FACULDADE EVANGÉLICA DE GOIANÉSIA

CURSO DE GRADUAÇÃO EM DIREITO

INVESTIGAÇÃO E ATUALIZAÇÃO: Abordando a Complexidade dos Crimes Cibernéticos na Sociedade Moderna

Karolaine Rayala Balsanulfo Araujo

Stephani Reis Oliveira Couto

Goianésia/Go

2023

Karolaine Rayala Balsanulfo Araujo
Stephani Reis Oliveira Couto

INVESTIGAÇÃO E ATUALIZAÇÃO: Abordando a Complexidade dos Crimes Cibernéticos na Sociedade Moderna

Trabalho de conclusão de curso apresentado à Faculdade Evangélica de Goianésia (FACEG), em nível de bacharel, como requisito parcial para obtenção do título de Bacharel em Direito
Orientador: Profa. Esp. Sara Moraes Vieira

Goianésia/Go
2023

FOLHA DE APROVAÇÃO

INVESTIGAÇÃO E ATUALIZAÇÃO: Abordando a Complexidade dos Crimes Cibernéticos na Sociedade Moderna

Este Artigo Científico foi julgado adequado para a obtenção do título de Bacharel em Direito e aprovado em sua forma final pela banca examinadora da Faculdade Evangélica de Goianésia/GO- FACEG

Aprovada em_____, de _____ de 2023

Nota Final_____

Banca Examinadora

Prof.ª Esp. Sara Moraes Vieira

Orientadora

Prof. Me. Jean Carlos Moura Mota

Professor convidado 1

Prof. Ma. Luana de Miranda Santos

Professor convidado 2

INVESTIGAÇÃO E ATUALIZAÇÃO: Abordando a Complexidade dos Crimes Cibernéticos na Sociedade Moderna

INVESTIGATION AND UPDATE: Addressing the Complexity of Cybercrime in Modern Society

Karolaine Rayala Balsanulfo Araujo [1]
Stephani Reis Oliveira Couto [2]
Sara Moraes Vieira [3]

[1] Discente do curso de Direito da Faculdade Evangélica de Goianésia- e-mail:
[2] Discente do curso de Direito da Faculdade Evangélica de Goianésia- e-mail:
[3] Docente do curso de Direito da Faculdade Evangélica de Goianésia- e-mail:

Resumo:
O estudo apresentado visa compreender a complexidade do ambiente digital e como os crimes cibernéticos geram problemas na obtenção de provas e em seu combate pelos órgãos de segurança pública. O estudo apresentado se justifica na intenção de compreender como houve uma evolução e um processo histórico e legislativo para buscar a proteção da sociedade perante este moderno meio de cometimento de crimes. O problema de pesquisa busca responder à seguinte indagação: como o Estado se atualiza e age diante da criminalidade cibernética? O objetivo geral do estudo é compreender as atualizações e ações do poder público frente aos crimes cibernéticos. Já os objetivos específicos são: em primeiro lugar, analisar a evolução histórica das normas de proteção digital; em segundo lugar, examinar as formas de obtenção de provas nos crimes digitais; e em terceiro lugar, apresentar os avanços tecnológicos no âmbito do poder público. A metodologia de pesquisa adotada foi um estudo bibliográfico, que envolveu a análise de obras científicas sobre o tema e suas informações. Trata-se de uma pesquisa qualitativa, focada em informações iniciais sobre a temática, caracterizando-se como pesquisa exploratória. As considerações do estudo apontam para uma atualização em curso por parte dos órgãos de segurança, embora exista uma clara dificuldade em obter provas e garantir a cadeia de custódia no processo de persecução penal.

Palavras-Chave: Direito; Crime; Digital; Segurança.

Abstract:
The study presented aims to understand the complexity of the digital environment and how cybercrimes create problems in obtaining evidence and combating it by public security agencies. The study presented is justified with the intention of understanding how there was an evolution and a historical and legislative process to seek the protection of society in the face of this modern means of committing crimes. The research problem seeks to answer the following question: how does the State update itself and act in the face of cybercrime? The general objective of the study is to understand the updates and actions of public authorities in the face of cybercrimes. The specific objectives are: firstly, to analyze the historical evolution of digital protection standards; secondly, examine the ways of obtaining evidence in digital crimes; and thirdly, present technological advances within the public sector. The research methodology adopted was a bibliographic study, which involved the analysis of scientific works on the topic and their information. This is qualitative research, focused on initial information on the topic, characterized as exploratory research. The study's considerations point to an ongoing update by security agencies, although there is a clear difficulty in obtaining evidence and guaranteeing the chain of custody in the criminal prosecution process.

keywords: Right; Crime; Digital; Security.

INTRODUÇÃO

Os crimes cibernéticos são aqueles que são praticados por meio do uso de tecnologias da informação e comunicação, como computadores, smartphones e redes de internet. Esses crimes são cada vez mais comuns, pois a tecnologia está cada vez mais presente em nossas vidas (Zambonato, 2022).

Neste sentido, a atuação do Estado em seu papel de proteção e punição, passa a ser necessário, demandando investigações, litigância e uma série de outras ações para coibir, impedir e punir crimes virtuais. Ocorre que estes tipos de crimes não são de fácil investigação, levando a uma consequente dificuldade de persecução penal e a punição de seus autores (Zambonato, 2022).

Assim, considerando tais informações, o estudo apresentado se justifica na intenção de compreender como houve uma evolução e um processo histórico e legislativo para buscar a proteção da sociedade perante este moderno meio de cometimento de crimes. Ainda além, o estudo visa compreender a dificuldade da obtenção de provas e os recursos contemporâneos para driblar tais dificuldades.

O estudo busca compreender como o meio digital possibilita um fácil anonimato, acarretando em cometimento de crimes de forma anônima e frustrando a percussão penal; criando a necessidade do Estado em se esforçar e se atualizar para proteger a sociedade. Neste sentido, sobre o problema de pesquisa, busca-se responder em: Como o Estado se atualiza e age em face da criminalidade cibernética?

Visando responder este problema de estudo, o objetivo geral do estudo é compreender as atualizações e atuações do poder público em face dos crimes cibernéticos. Já os objetivos específicos são, em primeiro, analisar a evolução histórica das normas de proteção digital, em segundo, análise das formas de obtenção de provas nos crimes digitais, e em terceiro, apresentar os avanços tecnológicos no poder público.

O estudo teve como metodologia de pesquisa um estudo bibliográfico, qualitativo e quantitativo, de pesquisa exploratória inicial, analisando obras cientificas sobre o tema e suas informações. Uma pesquisa em principal qualitativa, focada em informações iniciais sobre a temática.

