FUNDAÇÃO DE ENSINO “EURÍPIDES SOARES DA ROCHA” – FEESR
CENTRO UNIVERSITÁRIO EURÍPIDES DE MARÍLIA – UNIVEM
PROGRAMA DE PÓS-GRADUAÇÃO STRICTU SENSU EM DIREITO – PPGD
MESTRADO EM DIREITO

BRUNA BÁRBARA PAIZ ZEOTTI KANDA

INFILTRAÇÃO POLICIAL VIRTUAL:
MATERIALIZAÇÃO DE VESTÍGIOS DIGITAIS

MARÍLIA
2024

BRUNA BÁRBARA PAIZ ZEOTTI KANDA

INFILTRAÇÃO POLICIAL VIRTUAL:
MATERIALIZAÇÃO DE VESTÍGIOS DIGITAIS

Dissertação apresentada ao Programa de Pós-Graduação Stricto Sensu – Mestrado em Direito – do Centro Universitário Eurípides de Marília – UNIVEM, em sua área de concentração em Direito e Estado na Era Digital, Linha de Pesquisa Dogmática Jurídica e Transformação Digital, como requisito à obtenção do título de Mestre em Direito.

Orientador: Prof. Dr. José Eduardo Lourenço dos Santos

MARÍLIA
2024

Kanda, Bruna Bárbara Paiz Zeotti
Infiltração Policial Virtual: Da materialização de vestígios / Bruna Bárbara Paiz Zeotti Kanda; Orientador: Prof. Dr. José Eduardo Lourenço dos Santos. Marília,2024
177 p.

Dissertação (mestrado) – Curso de Mestrado em Direito Digital do Centro Universitário Eurípides de Marília - UNIVEM, Marília, 2024.

1. Infiltração Policial virtual. 2. Provas digitais. 3.Direito Processual Penal.

BRUNA BÁRBARA PAIZ ZEOTTI KANDA

INFILTRAÇÃO POLICIAL VIRTUAL: MATERIALIZAÇÃO DE VESTÍGIOS DIGITAIS

Dissertação apresentada ao Programa de Pós-Graduação *Stricto Sensu* – Mestrado em Direito – do Centro Universitário Eurípides de Marília – UNIVEM, em sua área de concentração em Direito e Estado na Era Digital, Linha de Pesquisa Dogmática Jurídica e Transformação Digital, e aprovada pela banca examinadora.

Marília, ____ de _____ de 2024.

COMISSÃO EXAMINADORA

_____

Prof. Doutor José Eduardo Lourenço dos Santos (orientador)
Centro Universitário Eurípides de Marília (UNIVEM)

_____

Prof. Doutor César Augusto Luiz Leonardo
Centro Universitário Eurípides de Marília (UNIVEM)

_____

Prof. Doutor Luiz Fernando Kazmierczak
Universidade Estadual do Norte do Paraná (UENP)

Dedico este trabalho ao meu marido Bruno pelo incentivo constante e apoio incondicional e à minha filha Elisa, que foi a força propulsora para sua realização.

AGRADECIMENTOS

Minhas primeiras palavras são de agradecimento ao Professor Pós-Doutor pela Universidade de Coimbra, José Eduardo Lourenço dos Santos, meu orientador que, mesmo com a distância geográfica entre nós sempre esteve disponível para discutir as diversas questões com as quais me deparei no curso deste trabalho. E não poderia ter sido diferente, pois a minha persistência em sorver todo conhecimento de um dos mais destacados professores do Centro Universitário Eurípides de Marília – UNIVEM foi completamente justificada, conhecimento este, que me granjeou experiências valiosas hauridas tanto na sua carreira jurídica quanto na acadêmica. Merece meu especial reconhecimento pela maneira respeitosa com que aborda o direito, demonstrando elegância e dedicação genuínas. Sua dedicação em me guiar através das complexidades deste processo de pesquisa foi fundamental, e sou verdadeiramente grata por sua paciência e orientação. Além disso, tive a honra de atuar como organizadora na criação do terceiro volume da obra literária "Direito Novas Tecnologias e Controle Social", onde pude aplicar os valiosos ensinamentos que adquiri por meio de sua orientação e compartilhar dessas lições com a comunidade acadêmica e a sociedade.

De igual modo, dirijo os meus agradecimentos ao corpo docente do Centro Universitário Eurípides de Marília – UNIVEM, e os faço na pessoa do querido Professor Doutor Mário Furlaneto Neto que muitas vezes travestido de “um pai” me direcionou aos primeiros passos na vida acadêmica com maestria e paciência. Ao seu lado, tive a oportunidade de exercer a função de monitora da disciplina de Direito Processual Penal, experiência essa que me oportunizou o envolvimento com lições sobre a tarefa do “ensinar e, sobretudo, do aprender” e que certamente me forjaram para a vida acadêmica com coragem e confiança. Oportunamente, sob sua orientação, pude organizar a obra literária “Direito na Era digital”, experiência esta que me atrelou ensinamentos invulgares, aos quais sou imensamente grata.

Dedico ainda palavras de agradecimentos ao Centro Universitário Eurípides de Marília, que nestes dois anos foi um abrigo de memórias e ensinamentos e os faço na pessoa da querida Professora Doutora Samyra Haydee Dal Farra Naspolini, na época Coordenadora do Programa de Mestrado, que com sua determinação e generosidade ganhou a admiração, respeito e confiança da comunidade acadêmica, destacando-se por suas decisões e pela herança deixada, caracterizada pela integridade e perspicácia institucional aliadas principalmente ao seu excepcional conhecimento jurídico. Expresso meus agradecimentos com as palavras emprestadas de José

Saramago[1]: "*Mesmo que a rota da minha vida me conduza a uma estrela, nem por isso fui dispensado de percorrer os caminhos do mundo*". Com essas palavras em mente, manifesto meu apreço, pois sem sua generosidade e amizade o percurso deste mestrado teria sido consideravelmente mais árduo e desafiador. Sua luz e sabedoria iluminaram meu coração de maneira inestimável. Por isso também, sou eternamente grata.

Em sequência, é com imensa gratidão que me dirijo à banca de qualificação e de defesa pública composta pelos Professores Doutores César Augusto Luiz Leonardo, Defensor Público da Defensoria Pública do Estado de São Paulo na Regional de Marília, professor das disciplinas de Direito Processual Civil e Direito Processual Constitucional no Curso de Graduação em Direito e no curso de Mestrado em Direito no Centro Universitário Eurípides de Marília - SP (UNIVEM) e Membro do CEAPRO (Centro de Estudos Avançados em Processo); bem como ao Professor Doutor Luiz Fernando Kazmierczak que atualmente é Professor Adjunto na graduação em Direito e na pós-graduação em Ciência Jurídica na Universidade Estadual do Norte do Paraná (UENP), onde exerce o cargo de Diretor do Campus de Jacarezinho e Coordenador Estadual do Programa Núcleo de Estudos e Defesa de Direitos da Infância e da Juventude – NEDDIJ. Suas análises criteriosas e apontamentos foram de inestimável valor enriquecendo não apenas a minha dissertação, como também a minha trajetória acadêmica como um todo. Cada uma das suas ponderações foi um farol iluminando caminhos e indicando direções e por isso sinto-me imensamente privilegiada por ter contado com a expertise de uma banca tão distinta e respeitada. Aos senhores, atribuo minha gratidão bem como minha admiração.

Meus agradecimentos à Senhora Marilena Neto Nakadaira (Leninha), na época Secretária do Departamento de Pós-Graduação do Centro Universitário Eurípides de Marília – UNIVEM, que com abnegação profissional sempre nos auxiliou.

Devo registrar uma palavra de agradecimento aos queridos e amados amigos Silvia Aparecida Servo, Edilaine Vanessa da Silveira e Rodrigo Oliveira por todo o apoio que me sustentou durante essa trajetória, principalmente quando mais precisei todos vocês estavam lá, com apoio e abnegação de que só os verdadeiros amigos são portadores. Que estes agradecimentos transmitam a magnitude da minha gratidão, mesmo que as palavras nunca possam capturar totalmente a profundidade do meu apreço por vocês.

[1] O renomado escritor português José de Sousa Saramago, laureado com o Prêmio Nobel de Literatura em 1998 e distinguido com o prestigiado Prêmio Camões, o mais significativo na literatura lusófona, deixou uma marca indelével ao explorar, por meio de suas obras, as trilhas da sociedade moderna.

Aos meus queridos pais Júlio e Conceição, aos meus sogros Paulo e Tiemi e demais familiares, ao concluir este capítulo significativo da minha jornada acadêmica, é com grande emoção que dedico um momento para expressar minha gratidão a cada um de vocês. Cada membro desta família é uma fonte inesgotável de inspiração. A dedicação, o amor e a resiliência que testemunhei em cada um de vocês moldaram não apenas a minha jornada acadêmica, mas também o meu caráter e a minha visão de mundo. Agradeço por compreenderem os momentos de ausência. Cada gesto, por menor que seja, foi uma demonstração palpável do amor e do apoio que sempre senti ao meu redor.

Reservo estas palavras de agradecimento ao meu marido Bruno que foi o alicerce que sustentou minha trajetória, proporcionando apoio incondicional, compreensão e incentivo em cada etapa desse caminho. As suas palavras de encorajamento foram um bálsamo nos momentos de dúvida e a confiança que depositou em mim foi a força motriz que impulsionou meu progresso. Hoje, ao compartilhar esta dissertação, celebro não apenas um marco acadêmico, mas também a nossa jornada como família. Cada linha escrita é um reflexo do amor e suporte que recebi. Certamente, esta conquista não é apenas minha, é nossa. E espero que este trabalho reflita não apenas o meu esforço, mas também a nossa força coletiva.

Por fim, gostaria de dedicar palavras de agradecimento à minha filha Elisa que desde o ventre, e após seu nascimento, foi minha companhia e fonte inesgotável de força e fé. Antes pequenina deitada perto dos livros, nos momentos de leitura; depois, já sentada, aos oito meses, abria os livros e não dava descanso às suas folhas com suas mãozinhas ávidas e seu olhar curioso. Ali, naquele momento, absorta no tempo de quem aprecia uma tela de arte particular, eu enxergava o futuro e o seu "fluir inexorável do tempo", ansiando pelo momento em que lhe contaria o quão grande foi a aventura que vivemos na travessia desta escrita.

À comunidade acadêmica e aos colegas de classe, sou grata pela troca de ideias e debates construtivos que moldaram minha compreensão do tema. Faço este agradecimento nas pessoas dos queridos amigos Heitor Moreira de Oliveira e João Biffe Júnior por compartilharem recursos e perspectivas que enriqueceram minha abordagem. Criamos um elo de amizade e uma comunhão na participação de situações significativas com reflexo na minha vida acadêmica, contando sempre com seus conselhos. Credito-lhes homenagens de saudade e agradecimento.

Esta pesquisa representa não apenas meu esforço individual, mas também uma colaboração de muitos corações e mentes que compartilharam sua paixão e conhecimento. Que estes agradecimentos transmitam a magnitude da minha gratidão porque cada um de vocês desempenhou um papel crucial e este trabalho é um reflexo tangível do apoio, colaboração e inspiração que recebi.

"Quem elegeu a busca não pode recusar a travessia".

Guimarães Rosa.

KANDA, Bruna Bárbara Paiz Zeotti. **Infiltração Policial Virtual: Materialização de vestígios digitais**. 2024. 177 f. Dissertação (Mestrado em Direito) – Centro Universitário Eurípides de Marília, Fundação de Ensino "Eurípides Soares da Rocha", Marília, 2024.

RESUMO

A sociedade 4.0 representa uma evolução marcante na forma como os seres humanos interagem, trabalham e vivem em um mundo cada vez mais interconectado e orientado pela tecnologia. Essa nova fase da sociedade, também chamada de Quarta Revolução Industrial, é caracterizada pela convergência de tecnologias digitais, físicas e biológicas, criando um ambiente de transformação profunda em todos os aspectos da vida cotidiana. No cerne dessa sociedade 4.0 está a conectividade digital ubíqua. Dispositivos inteligentes, a Internet das Coisas (IoT), a inteligência artificial e a análise de dados em tempo real permitem uma comunicação instantânea e uma troca constante de informações entre máquinas, sistemas e pessoas. Essa conectividade gera uma nova dinâmica nas áreas da indústria, da economia, da educação, da saúde e muito mais. No entanto, ao se imiscuir no terreno da internet, paralelamente as vantagens trazidas pelo uso da tecnologia, coabita uma nova forma de criminalidade, os crimes digitais, que se consolidou com a dispersão de delitos comuns que migraram para o meio digital. Em razão disso, urge no âmbito do processo penal, especificamente no que concerne a produção e obtenção dos meios de provas digitais, a necessidade de uma prática regida por normas e princípios derivados do devido processo legal. Especialmente, em consideração aos princípios do contraditório, da ampla defesa e a proibição de provas obtidas de forma ilegal que são aspectos que se destacam. É nesse cenário que se insere a infiltração policial virtual, uma técnica investigativa contemporânea que se tornou fundamental no combate aos crimes cibernéticos e à criminalidade digital. A infiltração policial virtual representa uma ferramenta valiosa no combate aos crimes digitais e na busca pela justiça na era digital e apresenta vantagens e desafios únicos. Por um lado, ela permite a coleta de informações em tempo real e a identificação de indivíduos ou grupos envolvidos em atividades criminosas, muitas vezes antes que esses crimes se concretizem. No entanto, por outro lado, seu uso deve ser equilibrado com princípios éticos, legais e de respeito aos direitos individuais, garantindo que sua aplicação contribua para um ambiente mais seguro e protegido na internet. A fim de garantir que a infiltração policial virtual seja realizada de maneira legal, é crucial estabelecer salvaguardas rigorosas. Isso inclui a necessidade de autorização judicial prévia, a definição clara dos limites da atuação dos agentes infiltrados, bem como a preservação da integridade das evidências coletadas. Além disso, é fundamental garantir que os direitos individuais e a privacidade dos cidadãos sejam respeitados durante todo o processo. Para tal desígnio, por meio do método dedutivo e dos procedimentos de revisão bibliográfica, como objetivo geral, apresentar-se-á um panorama do instituto da infiltração policial como gênero e da infiltração policial virtual, como espécie, introduzida no ordenamento jurídico brasileiro pelas Leis nº 12.850/2013 e nº 13.441/2017, como técnica investigativa contemporânea que se tornou fundamental no combate aos crimes cibernéticos e à criminalidade digital; e por conseguinte, a pesquisa tem como objetivo específico enfrentar a temática da obtenção e da materialização dos vestígios digitais no âmbito da persecução penal. Conclui-se que tanto nos meios de provas positivados no ordenamento jurídico pátrio, quanto no que toca às novas modalidades de obtenção de provas digitais, asseguradas através da cadeia de custódia das evidências digitais e de um processo penal respaldado nas garantias fundamentais, observa-se a suficiência e a propriedade das normas existentes no ordenamento atual.

Palavras-chave: direito processual penal; direito probatório; provas digitais; infiltração policial; infiltração policial virtual; materialização de vestígios.

KANDA, Bruna Bárbara Paiz Zeotti. **Police Virtual Infiltration: Materialization of digital traces**. 2024. 177 p. Dissertation (Master's Degree in Law) – Centro Universitário Eurípides de Marília, Fundação de Ensino "Eurípides Soares da Rocha", Marília, 2024.

ABSTRACT

Society 4.0 represents a significant evolution in the way humans interact, work, and live in an increasingly interconnected and technology-driven world. This new phase of society, also known as the Fourth Industrial Revolution, is characterized by the convergence of digital, physical, and biological technologies, creating an environment of profound transformation in all aspects of daily life. At the heart of this Society 4.0 is ubiquitous digital connectivity. Smart devices, the Internet of Things (IoT), artificial intelligence, and real-time data analysis enable instant communication and constant exchange of information between machines, systems, and people. This connectivity generates a new dynamic in industries, the economy, education, healthcare, and much more. However, as it integrates into the realm of the internet, alongside the benefits brought by technology usage, a new form of criminality coexists – digital crimes – which have solidified with the migration of common offenses to the digital realm. Because of this, within the scope of criminal procedure, specifically concerning the production and acquisition of digital evidence, the need for a practice governed by norms and principles derived from due process of law is urgent. Especially considering the principles of adversarial proceedings, the right to a fair trial, and the prohibition of illegally obtained evidence, which are prominent aspects. It is in this scenario that virtual police infiltration comes into play, a contemporary investigative technique that has become essential in combating cybercrimes and digital criminality. Virtual police infiltration represents a valuable tool in the fight against digital crimes and in the pursuit of justice in the digital age, presenting unique advantages and challenges. On one hand, it allows real-time information collection and the identification of individuals or groups involved in criminal activities, often before these crimes materialize. However, on the other hand, its use must be balanced with ethical, legal, and individual rights principles, ensuring that its application contributes to a safer and more secure online environment. In order to ensure that virtual police infiltration is carried out ethically and legally, it is crucial to establish rigorous safeguards. This includes the need for prior judicial authorization, a clear definition of the limits of undercover agents' actions, as well as the preservation of the integrity of collected evidence. Additionally, it is fundamental to ensure that individual rights and citizens' privacy are respected throughout the process. To achieve this objective, through deductive methods and bibliographic review procedures, a general overview of the institution of police infiltration as a whole and virtual police infiltration as a specific aspect will be presented. The latter was introduced into the Brazilian legal system by Laws No. 12.850/2013 and No. 13.441/2017, as a contemporary investigative technique that has become essential in combating cybercrimes and digital criminality. Consequently, the research has a specific objective to address the theme of obtaining and materializing digital traces within the scope of criminal prosecution. It is concluded that both in the means of evidence specified in the national legal system and regarding new methods of obtaining digital evidence, ensured through the chain of custody of digital evidence and a criminal procedure backed by fundamental guarantees, the sufficiency and propriety of existing norms in the current legal framework are observed.

Keywords: criminal procedural law; evidentiary law; digital evidence; police infiltration; virtual police infiltration; materialization of traces.

KANDA, Bruna Bárbara Paiz Zeotti. **Infiltrazione Poliziesca Virtuale: Materializzazione di tracce digitali**. 2024. 177 f. Tesi. (Laurea Magistrale in Giurisprudenza) – Centro Universitário Eurípides de Marília, Fundação de Ensino "Eurípides Soares da Rocha", Marília, 2024.

RIASSUNTO

La società 4.0 rappresenta un'evoluzione significativa nel modo in cui gli esseri umani interagiscono, lavorano e vivono in un mondo sempre più interconnesso e guidato dalla tecnologia. Questa nuova fase della società, chiamata anche Quarta Rivoluzione Industriale, è caratterizzata dalla convergenza delle tecnologie digitali, fisiche e biologiche, creando un ambiente di profonda trasformazione in tutti gli aspetti della vita quotidiana. Al centro di questa Società 4.0 c'è una connettività digitale ubiqua. Dispositivi intelligenti, l'Internet delle Cose (IoT), l'intelligenza artificiale e l'analisi dei dati in tempo reale consentono una comunicazione istantanea e uno scambio costante di informazioni tra macchine, sistemi e persone. Questa connettività genera una nuova dinamica nei settori dell'industria, dell'economia, dell'istruzione, della salute e molto altro. Tuttavia, mentre si integra nel mondo dell'Internet, parallelamente ai vantaggi apportati dall'uso della tecnologia, convive una nuova forma di criminalità: i reati digitali, che si sono consolidati con la migrazione di reati comuni nel mondo digitale. Per questo motivo, nell'ambito del procedimento penale, in particolare per quanto riguarda la produzione e l'acquisizione delle prove digitali, è urgente la necessità di una pratica regolata da norme e principi derivati dal giusto processo legale. Specialmente considerando i principi del contraddittorio, della difesa ampia e del divieto di prove ottenute illegalmente, che sono aspetti di rilievo. È in questo scenario che si inserisce l'infiltrazione virtuale della polizia, una tecnica investigativa contemporanea diventata fondamentale nella lotta contro i crimini informatici e la criminalità digitale. L'infiltrazione virtuale della polizia rappresenta uno strumento prezioso nella lotta contro i reati digitali e nella ricerca della giustizia nell'era digitale, presentando vantaggi e sfide uniche. Da un lato, consente la raccolta di informazioni in tempo reale e l'identificazione di individui o gruppi coinvolti in attività criminali, spesso prima che tali reati si concretizzino. Tuttavia, d'altra parte, il suo utilizzo deve essere bilanciato con principi etici, legali e di rispetto dei diritti individuali, garantendo che la sua applicazione contribuisca a un ambiente online più sicuro e protetto. Al fine di garantire che l'infiltrazione virtuale della polizia sia effettuata in modo etico e legale, è cruciale stabilire rigorose salvaguardie. Questo include la necessità di autorizzazione giudiziaria preventiva, la definizione chiara dei limiti dell'azione degli agenti infiltrati, nonché la preservazione dell'integrità delle prove raccolte. Inoltre, è fondamentale garantire il rispetto dei diritti individuali e della privacy dei cittadini durante l'intero processo. Per raggiungere questo obiettivo, attraverso metodi deduttivi e procedure di revisione bibliografica, verrà presentata una panoramica generale dell'istituto dell'infiltrazione della polizia nel suo complesso e dell'infiltrazione virtuale della polizia come aspetto specifico. Quest'ultima è stata introdotta nel sistema giuridico brasiliano dalle Leggi n. 12.850/2013 e n. 13.441/2017, come tecnica investigativa contemporanea diventata fondamentale nella lotta contro i reati informatici e la criminalità digitale. Di conseguenza, la ricerca ha come obiettivo specifico affrontare il tema dell'ottenimento e della materializzazione delle tracce digitali nell'ambito del procedimento penale. Si conclude che sia nei mezzi di prova specificati nel sistema giuridico nazionale, sia per quanto riguarda nuovi metodi di ottenere prove digitali, garantite attraverso la catena di custodia delle prove digitali e un procedimento penale supportato da garanzie fondamentali, si osserva la sufficienza e l'appropriatezza delle norme esistenti nel quadro giuridico attuale.

Parole chiave: diritto processuale penale; diritto probatorio; prove digitali; infiltrazione della polizia; infiltrazione virtuale della polizia; materializzazione delle tracce.

KANDA, Bruna Bárbara Paiz Zeotti. **Infiltration Policière Virtuelle : Matérialisation de traces numériques.** 2024. 177 f. Mémoire (Master em Droit) – Centro Universitário Eurípides de Marília, Fundação de Ensino “Eurípides Soares da Rocha”, Marília, 2024.

RESUMÉ

La société 4.0 représente une évolution marquante dans la manière dont les êtres humains interagissent, travaillent et vivent dans un monde de plus en plus interconnecté et orienté par la technologie. Cette nouvelle phase de la société, également appelée Quatrième Révolution Industrielle, se caractérise par la convergence des technologies numériques, physiques et biologiques, créant un environnement de transformation profonde dans tous les aspects de la vie quotidienne. Au cœur de cette Société 4.0 se trouve une connectivité numérique omniprésente. Les dispositifs intelligents, l'Internet des Objets (IoT), l'intelligence artificielle et l'analyse des données en temps réel permettent une communication instantanée et un échange constant d'informations entre les machines, les systèmes et les individus. Cette connectivité génère une nouvelle dynamique dans les domaines de l'industrie, de l'économie, de l'éducation, de la santé et bien plus encore. Cependant, en s'immisçant dans le domaine de l'Internet, parallèlement aux avantages apportés par l'utilisation de la technologie, une nouvelle forme de criminalité cohabite - les crimes numériques - qui s'est consolidée avec la migration d'infractions communes vers le numérique. Pour cette raison, dans le cadre de la procédure pénale, en particulier en ce qui concerne la production et l'obtention de preuves numériques, la nécessité d'une pratique régie par des normes et des principes découlant du droit processuel est urgente. Surtout en considération des principes du contradictoire, de la défense pleine et entière et de l'interdiction des preuves obtenues illégalement, qui sont des aspects importants. C'est dans ce contexte que s'inscrit l'infiltration policière virtuelle, une technique d'investigation contemporaine devenue essentielle dans la lutte contre les crimes cybernétiques et la criminalité numérique. L'infiltration policière virtuelle représente un outil précieux dans la lutte contre les crimes numériques et dans la quête de justice à l'ère numérique, présentant des avantages et des défis uniques. D'une part, elle permet la collecte d'informations en temps réel et l'identification d'individus ou de groupes impliqués dans des activités criminelles, souvent avant que ces crimes ne se concrétisent. Cependant, d'autre part, son utilisation doit être équilibrée avec des principes éthiques, légaux et de respect des droits individuels, garantissant que son application contribue à un environnement en ligne plus sûr et plus protégé. Afin de garantir que l'infiltration policière virtuelle soit menée de manière éthique et légale, il est crucial d'établir des garanties rigoureuses. Cela inclut la nécessité d'une autorisation judiciaire préalable, la définition claire des limites de l'action des agents infiltrés, ainsi que la préservation de l'intégrité des preuves recueillies. De plus, il est essentiel de veiller à ce que les droits individuels et la vie privée des citoyens soient respectés tout au long du processus. Afin d'atteindre cet objectif, à travers des méthodes déductives et des procédures de revue bibliographique, une vue d'ensemble générale de l'institution de l'infiltration policière dans son ensemble et de l'infiltration policière virtuelle en tant qu'aspect spécifique sera présentée. Cette dernière a été introduite dans le système juridique brésilien par les Lois n° 12.850/2013 et n° 13.441/2017, en tant que technique d'investigation contemporaine devenue essentielle dans la lutte contre les crimes cybernétiques et la criminalité numérique. Par conséquent, la recherche a pour objectif spécifique d'aborder le thème de l'obtention et de la matérialisation des traces numériques dans le cadre des poursuites pénales. Il est conclu que tant dans les moyens de preuve spécifiés dans le système juridique national que dans les nouvelles méthodes d'obtention de preuves numériques, garanties par la chaîne de garde des preuves numériques et par une procédure pénale soutenue par des garanties fondamentales, la suffisance et l'adéquation des normes existantes dans le cadre juridique actuel sont observées.

Mots-clés: droit pénal procédural; droit probatoire; preuves numériques; infiltration policière; infiltration policière virtuelle; matérialisation des traces.

LISTA DE ABREVIATURAS E SIGLAS

Art.	Artigo
CEDH	Convenção Europeia dos Direitos do Homem.
CF	Constituição Federal
CP	Código Penal
CPP	Código de Processo Penal
DEA	*Drug Enforcement Agency*
ECA	Estatuto da Criança e do Adolescente
FBI	*Federal Buerau Investigation*
GDPR	*General Data Protection Regulation*
HC	*Habeas Corpus*
IM	*Instant Messaging*
IMAP	*Internet Messaging Access Protocol*
IMEI	*International Mobile Equipment Identity*
IMSI	*International Mobile Subscriber Identity*
INPE	Instituto Nacional de Pesquisas Espaciais
IOCE	*International Organization of Computer Evidence*
LGPD	Lei Geral de Proteção de Dados
MCI	Marco Civil da Internet
MMS	*Multimedia Message System*
NIJ	*National Institute of Justice*
OSM	*Open Street Map*
PIN	*Personal Indetification Number*
POP3	*Post Office Protocol*
PUK	*Personal Unblocking Key*
SEM	*Search Engine Marketing*
SMTP	*Simple Mail Transfer Protocol*
SMS	*Short Message Service*
STF	Supremo Tribunal Federal
SIGWEB	Sistemas de Informações Geográficas na Web
URL	*Uniform Resource Locator*
WWW	*Word Wild Web*

SUMÁRIO

INTRODUÇÃO

Hodiernamente, estamos experimentando no âmbito jurídico um período caracterizado por uma profusão de leis. A sociedade está em constante transformação, buscando do direito ajustes substanciais e específicos para lidar com as questões que emergem no cotidiano.

Nesse contexto, com uma sociedade contemporânea cada vez mais complexa devido aos avanços tecnológicos e ao amadurecimento intelectual da população em geral, ou seja, do homem-médio, é possível observar um aumento na ocorrência de crimes cometidos no ambiente virtual. Esses delitos são cada vez mais graves e elaborados, e têm um impacto prejudicial em toda a sociedade.

Desse modo, os crimes na sociedade contemporânea refletem a complexidade e as mudanças trazidas pelo avanço tecnológico, pela globalização e pela interconexão das pessoas em níveis nunca vistos. Nesse cenário em constante evolução, os crimes assumiram novas formas e desafios, enquanto os sistemas processuais legais e de justiça se esforçam para se adaptar e responder de maneira eficaz.

Os avanços tecnológicos têm possibilitado uma nova gama de crimes, os cibercrimes. Roubo de informações pessoais, fraudes online, ataques cibernéticos e invasões de privacidade são apenas algumas das formas pelas quais criminosos se aproveitam do ambiente digital para cometer delitos. Esses crimes muitas vezes transcendem fronteiras e desafiam as tradicionais noções de jurisdição, tornando a cooperação internacional fundamental na busca por justiça, e principalmente na cooperação entre os países no que concerne à obtenção de provas, tendo em vista que a globalização trouxe uma maior interconexão entre os países, permitindo que redes criminosas operem em escalas globais, aproveitando-se das brechas e diferenças entre sistemas legais e regulatórios.

Isto porque os delinquentes, sob uma falsa percepção de estarem abarcados sob o manto do anonimato, usufruem dos proveitos da internet para cometer crimes porque acreditam que nunca serão identificados e devidamente punidos diante da falsa sensação de impunidade.

Outro aspecto importante dos crimes na sociedade da informação é a crescente preocupação com crimes de ódio e violência extremista. O acesso fácil à internet e às redes sociais permitiu que ideologias extremistas se espalhassem rapidamente levando a atos violentos e prejudicando a coesão social. A disseminação de desinformação e notícias falsas também tem contribuído para a polarização e a escalada de conflitos.

Os sistemas legais e de justiça estão trabalhando para enfrentar esses desafios, adaptando-se às novas realidades e desenvolvendo estratégias por meio de uma melhora no corpo legislativo para lidar com os crimes contemporâneos. Isto envolve a criação de leis mais abrangentes e atualizadas, à exemplo disto, destaca-se a novel legislativa nº 13.441/2017, que granjeou o advento da técnica especial de infiltração policial na internet, bem como mister se faz o fortalecimento da cooperação internacional, o investimento em tecnologias de investigação e vigilância, a melhora no aparato policial e judiciário e sobretudo a promoção de uma educação pública voltada para a prevenção e conscientização.

É nesse cenário jurídico que se insere o instituto da infiltração policial por meio virtual, tema da presente dissertação, instituto este dedicado a expandir de forma extraordinária as possibilidades de obtenção de provas digitais para o desenvolvimento da persecução penal, atreladas ao respeito e garantias fundamentais e aos sujeitos partícipes da operacionalização.

Para isso, através do método dedutivo e dos procedimentos metodológicos de revisão bibliográfica, doutrinária e legislativa. Ter-se-á como ponto de partida por objetivo geral os textos legislativos que fundamentam a infiltração policial, enquanto gênero e espécie, e buscar-se-á a fonte de produção literária especializada, nacional e estrangeira, sempre que necessário mostrar-se.

