PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
PRO-REITORIA DE GRADUAÇÃO
ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO
CURSO DE DIREITO
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO
ARTIGO CIENTÍFICO

CRIMES CIBERNÉTICOS E A INVIOLABILIDADE DE PROVAS

DELIMITAÇÃO DE CRITÉRIOS PARA GARANTIR A INTEGRIDADE DA CADEIA DE CUSTÓDIA NO ÂMBITO VIRTUAL

ORIENTANDA: GHEOVANNA SANTOS DA SILVA
ORIENTADORA: PROFª MS. ELIANE RODRIGUES NUNES

GOIÂNIA
2025

GHEOVANNA SANTOS DA SILVA

CRIMES CIBERNÉTICOS E A INVIOLABILIDADE DE PROVAS

DELIMITAÇÃO DE CRITÉRIOS PARA GARANTIR A INTEGRIDADE DA CADEIA DE CUSTÓDIA NO ÂMBITO VIRTUAL

Artigo Científico apresentado a disciplina de Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação da Pontifícia Universidade Católica de Goiás.
Profª Orientadora: Ms. Eliane Rodrigues Nunes.

GOIÂNIA
2025

GHEOVANNA SANTOS DA SILVA

CRIMES CIBERNÉTICOS E A INVIOLABILIDADE DE PROVAS

DELIMITAÇÃO DE CRITÉRIOS PARA GARANTIR A INTEGRIDADE DA CADEIA DE CUSTÓDIA NO ÂMBITO VIRTUAL

Data da Defesa: _____ de _____ de 2025.

BANCA EXAMINADORA

_____

Orientadora: Prof. Ms. Eliane Rodrigues Nunes Nota

_____

Examinador Convidado: Altamir Rodrigues Vieira Junior Nota

A minha avó, Maria Aparecida Silva (*in memoriam*), que sonhou com meu futuro, mas não pôde estar aqui para me ver vivendo-o. Espero estar te dando orgulho, vovó.

Agradeço, primeiramente, a Deus por me permitir viver meu sonho e concluir mais essa etapa.

Agradeço a minha mãe, Eliane Balbino Santos, que não só sonha para mim coisas maiores do que sequer imaginei, como também torce incondicionalmente por cada coisa que eu me proponha a fazer, vibrando por cada conquista minha.

Agradeço a meu pai, Winsthon Ilídio da Silva, que chorou comigo por meus sonhos e, mesmo de longe, vivenciou todas as minhas conquistas ao meu lado.

Agradeço minha vó, Eva de Fátima Carneiro, que é meu grande apoio em tudo, me ouvindo e se preocupando com meu bem-estar acima de qualquer coisa.

Agradeço as minhas tias, Monicc Stefânia da Silva e Lidiane Maria da Silva, que sempre estão disponíveis para toda e qualquer demanda que eu lhes traga, me ajudando em cada mínima coisa que peço. Nunca conseguirei retribuir tudo que fazem por mim.

Agradeço meu padrasto, Claudinei Rodrigues Nobre Cavalcante, que reduziu suas noites de sono nos últimos anos para que eu pudesse ir a faculdade todos os dias.

Agradeço meu namorado, Vitor Manoel Veloso Belo, que foi meu companheiro nesses anos e que, por incontáveis vezes, me ouviu falar de assuntos que não compreendia para me auxiliar em minhas dúvidas. Espero um dia retribuir o amor, companheirismo e carinho que tem por mim.

Agradeço a minha orientadora, Eliane Rodrigues Nunes, que me guiou com excelência nos caminhos desse trabalho. Jamais me esquecerei dos ensinamentos transmitidos e de seu apoio.

CRIMES CIBERNÉTICOS E A INVIOLABILIDADE DE PROVAS:
DELIMITAÇÃO DE CRITÉRIOS PARA GARANTIR A INTEGRIDADE DA CADEIA DE CUSTÓDIA NO ÂMBITO VIRTUAL

Gheovanna Santos da Silva[1]

O presente estudo pretendeu verificar como se garante a inviolabilidade das provas decorrentes dos cibercrimes. A relevância do tema se encontra na necessidade de assegurar a integridade da cadeia de custódia em relação as evidências virtuais por meio do estabelecimento de critérios seguros para garantir essa inviolabilidade. Objetivou-se demonstrar a necessidade de adaptação do Direito diante da ocorrência de delitos no âmbito virtual e/ou praticados por meio de equipamentos eletrônicos, bem como selecionar meios de se garantir a integridade das evidências digitais durante a coleta e o tratamento desses vestígios. Dessa forma, a abordagem metodológica utilizada foi o método dedutivo, mostrando-se essenciais a pesquisas bibliográfica e de campo. O estudo demonstrou a urgência de uma adaptação legislativa para acompanhar os avanços criminológicos no âmbito virtual, bem como evidenciou a necessidade de se delimitar técnicas e ferramentas a fim de asseverar a integridade das evidências digitais.

Palavras-chave: Cibercrimes; Cadeia de custódia; Inviolabilidade.

CYBERCRIMES AND THE INVIOLABILITY OF EVIDENCE:
DELIMITATION OF CRITERIA TO GUARANTEE THE INTEGRITY OF THE CHAIN OF CUSTODY IN THE VIRTUAL ENVIRONMENT

ABSTRACT

This study aimed to verify how the inviolability of evidence resulting from cybercrimes is guaranteed. The relevance of the topic lies in the need to ensure the integrity of the chain of custody in relation to virtual evidence by establishing secure criteria to guarantee this inviolability. The objective was to demonstrate the need to adapt the Law in the face of crimes occurring in the virtual environment and/or committed through electronic equipment, as well as to select means to guarantee the integrity of digital evidence during the collection and treatment of such traces. Thus, the methodological approach used was the deductive method, which has proven to be essential for bibliographic and field research. The study demonstrated the urgency of legislative adaptation to keep up with criminological advances in the virtual environment, as well as highlighted the need to define techniques and tools in order to assert the integrity of digital evidence.

