II ENCONTRO NACIONAL DE DIREITO DO FUTURO - II ENDIF

DIREITO PENAL E TECNOLOGIA II

D598
Direito penal e tecnologia II [Recurso eletrônico on-line] organização II Encontro Nacional de Direito do Futuro: Escola Superior Dom Helder Câmara – Belo Horizonte;

Coordenadores: Mariana Azevedo Couto Vidal e Priscila Gabrielle Rodrigues Carvalho – Belo Horizonte: Escola Superior Dom Helder Câmara - ESDHC, 2025.

Inclui bibliografia
ISBN: 978-65-5274-421-0
Modo de acesso: www.conpedi.org.br em publicações
Tema: Justiça social e tecnológica em tempos de incerteza.
1. Direito do Futuro. 2. Justiça Social. 3. Justiça Tecnológica. I. II Encontro Nacional de Direito do Futuro (1:2025 : Belo Horizonte, MG).

CDU: 34

Dom Helder
CENTRO UNIVERSITÁRIO

II ENCONTRO NACIONAL DE DIREITO DO FUTURO - II ENDIF

DIREITO PENAL E TECNOLOGIA II

Apresentação

O II Encontro Nacional de Direito do Futuro (II ENDIF), organizado pelo Centro Universitário Dom Helder com apoio técnico do Conselho Nacional de Pesquisa e Pós-graduação em Direito – CONPEDI, reafirma-se como um espaço qualificado de produção, diálogo e circulação do conhecimento jurídico, reunindo a comunidade científica em torno de um propósito comum: pensar, com rigor metodológico e sensibilidade social, os caminhos do Direito diante das transformações que marcam o nosso tempo. Realizado nos dias 09 e 10 de outubro de 2025, em formato integralmente on-line, o evento assumiu como tema geral "Justiça social e tecnológica em tempos de incerteza", convidando pesquisadoras e pesquisadores a enfrentar criticamente os impactos da inovação tecnológica, das novas dinâmicas sociais e das incertezas globais sobre as instituições jurídicas e os direitos fundamentais.

Nesta segunda edição, os números evidenciam a força do projeto acadêmico: 408 trabalhos submetidos, com a participação de 551 pesquisadoras e pesquisadores, provenientes de 21 Estados da Federação, culminando na organização de 31 e-books, que ora se apresentam à comunidade científica. Essa coletânea traduz, em linguagem acadêmica e compromisso público, a vitalidade de uma pesquisa jurídica que não se limita a descrever problemas, mas busca compreendê-los, explicar suas causas e projetar soluções coerentes com a Constituição, com os direitos humanos e com os desafios contemporâneos.

A publicação dos 31 e-books materializa um processo coletivo que articula pluralidade temática, densidade teórica e seriedade científica. Os textos que compõem a coletânea passaram por avaliação acadêmica orientada por critérios de qualidade e imparcialidade, com destaque para o método double blind peer review, que viabiliza a análise inominada dos trabalhos e exige o exame por, no mínimo, dois avaliadores, reduzindo subjetividades e preferências ideológicas. Essa opção metodológica é, ao mesmo tempo, um gesto de respeito à ciência e uma afirmação de que a pesquisa jurídica deve ser construída com transparência, responsabilidade e abertura ao escrutínio crítico.

O II ENDIF também se insere em uma trajetória institucional já consolidada: a primeira edição, realizada em junho de 2024, reuniu centenas de pesquisadoras e pesquisadores e resultou na publicação de uma coletânea expressiva, demonstrando que o Encontro se consolidou, desde o início, como um dos maiores eventos científicos jurídicos do país. A

continuidade do projeto, agora ampliada em escopo e capilaridade, reafirma a importância de se fortalecer ambientes acadêmicos capazes de integrar graduação e pós-graduação, formar novas gerações de pesquisadoras e pesquisadores e promover uma cultura jurídica comprometida com a realidade social.