Quanto aos objetivos específicos, realizar-se-á um exame da ação penal no Brasil, assim como das provas admitidas no procedimento penal expondo suas principais características além da importância da observação da cadeia de custódia, particularmente no que diz respeito às provas digitais. Em sequência, abordar-se-á o instituto da infiltração policial como método de obtenção de provas, explorando sua regulamentação legal no contexto nacional. Ter-se-á o cuidado de apresentar as particularidades do instituto tanto em solo brasileiro quanto no direito comparado, nos seguintes países: Estados Unidos, Itália, Alemanha, Espanha, França, Portugal e Argentina. Por último, será feita uma avaliação das possíveis formas de materialização das provas obtidas por meio da infiltração policial.

Primeiramente, no primeiro capítulo, será feita uma breve apresentação sobre a obtenção de provas no âmbito do Processo Penal abordando tanto a sua definição abrangente quanto a sua conceituação, enfatizando suas principais classificações: provas documentais, testemunhais e periciais. De maneira similar, o foco será direcionado para a exposição de cada um dos métodos de obtenção de provas já formalmente estabelecidos na legislação processual penal.

Ainda sobre a área temática, será exposta a admissibilidade das provas, as vedações positivadas em lei, e consequentemente, explorar as orientações doutrinárias relacionadas à busca pela verdade real e substancial. Isso serve para exemplificar a perspectiva doutrinária de

que essa verdade é estabelecida por meio dos procedimentos baseados nos princípios do contraditório e da ampla defesa, bem como no princípio do devido processo legal.

Feito o primeiro recorte temático, posteriormente, no segundo capítulo, serão apresentadas as provas digitais no curso da persecução penal, igualmente conceituando-a e explanando suas principais características, tipologias e especialmente caracterizando os meios de obtenção das provas no âmbito digital assim como destacando o instituto da cadeia de custódia e sua importância para assegurar os princípios e garantias fundamentais. Por fim, ao encerrar o tema de provas digitais, implica trazer à lume a importância da cooperação internacional para a obtenção de provas através da ratificação da Convenção de Budapeste, convenção do cibercrime.

Ao final, no último capítulo, é apresentado o instituto da infiltração policial nas suas particularidades, bem como as suas principais características: conceituação, modalidades, requisitos de admissibilidade, bem como os aspectos operacionais. Em seguida, após ser abordado o instituto da infiltração policial de uma forma genérica, analisar-se-á o instituto da infiltração policial por meio virtual que foi introduzido no ordenamento pátrio pelas Leis 12.850/2013 e nº 13.441/2017. Ter-se-á o cuidado de apresentar as particularidades do instituto tanto em solo brasileiro, quanto no direito comparado, nos seguintes países: Estados Unidos, Itália, Alemanha, Espanha, França, Portugal e Argentina.

Por último, será feita uma avaliação das possíveis formas de materialização das provas obtidas por meio da infiltração policial, condensando-se os principais pontos abordados durante a pesquisa e apresentando as considerações finais sobre o tema encimado.

1 DO DEVIDO PROCESSO LEGAL E VEDAÇÃO DA PROVA ILÍCITA

O princípio do devido processo legal é uma pedra angular dos sistemas jurídicos que buscam garantir justiça e equidade nas decisões judiciais. Ele é consagrado como um direito fundamental, servindo como um escudo protetor contra arbitrariedades e garantindo que todos os indivíduos tenham acesso a um processo justo e imparcial. O devido processo legal busca assegurar que nenhuma pessoa seja privada da vida, liberdade ou propriedade sem o devido processo legal.

Paralelamente a esse princípio, a vedação da prova ilícita representa outra salvaguarda fundamental para a justiça. Esta regra impede que provas ilícitas ou inconstitucionais obtidas sejam admitidas no processo, a título de exemplo.

A importância de abordar o tema do devido processo legal e a vedação da prova ilícita se faz necessário em virtude de ambos serem os alicerces essenciais para a justiça e a equidade no sistema processual penal. Servindo como um escudo ao salvaguardar que todos tenham acesso a um processo justo e imparcial.

1.1 Do devido Processo Legal

O princípio do devido processo legal é o cerne do sistema processual; como corolário dos direitos fundamentais a todos, na sua mais ampla acepção, trata-se das estruturas basilares que permeiam todos os demais princípios contidos na cepa processual, garantidor de um processo legítimo, equilibrado e justo.

Em artigo publicado de João Gualberto Garcez Ramos (2007), a origem do devido processo legal no ano de 1215[2], na Inglaterra, reafirmado pelo Rei Guilherme, "O conquistador", quando da sua coroação e se declarou um revente continuador das leis anteriormente editadas, assegurando que as leis editadas por um monarca anterior se tornam, com sua morte, Leis da Terra (*Legem Terrae*).

No ano de 1215, os barões ingleses exigem de Rei João I, o respeito às leis da terra proclamando que "nenhum homem livre será molestado, ou aprisionado, ou despojado, ou

[2] Sobre o tema importante leitura de artigo publicado pelo atual Ministro Luís Roberto Barroso em Revista do Ministério Público do Estado do Rio de Janeiro, que discorre: "O princípio da razoabilidade tem sua origem e desenvolvimento ligados à garantia do devido processo legal, instituto ancestral do direito anglo-saxão. De fato, sua matriz remonta à cláusula "*Law of the land"*, inscrita na *Magna Charta*, de 1215, documento que é reconhecido como um dos grandes antecedentes do constitucionalismo.

colocado fora de lei, ou exilado, ou de qualquer modo aniquilado, nem nós iremos contra ele, nem permitiremos que alguém o faça, exceto pelo julgamento legal de seus pares ou pelo direito da terra".

Estava assim delimitada a essência de um dos princípios norteadores do direito processual. O uso da expressão "devido processo legal" foi declarado pela primeira vez no ano de 1354 quando o Rei Eduardo III positiva as Leis da Terra e, entre elas, a Magna Carta das liberdades. O texto de Eduardo III dispõe que:

> Que nenhum homem de qualquer estado ou condição que ele seja, possa ser posto fora da terra ou da posse, ou molestado, ou aprisionado, ou deserdado, ou condenado à morte, sem ser antes levado a responder a um devido processo legal (Ramos, 2007, p.103).

No cenário norte-americano o devido processo legal originou-se através do *founding father Benjamin Franklin* que positivou o princípio na 5ª emenda da Carta de Direitos, em vigor em dezembro de 1791, e dispôs que "ninguém (...) poderá ser privado da vida, liberdade, ou propriedade, sem o devido processo legal"[3]

No direito brasileiro, o devido processo legal foi incluído de forma substancial na Constituição do Império de 1824, em seu artigo 179, inciso II (Brasil, 1824), e posteriormente foi positivada e enfatizada na constituição de 1988 (Brasil, 1988) conforme comando estampado na Constituição da República Federativa do Brasil em seu artigo 5º, LIV: "ninguém será privado da liberdade ou de seus bens sem o devido processo legal".

O disposto na constituição pátria refere-se a um conjunto de proteções processuais que se conectam à ideia de um estado democrático, fundado em direitos que visam proteger um indivíduo do abuso estatal. Essa coleção de proteções é chamada de Teoria do Garantismo Penal, formulada por *Luigi Ferrajoli*.

A Teoria do Garantismo Penal, não se atém somente à estrita formalidade legal, ou processualismo, mas sim, em salvaguardar os direitos fundamentais inerentes às liberdades individuas, civis, incluindo as do Estado (Ferrajoli, 2002, p.28-29).

A importância dada pelo contributo trazido por *Luigi Ferrajoli* implica na observância das garantias dos direitos fundamentais, nas concepções dos ordenamentos jurídicos, de modo

---

[3] Sobre a inserção do princípio na legislação norte americana, importante a leitura do artigo trazido por João Gualberto Garcez Ramos, uma vez que fatores políticos e étnicos moldaram o princípio do devido processo legal. Políticos porque existiam duas correntes à época, os federalistas e os antifederalistas, e étnicos, porque ainda existia a escravidão, e para o Estado membro do sul, era inadmissível que um princípio fundamental se aplicasse aos escravos, que àquele tempo estariam na condição de "coisa" e não de sujeitos detentores de direitos ou quaisquer garantias.

a dizimar os abusos legais, e que da criação destas normas permita a intervenção mínima do Estado e sofrimento das partes, para um adequado tratamento penal (Ferrajoli, 2002).

Portanto, o Devido Processo Legal advém como princípio corolário constitucional, e dele decorrem os demais direitos fundamentais como a ampla defesa e o contraditório, princípio do juízo natural, princípio da publicidade, princípio da identidade física do juiz, princípio da presunção de inocência, da não autoincriminação, aviso de Miranda (*Miranda rights* ou *Miranda warnings*)[4], dentre outros.

Nesta toada, Marco Aurélio Ferreira, lista as principais garantias atreladas ao princípio do devido processo legal, quais sejam: i) acesso ao sistema de justiça criminal; ii) juiz natural em matéria penal; iii) igualdade de tratamento das partes envolvidas no processo penal; iv) uma gama completa de opções de defesa para o acusado, condenado ou sentenciado; v) publicidade dos atos processuais; vi) duração razoável do processo; vii) decisões motivadas, dentre outras (Ferreira, 2004, p. 60-61).

O devido processo legal (*due process of law*) está adstrito à existência de um duplo aspecto, material e processual, também conhecidos como *substantive due process* e *procedural due process*. O primeiro aspecto material (*substantive due process*) opera na confecção das normas de direito material (legalidade penal); enquanto o segundo aspecto processual (*procedural due process*) resguarda os direitos através de um processo regular.

No mesmo sentindo leciona, Scarance Fernandes (2012, p. 51) "*a doutrina entende que a garantia não se circunscreve ao âmbito estritamente processual, assumindo também uma feição substancial* (…) *a observância da garantia exige que as normas advenham de um processo legislativo de elaboração previamente definido e que não sejam, portanto, injustas.*"

Na mesma toada, para Gustavo Badaró (2021, p.98) o devido processo legal antes estava associado apenas ao aspecto processual, mas que, hodiernamente, ganhou contornos mais amplos, de forma que o *due process of law* (devido processo legal) pode ser dividido em dois aspectos: *procedural due process* e o *substantive due process*.

Ainda, finaliza o autor que:

> O modelo constitucional do devido processo legal no sistema brasileiro é de um processo que se desenvolva perante o juiz natural, em contraditório, assegurada a ampla defesa, com atos públicos e decisões motivadas, em que

[4] Aviso de Miranda trata-se de mandamento constitucional norte-americano, que exige no momento da prisão, o dever de o oficial de polícia ler ao preso os seus direitos, sob pena de não ter validade o que por ele for dito, devendo ser claramente ao preso: i) que ele tem o direito de não responder, ii) que tudo o que disser pode vir a ser usado contra ele e iii) que tem o direito à assistência de um advogado escolhido ou nomeado.

> ao acusado seja assegurada a presunção de inocência, devendo o processo se desenvolver em um prazo razoável. Sem isso não haverá um *due process* (devido processo) ou um processo équo (Badaró, 2021, p. 99-100).

Isso posto, depreende-se que a legitimidade do processo penal decorre essencialmente da prática de contraditório, permitindo ao juiz a formação de sua convicção com base em provas legítimas apresentadas pelas partes em conformidade com o princípio do devido processo legal.

1.2 Da prova no Processo Penal

Feita a conceituação do direito à prova, mister se faz perpassar pela conceituação da instrução probatória. Adiante, para evitar descontextualizações, abordaremos brevemente as principais provas previstas na legislação processual penal do país.

De acordo com Cândido Rangel Dinamarco, a prova é definida como "um conjunto de atividades de verificação e demonstração, por meio das quais se busca alcançar a verdade dos fatos relevantes para o julgamento" (Dinamarco, 2001, p.43).

Em termos de origem, a palavra 'prova' tem suas raízes no latim *probatio* e *probus*, que se derivam, por sua vez, do verbo *probare*, cujo significado abarca reconhecer, demonstrar, "formar um juízo de", verificação e inspeção (Lima, 2016).

Nesse diapasão, o direito à prova representa um legítimo direito subjetivo no que se refere à apresentação das evidências no processo e à participação das partes em todas as etapas do procedimento. Por conseguinte, possui a mesma natureza constitucional dos direitos de ação e defesa.

Portanto, notadamente, o objetivo da prova é contribuir para que o juiz forme seu livre convencimento a respeito da veracidade ou não de uma alegação específica que reclama ser sanada. Assim, pode-se inferir que a prova representa um direito constitucionalmente legitimado para as partes, mas esse direito não é absoluto, uma vez que a admissão de provas deve seguir os princípios do devido processo legal e da inadmissibilidade das provas obtidas de forma ilícita.

Ainda, sobre o direito de provas, prelecionam Grinover, Scarance Fernandes e Gomes Filho (1998, p. 119) que:

> o direito à prova como aspecto de particular importância no quadro do contraditório, uma vez que a atividade probatória representa o momento central do processo: estritamente ligada à alegação e à indicação dos fatos, visa ela a possibilitar a demonstração da verdade, revestindo-se de particular relevância para o conteúdo do provimento jurisdicional. O concreto exercício da ação e da defesa fica essencialmente subordinado à efetiva possibilidade de

> se representar ao juiz a realidade do fato posto como fundamento das pretensões das partes, ou seja, de estas poderem servir-se das provas.

De acordo com as palavras de Antônio Magalhães Gomes Filho (1997, p. 85-89), podemos identificar diversos direitos intimamente relacionados ao direito à prova. Esses direitos incluem a faculdade de investigar, buscar e descobrir provas; a iniciativa das partes em apresentar, indicar e requerer provas; a permissão e introdução dos elementos probatórios propostos e/ou produzidos pelas partes; a exclusão das provas legalmente inadmissíveis; e, por último, o direito de contribuir para a formação e justificação do livre convencimento do magistrado por meio da valoração das provas, como mencionado anteriormente[5].

Após apresentar o conceito do direito à prova, é essencial compreender a noção da instrução probatória, considerando que a palavra "instrução" de acordo com a interpretação de Carnelutti (1950, p. 162), e também, referenciada por Frederico Marques (2000, p. 318), tem sua raiz na expressão "*in-struere*", que remete o provimento de recursos para construir. Nesse sentido, atribui-se ao juiz a capacidade de instrução, possibilitando que ele construa sua decisão ao ser equipado com os meios adequados.

De acordo com Renato Brasileiro, a expressão "fonte de prova" refere-se às pessoas ou objetos que fornecem elementos de prova, e são comumente classificadas como fontes pessoais e fontes reais. As fontes pessoais englobam provas obtidas por meio do ofendido, peritos, acusado e testemunhas, enquanto as fontes reais referem-se aos elementos probatórios provenientes de documentos em sentido amplo (Lima, 2019, p. 611).

Portanto, a inclusão dessas fontes de prova no processo é realizada por meio dos meios de prova. Por exemplo, Badaró esclarece que "a testemunha de um fato é a fonte de prova, enquanto suas declarações em juízo são o meio de prova" (2003, p. 166), fornecendo uma ilustração a esse respeito.

Nessa perspectiva, Eugenio Florian explica que o meio de prova é o momento em que a contribuição probatória alcança sua maior eficiência, permitindo o contato entre o objeto de prova e o juiz, bem como outros sujeitos processuais (1924, p. 1)[6].

---

[5] Importante ressaltar que anteriormente, no processo de natureza inquisitória, as formulações e pesquisas probatórias constituíam tarefa exclusivamente dos órgãos incumbidos da persecução penal – polícia judiciária e Ministério Público –, o que mais tarde passou a ser possível à ambas as partes – acusação e acusado –, com o advento do modelo acusatório, que consagrou o direito à prova sob o pálio processual penal constitucional.

[6] Tradução nossa. No original: "*Il mezzo di prova rappresenta il momento, in cui il cointributo della prova si explica nella sua maggiore efficienza. Per esso si attua il contato fra l'oggeto di prova ed il giudice: per esso l'oggeto di prova viene recato a cognizione del giudice e degli altri soggetti processual"*

Além disso, como mencionado anteriormente, apenas os meios de prova lícitos são admitidos pelo magistrado, conforme previsto no artigo 157 do Código de Processo Penal (Brasil, 1941). É crucial destacar que também são consideradas ilícitas as provas obtidas de maneira imoral, antiética, que violam a dignidade e liberdade da pessoa humana, bem como aquelas que vão de encontro aos bons costumes e princípios gerais, como, por exemplo, provas obtidas através de tortura.

É importante ressaltar que a obtenção dos meios de prova deve obedecer aos princípios do contraditório e da ampla defesa, garantindo o envolvimento efetivo de ambas as partes. Já no que toca ao tema da instrução probatória, conclui-se que consiste em uma série de atos processuais com o propósito de reunir provas para embasar a decisão do litígio.

No que tange à produção de provas, essa ocorre por meio de diversas modalidades que intermediam e possibilitam sua apresentação no âmbito probatório, sendo classificadas em: prova documental, prova testemunhal e prova pericial.

Dentre os meios de prova estabelecidos e incorporados na legislação do processo penal, encontram-se os seguintes: exame do corpo de delito e outras perícias (art. 158 e seguintes); interrogatório (art. 185 e seguintes); confissão (art. 197 e seguintes); oitiva do ofendido (art. 201); inquirição de testemunhas (art. 202 e seguintes); reconhecimento de pessoas ou coisas (arts. 226-228); acareação (arts. 229 e 230); e, documental (art. 231 e seguintes), todos eles dispostos no Código de Processo Penal (Brasil, 1941).

A primeira prova devidamente regulamentada no âmbito penal é a prova pericial, contemplada nos artigos 158 e seguintes do Código de Processo Penal (Brasil, 1941). Conforme Paolo Tonini explica, a perícia desempenha funções essenciais que exigem conhecimentos especializados, ou seja, técnicos, com o propósito de conduzir investigações para coletar dados probatórios. Posteriormente, esses dados devem ser selecionados e interpretados para, então, aplicar uma valoração aos resultados obtidos (Tonini, 2002, p. 183).

Portanto, fica evidente que a prova pericial compreende uma análise direcionada a questões que demandam perícia especializada (*expertise*), com o objetivo de contribuir para a formação do convencimento do juiz (Lima, 2019, p.711).

Sobre o exame de corpo de delito, representa apenas uma das categorias de perícias, e não a exclusiva. Isso se deve ao fato de que outras modalidades de perícia são aceitas conforme o artigo 159 do Código de Processo Penal (Brasil, 1941). Tanto o exame de corpo de delito quanto essas outras formas de perícia possuem a mesma natureza jurídica, sendo consideradas meios de prova que atuam como instrumentos para introduzir fontes probatórias no âmbito do processo. Portanto, o “corpo de delito é o conjunto de vestígios materiais ou sensíveis deixados

pela infração penal para comprovação da materialidade e autoria do delito" (Lima, 2019, p. 674).

Em relação ao interrogatório e à confissão, é importante mencionar que ambas constituem provas obtidas de forma direta ou indireta do próprio acusado. Quanto ao interrogatório, Lima (2019, p. 691) define:

> Interrogatório judicial é o ato processual por meio do qual o juiz ouve o acusado sobre sua pessoa e sobre a imputação que lhe é feita. (...) Portanto, trata-se de oportunidade que o acusado tem de se dirigir diretamente ao magistrado e expor a sua versão dos fatos. (...) ou seja, quer para apresentar a versão da defesa acerca da imputação que recai sobre a sua pessoa, podendo, inclusive, indicar meios de prova, quer para confessar, ou até mesmo para permanecer em silêncio, fornecendo apenas elementos relativos quanto à sua qualificação.

No contexto da confissão, conforme a definição de Lima (2019, p. 711), refere-se à "admissão por parte do acusado de ser responsável pela infração penal, diante da autoridade judiciária ou policial". No âmbito do direito processual penal, a confissão atua como um meio de prova, desempenhando o papel de contribuir para a avaliação e formação do juízo de convicção do magistrado

Em relação às suas características, é importante enfatizar que a confissão é um ato personalíssimo, cabendo exclusivamente ao acusado confessar sobre o ato que incide sobre si mesmo. Além disso, é um ato livre e espontâneo, o que significa que sua manifestação deve ocorrer sem qualquer forma de constrangimento moral ou físico, refletindo a vontade real do indivíduo em confessar.

Conforme preceitua o artigo 197 do Código de Processo Penal (Brasil, 1941), o valor da confissão será avaliado pelos mesmos critérios aplicados aos demais elementos de prova, e o juiz deverá confrontá-la com outras provas do processo para verificar sua compatibilidade ou concordância.

Outro meio de prova, inserido na categoria dos meios de provas, é a oitiva do ofendido, prevista no artigo 201 do Código de Processo Penal (Brasil, 1941), que determina que, "sempre que possível, o ofendido seja qualificado e interrogado sobre as circunstâncias do crime, a identificação ou suposta identificação do autor e quaisquer provas que possa indicar, registrando-se suas declarações".

Com base no exposto, é relevante ressaltar algumas considerações sobre esse meio de prova. Primeiramente, o ofendido não se equipara à figura de uma testemunha, não tendo o compromisso legal de falar a verdade, prestando apenas declarações sobre o ocorrido.

Em segundo lugar, o valor probatório da oitiva do ofendido deve ser relativo, devido à sua não obrigatoriedade de falar a verdade. Como toda prova produzida no decorrer do processo, a oitiva do ofendido deve ser submetida ao crivo do contraditório, em consonância com o artigo 5º, inciso LV, da Constituição Federal (Brasil, 1988).

Por outro lado, temos a prova testemunhal, que, ao contrário da oitiva do ofendido, possui a obrigação de dizer a verdade, uma vez que é considerada um dever e não um direito.

De acordo com Lima, uma testemunha é uma pessoa imparcial e capaz de depor, que perante a autoridade judiciária relata o que sabe sobre os fatos percebidos por seus sentidos, que têm influência direta na decisão (2019, p. 715).

Como mencionado anteriormente, depor como testemunha é um dever e não um direito, e, portanto, a legislação penal brasileira lista as pessoas que podem se recusar a testemunhar e aquelas que são proibidas de fazê-lo.

Em relação ao reconhecimento de pessoas ou coisas, trata-se de um meio de prova em que o indivíduo identifica uma pessoa ou objeto que lhe é apresentado, geralmente com base em informações prévias, e essa identificação ocorre por meio de um ato processual perante a autoridade policial ou judiciária.

Quanto à acareação, é importante esclarecer que é o ato de colocar frente a frente pessoas cujas declarações são divergentes. Portanto, a acareação é o procedimento em que as declarações de dois ou mais acusados, testemunhas ou ofendidos, que já foram ouvidos, sobre algum fato em que suas declarações são divergentes, são confrontadas (Mirabete, 2006, p. 311).

Concluindo a análise das provas regulamentadas na legislação processual brasileira, temos a prova documental, que é estruturada em duas formas. A primeira abrange a prova documental de forma estrita, considerando qualquer escrito ou grafia (seja público ou particular) como documento. Já a segunda, em sentido amplo, conceitua o documento como qualquer objeto representativo que seja relevante, como fotos, filmes, planilhas, mensagens eletrônicas.

O ponto importante, na prática, é que ambas as concepções convergem para a mesma característica: a capacidade da prova documental de expressar o pensamento contido nele e gerar consequências na ordem jurídica.

Por fim, conforme será resgatado posteriormente, é importante destacar que o processo penal brasileiro não se limita aos meios de prova mencionados expressamente na legislação. A

doutrina prevalecente considera que as partes têm liberdade probatória, desde que não violem as garantias constitucionais ou que sejam irrelevantes ou ilícitas[7].

1.3 *Procedural Due Process* e *Substantive Due Process*

O devido processo legal substantivo garante que as leis sejam razoáveis, de modo que o *substantive due process*, segundo Gustavo Badaró (2021), com fundamento em Carlos Alberto de Siqueira Castro (1989, p.383) é:

> Capaz de condicionar no mérito, a validade das leis e da generalidade das ações e omissões do Poder Público. A cláusula, segundo o autor, estabeleceu os dois principais requisitos dos atos estatais, o requisito de razoabilidade (*reasonableness*) e o requisito de racionalidade (*rationality*), que implicam como um tipo de aferição axiológica acerca da justiça das regras do direito.

Segundo Badaró uma lei (ou outro ato normativo qualquer) que não atende à razoabilidade (*reasonableness*) é inconstitucional, por ferir a cláusula do *due process*. E cabe ao Poder Judiciário, desde que foi concebido o judicial *review of legislation*, a tarefa de aferir a justiça da lei (Badaró, 2021, p.99).

Paralelamente, o devido processo legal guarda a sua essência processual, de sorte que, compreende um princípio síntese, que norteia, estrutura e abarca todos os demais princípios e garantias fundamentais asseguradas pela carta magna. Em outras palavras, significa dizer que, tendo a constituição assegurado o devido processo legal, todos os demais princípios dele se derivam.

Ainda, adverte Badaró (2021, p. 99) que:

> não se pode imaginar um *due process* que se desenvolva perante tribunais de exceção ou perante juízes diversos daqueles definidos na constituição. O processo não será devido, de sorte que nem processo será, mas sim um procedimento, se não se desenvolver em contraditório. Um processo secreto e com decisões não motivadas, implica num processo arbitrário. DINAMARCO

[7] Como visto, a legislação processual penal concede uma liberdade probatória às partes, em razão do direito à prova, já delineado acima. Entretanto, esse direito não é absoluto, pois está sujeito às limitações, de modo que, em face a isto, temos o preceito constitucional de inadmissibilidade das provas obtidas por meios ilícitos. Aliás, a prova é ilícita quando obtida em desobediência aos direitos fundamentais resguardados a todos, previstos na Constituição Federal (Brasil, 1988), como, a título de exemplo: a inviolabilidade da intimidade da vida privada, da honra, da imagem (art. 5º, X); inviolabilidade do domicílio (art. 5º, XI); inviolabilidade do sigilo das comunicações em geral e de dados (art, 5º, XII), dentre outras.

Finaliza o autor que o modelo constitucional do devido processo legal deve:

> Se desenvolver perante o juiz natural, declinado na constituição e sob o manto do contraditório, e das decisões motivadas nos termos do art. 93, da CF, bem como, que ao acusado seja-lhe assegurado o princípio da presunção de inocência, e devendo, o processo desenvolver-se em prazo razoável, sob pena, de na ausência de quaisquer um dos princípios fundamentais, incorre em um processo équo (Badaró, 2021, p.99-100).

Para Lopes Júnior (2019, p.35), o processo penal é um caminho necessário para se alcançar a pena e, principalmente, um caminho que condiciona o exercício do poder de penar (essência do poder punitivo) à estrita observância de uma série de regras que compõe o devido processo penal.

Vai além ao asseverar que o processo não pode mais ser visto como um simples instrumento a serviço do poder punitivo, preocupando-se apenas como limitador do poder e garantidor do indivíduo a ele submetido. Mas sim, um instrumento legítimo para se chegar à pena, de modo que só existe quando forem estritamente observadas e asseguradas as garantidas constitucionais.

1.4 Da vedação da Prova Ilícita

Infere-se sobre o tema de prova que, em verdade, há para as partes um direito à prova legitimado constitucionalmente, mas que não implica em um direito absoluto, uma vez que a admissão de provas deve ser pautada em observância aos princípios do devido processo legal e da inadmissibilidade das provas obtidas por meio ilícito, princípios declinados expressamente no artigo 5º, incisos LIV e LVI, da Constituição Federal (Brasil,1988).

Nesse sentido, importante preleção trazida em julgado pelo Ministro Celso de Mello acerca de prova ilícita:

> A ação persecutória do estado, qualquer que seja a instância de poder perante a qual se instaure, para revestir-se de legitimidade, não pode apoiar-se em elementos probatórios ilicitamente obtidos, sob pena de ofensa à garantia constitucional do *due process of law*, que tem no dogma da inadmissibilidade das provas ilícitas, uma de suas mais expressivas projeções concretizadoras no plano do nosso sistema de direito positivo – a Constituição da República, em norma revestida de conteúdo vedatório (CF, art. 5º, LVI), desautoriza, por incompatível com os postulados que regem uma sociedade fundada em bases democráticas (CF, art. 1º), qualquer prova cuja obtenção, polo Poder Público, derive de transgressão a cláusulas de ordem constitucional, repelindo, por isso mesmo, quaisquer elementos probatórios que resultem de violação do direito

> material (ou, até mesmo, do direito processual), não prevalecendo, em consequência, no ordenamento normativo brasileiro, em matéria de atividade probatória, a fórmula autoritária do *male captum, bene retentum* (Mello, 2007).

Entretanto, como dito alhures, este direito à prova não se consagra como um direito absoluto de modo que, na norma vedatória contida na constituição, constrita a liberdade de produção de provas e do mesmo modo sob o comando do artigo 157 do Código Processual Penal.

Segundo a nova redação do artigo 157 do CPP, dada pela Lei nº 11.690/2008, dispõe que "*São inadmissíveis, devendo ser desentranhadas do processo, as provas ilícitas, assim entendidas as obtidas em violação a normas constitucionais ou legais*". Ainda assim, a nova redação não conceituou ou trouxe uma distinção acerca do tema, ficando o mister a cargo da doutrina e jurisprudência que distinguiu a redação sobre os seguintes prismas prova ilícita *stricto sensu* e prova ilegítima.

Ainda acerca do tema de prova, não se deve olvidar sobre a distinção feita entre meio de prova e meio de obtenção de prova; enquanto aquele se refere ao meio através do qual se oferece ao magistrado os meios de conhecimento, de formação histórico-fático, dos quais os resultados poderão ser sopesados na decisão tais como a prova testemunhal, documental, as perícias produzidas, esta está adstrita aos instrumentos que permitem obter-se a prova, produzi-la e chegar até ela. Não se trata propriamente da prova e sim dos meios pelos quais se obtém a prova, como por exemplo, a busca e apreensão, a interceptação telefônica e até mesmo a técnica especial de investigação por meio da infiltração policial.

1.5 Prova ilegal e Prova ilegítima

Inicialmente, se faz necessária a distinção de prova ilegal, prova ilegítima e prova ilícita. Desse modo, prova ilegal é gênero, do qual são espécies a prova ilícita e a prova ilegítima, conforme ensina Grinover (1982, p.98-99) fundamentada em Nuvolone, considera que:

> "A prova será ilegal toda vez que caracterizar violação de normas legais ou de princípios gerais do ordenamento, de natureza processual ou material. Quando a proibição for colocada por uma lei processual, a prova (rectius, o meio de prova) será ilegítima (ou ilegalmente produzida); quando, pelo contrário, a proibição for de natureza material, a prova será ilícita (rectius), a fonte de prova será ilicitamente colhida).

Portanto a autora considera que provas contrárias à lei pertencem ao gênero das provas ilegais, as quais, por sua vez, se subdividem em duas modalidades: provas ilegítimas e provas ilícitas.

A respeito da prova ilícita, não houve uma conceituação por parte do legislador que apenas destacou através do comando constitucional em seu artigo 5º, inciso LVI, da CF, a inadmissibilidade da utilização no processo de provas ilícitas.