Keywords: Cybercrimes; Chain of custody; Inviolability.

---

[1] Acadêmica do curso de Direito da Pontifícia Universidade Católica de Goiás, monitora da disciplina intitulada DIREITO PENAL - TEORIA GERAL DA PENA durante o segundo semestre de 2024 e o primeiro semestre de 2025. E-mail: gheovanna_santos24@hotmail.com.

SUMÁRIO

INTRODUÇÃO

O presente artigo científico possui como objeto a garantia da inviolabilidade de provas durante o processamento de crimes cibernéticos. O interesse por esse eixo temático justifica-se pela necessidade de assegurar a integridade da cadeia de custódia em relação as evidências virtuais, bem como a urgência em se delimitar os critérios seguros para garantir essa inviolabilidade.

O objetivo desse trabalho é demonstrar a necessidade de adaptação do Direito diante da ocorrência de delitos no âmbito virtual e/ou praticados por meio de equipamentos eletrônicos, bem como selecionar as técnicas e ferramentas que poderiam contribuir para garantir a inviolabilidade das provas digitais.

Para tanto, a abordagem metodológica utilizada foi o método dedutivo, mostrando-se essenciais a pesquisa bibliográfica, na medida em que forneceu um estudo teórico, embasado na lei, na jurisprudência e nos princípios constitucionais da ampla defesa e do devido processo legal, e a pesquisa de campo visto que houve uma entrevista com um jurista, especialista na área de Direito Digital, a fim de identificar os problemas e a necessidade da adaptação do direito às novas tecnologias para que se possibilite a padronização dos meios de coleta de vestígios virtuais.

Com base na descrição do tema, pretende-se realizar uma abordagem doutrinária e jurisprudencial acerca dos meios utilizados pela perícia forense para garantir que a prova digital se mantenha íntegra e inviolável durante o processamento do delito que a originou.

Este trabalho encontra-se devidamente inserido na linha de pesquisa determinada pela Pontifícia Universidade Católica de Goiás, a saber: ESTADO, RELAÇÕES SOCIAIS E TRANSFORMAÇÕES CONSTITUCIONAIS, considerando que a presente temática engloba o debate de questões referentes ao direito penal e à criminalidade.

Quanto à estrutura, este artigo científico se encontra organizado em três seções. Na primeira seção realiza-se a conceituação e classificação dos cibercrimes, bem como se apresenta a evolução histórica dos delitos cibernéticos, retratando o surgimento da Internet e a dependência gradual entre o cotidiano humano e a tecnologia. Ademais, relaciona-se ainda o crescimento exponencial das ocorrências desses delitos com o período da pandemia do COVID-19.

Na segunda seção apresenta-se sobre o Direito Digital e a posição dos crimes digitais no acervo legislativo brasileiro. Além disso, se expõe sobre o chamado direito ao esquecimento, delimitando suas raízes e o posicionamento doutrinário e jurisprudencial acerca do tema.

Por fim, na terceira seção descreve-se o conceito e a importância da cadeia de custódia na garantia do devido processo legal, apresentando as consequências da quebra de seus procedimentos e traçando sobre as dificuldades apresentadas em relação a coleta e o tratamento das evidências digitais. Finaliza-se delimitando meios de se garantir a inviolabilidade dos vestígios no âmbito virtual diante da ausência de previsão legislativa específica.

1 DELITOS CIBERNÉTICOS

O crime cibernético, ou cibercrime, pode ser definido como toda atividade ilícita desenvolvida no ambiente virtual, praticada por meio da utilização de um equipamento eletrônico ou, ainda, perpetrada contra computadores e aparelhos similares.

Visando tornar a compreensão desses delitos mais clara e eficaz, os cibercrimes podem ser classificados de duas maneiras, a primeira se refere a divisão dos crimes como puros, mistos ou comuns e a segunda categoriza entre delitos próprios ou impróprios.

Em relação a primeira forma de classificação, temos que os crimes cibernéticos puros podem ser definidos como aqueles que objetivam atingir o sistema de um dispositivo, seja violando sua parte física (*Hardware*) ou a parte lógica (*Software*). Em contrapartida, os mistos se desenvolvem com a utilização de um dispositivo telemático e do meio virtual como ferramentas para atingir os bens/valores da vítima.

Tratando-se dos delitos cibernéticos comuns, esses se caracterizam como aqueles ilícitos penais que podem, ou não, se utilizar do meio virtual como ferramenta para sua consumação.

No que diz respeito a segunda classificação, os cibercrimes próprios são os comumente chamados de “novos delitos”, caracterizados por se desenvolverem exclusivamente por meio de um dispositivo tecnológico, possuindo como fim de sua conduta o sistema operacional. Nesse tipo de delito cibernético o bem jurídico tutelado será o próprio sistema informático, abrangendo sua integralidade, confiabilidade e disponibilidade.

Por sua vez, os delitos impróprios são aqueles que podem se utilizar do meio virtual e do dispositivo tecnológico como uma forma de executar a atividade ilícita. Desse modo, o bem jurídico tutelado nessa modalidade não é o sistema informático, podendo atingir a honra, a propriedade ou a liberdade, por exemplo.

1.1 EVOLUÇÃO HISTÓRICA DOS CIBERCRIMES

Em meio a necessidade de se calcular coordenadas e trajetórias de bombas e mísseis, na década de 1960, a corrida armamentista intensificou o investimento tecnológico em busca de tornar esse processo mais ágil.

Nesse contexto, foi criada a precursora da Internet, a *Advanced Research Projects Agency Network* (ARPANET). Assim, se consagrando como a primeira rede de computadores, a ARPANET foi um projeto que visava a transmissão de dados e informações entre instalações militares.

Desse modo, em que se pese a divergência doutrinária em definir o primeiro crime cibernético, sabe-se que, em meio a esse cenário, os primeiros delitos utilizando a tecnologia envolviam espionagem e sabotagem.