A programação científica do evento, organizada em painéis temáticos pela manhã e Grupos de Trabalho no período da tarde, foi concebida para equilibrar reflexão teórica, debate público e socialização de pesquisas. Nos painéis, temas como inteligência artificial e direitos fundamentais, proteção ambiental no sistema interamericano, proteção de dados e herança digital foram tratados por especialistas convidados, em debates que ampliam repertórios e conectam a produção acadêmica aos dilemas concretos vividos pela sociedade.

A programação científica do II ENDIF foi estruturada em dois dias, 09 e 10 de outubro de 2025, combinando, no período da manhã, painéis temáticos com exposições de especialistas e debates, e, no período da tarde, sessões dos Grupos de Trabalho. No dia 09/10 (quinta-feira), após a abertura, às 09h, realizou-se o Painel I, dedicado aos desafios da atuação processual diante da inteligência artificial ("Inteligencia artificial y desafios de derechos fundamentales en el marco de la actuación procesal"), com exposição de Andrea Alarcón Peña (Colômbia) e debate conduzido por Caio Augusto Souza Lara. Em seguida, às 11h, ocorreu o Painel II, voltado à proteção ambiental no Sistema Interamericano, abordando a evolução da OC-23 ao novo marco da OC-32, com participação de Soledad Garcia Munoz (Espanha) e Valter Moura do Carmo como palestrantes, sob coordenação de Ricardo Stanziola Vieira. No período da tarde, das 14h às 17h, desenvolveram-se as atividades dos Grupos de Trabalho, em ambiente virtual, com apresentação e discussão das pesquisas aprovadas.

No dia 10/10 (sexta-feira), a programação manteve a organização: às 09h, foi realizado o Painel III, sobre LGPD e a importância da proteção de dados na sociedade de vigilância, com exposições de Laís Furuya e Júlia Mesquita e debate conduzido por Yuri Nathan da Costa Lannes; às 11h, ocorreu o Painel IV, dedicado ao tema da herança digital e à figura do inventariante digital, com apresentação de Felipe Assis Nakamoto e debate sob responsabilidade de Tais Mallmann Ramos. Encerrando o evento, novamente no turno da tarde, das 14h às 17h, seguiram-se as sessões dos Grupos de Trabalho on-line, consolidando o espaço de socialização, crítica acadêmica e amadurecimento das investigações apresentadas.

Ao tornar públicos estes 31 e-books, o II ENDIF reafirma uma convicção essencial: não há futuro democrático para o Direito sem pesquisa científica, sem debate qualificado e sem compromisso com a verdade metodológica. Em tempos de incerteza — tecnológica, social,

ambiental e institucional —, a pesquisa jurídica cumpre um papel civilizatório: ilumina problemas invisibilizados, questiona estruturas naturalizadas, qualifica políticas públicas, tensiona o poder com argumentos e oferece horizontes normativos mais justos.

Registramos, por fim, nosso reconhecimento a todas e todos que tornaram possível esta obra coletiva — autores, avaliadores, coordenadores de Grupos de Trabalho, debatedores e equipe organizadora —, bem como às instituições e redes acadêmicas que fortalecem o ecossistema da pesquisa em Direito. Que a leitura desta coletânea seja, ao mesmo tempo, um encontro com o que há de mais vivo na produção científica contemporânea e um convite a seguir construindo, com coragem intelectual e responsabilidade pública, um Direito à altura do nosso tempo.

Belo Horizonte-MG, 16 de dezembro de 2025.

