UNIVERSIDADE ESTADUAL DO MARANHÃO
CAMPUS GRAJAÚ
CURSO DE DIREITO

GABRIEL BARROS NASCIMENTO

DARK WEB: Desafios da Persecução Penal na Repressão ao Cibercrime e a Salvaguarda dos Direitos Fundamentais no Ordenamento Jurídico Brasileiro

Grajaú
2026

GABRIEL BARROS NASCIMENTO

DARK WEB: Desafios da Persecução Penal na Repressão ao Cibercrime e a Salvaguarda dos Direitos Fundamentais no Ordenamento Jurídico Brasileiro

Trabalho de Conclusão de Curso apresentado ao curso de Direito da Universidade Estadual do Maranhão Campus Grajaú, para obtenção do grau de Bacharelado em Direito.

Orientador: Prof. Esp. Marcos Paulo Carola Sousa.

Grajaú

2026

Nascimento, Gabriel Barros.
Dark web: desafios da persecução penal na repressão ao cibercrime e a salvaguarda dos direitos fundamentais no ordenamento jurídico brasileiro / Gabriel Barros Nascimento. - Grajaú - MA, 2026.
27 f.

Artigo Científico (Graduação em Direito Bacharelado) - Universidade Estadual do Maranhão, Campus Grajaú, 2026.

Orientador: Prof. Esp. Marcos Paulo Carola Sousa.

1. Dark web. 2. Cibercrime. 3. Direitos fundamentais. 4. Investigação digital. 5. Processo penal. I. Título.

CDU: 342.7:004

Elaborado por Luciana de Araújo - CRB 13/445

GABRIEL BARROS NASCIMENTO

DARK WEB: Desafios da Persecução Penal na Repressão ao Cibercrime e a Salvaguarda dos Direitos Fundamentais no Ordenamento Jurídico Brasileiro

Trabalho de Conclusão de Curso apresentado ao curso de Direito da Universidade Estadual do Maranhão, Campus Grajaú, para obtenção do grau de Bacharelado em Direito.

Orientador: Prof. Esp. Marcos Paulo Carola Sousa.

Aprovado em: 02/07/2026

BANCA EXAMINADORA

gov.br
Documento assinado digitalmente
MARCOS PAULO CAROLA SOUSA
Data: 13/07/2026 17:51:43-0300
Verifique em https://validar.iti.gov.br

Prof. Esp. Marcos Paulo Carola Sousa (Orientador)

Universidade Estadual do Maranhão – UEMA

gov.br
Documento assinado digitalmente
BIANCA ALBUQUERQUE DE ABREU LIMA
Data: 13/07/2026 16:41:03-0300
Verifique em https://validar.iti.gov.br

Profa. Esp. Bianca Albuquerque de Abreu Lima

Universidade Estadual do Maranhão – UEMA

gov.br
Documento assinado digitalmente
WALESKA SOUSA CHAVES
Data: 13/07/2026 15:37:01-0300
Verifique em https://validar.iti.gov.br

Profa. Esp. Waleska Sousa Chaves

Universidade Estadual do Maranhão – UEMA

Em um cenário onde a tecnologia muitas vezes avança para excluir ou fraudar, dedico esta pesquisa ao povo maranhense, que enfrenta a negligência histórica e a negação sistemática de seus direitos básicos. Que o enfrentamento ao cibercrime e a preservação dos direitos fundamentais aqui discutidos encontrem eco na realidade de quem busca justiça em meio à pobreza estrutural. Este trabalho é para aqueles que, mesmo invisibilizados pelo sistema, são a razão última da existência do Direito e da minha busca por uma sociedade mais ética e humana.

AGRADECIMENTOS

Em primeiro lugar, agradeço a Deus, por ter me sustentado em cada passo desta jornada. Estar aqui, redigindo este trabalho acadêmico, só foi possível pela graça e força que dele recebi até aqui. Agradeço com profundo carinho à minha família que nunca mediram esforços para que eu pudesse alcançar meus objetivos. Em especial, à minha mãe, Elisângela Silva Barros e ao meu pai Jean Carlos Pires Nascimento, por acreditar nos meus sonhos e investir neles com coragem e amor. Por ser sinônimo de dedicação incansável e cuidado diário, ensinando, com palavras e atitudes, sobre gentileza, espiritualidade e amor incondicional. E, mesmo diante das dificuldades, sempre garantiram que eu tivesse acesso à educação de qualidade, me permitindo sonhar com voos mais altos. Aos amigos construídos ao longo desta jornada universitária, que estiveram presentes nos momentos de desafios e conquistas, minha sincera gratidão. Em especial, à Klebiane Santos, Denilson Silva, Júnior Nascimento e José Divino que, dia após dia, me acolheram e contribuíram para meu crescimento pessoal e acadêmico. Gratidão pelo apoio constante, pelos risos, o companheirismo e a troca de experiências, vocês foram fundamentais no caminho até aqui. Que os vínculos criados nesse percurso se mantenham firmes e significativos para além da graduação. À UEMA, por proporcionar um espaço singular de aprendizagem aos seus alunos com uma graduação completa, marcada por incentivos à pesquisa, à extensão. Em especial, à meu Orientador Prof. Esp. Marcos Paulo Carola Sousa, que conduziu o trabalho com paciência, disponibilizando tempo para tecer ensinamentos que permitiram-me apresentar um melhor desempenho no meu processo de realização deste trabalho. À Banca Examinadora, pela consideração e dedicação de tempo para estar nessa avaliação do presente trabalho, contribuindo nesta etapa fundamental para a minha formação acadêmica.

Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: (...) VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei."

Lei nº 12.965/2014 (Marco Civil da Internet)

O Direito não deve ser um obstáculo ao progresso, mas deve ser o freio necessário para que a técnica não ignore a dignidade humana."