Contudo, somente em 1985, após uma série de melhorias e ampliações, foi possibilitado o acesso da Internet em escala mundial. No Brasil, apenas nos anos 90, a revolução tecnológica se iniciou, sendo caracterizada por um processo lento e progressista de transformações, as quais, aos poucos, tornaram o uso comercial da Internet possível.

Em face a isso, em sua condição natural de animal político e destinado a viver em sociedade, o ser humano, agora com acesso às tecnologias em seu cotidiano, passou a investir em maneiras de satisfazer suas necessidades sociais, gerando uma série de transformações no modo em que as relações se desenvolviam a fim de facilitar a comunicação e interação a longa distância.

O crescimento exponencial dos meios tecnológicos acarretou modificações em sistemas inteiros, influenciando não só as relações dentro de uma sociedade, como também a economia global por inteira. Frente a geração contínua de tecnologias novas e mais sofisticadas, a expectativa é de, progressivamente, o mundo se tornar mais interconectado, possibilitando o atendimento, total ou parcial, de todas as necessidades humanas pela via digital.

À medida em que crescem as possibilidades de uso positivo das Internet e dos mecanismos tecnológicos e virtuais, os delitos, anteriormente ocorridos no meio bélico e militar, começam a se adaptar às constantes mudanças ocorridas no meio social.

Neste posto, torna-se imprescindível mencionar a relação entre delito e mudanças sociais destacada por Carnelluti (2001, p. 24):

> Pouco a pouco, à medida que a sociedade se adianta e, portanto, se organiza juridicamente, vão se manifestando outras formas de delito. Acrescentados na sociedade o sentido e a necessidade da ordem, multiplicam-se os preceitos penais e com eles as figuras do delito;

Em mesmo sentido, Lima (2021, p. 15), por sua vez, traça a relação e os impactos do crescimento da criminalidade em tempos de conectividade tecnológica em larga escala:

> Em um mundo hiperconectado, é fértil o espaço para a criatividade delitiva e para a atuação de novos sujeitos desestabilizadores. Estes anteriormente não se poderiam apresentar como verdadeiras ameaças à normalidade da vida humana, mas, por causa da sensibilidade e da virtualidade dos sustentáculos da comunicação e infraestrutura, podem abalar o estado de tranquilidade; podem gerar efeitos catastróficos e impactar significativamente a dinâmica regular de uma sociedade.

Assim, havendo intensa transformação na sociedade, na economia, e na forma em que os indivíduos se relacionam e utilizam os meios digitais, as práticas criminosas se modernizam para acompanhar as mudanças ocorridas, utilizando-se dos meios tecnológicos e virtuais para aprimorar suas técnicas.

Fertilizados pela possibilidade de operar de maneira global e em um suposto anonimato, os delitos cibernéticos ganham força com a inovação tecnológica gradual e infinita dos meios de comunicação e comercialização.

1.3 CRIMES DIGITAIS E A PANDEMIA DO COVID-19

O processo tecnológico, caraterizado pela celeridade de inovações, foi amplamente intensificado em 2020 com a ocorrência da pandemia do COVID-19. Assim, com a implementação do isolamento social, medida tomada para desacelerar a transmissão em larga escala do vírus, surgiu a necessidade da tecnologia se adaptar a fim possibilitar que o trabalho, as compras, o estudo e as demais atividades cotidianas fossem realizadas por via digital, promovendo assim o desenvolvimento de uma relação mais íntima e dependente entre o ser humano e a internet.

Em razão das interações se tornarem, majoritariamente, virtuais, o cenário se mostrou propício ao crescimento e à consumação das práticas ilícitas cibernéticas.

Foi nesse contexto que, em 18 de junho de 2020, o corregedor nacional de Justiça, Ministro Humberto Martins, afirmou, durante a abertura do seminário virtual Criminalidade em tempos de Covid-19: atuação do sistema de justiça, que, em que se pese a diminuição significativa de roubos e furtos com o isolamento social, houve também uma abertura de espaço para o desenvolvimento de outras práticas criminosas, como os cibercrimes.

Por sua vez, Brian O´Neal Rocha, procurador municipal de Mombaça/CE, em entrevista realizada a respeito do assunto, apresentou os possíveis motivos para o crescimento de delitos cibernéticos durante a pandemia do COVID-19:

> A pandemia do Covid-19 aumentou a ocorrência de crimes cibernéticos devido ao crescimento do uso de tecnologias digitais e à vulnerabilidade gerada pela transição para o trabalho remoto e o aumento das transações online, faltou educação digital, principalmente para quem não tinha tantas habilidades com o meio digital. A pandemia nos obrigou a avançar anos no uso das ferramentas digitais.

Outrossim, segundo o levantamento realizado pela empresa de segurança cibernética, Fortinet, nesse período pandêmico registrou-se o crescimento em larga escala de ameaças cibernéticas. Em 2021, o Brasil sofreu mais de 88,5 bilhões de ciberataques, representando um aumento de 950% em relação ao ano anterior. O cenário se mostrou mais grave no ano seguinte, sendo registrados 103 bilhões de tentativas e ameaças de ataques cibernéticos, representando cerca de 30% dos casos registrados em toda a América Latina e Caribe. (Fortinet, 2022/2023)

Visando explicar o crescimento dessas práticas delitivas, pode-se correlacionar algumas teorias aplicáveis a situação. A primeira tese, nomeada Teoria do Controle, afirma que qualquer pessoa é um criminoso em potencial, assim, desde que existam oportunidades favoráveis é possível que o crime se realize. Em seguida, tratando-se da Teoria da Escolha Racional, a ocorrência de um delito dependeria de uma análise entre custos e ganhos desencadeados com sua prática. Por sua vez, a Teoria das Atividades Rotineiras, preceitua que o criminoso age ao analisar situações rotineiras e encontrar a existência de um padrão que facilite a consumação do delito.