Prof. Dr. Paulo Umberto Stumpf – Reitor do Centro Universitário Dom Helder

Prof. Dr. Franclim Jorge Sobral de Brito – Vice-Reitor e Pró-Reitor de Graduação do Centro Universitário Dom Helder

Prof. Dr. Caio Augusto Souza Lara – Pró-Reitor de Pesquisa do Centro Universitário Dom Helder

SOMBRAS NO SILÍCIO: TUTELA PENAL E CRIMES CIBERNÉTICOS CONTRA O PATRIMÔNIO

SHADOWS IN SILICON: CRIMINAL PROTECTION AND CYBERCRIMES AGAINST PROPERTY

Rafael Diniz Souza

Resumo

A presente pesquisa, cujo tema é “Sombras no Silício: tutela penal e crimes cibernéticos contra o patrimônio”, aborda a evolução dos crimes patrimoniais para o ambiente digital e a discussão sobre a necessidade de novas leis para combatê-los. Este trabalho tem como finalidade analisar como esses crimes se modificaram na internet, discutir a adequação das normas penais já existentes e demonstrar a dispensabilidade da criação de nova legislação na maioria dos casos. Em suma, como adequar as normas penais já presentes no ordenamento jurídico brasileiro ao mundo cibernético?

Palavras-chave: Cibercrimes, Direito penal, Crimes patrimoniais, Internet, Hermenêutica

Abstract/Resumen/Résumé

This research, titled "Shadows in Silicon: Criminal Protection and Cybercrimes Against Property," addresses the evolution of property crimes into the digital environment and the discussion regarding the necessity of new laws to combat them. This work aims to analyze how these crimes have been modified on the internet, discuss the adequacy of existing penal norms, and demonstrate the dispensability of creating new legislation in most cases. In summary, how can the penal norms already present in the Brazilian legal system be adapted to the cyber world?

Keywords/Palabras-claves/Mots-clés: Cybercrimes, Criminal law, Property crimes, Internet, Hermeneutics

1. CONSIDERAÇÕES INICIAIS

O advento e a expansão vertiginosa da internet redefiniram as bases da sociedade contemporânea, moldando o cotidiano e as dinâmicas profissionais. A onipresença da rede, que se tornou um pilar fundamental para atividades que vão desde a gestão financeira pessoal até a comunicação global, gera a percepção de uma indispensabilidade quase absoluta. Contudo, essa revolução digital, embora carregada de avanços e facilidades, não se desvincula das complexidades inerentes ao progresso social. Assim como a tecnologia impulsiona o desenvolvimento, ela também oferece novos vetores para a evolução e aprimoramento de condutas criminosas, que encontram no ambiente cibernético um terreno fértil para sua manifestação.

Nesse contexto, esta pesquisa, cujo tema é "Sombras No Silício: Tutela Penal E Crimes Cibernéticos Contra O Patrimônio", emerge para analisar a intrínseca relação entre a digitalização e a criminalidade patrimonial. O cerne da discussão reside na observação de que, em grande parte dos casos, os ilícitos cibernéticos não representam uma ruptura conceitual com o direito penal vigente, mas sim uma metamorfose de crimes já tipificados, que agora se manifestam em um novo palco. A ofensa a institutos jurídicos já tutelados pelo Direito, como a propriedade, permanece, adaptando-se às nuances do meio digital.

Diante desse cenário, o presente trabalho propõe-se a investigar a fundo a forma como os crimes contra o patrimônio se reconfiguraram na internet, explorando as particularidades dessa transição. A finalidade precípua é analisar a adequação das normas penais já existentes no ordenamento jurídico brasileiro frente a essa nova realidade, bem como demonstrar a dispensabilidade da criação de nova legislação na maioria das situações. Argumenta-se que, em vez de uma proliferação legislativa, o desafio reside na interpretação e aplicação eficaz das ferramentas jurídicas já disponíveis.

Em suma, a questão central que permeia esta investigação é: como adequar as normas penais já presentes no ordenamento jurídico brasileiro ao dinâmico e complexo mundo cibernético, garantindo a efetividade da tutela penal e a proteção do patrimônio na era digital? Este estudo busca, portanto, oferecer subsídios para uma compreensão mais aprofundada e uma abordagem jurídica mais assertiva diante dos desafios impostos.

