), é possível automatizar etapas do pagamento, que são executados automaticamente quando determinadas condições previamente programadas são cumpridas.

Tais meios têm permitido a prática de delitos complexos, que escapam ao alcance dos tipos penais tradicionais e desafiam a capacidade investigativa do Estado.

Doutrinadores como Luiz Flávio Gomes e Guilherme de Souza Nucci já apontavam que o direito penal brasileiro sofre de um “déficit de modernização legislativa”, reagindo tardiamente às transformações sociais. A criminalidade digital, diferentemente da criminalidade convencional, opera de forma descentralizada, transnacional e com elevado grau de anonimato. Essa realidade exige não apenas novas figuras típicas, mas também uma reformulação do processo penal, com

procedimentos próprios para coleta, preservação e análise de provas digitais, bem como cooperação jurídica internacional mais eficiente.

Além da necessidade de novas tipificações, é imprescindível que a legislação avance na definição de responsabilidades compartilhadas entre os agentes econômicos envolvidos. Bancos digitais, plataformas de pagamento e provedores de serviços de internet devem ser juridicamente compelidos a adotar padrões mínimos de segurança e de prevenção a fraudes. A ausência de previsão expressa nesse sentido mantém a vítima em posição de vulnerabilidade e sobrecarrega o sistema penal, que passa a ser o único instrumento de tutela, sem apoio da esfera administrativa ou regulatória.

Há projetos de lei que buscam a alteração da lei de furto de forma indireta, como por exemplo o Projeto de Lei 4658/24, do deputado Paulo Litro (PSD-PR), que aumenta a pena para crimes cometidos com o uso da internet. O texto altera o Código Penal e está em análise na Câmara dos Deputados até o presente momento, segundo a Agência Câmara de Notícias. A mudança seria bem-vinda para os casos em que há carência de legislação rigorosa e específica.

Ainda nesse sentido, o Projeto de Lei Complementar nº 77, de 2023, propõe a criação do Cadastro Digital Certificado (CDC) para identificar correntistas de contas de depósito abertas por meio eletrônico. A proposta estabelece que todas as instituições financeiras, incluindo Sociedades de Crédito Direto e Sociedades de Empréstimo entre Pessoas, devem adotar esse cadastro, que inclui, entre outras coisas, dados pessoais, fotos, impressões digitais e documentos de identificação.

De acordo com o site do Senado, o projeto de lei em questão pode acarretar diversas consequências para diferentes setores. As instituições financeiras, por exemplo, terão que implementar e gerenciar o Cadastro de Contas Digitais (CDC), o que, por um lado, pode aumentar a segurança e reduzir fraudes, mas, por outro, pode gerar custos operacionais adicionais. Para os correntistas, a medida pode fortalecer a proteção das contas digitais, mas também exigirá mais tempo e esforço para manter os dados atualizados e fornecer as informações solicitadas. As entidades certificadoras, como serventias extrajudiciais e instituições autorizadas pela ICP-Brasil, podem encontrar uma nova oportunidade de serviços, gerando uma fonte adicional de receita. Por fim, o sistema financeiro como um todo pode se beneficiar com o aumento da confiança nas contas digitais, o que pode resultar em um ambiente

mais seguro e transparente (SENADO, 2025).

É necessário repensar o papel do direito penal dentro de um ecossistema digital complexo, integrando-o a políticas públicas de segurança da informação, proteção de dados e educação digital. A atualização normativa deve refletir a nova realidade social e tecnológica, garantindo que o direito penal cumpra sua função de prevenção e repressão eficaz, sem se tornar obsoleto diante das rápidas transformações da era digital.

3.3.1 A Responsabilidade dos Bancos

A doutrina e a jurisprudência brasileiras vêm consolidando o entendimento de que as instituições financeiras respondem objetivamente pelos danos decorrentes de falhas na segurança de seus sistemas, sobretudo quando ocorrem fraudes digitais. Essa responsabilização encontra respaldo na teoria do risco da atividade e no art. 14 do Código de Defesa do Consumidor (CDC), que impõe ao fornecedor o dever de garantir a segurança dos serviços prestados.