Em conclusão, ao analisar a situação vivenciada com a pandemia do COVID-19, torna-se evidente que o aumento na taxa de criminalidade cibernética é multifatorial, sendo a fragilidade dos usuários e as transformações ocorridas de forma precípite apontados como fatores determinantes para esse cenário.

2 DIREITO DIGITAL

Denominada como Revolução Industrial 4.0, ou Quarta Revolução Industrial, a presença constante e integrada da tecnologia em todos os aspectos da vida

humana impulsionou um processo de transformações sociais e industriais, no qual se observa a interconexão e o desenvolvimento exponencial e veloz das inovações como características principais.

Em face a isso, é cediço que, com as crescentes mudanças sociais impulsionadas pela evolução tecnológica, tornou-se indispensável que o Direito acompanhasse essas inovações em busca de garantir o respeito e proteção aos direitos fundamentais do ser humano.

À vista disso, o chamado Direito Digital surge como um ramo responsável por regular as relações e ações desenvolvidas no meio virtual, visando compreender o relacionamento entre o homem e a tecnologia, bem como promover o uso e desenvolvimento responsável dessas inovações.

Contudo, em que se pese a essencialidade desse ramo jurídico, no Brasil, temos que o avanço e desenvolvimento da informática jurídica e do Direito Digital encontra-se no estágio inicial, devido à escassa doutrina nacional e ausência de inclusão da matéria nas faculdades de direito, sendo visto como uma espécie de sub-ramo no escopo abrangente jurídico.

Nesse sentido, Pinheiro (2008, p. 29) entende que o Direito Digital seria uma evolução do próprio Direito, abrangendo assim todos os princípios fundamentais e institutos já vigentes, ao passo que introduz novos elementos em todo e qualquer ramo jurídico.

Em mesmo sentido, Araújo (2017, p. 24), define Direito Digital como “a extensão de diversos ramos da ciência jurídica, que cria novos instrumentos para atender a anseios e ao aperfeiçoamento dos institutos jurídicos em vigor”.

Entretanto, para Pereira (2003, p. 27) o Direito Digital possui todas as características para ser considerado uma disciplina autônoma, com objeto, metodologia e fontes próprias, sendo essa a justificativa utilizada para que, em diversos países, sobretudo os mais desenvolvidos, se criasse uma disciplina específica tratando desse ramo nos meios acadêmicos.

Destaca-se ainda que, com o avanço sem precedentes das novas tecnologias, torna-se urgente o aprofundamento no Direito Digital. Nesta senda, em entrevista realizada com Brian O´Neal Rocha, procurador municipal de Mombaça/CE, foi possibilitado o entendimento de que não só operadores do direito, como também estudantes na graduação, deveriam se atualizar para acompanhar os desdobramentos do Direito Digital e das novas tecnologias, dando-se ênfase na crescente influência da área

nas questões jurídicas.

Em suma, trata-se de um ramo novo, com idade estimada de duas décadas, se encontrando ainda nos estágios iniciais de desenvolvimento, onde se carece de autonomia, mas que, em razão dos impactos decorrentes das inovações tecnológicas, possui um crescimento gradual com a criação de novas normas e tipificações, sendo imprescindível o acompanhamento de seus desdobramentos.

2.1 LEGISLAÇÃO BRASILEIRA E DELITOS DIGITAIS

Em proêmio, cabe salientar que, com as modificações sociais provocadas pela Internet e pelas novas tecnologias, o Código Penal (Lei n. 2.848 de 7 de dezembro de 1940) se mostrou insuficiente para amparar novos fatos ocorridos no meio digital.

Frente a isso, em 1999, o projeto de lei n. 84, foi criado com o objetivo de dispor sobre os crimes cometidos no âmbito informático. Entretanto, em razão do receio de se restringir a privacidade ou liberdade no uso da Internet, em 2012, ao ser transformada em norma jurídica (Lei n. 12.735 de 30 de novembro de 2012) obteve veto parcial, tendo assim 17 de seus 23 artigos removidos pela Câmara de Deputados.

Ainda em 2012, em face ao fato da atriz Carolina Dieckmann ter seu computador pessoal acessado por hackers e, posteriormente, ter 36 fotos íntimas suas divulgadas na Internet pelos criminosos, a repercussão social do caso fomentou a tramitação, em tempo recorde, do projeto de lei n. 35. O referido projeto se mostrou uma alternativa ágil e simplista à demanda social, uma vez que se tipificou condutas criminosas sem enfrentar questões sobre direitos e deveres na Internet, as quais a Lei 12.735/2012 se propôs a dirimir.

Desse modo, a Lei n. 12.737/2012, também conhecida como Lei Carolina Dieckmann, quando promulgada ocasionou modificações ao Código Penal, introduzindo os artigos 154-A e 154-B, nos quais se dispõe sobre invasão de dispositivos e a ação penal nesses casos, e os artigos 266 (Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública) e 298 (Falsificação de documento particular e de cartão).

Dois anos mais tarde, foi criada a Lei n. 12.965/2014, também conhecida como Marco Civil da Internet ou Constituição da Internet, com 32 artigos e 5 capítulos, possuindo como fundamentos o respeito à liberdade de expressão e o

reconhecimento da Internet como um meio que merece regulamentação. Uma série de princípios foi pautada em seu corpo textual, em destaque a privacidade, a fiscalização e a neutralidade de rede.

Ademais, o Marco Civil da Internet foi responsável por proibir a utilização de dados dos usuários de forma diversa da permitida, exigindo das empresas presentes no âmbito virtual o esclarecimento de seus termos de uso e a realização de contratos virtuais que informassem sobre como os dados do usuário seriam coletados e usados.

Por sua vez, em 14 de agosto de 2018, foi sancionada a Lei n. 13.709, sendo comumente conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD). Em complemento ao Marco Civil da Internet, a Lei n. 13.709, nos termos de seu artigo 1º, objetivou "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.".