Lima (2016, p. 609), preleciona que a prova será ilegal sempre que sua obtenção se der por meio de violação de normas legais ou de princípios gerais do ordenamento, seja de natureza material ou processual, de modo que a prova ilegal é entendida como gênero, das quais são espécies as provas obtidas por meios ilícitos que se diferenciam das provas obtidas por meios ilegítimos.

Nesta toada, a doutrina e jurisprudência conceituam prova ilícita como aquelas obtidas através de violação de regra de direito material penal ou constitucional, ao passo que a prova será considerada ilegítima quando esta for obtida por meio de violação à norma de direito processual.

A título de exemplo, uma confissão tomada mediante o emprego de tortura ou maus-tratos torna a obtenção dessa prova ilícita, por ter violado norma de garantia constitucional disposta no artigo 5º, inciso III, da Constituição Federal. Por outro lado, numa oitiva de determinada testemunha, hipoteticamente, o magistrado se esquece de compromissá-la do dever de dizer a verdade, viola a norma processual contida no art. 203, do Código de Processo Penal, que dispõe sobre a obrigatoriedade de o magistrado compromissar a testemunha antes da colheita da oitiva.

Dessa forma, convém ressaltar o posicionamento de (Grinover, p.98-99, 1982) ao distinguir a prova ilícita da prova ilegítima, leciona que:

> a prova será ilegal toda vez que caracterizar violação de normas legais ou de princípios gerais do ordenamento, de natureza processual ou material. Quando a proibição for colocada por uma lei processual, a prova (*rectius*, o meio de prova) será ilegítima (ou ilegalmente produzida); quando, pelo contrário, a proibição for de natureza material, a prova será ilícita (*rectius*, a fonte de prova será ilicitamente colhida).

Nesse sentido, a autora tem um entendimento mais estrito no que se refere a distinção quanto às "provas ilícitas", entendimento este que, posteriormente, foi adotado pelo Supremo Tribunal Federal, no julgamento no HC de nº 69.912-0/RS (LEX – STF 183/320).

Entretanto, existe a possibilidade de as provas serem obtidas tanto por meio ilícito quanto ilegítimos, ou seja, quando a obtenção da prova viola tanto a norma de direito material quanto a de direito processual, simultaneamente. Por conseguinte, podemos ilustrar uma busca e apreensão domiciliar por uma autoridade policial, sem a devida autorização judicial e, tampouco, em situação de flagrante delito.

No exemplo ilustrado, temos dupla violação: a da norma legal, de modo que a conduta se amolda como crime de abuso de autoridade previsto na Lei nº 4.898/65, artigo 3º, alínea "b", bem como violação da norma processual que estabelece o preenchimento dos requisitos para realização de busca e apreensão domiciliares (CPP, art. 240 a 250).

Antes da inserção do art. 157, sobrevindo da lei nº 11.690 de 2008[8], quando violada uma norma material como, por exemplo, a violação de correspondência, existia uma sanção de cunho de direito material correspondente, no caso, a pena do crime do art. 151, do CP[9]. Ao passo que violada uma norma de cunho processual tal como o exemplo acima já mencionado, a oitiva de uma testemunha sem compromissá-la de dizer a verdade, implicava apenas na aplicação de uma sanção processual, no exemplo citado, a nulidade da prova testemunhal.

De sorte que a constituição ao inserir a inadmissibilidade da prova ilícita, nos dizeres de Badaró (2021, p.456), funcionou como uma ponte que ligou os dois planos, o do direito material e do direito processual. De maneira que a inadmissibilidade se torna uma sanção processual para uma violação de regra material. Atualmente, "as provas ilícitas são sancionadas tanto no plano material com a pena pelo delito correspondente como no campo processual, com a inadmissibilidade de tal prova" e consequentemente o seu desentranhamento.

Todavia, a crítica que se faz ao aludido dispositivo envolve a questão de valoração da prova pelo magistrado. Badaró (2021, p.457) defende a ideia que o simples fato de o juiz ter tido contato com a prova considerada ilegal, e posteriormente, desentranhada, seria o suficiente para fosse difícil para que o julgador desconsiderasse, por exemplo, a autoria delitiva, obtida através de uma escuta telefônica ilícita, no momento de julgar.

Nesse sentido Badaró vai além, ao mencionar a inserção do §5º do art.157, inserido pela Lei nº 13.964/2019, - atualmente com a vigência suspensa por força de liminar do STF -, que dispõe que "o juiz que conhecer do conteúdo da prova declarada inadmissível não poderá proferir a sentença ou acórdão" (Badaró, 2021, p.457.).

---

[8] BRASIL. Lei 11.690 de 2008. Que alterou os dispositivos do Decreto-Lei nº 3.689, de 3 de outubro de 1941 – Código de Processo Penal, relativos à prova, e outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11690.htm. Acesso em: 04 jun 2023.

[9] Art. 151, do Código Penal: "Devassar indevidamente o conteúdo de correspondência fechada, dirigida a outrem: Pena - detenção, de um a seis meses, ou multa".

Para o autor, em que pese a intenção correta do legislador de evitar o que ele chama de "tentação cognitiva", ainda é insuficiente, de modo que o autor defende a hipótese de afastamento absoluto do julgador tão logo tenha se dado o contato com a prova ilícita (Badaró, 2021, p.457).

1.6 Da admissibilidade das provas

Conforme dito alhures, em regra, é vedada a utilização da prova ilícita ou ilegítima no processo penal, devendo ser desentranhadas dos autos e entendidas tal qual não tiverem existido. Entretanto, subsiste em algumas correntes doutrinárias a possibilidade de serem admitidas no processo penal.

E essa possibilidade será apresentada de duas formas; a primeira, através de uma corrente minoritária que acolhe a admissibilidade da prova ilícita a partir da proporcionalidade *pro réu*, e a segunda, que define aqueles que admitem o uso da prova ilícita de modo geral.

A primeira corrente entende que a prova ilícita pode ser admitida e valorada em benefício do réu. Segundo Lopes Júnior (2019, p.398), trata-se da proporcionalidade *Pro Reo*, situações em que se pondera entre dois direitos conflitantes, como por exemplo, o direito da liberdade de um inocente sobre um direito que fora sacrificado na obtenção da prova ilícita.

Temos a título de ilustração, a situação de um acusado que viola, por exemplo, uma inviolabilidade de domicílio a fim de obter uma prova cabal de sua inocência, ou até mesmo, uma interceptação telefônica, propriamente dita, iniciada e executada pelo próprio réu, sem ordem judicial a fim de provar sua inocência.

Ainda sobre a admissibilidade da prova ilícita a partir da proporcionalidade *Pro Reo*, Aury Lopes ressalta que quando da obtenção ilícita da prova para benefício *Pro Reo*, afirma que o réu, neste caso, estaria abrigado pela excludente da legítima defesa ou do estado de necessidade. E mais além assevera ser sustentável também, a tese de inexigibilidade de conduta diversa, consequentemente, excluindo a culpabilidade.

Quanto à segunda corrente, segundo define Aury Lopes, possibilita a admissão da prova ilícita desde que esta não fosse vedada pelo ordenamento processual, independente da violação de direito material. Dessa forma, o "*responsável pela prova ilícita poderia utilizá-la no processo, respondendo em outro processo por eventual violação da norma de direito material, que poderia constituir um delito ou mesmo um ilícito civil*" (Lopes Júnior, 2019, p.395).

Por outro lado, há uma parte de juristas que defendem a inadmissibilidade absoluta das provas, sob o prisma de que na obtenção das provas ilícitas são violados direitos

constitucionalmente amparados. Para essa corrente, a vedação contida no diploma legal deve ser interpretada *ipsis literis*, não havendo azo para eventuais exceções.

1.7 Prova ilícita por derivação e a fonte de prova independente

Preleciona Badaró (2021, p.463) que a *Derivative Evidence Doctrine* (Doutrina da evidência derivada) foi concebida pelo direito norte-americano, conhecida como *Fruit Of the Poisonous Tree* (Frutos da árvore envenenada) e significa dizer que a prova ilícita por derivação é aquela que por si só é lícita, mas que foi obtida através de informações ou elementos decorrentes de uma prova ilicitamente obtida.

Segundo Lima (2016, p.613) "provas ilícitas por derivação, são os meios probatórios que, não obstante produzidos, validamente, em momento posterior, encontram-se afetados pelo vício da ilicitude originária, que a eles se transmite, contaminando-os, por efeito de repercussão causal".

A título de exemplo, é encontrado um cadáver, em cumprimento a um mandado de busca domiciliar (prova lícita), entretanto, a informação sobre o local em que o cadáver foi encontrado foi obtida através de uma confissão por meio de tortura.

Outro exemplo, trazido por Lopes Júnior (2019, p.401) trata da apreensão de objeto utilizado para a prática de um delito, mas que tenha sido obtido por meio de uma interceptação telefônica ilegal ou por meio de uma violação de correspondência eletrônica. Veja, mesmo que o mandado de busca e apreensão tenha sido devidamente regular, constitui um ato derivado do anterior e, portanto, ilícito, de sorte que, o mandado fica igualmente ilícito, contaminado.

Como toda regra tem exceção, não foi diferente com o instituto da prova ilícita por derivação que sofreu severas críticas por conta de sua rigidez pelos juristas norte-americanos. Em decorrência disso, a doutrina norte-americana desenvolveu exceções às *exclusionary rules.* Nos dizeres de Badaró (2021, p.463) admite-se a prova ilícita por derivação nos casos em que há quebra de nexo causal entre a prova ilícita original e a prova derivada, e aponta três exceções *i) attenuation of the taint; ii) independente source e iii) inevitable discovery*.

Para Lima (2016, p.616), o conceito da teoria da fonte independente consiste:

> se o órgão da persecução penal demonstrar que obteve, de forma legítima, novos elementos de informação, a partir de uma fonte autônoma de prova, que não guarde relação de dependência, nem decorra da prova originalmente ilícita, com esta não mantendo vínculo causal, tais dados probatórios são admissíveis, porque não contaminados pela mácula da ilicitude originária.

Para exemplificar a admissão da exceção pela teoria da fonte independente o caso mais emblemático citado pelos doutrinadores se trata do caso *Murray v. United States*, de 1988, policiais ao notarem uma atividade suspeita de tráfico de drogas em uma residência, adentraram ilegalmente na residência e confirmaram a suspeita; posteriormente, solicitaram ordem judicial para mandado de busca e apreensão, mencionando apenas a suspeita e omitindo qualquer menção à entrada anterior. Uma vez que eles tiveram a ordem, eles entraram novamente na residência e levaram as drogas sob custódia. A corte norte-americana entendeu a prova ser válida, de modo que, ainda que os policiais não tivessem realizado a primeira violação de residência, invariavelmente, seria obtido o mandado para ordem de busca e apreensão legítima, simplesmente com base nos indícios iniciais (Suprema Corte dos Estados Unidos, 1988)[10].

A Lei nº 11.690/08 incluiu expressamente no Código de Processo Penal a limitação da fonte independente, nos termos do art.157, parágrafos 1ºe 2º, do CPP "*são também inadmissíveis as provas derivadas das ilícitas, salvo quando não evidenciado o nexo de causalidade entre umas e outras, ou quando as derivadas puderem ser obtidas por uma fonte independente das primeiras*".

Quanto ao comando contido no §2º do art.157, que dispõe: *Considera-se fonte independente aquela que por si só, seguindo os trâmites típicos e de praxe, próprios da investigação ou instrução criminal, seria capaz de conduzir ao fato objeto da prova"*.

Entretanto, a disposição guarnecida no parágrafo 2º da referida lei encontra crítica por parte de alguns juristas, com relação à escrita do texto legal; para estes, o legislador ao definir o conceito de fonte independente o fez de forma ampla e abrangente, abarcando também a definição acerca da descoberta inevitável. Partilham deste entendimento Lima (2016, p. 618) e Badaró (2021, p. 464).

---

[10] Vide. *Murray v. United States*, 487 U.S 533 (1988). ***Justia U.S Supreme Court***. Disponível em : https://supreme.justia.com/cases/federal/us/487/533/. Acesso em: 18 jan. 2024.

Sobre a definição da teoria da descoberta inevitável, Lima (2016, p.617) a define como no "caso de se demonstrar que a prova derivada da ilícita seria produzida de qualquer outro modo - independentemente - da prova ilícita originária, tal prova deve ser validada".

A doutrina norte-americana traz um exemplo de aplicação da teoria da descoberta inevitável, no caso *Nix v. Williams-Williams II*, em 1984: Através de uma declaração obtida de forma ilegal do próprio acusado, foi possível a descoberta da localização do corpo da vítima de homicídio, que estava escondido em uma vala à beira de uma estrada. A corte norte-americana entendeu que em que pese a localização só ter sido obtida por meio da colheita ilegal da declaração do acusado, no caso concreto, ficou demonstrado que um grupo de duzentos voluntários estavam à procura do corpo seguindo um plano que inevitavelmente os levaria à descoberta do corpo desovado (Suprema Corte dos Estados Unidos, 1984)[11].

Assevera Renato Brasileiro de Lima que a teoria da descoberta inevitável não deve ser utilizada baseando-se em elementos de informações de forma especulativa; é indispensável a existência de dados concretos aptos a comprovar que a descoberta seria inevitável. Isto significa dizer não basta um "juízo do possível", mas provável com base em elementos concretos de prova.

O Supremo Tribunal Federal através da "Secretaria de Altos Estudos, Pesquisa e Gestão da Informação e Coordenadoria de Difusão de Informação – Jurisprudências Internacionais[12]" publicou uma pesquisa relacionada ao tema "Admissibilidade da Prova Ilícita", que foi realizada com dados e bases jurisprudenciais estrangeiras das quais se destaca a decisão da Corte Norte-americana sobre a *Independent source* e *Inevitable discovery,* colacionadas abaixo:

> **Independent source Segura v. United States, 468 U.S. 796 (1984)**. A teoria da fonte independente "remete à inaplicabilidade da teoria do *fruit of the poisonous tree* nos casos em que a prova deriva de uma fonte diversa da maculada pelo vício da ilicitude. Ela foi o fundamento da manutenção de condenação de indivíduo que teve seu domicílio ilicitamente invadido por policiais e, quando estes estavam no local, outros policiais ali chegaram munidos de competente mandado e lograram apreender drogas.
>
> **Inevitable discovery - Nix v. Williams, 467 U.S. 431 (1984).** A teoria da descoberta inevitável é semelhante à da fonte independente, com a diferença de a prova já ter sido obtida de maneira ilícita, mas se chega à conclusão que

[11] Vide. *Nix v. Williams*, 467 U.S 431 (1984). **Justia U.S Supreme Court**. Disponível em : https://supreme.justia.com/cases/federal/us/467/431/. Acesso em: 18 jan. 2024.

[12] Supremo Tribunal Federal: "Secretaria de Altos Estudos, Pesquisa e Gestão da Informação e Coordenadoria de Difusão de Informação – Jurisprudências Internacionais". Pesquisa de jurisprudência internacional sobre "Admissibilidade de Prova Ilícita". Disponível em: https://www.stf.jus.br/arquivo/cms/jurisprudenciaInternacional/anexo/PJI52021AdmissibilidadedaprovailcitaV3.pdf. Acesso em: 04 jun 2023.

> ela teria sido certamente descoberta licitamente, e.g., pelo segundo grupo de policiais que, ao dar cumprimento à mandado judicial, descobre que os objetos ilícitos já foram apreendidos pelo primeiro grupo de policiais, que invadiu o domicílio sem que tivessem obtido a competente ordem.

Do exposto, a prova ilícita, portanto, é inadmissível no direito processual, de forma que deve ser considerada como meio de prova inexistente, devendo ser desentranhada dos autos, com exceção de haver quebra do nexo causal entre ela e a prova originariamente ilícita, o que pode decorrer, por exemplo, nos casos de fonte independente ou de uma descoberta inevitável.

Por fim, Lopes Júnior (2019, p.404-405) faz uma crítica aos institutos apresentados. Para o autor, as teses da fonte independente e da descoberta inevitável, mesmo que definidas de forma clara e lógica, revelam uma perversidade ao dependerem da subjetividade do julgador, na medida em que "recorre a conceitos vagos e imprecisos no que tangenciam o nexo causal"e, para o autor, cria-se um tipo de discricionariedade judicial.

1.8 Liberdade Probatória x Rigidez Probatória

No Código de Processo Penal, adota-se a liberdade probatória em sua amplitude desde o momento de prova até a liberdade probatória quanto aos meios de provas. A respeito do momento de prova, no processo penal, as provas podem ser produzidas a qualquer tempo, como exemplo, assim dispõe o art. 231, do Código de Processo Penal: "*Salvo os casos expressos em lei, as partes poderão apresentar documentos em qualquer fase do processo*".

Entretanto, toda regra há uma exceção e com relação ao momento de produção de provas não seria diferente, uma delas está relacionada à apresentação de testemunhas. De acordo com o artigo 41 do Código de Processo Penal (CPP), o rol de testemunhas deve ser apresentado na própria peça acusatória. Quanto à defesa, o momento apropriado é durante a apresentação da resposta à acusação, conforme estipulado no artigo 396-A do CPP. Portanto, se a parte não incluiu a testemunha no momento processual adequado, haveria preclusão temporal, o que impediria que essa testemunha fosse ouvida no processo (Lima, 2016, p. 638).

Apesar disso, é crucial ter em mente que o princípio da busca da verdade autoriza o juiz a produzir provas de ofício durante o andamento do processo. Portanto, mesmo que as partes tenham deixado de apresentar a lista no momento apropriado, nada impede que o magistrado ordene a oitiva dessas testemunhas com base no artigo 156, inciso II, combinado com o artigo 209, caput, do CPP (Lima, 2016, p. 638).

Outra exceção em relação ao momento da produção da prova está prevista no artigo 479 do CPP. Conforme esse dispositivo, durante o julgamento no júri, não será permitida a leitura de documento ou a exibição de objeto que não tenha sido anexado aos autos com antecedência mínima de 3 (três) dias úteis, com ciência à outra parte, cujo conteúdo verse sobre a matéria de fato submetida à apreciação e julgamento dos jurados.

No que se refere aos meios de prova, subsiste no processo penal uma ampla liberdade probatória, de modo que, a parte tem ao seu dispor tanto os meios de produção de provas nominados quanto os meios de produção de provas inominados. O comando do art.155, do Código de Processo penal, corrobora a amplitude da liberdade probatória ao dispor: "*somente quanto ao estado das pessoas serão observadas as restrições estabelecidas na lei civil"*. Portanto, infere-se da norma legal, que desde que o objeto da prova não recaia sobre o estado das pessoas, poder-se-á utilizar qualquer meio de prova.

Entretanto, a liberdade probatória, no Direito Processual Penal, enfrenta algumas restrições como por exemplo, proíbe o uso de provas incompatíveis com os sistemas racionais e contrárias à ética, a moral e aos bons costumes. Outras restrições advêm do preceito fundamental, contido no inciso LVI do artigo 5º da CF/88, que versa sobre a proibição da utilização de provas ilícitas e das provas ilegítimas, visto que a prova ilícita acarreta violação material a direito constitucionalmente protegido como por exemplo no caso de uma confissão obtida por meio de tortura.

Não obstante, mesmo diante da inadmissibilidade das provas ilícitas no processo penal, a proibição não é absoluta, conforme abordado nos tópicos anteriores, a regra sofre a exceção em razão das teorias da fonte independente e da descoberta inevitável, conhecidas como *exclusionary rules* (regras de exclusão). Bem como sob o prisma do garantismo - baluarte da proteção das garantias penais - que também acolhe a admissibilidade da prova ilícita, a partir da proporcionalidade *pro réu.*

1.9 Vida privada x Liberdade probatória

É cediço que no Código de Processo Penal é estabelecida a adoção da liberdade probatória de forma abrangente, permitindo a apresentação de provas em qualquer fase do processo, bem como a utilização de meios probatórios de forma ampla. Entretanto, como foi apresentado, essa liberdade não é absoluta, tendo em visto que sofre a limitação do uso de provas ilícitas e ilegítimas bem como exige o respeito às garantias do devido processo legal.

A liberdade probatória e a proteção da vida privada são questões fundamentais no contexto do sistema legal de qualquer sociedade. Enquanto a liberdade probatória garante aos indivíduos a possibilidade de apresentar evidências para sustentar suas alegações perante um tribunal, a vida privada visa resguardar a intimidade e a privacidade das pessoas contra interferências externas

Em um recorte histórico, a preocupação com a privacidade remonta ao Brasil Imperial (1824), em que o primeiro registro de proteção estava relacionado ao "segredo da carta" e a "inviolabilidade da casa", conceito ligado a propriedade, protegendo o lugar físico e não o conteúdo em si. No entanto, apenas em 1890, com a publicação do ensaio "*The Right Privacy*" pelos advogados *Samuel D. Warren* e *Louis D. Brandeis*, o conceito de privacidade foi considerado como o verdadeiro ponto de partida, visto que apresentaram o conhecido "direito de estar só" e elencaram hipóteses que poderia infringir a inviolabilidade da vida privada (Maldonado, 2020, p.12).

Anos depois, devido as constantes guerras mundiais e a falta de normas de proteção do indivíduo, a Declaração Universal dos Direito Humanos, em seu art. 12[13], estabeleceu o direito a inviolabilidade à vida privada como um direito fundamental do homem. A partir desse momento, foram concebidos inúmeros documentos de iniciativas europeias, como exemplo, a Convenção Europeia dos Direitos dos Homens[14] em 1953, estabelecendo o direito à vida privada e familiar; a Convenção nº 108 de 1981, conhecida como o primeiro instrumento internacional vinculado a proteção dos dados pessoais; a Diretiva nº 45 da União Europeia em 1995, que visava também acerca da proteção de dados pessoais, propagando-se até o surgimento da GDPR (*General Data Protection Regulation)*; e a Carta dos Direitos Fundamentais da União Europeia, em 2000, que no art.8°, n.1 dá direito de proteção dos dados das pessoas.[15]

---

[13] O artigo 12 da DUDH dispõe que: "Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques".

[14] Artigo 8° Direito ao respeito pela vida privada e familiar ao dispor que: "1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar econômico do país, a defesa da ordem e a prevenção das infracções penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros".

[15] Artigo 8° Proteção de dados pessoais dispõe: "1. Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito

No Brasil, durante os anos 90, surgem os primeiros documentos legais sobre esse assunto. Além disso, o Código de Defesa do Consumidor, Lei n. 8.078/90, autorizou o uso de bases de dados de consumidores, garantindo-lhes acesso a "informações armazenadas em cadastros, fichas, registros e dados pessoais e de consumo relacionados a eles", o que motivou a formação da legislação brasileira de proteção de dados (LGPD). Em 1997, a Lei do Habeas Data (Lei 9.507/97) é implementada no sistema jurídico brasileiro, estabelecendo regras para acesso e correção de dados pessoais. Por fim, em 2002, o Código Civil Brasileiro incorpora um capítulo significativo sobre os Direitos da Personalidade, que, mesmo chegando tardiamente, enfatiza a privacidade como um direito subjetivo distinto, não centrado no direito à propriedade.

Ainda em solo brasileiro, no ano de 2011, duas leis significativas foram incorporadas no sistema jurídico, entre elas, a Lei do Cadastro Positivo (Lei nº 12.414/11) e a Lei de Acesso à Informação (Lei nº 12.527/11). A primeira, diz respeito consulta a banco de dados com informações de adimplemento para a formação de histórico de crédito; já a segunda, traz a conceituação de informação pessoal como ligada a pessoa natural identificada ou identificável, assinalando aos órgãos e entidades do poder público a proteção da informação sigilosa e pessoal. Por fim, em 2014, foi implantado no ordenamento jurídico o Marco Civil da Internet (Lei 12.965/2014), garantindo ao cidadão o direito de possuir acesso à internet.

Igualmente, no ano de 2016, foi criada a lei que deu ensejo a LGPD, o Regulamento Geral de Proteção de Dados da União Europeia (GDPR), que versou sobre a privacidade e a proteção de dados, aplicado aos indivíduos europeus e entrando em vigor apenas em 2018. Este regulamento também previa o envio desses dados para além do espaço europeu. O GDPR era aplicado aos indivíduos europeus e entrou em vigor apenas em 2018.

Em suma, é cediço afirmar que a proteção de informações pessoais é decorrente do progresso tecnológico dos últimos tempos, sendo, portanto, uma das facetas da definição de privacidade no ambiente jurídico. Além disso, era fundamental que o universo jurídico, tendo em vista esse progresso, elaborasse normas para a proteção desses novos preceitos, como foi mostrado até o momento pelo contexto histórico o quanto a evolução das normas nacionais e estrangeiras foram cruciais para que a LGPD ganhasse status de lei.

Sobre a Convenção Europeia dos Direitos dos Homens, o autor Jezler Júnior (2019, p. 53) destaca a amplitude na terminologia ampla da CEDH:

---

e de obter a respectiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente".

> A CEDH adotou uma terminologia ampla, que permite o silogismo garantidor do sigilo das comunicações telefônicas e telemáticas, bem como dos dados estanques, ao abranger qualquer modo de ofensa à intimidade, salvo quando presentes determinados valores supostamente superiores à vida privada, quando tais exceções permitirão a aludida ingerência Estatal.

Ainda sobre o mesmo protocolo da CEDH o autor ressalta que diante da mais recente diretriz europeia em março de 2006, o Tribunal Supremo da Espanha já estava considerando a extensão das comunicações eletrônicas e sua monitoração, assim como as informações e trocas presentes nos dispositivos de telefonia móvel. O avanço tecnológico de proporções significativas inevitavelmente impôs à investigação recursos de vigilância tecnológica, como a busca automatizada na internet, vigilância por videovigilância através do uso do *Internet Protocol* (IP) com ativação remota e sistemas de captura de imagens de natureza aérea, infravermelha ou noturna.

Portanto, a liberdade probatória é um princípio essencial do direito processual, que confere às partes envolvidas em um litígio a capacidade de produzir provas para comprovar suas versões dos fatos. Esse princípio assegura que todas as informações relevantes sejam consideradas durante o julgamento, proporcionando maior justiça ao processo. Através da liberdade probatória, testemunhas podem ser ouvidas, documentos podem ser apresentados e perícias podem ser realizadas, garantindo a busca pela verdade dos acontecimentos.

No entanto, a busca pela verdade não pode ocorrer em detrimento da privacidade e dignidade das pessoas envolvidas. A vida privada é um direito humano fundamental que visa proteger a esfera íntima das pessoas, resguardando informações pessoais, segredos familiares e a intimidade do indivíduo. A proteção da vida privada também é essencial para preservar a dignidade das pessoas e evitar abusos e intromissões indesejadas.

Quando a liberdade probatória entra em conflito com a vida privada, os tribunais e a legislação precisam encontrar um equilíbrio delicado. É importante que as partes envolvidas no processo tenham acesso aos meios necessários para comprovar suas alegações, mas também é essencial garantir que a obtenção das provas não viole a intimidade ou exponha informações sensíveis de maneira inadequada.

Quanto ao mencionado equilíbrio, leciona Jezler Júnior (2019, p. 71) nos seguintes dizeres:

> Defender a possibilidade de interceptação de dados telemáticos e sua captação – quando isolados em compartimentos eletrônicos -, sem violação ilegal à intimidade e ao sigilo das comunicações é, em uma via reflexa, também tutelar esses mesmos signos eletrônicos que, com sustentação de entendimento

> diverso, poderiam permanecer sem a proteção constitucional que alguns autores defendem como absoluta. Em contrapartida, admitir tal possibilidade é construir, ao mesmo tempo uma muralha de *standars*, com regras orientadoras fortes, sendo necessária a específica previsão legal por meio de uma norma qualificada e de previsão taxativa.

Em algumas jurisdições, existem regras e diretrizes específicas para garantir que as provas apresentadas sejam relevantes, lícitas e proporcionalmente necessárias para o processo. Isso pode incluir a exclusão de provas obtidas de forma ilegal ou mediante violação de direitos fundamentais.

Na legislação brasileira através da Lei nº 9.296/1996, que trata sobre a interceptação de comunicações telefônicas, dispõe em seu parágrafo único a inclusão e abrangência da interceptação aos sistemas de informáticas e telemáticas, de forma ampla: Art. 1º, parágrafo único: *"O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática"*.

Nucci (2006, p.347) defende a constitucionalidade da disposição trazida pelo parágrafo único do artigo 1º, "Não existe direito sem limitações, o que significa que a comunicação realizada por meio de tecnologias de informação e telecomunicações continua sendo uma versão contemporânea e avançada da comunicação por telefone".

Em sede de jurisprudência, ressalta Jezler Júnior (2019, p. 74) o entendimento trazido pelo STJ, através do julgado do HC nº 315.973 que chancelou o uso da interceptação das comunicações de dados telemáticos através da captação de conversas extraídas pelo aplicativo *Blackberry Messenger*, na operação Lava Jato, homologada com ordem judicial.

É inegável que a tecnologia digital trouxe novos desafios para a questão da liberdade probatória e vida privada, entretanto, com a proliferação de dispositivos eletrônicos e a facilidade de acesso a informações pessoais, é fundamental que as leis e regulamentos acompanhem essas mudanças para garantir a proteção dos direitos individuais.

1.10 Da Verdade Real ou Possível

A finalidade da prova é contribuir para a formação do livre convencimento do juiz, que é o seu destinatário final, sobre a veracidade, ou não, de uma determinada alegação que reclama ser solucionada.

Infere-se a respeito da prova, que, em verdade, "há para as partes um direito à prova legitimado constitucionalmente, mas que não implica em um direito absoluto, uma vez que a admissão de provas deve ser pautada em observância aos princípios do devido processo legal e da inadmissibilidade das provas obtidas por meio ilícito".

Tradicionalmente se dizia que o processo penal mira alcançar a verdade real ou material, contrapondo-se ao processo civil, que, noutro vértice, se contentaria com a verdade formal ou processual. Entretanto, modernamente, tal lição é contradita pela doutrina de escol, que defende ser inatingível a descoberta da verdade histórica dos fatos em julgamento. "Daí se dizer que a busca é da verdade processual, ou seja, daquela verdade que pode ser atingida através da atividade probatória desenvolvida durante o processo" (Lima, 2019, p. 610).

Avançando ainda mais na desconstrução do mito da verdade, Lopes Junior (2019, p.376) adverte que a verdade não é o elemento fundante do processo penal e tampouco a "decisão judicial não é a revelação da verdade (material, processual, divina etc.), mas um ato de convencimento formado em contraditório e a partir do respeito às regras do devido processo. (…) Conquanto, importa é considerar que a "verdade" é contingencial, e não fundante.

A bem dizer, para o festejado doutrinador o que legitima o processo penal não é a pretensão de se fiar na verdade real ou processual, mas, isto sim, o restrito respeito às regras do jogo, ou, melhor dizendo, a observância das regras do devido processo legal.

Noutros termos, a sentença não necessariamente revela a verdade, mas é um ato de convencimento do órgão julgador construído em procedimento informado pelo contraditório, pela ampla defesa e pelo devido processo. Em síntese, a proposta do autor é a de que "a verdade (ainda que processual) não é fundante ou legitimante do processo, senão contingencial. Importa fortalecer o respeito às regras do devido processo e evitar-se o outro extremo – decisionismo, processo inquisitório e sua verdade real" (Lopes Junior, 2019, p. 377).