No tocante à metodologia da pesquisa, o presente resumo expandido utilizou, com base na classificação de Gustin, Dias e Nicácio (2020), a vertente metodológica jurídico-social. Com relação ao tipo genérico de pesquisa, foi escolhido o tipo jurídico-projetivo. Por sua vez, o

raciocínio desenvolvido na pesquisa foi predominantemente dialético. Quanto ao gênero de pesquisa, adotou-se a pesquisa teórica-bibliográfica.

2. A EVOLUÇÃO DOS CRIMES PATRIMONIAIS NO MEIO AMBIENTE CIBERNÉTICO

A internet, hoje, transcende a mera ferramenta; ela se consolidou como um pilar indispensável para o funcionamento de empresas, instituições de ensino, do próprio Estado e, em última instância, para a vida do indivíduo. Contudo, essa revolução digital, embora repleta de benefícios e inovações, não está isenta de um lado sombrio. Assim como a tecnologia impulsiona o progresso em diversas esferas, ela também se revela um catalisador para a evolução e o aprimoramento de condutas criminosas. Os crimes, em sua essência, adaptam-se aos novos cenários, e os crimes contra o patrimônio, em particular, encontraram no ambiente digital um novo e vasto campo de atuação.

Sobre a necessidade de adaptação do Direito Penal aos avanços da sociedade, ensinam Ribeiro e Oliveira (2019, p. 110) que "é o direito penal que deve servir à vida e não o contrário, o que, em última instância, instiga a adaptação do referido ramo do direito para o enfrentamento dos novos desafios que lhe são impostos".

Os crimes contra o patrimônio são tradicionalmente definidos como toda e qualquer ação criminosa que visa atentar contra os bens de um indivíduo ou organização. No ordenamento jurídico brasileiro, estes são tipificados no Título II do Código Penal, abrangendo artigos que vão do 155 ao 183, e que tratam de delitos como furto, roubo, extorsão, usurpação, dano, apropriação indébita, estelionato e outras fraudes, além da receptação. A preocupação primordial do legislador, ao agrupar esses crimes, era a proteção do patrimônio em si. Esse fato é crucial, pois demonstra que, se tais condutas criminosas podem ser praticadas no meio ambiente virtual, a lógica jurídica subjacente permite que sejam punidas da mesma forma que seriam se praticadas no ambiente físico. A essência da lesão ao bem jurídico tutelado permanece, independentemente do meio em que o ato ilícito é perpetrado, o que reforça a tese da adequação das normas existentes frente à nova realidade digital.

Sobre a problemática dos crimes patrimoniais, leciona Rogério Greco (2021):

> De todos os Títulos constantes da Parte Especial do Código Penal, o Título II é um dos que mais se destacam nas estatísticas judiciárias e policiais. Os crimes contra o patrimônio figuram na lista daquelas infrações penais mais praticadas em nossa sociedade. A pergunta que devemos nos fazer nesse momento é: Por que isso acontece?

> Estudos criminológicos já demonstraram que as infrações patrimoniais são praticadas em decorrência da ausência do Estado, melhor dizendo, da má administração da coisa pública, que gera a desigualdade social, criando bolsões de miséria, separando, cada vez mais, as classes sociais existentes. A situação de miserabilidade gera revolta, indignação, desconfiança dos poderes públicos e cria um clima de tensão. De um lado, a mídia bombardeando nossa mente, forçando-nos a 'entrar na moda', obrigando-nos a todo tipo de compras inúteis e desnecessárias; de outro, pessoas desempregadas ou, mesmo empregadas, recebendo importâncias irrisórias, que mal atendem às suas necessidades básicas de subsistência, sofrem a consequência da pressão social, que as discrimina pela maneira de se vestir, falar, por não terem casa própria, veículos etc.

A transposição dos crimes patrimoniais para o ambiente digital não implica, necessariamente, a obsolescência das normas penais vigentes. Pelo contrário, uma análise aprofundada revela que a maioria dos ilícitos cibernéticos contra o patrimônio pode ser adequadamente enquadrada nas tipificações já existentes no Código Penal brasileiro. A chave reside na interpretação e aplicação desses dispositivos à luz das novas modalidades de execução, demonstrando a flexibilidade e a abrangência do direito penal.