Stefano Rodotà (Em A Vida na Sociedade de Vigilância)

RESUMO

O presente Trabalho de Conclusão de Curso investiga os desafios da persecução penal na repressão ao cibercrime na *Dark Web* e a salvaguarda dos direitos fundamentais no ordenamento jurídico brasileiro. Diante da opacidade, do elevado grau de anonimato e da transnacionalidade desse ecossistema virtual, delineia-se o seguinte problema de pesquisa: quais os principais desafios enfrentados pelo Estado na repressão a esses delitos e de que forma é possível garantir a salvaguarda das garantias constitucionais dos cidadãos? Objetiva-se analisar os óbices institucionais para a identificação de agentes, avaliar os limites de admissibilidade das provas eletrônicas e propor mecanismos que harmonizem a eficiência persecutória com a proteção dos direitos previstos no artigo 5º da Constituição Federal de 1988. Metodologicamente, a pesquisa adota uma abordagem interpretativa e qualitativa, de natureza bibliográfica e documental, amparada no método de análise de conteúdo de Bardin. A hipótese central, confirmada ao longo do estudo, aponta que a insuficiência de diplomas normativos tradicionais como o Marco Civil da Internet e a Lei Carolina Dieckmann frente a técnicas invasivas, como o *hacking* governamental e a infiltração virtual, gera uma crise de territorialidade e impulsiona a necessidade de uma disciplina jurídica própria para o processo penal digital. Os dados demonstram que a volatilidade intrínseca da evidência digital exige o respeito rigoroso e incondicional ao instituto da cadeia de custódia, sob pena de quebra de confiabilidade e ilicitude por derivação com base na teoria dos frutos da árvore envenenada. Conclui-se que o equilíbrio estrito entre a eficiência investigativa e a dignidade humana é o único caminho para assegurar a legitimidade democrática do sistema de justiça criminal em ambientes virtuais de alta complexidade.

Palavras-chave: Dark Web. Cibercrime. Direitos Fundamentais. Investigação Digital. Processo Penal.

ABSTRACT

The present Term Paper investigates the challenges of criminal prosecution in repressing cybercrime on the Dark Web and the safeguard of fundamental rights within the Brazilian legal system. Given the opacity, high degree of anonymity, and transnationality of this virtual ecosystem, the following research problem is outlined: what are the main challenges faced by the State in repressing these offenses, and in what way is it possible to ensure the safeguard of citizens' constitutional guarantees? The objective is to analyze the institutional obstacles in identifying agents, evaluate the admissibility limits of electronic evidence, and propose mechanisms that harmonize prosecutorial efficiency with the protection of rights provided for in article 5 of the 1988 Federal Constitution. Methodologically, the research adopts an interpretive and qualitative approach, of a bibliographic and documentary nature, supported by Bardin's content analysis method. The central hypothesis, confirmed throughout the study, points out that the insufficiency of traditional normative diplomas such as the Brazilian Civil Rights Framework for the Internet and the Carolina Dieckmann Law in the face of invasive techniques, such as government hacking and virtual infiltration, generates a territoriality crisis and drives the need for a specific legal discipline for digital criminal procedure. The data demonstrate that the intrinsic volatility of digital evidence requires rigorous and unconditional respect for the chain of custody institution, under penalty of breach of reliability and derivative unlawfulness based on the fruits of the poisonous tree doctrine. It is concluded that the strict balance between investigative efficiency and human dignity is the only way to ensure the democratic legitimacy of the criminal justice system in highly complex virtual environments.

Keywords: Dark Web. Cybercrime. Fundamental Rights. Digital Investigation. Criminal Procedure.

SUMÁRIO

1. INTRODUÇÃO

A *dark web*, caracterizada como um ambiente virtual de acesso restrito e marcado por elevado grau de anonimato e sofisticação tecnológica, representa um dos maiores desafios contemporâneos para o sistema jurídico-penal brasileiro. Diferente da internet superficial que se utiliza cotidianamente, este espaço utiliza camadas complexas de criptografia que ocultam a identidade dos usuários e a localização geográfica dos servidores, criando um cenário de difícil monitoramento pelas autoridades.

A opacidade desse ambiente, aliada à velocidade das transações digitais, impõe obstáculos significativos à atuação do Estado na proteção de bens jurídicos fundamentais, como a privacidade, a segurança pública e a própria dignidade da pessoa humana, exigindo uma releitura das práticas investigativas tradicionais. Nesse contexto, a cadeia de investigação e persecução penal na *dark web* enfrenta barreiras técnicas e jurídicas que impactam diretamente a efetividade das normas penais vigentes no Brasil.

Entre os principais problemas associados ao combate ao cibercrime nesse ecossistema, destacam-se a transnacionalidade das condutas criminosas e a carência de órgãos especializados com tecnologia de ponta para a quebra desse anonimato. Tais fatores colocam em xeque a capacidade do Estado em garantir a aplicação da legislação brasileira, especialmente o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Carolina Dieckmann (Lei nº 12.737/2012), que buscam regular o uso da rede e tipificar condutas ilícitas, mas que muitas vezes esbarram na invisibilidade proporcionada pelas redes sobrepostas.

Diante deste panorama complexo, o presente estudo delimita-se pelo seguinte problema de pesquisa: quais os principais desafios da persecução penal na repressão ao cibercrime na *Dark Web* e de que forma é possível garantir a salvaguarda dos direitos fundamentais no ordenamento jurídico brasileiro?

Para responder a esse questionamento, definiu-se como objetivo geral analisar os desafios da persecução penal na repressão ao cibercrime nesse ambiente, propondo mecanismos que harmonizem a eficiência persecutória com a salvaguarda dos direitos fundamentais no ordenamento jurídico brasileiro. Especificamente, busca-se examinar as dificuldades dos órgãos de persecução na identificação e responsabilização de agentes; analisar a admissibilidade das provas obtidas nesse ambiente no processo penal; e propor recomendações que equilibrem a eficiência repressiva e a salvaguarda de direitos.

A pesquisa justifica-se pela urgência social e jurídica do tema, dado o crescimento

exponencial das infrações digitais e a constante evolução das ferramentas de anonimização que facilitam a impunidade. Sob a perspectiva acadêmica, o trabalho ganha relevância ao colocar em evidência uma realidade ainda pouco explorada na doutrina nacional, colaborando com a produção científica ao dialogar com as necessidades locais das autoridades brasileiras.