Segundo a Ordem dos Advogados do Brasil – Seção Rio de Janeiro (2023, p. 3):

O cenário atual de constante avanço tecnológico trouxe novos riscos, o que é perceptível através das inúmeras notícias de golpes e fraudes digitais nos serviços financeiros. Em que pese o microssistema consumerista estabelecer a responsabilidade civil objetiva desses fornecedores, é imprescindível o fortalecimento dos mecanismos de segurança, a fim de evitar prejuízos aos consumidores.

O Tribunal de Justiça do Distrito Federal e Territórios (2023, p. 2) reforça o mesmo entendimento:

A atividade desenvolvida pelas instituições bancárias é naturalmente de risco, pois envolve disponibilidade e liquidez de recursos financeiros. Por isso, às instituições bancárias se aplica a responsabilidade civil objetiva, em virtude do risco da atividade exercida.

A jurisprudência do Superior Tribunal de Justiça consolida essa orientação, ao editar a Súmula nº 479, que dispõe: “As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias” (BRASIL, STJ, 2012).

Essas posições doutrinárias e jurisprudenciais demonstram que os bancos têm o dever de atuar não apenas como prestadores de serviços financeiros, mas como

garantidores da segurança digital das operações realizadas em seus sistemas.

Apesar da tendência jurisprudencial pela responsabilização objetiva, há limites a essa responsabilidade, sobretudo quando configurado o fortuito externo ou a culpa exclusiva da vítima.

Conforme acórdão do TJDF (2023, p. 4) “Em se tratando de atividade cujo risco lhe é inerente, o prestador do serviço não pode se eximir da responsabilidade em decorrência de fortuito interno. ”

Entretanto, o mesmo Tribunal ressalta que, em determinadas situações, a responsabilidade pode ser afastada:

Em que pese tenha sido vítima de um golpe, a autora foi a única responsável pela eclosão do resultado danoso, não se configurando falha na prestação dos serviços bancários, mas tão somente culpa exclusiva da correntista” (TJDF, 2023, p. 6).

Portanto, embora o regime de responsabilidade civil objetiva imponha rigor aos bancos, é necessário comprovar a falha do serviço, o que reforça a complexidade das disputas envolvendo crimes digitais.

Esse panorama evidencia a lacuna normativa tratada anteriormente: a inexistência de regulamentação específica sobre os deveres de segurança digital das instituições financeiras. Embora a Lei nº 14.155/2021 tenha alterado o Código Penal e o Código de Processo Penal para prever crimes cometidos por meio eletrônico, ainda não há previsão detalhada sobre a responsabilidade penal ou administrativa dos bancos em casos de falhas sistêmicas.

Essa ausência de previsão específica demonstra, conforme os doutrinadores citados, a necessidade de uma mudança legislativa que trate a segurança digital bancária como dever legal expresso, impondo às instituições financeiras padrões mínimos de proteção e auditoria tecnológica.

Assim, a fragilidade legislativa brasileira diante dos crimes digitais reflete-se também no campo civil, uma vez que a responsabilização dos bancos se apoia em normas gerais e interpretações jurisprudenciais, o que contribui para a insegurança jurídica e a divergência de decisões entre os tribunais.

3.4 A INSEGURANÇA JURÍDICA

A falta de uniformidade legislativa e a insuficiência conceitual do Código Penal

resultam em um cenário de insegurança jurídica no tratamento dos crimes digitais. O magistrado, ao se deparar com condutas praticadas por meios eletrônicos, frequentemente precisa adaptar tipos penais tradicionais a realidades tecnológicas inéditas. Essa prática interpretativa, embora necessária, compromete o princípio da legalidade estrita previsto no artigo 1º do Código Penal, segundo o qual não há crime sem lei anterior que o defina. Ao ampliar excessivamente o alcance dos tipos penais, o intérprete acaba invadindo a competência do legislador e gerando instabilidade jurisprudencial.