O estudo é dividido em três distintos tópicos, inicialmente um recorte histórico sobre o nascimento das normas de proteção digital e suas atuais conjunturas. Em

segundo tópico o estudo analisa a obtenção de provas em crimes no meio digital. Em terceiro tópico o estudo analisa e expõe os avanços tecnológicos nas delegacias especializadas.

1. RECORTE HISTÓRICO E O NASCIMENTO DAS NORMAS DE PROTEÇÃO DIGITAL

A proteção digital tem se tornado uma preocupação cada vez mais relevante na era da informação e da tecnologia, com a crescente dependência de sistemas digitais e a expansão da internet têm gerado uma necessidade premente de normas e regulamentos, que assegurem a segurança e a privacidade dos dados e informações transmitidos e armazenados eletronicamente (Tremel, Nascimento, 2020).

Neste contexto, é importante analisar a origem e a evolução das normas de proteção digital, com um foco especial na criação de normas brasileiras, os pontos principais das primeiras normas de proteção digital e seus diversos motivos de criação.

A origem das normas de proteção digital remonta ao surgimento dos primeiros sistemas de computadores e redes de comunicação. Inicialmente, essas normas eram escassas e fragmentadas, refletindo a falta de consciência sobre os riscos associados à disseminação da tecnologia digital. No entanto, à medida que os sistemas digitais se tornaram cada vez mais extensos, presentes no dia-a-dia e vitais para a sociedade, a necessidade de normas de proteção digital tornou-se evidente (Doneda, 2020).

Assim, é comum uma maior necessidade de regulamentação de meios de comunicação digital, protecionismo estatal e até mesmo uma real interferência do Estado no processo de supervisão de meios digitais. Isto ocorre, em razão do uso frequente de ambientes virtuais no cotidiano da população mundial (Doneda, 2020).

Como aponta Bioni (2020) os ambientes virtuais e as ferramentas digitais nasceram como simples ferramentas de apoio, durante o século XX, sendo disseminadas no mundo comum no final da década e 90. Ao passo que, na atualidade é uma parte essencial da comunicação, tornando necessária a interferência do Estado para regular as relações no meio digital.

A origem de grande parte das normas digitais, remonta o direito Estadunidense, tendo uma série de normativas e legislações que visavam a proteção das comunicações por telefone ou por outros meios de comunicação. Sendo as primeiras normas processos gerais de proteção de comunicação (Doneda, 2020).

Nos Estados Unidos, a proteção digital é abordada por meio de uma combinação de leis estaduais e federais. A Lei de Proteção de Dados Pessoais do Consumidor da Califórnia (CCPA), por exemplo, é uma das leis estaduais mais abrangentes dos EUA e regula a coleta e o uso de dados pessoais (Doneda, 2020).

Na legislação que aborda as telecomunicações, existem disposições relacionadas aos dados pessoais. *O Cable Communications Policy Act* (CCPA), de 1984, estabelece uma série de direitos para os assinantes de serviços de televisão a cabo em relação às informações pessoais deles. Este ato obriga as empresas que fornecem esses serviços a enviar anualmente aos assinantes um relatório detalhado sobre as informações pessoais que possuem e como essas informações são utilizadas (Tremel, Nascimento, 2020).

Além disso, elas são proibidas de coletar informações pessoais sobre o uso do serviço que não sejam estritamente necessárias para a operação do sistema, a menos que obtenham a autorização expressa do assinante por meio de um sistema de opção de exclusão (*opt-out*)

Além disso, os Estados Unidos ‘promulgaram várias leis federais, como a Lei de Privacidade do Consumidor de Comunicações (CCPA), a Lei de Proteção à Privacidade das Comunicações Eletrônicas (ECPA) e a Lei de Sigilo de Comunicações (CFAA), que tratam de questões relacionadas à proteção de dados e à segurança cibernética (Blum, 2020).

Estas normas americanas surgiram no ápice da comunicação telefônica americana, sendo desenvolvidas genericamente com a intenção de proteger as telecomunicações, não devidamente preparadas para a modernidade e a revolução digital dos cybers espaços atuais (Blum, 2020).

Em nível internacional, *o General Data Protection Regulation* GDPR da União Europeia tem influenciado significativamente a abordagem de outros países à proteção de dados pessoais. Vários países, como Canadá e Japão, adotaram regulamentações semelhantes inspiradas no GDPR (Basan, 2021).

A GDPR tinha como objetivo principal proteger os direitos e liberdades fundamentais das pessoas físicas no que diz respeito ao tratamento de dados

pessoais. Ela estabeleceu regras rigorosas sobre como as organizações devem coletar, processar e armazenar dados pessoais, garantindo que os indivíduos tenham controle sobre suas informações (Basan, 2021).

Tal norma também gerou uma série de mecanismos que permitiu uma cooperação entre empresas privadas e órgãos nacionais e internacionais no combate a crimes cometidos em meio digital. Criando uma ação internacional no combate aos abusos de meios digitais para anonimato de criminosos.

No contexto do direito brasileiro, a evolução das normas de proteção digital pode ser dividida em várias fases, tendo momentos que não existia ação do Estado sobre o ambiente digital, a aplicação de normas por interpretação, a criação das primeiras normas e o tempo contemporâneo atual em que se busca a criação de um código digital (Basan, 2021).

No Brasil o meio digital se manteve como pouco regulamento até meados da segunda década do século XXI, existindo apenas normas comuns para serem aplicadas ao meio digital. Muito embora uma série de normas tenham sido propostas na Câmara federal e Senado, a inovação legislativa caminhava a passos cursos (Tremel, Nascimento, 2020).

Somente em 2012 com a aprovação da Lei nº 12.737/2012 que houve surgiu uma inovação, causada por um grande escândalo e vazamento de fotos intimas. Esta lei, conhecida como Lei Carolina Dieckmann, representou um marco importante na regulamentação das atividades cibernéticas no Brasil. Ela tipifica crimes digitais, como invasão de sistemas e divulgação não autorizada de dados (Tremel, Nascimento, 2020).

Muito embora a maior parte da norma 12.737/2012 seja apenas uma especialização de quesitos que já existiam no código penal ou em outras normas esparsas, é evidente que esta foi a primeira inovação específica em quesito de proteção no meio digital, visando a punibilidade para casos complexos como a invasão de dispositivos de informática (Tremel, Nascimento, 2020).

A Lei Carolina Dieckmann, representou um marco significativo na regulamentação dos crimes cibernéticos no Brasil, esta legislação acarretou uma série de inovações no sistema jurídico brasileiro, com o objetivo de abordar as crescentes ameaças e desafios apresentados pelo mundo digital (Tremel, Nascimento, 2020).

O Brasil, como muitos outros países, enfrenta uma crescente onda de crimes cibernéticos, incluindo fraudes financeiras, crimes contra a honra, invasões de

sistemas, disseminação de malware, pornografia infantil, entre outros. Essas atividades ilícitas têm um impacto significativo na economia, na privacidade dos indivíduos e na segurança nacional.