Assim sendo, a Lei Geral de Proteção de Dados Pessoais foi estabelecer regras para o tratamento de dados pessoais no Brasil, incluindo informações sobre como deveria ser realizada a coleta, o uso, o armazenamento, o compartilhamento e a exclusão desses dados. Além disso, foi permitido aos usuários a requisição de informações das empresas sobre seus dados, podendo questionar o motivo do armazenamento e solicitar a exclusão quando não necessários para as finalidades de sua coleta.

Por fim, tendo em vista os cibercrimes ocorridos no contexto pandêmico, cabe mencionar ainda a Lei n. 14.155/2021, a qual trouxe alterações ao Código Penal visando tornar mais graves previstos os crimes de violação de dispositivo informático (artigo 154-A), furto (artigo 155) e estelionato cometidos de forma eletrônica ou pela internet (artigo 171), bem como definiu, no parágrafo 4º do artigo 70 do Código Penal, a competência em modalidades de estelionato.

2.3 DIREITO AO ESQUECIMENTO

Aliado aos direitos de personalidade e amparado pelo princípio da dignidade da pessoa humana, o direito ao esquecimento consiste na faculdade de proibir a exposição pública de um fato verídico vexatório ou danoso a índole e privacidade do indivíduo, em razão do decurso de tempo em que ele ocorreu.

Nesta senda, se faz indispensável a delimitação do tema realizada por

Anderson Schreiber (*apud* Tepedino; Frazão; Oliva, 2019, p. 376):

> (...) o direito ao esquecimento é, portanto, um direito (a) exercido necessariamente por uma pessoa humana; (b) em face de agentes públicos ou privados que tenham a aptidão fática de promover representações daquela pessoa sobre a esfera pública (opinião social); incluindo veículos de imprensa, emissoras de TV, fornecedores de serviços de busca na internet etc.; (c) em oposição a uma recordação opressiva dos fatos, assim entendida a recordação que se caracteriza, a um só tempo, por ser desatual e recair sobre aspecto sensível da personalidade, comprometendo a plena realização da identidade daquela pessoa humana, ao apresenta-la sob falsas luzes à sociedade.

O referido direito possui suas origens no âmbito penal, sendo plenamente reconhecido no artigo 93 do Código Penal, no artigo 748 do Código de Processo Penal e no artigo 202 da Lei de Execução Penal, onde, em suma, se prevê que, salvo por requisição de juízo criminal, não serão divulgados os antecedentes criminais de um ex-detento.

Contudo, com a ampliação da disseminação de informações possibilitada pelos meios de comunicação, as discussões sobre a necessidade de se proteger os direitos de intimidade e privacidade elevaram o debate sobre o direito ao esquecimento na seara cível. Atualmente, a polêmica gira em torno do potencial lesivo futuro de uma rede mundial de computadores que eterniza as notícias e informações.

Assim sendo, no campo do direito civil, em que se pese inexistir previsão legislativa do tema, o debate doutrinário se estende a mais de uma década, sendo majoritariamente defendida a necessidade de se ter o direito ao esquecimento.

Em mesmo sentido, em razão dos danos provocados pelas novas tecnologias de informação, em 2013, na VI Jornada de Direito Civil do Conselho de Justiça Federal (CJF), foi aprovado o Enunciado 531, o qual defendia que “a tutela da dignidade da pessoa humana na sociedade da informação inclui o direito ao esquecimento”.

Entretanto, apesar do entendimento majoritário da doutrina, em 11 de fevereiro de 2021, o Supremo Tribunal Federal, no julgamento do Recurso Extraordinário n. 1.101.606/RJ, em apreciação do tema n. 786 da repercussão geral, concluiu que o direito ao esquecimento seria incompatível com a Constituição Federal. À vista do entendimento firmado pela Suprema Corte, imperiosa se faz a citação da tese firmada no referido julgamento:

> É incompatível com a Constituição a ideia de um direito ao esquecimento, assim entendido como o poder de obstar, em razão da passagem do tempo,

> a divulgação de fatos ou dados verídicos e licitamente obtidos e publicados em meios de comunicação social analógicos ou digitais. Eventuais excessos ou abusos no exercício da liberdade de expressão e de informação devem ser analisados caso a caso, a partir dos parâmetros constitucionais – especialmente os relativos à proteção da honra, da imagem, da privacidade e da personalidade em geral – e das expressas e específicas previsões legais nos âmbitos penal e cível.

Em síntese, entende-se que, diante da eternização de informações possibilitada pelos meios de comunicação digitais, a discussão em torno da necessidade de se existir um direito ao esquecimento no âmbito cível ganharam espaço na última década, definindo-o como uma garantia fundamental de proteção aos direitos de privacidade e intimidade. Contudo, sendo determinada sua incompatibilidade com a Constituição Federal, atualmente, o direito ao esquecimento se encontra restrito a esfera criminal, como amparo a ressocialização social do egresso prisional visto que impede a divulgação dos antecedentes criminais desses indivíduos.

3 A CADEIA DE CUSTÓDIA E AS PROVAS DIGITAIS

Prevista desde julho de 2014 na Portaria SENASP n. 82 e possuindo extensa exploração doutrinária, a cadeia de custódia somente foi introduzida na legislação penal brasileira com o advento da Lei n. 13.964/2019. Nos termos do artigo 158-A do Código de Processo Penal, esse instituto pode ser caracterizado como o conjunto de procedimentos utilizados, desde o reconhecimento do vestígio até seu descarte, para manter e documentar a história cronológica das provas coletadas em locais ou em vítimas de crimes, visando asseverar a autenticidade das evidências apanhadas.

Segundo Machado (2017, p. 9), “a finalidade desses procedimentos é fornecer segurança técnica e legal, quanto à certificação da origem dos vestígios, como dos níveis de confiança e excelência dos exames periciais”.