A insegurança jurídica manifesta-se de forma acentuada nos crimes contra o patrimônio cometido em ambiente digital. As decisões judiciais variam conforme a interpretação adotada: em alguns casos, a subtração eletrônica de valores é tratada como furto; em outros, como estelionato; e, em certas situações, como mera fraude eletrônica ou crime de invasão de dispositivo informático. Essa oscilação compromete a coerência do sistema penal e dificulta a atuação dos órgãos de persecução, que não dispõem de diretrizes claras sobre o enquadramento das condutas.

O Superior Tribunal de Justiça tem reconhecido tais dificuldades em diversos precedentes, destacando a necessidade de uma atualização legislativa mais abrangente. No julgamento do AgRg no REsp 1.972.561/PR, a Corte observou que a aplicação dos tipos penais tradicionais a condutas digitais requer cautela, para evitar analogias *in malam* partem e violações ao princípio da taxatividade. A insegurança é agravada pela ausência de uniformização entre as esferas cível e penal: enquanto na esfera cível prevalece a responsabilidade objetiva das instituições financeiras por falhas de segurança, na esfera penal muitas vezes não se identifica o nexo causal necessário para imputar dolo ou culpa aos agentes envolvidos.

Essa falta de harmonia entre os ramos do direito compromete a efetividade da tutela jurídica. O cidadão vê-se desprotegido, pois a legislação penal não consegue acompanhar a velocidade e a sofisticação das novas modalidades criminosas. Além disso, a escassez de especialização técnica entre os operadores do direito agrava o problema, gerando decisões inconsistentes e investigações ineficientes. Como observa Silva Sánchez (2020), o direito penal contemporâneo enfrenta o desafio de equilibrar o princípio da legalidade com a necessidade de adaptação às transformações tecnológicas, evitando tanto a obsolescência normativa quanto o arbítrio judicial.

A insegurança jurídica derivada da ausência de tipificação clara dos crimes digitais compromete a credibilidade do sistema penal e reforça a sensação de impunidade. A superação desse quadro exige não apenas reformas legislativas, mas também o fortalecimento da formação técnica de magistrados, promotores e peritos, além da criação de instâncias especializadas para análise e julgamento de delitos cibernéticos. Somente assim o direito penal brasileiro poderá responder de forma segura, coerente e eficaz aos desafios impostos pela era digital.

CONCLUSÃO

O presente trabalho buscou analisar a fragilidade da legislação penal brasileira no enfrentamento dos crimes de furto praticados no ambiente dos bancos digitais, por meio de uma investigação sobre as lacunas normativas e a ausência de tipificação específica que acompanhe a evolução tecnológica. A pesquisa, desenvolvida com base em levantamento bibliográfico e documental, confirmou a hipótese inicial de que o ordenamento jurídico pátrio se encontra em crise conceitual e normativa diante da desmaterialização do patrimônio.

No primeiro capítulo, demonstrou-se que o conceito clássico de furto, previsto no artigo 155 do Código Penal de 1940, está intrinsecamente ligado à materialidade da "coisa alheia móvel", o que gera dificuldades de enquadramento para as apropriações de ativos virtuais, dados e valores que não se enquadram na concepção corpórea tradicional. Essa limitação é um reflexo do descompasso histórico entre o Direito Penal e o acelerado avanço das tecnologias digitais.

A análise do "Novo Mundo da Era Digital" evidenciou a profunda transformação dos crimes patrimoniais, nos quais o ciberespaço se torna um ambiente propício para a ação criminosa, prevalecendo, muitas vezes, o anonimato e a dificuldade de rastreamento. A aplicação da Teoria das Atividades Rotineiras ao contexto cibernético reforçou o entendimento de que a convergência de ofensores motivados, alvos disponíveis (vulnerabilidades dos sistemas bancários) e a ausência de guardiões adequados propiciam o aumento exponencial de vítimas.