Neste ínterim, a Lei 12.737/2012 foi o primeiro marco protetivo para o meio digital e contraponto os avanços da criminalidade no meio digital. A Lei nº 12.737/2012 introduziu alterações importantes no Código Penal Brasileiro e no Código de Processo Penal para abordar questões relacionadas à cibersegurança e à repressão aos crimes cibernéticos. A lei definiu novos tipos penais, como a invasão de dispositivos informáticos alheios, a divulgação de informações sigilosas e a obtenção não autorizada de dados pessoais. A legislação estabeleceu penas mais severas para os crimes cibernéticos quando cometidos contra autoridades públicas ou em casos de divulgação de informações pessoais (Bioni, 2020).

A Lei Carolina Dieckmann também tratou da admissibilidade de provas obtidas digitalmente em processos judiciais, estabelecendo regras específicas para a coleta e a apresentação de evidências eletrônicas. A lei permitiu uma maior cooperação entre o Brasil e outros países no combate aos crimes cibernéticos, incluindo a possibilidade de extradição de suspeitos (Tremel, Nascimento, 2020).

A Lei nº 12.737/2012 teve um impacto significativo na abordagem do Brasil em relação aos crimes cibernéticos. Ela proporcionou uma base legal sólida para a investigação e a persecução desses delitos, ao mesmo tempo em que incentivou a conscientização sobre a importância da cibersegurança (Bioni, 2020).

A legislação também teve um efeito repressivos, uma vez que aumentou as penalidades e as consequências legais para os infratores. Além disso, a Lei Carolina Dieckmann incentivou a cooperação entre as autoridades brasileiras e internacionais, fortalecendo a capacidade de combate aos crimes cibernéticos que transcendem as fronteiras nacionais (Tremel, Nascimento, 2020).

Em 2014 ainda adveio o Marco Civil da Internet, através da Lei nº 12.965/2014, este marco legal estabelece princípios fundamentais para o uso da Internet no Brasil, incluindo a neutralidade da rede e a proteção da privacidade dos usuários. Outro ponto marcante para garantir a proteção estatal a privacidade nas redes, pode-se ressaltar a melhoria de visibilidade dos crimes digitais, cometidos diante do anonimato que é facilmente propiciado por meios digitais (Basan, 2021).

> O Marco Civil da Internet – Lei 12. 965/2014 – também abordou a proteção de dados em alguns aspectos, sendo o principal deles no inciso III do art. 3º, elegendo-o como um princípio do uso da internet no Brasil. Entre os direitos do usuário, estão a inviolabilidade de sua vida privada – condição para pleno exercício do direito de acesso –; o sigilo de suas comunicações; as informações claras, inclusive sobre a proteção de dados pessoais, cujo uso é restringido à finalidade informada; e o necessário consentimento prévio para coleta e armazenamento de dados pessoais e exclusão desses sob requerimento. O art. 11 assegura a aplicação da legislação brasileira para proteção dos dados quando ao menos uma das atividades de tratamento seja realizada no Brasil. (Tepedino, 2019, p. 28).

Estas normas diversas criadas para o desenvolvimento da proteção no meio digital, permitiram que o processo de punição de crimes ocorresse de forma mais ágil, com a facilitação de meios regulamentários. Em especial a Lei 12.737/2012, pois foi um dos primeiros pontos que garantiam a punição específica, levando-se em consideração os crimes que dependiam de uma ampla interpretação jurídica (Blum, 2020).

É certo que a norma brasileira foi fortemente influenciada por marcos estrangeiros e especialmente por polêmicas nacionais, porém, até a atualidade o processo de proteção no meio digital e combate aos crimes cibernéticos não é perfeito e até considerado amplamente falho, com grandes problemas para o combate ao anonimato e obtenção de provas.

Desta forma, embora normas complexas venham se formando no ordenamento jurídico brasileiro, regulamentando os crimes digitais, percebe-se a dificuldade na obtenção de provas nos crimes cometidos no meio digital, ocasionando um fator de empecilho na punibilidade destas infrações.

2. A OBTENÇÃO DE PROVAS DE CRIMES NO MEIO DIGITAL

Considerando as informações apresentadas anteriormente, urge o questionamento sobre como se dá a obtenção de provas de crimes e delitos no meio digital. Sendo o meio digital tão complexo e facilitador do anonimato, de difícil investigação e sem deixar grandes vestígios, é necessário apresentar como são dadas as investigações e todo o processo persecutório dos infratores que se utilizam do meio eletrônico.

Fiarilla (2016) entende que o conceito de internet e meio digital é amplamente difundido na sociedade e tendo crescido cada vez mais, porém, as tecnicalidades do meio ambiente digital é um conhecimento restrito a poucos profissionais e entusiastas. A falta de conhecimentos profundos do meio ambiente digital assola até mesmo os órgãos públicos nas pessoas de seus agentes, levando a uma falta de conhecimento por parte de investigadores, policiais e profissionais de segurança pública.

A sociedade contemporânea, imersa na era digital, confronta-se com desafios únicos no que tange à investigação e obtenção de provas de crimes cometidos no meio eletrônico. Isso ocorrendo por uma série de fatores como o desconhecimento dos limites do meio digital, a falta de colaboração e tantas outras motivações que impede uma persecução criminal e investigação comuns para crimes cibernéticos (Tremel, Nascimento, 2020).

Tremel e Nascimento (2020) apontam para uma grande complexidade dos meios digitais, levando a defasagem das formas de proteção social desenvolvidas por segurança pública. Tremel e Nascimento (2019) entendem que os avanços da internet, dos ciberespaços e das ferramentas digitais não foram acompanhados por parte do poder público, levando a uma falta de profissionais capacitados para investigação, repressão e persecução criminal.

Para Fiarilla (2016) a criação de medidas ágeis é essencial para garantir que a volatilidade dos dados do meio digital não afete a obtenção de provas, de forma que sejam feitas investigações céleres e que atuem prontamente para encontrar os finos resquícios do cometimento de crimes e delitos no meio digital.

A sociedade contemporânea, imersa na era digital, confronta-se com desafios únicos no que diz respeito à investigação e obtenção de provas de crimes cometidos no meio eletrônico. Tais desafios são complexos quando se fala do Estado e seu dever de proteção, vez que a burocracia do Estado alinhada com falta de eficiência e celeridade, resultam em impunidade no meio digital e problemas para a sociedade (Zambonato, 2023).

A popularização do mundo digital e especialmente das redes sociais trouxe consigo a virtualização de diversas atividades humanas, incluindo a socialização, o trabalho e a prática de crimes. Desde fraudes financeiras até crimes contra a honra, a esfera eletrônica tornou-se palco para a perpetração de delitos complexos e muitas vezes sofisticados (BARRETO, 2016).