Sobre verdade substancial (ou material) e verdade processual (ou formal), *Luigi Ferrajoli* define a primeira como parte do modelo substancialista do direito penal, como "*uma verdade absoluta e onicompreensiva em relação às pessoas investigadas, carente de limites e de confins legais, alcançável por qualquer meio, para além das rígidas regras procedimentais*".

Diferentemente, é a distinção trazida pelo citado autor acerca da verdade formal ou processual, regida por meio da estrita observância do contraditório e do devido processo legal:

> A verdade perseguida pelo modelo formalista como fundamento de uma condenação é, por sua vez, uma verdade formal ou processual, alcançada pelo respeito a regras precisas e relativas somente a fatos e circunstâncias perfilados como penalmente relevantes. Esta verdade não pretende ser a verdade; não é obtida mediante indagações inquisitivas alheias ao objeto pessoal; está condicionada em si mesma pelo respeito aos procedimentos e às garantias da defesa. E, em suma, uma verdade mais controlada quanto ao método de aquisição, porém mais reduzida quanto ao conteúdo informativo do que qualquer hipotética "verdade substancial", no quádruplo sentido de que se circunscreve às teses acusatórias formuladas de acordo com as leis, de que deve estar corroborada por provas recolhidas por meio de técnicas normativamente preestabelecidas, de que é sempre uma verdade apenas provável e opinativa, e de que na dúvida, ou na falta de acusação ou de provas ritualmente formadas, prevalece a presunção de não culpabilidade, ou seja, da falsidade formal ou processual das hipóteses acusatórias. Este, ademais, é o valor e, também, o preço do "formalismo", que no direito e no processo penal preside normativamente a indagação judicial, protegendo, quando não seja inútil nem vazio, a liberdade dos cidadãos, justamente contra a introdução de verdades substanciais, tão arbitrárias quanto intoleráveis (Ferrajoli, 2002, p.38).

Ainda sobre a verdade, o doutrinador italiano Malatesta (1927, p.36) trabalha as espécies e subespécies de certeza, ao definir que "*a certeza trata-se de uma percepção, um "estado de alma", que não necessariamente dependente da verdade*" e ao tratar sobre a "noção subjetiva da certeza" preleciona que hodiernamente quanto à determinação de suas espécies como "critérios igualmente objetivo das verdades", e que podem ser objetos à ela, três critérios: i) da necessidade; ii) da constância e iii) da eventualidade:

> A distinção da verdade em necessária, constante e eventual é exactíssima, enquanto se refere à verdade. Mas se quer aplicar esta mesma distinção à determinação das espécies de certeza, e da sua natureza, não se faz mais do que desnaturar a certeza. A certeza não é mais do que um estado subjetivo do espírito humano: seja de que natureza for a verdade, ela só é certa para o espírito humano enquanto se julga conforme ao conceito que dela se tem. É nesta crença da conformidade da noção ideológica com a verdade ontológica, que assenta a essência da certeza; e por isso quando a verdade ontológica nos parece conforme com a noção que dela temos, ela é sempre, e do mesmo modo, igualmente certa para nós, seja qual fôr a sua natureza. Uma, objetivamente, será verdade necessária, outra constante, outra eventual; mas se todas as três nos parecem existentes no mundo da realidade, tal qual nos são presentes ao pensamento, todas as três serão do mesmo modo certas para nós.

E sobre a noção de certeza, nos dizeres de Malatesta (1927, p. 47):

> […] vimos que ela consiste em um estado da alma; e só com isto temos determinado o sujeito. Se a certeza tem uma natureza subjetiva, o sujeito natural da certeza não é, nem pode ser, senão o espírito do julgador. Por virtude de uma simples dedução, poder-se-ia obter sem necessidade de qualquer outra investigação, sob o ponto de vista racional. Mas o movimento histórico gradualmente ascendente da humanidade conduziu, em matéria probatória, à preponderância da substância das provas, com critérios fixados pela lei, determinando em que condições probatórias se deve estar certo, e em quais não: obtiveram-se assim as provas legais.

Quanto à certeza legal, se a certeza consistir em algumas condições predeterminadas pela lei e sujeitas ao "espírito do juiz", o que se busca na certeza legal, não no espírito julgador, mas nos critérios legislativos. Legislativamente, essa certeza pode ter maior ou menor entendimento. De sorte que, é possível não admitir o livre critério do juiz, que ao julgar, será obrigado a condenar, se estiverem preenchidos os critérios de imputabilidade previstos na lei, e se não as encontrar (caso de inimputabilidade legal) deverá absolver; esta é a certeza "completamente legal" (Malatesta, 1927, p.46).

Para Tavares e Casara (2020, P.113) A noção de verdade pertence, portanto, ao domínio da reflexão, que abrange tanto objetos empíricos quanto transcendentais. A verdade, nesse contexto, refere-se a um julgamento de relação, marcando um predicado em relação a determinados objetos, proposições ou declarações, seja sobre entidades empíricas ou princípios concebidos independentemente da experiência. Pode-se classificar como verdadeiros tanto os objetos tangíveis do mundo real quanto os objetos simbólicos que os representam. Nesse sentido, a verdade pode ser derivada das coisas existentes em sua conexão com o pensamento, independentemente de essas coisas serem acessíveis materialmente ou reflexivas em um processo imaterial de autoconsciência ou consciência dos outros.

Para os autores "*uma teoria da verdade dever ser, contudo, uma explicação convincente dos objetos e das proposições*". Assevera ainda, que a veracidade de uma proposição ou declaração resulta de um julgamento e corresponde a uma certa maneira de interpretar a realidade. É crucial lembrar que a realidade sempre envolve uma interação entre o simbólico (o domínio da linguagem e dos limites) e o imaginário (a representação mental das coisas). A causalidade em si não tem valor intrínseco, a menos que possa ser formulada de maneira convincente por meio da linguagem, incorporando tanto imagens quanto ideias, de modo a se destacar com pretensão de validade. Assim como ocorre com a causalidade, o conceito de verdade está sempre ligado a critérios que possam explicar a declaração dentro do contexto de uma explicação persuasiva. Portanto, o conceito de verdade não é algo autoimposto, mas sim

algo inferido a partir de uma forma de explicação, ou seja, de critérios ou teorias que buscam a melhor fundamentação. (Tavares; Casara, 2020, p. 118-119).

Quanto ao critério de determinação de verdade teria, portanto, um caráter normativo, enquanto a teoria da verdade teria uma natureza descritiva. O aspecto normativo se refere a elementos que carecem de qualquer ligação factual (relacionada ao evento em questão), exceto semanticamente. Em contrapartida, a teoria da verdade já estaria ligada a componentes empíricos.

Assevera os autores Tavares e Casara (2020, p.139) que alcançar uma verdade absoluta e incontestável é impossível. Por outro lado, a coesão e consistência de declarações não são suficientes para estabelecer sua correspondência com os fatos. De forma que se pode, atribuir validade ao enfoque deflacionário, mas com a ressalva de que deve se sujeitar a argumentos de refutação. Assim, a coerência das declarações deve estar sempre pronta para ser contestada diante de novas descobertas ou formulações.

Ressalta que na busca pela verdade, é crucial não esquecer que a verdade de uma parte nem sempre reflete a verdade do todo. E discorre que os argumentos racistas apresentados durante o nazismo eram todos logicamente coesos e consistentes com um projeto global discriminatório, mas não eram verdadeiros quando confrontados com a necessidade de preservar a liberdade e a igualdade como condição global para a existência de todos. De modo que o fato de uma declaração ser coerente não implica automaticamente que seja verdadeira.

No que toca aos limites da busca da verdade Tavares e Casara (2020, p. 147) finaliza que no contexto brasileiro, os códigos de processo civil e penal abordam especificamente a validade da evidência da verdade, estabelecendo diretrizes para um procedimento que não surpreenda as partes (assegurando livre acesso, e promova sua participação efetiva no debate sobre o assunto (contraditório), seja apropriado e confiável para comprovar o fato desejado, e que não seja obtido de maneira ilegal. A busca pela verdade não visa alcançar a verdade substancial, mas sim a verdade provavelmente aceita. Portanto, no processo legal, não se busca mais a verdade absoluta, considerando audaciosa a idéia de que o juiz possa alcançá-la exclusivamente por meio de instrumentos legais, uma vez que não há uma verdade real presumida.

Sobre a verdade correspondente Khaled Jr. (2023, p.41) ressalta que a verdade correspondente não é apenas um conceito; trata-se de um critério argumentativo que sustenta a estrutura inquisitorial do processo, a qual persiste mesmo em um Estado Democrático de Direito, onde, idealmente, não deveria haver espaço para abordagens inquisitórias. A flexibilidade do conceito de verdade correspondente permite que ele seja adaptado sob diversas

denominações, como real, substancial e material, mantendo sua essência mesmo em abordagens que defendem uma noção relativa ou aproximativa da verdade. Essas perspectivas continuam a justificar a busca pela verdade como um elemento central do processo.

Para o autor, algumas correntes do direito ainda mantêm, pelo menos em parte, uma abordagem científica reminiscente do século XIX, essencialmente associada à concepção de verdade correspondente, neutralidade e correspondência direta entre o ocorrido e o que o processo alegadamente confirmou, através da convicção do juiz. De acordo com essa visão, amplamente compartilhada por muitos estudiosos, o processo penal é caracterizado por uma lógica que busca uma verdade correspondente à realidade, derivada do que eles definem como "fatos" (Khaled Jr, 2023, p.177).

Ressalta o autor que a verdade não pode assumir uma posição predominante no processo devido à presença de diversas restrições à atividade probatória, inerentes à sua estrutura formal, como a título de exemplo a vedação de provas ilícitas. Embora o processo penal, seja orientado pelo princípio da liberdade dos meios de prova, isso não impede a identificação de certos meios de prova com caráter obrigatório, e em algumas situações, há um sistema que proíbe determinados meios de prova ou modos de obtenção. Nesse contexto, antes de considerar a possibilidade de alcançar a verdade nos âmbitos ontológico e epistemológico, é crucial estabelecer uma fronteira intransponível entre qualquer aspiração nesse sentido e as limitações impostas ao processo na configuração democrática requerida pelo devido processo legal (Khaled Jr, 2023, p.178-179).

Assevera ainda sobre a importância de não ser mais aceitável a “objetificação do acusado”, uma característica marcante da abordagem inquisitória, justificando diversas violações em nome da suposta busca pela verdade. Além disso, a existência de um processo penal que perseguia o acusado como se fosse um inimigo não é mais justificável no contexto democrático atual.

Ainda sobre a verdade correspondente, Khaled faz uma crítica sobra a ambição da verdade, defendida e delineada por Bettiol, Manzine e Leone, que devem ser confrontadas sob o aspecto de fundo epistemológico, no sentido de que, para o autor não existe um mecanismo que possa superar os numerosos obstáculos para alcançar uma verdade que corresponda integralmente à realidade, permitindo a ideia de que o historicamente verificável pode ser obtido sem distorções. Isso representa uma visão antiquada de cientificidade até mesmo para as ciências naturais que a originaram: é uma recusa explícita da complexidade, combinada com uma confiança infundada na capacidade da técnica de extrair a essência do real (Khaled Jr, 2023, p.181).

Defende Khaled que o passado, preservado através de vestígios e recriado narrativamente, não deve ser categorizado exclusivamente como do "Mesmo" ou do "Outro"[16]. Para o autor, a narrativa construída pelo juiz deve ser colocada em uma terceira esfera ontológica: a qual deu o signo do "Análogo", que não exclui completamente as outras duas, mas as reposiciona de maneira apropriada. Por "Análogo", entende-se simultaneamente "Ser-como" e "Não-ser"; uma verdade que opera na constante tensão entre revelação e ocultação, para ser finalmente produzida analogicamente como um artefato narrativo elaborado pelo juiz, a partir de vestígios do passado. Portanto, trata-se de uma verdade produzida analogicamente em forma narrativa, estabelecendo um critério de verdade como uma (re)produção analógica do passado e não como uma correspondência - seja absoluta ou relativa - a um evento pertencente a um tempo passado (Khaled Jr, 2023, p.536).

Dessa forma, não o autor não excluí a verdade por completo, mas apenas a reposiciona para eliminar seu caráter dogmático, pois a concepção de verdade sob o "signo do Análogo" reflete uma abordagem cautelosa, em contraste com a ideia de correspondência do "Igual" que resulta na aceitação de uma busca persecutória impulsionada por uma ambição insaciável pela verdade.

Finaliza o autor que não se resume apenas à necessidade de conter o poder punitivo, o que implica abandonar uma abordagem do processo voltada para a busca da verdade. A impossibilidade intrínseca de alcançar uma verdade correspondente, mesmo que relativa ou aproximada, é o principal argumento para conceder primazia às regras do jogo em detrimento de qualquer aspiração à verdade, resultando em última instância na mera representação. Nesse sentido, argumenta-se que a verdade será, na melhor das hipóteses, contingencial, e a sentença condenatória só pode ser validada se as regras do devido processo legal forem rigorosamente seguidas, maximizando assim as oportunidades de minimizar danos decorrentes de condenações equivocadas (Khaled Jr, 2023, p. 536).

---

[16] Sobre o “Mesmo” e o “Outro” o autor explica que existem duas posições que, na sua perspectiva, são equivocadas: a primeira é sobre a crença na possibilidade de alcançar uma verdade absoluta e a ta segunda é sobre a total desconsideração da verdade. Essas duas posições correspondem aos sinais que o autor denomina como "Mesmo" e "Outro", sendo eles essenciais para a aporia da "passeidade" do passado. Frente ao paradoxo apresentado pela categorização das possibilidades de conhecimento sobre o passado, aborda essa aporia, historicamente insuperável quando se trata do problema da verdade no processo penal. Por um lado, o "Mesmo" representa um excesso epistêmico, já que elimina a distância e, consequentemente, as características fundamentais do evento desejado de ser conhecido: sua "passeidade”, intrinsecamente ontológica e impossível de ser superada por qualquer epistemologia. Por outro lado, ressalta que, se o passado estiver parcialmente preservado na forma de vestígios, não pode ser simplesmente considerado como um "Outro", uma vez que há uma presença que, de certa forma, indica sua existência contínua, tornando inviável a exclusão completa da verdade no conhecimento estruturado a partir dos vestígios do passado (Taruffo, 2005, p.535).

Além disso, para além da busca pela verdade, a presunção de inocência deve ser considerada como alicerce e elemento formador de um processo penal alinhado com os princípios democrático-constitucionais, inclusive no que diz respeito à missão e função do juiz. Isso permite romper com a epistemologia inquisitória voltada para a perseguição do inimigo, cujo cerne é o mito da busca pela verdade (Khaled Jr, 2023, p.542).

O renomado jurista Michele Taruffo defende que existem pelo menos dois tipos de razões pelas quais o conceito de verdade dos fatos no processo é altamente problemático e produz complicações e incertezas relevantes ao nível da definição do papel da prova no processo.

Leciona o autor que o primeiro tipo de razões está relacionado com a conexão entre a concepção de uma verdade especial, seja "judicial" ou "processual", e as ideias de verdade fora do contexto legal. A questão central visa determinar se há uma identidade ou analogia entre essas concepções de verdade, ou se a verdade no processo é genuinamente única ou especial. Para o jurista esta complexidade é agravada pela dificuldade em definir claramente o que se entende por "verdade judicial" e, ainda mais, o que se entende por "verdade" em termos gerais.

Ressalta que diversos juristas frequentemente tentam contornar esse dilema utilizando uma distinção entre verdade "formal" (ou "judicial" ou "processual"), estabelecida no processo por meio de provas e procedimentos, e verdade "material" (ou "histórica", "empírica" ou simplesmente "verdade"), referente ao mundo dos fenômenos reais ou a áreas de experiência além do processo, obtida através de métodos cognitivos diferentes das provas judiciais. A distinção comum entre verdade "relativa", típica do processo, e verdade "absoluta", existente externamente ao processo, também é frequentemente mencionada.

No entanto, questiona-se se a distinção entre verdade formal e material é aceitável por várias razões evidenciadas por doutrinas mais aprofundadas. Em particular, a ideia de uma verdade judicial completamente "distinta" e autônoma da verdade em geral parece insustentável, baseando-se apenas no fato de ser determinada no processo e por meio de provas. As regras e limites legais, no máximo, excluem a obtenção de verdades absolutas, mas não são suficientes para diferenciar completamente a verdade estabelecida no processo daquela que é discutida fora dele (Taruffo, 2005, p.24-25).

Para Taruffo, é crucial ter em mente que a busca pela verdade é um objetivo fundamental do processo e uma condição indispensável para a justiça da decisão, embora não seja o único propósito que o processo busca atingir: ele também é um contexto em que normas são aplicadas, valores são realizados, garantias são asseguradas, a liberdade dos indivíduos é protegida, a autoridade do Estado é manifestada e disputas são resolvidas por meio de decisões desejadas

como justas. Segundo o autor, a verdade deve ser concebida sob o "signo correspondente", mesmo que de maneira relativa.

Ainda, a constatação de que o processo não visa estabelecer verdades absolutas e imutáveis parece ser bastante evidente, implicando que só faz sentido considerar verdades relativas. No entanto, essa constatação não implica uma diferença fundamental entre a verdade formada no processo e aquela formada fora dele, pois esta última também é intrinsecamente relativa (pelo menos quando se pensa em verdades nas afirmações empíricas relacionadas a eventos materiais). Em todo caso, é conveniente distinguir pelo menos dois sentidos nos quais se pode afirmar que a verdade estabelecida no processo é relativa.

Para o autor essa verdade é relativa devido aos limites impostos aos instrumentos cognitivos que podem ser empregados para determiná-la. Mesmo admitindo a possibilidade de uma verdade absoluta que pudesse ser estabelecida caso houvesse meios cognitivos ilimitados, a verdade do processo é relativa porque os instrumentos cognitivos disponíveis são restritos, seja pelo tempo, pelas capacidades humanas ou pelas normas. Esta abordagem, no entanto, é quase sem sentido, dada a natureza imaginária da situação de uma verdade absoluta alcançável por meio de recursos cognitivos ilimitados (Taruffo, 2005, p.187-188).

Por fim, acerca da distinção de verdade absoluta ou objetiva convém traçarmos a distinção elucidada por (Ferrajoli, 2002, p.44), no sentido de que é dispensável falar em verdade objetiva ou em verdade absoluta. Posto isto, a verdade não passa de um ideal inatingível. Como não há verdade substancial no sistema de justiça criminal, apenas uma verdade aproximada ou verdade processual, seria ingenuidade acreditar em uma verdade que não pode ser superada.

Ainda, não se pode olvidar a garantia constitucional advinda do art. 5º, inciso LXIII princípio do "*nemo tenetur se detegere*", que garante o direito constitucional outorgado ao acusado de permanecer em silêncio e de "não produzir provas a si mesmo". Isto significa dizer que no jogo das provas, onde o acusado tem o direito ao silêncio, e o de não produzir provas contra si mesmo, podendo mentir e omitir fatos que diretamente ou indiretamente o incrimine, é utopia alvitrar uma verdade absoluta, e sim, uma mais próxima possível que permita a reprodução fática da maneira como sucederam.

2 DAS PROVAS DIGITAIS

2.1 Conceito

Num primeiro momento podemos emprestar a conceituação sobre prova trazida na Convenção de Budapeste[17], do ano de 2011, muito embora tal definição utilizar-se da expressão "dados informáticos" poder-se-á ser interpretada nos seguintes termos:

> Art. 1º […] b) "Dados informáticos" significa qualquer representação de factos, de informações ou de conceitos sob uma forma suscetível de processamento, num sistema de computadores, incluindo um programa, apto a fazer um sistema informático executar uma função […]

Outra definição trazida por Paulo Roberto de Lima Carvalho (2009, p.87), que conceitua a prova cibernética como sendo:

> O registro de um fato, originariamente, por meios eletrônicos ou tecnológicos, documentado sob a forma digital, através de codificação binária, capaz de ser traduzido para uma linguagem inteligível ao homem, dotado de abstração quanto ao meio em que ocorreu o fato objeto do registro e a respectiva forma de armazenagem, presente a portabilidade do código binário para suporte material diverso, conservando a integridade original do registro, sua autenticidade e possibilidade de utilização sob a forma de pelo menos outra mídia que não a originalmente obtida.

Benjamim Silva Rodrigues (2009, p.722), define "prova *electrónico-digital*" como qualquer tipo de informação, com valor probatório, armazenada em repositórios eletrônicos-digitais de armazenamento ou transmitida em sistemas e redes informáticas ou redes de comunicações *electrônicas*, privadas ou publicamente acessíveis, sob a forma binária ou digital"

Denise Vaz (2012, p.63) define prova digital como "*dados em forma digital (no sistema binário) constantes de um suporte eletrônico ou transmitidos em rede de comunicação, os quais contêm a representação de fatos ou ideias*".

Trazendo uma definição por parte da doutrina americana (Casey, 2011, p. 07) conceitua prova digital como "quaisquer dados armazenados ou transmitidos usando um computador que suportem ou refutem a teoria de como ocorreu um crime que aborde

[17] Trata-se a Convenção de Budapeste do primeiro documento internacional que conceitua, define e traça diretrizes acerca do cibercrime.

elementos-chave do crime, como intenção ou álibis", ou seja, é uma evidência digital relevante (tradução nossa)[18].

E por fim, citando a conceituação trazida pelo *National Institute of Justice* – NIJ[19], define evidência digital como a "informação armazenada ou transmitida em formato binário que pode ser invocada em tribunal. Pode ser encontrado no disco rígido de um computador, num telemóvel, entre outros locais" (tradução Nossa).[20]

Importante ressaltar que a definição trazida pelo site do Departamento de Justiça dos Estados Unidos é bem similar a definição trazida pela conferência de 1999, da *International Organization of Computer Evidence* (IOCE)[21].

De forma mais ampla, Dário José Kist (2019, p. 107) conceitua prova digital desde o seu sentido etimológico, ao lecionar que a palavra "digital" tem sua origem no termo "dígito", o qual refere-se a cada um dos algarismos arábicos, ou seja, os números de zero a nove. Esse conceito é relevante devido ao fato de que os sistemas de computação manipulam informações por meio do sistema binário. Esse sistema é utilizado pelas máquinas que possuem circuitos digitais para interpretar dados e realizar ações. Funciona como uma forma de linguagem através da qual o computador processa textos, números e imagens. Isso ocorre porque o computador lê apenas sinais elétricos em sua forma mais básica, representados pelos números 0 e 1, correspondendo, respectivamente, à ausência e à presença de corrente elétrica.

---

[18] Traduzido do original : "*any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi*" (Casey, 2011, p.07).

[19] NIJ é a agência de pesquisa, desenvolvimento e avaliação do Departamento de Justiça dos Estados Unidos.

[20] *Digital evidence is information stored or transmitted in binary form that may be relied on in court. It can be found on a computer hard drive, a mobile phone, among other place s. Digital evidence is commonly associated with electronic crime, or e-crime, such as child pornography or credit card fraud.* Disponível em: https://nij.ojp.gov/digital-evidence-and-forensics. Acesso em 09 mai 2023.

[21] Uma das organizações internacionais mais antigas a lidar com evidências digitais é a IOCE. Formado em 1995, tem servido tanto como um fórum para o intercâmbio de informações e um líder no desenvolvimento de padrões. Apenas dois meses depois o último Simpósio de Ciência Forense da INTERPOL, o Subgrupo de Crimes de Alta Tecnologia do G-8 pediu à IOCE que empreendesse o desenvolvimento de normas que permitissem para a troca de evidências digitais além das fronteiras nacionais. Reconhecendo que seria difícil conseguir isso nas reuniões anuais, o IOCE procurou grupos forenses digitais regionais e nacionais para promover o trabalho durante todo o ano enquanto permite uma maior participação. Durante a reunião de outubro de 1999 da IOCE (organizada pela ACPO/FCG), um conjunto de cinco princípios e definições que os acompanham foram desenvolvidos e acordados. Esses foram então submetidos ao Subgrupo G-8 sobre Crimes de Alta Tecnologia e com menor edição foram adotadas pelo Grupo Lyon do G-8. Disponível em: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=aa826d53e724c61f9e71afe9a8e293b046bd9dcb. Acesso em 09 mai 2023.

Para o autor o termo “prova digital” significa dizer que esta é dotada de natureza digital, de modo que “*os sistemas digitais utilizados pelos dispositivos informáticos e por meio dos quais processam e transmitem informações e dados. E quando, transmitindo dados, o dispositivo informático é instrumento para a prática de ilícito penal, as evidências deste também terão esta característica digital*”.

Ainda, na concepção de Thamay e Tamer (2022, p.33) a prova digital é conceituada como:

> instrumento jurídico vocacionado a demonstrar a ocorrência ou não de determinado fato e suas circunstâncias, tendo ele ocorrido total ou parcialmente em meios digitais ou, se fora deles, esses sirvam como instrumento para sua demonstração. A prova digital é o meio de demonstrar a ocorrência de um fato ocorrido em meio digital, ou que tem no meio digital um instrumento de demonstração de determinado fato de seu conteúdo.

Depreende-se dos conceitos colacionados que prova digital corresponde a fonte de prova, da qual se podem extrair informações que concernem à persecução penal.

2.2 Características da prova digital

Para Denise Vaz (2012) as provas digitais se destoam dos outros tipos de provas, no que concerne ao seu “registro, extração, conservação e sua apresentação em juízo, de modo que as provas digitais possuem características inerentes e individualizadas, e para isso ela cataloga a prova digital em quatro características: i) imaterialidade e desprendimento do suporte físico originário; ii) volatilidade; iii) suscetibilidade de clonagem; e iv) necessidade de intermediação de equipamento para ser acessada.

Trata-se a característica da imaterialidade o que “não é feito de natureza material, intocável, impalpável”. Essa característica, quando atrelada à prova digital se refere aos dados informáticos ou *bits*, que possuem sua existência imaterial, impalpável, mas que existem através de impulsos elétricos.

De forma que os dados digitais não prescindem de suporte físico originário para existir, e tampouco impede a transferência entre outros dispositivos eletrônicos, e possibilitam o armazenamento em larga escala de quantidade, devido ao fato de não ocuparem espaço físico.

A volatilidade no sentido figurado caracteriza aquilo que muda de forma fácil ou frequente, incerto, inconstante; instável[22].

Na sua imaterialidade, um dado digital revela-se frágil porque está facilmente sujeito a alterações ou desaparecimento com base em alterações na sequência numérica subjacente.

Como resultado, é possível perder qualquer informação armazenada digitalmente e/ou sofrer alterações que prejudiquem sua credibilidade de forma acidental ou intencionalmente. Em razão de sua instabilidade, que facilmente sujeita-se a modificações e dispersões.

Segundo Vaz (2012, p.69) a clonagem é um método usado em genética que produz organismos idênticos. Quando aplicada à informática, permite a criação de uma cópia completa de um documento digital, que contém todos os *bits* que compõem esse documento. Técnica da qual muitas vezes são referidas como "espelhamento" ou "imagem".

Dando sequência ao raciocínio trazido por Denise Vaz (2012), quanto à quarta característica que trata da "Necessidade de Intermediação", conclui que o dado digital por ser uma sequência numérica, prescinde da utilização de um equipamento capaz de processar a informação, dispondo-a de maneira inteligível para o homem-médio.

De modo semelhante, Paulo Roberto de Lima Carvalho delimita cinco características como "requisitos fundamentais caracterizadores" que devem ser preenchidos cumulativamente para ensejar a admissão da prova cibernética na persecução penal ou cível:

> a) Ocorrência de um fato originado ou capaz de ser registrado por um meio tecnológico ou eletrônico que assegure a sua autenticidade;
> b) O fato deve ser documentado sob a forma digital através de um código binário (conjunto de *bits*) capaz de ser traduzido para uma linguagem inteligível ao homem;
> c) O conjunto de dados deve ser armazenado em um suporte material mantendo a sua integridade original;
> d) Ocorrência de abstração quanto ao meio em que ocorreu o fato objeto do registro e quanto à forma em que foi originalmente do registro do fato;
> e) Portabilidade de o código binário, para outro tipo de suporte material, conservando a integridade original do registro do fato;
> f) Possibilidade de o código binário, para um mesmo fato documentado, gerar uma forma diferenciada de mídia apresentação do conteúdo registrado, mantendo sua integridade.

Quanto ao aspecto da autenticidade, Paulo Roberto leciona que a autenticidade de um evento que teve origem ou foi registrado por meio tecnológico está relacionada com a

[22] Segundo definição extraído do dicionário Preberam. Disponível em: https://dicionario.priberam.org/vol%C3%A1til. Acesso em 12 mai 2023.

capacidade de se determinar a fonte e atribuir a autoria da origem ao registro. A título de exemplo, o autor ilustra um radar móvel digital usado para monitorar o tráfego em estradas, o qual deve possuir mecanismos de identificação exclusiva que garantam a procedência do registro feito para cada infração de excesso de velocidade.

Quanto à parte do registro e armazenamento, o autor ressalta que as infrações são registradas de forma digital, utilizando um código binário composto por uma sequência lógica e ordenada de *bits* que é entendida apenas por máquinas, mas que pode ser traduzida para uma linguagem compreensível para o homem. Esse conjunto de *bits* deve ser preservado/armazenado em um meio físico, garantindo a sua integridade original, o que reflete a precisão e "fidelidade" do registro do evento.

O requisito da característica da abstração é tratado pelo autor como "*característica da abstração, liga-se ao conceito de que há uma total desvinculação quanto ao meio em que originariamente o ocorreu o fato objeto do registro e a forma em que foi originalmente armazenado*". Na mesma linha exemplificativa, seria hipoteticamente, o guarda de transito constatar por meio de um radar portátil, um condutor trafegando em excesso de velocidade e lavrar o auto de infração manualmente.

O penúltimo requisito que trata da portabilidade, se relaciona com a capacidade de transferir o registro eletrônico de um evento para um meio físico alternativo, garantindo que ele permaneça íntegro e fiel ao registro original. No caso mencionado, o registro eletrônico da infração é transferido para o papel, que desempenhará o papel de um novo suporte material para o evento.

E por fim, o autor trata como último aspecto da possibilidade de o código binário, para um mesmo fato documentado, gerar uma forma diferenciada de mídia apresentação do conteúdo registrado, mantendo sua integridade: que o autor faz uma associação de que "*um mesmo código eletrônico é capaz de apresentar o mesmo fato sob formas distintas*".

Neste caso, o autor ilustra a possibilidade de um conteúdo de uma filmadora digital que contêm um fato de uma colisão de veículo, que a partir de capturas estáticas, sob a forma de fotos que podem ser impressas, e convertidas, ou melhor dizendo, transportados para o papel a fim de instruir um conjunto probatório na esfera cível. Neste exemplo, têm-se um meio digital dinâmico, através da filmagem, e o transporte para outro material físico, sob a forma de papel.