Por fim, o estudo da "Fragilidade Legislativa e os Desafios Jurídicos" apontou que a Lei nº 14.155/2021, embora relevante no combate aos crimes digitais, revelou-se insuficiente para resolver a problemática do furto em bancos digitais. Isso ocorre porque a tipificação da fraude eletrônica (art. 171, §2º-A, CP) não abarca, com perfeição técnica, a conduta do furto realizado sem a participação da vítima (como nos casos de invasão de sistemas), evidenciando a necessidade de uma tipificação autônoma. A omissão do legislador em adaptar o tipo penal de furto à realidade virtual tem gerado insegurança jurídica e disparidade de decisões judiciais no enquadramento desses delitos.

Conclui-se, portanto, que a tutela do patrimônio digital exige uma urgente reforma legislativa que promova a atualização do Direito Penal. A sugestão é a criação

de um tipo penal específico para o furto eletrônico, que considere a desmaterialização do objeto e as particularidades do *modus operandi* no ambiente virtual, assegurando maior eficácia na repressão e, conseqüentemente, maior segurança jurídica e proteção aos cidadãos brasileiros.

REFERÊNCIAS

ÂNGELO, Luíza Alice Torres. **Crimes cibernéticos: as limitações da resposta estatal à criminalidade informática**. 2017.

BICALHO, Camila Fernandes et al. **Crimes patrimoniais na era digital: contribuições da teoria das atividades rotineiras**. 2024.

BITENCOURT, Cezar Roberto. **Tratado de Direito Penal: parte especial – crimes contra o patrimônio**. 22. ed. São Paulo: Saraiva, 2022.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. **Código Penal**. Diário Oficial da União, Brasília, 31 dez. 1940.

BRASIL. Decreto-Lei nº 3.689, de 3 de outubro de 1941. **Código de Processo Penal**. Diário Oficial da União, Rio de Janeiro, 13 out. 1941.

BRASIL. Lei nº 14.155, de 27 de maio de 2021. **Altera o Código Penal e o Código de Processo Penal para prever crimes cometidos por meio eletrônico**. Diário Oficial da União, Brasília, 28 maio 2021.

BRASIL. Superior Tribunal de Justiça (STJ). **Súmula nº 479. As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias**. Brasília, DF, 2012. Disponível em: <https://www.tjdft.jus.br/consultas/jurisprudencia/jurisprudencia-em-temas/jurisprudencia-em-detahes/responsabilidade-civil/fraude-bancaria-2013-responsabilidade-objetiva-do-banco-2013-fortuito-interno>. Acesso em: 29 out. 2025.

BRASIL. Tribunal de Justiça do Distrito Federal e dos Territórios (TJDFT). **Responsabilidade civil das instituições financeiras nas fraudes eletrônicas**. Brasília, DF, 2023. Disponível em: <https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/artigos-discursos-e-entrevistas/artigos/2023/responsabilidade-civil-das-instituicoes-financeiras-nas-fraudes-eletronicas>. Acesso em: 29 out. 2025.

CÂMARA DOS DEPUTADOS. **Projeto aumenta pena para crimes praticados no meio digital**. Disponível em: <https://www.camara.leg.br/noticias/1139965-projeto-aumenta-pena-para-crimes-praticados-no-meio-digital/>. Acesso em: 19 out. 2025.

CARELLI, Ana Esmeralda; MONTEIRO, Silvana Drumond. **Ciberespaço, memória e esquecimento**. 2007.

DE MELO SILVA, Felipe Augusto; MOTA, Luiz Victor Moreira; DA SILVA, Hernando Fernandes. **Responsabilidade civil das instituições financeiras: análise quanto às fraudes realizadas em aplicativos bancários após roubos ou furtos**. Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 11, n. 4, p. 2587-2599, 2025.

DE OLIVEIRA, João Miguel Soares et al. **Criminalidade Digital: Desafios Legais no Enfrentamento**. Facit Business and Technology Journal, v. 2, n. 62, 2025.