No entanto, tratando-se especificamente dos delitos cibernéticos, em razão de sua natureza imaterial, as provas digitais possem características próprias, podendo destacar a volatilidade, a suscetibilidade de clonagem, a facilidade de dispersão e a sensibilidade ao tempo de uso e necessidade de dispositivo para transmissão como elementos essenciais (Pereira, 2024).

Sobre o assunto, Padro (2014, p. 74 *apud* Silva; Barbosa, 2024, p. 6) leciona acerca da possibilidade de manipulação e adulteração de provas digitais:

> As técnicas de captação de som, imagem e até de captura de outros elementos originalmente produzidos em meio digital não estão imunes à corrupção em termos metodológicos. Muito menos há isenção de risco de manipulação do produto obtido por meios dos métodos ocultos de investigação.

Para Pereira (2024) é possível notar ocorrência de falhas nos procedimentos relativos à cadeia de custódia em delitos digitais visto que a preservação de cada prova digital ser definida conforme sua particularidade, porém, o ordenamento vigente prevê normas genéricas para seu tratamento.

Em mesmo sentido, Silva e Barbosa (2024) reconhecem a necessidade de uma cadeia de custódia mais específica para elementos digitais, com regras próprias para a produção, admissão e valoração dessas evidências, uma vez o atual arcabouço jurídico demonstra a inexistência de previsão e detalhamento legal do manejo e preservação das provas digitais.

Merece destaque ainda, os comentários do procurador municipal de Mombaça/CE, Brian O´Neal Rocha, que, em entrevista sobre o tema, ressaltou que a padronização nos meios de coleta e preservação de provas digitais "traria benefícios significativos ao processo criminal, garantindo maior segurança, confiabilidade e uniformidade na análise das provas". Sob um olhar empírico, O´Neal mencionou ainda que, em sua atuação no ano de 2024, notou que o processo está mais dinâmico, com a maior aceitação de meios de provas digitais, como prints, desde que contextualizados com links e harmônicos com outras provas.

À vista do colecionado, é possível compreender que, apesar da essencialidade de se resguardar a adulteração de vestígios criminais, a legislação vigente não fornece disposições sobre meios de se garantir a integridade da cadeia de custódia em delitos cibernéticos, inexistindo padronização sobre como os procedimentos para asseverar a autenticidade de uma prova digital deveriam ocorrer.

3.1 CONSEQUÊNCIAS JURÍDICAS DA QUEBRA DA CADEIA DE CUSTÓDIA

O sistema processual penal brasileiro é revestido de princípios constitucionais para que se resguarde os direitos e garantias fundamentais do indivíduo

enquanto impõe limites ao arbítrio estatal, dentre eles o princípio do devido processo legal, previsto no artigo 5°, inciso LIV, da Constituição da República Federativa do Brasil de 1988, visa garantir aos cidadãos um processo justo e adequado.

Assim sendo, para a garantia de um justo processamento criminal, a observância à licitude do acervo probatório é um instrumento essencial para que não haja abusos por parte da acusação. Nesta senda, a preservação da cadeia de custódia se caracteriza como o meio de asseverar que as provas oriundas de delitos não formam obtidas de forma ilícita ou adulteradas.

Desse modo, sendo constatada a quebra da cadeia de custódia, torna-se incerta a confiabilidade na autenticidade e integridade dos vestígios criminais. O entendimento doutrinário se firma no sentido de que a quebra da cadeia de custódia acarretaria sua ilicitude e, consequentemente, em sua exclusão do processo criminal.

Ademais, em conformidade com a Teoria dos Frutos da Árvore Envenenada, oriunda da jurisprudência norte-americana, e com o artigo 157 do Código de Processo Penal, não só a prova ilícita seria considerada inadmissível, mas também aquela obtida por derivação, ou seja, por meio de informações ou elementos declarados ilícitos.

Por outro lado, sob a ótica do Superior Tribunal de Justiça (STJ), verifica-se que os efeitos da quebra da cadeia de custódia não levariam necessariamente à exclusão imediata da prova, exigindo-se que cada caso seja analisado de forma cuidadosa.

Nessa perspectiva, em casos de falhas graves, como adulteração, perda ou impossibilidade de rastrear a posse da prova, ou ainda quando a falha prejudicar a defesa, o resultado seria a exclusão da evidência, porém, se tratando de falhas menores, como inconsistências na documentação, não seria determinada a exclusão, em razão de não comprometer a validade, a autenticidade e integridade da prova (Silva, Puhl, 2024).

Menciona-se, por fim, que, sendo constatada dúvida em relação a autenticidade ou integridade das provas, deve-se aplicar o princípio *in dubio pro reo*, sendo a absolvição a medida mais adequada visto que a liberdade está acima da pretensão punitiva do Estado.

3.2 PROPOSTAS DE MEIOS PARA GARANTIR A INVIOLABILIDADE DE PROVAS DIGITAIS

Em face ao colecionado anteriormente, é notória a ausência de previsão normativa sobre as provas digitais no sistema processual penal brasileiro. Assim, sendo, a coleta e o tratamento dos vestígios digitais são realizados de forma análoga aos procedimentos em provas físicas, o que não se mostra adequado visto as peculiaridades das evidências virtuais.

Nesta senda, frente a lacuna legislativa, a doutrina processual penal tem adotado e recomentado a *computer forensics*, na qual, de acordo com o *National Institute for Standard and Technology* (NIST), deverá ser desenvolvida em quatro distintas fases para garantir a inviolabilidade probatória.

A primeira fase, nomeada de coleta, é de extrema importância para a garantia da cadeia de custódia, se qualificando como o momento em que, dentro de uma área isolada, se tem a apreensão de aparelho eletrônicos, a identificação, classificação e registro dos dados digitais.