Sobre o tema encimado, Kist ressalta que a literatura especializada frequentemente enfatiza a inapropriada comparação entre a prova digital e a prova física, alertando para o risco de considerar a prova digital como uma extensão da prova física e tentar regulá-la com base

em analogias aos sistemas concebidos para a evidência física. Dado que essas duas realidades são fundamentalmente diferentes, elas exigem abordagens jurídicas igualmente distintas. De modo que a prova digital deve ser sujeita a um quadro jurídico independente, com poucas ou mesmo nenhuma referência a outros sistemas, e deve incluir diretrizes sobre como obter diversos tipos de evidência digital, garantindo a confiabilidade (fidedignidade) na coleta e preservação da cadeia de custódia, levando em consideração as peculiaridades do ambiente digital (Kist, 2019, p.117-118).

Acerca da caracterização das provas digitais, Dário José Kist elenca as seguintes características da prova digital: i) Imaterialidade ou invisibilidade; ii) Volatilidade e fragilidade e iii) dispersão.

Sobre a característica da imaterialidade ou invisibilidade, o autor explica que a prova analógica é intrinsecamente vinculada a uma forma material, pois sua representação depende de um suporte físico de tamanho variável, sem o qual ela não pode existir. Em contraste, a prova digital consiste essencialmente em uma sequência de *bits* e existe de forma independente do suporte físico em que é armazenada. Embora a prova digital precise de um suporte material para ser transportada, sua existência não está limitada a esse suporte e não se reduz a ele. Portanto, a necessidade de mediação por sistemas informáticos com várias tecnologias faz com que a prova digital seja interpretada de maneira distinta em cada um desses sistemas.

Já no que toca a característica da volatilidade e fragilidade, a prova digital é frágil, pois, se for manuseada de maneira negligente, suas características podem ser comprometidas ou até mesmo desaparecer. Essa manipulação pode ocorrer de duas maneiras: pelo próprio usuário do sistema de informática que acessa os dados, realiza edições e depois salva o arquivo, ou de forma automática pelo sistema operacional. Além disso, em situações em que a prova pode ser acessada remotamente, um terceiro com interesse em alterar ou eliminar a prova pode fazê-lo à distância, o que também contribui para a mencionada fragilidade da prova digital.

A prova digital é volátil, pois pode desaparecer devido a diversos eventos que podem ser causados deliberadamente pelo usuário ou ocorrer de forma acidental. Isso inclui situações como a falta de energia para alimentar o dispositivo que armazena o sistema de informática, levando ao desligamento do sistema, a sobreposição automática ou não de novos dados sobre os dados antigos, ou o fato de que alguns tipos de informações são naturalmente temporários e são apagados após um período específico ou a ocorrência de um determinado evento.

Quanto a estas duas características, o autor ressalta a importância de uma abordagem e tratamentos técnicos qualificados para sua produção, seja no momento de acessar o

conteúdo, quanto no momento de custódia e preservação, sob pena da não observação da estrita metodologia implicar na perda relevante dos dados.

Nesse sentido, arremata o autor, a importância de seguir uma metodologia rigorosa, principalmente, no que diz respeito ao acesso a dados cifrados ou criptografados:

> Essa observação vale de modo especial para acessar dados cifrados ou criptografados, acessar o "metadata", isto é, extrair os dados sobre dados, como a data e hora em que o arquivo foi criado, acessado ou modificado, quem tinha permissão para esse acesso, o nome constante no computador ou no *software*, a última pessoa que editou o arquivo; no caso de *e-mails*, quem foram os destinatários incluídos em *blind carbon copy* – "bcc" (em português, com *cópia oculta* ou *cco*; na análise de fotografias, o próprio arquivo que a contém pode também conter o número de série da máquina fotográfica utilizada e outros dados sobre esta e que podem conduzir à pessoa que a utilizou no momento; há aparelhos, como é o caso dos *smartphones* e *tablets* e algumas máquinas fotográficas, que utilizam, no momento da operação, os *geo-tags*, que revelam a localização geográfica do aparelho e o momento em que a imagem foi capturada (Kist, 2019, p. 119-120).

A última característica trazida por Kist trata-se da dispersão, que o autor divide em duas dimensões. A primeira refere-se a prova digital poder estar situada em locais diferentes, mas dentro de um mesmo sistema informático; a segunda dimensão trata da dispersão da prova digital em seu aspecto geográfico.

Na primeira dimensão, a prova digital pode ser dispersa em distintos locais dentro do sistema informático em questão. Por exemplo, algumas evidências de um determinado evento podem ser encontradas na seção designada para o armazenamento de arquivos, enquanto outras podem estar em cache. Além disso, parte das evidências, como imagens ou vídeos, pode estar alojada em um local específico destinado a esse fim, ou ainda em diários digitais, caixas de *e-mail* variadas, dependendo do número de contas que o usuário tenha e acesse através do sistema informático sob análise.

Na segunda dimensão, a dispersão da prova digital diz respeito à sua localização geográfica. Isso significa que os dados que compõem essa evidência podem estar distribuídos em diversos lugares ao redor do mundo, devido ao fato de os provedores de serviços, especialmente de armazenamento, terem suas sedes espalhadas globalmente. Portanto, se uma comunicação percorreu vários desses provedores desde o sistema informático de origem até o de destino, o que é bastante comum, em cada um deles haverá vestígios a serem coletados. O mesmo ocorre quando a informação desejada está armazenada em partes, em servidores

diferentes, os quais também podem estar situados em locais distintos, uma situação típica em dados armazenados na nuvem.

Como visto, a maioria dos autores convergem no sentido que os dados digitais não necessitam de um suporte físico original para existir, e também podem ser transferidos entre outros dispositivos eletrônicos. Bem como ressaltam a fragilidade e a volatilidade da prova digital, e a importância da necessidade de observar uma metodologia rigorosa tanto no acesso quanto na recolha destas provas, evitando que as mesmas sejam alteradas e/ou destruídas.

2.3 Prova digital vs. Prova Eletrônica

A distinção entre prova eletrônica e prova digital é fundamental no contexto jurídico e tecnológico, delineando nuances significativas no modo como informações são apresentadas e validadas em processos legais e transações digitais.

A prova eletrônica abrange qualquer tipo de evidência que seja gerada, armazenada ou transmitida eletronicamente. Isso inclui não apenas documentos digitais, como *e-mails*, mensagens de texto e registros de atividades *online*, mas também dados de sistemas de vigilância, gravações de áudio e vídeo, entre outros. A natureza da prova eletrônica é mais abrangente, englobando qualquer forma de informação digital que possa ser relevante para a persecução penal.

Por outro lado, a prova digital está relacionada especificamente a dados ou documentos digitais que são apresentados como evidência em um contexto legal. Isso pode incluir contratos eletrônicos, registros financeiros digitais, capturas de tela, registros de metadados e muito mais. A prova digital é espécie da prova eletrônica, focando nas informações contidas em formatos digitais que podem ser usadas para demonstrar fatos relevantes em um caso.

Dessa forma, Kist (2019, p. 108) reconhece a conexão de gênero e categoria entre prova eletrônica e prova digital:

> (...) identifica-se uma relação de gênero e espécie entre prova eletrônica e prova digital, aquela sendo o gênero e esta a espécie. Com efeito, e tendo em consideração que a eletrônica abrange todo e qualquer dispositivo que funcione a partir do movimento de elétrons em semicondutores, no vácuo e nos gases, podem ser classificadas como eletrônica as provas existentes em formato analógico, como eram as gravações de vídeo e áudio feitas em fita-rolo e as imagens gravadas no assim chamado filme fotográfico que depois era revelado (a câmera analógica utilizava um filme fotográfico na captura da imagem, que pudesse ser vista fazia-se necessária a revelação do filme; esses dados analógicos não se confundem com os de natureza digital, isto é, aqueles produzidos e processados a partir da lógica binária acima mencionada e que, por

> conta dela, são chamados de dados digitais (é o caso de fotografias, vídeos e todo e qualquer dado que tenha a natureza digital por haver sido produzido desse modo, independentemente do local em que se encontre armazenado – CD (*compact disc*), pen drive, cartão de memória ou na memória interna dispositivo utilizado para a produção/captura). Mas tanto os dados com formato analógico como os que têm natureza digital pertencem ao mundo da eletrônica, e é essa razão pela qual se afirma que o gênero é a prova eletrônica, sendo as provas analógicas e as digitais suas espécies, sem descuidar que no campo da cibercriminalidade interessa apenas o estudo da prova digital.

Acerca da temática, Vaz (2012, p.65) diferencia prova digital da prova eletrônica, de forma que "*a prova digital corresponde aos dados binários, e a prova eletrônica está diretamente relacionada aos suportes físicos que armazenam os arquivos digitais*".

Portanto, enquanto a prova eletrônica compreende um leque mais amplo de evidências, a prova digital se concentra especificamente nas informações contidas em formatos digitais. Ambas as formas de prova têm implicações significativas no campo jurídico, onde a autenticidade, integridade e origem das informações são essenciais para estabelecer a validade de argumentos e fatos.

2.4 Convenção de Budapeste

A Convenção de Budapeste, também conhecida como Convenção sobre o Cibercrime (CETS nº 185), foi elaborada em 21 de setembro de 2001, contando com a adesão de mais de quarenta países, incluindo os Estados Unidos da América, Canadá, Japão e África do Sul. Seu objetivo é estabelecer uma política criminal unificada para proteger a sociedade contra a criminalidade virtual, reconhecendo a importância de uma legislação atualizada diante do avanço tecnológico.

Em termos gerais, a Convenção de Budapeste busca promover um tratado internacional que harmonize as leis penais e processuais referentes aos cibercrimes. Representando o mais abrangente instrumento jurídico nesse âmbito, ela busca, por meio da cooperação internacional, combater os crimes cibernéticos, abordando temas como a segurança de redes de computadores, violações de direitos autorais, fraude digital e pornografia infantil. O acordo entrou em vigor em 01 de julho de 2004.

Além disso, a convenção promove a cooperação internacional entre os países signatários, incentivando a troca de informações e provas eletrônicas no contexto de investigações e processos judiciais relacionados a crimes cibernéticos. Isso é de extrema

importância, visto que muitos desses crimes transcendem fronteiras e exigem uma abordagem colaborativa para sua prevenção e punição eficaz.

Outro aspecto fundamental da Convenção de Budapeste é o estabelecimento de um quadro legal para a proteção dos direitos humanos no ambiente digital. Ela busca garantir que as medidas adotadas para combater crimes cibernéticos não infrinjam os direitos fundamentais dos indivíduos, como a liberdade de expressão, a privacidade e o devido processo legal.

Os redatores da Convenção de Budapeste discutiram aspectos cruciais, como o direito substantivo, processual e a jurisdição. Assim, a convenção foi elaborada não apenas para introduzir novos tipos de crimes, mas também para estabelecer regulamentos de procedimento penal que conciliam práticas do direito penal internacional, bem como, para estipular acordos relacionados à tecnologia da informação.

Para (Boiteux, 2004, p. 170-171), no que se refere ao direito substantivo (material), a mencionada Convenção definiu e classificou os crimes cibernéticos, abrangendo a invasão e interceptação ilegal, manipulação de dados e sistemas, uso indevido de dispositivos, falsificação de dados, fraudes cibernéticas, bem como pornografia infantil virtual e violação de direitos autorais. Outras atividades ilícitas debatíveis, como o jogo online ilegal e o terrorismo cibernético, foram deliberadamente deixadas de fora da Convenção para que cada país pudesse decidir sobre sua criminalização. Quanto à responsabilidade das entidades jurídicas, a Convenção limita-se a afirmar que elas podem ser responsabilizadas em esferas criminal, civil ou administrativa. É relevante destacar que todos os crimes definidos nessa Convenção são intencionais, ou seja, não se admite a possibilidade de conduta criminosa realizada por meio de computador sem a verdadeira intenção de cometê-la.

Segundo Marques (2014, p.6) a Convenção de Budapeste contemplou as seguintes diretrizes: *i) um conjunto de conceitos informáticos-jurídicos; ii) um conjunto de ilícitos criminais; iii) Um conjunto de medidas processuais destinadas a regular a forma de obtenção de prova em ambiente digital e, vi) mecanismos destinados a promover a cooperação internacional.*

Em sua estrutura, a convenção foi dividida em quatro capítulos, no primeiro capítulo, intitulado como "terminologia" inaugura em seu artigo primeiro, um conceito e distinção sobre "sistema informático" e "dados informáticos" nos seguintes termos[23]:

[23] *Council of Europe*. Convenção de Budapeste. Disponível em: https://www.coe.int/en/web/cybercrime/the-budapest-convention. Acesso em: 08 set. 2023.

> a) “sistema informático” significa qualquer dispositivo isolado ou grupo de dispositivos relacionados ou interligados, em que um ou mais de entre eles, desenvolve, em execução de um programa, o tratamento automatizado de dados;
> b) “dados informáticos” significa qualquer representação de factos, de informações ou de conceitos sob uma forma susceptível de processamento num sistema de computadores, incluindo um programa, apto a fazer um sistema informático executar uma função.

No segundo capítulo, intitulado como “medidas a tomar a nível nacional” a convenção cuidou das matérias de Direito Penal e Processual penal. Na secção 1 – Direito penal material, a convenção cuidou de orientar e traçar diretrizes acerca da tipicidade de determinados delitos, intitulado como “infrações contra a confidencialidade, integridade e disponibilidade de sistemas e dados informáticos”, que trata sobre o acesso ilegítimo à um sistema informático (artigo 2º), interceptação ilegítima de dados informáticos (artigo 3º); interferência de dados, tais como, alterações no conteúdo, danos, conteúdo eliminados, etc.; interferência em sistemas (artigo 5º) através de alteração de conteúdo, supressão, transmissão dentre outros artigos.

No título 2 – aborda as infrações relacionadas com computadores (artigos 7º e 8º), e no título 3, trouxe notadamente, a importância da normatização sobre infracções relacionadas com pornografia infantil.

Já na secção 2 – de direito processual, trata o âmbito da matéria de direito processual penal, cuidou do contexto de investigações e procedimentos criminais, como por exemplo, recolha de prova (artigo 14º), conservação expedida de dados informáticos armazenados (artigo 16º), conservação expedida e divulgação parcial de dados de tráfego (artigo 17º) e no artigo 18º, inovou ao trazer o instituto da injunção que habilita poderes inerentes as autoridades competentes. No título 4, buscou detalhar o procedimento de uma busca e apreensão à dados digitais armazenados, bem como, a recolha em tempo real de dados informáticos (artigo 20º e 21º); e para fechar o calabouço de normas e diretrizes, na última secção (secção 3), tratou os aspectos de competência e jurisdição.

No capítulo 3º a convenção, traça aspectos relacionados à cooperação internacional, abordando os princípios gerais da cooperação internacional, e também, mecanismos como extradição e assistência mútua, e a necessidade de os países signatários adotarem a ”Rede 24/7” que faz alusão à um ponto de contato/apoio disponível vinte e quatro horas por dia, sete dias na semana, a fim de assegurar a assistência imediata às investigações e procedimentos a respeito de infrações penais relacionadas com dados e sistemas informáticos. Por fim, o capítulo IV, aplica as disposições finais e os efeitos da convenção como um todo.

Atualmente, a Convenção de Budapeste conta com um número significativo de países signatários, dos quais o Brasil, que, em 17 de dezembro de 2021, através do Decreto Legislativo nº 37/2021[24], ratificou a Convenção de Budapeste sobre o Cibercrime. Isto demonstra o reconhecimento global da importância de se combater os crimes cibernéticos de forma coordenada e eficaz. No entanto, é importante ressaltar que a evolução rápida da tecnologia continua a desafiar os esforços para manter a Convenção atualizada e relevante no contexto em constante mudança do cibercrime.

A Convenção de Budapeste representa um marco crucial na luta contra o cibercrime e na promoção da segurança digital em escala global. Ao estabelecer um quadro legal e promover a cooperação internacional, ela contribui significativamente para a proteção dos direitos dos cidadãos no mundo digital e para a segurança das sociedades modernas cada vez mais dependentes da tecnologia da informação.

2.5 Meios de obtenção da prova digital na Convenção de Budapeste

Tendo em vista a ratificação da Convenção de Budapeste pelo Brasil, importa apresentar uma análise superficial dos principais meios de obtenção da prova digital, concebidos através do Tratado da Convenção de Budapeste, uma vez que inevitavelmente, o Brasil deverá adotar tais institutos por meio de implementação legislativa. Quais sejam: Preservação Expedita de dados; Preservação e a Revelação expedita de tráfego de dados; Injunção para apresentação de dados ou concessão de acesso; Busca e Apreensão de dados informáticos; Interceptação da comunicação de dados ou Obtenção (recolha) de dados de tráfego em tempo real e Obtenção de meio de prova com recurso da infiltração policial digital.

[24] Insta salientar que o Brasil, ainda não inseriu no ordenamento jurídico pátrio as diretrizes e normativas difundidas na Convenção de Budapeste. Entretanto, numa busca atualizada junto ao site principal do conselho da Europa consta na aba de declarações, que o Brasil Nos termos do artigo 24, parágrafo 7.a, e do artigo 27, parágrafo 2.c, da Convenção, a República Federativa do Brasil, declara que a autoridade responsável por formular pedidos de extradição e prisão provisória e para exercer a função competente é oMinistério da Justiça e Segurança Pública. E que nos termos do artigo 35 da Convenção, a República Federativa do Brasil declara que a função de ponto de contato da Rede 24 horas por dia, 7 dias por semana será exercida pela Polícia Federal. Disponível em: https://www.coe.int/it/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=3&codePays=BRA. Acesso em 09 set. 2021.

2.5.1 Preservação Expedita de dados

Segundo Vaz (2012, p.81) trata-se a preservação expedida de dados em uma "ordem de "congelamento", dirigida àquele que tenha a disponibilidade ou controle de dados informáticos armazenados em um sistema operacional, incluindo dados de tráfego, para que preserve esses dados até que as autoridades obtenham autorização para seu acesso".

Trata o artigo 16º da Convenção de Budapeste sobre o instituto da Conservação Expedita de dados informáticos armazenados, do qual consta a seguinte redação:

> Artigo 16º - Conservação expedita de dados informáticos armazenados
> Cada Parte adotará as medidas legislativas e outras que se revelem necessárias para permitir às suas autoridades competentes exigir ou obter de uma outra forma a conservação expedita de dados informáticos específicos, incluindo dados relativos ao tráfego, armazenados por meio de um sistema informático, nomeadamente nos casos em que existem motivos para pensar que os mesmos são suscetíveis de perda ou alteração.
> Sempre que a Parte aplique o disposto no n.º 1, através de uma injunção ordenando a uma pessoa que conserve os dados informáticos específicos armazenados que estão na sua posse ou sob o seu controle, esta Parte adotará as medidas legislativas e outras que se revelem necessárias para obrigar essa pessoa a conservar e proteger a integridade dos referidos dados durante um período de tempo tão longo quanto necessário, até um máximo de 90 dias, de modo a permitir às autoridades competentes obter a sua divulgação. Uma Parte pode prever que essa injunção seja subsequentemente renovada.
> Cada Parte adotará as medidas legislativas e outras que se revelem necessárias para obrigar o responsável pelos dados, ou outra pessoa encarregada de os conservar a manter segredo sobre a execução dos referidos procedimentos durante o período previsto pelo seu direito interno.
> Os poderes e procedimentos referidos no presente artigo devem estar sujeitos aos artigos 14º e 15º.

De acordo com o texto normativo, cada parte, ou seja, cada estado signatário, tomará as providências legais e outras que se mostrem indispensáveis para possibilitar às suas autoridades competentes solicitar ou adquirir de maneira eficiente a preservação rápida de dados informáticos específicos, abrangendo informações sobre o tráfego, armazenadas por um sistema de computador. De forma que isso se aplica especialmente em situações em que haja razões para crer que tais dados estão sujeitos a possíveis perdas ou modificações.

Além disso, a cláusula estabelece que, além de a parte contratante aplicar as disposições previstas no primeiro parágrafo, isso deve ser conseguido através de uma injunção que ordene a uma pessoa que retenha dados informáticos armazenados específicos sob a sua propriedade ou sob o controle dessa pessoa. Para este fim, cada Estado signatário tomará as medidas legislativas e outras medidas necessárias para exigir que essa pessoa retenha e proteja a

integridade desses dados durante o período necessário, até um máximo de 90 (noventa) dias, para permitir a autorização às autoridades competentes para divulgação. Uma Parte pode prever uma prorrogação desta ordem numa data posterior.

Ao contrário da posição seguida por Vaz que adota a posição de "congelamento" de dados, referindo-se à preservação dos dados, Kist (2019, p. 221-222) difere quanto ao termo "preservação" e leciona que:

> O termo "preservação" não significa dizer que os dados sejam "congelados", ou seja, tornados inacessíveis, em especial para os seus utilizadores legítimos. A pessoa à qual a ordem é dirigida poderá continuar a acessá-los, ficando tal acesso dependente das especificações que figurarem na referida ordem de preservação. Além disso, o poder de ordenar a preservação expedita de dados aplica-se a qualquer tipo de dados informatizados armazenados, como registros comerciais, médicos, pessoais e outros.

Completa o autor que, dessa forma, a ação de preservar dados serve como um meio para uma posterior ação, que é o "*acesso, conhecimento e utilização*" de informações digitais como prova em processos criminais. Conforme se depreende das regras mencionadas, seu propósito é conservar dados que de acordo com as autoridades que estão investigando um determinado fato, possam ser cruciais para a busca da verdade, havendo suspeitas de possíveis alterações ou destruições.

No que diz respeito a quais tipos de dados devem ser conservados, aduz que a medida de preservação visa a conservação de quaisquer tipos de dados: dados de base, dados de tráfego, de localização, conteúdo, bem como de registro em geral, comerciais, médicos e pessoais, protegendo tais dados de eventuais modificações, danos e eliminação.

Outro aspecto importante sobre o tema, desenvolvido por Kist, diz respeito aos tipos de pessoas cujos dados podem ser alvos da preservação expedida de dados, dentre as quais o autor lista quatro categorias: suspeito/investigado, ao acusado, à vítima e ao intermediário.

Os dados relativos ao suspeito e ao acusado desempenham um papel crucial na determinação da autoria e evidências do crime. Da mesma forma, as informações referentes à vítima também podem fornecer indícios sobre quem cometeu o delito e como foi perpetrado. No entanto, no caso da vítima, é razoável condicionar a preservação dos dados ao seu consentimento, seja ele explícito ou presumido. Por último, o "intermediário" é a pessoa que mantém uma relação próxima com o investigado, seja por laços familiares, profissionais, amizades ou de outra natureza, o que se reflete em contatos frequentes. Isso suscita a suspeita

de que nesses encontros possam ser discutidos assuntos que, de maneira direta ou indireta, tenham relação com a investigação do delito.

Finaliza o autor, a importância da medida de preservação diante da volatilidade das evidências digitais, presentes nos dados informáticos, e em razão dessa volatilidade, estão sujeitos a "ingerências e injunções" que acarretam alterações, danificações e até mesmo eliminações de tais evidências, comprometendo prejudicialmente, evidências essenciais para o sucesso na persecução penal.

2.5.2 Preservação e a Revelação expedida de tráfego de dados

Acerca do tema da preservação e revelação expedita de tráfego de dados, inserida através do artigo 17º da Convenção de Budapeste, aborda outro tipo de medida de conservação dos dados relativos ao tráfego, conforme texto colacionado:

> Artigo 17º - Conservação expedita e divulgação parcial de dados de tráfego
> A fim de assegurar a conservação de dados relativos ao tráfego em aplicaçãodo artigo 16º, cada Parte adotará as medidas legislativas e outras que se revelem necessárias, para:
> a) Assegurar a conservação rápida desses dados de tráfego, quer tenham participado na transmissão dessa comunicação um ou vários fornecedores de serviços; e
> b) Assegurar a divulgação rápida à autoridade competente da Parte ou a umapessoa designada por essa autoridade, de uma quantidade de dados de tráfego, suficiente para permitir a identificação dos fornecedores de serviços eda via através do qual a comunicação foi efetuada.

Depreende-se do texto normativo que cabe a cada um dos Estados signatários adotar medidas legislativas, direcionadas aos fornecedores de serviços que tenham participado da transmissão da comunicação, divulgando-os à autoridade competente, a fim de objetivar a conservação de dados relativos ao tráfego.

Nesse sentido, para Kist (2019, p.142-143) a medida tem especial importância em razão da anonimização adotada pelos agentes para a prática dos cibercrimes, que dificulta a persecução penal:

> A medida é arquitetada para as hipóteses, que são comuns, em que no processo comunicacional intervieram vários fornecedores de serviço, o que determinará que cada um deles terá na sua posse apenas uma parte do conjunto de dados gerados pela comunicação, a análise separada destas partes não surtirá efeitos positivos na investigação, sendo necessário reconstruir todo o caminho

> trilhado pela mensagem durante a sua transmissão e, somente assim, será possível identificar o respectivo emissor e receptor; a conservação de apenas uma parte do conjunto será insuficiente, e é nisso que reside a importância da revelação, por parte de um desses fornecedores, os demais que participaram da transmissão.

Ainda segundo ao autor, o propósito almejado com a medida em questão é o de identificar todos os provedores de serviço utilizados na transmissão, já que é por meio deles que é possível adquirir os dados digitais gerados durante o trajeto da comunicação: sua origem, destino, rota, horário, data, quantidade e duração, que compõem os dados de tráfego associados a ela.

2.5.3 Injunção para apresentação de dados ou concessão de acesso

O artigo 18 da Convenção de Budapeste, sob o título "injunção", autoriza os Estados a adotarem medidas legislativas que permitam às autoridades ordenar a qualquer pessoa que possua ou tenha sob seu controle dados informáticos específicos, pertinentes a provas, para que tenham acesso a estes dados ou os apresente:

> Artigo 18º - Injunção
> 1. Cada Parte adotará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes para ordenar:
> a) A uma pessoa que se encontre no seu território que comunique os dados informáticos específicos, na sua posse ou sob o seu controle e armazenados num sistema informático ou num outro suporte de armazenamento de dados informáticos; e
> b) A um fornecedor de serviços que preste serviços no território da Parte, que comunique os dados na sua posse ou sob o seu controlo, relativos aos assinantes e respeitantes a esses serviços
> 2. Os poderes e procedimentos referidos no presente artigo devem estar sujeitosaos artigos 14º e 15º.
> 3. Para os fins do presente artigo, a expressão “dados relativos aos assinantes” designa qualquer informação, contida sob a forma de dados informáticos ou sob qualquer outra forma, detida por um fornecedor de serviços e que diga respeito aos assinantes dos seus serviços, diferentes dos dados relativos ao tráfego ou ao conteúdo e que permitam determinar:
> a) O tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço;
> b) A identidade, a morada postal ou geográfica e o número de telefone do assinante, e qualquer outro número de acesso, os dados respeitantes à faturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços;
> c) Qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços.

Conforme demostrado, o presente artigo denota uma atenção especial aos "assinantes de serviços", de forma a autorizar as respectivas autoridades a obrigar o fornecimento de dados armazenados de qualquer pessoa que os tenha em custódia, bem como, obriga os fornecedores a prestarem informações dos respectivos clientes (assinantes de serviços).

Nesse sentindo Kist (2019, p.146) ressalta o item explicativo de nº 171, contido no "Relatório Explicativo da Convenção":

> Consta que se trata de uma "ordem de produção" endereçada a particulares que tenham em seu poder dados informáticos relevantes, para que os exibam ou permitam que as autoridades as acessem. Nessa acepção, a medida é compreendida com uma alternativa a outras, mais intrusivas, como a busca e apreensão de dados informáticos. Ademais, a locução "posse ou controle" abrange a posse física dos dados e, quando o destinatário da ordem não a tiver, sobre eles tenha controle, isto é, domine o processo de produção dos dados.

Depreende-se do exposto que a utilização do instituto da injunção, no que toca ao "acesso às informações relacionadas aos assinantes de serviços (cliente)", podem ser necessárias em dois tipos de situações, i) Quando for importante determinar os serviços empregados por ele, como o tipo de serviço telefônico e os serviços associados, assim como o número de telefone ou outro endereço técnico, como o de e-mail. ii) se o endereço técnico for conhecido, os dados sobre o cliente são essenciais para identificar a pessoa.

Desse modo, temos a título de comparação a inserção do instituto da injunção na Lei do Cibercrime Portuguesa[25], nos seguintes termos:

> Artigo 18º - Injunção
> 1. Cada Parte adotará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes para ordenar:
> a) A uma pessoa que se encontre no seu território que comunique os dados informáticos específicos, na sua posse ou sob o seu controlo e armazenados num sistema informático ou num outro suporte de armazenamento de dados informáticos; e
> b) A um fornecedor de serviços que preste serviços no território da Parte, que comunique os dados na sua posse ou sob o seu controlo, relativos aos assinantes e respeitantes a esses serviços
> 2. Os poderes e procedimentos referidos no presente artigo devem estar sujeitos aos artigos 14º e 15º.

[25] PORTUGAL. **Lei nº 109/2009, de 15 de setembro de 2009**. Aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa. Disponível em: https://dre.pt/dre/detalhe/lei/109-2009-489693. Acesso em: 29 mai. 2023.

> 3. Para os fins do presente artigo, a expressão "dados relativos aos assinantes" designa qualquer informação, contida sob a forma de dados informáticos ou sob qualquer outra forma, detida por um fornecedor de serviços e que diga respeito aos assinantes dos seus serviços, diferentes dos dados relativos ao tráfego ou ao conteúdo e que permitam determinar:
> a) O tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço;
> b) A identidade, a morada postal ou geográfica e o número de telefone do assinante, e qualquer outro número de acesso, os dados respeitantes à faturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços;
> c) Qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços.

Como mostra a lei apresentada, pode dizer-se que a injunção tanto para apresentação, quanto para conceder acesso a dados inclui uma ordem de uma autoridade competente a qualquer pessoa que tenha disponíveis o controle de dados informáticos específicos e determinados dados armazenados em sistemas informáticos, para que possam transmitir e encaminhá-los para procedimentos/processos investigativos ou permitir o acesso ao sistema informático onde se encontram, tendo em conta a necessidade dos dados deste material para produção de provas. Entretanto, a ordem deve indicar claramente os dados solicitados, medida que visa impedir o acesso desconhecido e indiscriminado a todos os dados em poder do destinatário da ordem Kist (2019, p.147-148).

Quanto aos tipos de dados passíveis para injunção, a título comparativo através da Lei Portuguesa, entende-se que a injunção pode referir-se a quaisquer dados de natureza informática, e abrangerá somente os dados de base e de localização.

Segundo Kist, os dados de base compreendem o nome, a assinatura, o número de telefone designado, a data de nascimento do cliente e quaisquer outros detalhes incluídos no contrato que formaliza a prestação do serviço, como o endereço, estado civil, endereço de e-mail, IMEI, IMSI, PIN e PUK do telefone móvel, data de início do contrato, entre outros.

Quanto aos dados de localização, podem ser objeto de ordem tanto dados de localização celular de sistemas informáticos incluindo telefones móveis, computadores fixos ou portáteis, *tablets*, quanto os dados de localização obtidos por meio do GPS (*Global Positioning System)*.