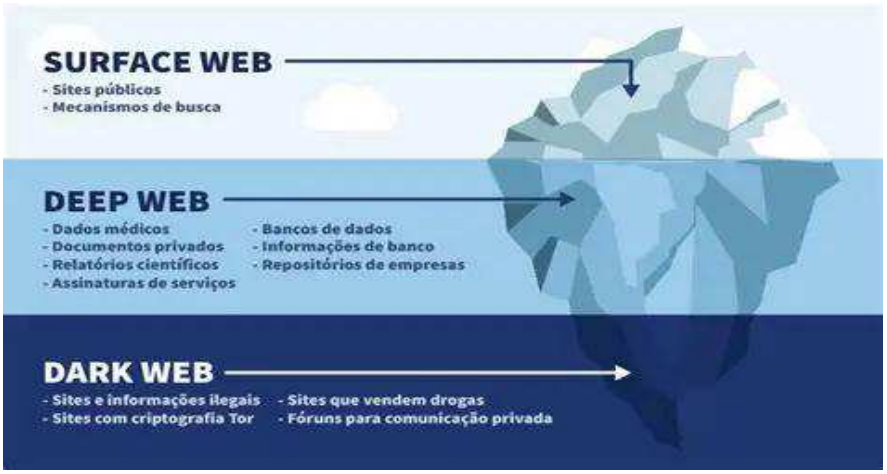
Para tanto, o trabalho está estruturado de modo que, inicialmente, aborda-se a estratificação da rede, estabelecendo as diferenciações técnicas entre *Surface*, *Deep* e *Dark Web*. Em seguida, analisa-se a fenomenologia do cibercrime e o papel da *Dark Web* como catalisadora da delinquência digital, para então discutir a tutela dos direitos fundamentais na era do processo penal digital. Por fim, examinam-se os desafios e limites da obtenção e admissibilidade de provas em ambientes virtuais, encerrando-se com as considerações finais e recomendações pertinentes.

2. A ESTRATIFICAÇÃO DA REDE: DIFERENCIAÇÃO ENTRE SURFACE, DEEP E DARK WEB

Considerada o maior sistema global de informações da atualidade, a Internet é constituída por diferentes camadas que variam significativamente em visibilidade, acessibilidade e profundidade de dados. Essa segmentação não ocorre de forma aleatória, mas reflete a própria evolução da arquitetura da rede mundial de computadores e a necessidade de categorizar e proteger o fluxo de informações públicas, corporativas e governamentais. Conforme ilustrado na analogia do *iceberg* na Figura 1, logo abaixo, essa organização estrutural divide o ciberespaço em diferentes níveis de acesso e privacidade, cujas complexidades e características técnicas são detalhadas e fundamentadas por Basheer e Alkhatib (2021).

Sob essa perspectiva, a *Surface Web* constitui a camada mais superficial e visível, composta por páginas e conteúdos abertos que são facilmente indexados por mecanismos de busca tradicionais, como o Google e o Bing. Logo abaixo dessa linha, a *Deep Web* engloba conteúdos não indexados e protegidos por autenticação, como registros médicos, relatórios acadêmicos e documentos legais, possuindo uma natureza estritamente legítima e corporativa. Por fim, na base oculta dessa estrutura, reside a *Dark Web*, uma porção restrita e acessível apenas por meio de *softwares* e protocolos específicos, onde a criptografia garante o anonimato absoluto dos usuários, o que acaba tornando esse ambiente altamente propício para práticas ilícitas e o tráfego de conteúdos confidenciais.

Figura 1 – Diferenças entre *Surface*, *Deep* e *Dark Web*. [Imagem de um *iceberg* representando as camadas da internet]



(Fonte: VPNOverview (2026)).

É imperativo destacar que a *Dark Web* não é um subproduto acidental da arquitetura da rede, mas sim uma construção deliberada baseada em redes sobrepostas (*overlay networks*). Diferente da *Deep Web*, onde a não indexação decorre de questões de segurança privada ou volume de dados, a *Dark Web* utiliza protocolos como o *The Onion Router* (Tor), que encaminha o tráfego por múltiplos nós criptografados. Sob a ótica penal, essa estrutura é o que viabiliza o *dolus* (dolo) da ocultação, permitindo que o agente criminoso opere em uma jurisdição virtual aparentemente imune às ferramentas de interceptação telemática previstas na legislação brasileira, como as dispostas na Lei nº 9.296/1996.

A metáfora do *iceberg* é comumente empregada para representar as camadas da Internet, uma vez que enfatiza que a maior parte da *web* é oculta aos usuários comuns. Contudo, para o Direito Penal, essa imagem transcende a mera curiosidade técnica e revela um vácuo de jurisdição. Essa estratificação impõe o que a doutrina moderna chama de "crise de territorialidade". O Marco Civil da Internet (Lei nº 12.965/2014) estabeleceu pilares baseados na identificação por registros de conexão e acesso. Todavia, a arquitetura da base do iceberg ignora tais premissas.

Enquanto o Estado exerce controle sobre a "superfície" da rede, a vastidão submersa impõe uma barreira de invisibilidade que não é apenas tecnológica, mas também estratégica para a prática de delitos. É nesse ambiente de opacidade que os

direitos fundamentais e a necessidade de repressão criminal entram em rota de colisão, exigindo que o operador do Direito compreenda que a proteção jurídica deve alcançar inclusive as profundezas que os mecanismos de busca convencionais não conseguem indexar.

Dessa forma, compreender a estratificação da rede é o primeiro passo para delimitar o campo de batalha do Direito Penal contemporâneo. A distinção técnica entre o que é meramente privado (*Deep Web*) e o que é propositalmente oculto (*Dark Web*) é o que permite separar o direito fundamental à privacidade da utilização abusiva do anonimato para a prática de ilícitos. Esta base conceitual é essencial para analisar, a seguir, como o cibercrime evoluiu para explorar precisamente essas fissuras na visibilidade estatal.

3. A FENOMENOLOGIA DO CIBERCRIME: A DARK WEB COMO CATALISADORA DA DELINQUÊNCIA DIGITAL

O surgimento do cibercrime não ocorreu de forma isolada, mas acompanhou a própria evolução e popularização da rede mundial de computadores. Inicialmente, as condutas ilícitas no ambiente virtual eram praticadas por indivíduos com alto conhecimento técnico (*hackers*), motivados muitas vezes pelo desafio intelectual ou pelo reconhecimento entre pares. Contudo, com a migração das relações sociais, financeiras e jurídicas para o ambiente digital, o crime de informática transmutou-se em uma atividade profissionalizada, organizada e altamente lucrativa.

Segundo Medeiros (2020, p. 42), o cibercrime pode ser compreendido sob duas vertentes principais: os crimes de informática impróprios, nos quais a tecnologia é utilizada como mero instrumento para a prática de delitos já previstos no ordenamento (como o estelionato ou a injúria), e os crimes de informática próprios, em que o bem jurídico atingido é o próprio dado informático ou a disponibilidade do sistema. Sobre essa transição, o autor destaca que a rede deixou de ser apenas uma ferramenta de comunicação para se tornar um novo território de conflitos, onde a velocidade da informação supera a capacidade de resposta das normas penais tradicionais.