Nessa etapa, a coleta pode se dar de duas formas: a quente (*online*) e a frio (*offline*). Em relação a primeira forma, essa será aplicada durante a coleta de dados voláteis e não voláteis de um computador ainda em funcionamento, sendo os primeiros aqueles presentes apenas na memória RAM e perdidos após o desligamento do sistema, e os segundos aqueles que permanecem a longo prazo, podendo ser recuperados após o desligamento. Já a segunda, também conhecida como análise post-mortem, diz respeito a coleta em aparelhos desligados, devendo mantê-los nesse estado e realizar a documentação e fotografia de todos os periféricos, identificando possíveis unidades removíveis.

Ainda nesse primeiro momento, visando comprovar a inviolabilidade dos vestígios, recomenda-se que o ambiente e os dispositivos que virão a ser apreendidos sejam fotografados antes e após a coleta.

Aliás, se faz imprescindível também que os cabos existentes no local sejam numerados, incluindo cabos de força, antes do desmonte, bem como que as evidências sejam etiquetadas e lacradas em envelope *starlock.*

Destaca-se que, durante a etiquetação das provas, o uso da técnica de algoritmo HASH é indicado pelos tribunais, uma vez que ele contém informações de data, hora e quem foi o responsável pela aquisição, sendo registrado cada novo

acesso aos vestígios coletados. Acerca do HASH, Silva e Barbosa (2024, p. 16) comentam:

> Referido código eletrônico garante a inalterabilidade dos dados apreendidos, indicando *bit* a *bit* exatamente qualquer alteração ocorrida, pois gera um código *hash* diferente, indicando que até aquele momento o código era um e foi alterado para outro. Diante desta alteração é possível indicar em qual momento houve a alteração e preservar os elementos de prova ou até mesmo resgatar de forma idônea.

Em relação a segunda fase, essa se qualifica como o exame do material colhido, compreendendo o momento em que ferramentas e técnicas forenses são executadas para localizar, filtrar, identificar e extrair informações relevantes dos dados coletados, sendo necessário que todos os procedimentos e a metodologia utilizada sejam documentados.

Ressalta-se que, nessa etapa, verifica-se a integridade das embalagens que guardam as evidências e realiza-se a identificação de cada item enviado para a perícia, com a descrição de seu estado geral e a documentação de qualquer alteração que possa alterar o conteúdo.

Ademais, tratando-se especificamente de discos rígidos, esses devem possuir etiqueta própria, com marca, modelo, capacidade e número de série identificados, sendo realizada a duplicação pericial das mídias.

Por sua vez, a terceira fase, denominada análise, é o momento em que os resultados dos exames serão analisados a fim de se obter informações úteis acerca de questões levantadas na primeira e segunda fase.

Finaliza-se com a quarta fase, chamada de relatório, onde se elabora um laudo pericial contendo o relato minucioso dos procedimentos, da metodologia e das ferramentas utilizadas, bem como se apresenta a descrição dos resultados encontrados durante a análise, possibilitando assim o entendimento da sequência de eventos aplicados as evidências encontradas. Essa etapa se qualifica como essencial para a comprovação de que as provas se mantiveram invioláveis e que a cadeia de custódia foi garantida durante a realização da perícia forense.

À vista de todo o exposto, entende-se que, diante da inexistência de previsão legislativa sobre a coleta e o tratamento das provas digitais, a utilização da *computer forensics* se mostra eficaz para garantir a integridade das evidências coletadas após constatada a ocorrência de um delito cibernético.

CONCLUSÃO

O presente estudo partiu da análise de instrumentos e ferramentas disponíveis para asseverar a inviolabilidade das provas obtidas a partir da ocorrência de um delito cibernético.

Assim sendo, objetivou-se com esse trabalho conhecer questões relacionadas aos delitos ocorridos no âmbito virtual, explorando sua classificação, peculiaridades e causas de aumento nos últimos anos, bem como buscou-se investigar os procedimentos aplicáveis a coleta e ao tratamento de evidências digitais a fim de asseverar a integridade da cadeia de custódia.

A pesquisa mostrou que o crescimento exponencial das inovações tecnológicas acarretou modificações em sistemas inteiros, influenciando as relações desenvolvidas em âmbito global, contudo, a medida em que o mundo se torna mais conectado, se possibilita, não só o uso da tecnologia de forma positiva, como também a adaptação de criminosos ao meio virtual, encarando-o como um novo cenário para o desenvolvimento de delitos.

Em relação ao apanhado legislativo, compreende-se que a tipificação dos cibercrimes, por si só, mostra-se insuficiente para seu combate, sendo necessário a previsão legal de meios de coleta e tratamento dos vestígios digitais, uma vez que a quebra da cadeia de custódia acarreta diretamente na credibilidade e veracidade do material probatório apresentado em juízo.

Por sua vez, diante da lacuna legislativa, a doutrina tem adotado e recomentado a *computer forensics* como referência para o tratamento de provas virtuais, delimitando quatro fases para asseverar a integridade da cadeia de custódia: coleta, exame, análise e relatório.

À vista de todo o colecionado, demonstrou-se a urgência de uma adaptação legislativa para acompanhar os desdobramentos criminológicos ocasionados pelo advento das novas tecnologias, visando definir, de forma padronizada, técnicas e ferramentas que poderiam contribuir para a garantia da integridade das evidências digitais durante a investigação de um cibercrime.

REFERÊNCIAS

ARAÚJO, Cláudio Rodrigues. **Crimes Virtuais.** Belo Horizonte: Editora Expert, 2023.

ARAÚJO, Marcelo Barreto de. Comércio eletrônico; Marco Civil da Internet; Direito Digital. **Confederação Nacional do Comércio de Bens, Serviço e Turismo**. Rio de Janeiro: 2017.

BRASIL. **[Constituição (1988)]**. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, [2023]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 02 mar. 2025.

BRASIL. **Decreto-Lei nº 2.848, de 07 de dezembro de 1940.** Código Penal. Rio de Janeiro, RJ: Presidência da República, [1991]. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 02 mar. 2025.