Zambonato (2023) informa que a complexidade do meio eletrônico, a facilidade em esconder seus rastros e ainda mais a popularização de redes que não apresentam colaboração com as persecuções por ordem pública, geram processos judiciais carentes de provas e que recorrentemente são inconclusivos.

O Direito Brasileiro busca constantemente adequar-se às inovações tecnológicas, visando assegurar a eficácia da justiça e a proteção dos cidadãos. As delegacias especializadas em crimes eletrônicos desempenham papel crucial nesse cenário, demandando a análise criteriosa das formas de obtenção de provas, a fim de garantir a legalidade, a ética e a eficiência nos processos investigativos (Tepedino, 2019).

Ocorre que muito embora haja uma intenção de desenvolver os processos para atualização das normas, criação de novos parâmetros para proteção da sociedade e manutenção da ordem, o meio digital teve uma série de problemas em inovação legislativa ao longo das últimas 3 décadas. As normas criadas focaram quase que exclusivamente em quesitos cíveis no meio digital e quedando-se quase que inertes para com a criação de proteções em face dos crimes cometidos em meio eletrônico (Tepedino, 2019).

É certo e pacifico entre a doutrina que a maioria das normas foram e ainda são ineficazes para o combate à criminalidade no meio digital, tal como os diversos casos de estelionato, fraude e até mesmo obtenção ilegal de informação de usuários. Uma das poucas normas que tiveram um vislumbre de eficácia foi a Lei 12.737/2012, conhecida amplamente como Lei Carolina Dieckmann, criando delegacias especializadas e tipificando crimes cibernéticos.

> Art. 2º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B:
> “Invasão de dispositivo informático
> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: [...]
> Art. 4º Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado. (Brasil, 2012, p. 1).

As delegacias especializadas em crimes em meio eletrônico são também conhecidas como delegacias de polícia cibernética, sendo responsáveis pela

investigação de crimes em ambiente digital. Essas delegacias possuem equipes especializadas em obtenção de provas digitais, que são capazes de realizar perícias em computadores, celulares e outros dispositivos eletrônicos (Nunes, 2021).

A obtenção de provas no meio digital não se restringe apenas a desafios legais, mas também éticos e tecnológicos, vez que, a preservação da integridade das evidências, a garantia da imparcialidade dos peritos e a atualização constante dos profissionais envolvidos são elementos essenciais para assegurar a validade das provas. Além disso, a rápida evolução tecnológica exige uma constante adaptação das técnicas investigativas, para que estas se mantenham eficazes diante das novas ameaças (Ramos, 2022).

A coleta de dados mesmo diante de um crime é uma questão de grande complexidade, vez que as relações entre Estado e Cidadão, relações verticais, são protegidas por uma série de princípios como o da privacidade, o princípio da presunção de inocência e diversos outros que limitam o poder do Estado. Diante de tal complexidade as investigações não podem a bel prazer coletar dados que sejam privados ou adentrar dispositivos sem mandado digital (Ramos, 2022).

Diante destas informações fica evidente em como há uma complexidade em desenvolver a investigação, não podendo o poder público e mesmo as delegacias especializadas adentrarem o cyber espaço para obter dados que sejam sensíveis. Para investigação de perfis digitais, em seu íntimo, obtenção de conversas e dados sensíveis, há a necessidade de mandado de busca e ao menos o fumo do cometimento do delito *(fumus commissi delicti)* (Nunes, 2021).

O ordenamento jurídico brasileiro, atento às demandas da sociedade digital, ainda reconhece a importância das provas eletrônicas, prova disto sendo o Marco Civil da Internet (Lei nº 12.965/2014) e diversas alterações do Código de Processo Penal (CPP), os quais estabelecem parâmetros para a coleta e aceitação dessas evidências, garantindo a sua validade quando obtidas de maneira lícita. Contudo, a complexidade técnica envolvida na obtenção de provas eletrônicas demanda uma constante atualização normativa (Nunes, 2021).

Para obtenção de provas com o consentimento do investigado, mesmo que sejam aquelas informações que se colocam quase como que públicas, tais como os perfis abertos em redes sociais, é a mais simples, pois não exige autorização judicial. O investigado pode, por exemplo, voluntariamente entregar o seu dispositivo eletrônico à polícia ou fornecer as informações necessárias para a obtenção das

provas; tendo até mesmo a possibilidade de coleta de dados evidentemente criminosos por parte das polícias especializadas (Ramos, 2022).

Já quando há uma barreira de direitos, tal como a privacidade ou informações sigilosas, similares a conversas privadas, fotos íntimas e dados protegidos por parte da Lei Geral de Proteção de Dados, há a necessidade de autorização judicial para coleta. As hipóteses de autorização judicial para obtenção de provas digitais estão previstas na Lei nº 12.965/2014, conhecida como Marco Civil da Internet (Ramos, 2022).

A obtenção de provas digitais é um processo complexo e que exige a observância de diversas normas legais. As delegacias de polícia cibernética são essenciais para a investigação de crimes cibernéticos, pois possuem a expertise e os recursos necessários para obter provas digitais de forma lícita e eficaz (Nunes, 2021).

Sobre estas provas O Ministério Público Federal (MPF) ainda fixa princípios sobre as provas em meio digital, definindo que as provas precisam de uma base sólida para que possam ser utilizadas no processo contencioso. Os princípios fixados por parte do MPF são:

> 1. Admissível: ou seja, estar em plena conformidade com a lei para que possa ser apresentada à justiça.
> 2. Autêntica: as provas devem ser comprovadamente relacionadas ao incidente/crime investigado. O trabalho de uma documentação de qualidade é essencial para o cumprimento deste item.
> 3. Completa: o conjunto de evidências deve fornecer uma apresentação completa acerca do evento investigado. Nunca deve depender de elementos faltantes ou duvidosos. Deve " contar a história" completa, e não apenas fornecer perspectivas particulares.
> 4. Confiável: não deve haver incertezas acerca da autenticidade e veracidade das evidências, bem como sobre as formas como foram coletadas e posteriormente manuseadas durante a investigação.
> 5. Convincente: além de todas as características anteriores, deve ser documentada e apresentada de forma clara e organizada. (Brasil, 2016, p. 157).

Muito além da complexidade que é a obtenção por vias legais de dados que possam servir como prova, ainda há o meio digital como um módulo de fácil modificação. O mundo digital seus dados podem ser modificados quase que ao bel prazer do usuário (Nunes. 2021).