Nesse contexto evolutivo, a *Dark Web* surge como um divisor de águas e um catalisador de novas modalidades delitivas. Enquanto na *Surface Web* a identificação do usuário é viabilizada por meio de registros de IP e pela cooperação de provedores de serviço, na *Dark Web* o anonimato é a regra arquitetural. O papel desse ecossistema no

cenário atual transcende a mera ocultação, funcionando como um verdadeiro mercado de serviços ilícitos, conhecido como *Cybercrime as a Service* (CaaS). Nesse ambiente, cibercriminosos comercializam desde bancos de dados vazados até *softwares* de invasão prontos para uso, democratizando o acesso a ferramentas de ataque.

Para Reis (2023), a eficácia da legislação brasileira, notadamente a Lei Carolina Dieckmann (Lei nº 12.737/2012), encontra limites severos quando confrontada com as redes de anonimização. O autor observa que o grande desafio da persecução penal contemporânea reside na transposição da barreira tecnológica:

> O grande desafio da persecução penal contemporânea não é apenas a tipificação da conduta, mas a transposição da barreira do anonimato. Na *Dark Web*, o criminoso goza de uma sensação de impunidade conferida por camadas de criptografia que muitas vezes tornam a jurisdição nacional inócua.

Um fator determinante para o papel da *Dark Web* no cenário atual é a sua natureza intrinsecamente transnacional. Um crime pode ser arquitetado em um continente, executado através de servidores localizados em um segundo país, para atingir uma vítima em solo brasileiro. Essa ausência de fronteiras físicas, aliada ao uso de criptoativos (como o Bitcoin e o Monero) para o pagamento de resgates e transações ilícitas, dificulta o rastreamento do proveito econômico do crime, tornando as técnicas de investigação financeira tradicionais obsoletas frente à tecnologia de *blockchain*.

Portanto, a evolução do cibercrime aponta para um cenário onde a *Dark Web* não é apenas um esconderijo, mas a estrutura que sustenta a impunidade digital. Para o Direito Penal brasileiro, o desafio não reside apenas em atualizar o rol de crimes, mas em reformular as estratégias de investigação e cooperação internacional para que o Marco Civil da Internet e as garantias constitucionais não sejam ignorados diante da complexidade técnica dessas redes sobrepostas.

4. LIMITES CONSTITUCIONAIS À PERSECUÇÃO PENAL NA ERA DIGITAL

A expansão da criminalidade para as camadas mais profundas da rede mundial de computadores impôs uma profunda releitura dos institutos tradicionais do Direito Processual Penal. Se, por um lado, o Estado necessita de ferramentas ágeis e invasivas para romper o manto de anonimato da *Dark Web*, por outro, a atividade persecutória encontra limites intransponíveis nas garantias fundamentais esculpidas na Constituição Federal de 1988. O processo penal digital, portanto, não pode se converter em um espaço

de exceção onde a eficácia investigativa se sobreponha à dignidade da pessoa humana e aos direitos individuais.

No centro desse debate jurídico está o direito à privacidade e à inviolabilidade do sigilo de dados telemáticos, resguardados pelo artigo 5º, incisos X e XII, da Carta Magna. No ambiente virtual, os dados de um indivíduo refletem sua intimidade, seus hábitos, pensamentos e interações mais profundas. Por essa razão, a intervenção estatal sobre esses registros exige o estrito cumprimento do princípio da legalidade e da reserva de jurisdição. Qualquer medida de captação, interceptação ou acesso a dados na *Dark Web*, por mais grave que seja o crime investigado, depende de prévia e fundamentada autorização judicial, sob pena de nulidade absoluta da prova obtida.

A doutrina processual penal contemporânea alerta para o risco do chamado *fishing expedition* (ou pescaria predatória) no ambiente digital. Essa prática, conforme definição acolhida pela jurisprudência do Superior Tribunal de Justiça (STJ), consiste na "procura especulativa, no ambiente físico ou digital, sem 'causa provável', alvo definido, finalidade tangível ou para além dos limites autorizados" (Rosa, 2020 *apud* STJ, HC 663.055/SP). No processo penal democrático, a busca por provas deve ser cirúrgica. A devassa indiscriminada em dispositivos, servidores ou contas de usuários sob o pretexto de combater o anonimato da *Dark Web* subverte a lógica das garantias constitucionais, transformando a legítima investigação criminal em um mecanismo de vigilância em massa ilegal e eivado de nulidade.

Além disso, a introdução de novas técnicas de investigação tecnológica, como o uso de softwares espiões (*malwares*) ou a infiltração virtual de agentes em fóruns restritos da *Dark Web*, tenciona o princípio da não autoincriminação (*nemo tenetur se detegere*). A linha que separa a legítima colheita de provas da indução ou provocação de condutas delitivas por parte do Estado é tênue. Portanto, a atuação das autoridades no ambiente digital deve ser balizada pelos princípios da proporcionalidade e da necessidade, demonstrando-se que a medida invasiva é o único meio capaz de elucidar o fato e que o interesse público na repressão penal supera o sacrifício temporário do direito individual.

Dessa forma, a proteção dos direitos fundamentais no processo penal digital funciona como a garantia de legitimidade da própria sanção penal. O combate ao cibercrime na *Dark Web* não demanda o esvaziamento das garantias constitucionais, mas sim o aperfeiçoamento técnico e ético dos métodos investigativos. Afinal, a higidez democrática do Estado se mede não apenas pela sua capacidade de punir, mas, fundamentalmente, pelo respeito aos limites legais estabelecidos para o exercício dessa

punição.

4.1 Técnicas Invasivas de Investigação: Infiltração Virtual de Agentes *vs.* Provocação de Flagrante

A necessidade de romper o manto de anonimato que protege organizações criminosas na *Dark Web* impulsionou a adoção da infiltração virtual de agentes, regulamentada pela Lei nº 12.850/2013, com as alterações da Lei nº 13.964/2019. Essa técnica autoriza policiais a operarem disfarçados em ambientes digitais e mercados ilícitos para colher informações. Contudo, por se tratar de uma medida de altíssima intromissão nos direitos fundamentais, sua execução exige estrito cumprimento dos limites constitucionais, sob pena de desvirtuar a atividade persecutória em prática abusiva. O principal ponto de tensão reside na linha divisória entre a legítima infiltração passiva e a ilegal provocação de flagrante por parte do agente estatal.