3. UMA RELEITURA DOS CRIMES PATRIMONIAIS CLÁSSICOS NA ERA DIGITAL: TIPICIDADE E DESAFIOS NO CIBERESPAÇO

O furto e a fraude emergem como figuras penais de especial relevância na análise da evolução dos crimes patrimoniais no cenário cibernético. Tradicionalmente associados a ações físicas de subtração ou engano, esses delitos ganham novas roupagens no mundo digital. Um exemplo paradigmático é a clonagem de cartões de crédito, uma prática criminosa que, embora preexistente à internet, e notória pela utilização de dispositivos como os "chupa-cabras" em terminais físicos, encontrou no ambiente online um terreno fértil para sua sofisticação e proliferação.

Atualmente, a clonagem e o uso indevido de dados bancários são predominantemente orquestrados através de páginas falsas (phishing) e invasões a sistemas. As páginas falsas, meticulosamente elaboradas para mimetizar sites de grandes redes de comércio eletrônico ou instituições financeiras, induzem a vítima ao erro, levando-a a fornecer suas informações bancárias e pessoais sob a falsa crença de estar em um ambiente legítimo. No cenário descrito, configura-se claramente o crime de estelionato (art. 171 do Código Penal), pois há a obtenção de vantagem ilícita em prejuízo alheio, mediante fraude que induz ou mantém a vítima em erro. A conduta do agente, ao enganar a vítima para que voluntariamente entregue seus dados, encaixa-se perfeitamente na descrição típica do estelionato.

Por outro lado, as invasões a sistemas informáticos representam outra faceta da criminalidade cibernética. Nesses casos, o agente, explorando vulnerabilidades de segurança,

acessa indevidamente sistemas, como os de e-commerce, para subtrair dados de clientes armazenados em bancos de dados. Tal modalidade pode ser direcionada a grandes empresas ou a indivíduos específicos. Aqui, a conduta de subtrair dados sem o consentimento da vítima, com o intuito de obter vantagem indevida, pode ser enquadrada como furto (art. 155 do Código Penal), especialmente quando há a apropriação de informações que representam valor econômico. Além disso, a invasão de dispositivo informático (art. 154-A do Código Penal) é um crime autônomo que frequentemente ocorre em concurso material com o furto, agravando a situação penal do agente. A distinção entre furto e estelionato no ambiente digital, portanto, reside na forma como a vítima tem o seu patrimônio subtraído: no furto, a subtração é direta e sem consentimento; no estelionato, a vítima é induzida ao erro e entrega voluntariamente o bem ou a informação.

Contudo, a vulnerabilidade do patrimônio no ciberespaço não se resume apenas à sua subtração ou apropriação fraudulenta. A própria integridade e disponibilidade dos ativos digitais são alvos de condutas criminosas, o que nos leva à análise de outro tipo penal clássico.

O crime de dano, tipificado no art. 163 do Código Penal como "Destruir, inutilizar ou deteriorar coisa alheia", também se adaptou de maneira notável à realidade digital. Embora a interpretação mais restritiva possa sugerir que o dano se limita a bens físicos, tal tese carece de fundamento diante da evolução tecnológica. O dano causado em ambientes digitais pode gerar prejuízos patrimoniais de magnitude igual ou até superior aos danos materiais tradicionais.