DOS SANTOS, Gabriel Rocha. **O Direito e a evolução das relações no mundo digital**. Revista Eletrônica Multidisciplinar UNIFACEAR, v. 2, n. 7, p. 1-15, 2018.

FAVARETTO, Eduardo. **Lei 14.155/2021: entenda tudo sobre a nova lei de crimes cibernéticos**. Revista Migalhas, São Paulo, 2022.

FERREIRA, João. **A fraude no ambiente digital: uma análise crítica das práticas criminosas nos sistemas bancários eletrônicos**. Rio de Janeiro: Editora Jurídica, 2021.

GRECO, Rogério. **Código Penal Comentado**. 15. ed. Rio de Janeiro: Impetus, 2023.

JUSBRASIL. **Fraudes bancárias: responsabilidade civil dos bancos e os direitos do consumidor digital. 2024**. Disponível em: <https://www.jusbrasil.com.br/artigos/fraudes-bancarias-responsabilidade-civil-dos-bancos-e-os-direitos-do-consumidor-digital/4268926958>. Acesso em: 29 out. 2025.

MONTEIRO, Silvana Drumond; PICKLER, Maria Elisa Valentim. **O ciberespaço: o termo, a definição e o conceito**. DataGramaZero – Revista de Ciência da Informação, v. 8, n. 3, p. 1-21, 2007.

NUCCI, Guilherme de Souza. **Leis Penais e Processuais Penais Comentadas**. 19. ed. São Paulo: Forense, 2022.

OAB/RJ. **A responsabilidade civil das instituições financeiras diante de golpes e fraudes digitais**. Revista Eletrônica OAB/RJ, Rio de Janeiro, 2023. Disponível em:

https://revistaeletronica.oabrp.org.br/wp-content/uploads/2023/10/05_A_responsabilidade_civil_instituicoes_financeiras_golpes_fraudes_digitais_Gleyce_Santos_ok.pdf. Acesso em: 29 out. 2025.

OLIVEIRA, Marcos. **Golpes digitais atingem 24% da população brasileira. Agência Senado, 2024.** Disponível em: <https://www12.senado.leg.br/noticias/materias/2024/10/01/golpes-digitais-atingem-24-da-populacao-brasileira-revela-datasenado>.

REVISTA GLOBO. **Fraudes bancárias aumentam e prejudicam clientes e bancos.** Disponível em: <https://valor.globo.com/patrocinado/dino/noticia/2024/05/17/fraudes-bancarias-aumentam-e-prejudicam-clientes-e-bancos.ghtml>.

SANCHES, Marcelo; SILVA, Maria. **Crimes cibernéticos e a vulnerabilidade dos sistemas bancários digitais.** São Paulo: Editora Penal, 2018.

SANCHES, Rogério. **Manual de direito penal.** 13. ed. São Paulo: JusPodivm, 2024.

SENADO FEDERAL. **Projeto de lei propõe medidas de segurança para contas digitais.** Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/156564>. Acesso em: 19 out. 2025.

SILVA, Ana. **O impacto das falhas de segurança nos sistemas bancários digitais e as estratégias de prevenção contra furtos eletrônicos.** Brasília: Editora Jurídica, 2020.

SILVA SÁNCHEZ, Jesús-María. **A expansão do direito penal: aspectos da política criminal nas sociedades pós-industriais.** 4. ed. São Paulo: Revista dos Tribunais, 2020.

SUPERIOR TRIBUNAL DE JUSTIÇA (STJ). **AgRg no REsp 1.972.561/PR.** Rel. Min. Sebastião Reis Júnior, 6.^a Turma, julgado em 15 ago. 2023.

SUPERIOR TRIBUNAL DE JUSTIÇA (STJ). **AgInt no AREsp 2.201.694/SP.** Rel. Min. Marco Aurélio Bellizze, 3.^a Turma, julgado em 12 mar. 2024.

SUPERIOR TRIBUNAL DE JUSTIÇA (STJ). **REsp 1.899.383/DF.** Rel. Min. Nancy Andrighi, 3.^a Turma, julgado em 10 abr. 2023.