No ambiente opaco da *Dark Web*, onde as interações ocorrem por avatares e pseudônimos, há o risco iminente de o policial infiltrado deixar de ser observador e atuar como agente provocador, induzindo o suspeito a praticar um crime que não cometeria voluntariamente. No direito processual penal pátrio, essa conduta configura o flagrante preparado ou provocado, vício insanável que atrai a aplicação imediata da Súmula nº 145 do Supremo Tribunal Federal, que preconiza não haver crime quando a preparação da polícia torna impossível sua consumação. Ao analisar esses limites, Lopes Jr. (2022, p. 612) adverte que "o Estado não pode criar o crime para depois puni-lo; a infiltração digital legítima pressupõe a descoberta de uma atividade criminosa preexistente, e não a sua geração por induzimento".

Dessa forma, a validade jurídica da infiltração virtual na *Dark Web* está umbilicalmente ligada ao controle judicial prévio e concomitante da medida, em obediência ao princípio da reserva de jurisdição. Cabe ao magistrado delimitar com precisão o escopo da atuação do agente disfarçado, estabelecendo balizas temporais e operacionais que impeçam desvios de finalidade. Somente através de uma fiscalização rigorosa dos relatórios parciais de investigação e da garantia de que os métodos empregados possam ser integralmente auditados pela defesa, será possível harmonizar a eficiência da repressão ao cibercrime organizado com a higidez das garantias do devido processo legal.

4.2 O Hacking Governamental e os Limites Constitucionais da Cláusula de Reserva de Jurisdição

O avanço das tecnologias de criptografia de ponta a ponta na *Dark Web* criou o fenômeno que a doutrina estrangeira classifica como *going dark*, situação na qual os meios tradicionais de interceptação telemática previstos na Lei nº 9.296/1996 tornam-se inócuos. Diante dessa barreira técnica, surge o *hacking* governamental, prática pela qual o Estado utiliza softwares espiões (*malwares*) para invadir remotamente o dispositivo do investigado. Essa medida permite capturar dados diretamente na fonte, antes da cifragem ou após a decodificação pelo usuário. Todavia, por se tratar de uma devassa irrestrita na intimidade digital, essa técnica tenciona severamente as garantias constitucionais da privacidade e do sigilo de dados (art. 5º, X e XII, da CF/88), exigindo uma releitura estrita da cláusula de reserva de jurisdição.

Diferente de uma interceptação telefônica comum, que colhe fluxos de comunicação em tempo real, a infiltração por *malware* concede ao Estado acesso retroativo a arquivos armazenados, metadados, senhas, câmera e microfone do aparelho. Portanto, no processo penal democrático, a autorização para o emprego do *hacking* governamental não pode se basear em mandados genéricos de "interceptação", demandando uma decisão judicial cirúrgica, exaustivamente motivada, que comprove a indispensabilidade da medida. A ausência de uma disciplina legal própria no Brasil gera o risco iminente de investigações especulativas, as quais convertem o poder de polícia em vigilância em massa ilegal, resvalando na prática abusiva do *fishing expedition*.

Como adverte Coutinho (2021, p. 189), "o processo penal não pode tolerar o uso de ferramentas tecnológicas que transformem o Estado em um intruso onipresente, sob pena de sepultar o sistema acusatório e restabelecer premissas inquisitoriais de devassa cega". Alinhada a esse entendimento, a jurisprudência do Superior Tribunal de Justiça (STJ) caminha no sentido de impor freios rigorosos ao acesso estatal a dispositivos informáticos, exigindo fundada causa provável e delimitação de escopo. Conclui-se, assim, que a admissibilidade das informações coletadas por invasão cibernética estatal pressupõe a edição de uma lei regulamentadora detalhada, que fixe limites técnicos auditáveis e assegure o pleno respeito às garantias do devido processo legal.

5. OS DESAFIOS E LIMITES DA OBTENÇÃO E ADMISSIBILIDADE DE PROVAS EM AMBIENTES VIRTUAIS

A colheita e a introdução de elementos probatórios colhidos no ambiente virtual representam uma das engrenagens mais sensíveis do moderno processo penal democrático. Quando o cenário dessa busca se desloca para a *Dark Web*, os desafios técnicos de extração de dados são severamente multiplicados pela volatilidade intrínseca dos arquivos digitais e pela arquitetura de ocultação da rede. Nesse contexto, a admissibilidade da prova digital não se limita à análise de sua relevância causal, mas depende, fundamentalmente, da demonstração cabal de sua integridade, fidedignidade, veracidade e de sua licitude de obtenção.

A maior vulnerabilidade da evidência digital reside na sua facilidade de alteração, supressão ou corrupção sem que se deixem vestígios aparentes. Por essa razão, a observância rigorosa do instituto da cadeia de custódia positivada no ordenamento jurídico brasileiro pelas reformas introduzidas pela Lei nº 13.964/2019 (Pacote Anticrime) nos artigos 158-A a 158-F do Código de Processo Penal assume papel de destaque indispensável. Toda prova digital extraída da *Dark Web* deve ter sua história cronológica perfeitamente documentada, desde o momento de seu isolamento e fixação até o descarte, garantindo que o elemento examinado pelo perito e pelo magistrado seja idêntico ao coletado na fase investigativa.

Analisando a necessidade de parâmetros próprios para essa realidade, Saad, Rossi e Partata (2024) provocam uma reflexão indispensável sobre a autonomia desse ecossistema probatório. Os autores argumentam que a transposição automática das regras de provas físicas para o ambiente computacional é insuficiente para tutelar as garantias processuais. Conforme destacam:

> A obtenção de prova digital em processo penal exige disciplina jurídica própria, pautada por critérios técnicos que assegurem não apenas a autenticidade da fonte, mas também a auditabilidade dos métodos utilizados pelo Estado.

A ausência dessa "disciplina própria" e a quebra da cadeia de custódia geram o que a jurisprudência e a doutrina classificam como a quebra da confiabilidade da prova. Na *Dark Web*, se a polícia realiza a infiltração virtual ou a apreensão de dados de um servidor sem utilizar métodos de espelhamento que gerem uma assinatura digital única (como o algoritmo *hash*), torna-se impossível realizar a contraperícia pela defesa. Essa assimetria técnica viola o princípio do contraditório e da ampla defesa, transformando o elemento informativo em prova ilícita por derivação, contaminando toda a ação penal subsequente com base na teoria dos frutos da árvore envenenada.