BRASIL. **Decreto-Lei nº 3.689, de 3 de outubro de 1941.** Código de Processo Penal. Rio de Janeiro, RJ: Presidência da República, [2024]. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 02 mar. 2025.

BRASIL. **Lei nº 7.210, de 11 de julho de 1984.** Institui a Lei de Execução Penal. Brasília, DF: Presidência da República, [2024]. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l7210.htm. Acesso em: 03 mar. 2025.

BRASIL. **Lei nº 12.735, de 30 de novembro de 2012**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Brasília, DF: Presidência da República, [2012]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 03 mar. 2025.

BRASIL. **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. Brasília, DF: Presidência da República, [2012]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 03 mar. 2025.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, [2021]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-

2014/2014/lei/l12965.htm. Acesso em: 03 mar. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 03 mar. 2025.

BRASIL. **Lei nº 14.155, de 27 de maio de 2021**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Brasília, DF: Presidência da República, [2021]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 03 mar. 2025.

Brasil sofreu mais de 88,5 bilhões de tentativas de ataques cibernéticos em 2021. **Fortinet**, 2022. Disponível em: https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2022/fortiguard-labs-relatorio-ciberataques-brasil-2021. Acesso em: 20 nov.2024.

BRASIL. Supremo Tribunal Federal (Décima Quinta Câmara Cível do Tribunal de Justiça do Estado do Rio de Janeiro). Recurso Extraordinário 1.010.606/RJ. Caso Aída Curi. Direito ao esquecimento. Incompatibilidade com a ordem constitucional. Recorrente: Nelson Curi e Outro (A/S). Recorrido: Globo Comunicação e Participações S/A. Relator: Min. Dias Toffoli, 11 de fevereiro de 2021. Disponível em: https://jurisprudencia.stf.jus.br/pages/search?classeNumeroIncidente=%22RE%201010606%22&base=acordaos&sinonimo=true&plural=true&page=1&pageSize=10&sort=_score&sortBy=desc&isAdvanced=true. Acesso em: 02 mar. 2025.

CARNELUTTI, Francesco. **Como nasce o Direito.** Belo Horizonte: Líder Cultura Jurídica, 2001.

Crime cibernético tomou lugar de roubos e furtos na pandemia, diz ministro Humberto Martins. **STJ**, 2020. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/Crime-cibernetico-tomou-lugar-de-roubos-e-furtos-na-pandemia--diz-o-ministro-Humberto-Martins.aspx. Acesso em: 20 nov. 2024.

DEMENTSHUK, Marcia. **Pássaros Voam Em Bando: a história da internet do século XVIII ao século XXI**. João Pessoa: Editora ANID, 2019.

FERNANDEZ, Luis Gustavo Santos. **Análise forense de intrusões em sistemas computacionais.** Trabalho de Conclusão de Curso (Graduação em Engenharia da

Computação) - Faculdade de Tecnologia e Ciências, Centro Universitário de Brasília (UNICEUB), Brasília, 2009.

Fortinet relata que a América Latina foi alvo de mais de 360 bilhões de tentativas de ataques cibernéticos em 2022. **Fortinet**, 2023. Disponível em: https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2023/fortiguard-labs-reports-destructive-wiper-malware-increases-over-50-percent. Acesso em: 14 set. 2024.

LIMA FILHO, Paulo Roberto Aguiar de. O Direito Penal na Quarta Revolução Industrial: A expansão razoável frente aos crimes cibernéticos. **Delictae: Revista De Estudos Interdisciplinares Sobre O Delito**. v.6, n. 10, p. 8-12, 2021. ISSN 2526-5644.

MACHADO, Michelle Moreira. IMPORTANCIA DA CADEIA DE CUSTÓDIA PARA PROVA PERICIAL. **Revista Criminalística e Medicina Legal**, v.2, n. 1, 2017. ISSN 2526-0596

MENDES, Beatriz Ribeiro Soares Mendes; FERREIRA, Ingrid de Oliveira; SANTOS, Jorge Gabriel Cruz dos. A influência da pandemia do COVID-19 no aumento dos crimes cibernéticos. **JusBrasil**, 2021. Disponível em: https://www.jusbrasil.com.br/artigos/a-influencia-da-pandemia-do-covid-19-no-aumento-dos-crimes-ciberneticos/1308143695. Acesso em: 20 nov. 2024.

PEREIRA, Marcelo Cardoso. **Direito à Intimidade na Internet**. Juruá Editora, 2003.

PEREIRA, Ketelyn Santos. **A cadeia de custódia e a perícia técnica nas provas digitais como instrumento de garantia dos direitos fundamentais.** Trabalho de Conclusão de Curso (Graduação em Direito) - Faculdade de Direito, Universidade Federal de Mato Grosso do Sul, Campo Grande, 2024.

PIMENTEL, José Eduardo de Souza. Introdução ao Direito Digital. In: **Revista Jurídica da Escola Superior do Ministério Público de São Paulo**, São Paulo, v. 13, n.1, p. 16-39, 2018. ISSN: 2316-6959.

PINHEIRO, Patricia Peck. **Direito digital**. 2. ed. São Paulo: Saraiva, 2008.

ROCHA. Brian O'Neal. **Manual Sistematizado de Direito Digital.** 2º Ed. Independently Published, 2023.

SILVA, Arthur Saatkamp da; PUHL, Eduardo. Efeitos da inobservância da cadeia de custódia sob à ótica do Superior Tribunal de Justiça (STJ). **Academia de Direito**, v. 6, p. 3740-3757, 2024. ISSN: 2763-6976.

SILVA, Danilo Bacarin; BARBOSA, Rodrigo de Sá. PROVAS DIGITAIS E A CADEIA DE CUSTÓDIA NO RHC 143.169. **Revista Contemporânea**, v. 4, n. 12, p. 01-23, 2024. ISSN: 2447-0961.

TEPEDINO, G; FRAZÃO, A; OLIVA, M.D. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.