Exemplos claros incluem ataques de Negação de Serviço Distribuída (DDoS), que, ao sobrecarregarem sistemas, impossibilitam o acesso de usuários e clientes, gerando perdas financeiras significativas para empresas. A coisa alheia aqui não se restringe ao hardware, mas se estende à funcionalidade e à disponibilidade dos sistemas e dados, que possuem valor econômico inegável. Outra forma comum de dano cibernético ocorre pela destruição de dados alheios mediante invasão. Um atacante pode infectar máquinas, seja através de uma invasão que explore vulnerabilidades do sistema, seja através do uso de engenharia social, obter acesso e apagar informações cruciais de bancos de dados, causando prejuízos incalculáveis, especialmente na ausência de *backups*. Nesses casos, a inutilização ou deterioração de dados, que são ativos valiosos, configura o crime de dano, demonstrando que a materialidade do bem não é um impedimento para a aplicação da norma penal.

Indo além da apropriação e da destruição, a criminalidade digital alcançou um patamar ainda mais complexo, no qual a ameaça ao patrimônio é utilizada como ferramenta

de coerção direta para obter vantagem econômica, caracterizando outra modalidade delitiva de grande impacto.

O crime de extorsão, previsto no art. 158 do Código Penal: “Constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar de fazer alguma coisa", encontrou no ambiente cibernético uma de suas manifestações mais perversas e crescentes: o *ransomware*. Esse tipo de ataque, que tem grandes empresas como alvos preferenciais, baseia-se na infecção de redes de computadores e na criptografia de seus arquivos, tornando-os inacessíveis.

O atacante, então, exige um resgate, geralmente em criptomoedas, o que dificulta o rastreamento, para a liberação dos dados. A grave ameaça, elemento central da extorsão, materializa-se na privação do acesso a informações vitais, cuja perda pode significar a paralisação de operações e prejuízos financeiros catastróficos. A coerção exercida sobre a vítima para que ela "faça" (pague o resgate) algo em troca da recuperação de seus bens digitais se alinha perfeitamente à descrição legal do art. 158. A experiência, contudo, mostra que, mesmo após o pagamento, a recuperação integral dos arquivos não é garantida, evidenciando a natureza predatória desses ataques.

Dados do relatório "The State of Ransomware 2022" da Sophos corroboram a gravidade do cenário: cerca de 55% das empresas brasileiras entrevistadas já foram vítimas de *ransomware*. Dessas, 40% cederam às exigências dos criminosos, recuperando, em média, apenas 55% dos dados criptografados. O custo médio do resgate para 25% dos entrevistados atingiu US$ 211.790,00, com 9% pagando US$ 500.000,00 ou mais. Tais estatísticas sublinham não apenas a prevalência, mas também o impacto econômico devastador dos ataques com *ransomware*, reforçando a necessidade de uma resposta penal robusta, que pode ser encontrada na aplicação do tipo de extorsão já existente.

4. DA DISPENSABILIDADE DA PROLIFERAÇÃO LEGISLATIVA

Após demonstrar a adequação das normas penais existentes aos crimes cibernéticos, este trabalho argumenta contra a criação indiscriminada de novas leis para cada manifestação tecnológica do crime. A busca por soluções legislativas pontuais pode gerar o que chamamos de “hiperlegislação”, caracterizada pelo excesso de normas que, paradoxalmente, causa insegurança jurídica. Leis excessivamente específicas para o ciberespaço correm o risco de se tornarem obsoletas rapidamente, minando a credibilidade do sistema e dificultando a atuação

dos operadores do direito.

A proliferação legislativa pode levar à sobreposição de normas e lacunas na aplicação da lei, fragmentando a proteção jurídica. O Direito Penal, como *ultima ratio*, deve intervir com clareza e estabilidade, e a criação desenfreada de novas leis coloca em risco esse princípio. O verdadeiro desafio reside na hermenêutica, isto é, na interpretação e aplicação eficaz das ferramentas jurídicas já disponíveis. A robustez do Código Penal brasileiro permite que conceitos como coisa alheia, vantagem ilícita mediante fraude e grave ameaça sejam interpretados no contexto digital, enquadrando novas formas de manifestação de um mesmo tipo penal.