Portanto, os limites para a admissibilidade das provas obtidas em ambientes virtuais profundos estão diretamente conectados à transparência estatal. O combate ao cibercrime não legitima o uso de "caixas-pretas" tecnológicas em que o perito oficial apresenta uma conclusão sem que a defesa possa auditar o caminho digital percorrido. A validação jurídica da prova extraída da *Dark Web* exige o respeito irrestrito aos protocolos legais de custódia, consagrando que a justiça da decisão penal está condicionada à confiabilidade científica dos métodos empregados na busca da verdade real.

5.1 A Quebra da Cadeia de Custódia Digital e a Teoria dos Frutos da Árvore Envenenada na Jurisprudência Pátria

A volatilidade intrínseca dos elementos informativos extraídos da *dark web* exige do Estado um rigor procedimental sem precedentes na colheita e preservação dos dados telemáticos. A introdução dos artigos 158-A a 158-F no Código de Processo Penal, por meio da Lei nº 13.964/2019 (Pacote Anticrime), positivou o instituto da cadeia de custódia, estabelecendo um conjunto de etapas indispensáveis para garantir a rastreabilidade e a incolumidade da prova. No ambiente virtual, essa exigência assume caráter mandatório, uma vez que a ausência de um registro cronológico e documentado desde o momento do isolamento do dado até a sua fase de valoração judicial impede a verificação de que o elemento examinado não sofreu adulterações.

Nesse cenário, a integridade da evidência digital colhida em ambientes de alto anonimato depende da aplicação de critérios periciais estritamente científicos, como a geração de assinaturas digitais únicas por meio do algoritmo *hash*. A falta de fixação desse código identificador ou a realização de acessos diretos aos servidores e dispositivos apreendidos sem técnicas de espelhamento adequadas inviabilizam a realização de contraperícia pela defesa. Conforme adverte Badaró (2022, p. 341), "a quebra da cadeia de custódia digital não representa mera irregularidade formal, mas sim a perda irremediável da confiabilidade da prova, retirando do magistrado a base empírica necessária para proferir um decreto condenatório legítimo".

Sob a ótica jurisprudencial, o Superior Tribunal de Justiça (STJ) tem consolidado o entendimento de que a prova obtida mediante acesso direto a dispositivos eletrônicos, sem a observância de protocolos que garantam a imutabilidade do dado, padece de vício insanável. Ao julgar o RHC 99.735/SC, a Quinta Turma do STJ reforçou a necessidade de que a extração de dados de aplicativos de mensagens seja precedida de cautelas

técnicas que assegurem a integridade da prova, sob pena de sua contaminação. A transposição desse entendimento para as investigações na *dark web* é imediata: a opacidade na atuação estatal ou a supressão de etapas de custódia como a omissão na realização de espelhamento forense retira da prova sua idoneidade técnica e jurídica.

As repercussões processuais do descumprimento desses protocolos atraem a incidência da teoria dos frutos da árvore envenenada (*fruits of the poisonous tree*), consagrada no artigo 157, § 1º, do Código de Processo Penal. Se o dado inicial colhido na internet profunda possui sua autenticidade comprometida pela quebra da cadeia de custódia, todas as provas subsequentes que dele derivarem restam irremediavelmente maculadas. Garante-se, assim, que o contraditório e a ampla defesa não sejam convertidos em meras formalidades retóricas, impondo ao Estado o ônus de demonstrar a transparência e a auditabilidade de seus métodos cibernéticos para legitimar o *jus puniendi*.

5.2 Cooperação Jurídica Internacional e a Obtenção de Provas em Servidores Estrangeiros

A natureza intrinsecamente transnacional dos delitos praticados na *Dark Web* impõe severos obstáculos à aplicação prática do princípio da territorialidade da lei processual penal, previsto no artigo 1º do Código de Processo Penal. Com frequência, um crime cibernético atinge vítimas em solo nacional, mas é executado por meio de servidores localizados em múltiplas jurisdições estrangeiras, os quais operam sob legislações de proteção de dados distintas. Essa fragmentação geográfica exige que as autoridades brasileiras recorram a mecanismos de cooperação jurídica internacional para obter a transferência legítima de dados e metadados informáticos, sob pena de violação da soberania dos Estados cooperantes.

Tradicionalmente, a obtenção de elementos probatórios situados no exterior ocorre por meio de Cartas Rogatórias ou de Tratados de Assistência Judiciária Mútua (MLAT). Todavia, esses instrumentos tradicionais foram estruturados sob a lógica da evidência física, demandando meses ou até anos para o seu cumprimento definitivo. No cenário da *Dark Web*, onde a volatilidade da prova digital permite que arquivos e registros de conexão sejam apagados ou transferidos de servidor em frações de segundo, a lentidão dos canais diplomáticos convencionais converte-se em um vetor de impunidade e de ineficácia da tutela penal.

Diante da urgência por respostas céleres, o cenário normativo nacional passou por uma importante virada com a promulgação do Decreto nº 11.491/2023, que internalizou a Convenção de Budapeste sobre o Cibercrime, estabelecendo procedimentos simplificados para a preservação imediata de dados em servidores estrangeiros. Conforme pondera Bottini (2024, p. 92), "a adesão a tratados multilaterais específicos para o ambiente digital é o único caminho para harmonizar a celeridade investigativa com as garantias de legalidade e respeito à soberania das nações". Contudo, a introdução dessas provas colhidas no exterior exige um rigoroso juízo de admissibilidade pelo magistrado nacional, verificando se os métodos de obtenção respeitaram direitos equivalentes às garantias fundamentais da ampla defesa e do contraditório.

6. METODOLOGIA

O presente estudo adota a abordagem interpretativa, porquanto busca compreender como o ordenamento jurídico brasileiro constrói sentidos e estratégias voltados aos desafios da persecução penal na repressão ao cibercrime na *Dark Web* e a salvaguarda dos direitos fundamentais. Parte-se do pressuposto de que o conhecimento jurídico resulta de interpretações e práticas institucionais situadas em contextos sociais, tecnológicos e normativos específicos (COUTINHO, 2011). O caráter exploratório da pesquisa justifica-se pelo ineditismo e pela escassa produção acadêmica nacional acerca dos desafios jurídico-penais impostos pelas redes criptografadas, o que demanda o mapeamento de práticas, a delimitação de conceitos e a identificação de padrões argumentativos em decisões judiciais, relatórios oficiais e literatura especializada (GIL, 2017).