Como apresentam os estudos de Basan (2021) o meio digital é volátil, permitindo ferramentais como *proxy*, máscaras de rede, encriptação de dados, cópia,

alteração e até exclusão de dados ao toque de um simples botão. Outrossim, o cyber espaço permite que usuários com alto conhecimento possam facilmente se esconder na atuação de suas ações criminosas.

Basan (2021) explica que o *proxy* permite acessar dados de uma rede utilizando a conexão de outro dispositivo, algo como vestir a imagem de outro computador, garantindo o anonimato o real indivíduo que acesse um espaço digital. Tal meio esconde rastros, impede localização, oculta dados pessoais e garante que o usuário esteja anônimo em uma rede. Tal autor ainda informa que, quando utilizado de maneira eficiente, o *proxy* impede qualquer possibilidade de rastreamento e identificação do criminoso.

Outro ponto, que eleva ainda mais o papel das delegacias especializadas é a cadeia de custodia das provas coletadas. Obter provas é complexo e demanda esforço das autoridades, porém, uma vez obtidas devem ser seguidos rígidos regramentos do código de processo penal para garantir que tais provas não sejam adulteradas (Nunes, 2021).

A cadeia de custodia em sua inovação legislativa em 2019 acrescentou os artigos 158-A até 158-F no Código de Processo Penal (CPP), criando formas de garantir a autenticidade e realidade das provas. Para o meio digital este quesito deve ser ainda mais rígido, diante da possibilidade de alterações ou até exclusão facilitada da prova coletada (Nunes, 2021).

Para a cadeia de custodia de provas digitais, é necessário que as imagens, vídeos e documentos coletados sejam acompanhados de metadados do arquivo que possam ser utilizados posteriormente como identificador e que garantem que o arquivo apresentado em juízo seja o mesmo do coletado (Milheiro, 2020).

Há ainda a necessidade de que os materiais coletados não sejam eivados de vícios de coleta, tal como obtenção por meio fraudulento e violação de direitos, assim, a maioria dos documentos apresentados diante do juízo precisam de identificadores que apresentem seus respectivos mandados de coleta ou quebras de sigilos telefônicos, telemáticos e bancários (Milheiro, 2020).

É importante frisar que os metadados das coletas de dados de provas eletrônicas devem acompanhar metadados. Bioni (2020) explica que estes metadados são as informações escondidas dos documentos, sendo dados internos de imagens, vídeos, arquivos, documentos e outros itens digitais que o identificam em sistemas.

Tais metadados se apresentam na forma de *Hashs,* codificação de segurança, que detém informações de identificadores internos de certos sistemas, ou datas, ou valores específicos de controle, ou até mesmo informações do dono ou autor do arquivo (Bioni, 2020).

Nunes (2022) afirma que estes metadados são os únicos itens que servem com veracidade e fidedignidade para identificar um arquivo. Apesar de poderem ser alterados, modificados e excluídos, Nunes (2022) informa que a alteração de tais dados requer expertise e acessos privilegiados que por si só serviriam como prova para identificar a alteração, considerando que os indivíduos que teriam conhecimento e acesso a tais metadados para altera-los, exclui-lo ou modifica-los seriam pessoas facilmente identificáveis em um contexto concreto.

Assim, de acordo com os estudos de Nunes (2022) e Bioni (2020) os metadados de arquivos digitais seriam a forma mais crível de identificar imagens, arquivos, fotos ou vídeos que sirvam como vestígios de crimes e delitos cometidos em meio eletrônico. Porém a sua obtenção demanda uma alta investigação, expertise dos profissionais investigadores e obviamente os crivos legais de violação legal da privacidade.

A obtenção de provas de crimes no meio digital, no contexto das normas voltadas para o ambiente cibernético e das delegacias especializadas em crimes eletrônicos, apresenta-se como um desafio multifacetado. A legislação vigente, aliada à atuação especializada das delegacias, oferece uma estrutura sólida para enfrentar os desafios da era digital. Contudo, é imperativo que a sociedade, o poder judiciário e os órgãos de segurança continuem a dialogar e a evoluir, a fim de garantir que a justiça seja efetiva sem comprometer os direitos fundamentais dos cidadãos. A busca constante por inovações legislativas e tecnológicas é essencial para manter o equilíbrio entre a segurança digital e os princípios democráticos que fundamentam o Estado de Direito.

3. OS AVANÇOS TECNOLÓGICOS NAS DELEGACIAS ESPECIALIZADAS

Como já informado as delegacias especializadas em crimes cibernéticos atuam no brasil como sendo o órgão da polícia judiciária que lida especialmente com esta fatia da criminalidade, isto é, sendo a polícia para os crimes em ambiente digital. Porém, resta a dúvida sobre quais os avanços tecnológicos que as delegacias especializadas implicam no avanço da persecução penal, da coação a criminalidade e no desenvolvimento de um ambiente digital saudável e ordenado para a população.

As delegacias especializadas são diversas, tendo papais de grande importância em centralizar tarefas e com isso podendo concentrar forças humanas especializadas e com conhecimento favorecido para a as temáticas necessárias e assim garantir um trabalho célere, especializado e coeso com a realidade de cada tema.

São conhecidas popularmente as delegacias da mulher, que visam ter seus times de policias, servidores e auxiliares especializados em um atendimento humanizado e com todo o crivo necessário para que a vítima possa ser auxiliada e que os crimes ocorridos com a temática da mulher possam ser melhores combatidos e punidos. Os agentes em delegacias especializadas da mulher devem ter especializações e conhecimento sobre o atendimento especializado para a mulher (Brasil, 2023).

Em mesmo sentido, com menor conhecimento popular, existem as delegacias especializadas em crimes virtuais. Tais unidades detém peculiaridades muito particulares, vez que demandam conhecimento profundo de informática por parte dos seus servidores (Greco, 2022).

Caetano (2015) apresenta de seus estudos que, ao seu tempo, havia a falta de investimento em efetivo combate e investigação dos crimes digitais, ocorrendo fraudes e ações criminosas recorrentes no meio eletrônico. Porém tal realidade vem mudando com o tempo e nos últimos anos existindo ações mais incisivas de políticas públicas e alocação de recursos para as delegacias especializadas em crimes cibernéticos.

Os gastos com segurança pública na atualidade vêm sendo amplamente melhorados, utilizando de políticas fixadas com a nova norma da Lei nº 13.675/2018 criando o Sistema Único de Segurança Pública (Susp). Permitindo um controle nacional de políticas de segurança, melhorias de sistemas de informática, unificação de dados e especialmente melhor provisão de dados para estratégias de combate a criminalidade que sejam baseados em sólidas pesquisas (Brasil, 2022).