No que diz respeito ao modo de cumprimento da ordem de injunção, a Convenção de Budapeste destaca duas formas diferentes de cumprimento da ordem pelo destinatário da injunção; uma delas trata da entrega do suporte no qual os dados encontram-se armazenados, e a outra trata da permissão concedida às autoridades para que estas promovam o acesso ao sistema informático.

De igual modo, a diretriz contida na Convenção de Budapeste cuidou de estabelecer as pessoas que podem figurar como destinatários da ordem de injunção, de modo que a normativa estabelece que qualquer pessoa física ou jurídica pode ser destinatário da ordem de injunção, que tenha a posse ou controle sobre os dados, com exceção de o investigado não pode figurar como destinatário de ordem de injunção.

Outrossim, no que toca às pessoas cujos dados podem ser objeto de injunção, assim como na conservação expedita de dados, recaem sobre os dados pertencentes ao investigado/acusado, ao intermediário e também à vítima, com consentimento.

Nesta toada, Minto (2021, p.38) defende que a utilidade deste meio de obtenção de prova consiste:

> (…) Na circunstância de as autoridades obterem acesso a dados necessários para a investigação criminal com a colaboração do seu detentor. Com efeito, ainda que haja outros mecanismos de acesso aos dados, nomeadamente a busca e apreensão, as inúmeras possibilidades de ocultar a informação e de bloquear o acesso a ela podem determinar o insucesso das diligências.

Por fim, Kist (2019, p.151) ressalta a hipótese legítima recusa na apresentação dos dados ou na permissão de acesso a eles, dos quais se destacam o sigilo profissional do advogado, médico, jornalista, bem como segredos de Estado, do funcionário público, e segredo religioso (exceto se o líder religioso for a pessoa acusada).

2.5.4 Busca e Apreensão de dados informáticos

Para Denise Vaz (2012, p.82) no que se refere à busca e a apreensão de dados informáticos, destaca que:

> A convenção não distingue a diligência efetuada sobre os suportes físicos daquela realizada remotamente. Os Estados devem prever medidas que confiram poder às autoridades para apreender ou de maneira similar assegurar a preservação de um sistema computacional ou de um meio de armazenamento de dados, promover e custodiar a cópia dos dados computacionais, manter a integridade dos dados relevantes e tornar inacessível ou remover os dados computacionais no sistema informático acessado.

Esse meio de obtenção está contemplado no art. 19 da Convenção de Budapeste, nos seguintes termos:

> Artigo 19º - Busca e apreensão de dados informáticos armazenados
>
> Cada Parte adotará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes para proceder a buscas ou aceder de modo semelhante:
> A um sistema informático ou a uma parte do mesmo, bem como a dados informáticos que nele se encontrem armazenados; e
> A um suporte que permita armazenar dados informáticos.
> Cada Parte adotará as medidas legislativas e outras que se revelem necessárias para assegurar que, nos casos em que as suas autoridades procedam a buscas ou acedam de forma semelhante a um sistema informático específico ou a uma parte do mesmo, em conformidade com o disposto no n.º 1, a), e tenham razões para pensar que os dados procurados se encontram armazenados noutro sistema informático ou numa parte do mesmo situado no seu território, e que esses dados são legalmente acessíveis a partir do sistema inicial ou obteníveis a partir desse sistema inicial, as referidas autoridades estejam em condições de estender de forma expedita a busca, ou o acesso de forma semelhante ao outro sistema.
> Cada Parte adotará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes para apreender ou para obter de forma semelhante os dados informáticos relativamente aos quais o acesso foi realizado em aplicação dos n.ºs 1 ou 2. Essas medidas incluem as prerrogativas seguintes:
> Apreender ou obter de forma semelhante um sistema informático ou uma parte deste ou um suporte de armazenamento informático;
> Realizar e conservar uma cópia desses dados informáticos;
> Preservar a integridade dos dados informáticos pertinentes armazenados; e
> Tornar inacessíveis ou eliminar esses dados do sistema informático acedido.
> Cada Parte adotará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes a ordenar a qualquer pessoa que conheça o funcionamento do sistema informático ou as medidas utilizadas para proteger os dados informáticos nele contidos, que forneça na medida do razoável as informações razoavelmente necessárias, para permitir a aplicação das medidas previstas nos n.ºs 1 e 2.
> Os poderes e procedimentos referidos no presente artigos devem estar sujeitos aos artigos 14º e 15º.

Sobre o assunto, de forma bem mais delimitada sua natureza e seus objetivos, contemplados no art. 184 e seguintes do Relatório Explicativo da Convenção, que segundo Kist (2019, p. 155-157) colhem-se importantes diretrizes, textualmente:

> a) o objetivo a ser alcançado com o art. 19 da Convenção é a "modernização e a harmonização das legislações nacionais relativamente à busca e apreensão de dados informatizados armazenados, para fins de obtenção de provas relacionadas com investigações criminais ou ações penais específicas".
> b) as legislações, no geral, contemplam poderes para a "busca e apreensão de objetos tangíveis. Contudo, em muitos Estados ou jurisdições, os dados informatizados armazenados, por si só não serão considerados como algo tangível, pelo que não poderão ser adquiridos a título de investigações criminais e ações penais da mesma forma que os bens corpóreos, a não ser através da obtenção do suporte no qual se encontram armazenados os dados". Nesse contexto, o dispositivo em questão pretende "estabelecer um poder

equivalente relativo aos dados armazenados", partindo da premissa de que "tais dados têm a sua existência material num determinado local e são passíveis de fornecer provas de uma infração penal específica".

c) na busca e apreensão de dados informatizados devem ser tomados em consideração os requisitos que, ordinariamente, são observados em relação à busca e apreensão de bens corpóreos, nomeadamente a prévia autorização judicial em que deve ser ponderada a presença de condições, como evidências da materialidade e suficientes indícios de autoria da infração penal; mas, "no que se refere à investigação de dados informatizados, são necessárias disposições processuais complementares", a fim de assegurar que eles possam ser "obtidos com a mesma eficácia de uma operação de busca e apreensão de suportes de dados tangíveis. Existem diversas razões para este fato: em primeiro lugar, os dados são intangíveis, como é o caso dos dados sob a forma eletromagnética. Em segundo lugar que os dados podem ser lidos através da utilização de um equipamento informático, o mesmo não se passa relativamente à apreensão e transporte desses mesmos dados, tal como acontece com um documento em suporte papel. O suporte físico se encontram armazenados os dados intangíveis (por exemplo, o disco rígido de um computador (...) deverá ser apreendido e retirado do local, ou deverá ser efetuada uma cópia dos dados, quer sob uma forma tangível (por exemplo, uma impressão feita a partir de um computador) quer sob uma forma intangível, num suporte físico (por exemplo, um disco), antes que o suporte tangível que contém a cópia possa ser apreendido e transportado para fora do local (...). Em terceiro lugar, devido à conectividade dos sistemas informáticos, os dados poderão não se encontrar armazenados no computador alvo de busca, podendo ser facilmente acessíveis a partir desse mesmo sistema. Os dados poderão ser armazenados numa unidade de armazenamento de dados associada, que se encontre diretamente ligada ao computador, ou indiretamente através do recurso a sistemas de comunicação, tais como a Internet", o que poderá determinar a necessidade de implementação de medidas legais que permitam "alargar a extensão da busca ao sistema no qual os dados se encontrem efetivamente armazenados". Mas, as medidas previstas englobam o poder de apreensão de material informático e de suportes de armazenamento de dados informatizados. "Em certos casos - por exemplo, quando os dados se encontram armazenados num sistema operativo cuja especificidade não permite efetuar cópia dos dados -, não resta outra solução senão a de proceder à apreensão do próprio suporte de dados. Tal poderá revelar-se igualmente necessário nos casos em que o suporte de dados tenha que ser sujeito a uma análise no sentido de dele extrair os antigos dados a que foram sobrepostos outros, mas dos quais, ainda assim, é possível detectar alguns vestígios no suporte de dados".

d) o artigo 19 da Convenção "é consagrado aos dados informatizados armazenados". Ademais, a "utilização do termo tradicional de 'busca' traduz a ideia de exercício do poder coercivo por parte do Estado (...) análogo à busca clássica. 'Busca' significa procurar, ler, inspecionar ou rever dados. Inclui a noção de pesquisa a dados e de análise de dados. Por outro lado, a palavra 'acesso' encerra um significado neutro, mas reflete com maior exatidão a terminologia informática. Ambos os termos são utilizados de forma a conciliar os conceitos tradicionais com a terminologia moderna". Além disso "o termo "apreender' significa transportar o suporte físico no qual foram registrados os dados ou as informações, ou efetuar e guardar uma cópia de tais dados ou informações". O termo inclui, ainda "a utilização ou apreensão de programas necessários para acessar aos dados objeto de busca e investigação".

e) tratando-se de medidas referentes "aos dados intangíveis armazenados, torna-se necessário que as autoridades competentes adotem medidas

> complementares no sentido da aquisição e guarda dos, isto é, de maneira a preservar a integridade dos dados, ou manter a cadeia de posse dos dados, o que significa que aqueles copiados ou removidos são conservados no estado em que foram encontrados quando da apreensão, mantendo-se inalterados no período durante o qual é intentada a ação penal".
> f) a norma que permite à autoridade demandar o auxílio de terceiros que conheçam o sistema informático ou os mecanismos de proteção dos dados nele constantes é "uma medida coerciva cujo objetivo é o de facilitar a busca e apreensão de dados informatizados". O que está em causa é a "dificuldade de acesso aos dados investigados e da sua identificação enquanto elementos constituintes de prova, devido à quantidade de dados passíveis de processamento e armazenamento, ao desenvolvimento de medidas de segurança, bem como à natureza das operações informáticas. Reconhecendo a possibilidade de ser necessário consultar os administradores de sistema - em virtude dos conhecimentos particulares que estes possuem acerca do sistema informático relativamente à melhor forma de conduzir o - processo de investigação em termos das modalidades técnicas existentes"; é com essa base que a disposição "autoriza as entidades competentes a obrigar um administrador de sistema a prestar o seu contributo, da forma que se afigure razoável, no quadro da operação de busca e apreensão "Ou seja, "a informação cujo fornecimento é passível de ser solicitado é aquela necessária à execução das operações de busca e apreensão, ou de forma semelhante, acesso e guarda".

Ainda, Kist conceitua que a pesquisa informática se refere à ação de conduzir buscas e investigações em sistemas de computadores, com o propósito de identificar evidências digitais relevantes para a comprovação do fato sob investigação. Essa prática compartilha semelhanças com a busca convencional regulamentada pelos procedimentos legais e tem como objetivo encontrar e localizar itens relacionados à infração penal, os quais serão posteriormente apreendidos. Além disso, a pesquisa informática precede a apreensão dos dados digitais identificados por meio dela.

Acerca da natureza da pesquisa ou busca informática, define que se concretiza através da busca e procura de dados por meio de acesso a determinado sistema informático, bem como pela procura de dados desta natureza armazenados, podendo incidir sobre a totalidade do sistema informático ou parte dele, como *clouds*, ou dispositivos e suportes independentes, tais como, *pendrive*, HD externo, dentre outros.

No que toca ao local da busca, leciona o autor que a busca de dados informáticos pode ser efetivada de dois modos, através da "*busca presencial no sistema informático em que se encontra e a busca remota*"

> Os dados informáticos, ainda que se trate de bens incorpóreos ou realidades intangíveis aos sentidos, têm existência "física" em algum lugar, e é neste que devem ser procurados e buscados.
> Esse "lugar" pode ser também de natureza física e encontrar-se no interior do suporte ou dispositivo informático; é o caso do disco rígido de um computador, da memória de um smartphone ou tablet, um compact disc (CD) um pen drive um HD externo. Mas o lugar em que os dados se encontram pode

> ser meramente virtual situação exemplificada de forma partícula cloud computing (2019, p.159).

Na busca presencial, de maneira intuitiva, o investigador se desloca e entra no local físico onde está o dispositivo de armazenamento. Em alguns casos, pode ser necessário obter autorização judicial para entrar na residência, especialmente se o dispositivo estiver lá. Uma vez no local, o investigador decide, dependendo das circunstâncias, se irá apreender e levar consigo o dispositivo, realizar a pesquisa diretamente ou fazer uma cópia completa ou parcial dos dados para análise posterior.

A situação é distinta na pesquisa remota, pois neste caso, os dados procurados não estão armazenados no dispositivo ou sistema informático sob investigação, mas sim em outro sistema, localizado geograficamente em um ambiente físico diferente daquele onde a diligência está ocorrendo, como por exemplo, os dados armazenados na nuvem.

Ainda sobre as pessoas que recai o instituto da busca informática, tem como objeto dados pertencentes ao investigado/acusado, intermediário e à vítima com consentimento.

Segundo Kist, o instituto da Apreensão de dados informáticos é subsequente a fase de busca (pesquisa) de dados informáticos, que se concretiza com a apreensão dos dados localizados tanto nos sistemas informáticos quanto em outros suportes autônomos já mencionados.

O autor destaca norma declinada no art.16 da Lei de Cibercrime Portuguesa, elucidadas da seguinte forma:

> quando, no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, forem encontrados dados ou documentos informáticos necessários à produção de prova, tendo em vista a descoberta da verdade, a autoridade judiciária competente autoriza a sua apreensão;
> havendo urgência ou perigo na demora, o órgão de polícia criminal pode efetuar apreensões sem prévia autorização da autoridade judiciária, desde que o seja no decurso de pesquisa informática legitimamente ordenada e executada; neste caso, elas devem ser comunicadas à autoridade judiciária em 72 horas, para validação;
> se apreendidos dados ou documentos informáticos cujo conteúdo possa revelar dados pessoais ou íntimos e que, assim, possam pôr em causa a privacidade do respectivo titular ou de terceiro, esses dados ou documentos devem ser apresentados ao juiz, que ponderará a sua junção aos autos, tendo em conta os interesses do caso concreto;
> a apreensão de sistemas informáticos utilizados para o exercício da advocacia e de atividades médica e bancária está sujeita, também e com as necessárias adaptações, às regras e formalidades previstas no Código de Processo Penal, e a apreensão de sistemas informáticos utilizados para o exercício da profissão de jornalista às regras e formalidades previstas no Estatuto do Jornalista; também é resguardado o regime de segredo profissional, de funcionário e de Estado.

> a apreensão de dados informáticos, consoante seja mais adequado e proporcional, e também tendo em conta os interesses do caso concreto, pode revestir as formas seguintes: e. 1) apreensão do suporte onde está instalado o sistema ou onde estão armazenados os dados informáticos, bem como dos dispositivos necessários à respectiva leitura; e.2) realização de uma cópia dos dados, em suporte autônomo, que será junto ao processo; e.3) preservação, por meios tecnológicos, da integridade dos dados, sem realização de cópia nem remoção; e.4) eliminação não reversível ou bloqueio do acesso aos dados;
> se a opção tiver sido a apreensão na forma de cópia dos dados, a cópia deve ser duplicada e uma delas selada e confiada ao secretário judicial dos serviços onde o processo correr; caso tecnicamente possível, os dados apreendidos devem ser certificados por meio de assinatura digital.

Quanto ao objeto da apreensão, consiste nos dados ou documentos digitais guardados em um sistema informático e que foram identificados durante a etapa da busca. No caso de dados em armazenamento, essa ação não pode ser aplicada aos que estão em processo de comunicação em tempo real. No entanto, é possível apreender a impressão do conteúdo de uma página da internet que os investigadores encontraram aberta, bem como a impressão dos elementos que representam o perfil da pessoa em uma rede social.

Conforme mencionado anteriormente, em relação ao local da pesquisa informática, esta pode ser realizada de forma presencial ou remota. As considerações feitas sobre essas diferentes situações também se aplicam à apreensão dos dados. Portanto, a apreensão pode ocorrer no local onde os dados estão fisicamente armazenados, o que requer a presença física do investigador no ambiente correspondente. Se os dados estiverem em um local diferente, mas forem acessados por meio da pesquisa remota, a apreensão também pode ser realizada de forma remota, ou seja, à distância.

Em outras palavras, a busca online tende a resultar na apreensão remota dos dados informáticos localizados, e se estes estiverem em um país estrangeiro, trata-se de um acesso transfronteiriço, um assunto que será discutido posteriormente.

Ainda, outro ponto importante a ser destacado por Kist, é o que diz respeito a apreensão de correio eletrônico e registros de comunicações de natureza semelhante, que segundo o autor não encontra guarida na convenção de Budapeste a essas modalidades de comunicação. Entretanto, menciona o autor que a legislação portuguesa cuidou do assunto ao transpô-lo para o ordenamento jurídico interno disciplinado pelo art. 17 da Lei do Cibercrime:

> Quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio eletrônico o registro de comunicações de

> natureza semelhante, o juiz pode autorizar o ordenar por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal.

Conforme observado, a norma aborda a apreensão de dados informáticos provenientes de comunicações anteriores, como e-mails ou similares, e é aplicável nos casos em que durante a investigação informática é identificado que nos sistemas analisados existem dados constituídos por esse tipo de mensagens.

O termo "correio eletrônico", como comumente conhecido, refere-se ao sistema operado, geralmente por meio da Internet, que permite a transmissão de mensagens através de servidores que atuam como provedores desse serviço. Para isso, são utilizados diversos protocolos, sendo os mais conhecidos o SMPT - Simple Mail Transfer Protocol- (Protocolo Simples de Transferência de E-mail) e o POP3 - Post Office Protocol (Protocolo de Correio de Entrada), que evoluiu para o IMAP – Internet Message Access Protocol (Protocolo de Acesso à Mensagem da Internet). Essas mensagens são transmitidas entre a pasta do remetente e a do destinatário e, além do texto, é possível anexar arquivos de texto, imagens, áudios e vídeos (combinando imagem e áudio). São esses dados contidos nas mensagens que podem ser sujeitos a apreensão durante a análise.

Para Kist (2019, p.171) ainda existem dois tipos de serviços com duas naturezas distintas que a legislação portuguesa denominou como “comunicações de natureza semelhante”. Uma trata de comunicações similares ao correio eletrônico, mas que baseia-se por um serviço de telefonia, quais sejam, SMS, SEM e MMS. A segunda trata de comunicações cuja base consiste na tecnologia Voip – Voz sobre IP, que intensificou a comunicação por meio da internet, constituídas pela chamada IM – Instant Messenger e chats ou chatrooms:

> A mensagem instantânea (IM), viabilizada pelos mensageiros eletrônicos instantâneos, permite comunicações na forma de mensagens escritas, de voz, em fotografias, e vídeos, de forma instantânea entre os interlocutores, além de permitir videoconferências (chamadas de vídeo). Os principais exemplos, atualmente, são o Messenger, o WhatsApp, o Skype, o Facebook Messenger, o Telegram, o Viber, o Snapchat, entre outros. Em regra, os dados transmitidos por esses mecanismos ficam armazenados na memória do dispositivo informático utilizado para a comunicação ou na plataforma do aplicativo utilizado, permitindo a posterior apreensão.

É diferente a situação dos chats ou *chatrooms*. Traduzidas como "salas de bate-papo" ou "salas de conversação", são lugares virtuais ou on-line nos quais duas ou mais pessoas podem se encontrar, logicamente de forma virtual, e por esses mecanismos conversar, bem como trocar

mensagens e arquivos, que podem ter natureza lícita ou ilícita, sendo esses mecanismos os mais utilizados para a troca de arquivos com conteúdo pedo-pornográfico. Nos casos em que tal conteúdo é armazenado na memória do dispositivo informático, ele é passível de apreensão, que também se viabiliza com os dados de tráfego gerados pelo acesso a frequência a essas salas (Kist, 2019, p.171-172).

Nesse sentido, se durante a etapa de pesquisa em um sistema informático forem encontrados dados digitais que tenham valor como evidência e tenham sido gerados por meio de comunicação anterior, como e-mails ou meios similares, eles podem ser sujeitos à apreensão. Isso também se aplica aos casos em que esses dados, ao invés de serem encontrados durante a busca, são entregues às autoridades por uma pessoa específica, como no caso da pessoa que foi alvo da injunção previamente examinada; ou também quando alguém, por ter recebido mensagens por esses meios, entrega voluntariamente os dados à autoridade ou consente de forma válida com a apreensão, como geralmente ocorre com vítimas de ameaças ou difamação (Kist, 2019, p. 172).

2.5.5 Interceptação da comunicação de dados ou Obtenção (recolha) de dados de tráfego em tempo real

O Título 5 das disposições processuais da Convenção de Budapeste, composto pelos artigos 20 e 21, aborda um método diferente de obtenção de provas, denominado "Recolha, em tempo real, de dados informáticos". A expressão "em tempo real" indica que não se trata mais de buscar dados digitais armazenados em um sistema informático como resultado de uma comunicação passada, mas sim de coletar e interceptar dados digitais enquanto estão sendo gerados por um processo de comunicação ativo e atual, ou seja, durante sua transmissão. Além do mais, esses dados mencionados nos dois dispositivos têm duas naturezas distintas: dados de tráfego e dados de conteúdo. Por isso, o artigo 20 da Convenção trata dos "dados informáticos relativos ao tráfego", enquanto o artigo 21 aborda a "interceptação de dados relativos ao conteúdo.

Sobre o assunto, Kist (2019, p. 173-175) destaca os itens 205 a 215 do Relatório Explicativo da Convenção de Budapeste, dos quais sintetizou as principais disposições processuais que norteiam o instituto da interceptação de dados informáticos, em linhas gerais:

> após reafirmar que os artigos 20 e 21 ofertam guarida para que os Estados signatários promovam medidas para recolher dados enquanto estão sendo

gerados por uma comunicação informática ativa, por estarem associados a comunicações específicas transmitidas por meio de um sistema informático (dados de tráfego) bem como de interceptar em tempo real dados de conteúdo, é ali consignado que a "intercepção de telecomunicações refere-se, normalmente, às redes de telecomunicações tradicionais. Estas redes podem incluir infraestruturas por cabo, quer de cabo metálico quer de fibras ópticas, bem como interligações com redes sem fio, incluindo sistemas telefônicos móveis e sistemas de transmissão por microondas. (...). As redes informáticas consistem igualmente numa infraestrutura por cabos fixa e independente, mas são mais frequentemente operados como uma rede virtual através de ligações efetuadas por meio de infraestruturas de telecomunicação, permitindo assim a criação de redes informáticas ou a ligação de redes de dimensão global. Em resultado da convergência das tecnologias da informação e das telecomunicações, torna-se pouco nítida a distinção existente entre as telecomunicações e as comunicações informáticas, bem como a especificidade das suas infraestruturas".

Nessa perspectiva, as duas medidas em questão aplicam-se "a comunicações específicas transmitidas por meio de um sistema informático, nelas se incluindo a transmissão de uma comunicação através de redes de telecomunicação antes de ser recebida por um outro sistema informático".

Há dois tipos de dados "passíveis de serem recolhidos, a saber, os dados de tráfego e os dados de conteúdo. O termo 'dados de tráfego' (...) designa qualquer dado informatizado, relacionado com uma comunicação efetuada por meio de um sistema informático, gerado por esse sistema e que integra a cadeia de comunicação; indicam aspectos da comunicação, tais como a sua origem, o destino, o caminho, a hora, a data, a dimensão, a duração ou o tipo do serviço subjacente à mesma. O termo dados de conteúdo' (...) designa o conteúdo informativo da comunicação, ou seja, o significado ou o teor da comunicação, ou a mensagem ou informação veiculada pela comunicação (que não a relativa aos dados de tráfego)".

A recolha de dados de tráfego, como mecanismo de "recolha de provas contidas nas comunicações em curso (...) tem lugar quando da transmissão da comunicação, isto é, em tempo real (...). A recolha não interfere significativamente na circulação dos dados, pelo que a comunicação chega ao seu destinatário. Em vez de uma apreensão física dos dados, é efetuado um registro, isto é, uma cópia dos dados que sendo comunicados. A recolha destas provas ocorre durante um determinado período de tempo. A autorização legal mediante a qual é possível efetuar a recolha é sempre solicitada relativamente a um acontecimento futuro, isto é, uma futura transmissão de dados.

Os meios de obtenção de prova em tela podem representar "técnicas cruciais para a investigação de algumas das infrações definidas pela Convenção, tais como as que envolvem o acesso ilícito a sistemas informáticos, a propagação de vírus informáticos ou a distribuição de pornografia infantil. A origem da intrusão ou da distribuição, por exemplo, nem sempre poderá ser detectada sem que se proceda a uma recolha em tempo real dos dados de tráfego. Da mesma maneira, nalguns casos, a natureza da comunicação não poderá ser descoberta sem que se proceda a uma intercepção em tempo real dos dados de conteúdo";

Por outro lado, é certo que "a intercepção de dados de conteúdo representa uma medida com elevado grau de intrusão na vida privada"; em consequência, "torna-se necessária a implementação de salva-guardas rigorosas de modo a garantir um equilíbrio adequado entre os interesses da justiça e os direitos fundamentais do Homem". A título de exemplo, podem ser previstas condições e salvaguardas consistentes na "supervisão por parte de um órgão judiciário ou outro independente; especificidade das comunicações ou das

> pessoas alvo de intercepção; necessidade, subsidiariedade e proporcionalidade, como condições jurídicas justificativas da aplicação da medida e ineficácia de outras medidas com menor grau de intrusão; ainda, a limitação do período de duração da intercepção e direito de recurso".

Quanto à recolha dos dados informáticos relativos ao tráfego, a Convenção de Budapeste disciplinou em seu art. 20 – "Recolha em tempo real de dados relativos ao tráfego", que:

> Cada Parte adotará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes a:
> Recolher ou registar, através da aplicação de meios técnicos existentes no seu território, e
> Obrigar um fornecedor de serviços, no âmbito da sua capacidade técnica existente, a:
> Recolher ou registar por meio da aplicação de meios técnicos no seu território, ou
> Prestar às autoridades competentes o seu apoio e assistência para recolher ou registrar, em tempo real, dados de tráfego relativos a comunicações específicas no seu território transmitidas através de um sistema informático.
> Quando uma Parte, em virtude dos princípios estabelecidos pela sua ordem jurídica interna, não pode adoptar as medidas descritas no nº 1, alínea a), pode, em alternativa, adoptar as medidas legislativas e outras que se revelem necessárias para assegurar a recolha ou o registo em tempo real dos dados de tráfego associados a comunicações específicas transmitidas no seu território através da aplicação de meios técnicos existentes nesse território.
>
> 1. Cada Parte adotará as medidas legislativas e outras que se revelem necessárias para obrigar um fornecedor de serviços a manter secreto o fato de qualquer um dos poderes previstos ter sido executado, bem como qualquer informação a esse respeito.
> 2. Os poderes e procedimentos referidos no presente artigo devem estar sujeitos aos artigos 14º e 15º.

Tendo em vista a importância do assunto, Kist (2019, p.176-178) destaca os itens 216 a 227, contidos no Relatório Explicativo da Convenção, onde separa os principais conteúdos norteadores acerca do tema:

> a) É comum que o agente do cibercrime, ao mesmo tempo em que perpetra a atividade criminosa, adote providências voltadas para apagar o "rastro" deixado por ela, como alterar o caminho que a comunicação percorreu; em casos assim, frequentes, os dados de tráfego iniciais já não estão disponíveis ao tempo da investigação, ou já não se mostram relevantes, por ter sido alterado o citado caminho da comunicação. É neste contexto que a "recolha em tempo real dos dados de tráfego constitui uma medida de investigação de extrema importância".
> b) A recolha de dados de tráfego relativamente às telecomunicações (por exemplo, nas conversas telefônicas) "desde sempre se afigurou como sendo um instrumento de investigação útil na medida em que permite a identificação da origem ou destino (por exemplo, os números de telefone) e dos dados conexos (por exemplo,hora, data e duração) sobre vários tipos de

comunicações ilegais (por exemplo, no caso de ameaças de crimes e assédio, conspiração de índole criminosa declarações falsas) e sobre comunicações que forneçam provas de crimes passados ou futuros (por exemplo, tráfico de estupefacientes, homicídio, infrações de cariz econômico, etc.)".

c) "As comunicações através de computadores podem constituir ou servir de prova dos mesmos tipos de atos criminosos". Mas, há neste caso particularidades a serem observadas: "a tecnologia informática permite transmitir grandes quantidades de dados, incluindo textos imagens e sons", razão pela qual também existe "um maior potencial para a prática de crimes que envolvam a distribuição de conteúdos ilegais (por exemplo, pornografia infantil). (...) Nos casos de distribuição de pornografia infantil, acesso ilícito a um sistema informático ou interferência no correto funcionamento do sistema informático ou na integridade dos dados e em particular quando estas infrações são cometidas a distância, por exemplo, via Internet, torna-se não só necessário, mas vital detectar o caminho das comunicações entre a vítima e o autor da infração". Nesse panorama, "a capacidade de recolher dados de tráfego relativos a comunicações informáticas é tão ou mais importante do que essa mesma capacidade relativamente às tradicionais telecomunicações. Esta técnica de investigação permite relacionar a hora, a data, a origem e o destino das comunicações efetuadas pelo suspeito com a hora da intrusão no sistema da vítima, possibilitando a identificação de outras vítimas ou revelando ligações com cúmplices".

d) A recolha de dados de tráfego associados deve ter por objeto comunicações especificas; a Convenção não autoriza "a vigilância ou a recolha, geral ou indiscriminada, de grandes quantidades de dados de tráfego. Do mesmo modo a Convenção não permite a realização de "missões de exploração" através das quais se espera descobrir atividades de índole criminosa sendo estas situações muito diferentes das investigações levadas a cabo relativamente a casos específicos de criminalidade". É por isso que "a ordem judicial ou outra que autorize a recolha deverá indicar expressamente quais as comunicações cujos dados de tráfego deverão ser recolhidos".

e) A Convenção faz alusão a dois modos diferentes de recolher os dados de tráfego; de um lado, e estando disponíveis "meios técnicos", a recolha e o registro podem ser feitos pelas próprias instâncias investigatórias; mas, também há a opção de "obrigar um fornecedor de serviços, no âmbito da sua capacidade técnica", i) a fazer a recolha ou o registro de ambas as atividades ou ii) prestar às autoridades competentes o seu apoio e a sua assistência na recolha ou no registro (para o caso em que a própria instância investigatória esteja efetuando estas atividades). É fundamental que seja averiguada a questão da capacidade técnica" pois no caso de um fornecedor de serviços não dispor da capacidade técnica necessária para levar a cabo a operação de recolha ou registro de dados de tráfego, as autoridades competentes para a aplicação da lei deverão ter a possibilidade de tomar a seu cargo a execução de tal operação". Além disso, "no caso de algumas redes de área local (LAN), em que não existe a participação de um fornecedor de serviços, a única forma de efetuar a recolha e o registro dos dados" é a própria autoridade investigadora que deverá desincumbir-se dessa tarefa.

f) A medida investigatória em análise "apenas será eficaz se for realizada sem o conhecimento das pessoas que são objeto da investigação. A interceptação é uma operação, por natureza, sub-reptícia e deverá ser executada de forma a que as partes intervenientes na comunicação, dela não se apercebam. Sobre os fornecedores de serviços e seus colaboradores, que tenham conhecimento da interceptação, recairá a obrigação de manter o sigilo por forma a que a operação seja bem-sucedida". Por isso, as medidas legislativas devem "obrigar um fornecedor de serviços a manter confidenciais quaisquer informações, ou

> fatos com estas relacionados, acerca da execução" da medida de recolha e registro de dados de tráfego; uma tal "disposição não apenas garante a confidencialidade da investigação, como também isenta o fornecedor de serviços de quaisquer obrigações contratuais ou outras, previstas pelo sistema jurídico vigente, de notificação dos subscritores acerca dos quais estão a ser recolhidos os dados".