Trata-se de uma pesquisa qualitativa, de natureza bibliográfica e documental. O delineamento empírico manifesta-se na análise de fontes secundárias acessíveis em ambiente digital, tais como livros, artigos científicos, legislações, decisões judiciais e relatórios técnicos. Todo o material é obtido em bases de dados *online*, bibliotecas virtuais, portais jurídicos e sítios institucionais. Conforme assevera Gil (2017), a pesquisa empírica pode ser realizada a partir da observação e da análise de fenômenos concretos registrados em documentos, mesmo quando esses dados são acessados remotamente. A abordagem qualitativa, portanto, privilegia a compreensão dos significados, processos e relações presentes nos discursos jurídicos e institucionais, buscando captar a complexidade do fenômeno estudado sem se restringir à quantificação estatística dos

dados (MINAYO, 2010).

A escolha da pesquisa documental digital justifica-se pela centralidade de documentos oficiais, acórdãos e relatórios técnicos enquanto registros públicos indispensáveis para a compreensão dos sentidos e das práticas produzidas no âmbito da persecução penal na *Dark Web*. O levantamento do manancial documental ocorre por meio de buscas sistematizadas em bases acadêmicas (como Google Acadêmico, SciELO e Repositórios Universitários), portais jurídicos (como os repositórios de jurisprudência do STF e STJ) e sites especializados, utilizando os descritores: "*Dark Web*", "cibercrime", "direitos fundamentais" e "investigação digital". Os documentos selecionados são catalogados e organizados em um banco de dados digital para posterior análise, observando-se rigorosos critérios de inclusão (pertinência temática direta) e exclusão (duplicidade ou tangencialidade), com estrito respeito à integridade das informações e à autenticidade das fontes.

A técnica de documentação adotada envolve a seleção criteriosa de decisões judiciais, relatórios e documentos institucionais digitais, preservando sua fidedignidade original, conforme as orientações metodológicas de Cellard (2008) e Sá-Silva, Almeida e Guindani (2009).

Para o tratamento dos dados, emprega-se a análise qualitativa de conteúdo, fundamentada nos referenciais teóricos do Direito Penal, do Direito Constitucional e da Segurança Digital. A análise de conteúdo, conforme o modelo proposto por Laurence Bardin (2016), permite compreender como as práticas institucionais e normativas se articulam na produção de sentidos sobre o combate à criminalidade oculta, especialmente no que tange à proteção das garantias fundamentais. A partir dessa abordagem, busca-se identificar regularidades, rupturas, estratégias institucionais e os reflexos das práticas de investigação e instrução processual, desvelando como o sistema jurídico brasileiro constrói e legitima determinados entendimentos sobre privacidade, segurança e cidadania no ambiente digital.

Tal perspectiva encontra respaldo na literatura especializada, a exemplo dos estudos de Cordova (2021), que destaca a importância de examinar as conexões entre o crime, a tecnologia e as consequências jurídicas das condutas no ambiente digital, especificamente no contexto da *Deep Web* e da *Dark Web*. O referido autor ressalta que a análise qualitativa de conteúdo é fundamental para captar a complexidade dos fenômenos digitais e para compreender como as respostas jurídicas se adaptam aos desafios impostos pelas novas tecnologias de informação, sem perder de vista a imperiosa

necessidade de tutela dos direitos fundamentais.

Por conseguinte, a conjugação das abordagens qualitativa, bibliográfica e documental, aliada à análise de conteúdo, permite examinar de modo crítico e aprofundado os sentidos atribuídos pelo sistema jurídico brasileiro ao enfrentamento do cibercrime na *Dark Web*, evidenciando os processos interpretativos, os discursos de poder e os impactos sobre a proteção de direitos no ambiente virtual. Essa engenharia metodológica contribui para o avanço do conhecimento científico e para o refinamento do debate sobre políticas públicas de segurança digital e garantias constitucionais.

7. CONSIDERAÇÕES FINAIS

A presente investigação permitiu analisar, de forma crítica e aprofundada, o complexo panorama que envolve os desafios da persecução penal na repressão ao cibercrime na *Dark Web* e a salvaguarda dos direitos fundamentais no ordenamento jurídico brasileiro. Diante da problemática inicialmente proposta, constatou-se que a estratificação da rede não configura apenas um fenômeno de engenharia de software, mas estabelece um verdadeiro desafio à soberania estatal, impondo uma severa crise de territorialidade e de jurisdição frente ao alto grau de anonimato e à transnacionalidade das condutas ilícitas.

Os objetivos delineados foram integralmente alcançados. Ao examinar a evolução do cibercrime, restou evidente que o ecossistema da *Dark Web* superou a fase do amadorismo técnico para se consolidar como um mercado altamente profissionalizado e lucrativo, estruturado sob a lógica do *Cybercrime as a Service* (CaaS). Essa sofisticação digital coloca em xeque a eficácia de diplomas normativos tradicionais, como a Lei Carolina Dieckmann e o Marco Civil da Internet, cujas premissas de identificação por registros de conexão mostram-se insuficientes diante de camadas complexas de criptografia e do uso de criptoativos.

A hipótese central do trabalho foi confirmada. A insuficiência normativa e a tentativa de transpor compulsoriamente as regras de captação de provas físicas para o ambiente computacional geram assimetrias que fragilizam o processo penal democrático. A atuação persecutória do Estado, embora legítima na busca pela segurança pública, encontra limites semânticos e éticos nos direitos fundamentais à privacidade, à inviolabilidade de dados e ao princípio do *nemo tenetur se detegere*. Consequentemente, práticas especulativas como o *fishing expedition* e o uso desmedido de *malwares*

governamentais sem causa provável violam a higidez constitucional e contaminam a admissibilidade dos elementos probatórios.

Ademais, o estudo evidenciou que a volatilidade intrínseca da prova digital exige o respeito rigoroso e incondicional ao instituto da cadeia de custódia, conforme positivado pelo Pacote Anticrime. A ausência de metodologias auditáveis e a falta de fixação de assinaturas digitais únicas (*hash*) impossibilitam a realização de contraperícia pela defesa, resultando na quebra da confiabilidade da prova e na sua consequente ilicitude por derivação.