Tabela 01 - Gastos com segurança pública 2019 – 2020

Regiões e UF	2019	2020	2021	2022
Acre	793.456.980,33	574.862.510,52	605.440.983,58	974.366.892,28
Amapá	694.695.776,98	875.817.884,88	792.512.668,14	907.088.653,91
Amazonas	2.415.599.556,34	2.446.652.838,15	2.500.941.436,14	2.662.045.997,71
Pará	3.372.219.873,84	3.453.871.297,89	3.461.093.316,32	4.103.685.252,74
Rondônia	978.369.052,31	1.163.157.615,06	1.251.528.895,62	1.601.303.839,05
Roraima	330.179.769,30	455.437.560,95	542.073.294,66	634.471.576,06
Tocantins	1.282.222.632,96	1.233.808.445,59	1.114.390.400,99	1.149.665.495,72
Alagoas	1.328.013.616,56	1.577.570.858,44	1.495.061.310,92	1.623.759.179,88
Bahia	5.364.489.586,10	5.031.586.127,80	4.621.148.363,14	5.277.119.893,83
Ceará	3.256.406.668,73	3.545.882.765,05	3.528.761.766,70	4.186.299.676,85
Maranhão	2.295.533.146,88	2.280.318.189,00	2.095.014.797,74	2.062.110.314,84
Paraíba	1.588.174.254,35	1.650.460.531,26	1.550.241.625,64	1.780.596.385,62
Pernambuco	3.419.991.741,27	3.353.275.905,54	3.051.474.870,57	3.320.671.005,89
Piauí	1.023.422.464,08	914.920.945,46	891.197.662,39	999.571.783,20
Rio Grande do Norte	1.379.024.857,66	1.208.767.290,00	1.302.680.054,36	1.393.230.138,76
Sergipe	1.133.214.839,20	1.113.956.079,08	1.615.504.371,62	1.284.898.903,55
Goiás	4.398.536.942,51	3.716.068.181,70	3.508.149.879,42	3.519.465.640,61
Mato Grosso	2.849.139.500,75	3.000.337.644,71	3.312.424.055,76	3.645.305.970,67
Mato Grosso do Sul	1.442.821.077,71	1.443.809.375,20	1.648.400.740,68	1.991.889.298,44
Distrito Federal	1.067.750.210,78	1.136.925.275,17	1.050.959.837,67	1.146.946.782,02
Espírito Santo	1.635.689.517,75	1.639.757.073,24	1.733.101.397,09	2.247.668.152,57
Minas Gerais	10.664.715.315,19	9.852.564.392,51	10.087.881.833,42	11.139.603.561,08
São Paulo	14.116.905.868,32	13.896.330.265,96	14.643.724.342,79	14.840.589.983,94
Rio de Janeiro	11.497.110.095,69	11.003.014.228,84	10.535.004.385,44	13.891.833.966,32
Paraná	4.566.703.630,88	4.292.668.293,81	4.334.949.779,25	5.104.810.384,26
Rio Grande do Sul	5.772.742.783,40	6.439.280.791,88	6.135.449.677,50	7.000.418.171,24
Santa Catarina	2.745.178.297,08	2.801.658.636,01	2.848.893.436,68	3.369.120.457,15
Total	**91.412.308.056,95**	**90.102.761.003,72**	**90.258.005.184,25**	**101.858.537.358,19**

Fonte: Adaptado de FBSP (2023).

Conforme a tabela 01, os gastos com segurança pública vêm aumentando ano a ano, resultando em melhores condições para os profissionais de segurança, garantia de benefícios para a população e possibilidade de investimentos em uma área que carece de recursos.

Tal como os estudos de Dias (2023) a proteção da sociedade por meios de policiamento e ações em geral de segurança pública costuma ser ineficiente, uma vez que carece de recursos. Porém, ano a ano os investimentos vem gradativamente se acentuando para buscar a ordem social.

Como é visto na Tabela 01 os dados apontam para uma melhoria dos recursos para a segurança pública em todo o país. Tais recursos podem ter impacto em todas as frentes de proteção da segurança pública, tendo tendências para atualização e modernização das ferramentas dos órgãos de segurança pública.

Tabela 02 – Estelionato por meio eletrônico 2021 e 2022

Brasil e Unidades da Federação	Estelionato por meio eletrônico			
	Nºs. Absolutos	Taxas		Variação (%)
	2022	2021	2022	
Brasil	**200.322**	**115,0**	**189,9**	**65,2**
Acre	153	6,1	18,4	203,0
Alagoas	4.911	106,1	157,0	47,9
Amapá	374	10,7	51,0	376,0
Amazonas	404	2,4	10,3	321,2
Bahia	...	...	...	...
Ceará	...	...	...	...
Distrito Federal	15.580	359,3	553,1	53,9
Espírito Santo	15.277	277,0	398,5	43,9
Goiás	1.461	1,8	20,7	1.027,2
Maranhão	6.724	19,1	99,2	419,6
Mato Grosso	9.253	182,3	252,9	38,7
Mato Grosso do Sul	2.524	33,3	91,6	174,8
Minas Gerais	35.749	125,0	174,1	39,3
Pará	12.988	29,0	160,0	451,1
Paraíba	406	1,7	10,2	503,3
Paraná	5.685	16,6	49,7	198,6
Pernambuco	14.060	108,9	155,2	42,5
Piauí	246	2,0	7,5	277,0
Rio de Janeiro	...	...	...	...
Rio Grande do Norte	...	...	...	...
Rio Grande do Sul	...	...	...	...
Rondônia	5.932	176,5	375,2	112,6
Roraima	759	9,5	119,3	1.155,1
Santa Catarina	64.230	573,3	844,1	47,2
São Paulo	...	...	...	...
Sergipe	432	3,6	19,6	437,1
Tocantins	3.174	116,2	210,0	80,7

Fonte: Adaptado de FBSP (2023).

Já dos dados da Tabela 02 é evidente que os crimes de estelionato em meio virtual vêm crescendo amplamente, demandando atuação incisiva dos órgãos especializados e ainda mais das ações de segurança especializada das delegacias especializa em crimes virtuais.

Como apontado por Maia e Costa (2023) os investimentos são um item de grande importância para o desenvolvimento de combates eficientes quando se fala em um quesito de criminalidade digital. Sendo necessários investimentos para proteção que evite as violações e ainda investir para a investigação de crimes cometidos e busca de provas.

> Quatro elementos essenciais que são reforçados significativamente para essa luta são o investimento em tecnologia, a sensibilização a educação, a cooperação internacional e a criação de legislação

> abrangente. O investimento em tecnologia desempenha um papel crucial na prevenção e combate aos crimes cibernéticos. Isso envolve uma alocação de recursos para desenvolver sistemas de segurança cibernética robustos, atualizados e proativos. Isso inclui o aprimoramento de firewalls, sistemas de detecção de intrusões e criptografia de dados. Além disso, os governos devem investir em treinamento e capacitação para seus especialistas em segurança cibernética, para que estejam preparados para enfrentar ameaças em constante evolução. (Maia, Costa, 2023, p. 122).