No que diz respeito ao conteúdo da interceptação de dados informáticos, Kist entende que segundo a convenção, "*cabem aos estados adotarem as medidas legislativas para habilitar as autoridades competentes, relativamente a um conjunto de infrações graves a definir no âmbito do direito"*:

> a) recolher ou registrar, através da aplicação de meios técnicos existentes no seu território; b) obrigar um fornecedor de serviços, no âmbito da sua capacidade técnica, a: i) recolher ou registrar, através da aplicação dos meios técnicos existentes no seu território, ou ii) prestar às autoridades competentes o seu apoio e a sua assistência na recolha ou no registro, em tempo real dos dados relativos ao conteúdo de comunicações específicas feitas no seu território, transmitidas através de um sistema informático" (Kist, 2019, p.178).

De modo a tratar-se a interceptação de dados informáticos como o meio de obtenção de prova mais invasivo, Kist (2019, p.179) observa os seguintes conceitos colhidos no Relatório Explicativo da Convenção, itens 228 a 231, quais sejam:

> a) A interceptação do conteúdo das telecomunicações, nomeadamente as telefônicas, desde sempre tem demonstrado ser uma ferramenta útil de investigação para determinar se a comunicação se reveste de um caráter ilegal (por exemplo, quando a comunicação constitui uma ameaça de crime ou assédio, uma conspiração de índole criminosa ou declarações falsas), bem como para reunir provas sobre infrações passadas. "As comunicações através de computadores podem constituir ou servir de prova dos mesmos tipos de atos criminosos. (...) A prática de muitos dos crimes informáticos conhecidos implica a transmissão ou a comunicação de dados. (...) e não é possível determinar, em tempo real, a natureza ilegal e nociva destas comunicações sem que se proceda à interceptação do conteúdo da mensagem. Não existindo a possibilidade de determinar e impedir a ocorrência de criminalidade, apenas restaria às autoridades competentes a investigação dos crimes cometidos no passado, cujos efeitos prejudiciais já não podem ser travados. Assim sendo, a interceptação em tempo real de dados de conteúdo relativos a comunicações informáticas é tão ou mais importante do que a interceptação em tempo real de telecomunicações".
> b) "O termo 'dados de conteúdo' refere-se ao conteúdo informativo da comunicação, isto é, o significado ou o teor da comunicação, ou a mensagem ou informação transmitida pela comunicação. Designa, assim, todos os elementos transmitidos como parte da comunicação, mas que não constituam dados de tráfego".
> c) A maioria das observações feitas a propósito da recolha e registro de dados de tráfego é aplicável à interceptação de dados de conteúdo, nomeadamente

> as obrigações impostas ao fornecedor de serviço de colaboração e apoio prestação de apoio, bem como acerca da confidencialidade; também com relação à salvaguarda dos interesses do investigado, considerando a interceptação dos dados de conteúdo é a mais invasiva de todas e, também por isso, na perspectiva de limitar o seu uso, é recomendado seja estabelecido um catálogo de crimes, os mais graves, e somente para a investigação destes é que se pode lançar mão da medida.

Para o autor (Kist, 2019, p. 181-183), a Convenção de Budapeste aborda os meios de obtenção de prova que têm aplicação em dois tipos diferentes de dados. Ambos são capturados no momento em que são produzidos e comunicados, envolvendo a intervenção do estado em uma comunicação em curso, o que levou a Convenção a se referir a eles como intromissões "em tempo real".

De um lado, existem dados gerados automaticamente pelos sistemas informáticos sobre a comunicação, fornecendo informações essenciais como origem, destino, percurso, horário, data, tamanho/volume, duração ou tipo de serviço associado. Esses são os dados de tráfego, que não revelam o conteúdo da comunicação, mas são cruciais para identificar as pessoas envolvidas na comunicação. Portanto, a obtenção desses dados muitas vezes é crucial para comprovar a autoria de atividades criminosas em investigação. Esses dados são coletados e registrados no exato momento em que são gerados pelo sistema informático, e é essa cópia que será incluída no processo investigatório.

Por outro lado, temos os dados que refletem o conteúdo da comunicação, ou seja, o que é efetivamente transmitido pelo sistema informático. Essa prática é semelhante à interceptação de comunicações telefônicas, regulada nos sistemas legais. Envolve a interceptação de e-mails, SMS, EMS, MMS, conversas em plataformas como *messenger*, comunicações em newsgroups, chats, videoconferências, *webconferências* etc. O investigador tem acesso ao conteúdo das conversas ou comunicações em tempo real.

Desse modo, há o acesso ao conteúdo das mensagens transmitidas em comunicações por VoIP, que externamente se assemelham a comunicações telefônicas, mas operam de maneira estruturalmente diferente. A comunicação por VoIP requer a instalação de um aplicativo ou programa no dispositivo informático, que inclui a criptografia das mensagens transmitidas. A criptografia torna a mensagem ilegível até ser desencriptada (desencriptação). Por isso, para interceptar mensagens em base VoIP, é necessário realizar uma "vigilância nas fontes", o que envolve a instalação de um software no dispositivo informático que captura o conteúdo da mensagem antes de ser criptografado e transmitido.

Quanto às pessoas passíveis de interceptação de dados e segredos, a convenção declina que recai ao suspeito/investigado, ao intermediário, e à vítima com consentimento. Entretanto, quando as informações recaem sobre o segredo de Estado e Religioso, estas não poderão ser valoradas. Mas isto não implica dizer que seus titulares não possam ser alvos de diligências probatórias, de modo que a tutela recai sobre as informações (matérias) relacionadas ao segredo e não quanto a seus portadores.

Com relação ao sigilo entre advogado e seu constituinte, podem ser alvos de interceptação de dados se houver fundadas razões de que a natureza da comunicação constitua elemento de crime, de forma que se torna convencido que o advogado se afastou do exercício da defesa.

2.5.6 Obtenção de meio de prova com recurso da infiltração policial digital

Kist (2019, p.191) conceitua o agente infiltrado como:

> Trata-se do agente que, também sem revelar sua identidade e qualidade, e com a finalidade de obter provas para a incriminação de um suspeito ou para obter uma *notitia criminis*, infiltra-se, com qualificação fictícia, no meio com a conotação criminal. Diferentemente do agente encoberto, a infiltração tende a se prolongar mais no tempo, pois é essencial para o agente infiltrado relacionar-se com o visado e/ou seu grupo para angariar confiança pessoal e, por esse meio, ter condições de acompanhar os acontecimentos e a execução das atividades; admite-se, inclusive, que participe da prática de atos preparatórios de infrações penais e mesmo de atos executórios, desde que isso se mostre necessário no contexto da aquisição e manutenção da confiança; o que não se admite é que o agente determine a prática de infrações, pois caso o faça sua condição transmuda para a de agente provocador.

Para o autor, dentro do contexto "informático-digital", a infiltração implica em uma ação mais incisiva e profunda se comparada à do agente encoberto. Em outras palavras, com o objetivo de ganhar a confiança dos alvos e, consequentemente, entender e acompanhar os eventos em curso, o agente não se limitará a uma participação passiva. Poderá, de fato, ingressar em chats, sites, blogs ou outros fóruns, interagindo ativamente com os demais participantes, chegando ao ponto de realizar atos preparatórios e, se necessário, executórios de crimes. No entanto, é importante ressaltar que mesmo aqui, o agente não pode instigar a prática de tais ações, de modo a se afastar da figura de agente infiltrado, para agente provocador.

Diante do assunto, outrora já profundamente abordado, importa destacar os meios para promover as ações de infiltração em ambiente digital, através das buscas on-line, pesquisa

informática remota on-line e buscas com o recurso de *malware*. Nesse sentido, Manuel da Costa Andrade analisa as buscas online ao abordar como o avanço técnico-científico afeta a legislação processual penal. Ele expressa uma perspectiva que busca harmonizar a utilização das novas ferramentas tecnológicas, que têm surgido para aprimorar e tornar mais eficiente a investigação criminal, com a imperativa necessidade de preservar e proteger os direitos fundamentais (Andrade, 2009, p.145).

Ainda ressalta o autor, que a busca online envolve uma variedade de procedimentos que dependem das técnicas e métodos de intervenção utilizados, destaca que a medida consiste em "acessar, de forma oculta e à distância, via internet, os dados armazenados em um computador", com o propósito de "observá-los e, se necessário, fazer cópias deles em maior ou menor extensão". Além disso, isso pode ocorrer de forma instantânea e intermitente através de um "espelho" ou de maneira contínua, permitindo o registro de alterações nos computadores-alvo através de um "monitoramento". Em outra ocasião, o mesmo autor se refere às buscas online de maneira concisa, como a "infiltração clandestina em um sistema informático para observar seu uso e ler os dados armazenados nele" (Kist, 2019, p.202).

Importa lembrar que os sistemas informáticos podem ser acessados de forma remota ou a distância, de modo que as pesquisas online referem-se especificamente às realizadas de forma remota. O cenário mais comum é a busca presencial, na qual o investigador se encontra diante de um dispositivo informático para acessar e descobrir os dados armazenados nele, visando a posterior apreensão. No entanto, é possível que durante esse processo ele perceba que os dados procurados não estão na memória desse dispositivo, mas sim em outro local, como em um ambiente de nuvem, acessível através do dispositivo à sua frente, desde que esteja conectado à Internet. Como já mencionado, é para essas situações que as leis mencionadas anteriormente permitem a extensão da pesquisa para esse outro sistema informático - que pode até estar localizado em outro país. Obviamente, se a pesquisa for presencial, não pode ser considerada uma ação encoberta, já que, normalmente, é realizada na presença do investigado.

Manuel da Costa Andrade (2009, p.153) considera que a busca online consiste em “aceder, de forma oculta e à distância, via internet, aos dados contidos num computador, observá-los e, sendo caso disso, copiá-los em maior ou menor medida. O que pode acontecer sob a forma de intromissão instantânea e descontínua (“espelho”) ou de forma contínua, permitindo o registo das alterações ocorridas nos computadores-alvo (*monitoring*).”

A pesquisa é um procedimento instrumental para outro processo, que é a apreensão dos dados identificados pelo investigador como potencialmente probatórios. No entanto, a apreensão constitui um ato subsequente e distinto da pesquisa. É importante notar que o termo

"pesquisa informática online remota", se refere a uma investigação que envolve um único acesso à distância ao sistema informático em questão, com o intuito de identificar dados previamente armazenados e relevantes para a investigação do crime. Esses dados já foram gerados anteriormente e permanecem no sistema informático. Esta situação não deve ser confundida com outra em que a busca se concentra em dados em produção, que estão em processo de serem gerados.

2.5.7 Busca e apreensão online com recurso a *Malware*

Como foi evidenciado, a pesquisa informática online ocorre como uma extensão de uma pesquisa presencial. Neste caso, o investigador, ao realizar uma busca presencial, utiliza o dispositivo informático para acessar outro sistema informático. Dependendo das circunstâncias, essa ação pode ser considerada “ação encoberta”. A situação em questão é distinta, pois o acesso ao computador, dispositivo ou sistema informático do alvo é realizado por meio de um software malicioso (*malware*).

À título de conceituação, para kist (2019, p.205) o termo *Malware* é definido como:

> O termo *malware* nasce da junção das palavras software, no sentido de programa informático, e *malicious*, significando malicioso, e tais elementos *malware* são suficientes para revelarem a sua essência: um programa de computador destinado a infectar sistemas informáticos. É por isso que a conotação ordinariamente associada ao *malware* é negativa e expressiva de algo ou de atividade ilícita, o que pode gerar dúvidas sobre a legitimidade de seu uso na investigação criminal.

Isto significa dizer que o emprego de *malware* é uma estratégia de investigação que envolve a infecção do sistema informático do investigado para obter provas a serem usadas em um processo penal. Isso requer a intervenção prévia do legislador para definir essa técnica como meio legítimo de obtenção de prova. Uma vez cumprida essa condição, não é correto rotulá-la genericamente como ilegal. No entanto, dada a natureza altamente invasiva desse método, especialmente em relação à privacidade e intimidade do investigado, além da tipificação legal, seu uso deve ser devidamente regulamentado para equilibrar os interesses individuais e coletivos envolvidos. O mesmo raciocínio, com as devidas adaptações, se aplica à interceptação de comunicações telefônicas: na presença de uma norma autorizadora, se os requisitos legais são devidamente cumpridos e a ação é conduzida por órgãos do Estado, não se pode considerar a prática como ilegal.

Outra conceituação de *malware* trazida por Eric Filiol (2004, p.83) de forma mais abrangente por conter elementos que importam à área jurídica, principalmente, no que toca a inserção do cibercrime na sociedade contemporânea:

> Um programa de infecção de computador é um programa simples ou de replicação [reprodução] automática, que se instala discretamente em um sistema de processamento de dados, sem o conhecimento ou consentimento dos usuários, visando colocar em risco a confidencialidade dos dados e a integridade ou disponibilidade do sistema". Cumpre ter em mente, ademais, que malware é um termo genérico para se referir a uma variedade de formas de software hostil ou de intrusão[26].

No que diz respeito às variedades de *malware*, cumpre destacar que o termo engloba uma série de espécies distintas, todas compartilhando a característica de serem instaladas de maneira dissimulada e executarem suas funções de forma oculta, sem o conhecimento ou percepção do usuário ou do titular do sistema informático. As seguintes categorias são as mais comuns, sendo o Cavalo de Tróia talvez o mais reconhecido.

O Cavalo de Tróia é um tipo de *malware* que se disfarça como um arquivo ou site inofensivo. Por causa dessa aparência enganosa, os usuários, sem suspeitar que se trata de *malware*, ativam suas funções ao abrir o arquivo, geralmente enviado como anexo de e-mail ou através do acesso a um site infectado ou falsas atualizações de software. Uma vez instalado, o Cavalo de Tróia pode realizar várias ações no sistema como copiar, modificar e excluir arquivos, coletar senhas, ativar ou desativar funções de hardware e monitorar a atividade do usuário no computador infectado.

Outro formato de *malware*, conhecido como *spyware*, é um programa de computador que coleta informações sobre uma pessoa ou organização, incluindo nomes, endereços e histórico de navegação na web. Alguns spywares (programa espião) também incluem *keyloggers*, que registram as teclas digitadas pelo usuário, o que é útil para obter nomes de usuário, senhas, números de cartão de crédito e assim por diante. Programas de spyware podem se atualizar e instalar novas versões por conta própria, tornando-os mais difíceis de detectar por programas antivírus ou *anti-spyware*.

Os *rootkits*, outra forma de *malware*, permitem que um invasor obtenha acesso exclusivo e remoto a um sistema informático, equivalente ao acesso de um administrador. Eles são usados

---

[26] No original: "A computer infection program is a simple or self-replicating program, which discreetly installs itself in a data processing system, without users knowledge or consent, with a view to either endangering data confidentiality, data in- tegrity and system availability or making sure that users to be framed for computer crime.” Tradução Nossa.

para ocultar outros tipos de *malware*, como spyware ou Cavalos de Tróia, tornando-os invisíveis para programas antivírus ou *anti-spyware*. A instalação de r*ootkits* pode explorar vulnerabilidades no sistema operacional ou usar senhas previamente obtidas.

Logic bombs são um tipo de *malware* que permanece inativo em um sistema informático até que ocorra um evento específico, conhecido como "gatilho". Esse evento desencadeia a ativação do *malware*, que pode ser uma data, um horário, um comando específico, entre outros. Uma vez ativado, o *malware* pode causar danos ao sistema infectado, como a criptografia ou exclusão de documentos.

Os vírus são um tipo de *malware* projetado para se reproduzir e se espalhar em sistemas informáticos. Suas funções incluem danificar o sistema, excluir ou criptografar dados e desativar programas de segurança. Geralmente, eles requerem interação humana para se instalar e se propagar, como o uso de um CD-ROM ou um dispositivo USB. No entanto, existem os *worms*, um tipo específico de vírus, que se propagam pela Internet sem interação humana, sendo usados em ataques cibernéticos em larga escala.

A escolha entre esses métodos, no contexto de investigação criminal, depende das características específicas do caso em questão, como o tipo de sistema informático alvo, as medidas de segurança implementadas, os objetivos da investigação e outras variáveis. Independente da escolha de métodos, significa dizer que utilizar um *malware* como meio de obtenção de provas, implica na instalação desse software em um sistema informático, geralmente sem o conhecimento do alvo, a fim de obtenção de provas que corroborem a persecução penal.

No que toca a parte de apreensão de dados informáticos, restou devidamente demonstrado que a apreensão de dados informáticos é outro método aceito pela Convenção de Budapeste e regulamentado em vários países. Normalmente, essa apreensão ocorre após uma pesquisa informática, que tem como objetivo identificar dados relevantes para a prova.

No entanto, a identificação desses dados também pode ser feita usando *malware*. Como mencionado anteriormente em relação à vigilância online, em certos casos, pode ser necessário para a investigação criminal que os dados, cuja existência e produção em tempo real foram observados, sejam apreendidos na forma de cópia e transferidos para o dispositivo ou sistema informático utilizado pelo investigador.

Geralmente, o mesmo *malware* que permite a vigilância também facilita a cópia dos dados. Quando essa opção é escolhida, ocorre a apreensão online de dados informáticos usando esse método. Em outras palavras, é factível e, em determinados casos, necessário ir além do simples monitoramento ou observação da atividade virtual, transmitindo ou transferindo dados

específicos para o sistema informático do agente que está conduzindo a operação encoberta no contexto da investigação criminal.

2.6 Meios de obtenção da prova digital na Legislação Brasileira

A maioria dos meios para obtenção de prova digital, analisados anteriormente, teve sua origem na Convenção de Budapeste. Ao serem incorporados à legislação pátria dos países signatários, foram moldados de forma diferente do que foi inicialmente proposto pela Convenção.

A ratificação da Convenção de Budapeste pelo Brasil é de grande relevância, visto que ela representa o documento internacional mais influente e crucial no tratamento das questões relacionadas à cibercriminalidade, tanto em termos materiais quanto processuais. Assim, é inevitável que a abordagem desse tema na legislação brasileira se baseie e considere o delineamento estabelecido por essa Convenção, o que também se aplica aos meios de obtenção de prova digital.

Além do Código de Processo Penal, que pode conter os fundamentos para a utilização desses meios de obtenção de prova, existem pelo menos três leis específicas que devem ser consideradas na análise: a já mencionada Lei nº 9.296/96, que trata da interceptação telefônica e telemática, a Lei nº 12.965/14, conhecida como Marco Civil da Internet, e a Lei nº 13.441/17, que alterou o Estatuto da Criança e do Adolescente para incluir, de fato, a figura da infiltração de agentes policiais no meio digital para a investigação de crimes contra a dignidade sexual de criança e adolescente.

2.6.1 Busca e apreensão (de dados informáticos)

O artigo 19 da Convenção de Budapeste aborda a obtenção de prova digital através da busca e apreensão de dados armazenados em meios informáticos. Essencialmente, isso envolve o poder das autoridades investigativas de realizar buscas em sistemas e dispositivos destinados ao armazenamento de dados digitais, como CDs, *pen drives* e discos rígidos externos. A medida também abrange a situação em que os dados não estão no sistema ou dispositivo inicialmente pesquisado, mas sim em outro acessível a partir desse sistema, como quando os dados estão em uma nuvem acessível pela internet.

Uma vez que dados relevantes para a investigação são localizados por meio da pesquisa informática, a instância investigativa tem a autorização para a) apreender o sistema informático

ou parte dele, ou o suporte de armazenamento; b) fazer e manter uma cópia desses dados; c) adotar medidas para preservar a integridade dos dados no local onde estão armazenados; e d) torná-los inacessíveis ou removê-los do sistema informático.

A pesquisa informática é equivalente à busca tradicional de bens tangíveis que, em geral, precede a sua apreensão, desde que tenham relevância como prova. No caso de dados digitais, também é necessário localizá-los para determinar sua existência e localização, como condição prévia para a subsequente apreensão e uso como prova em processos penais.

Portanto, a pesquisa informática é um meio de obtenção de prova contemplado na legislação brasileira, sujeito às regulamentações do Código de Processo Penal referentes a busca e apreensão (artigos 240 a 250). Essa regulação pressupõe que o objeto buscado e passível de apreensão esteja no domicílio do investigado, necessitando de autorização judicial prévia, pois flexibiliza a inviolabilidade associada a esse local. Em casos menos comuns, a busca inicial é pelos suportes físicos dos dados (computadores, CDs, pen drives, etc.) que, em seguida, são apreendidos e levados para a sede da instância investigativa, onde a busca pelos dados armazenados nesses suportes é realizada. A "pesquisa informática" corresponde a essa segunda fase, em que o conteúdo armazenado nos suportes apreendidos é analisado em relação ao seu potencial como prova do fato investigado; e a "apreensão informática" refere-se aos dados informáticos localizados nesse processo de busca e que, na avaliação do investigador ou analista, têm a capacidade de fornecer a prova desejada.

Em resumo, mesmo sem uma legislação específica no Brasil sobre a busca e apreensão informática como mecanismo de obtenção de prova digital, é possível recorrer a ela, com base na regulação básica presente no Código de Processo Penal.

2.6.2 Interceptação Telemática – Lei nº 9.296/96

Conforme anteriormente demonstrado, a forma de comunicação telemática mais tradicional, representada pelo correio eletrônico (e-mail), foi a primeira a surgir. Atualmente, existem os mensageiros eletrônicos instantâneos que facilitam um grande volume de comunicações dessa natureza, incluindo os *chats* em plataformas específicas, cujo funcionamento se baseia na telemática.

A comunicação telemática difere da comunicação telefônica devido a uma peculiaridade: os dados de conteúdo transmitidos são armazenados em algum lugar após o término do processo de comunicação, geralmente na memória do dispositivo informático usado para a transmissão. Por exemplo, o e-mail permanece na caixa de mensagens após ser lido,

assim como o conteúdo transmitido por meio de mensageiros eletrônicos instantâneos (como *WhatsApp* e *Telegram*) é armazenado na plataforma do dispositivo e pode ser acessado pelo aparelho (normalmente um *smartphone*) usado para isso. Assim como conversas em *chats* também são registradas.

Para Kist (2019, p.251), essa situação não deve ser confundida com a transmissão atual das mensagens pela via telemática. Isso significa que essa forma de comunicação apresenta duas realidades que, embora relacionadas e sequenciais, não se confundem: a primeira envolve a transmissão de mensagens, criando uma relação triangular entre o remetente, o destinatário e o terceiro responsável pelo transporte (o provedor de serviços). Enquanto a mensagem estiver sob posse desse terceiro, ela pode ser acessada por alguém que não seja o destinatário, configurando a interceptação da comunicação telemática. A segunda realidade diz respeito ao acesso ao conteúdo transmitido por essa via após a conclusão do processo de comunicação. Neste caso, não há comunicação em curso e, portanto, o conteúdo não está sujeito a interceptação. Para acessar esse conteúdo, são necessárias outras medidas como o acesso à memória do dispositivo informático usado para a comunicação onde o conteúdo está armazenado, ou à respectiva nuvem, onde os dados podem estar em backup (cópia de segurança).

Essa distinção é de grande importância, pois afeta o regime jurídico a ser aplicado para acessar o conteúdo em cada um dos casos: no primeiro, o regime de proteção do sigilo das comunicações privadas é aplicável, enquanto no segundo, o regime de proteção da privacidade e intimidade deve ser invocado.

Considerando essa distinção como ponto de partida, surge um acréscimo quando se menciona "interceptação de comunicação telemática". Trata-se da atividade estatal de acessar o conteúdo da mensagem telemática durante sua transmissão, ou seja, enquanto está sob posse do responsável pelo seu transporte. Em outras palavras, a interceptação ocorre durante o percurso da transmissão, representando uma intervenção na comunicação atual em tempo real. Isso implica uma referência à terceira parte envolvida.

Essa definição implica que a legislação brasileira, mais precisamente a Lei nº 9.296/96, que regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal, abrange explicitamente esse meio de obtenção de prova. Após estipular que "A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça", a lei incluirá a interceptação das

comunicações telemáticas no parágrafo único: "O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática".

A expressão "interceptação do fluxo de comunicações" claramente destaca o aspecto mencionado anteriormente, ou seja, essa medida probatória visa acessar o conteúdo da comunicação telemática enquanto está sendo transmitido, em tempo real, abrangendo o seu fluxo, termo que denota o movimento ou algo em movimento.

Assevera Kist (2019, p.252) que a Convenção de Budapeste, em seus artigos 20 e 21, trata do meio de obtenção de prova digital, referindo-se a ele como "recolha, em tempo real, de dados informáticos", abordando tanto os dados de tráfego (art. 20) quanto os dados de conteúdo (art. 21). E que embora essa distinção não seja explícita na legislação brasileira, ambas as formas de dados podem ser interceptadas com base no parágrafo único do art. 1º da Lei n° 9.296/96 (lei que trata sobre interceptação de comunicações telefônicas), uma vez que fazem parte do processo de comunicação telemática. Portanto, é respaldado pela legislação brasileira o método de obtenção de evidências digitais que envolve a interceptação de dados gerados a partir de comunicações telemáticas, abrangendo tanto informações de tráfego quanto de conteúdo.

2.6.3 Prova documental

O conceito de documento, em termos de prova, não se restringe apenas a uma escrita em papel. No contexto do direito digital, essa ideia se torna ainda mais evidente. De maneira abrangente, um documento é qualquer objeto capaz de materializar um fato, podendo ser através de escrita, sinais gráficos, símbolos, entre outros. Assim, filmes, fotografias, transcrições e desenhos também são considerados documentos. Até mesmo a ata notarial, que é em si um meio probatório, pode ser considerada um documento, embora possua requisitos específicos para garantir sua autenticidade, o que justifica sua categorização distinta.

Para Thamay e Tamer (2022, p. 115), a definição de prova documental consiste:

> o termo prova documental abrange os instrumentos e os documentos, públicos e privados. Qualquer representação material que sirva para reconstituir e preservar através do tempo a representação de um pensamento, ordem, imagem, situação, ideia, declaração de vontade etc., pode ser denominada documento. Os escritos que são celebrados, por oficial público no exercício de seu mister, na forma prevista pela lei, com o intuito de fazer prova solene de determinado ato jurídico, compondo, por assim dizer, a própria essência do negócio (CC 104), ou não, denominam-se instrumentos. Estes são constituídos

> com a finalidade de servirem de prova. O documento não é confeccionado para o fim de servir de prova, mas pode ser assim, utilizado, casualmente.

Documento é qualquer meio físico ou eletrônico em que um acontecimento e suas circunstâncias estão registrados. A prova documental, por sua vez, é o resultado obtido em um processo ou procedimento a partir do uso desse documento.

Exemplos de provas documentais incluem o resultado de um processo baseado em um CD, mídia ou HD anexado aos autos que contenha um vídeo relevante para a discussão jurídica em questão. Da mesma forma, a documentação resultante de um contrato incluído no processo também se enquadra nessa categoria. Além disso, a prova documental pode ser obtida a partir da inclusão de extratos de registros eletrônicos (como IP, data e hora) adquiridos em uma demanda anterior que envolva a quebra de sigilo em relação a um provedor. Capturas de tela ou *printscreens* também constituem provas documentais. Portanto, se um evento está registrado em um suporte físico ou eletrônico, e esse suporte não pertence a outra categoria específica, então o resultado extraído será considerado documental.

Ainda sobre o tema de prova documental, insta salientar que os documentos são categorizados como públicos ou particulares. De forma que um documento público é aquele criado total ou parcialmente com a colaboração de alguma autoridade pública, ou para o qual o Estado, por lei, confere fé pública à sua autenticidade (como em tabelionatos de notas). O documento público, devido à participação de autoridades em sua criação, possui uma presunção de veracidade em termos práticos. Isso significa que o conteúdo do documento é presumivelmente autêntico, íntegro e mantido sob custódia adequada. Portanto, é necessária uma prova contrária legal e eficaz para contestar essa presunção em casos específicos. Exemplos de documentos públicos incluem atas notariais e certidões emitidas por autoridades competentes.

Por outro lado, um documento particular é qualquer documento que não se enquadra na categoria de público, sendo classificado de forma subsidiária. Esses documentos são elaborados sem a participação de alguma autoridade pública ou a concessão de fé pública por lei. No contexto da formatação documental, a participação de uma autoridade ou de alguém com tal função delegada deve ser determinante. Por exemplo, um documento eletrônico que contenha uma assinatura eletrônica baseada na estrutura e chaves públicas da ICP-Brasil não é considerado público. Mesmo com a existência de entidades certificadoras e registradoras públicas e privadas, o documento mantém sua natureza particular. Exemplos de documentos

particulares incluem contratos, trocas de e-mails entre as partes e capturas de tela de conversas em aplicativos de mensagens como WhatsApp e Telegram, por exemplo.

Por fim, no que toca ao momento da juntada do documento probatório no processo penal, ocorre no momento da apresentação da denúncia, no caso de ação penal pública, juntado pela acusação, ou junto com a queixa-crime, se ação penal privada, nos termos do art. 41, do CPP.

2.6.4 Ata notarial

A ata notarial representa um documento de significativa importância no contexto probatório relacionado ao direito digital e à utilização da tecnologia para a realização de fatos com implicações legais. Essa ata, em essência, configura-se como um suporte físico onde um acontecimento e suas circunstâncias são registrados. A distinção reside no fato de que a ata notarial possui características específicas em sua formatação, justificando sua previsão legal como um meio de prova distinto, inclusive inaugurando essa categoria no Código de Processo Civil.

Originalmente prevista no artigo 7°, III, da Lei n° 8.935 de 199428, conhecida como Lei dos Cartórios, que regulamenta o artigo 236 da Constituição Federal29, a ata notarial também é definida no CPC em seu artigo 384, assumindo, a partir de então, a condição de meio de prova típico. Segundo o dispositivo: "A existência e o modo de existir de algum fato podem ser atestados ou documentados, a requerimento do interessado, mediante ata lavrada por tabelião". Além disso, é possível incluir na ata "dados representados por imagem ou som gravados em arquivos eletrônicos" (artigo 384, parágrafo único, CPC). O que se extrai dessa disposição é justamente o reconhecimento da realidade das coisas, permitindo que o tabelião registre documentalmente, em ata, fatos observados eletronicamente. Para os processos penais e trabalhistas, bem como aos procedimentos administrativos ou particulares, a regra é a mesma.