A resposta mais eficaz à criminalidade cibernética não está em novas proibições, mas no investimento em inteligência, capacitação e adaptabilidade. É fundamental que profissionais do direito recebam treinamento contínuo sobre o ambiente digital, técnicas de investigação forense e prova eletrônica. Aprimorar a capacidade de investigação e a compreensão técnica dos fenômenos cibernéticos é mais promissor do que a adição infinita de artigos ao Código Penal. A tecnologia, palco do crime, deve ser usada como ferramenta para a persecução penal, rastreando e responsabilizando criminosos digitais.

Em suma, a dispensabilidade de nova legislação para a maioria dos crimes cibernéticos contra o patrimônio não é inação, mas um apelo à valorização e aprimoramento da própria técnica. A solidez dos princípios jurídicos e a capacidade de adaptação são mais eficazes do que soluções legislativas efêmeras.

5. CONSIDERAÇÕES FINAIS

Com este trabalho, buscou-se introduzir e aprofundar a problemática dos crimes contra o patrimônio no meio ambiente cibernético, um cenário em constante mutação que desafia as fronteiras tradicionais do Direito Penal. Ao longo da pesquisa, demonstrou-se que tais crimes, embora se manifestem em um novo palco digital, já possuem tipificação e sanções previstas no ordenamento jurídico brasileiro. A essência da lesão ao bem jurídico tutelado aqui estudado, o patrimônio, permanece inalterada, o que permite a aplicação das normas penais já existentes.

É imperativo que o Direito, como reflexo e regulador da sociedade, acompanhe suas transformações e avance com ela. Contudo, esse acompanhamento não se traduz, necessariamente, na criação incessante de novas leis para cada nova modalidade criminosa que surge no ciberespaço. Pelo contrário, a análise detalhada das modalidades de furto, fraude, dano e extorsão no ambiente digital revelou que o Código Penal brasileiro já possui a

flexibilidade e a abrangência necessárias para tutelar o patrimônio na era digital. A tese central deste trabalho, portanto, é a de que a criação indiscriminada de novas leis para cada nova manifestação tecnológica do crime pode ser não apenas desnecessária, mas até contraproducente.

Assim, é necessário que os atos aqui estudados sejam punidos na esfera criminal com a aplicação das sanções cabíveis já previstas no Código Penal. A solidez dos princípios jurídicos e a capacidade de adaptação interpretativa são mais eficazes do que a busca incessante por soluções legislativas pontuais, que podem se mostrar efêmeras e ineficazes diante da dinâmica do ciberespaço. A tutela penal na esfera cibernética possui suas "sombras" bem definidas, e a luz para combatê-las reside na hermenêutica, e não na profusão de novas fontes. Este estudo busca, portanto, reforçar a importância de uma abordagem tecnicamente jurídica que valorize a profundidade e a capacitação das normas.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. **Código Penal**. Diário Oficial da União, Seção 1, Brasília, DF, ano 79, n. 297, p. 23911–23916, 31 dez. 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 17 set. 2025.

GRECO, Rogério. **Curso de Direito Penal: Parte Geral**. 23. ed. Rio de Janeiro: Impetus, 2021. v. 1.

GUSTIN, Miracy Barbosa de Sousa; DIAS, Maria Tereza Fonseca; NICÁCIO, Camila Silva. **(Re)pensando a pesquisa jurídica: teoria e prática**. 5. ed. São Paulo: Almedina, 2020.

RIBEIRO, Luiz Gustavo Gonçalves; OLIVEIRA, Camila Martins de. **A legitimidade da tutela penal no ciberespaço: breves considerações**. In: CONGRESSO NACIONAL DO CONPEDI, 10., 2019, Valência. **Anais** […]. Valência: CONPEDI, 2019.

SOPHOS. **O estado do ransomware no Brasil 2022**. [S. l.]: Sophos, 2022. Disponível em: https://assets.sophos.com/X24WTUEQ/at/t5mxk5jh54qtfm6f9t6wxqx/sophos-state-of-ransomware-2022-br-wpptbr.pdf. Acesso em: 25 jun. 2022.