As lições de Barreto (2016) ainda explicam que conforme o crime avança, também deve avançar o poder público em seu encalço, visando o coibir e punir. Assim, investimentos devem ser alocados de acordo com o crescimento de índices criminais e dados que demonstrem o crescimento de recorrência em certo tipo penal.

Como a tabela 02 apresenta, há um claro avanço da criminalidade em m tipo penal que ocorre exclusivamente no meio cibernético. Assim, os dados apontam para a existência de crescente criminalidade em meio digital, devendo o investimento ser também crescente.

Evidencia do crescimento e atualização do poder público para com a esfera digital é a criação de planejamento do Susp em uma ampla popularização e implementação de delegacias estaduais especializadas em crimes cibernéticos. Assim, garantindo que todas as unidades federativas tenham expertise no combate a criminalidade cibernética (Brasil, 2022).

O Susp permitiu a ampliação das já existentes delegacias estaduais e forças tarefa de repressão de crimes digitais, unificando sistemas de proteção do ambiente digital e modernizando o contato dos profissionais de segurança pública especializada (Brasil, 2022).

O Susp criou especificamente a Unidade Especial de Investigação de Crimes Cibernéticos (UEICC) que conta com expertise e profissionais super capacitados para o processo de combate à criminalidade. Sendo uma atuação de proteção cibernética moderna (Brasil, 2022).

> O lançamento da UEICC faz parte da Semana Nacional de Segurança Pública comemorativa ao Bicentenário do MJSP. No período de 27 de junho a 1º de julho, o Ministério entrega à sociedade uma série de programas e iniciativas na área da segurança. Além de crimes cibernéticos relacionados a instituições bancárias, a UEICC irá intensificar a repressão a diversos outros crimes praticados no ambiente virtual, como a pornografia infantil, contra instituições públicas, setor varejista, operadoras de telefonia, telecomunicações,

> entre outros. De acordo com o Diretor-Geral da PF, Márcio Nunes, o órgão já vem combatendo esses crimes por meio dos rastros que os criminosos deixam e procedido com a responsabilização dos autores a partir de investigações. (Brasil, 2022, p. 8)

A criação da UEICC contou especialmente com processos de troca de conhecimento entre os entes federados, linhas de comunicação e treinamento de profissionais para as formas modernas de coleta de dados em meio digital que visam identificação de criminosos que usam de tal meio para garantir seu anonimato (BRASIL, 2022).

Caetano (2023) aponta em como a obtenção de provas no meio digital é complexo, demandando a atuação de experts em coleta de dados e ainda mais em contar com maquinário e permissões de última geração. Em tal meio são necessários servidores robustos para coletar, armazenar e tratar dados, bem como a permissão para coletar tais dados.

A dificuldade em rastrear e identificar os atuantes de crimes digitais é extrema e causada pelo anonimato proporcionado pela internet. Muitas vezes, os criminosos utilizam técnicas avançadas para esconder sua identidade, dificultando a coleta de evidências (Caetano, 2023).

O Susp vem sendo implementado justamente visando retirar o anonimado de usuários criminosos, colocando o agente de segurança pública no encalço do criminoso, analisando dados, rastreando e ainda mais atuando em colaboração com empresas e entidades para proteção de sistemas recorrentemente alvo de criminosos.

O uso generalizado de criptografia e técnicas avançadas de ocultação de dados cria barreiras substanciais para os órgãos de segurança. Para o combate de tal questão a Unidade Especial de Investigação de Crimes Cibernéticos (UEICC) conta com acesso ao super computador brasileiro Santos Dumont para tratar dados criptografados e extrair a identidade dos criminosos.

Após as informações apresentadas, é evidente em como há uma complexidade em obter provas no meio digital, porém, a modernização e investimento acompanham a evolução da sociedade e desde o ano passado apresentam investimentos e estratégias robustas para o combate da criminalidade cibernética.

A criação do Susp e da Unidade Especial de Investigação de Crimes Cibernéticos (UEICC) auxiliam fortemente o combate ao crime no ambiente digital e

dá ferramentas para obtenção de provas que sejam utilizadas em processos criminais futuros.

CONSIDERAÇÕES FINAIS

Após a apresentação do estudo há a certeza de que o meio digital ainda carece de normas eficazes no combate à criminalidade. Muito embora existam normas que regulem o meio ambiente virtual, ainda não são normas bem conhecidas, fixadas ou com eficácia total.

A capacidade de criminosos digitais se esconderem por trás de identidades virtuais e de serviços que garantem o anonimato dificulta a identificação dos responsáveis por atividades ilícitas. O uso de técnicas avançadas para mascarar a origem e a autoria de ações maliciosas, como o uso de VPN’s e técnicas de criptografia, torna o rastreamento mais complexo ou até mesmo impossível.

A obtenção de provas de crimes no meio digital é difícil, indo muito além da já complexa forma de investigação e obtenção de provas no mundo material. As delegacias de polícia cibernéticas são o bastião da investigação em tais casos, tendo profissionais capacitados, treinados e que dedicam seus esforços para tal tarefa complexa.

O cumprimento da cadeia de custódia é outro ponto essencial no processo de obtenção de provas. As provas que não forem coletadas e armazenadas de acordo com a cadeia de custódia podem ser consideradas inadmissíveis, o que pode prejudicar o processo penal.

A colaboração entre órgãos de segurança pública, empresas de tecnologia e organizações da sociedade civil é crucial. Parcerias estratégicas podem fornecer acesso a informações valiosas e recursos necessários para combater crimes digitais de maneira mais eficaz.

A legislação precisa evoluir para lidar adequadamente com os desafios legais apresentados pelo meio digital. Atualizações nas leis de proteção de dados, cibersegurança e crimes digitais são essenciais para proporcionar um arcabouço jurídico sólido e adaptável.

A natureza global da internet muitas vezes ultrapassa as fronteiras jurisdicionais, criando desafios legais para a aplicação da lei, pois a legislação varia significativamente de um país para outro. O combate eficaz aos crimes digitais pode exigir ainda uma cooperação internacional robusta entre países, agências de aplicação da lei e empresas privadas, o que nem sempre é fácil de alcançar devido a diferenças políticas e jurídicas.

Investir na capacitação e treinamento contínuo dos profissionais de segurança é crucial. A rápida evolução das tecnologias exige que os investigadores estejam atualizados, aptos e munidos de ferramentas de última geração para lidar com as complexidades do ambiente digital.

Os governos devem investir em tecnologia avançada e treinamento especializado para fortalecer as capacidades das agências de aplicação da lei no combate a crimes digitais. A colaboração entre governos, empresas privadas e organizações da sociedade civil pode ser um ponto fundamental para enfrentar os desafios de segurança digital, demandando estudos de viabilidade.