Por todo o exposto, conclui-se que o enfrentamento eficiente da criminalidade na *Dark Web* não demanda o esvaziamento das garantias constitucionais, mas sim o aperfeiçoamento técnico, ético e normativo das instituições de persecução penal. Torna-se imperativa a formulação de uma disciplina jurídica própria para o processo penal digital, aliada ao fortalecimento da cooperação internacional e à capacitação de órgãos especializados. Somente por meio do equilíbrio estrito entre a eficiência investigativa e a salvaguarda da dignidade humana será possível assegurar a legitimidade democrática do sistema de justiça criminal nos ambientes virtuais de alta complexidade.

REFERÊNCIAS

BADARÓ, Gustavo Henrique. **Processo penal**. 10. ed. São Paulo: Thomson Reuters Brasil, 2022.

BARDIN, Laurence. **Análise de conteúdo**. São Paulo: Edições 70, 2016.

BASHEER, Randa; ALKHATIB, Bassel. Threats from the Dark: A Review over Dark Web Investigation Research for Cyber Threat Intelligence. **Journal of Computer Networks and Communications**, v. 2021, p. 1-21, 2021. Disponível em: https://doi.org/10.1155/2021/1302999. Acesso em: 15 maio 2026.

BASHEER, R.; ALKHATIB, G. Understanding the layers of the electronic web: Surface, Deep, and Dark Web. **International Journal of Computer Science and Information Security**, [s. l.], v. 19, n. 4, p. 12-25, 2021. Acesso em: 15 maio 2026.

BOTTINI, Pierpaolo Cruz. **Direito penal digital**: crimes cibernéticos, prova eletrônica e cooperação internacional. São Paulo: Revista dos Tribunais, 2024.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [1988]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 18 maio 2026.

BRASIL. Superior Tribunal de Justiça (6ª Turma). **Recurso em Habeas Corpus nº 99.735/SC**. Relatora: Ministra Laurita Vaz, 27 de novembro de 2018. Brasília, DF: Superior Tribunal de Justiça, 2018. Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1777437&num_registro=201801533498&data=20181212. Acesso em: 10 jul. 2026.

_____. **Decreto-Lei nº 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Brasília, DF: Presidência da República, [1941]. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 05 jun. 2026.

_____. **Decreto nº 11.491, de 12 de abril de 2023**. Promulga a Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001. Brasília, DF: Presidência da República, [2023]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11491.htm. Acesso em: 05 jun. 2026.

_____. **Lei nº 9.296, de 24 de julho de 1996**. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal [interceptação de comunicações telefônicas]. Brasília, DF: Presidência da República, [1996]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 15 maio 2026.

_____. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências [Lei Carolina Dieckmann]. Brasília, DF: Presidência da República, [2012]. Disponível em:

http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 18 maio 2026.

_____. **Lei nº 12.850, de 2 de agosto de 2013**. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal. Brasília, DF: Presidência da República, [2013]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. Acesso em: 05 jun. 2026.

_____. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil [Marco Civil da Internet]. Brasília, DF: Presidência da República, [2014]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 18 maio 2026.

_____. **Lei nº 13.964, de 24 de dezembro de 2019**. Aperfeiçoa a legislação penal e processual penal [Pacote Anticrime]. Brasília, DF: Presidência da República, [2019]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm. Acesso em: 05 jun. 2026.

_____. Superior Tribunal de Justiça. **Habeas Corpus nº 663.055/SP**. Relator: Ministro Rogerio Schietti Cruz. Sexta Turma, julgado em 22 de março de 2022. Brasília, DF: STJ, [2022]. Disponível em: https://www.stj.jus.br. Acesso em: 15 maio 2026.

_____. Supremo Tribunal Federal. **Súmula nº 145**. Não há crime, quando a preparação da polícia torna impossível a sua consumação. Brasília, DF: STF, [1964]. Disponível em: https://jurisprudencia.stf.jus.br. Acesso em: 05 jun. 2026.

CELLARD, André. A análise documental. In: POUPART, Jean et al. **A pesquisa qualitativa**: enfoques teóricos e metodológicos. Petrópolis: Vozes, 2008. p. 295-316.

CORDOVA, Rogério Goularte. **Cibercrime e direito penal**: os desafios da persecução penal na deep e dark web. Curitiba: Juruá, 2021.

COUTINHO, Clara Pereira. **Metodologia da investigação em ciências sociais e humanas**: teoria e prática. Coimbra: Almedina, 2011.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 6. ed. São Paulo: Atlas, 2017.

LOPES JR., Aury. **Direito processual penal**. 19. ed. São Paulo: SaraivaJur, 2022.

MEDEIROS, C. **Cibercrime e Direito Penal**: a nova face dos delitos virtuais. 2. ed. São Paulo: Saraiva, 2020.

MINAYO, Maria Cecília de Souza (org.). **Pesquisa social**: teoria, método e criatividade. 29. ed. Petrópolis: Vozes, 2010.

REIS, Caio Gonçalves. Crimes de virtude: Uma análise sobre a (in)eficácia da legislação e os desafios da sua persecução penal. **Jusbrasil**, 2023. Disponível em:

https://www.jusbrasil.com.br/artigos/crimes-virtuais-uma-analise-acerca-da-in-eficacia-da-legislacao-e-os-desafios-de-sua-persecucao-penal/1220973039. Acesso em: 18 maio 2026.

ROSA, Alexandre Morais da. **Guia do Processo Penal conforme a Teoria dos Jogos**. 6. ed. Florianópolis: EMais, 2020.

SAAD, M.; ROSSI, M.; PARTATA, A. A obtenção de prova digital em processo penal exige disciplina jurídica própria? **Revista Brasileira de Direito Processual Penal**, Porto Alegre, v. 10, n. 3, p. 1-28, 2024. Disponível em: https://revista.ibraspp.com.br/RBDPP/article/view/1071. Acesso em: 18 maio 2026.

SÁ-SILVA, Jackson Ronie; ALMEIDA, Cristóvão Domingos de; GUINDANI, Joel Felipe. Pesquisa documental: trilhas teóricas e metodológicas. **Revista Brasileira de História & Ciências Sociais**, [s. l.], v. 1, n. 1, p. 1-15, jul. 2009. Disponível em: https://periodicos.furg.br/rbhcs/article/view/10351. Acesso em: 18 maio 2026.

VPNOVERVIEW. As diferenças entre Surface Web, Deep Web e Dark Web. [S. l.]: **VPNOverview**, 2026. Disponível em: https://vpnoverview.com. Acesso em: 15 maio 2026.