Enfrentar a criminalidade no meio digital exige uma abordagem que combine tecnologia, legislação, colaboração e capacitação. A superação dos desafios na obtenção de provas requer inovação constante e uma adaptação ágil dos órgãos de segurança pública às dinâmicas complexas do ciberespaço. Somente através de uma abordagem integrada será possível construir uma resposta eficaz e justa para a crescente ameaça dos crimes digitais.

REFERÊNCIAS BIBLIOGRÁFICAS

BASAN, Arthur Pinheiro**. Publicidade digital e proteção de dados pessoais** [recurso eletrônico]: o direito ao sossego / Arthur Pinheiro Basan. - Indaiatuba, SP: Editora Foco, 2021.'

BARRETO, Alesandro Gonçalves, BRASIL, Beatriz Silveira. **Manual de Investigação Cibernética** / Alesandro Gonçalves Barreto – Beatriz Silveira Brasil. 2º Ed. rev. ampl. Brasport. São Paulo – SP, 2016.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento / Bruno Ricardo Bioni. – 2. ed. – Rio de Janeiro:Forense, 2020.

BLUM, Renato Opice; MALDONADO, Viviane Nóbrega. **LGPD:** Lei Geral de Proteção de Dados comentada [livro eletrônico] / coordenadores Viviane Nóbrega

Maldonado e Renato Opice Blum. – 2. ed. rev., atual. e ampl. – São Paulo: Thomson Reuters Brasil, 2020.

BRASIL. Ministério Público Federal. **Roteiro de atuação:** crimes cibernéticos / 2. Câmara de coordenação e revisão. – 3.ed. rev. e ampl. – Brasília: MPF, 2016.

BRASIL. Ministério da Justiça e Segurança Pública. **Projeto estratégico Susp** – plano nacional de modernização e atuação. Gov, 2022. Disponível em: https://www.gov.br/mj/mjsp-comemora-200-anos-com-entrega-de-projetos-e-programas-para-a-seguranca-publica. Acesso em 24 nov. 2023

BRASIL, Legislativo. LEI Nº 14.541 DE 03 DE ABRIL DE 2023. **Dispõe sobre a criação e o funcionamento ininterrupto de Delegacias Especializadas de Atendimento à Mulher**. Brasília, 3 de abril de 2023.

CAETANO, Aldo Maxuell Pereira de Mesquita. **Crimes virtuais: aplicação, falibilidade e impunidade**. Curso de Direito da Universidade Tiradentes–UNIT. Aracaju, 2015. Disponível em: https://egov.ufsc.br/portal/sites/default/files/tcc_-_crimes_virtuais.pdf. Acessado em 18 nov. 2023.

DIAS, Paulo Eduardo Leite. **A evolução cibernética e a falta de punibilidade célere dos crimes digitais:** crimes digitais na plataforma Whatsapp. Trabalho de Conclusão de Curso. Pontifícia Universidade Católica de Goiás. 2023. Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/5966. Aceso em 23 nov. 2023.

DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais** [livro eletrônico]: elementos da formação da Lei Geral de Proteção de Dados / Danilo Cesar Maganhoto Doneda. -- 2. ed. -- São Paulo: Thomson Reuters Brasil, 2020.

FBSP, Fórum Brasileiro de Segurança. Anuário Brasileiro de Segurança Pública / Ano 17 - Fórum Brasileiro de Segurança Pública. – 1 (2006)- . – São Paulo: FBSP, 2023.

FIARILLA, Celso Antonio Pacheco. **Crimes no meio ambiente digital e a sociedade da informação** / Celso Antonio Pacheco Fiorillo, Chris~any Pegorari Conte. - 2. ed. - São Paulo: Saraiva, 2016.

GRECO, Rogério. **Curso de direito penal**: volume 2: parte especial: artigos 121 a 212 do código penal / Rogério Greco. – 19. ed. – Barueri [SP] : Atlas, 2022.

MAIA, K. B.; COSTA, C. H. F. CRIMES CIBERNÉTICOS. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, [S. l.], v. 9, n. 10, p. 109–126, 2023. DOI: 10.51891/rease.v9i10.11580. Disponível em: https://periodicorease.pro.br/rease/article/view/11580. Acesso em: 25 nov. 2023.

MILHEIRO, Tiago Caiado. **Comentário judiciário do código de processo penal:** artigos 124º a 190º. t. II. Coimbra: Almedina, 2012.

NUNES, Duarte Rodrigues. **Os meios de obtenção de prova previstos na lei do cibercrime**. 2. ed. Coimbra: Gestlegal, 2021

NUNES, Duarte Rodrigues. Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor? In: **Revista Ultracontinental de Literatura Jurídica, Montes Claros**, Ed. Associação de Letras Jurídicas de Montes Claros, v. 3, n. 3, p. 65-107, set.-dez. 2022. Disponível em: https://www.ajurmoc.com.br/files/anexos/revista/887250db9cae36ce60c3ac5fa96bbbe4.pdf#page=65. Acesso em 16 nov. 2023.

RAMOS, Armando Dias. **O agente encoberto digital**. Coimbra: Almedina, 2022.

SILVA, Natália dos Santos. **O estelionato virtual e a sua estrutura jurídica**. 2023. 76 f. Dissertação (Mestrado Profissional em Direito Econômico e Desenvolvimento) - Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, Brasília, 2023. Disponível em: https://repositorio.idp.edu.br//handle/123456789/4809. Acesso em 24 nov. 2023.

TEPEDINO, Gustavo. **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro** - Ed. 2ª, Revista dos Tribunais. São Paulo, SP. 2019

TREMEL, Rosangela; NASCIMENTO, Claudio Joel Brito Lóssio Luciano. **Cibernética jurídica: estudo sobre o direito digital**.⁄Claudio Joel Brito Lóssio Luciano Nascimento, Rosangela Tremel (Organizadores). – Campina Grande: EDUEPB, 2020.

VELOSO, Waldir de Pinho; MENDES, Maria Rodrigues. **Revista Ultracontinental de Literatura Jurídica**. Vol. 3, n.º 3. Montes Claros/MG, Brasil, Associação de Letras Jurídicas de Montes Claros, 2022.

WACHOWICZ, Marcos. **Proteção de dados pessoais em perspectiva**: LGPD e RGPD na ótica do direito comparado / organização de Marcos Wachowicz – Curitiba: Gedai, UFPR 2020.

ZAMBONATO, Matheus Schultz. **Avanços da legislação brasileira no combate aos crimes cibernéticos**. Trabalho de Conclusão de Curso, Porto Alegre, RS. 2022. Disponível em: http://hdl.handle.net/10183/252036. Acesso em 01 out. 2023