A ata notarial é um documento no qual o notário registra o que foi observado através dos seus sentidos. Como destacado por Arruda Alvim: "Trata-se, em verdade, de um misto de documento público e testemunho oficial do tabelião, que pode conter a apreensão de fatos ou dados, tais como: (a) o conteúdo de sites da Internet; (b) o conteúdo de programas de televisão; (c) quaisquer outros dados representados por som ou imagem gravados em arquivos eletrônicos (artigo 384, parágrafo único do CPC/2015); (d) estado de imóvel no momento da vistoria".

O notário observa e percebe o fato e o descreve com todas as suas circunstâncias em um documento que, por força legal, lhe é peculiar: a ata notarial. Todo e qualquer fato de qualquer

natureza, especialmente os ocorridos em meios eletrônicos ou digitais, podem ser registrados em ata. O que não for observado presencial e pessoalmente pelo notário não poderá constar na ata. Portanto, por exemplo, o notário não pode lavrar ata notarial com base em capturas de tela recebidas pelo WhatsApp do cartório; é preciso que o notário tenha acesso, pessoal e presencialmente, ao telefone celular. A parte deve levar o dispositivo até ele para que possa verificar presencialmente e registrar em ata, ou então ele pode se dirigir até a parte para a constatação *in loco*.

Além disso, o notário não pode incluir juízos de valor ou conclusões técnicas sobre os fatos. Essas atribuições são reservadas, respectivamente, ao destinatário da prova e ao perito. Em resumo, embora a ata notarial seja uma prova de grande relevância, o fato nela documentado não está completamente isento de questionamentos quanto à autenticidade, integridade ou avaliação, como poderia estar caso houvesse uma presunção absoluta de veracidade sobre o ocorrido narrado.

Assim, a ata notarial é um meio de prova seguro e altamente recomendado, o que significa que, em caso de dúvida e sempre que possível, o interessado deve proceder com a sua elaboração. No entanto, é importante ter em mente que, em determinados casos, a veracidade ou integridade do fato registrado na ata pode ser questionada ou contestada, e o valor da prova resultante dela pode ser relativizado diante do conjunto probatório como um todo.

2.6.5 Informações fornecidas por provedores de internet

Os provedores de internet são fontes de informação relevantes como meio de prova, pois a obtenção dessas informações resulta na comprovação de eventos ocorridos no meio digital. A obtenção de dados eletrônicos mantidos pelos provedores de internet é especialmente crucial para autenticar o evento e a prova, sendo essencial para determinar a autoria do fato. Essa medida probatória é acessória e visa facilitar a identificação de usuários de internet.

Provedores de internet englobam tanto os provedores de conexão como os provedores de aplicação. Os primeiros são empresas que oferecem serviços de acesso à internet para usuários, seja por meio de redes fixas ou móveis. Nesta categoria estão incluídas as empresas de telecomunicações e de fornecimento de conexão à internet. Os provedores de aplicação, por outro lado, são empresas que fornecem funcionalidades acessíveis na internet, como e-mails, portais de notícias, lojas online, aplicativos de mensagens, serviços de armazenamento em nuvem, entre outros.

Para possibilitar a identificação dos autores de eventos digitais, especialmente aqueles envolvendo atividades ilícitas, a Lei nº 12.965/2014, conhecida como Marco Civil da Internet, exige que os provedores de internet armazenem as informações relacionadas ao uso de seus serviços. Para provedores de aplicação, o prazo de armazenamento é de 6 meses, enquanto para provedores de conexão é de 1 ano.

Os provedores de aplicação mantêm registros de acesso às aplicações de internet, que incluem informações sobre data e hora de uso de uma aplicação específica a partir de um endereço IP determinado. Essas informações dizem respeito à conexão utilizada para o acesso à aplicação, incluindo endereços IP, data e hora (incluindo o fuso horário). Com base nessas informações, é possível identificar os provedores de conexão associados ao acesso à internet. Existe um debate se esses provedores devem ou não armazenar e fornecer o conteúdo produzido em suas funcionalidades específicas, envolvendo questões de privacidade e interceptação de comunicações.

Por sua vez, os provedores de conexão mantêm registros de conexão que englobam informações sobre data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal. Além disso, incluem os dados cadastrais fornecidos pelo usuário ao contratar os serviços de conexão. Em resumo, essas informações permitem identificar quem utilizou a internet por meio dos serviços fornecidos pelo provedor, em qual data e hora, e também fornecem detalhes sobre o contratante dos serviços de conexão.

Com relação às empresas de telefonia que oferecem serviços de internet móvel, elas também são classificadas como provedores de internet. No entanto, se o evento estiver relacionado diretamente à prestação dos serviços de telefonia em si, as empresas devem cooperar na identificação do usuário, conforme orientação da Agência Nacional de Telecomunicações (ANATEL).

Para a realização de qualquer evento no ambiente digital, como o uso de e-mails, redes sociais, transações fraudulentas, compras online, envio de mensagens, entre outros, o usuário primeiro precisa utilizar um provedor de conexão para se conectar à internet. Em seguida, acessa as funcionalidades disponíveis na internet por meio do provedor de aplicação, e por meio dessas funcionalidades, realiza o evento digital cuja autenticidade precisa ser comprovada, como enviar ou receber e-mails, fazer postagens em redes sociais, enviar mensagens por aplicativos, disponibilizar conteúdo online, criar páginas na internet, entre outros. Esse processo representa os passos para a realização de um evento digital na internet: usuário, provedor de conexão, provedor de aplicação e, finalmente, a execução do evento.

Ressalta Thamay e Tamer (2022, p.144-145) que a identificação da autoria ou a comprovação da autenticidade do evento digital na internet depende da realização desse processo e da obtenção das informações correspondentes que serão desenvolvidas em cinco fases: (i) identificação e preservação do evento na internet; (ii) identificação do provedor de aplicação utilizado (por exemplo, e-mail, hospedagem, rede social, etc.); (iii) obtenção das informações junto ao provedor de aplicação; (iv) identificação do provedor de conexão utilizado (empresas que fornecem internet banda larga ou serviços de internet móvel); e (v) obtenção das informações junto ao provedor de conexão. Nem sempre todas essas fases serão necessárias, pois dependem das circunstâncias específicas do evento em questão. Por exemplo, no caso de um e-mail recebido, é possível identificar diretamente o provedor de conexão com base no cabeçalho técnico da mensagem eletrônica.

O Marco Civil da Internet estabelece diretrizes específicas para o processo de retorno na identificação do autor do evento, principalmente para proteger a privacidade dos usuários da internet. As principais diretrizes incluem: (i) a existência de evidências de atividades ilegais; (ii) a identificação precisa do conteúdo fático; e (iii) a aplicação da cláusula de reserva da jurisdição, que implica na necessidade de uma ordem judicial para obter as informações.

A necessidade de indícios de ilegalidade em relação ao evento cuja autenticidade está sendo investigada é justificada pela própria relativização da privacidade que o processo de fornecimento de informações pelos provedores implica. Isso significa que deve haver uma suspeita fundamentada de atividade ilegal para justificar a identificação do usuário, afastando sua privacidade de forma concreta. Essa premissa é extraída do artigo 10 do Marco Civil da Internet, que destaca a importância de preservar a intimidade, a vida privada, a honra e a imagem das partes envolvidas, direta ou indiretamente.

Quanto à identificação e preservação do conteúdo (primeira fase), isso envolve identificar o conteúdo específico, especialmente indicando a URL correspondente (*Uniform Resource Locator*), ou seja, o endereço eletrônico que identifica um conteúdo na Internet por meio de um link. Normalmente, a URL está na barra de endereços do navegador da Internet, seja de uma página, uma postagem, uma imagem, entre outros. Também pode estar presente em uma postagem ou compartilhada por aplicativos de mensagens (como o WhatsApp) ou por e-mail. Cada conteúdo criado possui uma URL específica correspondente. A identificação específica do evento e sua preservação dependem das circunstâncias particulares do evento em si. Por exemplo, se o conteúdo está acessível por meio de um navegador ou link recebido, a identificação da URL é essencial. Se for encaminhado um e-mail, é necessário identificar o remetente. Se uma mensagem for recebida por meio de um aplicativo, é necessário identificar

o número de telefone do remetente. Após a identificação específica do conteúdo, recomenda-se a preservação por meio de uma ata notarial, ou, dependendo das circunstâncias, por meio de *blockchain*.

O artigo 22 do Marco Civil da Internet estabelece os requisitos legais que autorizam a parte interessada a solicitar judicialmente o fornecimento de informações dos provedores. A primeira regra, que diz respeito aos indícios de ilicitude, é detalhada no inciso I do parágrafo único, enquanto a identificação precisa do conteúdo é abordada nos incisos II e III. Em resumo, o requerimento deve conter fundamentos sólidos da ocorrência do ilícito, uma justificativa fundamentada sobre a utilidade dos registros para fins de investigação ou instrução probatória, e o período ao qual os registros se referem.

A terceira regra crucial para a obtenção de informações pelos provedores de internet é a cláusula de reserva de jurisdição, o que significa que a obtenção dos registros de acesso ou conexão depende estritamente de uma ordem judicial específica, relacionada diretamente ao fato identificado conforme o artigo 22 do Marco Civil da Internet. Essa determinação é estabelecida nos artigos 10, 13 (§ 5º) e 15 (§ 3º) do MCI. Importante mencionar que o MCI se refere explicitamente aos registros de acesso ou conexão, não incluindo os dados cadastrais. Portanto, para obter essas informações, não é necessária uma ordem judicial. O artigo 10, § 3º da Lei, faz essa ressalva: "§ 3º O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição". A parte interessada pode obter essas informações diretamente dos provedores de forma extrajudicial.

Além disso, a Polícia Civil, por exemplo, pode obter essas informações diretamente dos provedores, sem precisar solicitar uma quebra de sigilo ao juízo competente, através do envio de um ofício no âmbito de um inquérito policial. Vale ressaltar que nos procedimentos de investigação criminal relacionados a organizações criminosas (conforme a Lei nº 12.850/2013), também há uma ressalva explícita: "Art. 15. O delegado de polícia e o Ministério Público terão acesso, independentemente de autorização judicial, apenas aos dados cadastrais do investigado que informem exclusivamente a qualificação pessoal, a filiação e o endereço mantidos pela Justiça Eleitoral, empresas telefônicas, instituições financeiras, provedores de internet e administradoras de cartão de crédito". Além disso, a mesma lei define como crime a recusa ou omissão no fornecimento das informações necessárias à investigação:

> Art. 21. Recusar ou omitir dados cadastrais, registros, documentos e informações requisitadas pelo juiz, Ministério Público ou delegado de polícia,

> no curso de investigação ou do processo: Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa. Parágrafo único. Na mesma pena incorre quem, de forma indevida, se apossa, propala, divulga ou faz uso dos dados cadastrais de que trata esta Lei.

Por último, é crucial ressaltar que, como em qualquer processo probatório, essa atividade é contingente, ou seja, estará sujeita à avaliação das particularidades do caso em questão. A finalidade primordial das medidas de obtenção de informações junto aos provedores de internet, como destacado, é validar a autoria do fato. Contudo, o alcance efetivo dessa finalidade dependerá das circunstâncias específicas de cada situação.

2.6.6 *Blockchain*

O *blockchain* é uma tecnologia revolucionária que se destaca pela sua excepcional autenticidade e integridade. Sua arquitetura inovadora cria um ambiente de confiança inigualável para a troca de informações e transações digitais. Em termos simples, o conceito de blockchain em inglês sugere a ideia de uma corrente de blocos. Essa é a representação central de sua estrutura essencial. O *blockchain* pode ser entendido como uma rede de terminais eletrônicos, principalmente computadores, distribuídos globalmente e interligados através da internet.

A internet é definida estruturalmente como "o sistema composto por um conjunto de protocolos lógicos, organizado em escala global para uso público e aberto, com o propósito de viabilizar a comunicação de dados entre terminais por meio de diversas redes" (art. 5º, IMCI). É uma rede de alcance global em que qualquer computador, dispositivo eletrônico ou sistema computacional (terminal art. 5º, IIMCI) pode estar conectado para a transmissão de informações. O blockchain é, portanto, uma rede que utiliza essa infraestrutura técnica para uma forma específica de troca de informações, em uma dinâmica particular.

Trata-se de uma rede *peer-to-peer*, na qual cada usuário contribui voluntariamente com seu dispositivo para essa malha descentralizada de dispositivos. O traço distintivo das redes *peer-to-peer* é que cada dispositivo conectado a essa rede descentralizada atua simultaneamente como cliente, recebendo informações, e como servidor da rede. Cada dispositivo, assim, desempenha essa dupla função. Isso contrasta com a rede mais comum, em que há um servidor central responsável pela emissão de informações, enquanto os demais dispositivos conectados agem apenas como clientes ou receptores dessas informações ou mensagens eletrônicas. Cada dispositivo, portanto, representa um nó ou ponto de interseção nessa rede.

Sobre o tema, Schwab (2016, p.27-28) retrata um conceito sobre blockchain e discorre sobre a sua importância, por ser caracterizado como protocolo seguro:

> A revolução digital está criando abordagens radicalmente novas que revolucionarão o envolvimento e a colaboração entre indivíduos e instituições. Por exemplo, o blockchain, muitas vezes descrito como um "livro-razão distribuído", é um protocolo seguro no qual uma rede de computadores verifica de forma coletiva uma transação antes de registrá-la e aprová-la. A tecnologia que sustenta o *blockchain* cria confiança, permitindo que pessoas que não o conheçam (e, portanto, não têm nenhuma base subjacente de confiança) colaborem sem ter de passar por uma autoridade central neutra ou seja, um depositário ou livro contábil central. Em essência, o *blockchain* é um livro contábil compartilhado, programável, criptograficamente seguro e, portanto, confiável; ele não é controlado usuário único, mas pode ser inspecionado por todos. O *Bitcoin* é o *blockchain* mais conhecido neste momento, mas essa tecnologia logo dará origem a inúmeros outros. Se, agora, a tecnologia do *blockchain* registra transações financeiras feitas com moedas digitais (o *Bitcoin*, por exemplo), futuramente ele servirá para registrar coisas bem diferentes, como nascimentos e óbitos, títulos de propriedade, certidões de casamento, diplomas escolares, pedidos às seguradoras, procedimentos médicos e votos - essencialmente, quaisquer tipos de transação que podem ser transformadas em código. Alguns países ou instituições já estão investigando o potencial do *blockchain*.

Ao contrário do método mais convencional de armazenamento centralizado, que inclui serviços de nuvem, todas as informações na rede *blockchain* não estão concentradas em um único dispositivo ou servidor, mas são compartilhadas por todos os dispositivos. Além disso, cada um desses terminais ou nós, possui uma cópia idêntica e completa de todo o conteúdo da rede. Por exemplo, se um leitor cria um arquivo de texto em seu computador pessoal, esse arquivo é armazenado localmente na máquina, seja em um disco rígido ou SSD. Ele pode optar por fazer uma cópia em um dispositivo de armazenamento móvel, como um pen-drive, ou salvá-lo na nuvem, em serviços oferecidos por empresas como *Google*, *Microsoft*, *Samsung* ou *Apple*. Em todos esses casos, o armazenamento é centralizado.

No contexto do *blockchain*, as informações são armazenadas de forma descentralizada e completa em cada terminal conectado à rede. Em outras palavras, qualquer ação online realizada fica registrada em toda a rede. Isso significa que qualquer dispositivo integrante do *blockchain*, seja um computador, dispositivo eletrônico ou estrutura computacional, possui uma cópia completa das informações, como arquivos e transações, e pode acessá-las instantaneamente. Além disso, cada um desses terminais é encarregado de validar digitalmente qualquer modificação nas informações da rede, sendo necessária a aprovação unânime de toda a estrutura do *blockchain* para qualquer alteração. Funciona como um registro eletrônico distribuído de informações.

Segundo explicam Thamay e Tamer (2022, p. 178), a estrutura da rede não se limita apenas ao armazenamento distribuído, mas também abrange a construção e evolução da rede em blocos sucessivos, formando uma cadeia de elos. É dessa característica estrutural que a tecnologia recebe o nome. Além disso, essa cadeia não apenas define a forma, mas também a formatação e a segurança do conteúdo que ela contém.

O segundo bloco inclui as informações do primeiro e do segundo bloco. O terceiro bloco contém não apenas suas próprias informações, mas também as dos três blocos anteriores. O quarto bloco, por sua vez, abriga suas próprias informações e as dos três blocos precedentes, e assim por diante. Cada novo bloco de informações é gerado a partir e com base em todas as informações dos blocos anteriores, além de conferir validade a todas as informações anteriores.

De forma ilustrativa, a compreensão do *blockchain* pode ser visualizada através de duas perspectivas: a primeira é vertical e sequencial, destacando uma cadeia de blocos de informação em que cada bloco contém suas próprias informações e as de todos os blocos anteriores; a segunda é horizontal e distributiva, representando o *blockchain* como uma rede descentralizada de dispositivos, onde cada dispositivo possui uma cópia autêntica da cadeia de blocos.

Isso implica que para modificar ou eliminar uma informação presente em qualquer um dos blocos, seria necessário alterar todos os outros. No entanto, o armazenamento em uma rede descentralizada e a existência de cópias fiéis em cada dispositivo ou nó dessa rede implicam que qualquer alteração em qualquer bloco precisa ser tecnicamente validada por todos os dispositivos da rede. Isso proporciona uma camada adicional de segurança ao sistema, tornando ineficaz um ataque a apenas um dos dispositivos.

No que toca a segurança estrutural, cada bloco de informação no blockchain contém uma referência ao bloco anterior, criando uma cadeia ininterrupta de registros. Isso implica que qualquer alteração em um bloco teria ramificações em todos os blocos subsequentes, exigindo o consenso da rede para ser validada. Portanto, a autenticidade do blockchain é garantida pela necessidade de consenso e validação de múltiplos participantes, tornando extremamente difícil a adulteração de informações.

Sobre o assunto, Thamay e Tamer (2022, p.179) descrevem que:

> cada dispositivo (usuário) pertencente ao blockchain recebe uma chave privada para adicionar e alterar informações na rede. Privada porque apenas o usuário possui essa chave. Inserida e validada na rede, para todos os demais usuários ela é tecnicamente convertida em uma chave pública à qual todos têm acesso e que confere a segurança de que aquele determinado usuário foi quem de fato tratou a informação na rede. A chave pública é, por assim dizer, a face externa e validada pelo blockchain da chave privada, confirmando-a. Essa estrutura

> descentralizada (com a multiplicidade de cópias fidedignas - uma idêntica em cada terminal ou *peer* da rede - e criptografada) faz com que - salvo programação em contrário específica - se for inserida uma informação na rede blockchain, ela não pode ser mais alterada, o que assegura a validade e utilidade prática da rede, inclusive probatória. Traz, igualmente e pelas mesmas razões, alta confiabilidade ao sistema.

Além disso, o uso de criptografia avançada desempenha um papel crucial na autenticidade do *blockchain*. Cada transação é protegida por algoritmos criptográficos complexos, garantindo a confidencialidade e a integridade dos dados. Essa camada adicional de segurança torna praticamente impossível decifrar ou manipular as informações contidas em um bloco. Quanto á transparência, todas as transações e registros são visíveis para todos os participantes da rede, proporcionando um alto grau de visibilidade e auditabilidade. Isso significa que qualquer irregularidade pode ser prontamente identificada e corrigida, promovendo a confiança entre os membros da comunidade blockchain.

No que toca sobre a utilidade probatória, Thamay e Tamer destacam a autenticidade e integridade da prova documental acerca da utilização do *blockchain*, como exemplo cita precedente obtido através da 5ª Câmara de Direito Privado, do Tribunal de Justiça do Estado de São Paulo, no julgamento de Agravo de Instrumento sob o nº 2237253-77.2018.8.26.0000, que "embora o juízo não tenha enfrentado a questão da validação da prova preservada por meio de blockchain, a decisão reconhece a utilidade da tecnologia.

Para os autores, a Corte Paulista concluiu que não havia risco na comunicação dos usuários, pois o conteúdo já havia sido preservado por meio do *blockchain*, garantindo sua validação jurídica, mesmo que fosse posteriormente removido pelos próprios usuários ou pelo provedor. Funcionando como uma plataforma de armazenamento digital descentralizado conectada, ela possibilita o salvamento de documentos de natureza factual, dos quais, como qualquer documento, é possível extrair o respectivo resultado probatório e, em seguida, conferir-lhe utilidade jurídica. Assim como em qualquer meio de prova, é responsabilidade do destinatário formar sua convicção, utilizando a persuasão racional para atribuir o valor que julgar apropriado de forma fundamentada.

Asseveram ainda os autores que a preservação de conteúdo factual no *blockchain* pode ocorrer de duas maneiras ou por meio de duas funcionalidades principais. Na primeira, que é aparentemente mais simples de compreender, um documento eletrônico (geralmente em formato .pdf) é salvo na rede *blockchain* ou o próprio documento é criado dentro da rede (como os chamados "*smart contracts*" ou contratos inteligentes). Em resumo, nessa primeira finalidade, a rede age como um dispositivo eletrônico comum de armazenamento, com a

diferença de que a informação é inserida em uma rede descentralizada e o conteúdo tende a ser imutável. Na segunda funcionalidade de preservação probatória, a rede *blockchain* possibilita a verificação da existência de um conteúdo específico disponível na internet (precisamente na *World Wide Web*). Ao indicar a URL ou o endereço específico da página web publicamente acessível, a rede blockchain verifica se a página está realmente disponível e salva uma cópia idêntica do conteúdo na própria rede, garantindo sua existência no momento da verificação. Por exemplo, se uma página for criada com o propósito de divulgar informações falsas sobre uma pessoa, como uma forma de difamá-la, ao utilizar essa segunda funcionalidade de salvamento na rede blockchain, mesmo que a página seja posteriormente removida, a prova permanece preservada.

Nesse sentido, lecionam os autores que a cada nova alteração ou inserção de informação/conteúdo na rede blockchain, a informação é validade por toda a rede, e automaticamente é salva uma cópia idêntica e fidedigna em cada um de seus terminais:

> Nesse processo de validação, é calculado e extraído um código *hash* correspondente à nova informação e que assegura que de fato ela está salva na rede e de forma autêntica e integra. (…), o *hash* se trata de um código de composição alfanumérica (ex. 0956bcaf7fe61322696edb2efb0cf7fe5d) e corresponde ao resultado de uma análise byte por byte do arquivo e de seu armazenamento e validação na rede. Além dele, é atribuído ao documento um *timestamp* (uma marca temporal com a data e hora precisa de criação/ salvamento do arquivo). Qualquer alteração futura do arquivo, alterará seu próprio *hash* e o *timestamp*, o que assegura a verificação de imutabilidade do conteúdo. Inclusive, caso o usuário deseje fazer a conferência, isso será possível com a resposta positiva do sistema se o arquivo for idêntico. Qualquer alteração impedirá a verificação. Ou, em outras palavras, se o arquivo salvo for alterado, o *hash* será também mudado. O código é, nessa perspectiva, a segurança de integridade e autenticidade da prova verificada de forma on-line (existência, conteúdo, momento de sua elaboração e quem teria feito a partir das informações públicas que nele constam).

Por fim, ao analisar o passo a passo da cadeia de custódia da prova, para os autores Thamay e Tamer (2022, p. 184), o *blockchain* garante a autenticidade e a integridade do documento a partir do momento em que é incorporado em sua rede. Antes desse ponto, essa responsabilidade não recai sobre ele. No caso de um documento eletrônico, a autenticidade e a integridade são presumidas quando há uma assinatura eletrônica presente. Essa presunção pode ser dispensada se for devidamente comprovada de outra maneira. Já em relação a um documento digitalizado, a autenticidade e a integridade são verificadas ao considerar a formatação do documento físico original e o processo de digitalização, através da comparação com a versão física original. Em resumo, o blockchain é um recurso de grande utilidade na confirmação de

provas, contudo, é crucial compreender com clareza como os requisitos de validade e utilidade da evidência digital são atendidos por meio dele.

2.6.7 *Verifact*

O *Verifact* representa uma ferramenta online especializada na coleta de provas digitais, oferecendo um método intuitivo e eficiente para reunir conteúdo da internet com validade jurídica. A plataforma permite a coleta de diversos formatos, como áudios, vídeos, imagens, textos e arquivos, provenientes de fontes como aplicativos de mensageria (WhatsApp e Telegram), redes sociais (*TikTok*, *Instagram*, *Facebook*, *Twitch*, *Twitter*, entre outros), plataformas de vídeos (*YouTube* e *Vimeo*), *webmails* e sites, tudo acessível por meio de um navegador de internet.

O resultado dessa coleta é um relatório técnico certificado, contendo telas registradas, dados e metadados técnicos auditáveis, preparados para possíveis perícias técnicas. Além disso, é gerado um vídeo que registra a navegação, incluindo áudio, e os arquivos baixados durante a sessão. A assinatura certificada da *Verifact* e o carimbo de tempo ICP-Brasil proporcionam imutabilidade aos dados, registrando precisamente o momento em que o conteúdo foi acessado na internet, prevenindo alterações ou exclusões após o registro.

Mesmo se o conteúdo original desaparecer da internet, os dados e metadados coletados possibilitam uma perícia técnica abrangente para validar a autenticidade e procedência do material. Destaca-se a importância de coletar o conteúdo diretamente da fonte original, evitando encaminhamentos ou salvamentos em outros locais, que podem resultar na perda de dados cruciais para comprovar a origem e integridade. A *Verifact* destaca-se como o único meio de coleta online de provas digitais que preserva todas as etapas aplicáveis da cadeia de custódia do Código de Processo Penal (CPP) e está em conformidade com a ISO 27037, uma norma internacionalmente reconhecida para a identificação, coleta, aquisição e preservação de evidências digitais em casos judiciais diversos.

Esta solução atende aos requisitos estabelecidos por normas internacionais e aos princípios da cadeia de custódia previamente mencionados, destacando-se pela sua acessibilidade universal, disponível a qualquer pessoa em qualquer momento e com custos mais atrativos. A empresa assegura que seu procedimento é capaz de fundamentar argumentos e conteúdos encontrados na internet quanto à sua integridade, anterioridade, origem, contexto e ausência de adulteração durante e após o processo de coleta. Em outras palavras, possibilita

afirmar que determinado conteúdo estava publicado em um site específico, em um momento específico, exatamente como os conteúdos foram captados, oferecendo um meio eficaz para evitar interferências indevidas.

Para respaldar sua eficácia, a empresa *Verifact* disponibiliza em seu site diversos laudos emitidos por empresas de cibersegurança, atestando sua habilidade em prevenir a manipulação do conteúdo durante e após a coleta, bem como certificados de capacidade técnica emitidos por órgãos públicos de investigação, como Ministérios Públicos e Polícias Civis, confirmando sua aptidão para atender aos requisitos de custódia relacionados à coleta e preservação de evidências. Até o momento, é a única solução online com essas validações. Ao contrário de outras soluções online, a abordagem técnica utilizada pela Verifact envolve a criação de um ambiente virtualizado a cada sessão de registro, com um sistema operacional sem histórico de atividades anteriores, uma conexão de internet independente e um acesso remoto limitado para permitir a interação do usuário com o ambiente. Todo o processo de coleta ocorre nos servidores da empresa, afastado das possibilidades técnicas de interferência que podem ocorrer no dispositivo do usuário. A empresa detém uma patente nacional para esse procedimento.

Com uma interface fácil de usar, a *Verifact* automatiza um processo complexo de coleta de evidências na internet, acessível a pessoas sem conhecimento técnico avançado, com resultados consistentes com as melhores práticas forenses. Os conteúdos podem ser registrados como telas estáticas em formato PNG, vídeos capturando a tela com registros de áudios e vídeos, além de arquivos baixados durante a navegação, acompanhados de amplos metadados técnicos sobre a situação que geram uma auditabilidade consistente do resultado. A preservação do conteúdo contra manipulações posteriores é realizada mediante o uso da Certificação Digital ICP/Brasil, gerenciada pelo Instituto Nacional de Tecnologia da Informação/Casa Civil da Presidência da República e regulamentada pela MP nº 2.200-2/2001, sendo capaz de autenticar documentos conforme o art. 411, II, do CPC.

2.6.8 Geolocalização, Mapas e Georreferenciamento

A prova de geolocalização refere-se à utilização de informações de posição geográfica para identificar a presença de um dispositivo ou pessoa em uma determinada localidade. Existem várias maneiras de adquirir esses dados, incluindo o uso de sinais de internet, GPS, radiofrequência e outros métodos de posicionamento. É comum encontrar a geolocalização em dispositivos móveis, como *smartphones*, *smartwatches* e *tablets*, desempenhando um papel essencial em aplicativos como *Google Maps* e *Waze*.

Ressaltam os autores Souza, Munhoz e Carvalho (2023, p.150-151) que a validade da prova de geolocalização na esfera criminal, pode ser empregada pelos órgãos responsáveis pela persecução penal, como a Polícia Judiciária e o Ministério Público, com o objetivo de investigar e comprovar a prática de delitos, identificar responsáveis, coautores e participantes, localizar testemunhas e vítimas, e reconstruir a trajetória de suspeitos antes e após a ocorrência do crime, entre outras finalidades. Por sua vez, os advogados de defesa de investigados e acusados têm a possibilidade de utilizar essa prova para apresentar álibis, evidenciando que o cliente se encontrava em outra localidade no momento do crime, contestar depoimentos de testemunhas que associam o cliente ao local do incidente e reforçar a estratégia de defesa ao fornecer informações precisas sobre a localização e movimentação do cliente.

A utilização da evidência de geolocalização tem sido aceita para esclarecer casos criminais. Em decisões recentes, o Superior Tribunal de Justiça (STJ) determinou que a quebra de sigilo dos dados de geolocalização é apropriada, necessária e proporcional em situações em que não há outra medida viável para desvendar o delito (AgRg no RMS 68487/PE). Essa abordagem é considerada menos intrusiva do que a interceptação telefônica, que permite o acesso ao fluxo de comunicações de dados e ao conteúdo integral das conversas (AgRg no RMS 67093/MT).

No que diz respeito ao Supremo Tribunal Federal (STF), a questão da quebra de sigilo dos dados de geolocalização está em discussão no Recurso Extraordinário (RE) 1.301.250 RG/RJ, sob a relatoria da Ministra Rosa Weber. Esse caso teve sua repercussão geral reconhecida (tema 1.148) em junho de 2021 e ainda não foi submetido a julgamento até o momento.

O georreferenciamento na definição trazida por Souza, Munhoz e Carvalho (2023, p.211) é uma tecnologia que possibilita a representação visual de dados geográficos por meio de mapas, englobando informações como pontos de interesse, trajetos, imagens de satélite e dados relacionados ao tráfego aéreo.

O georreferenciamento é uma técnica essencial na área de geotecnologias, que visa associar informações a uma localização geográfica específica, permitindo uma análise espacial mais precisa e eficiente. Essa prática torna-se cada vez mais relevante em diversas áreas, como cartografia, agricultura, meio ambiente, urbanismo, e diante da evolução tecnológica, ganhou espaço no âmbito jurídico, principalmente como fonte de obtenção de prova.

Exemplos de georreferenciamento citados por Souza, Munhoz e Carvalho (2023, p. 211-213) fazem parte a imagens de satélite, radar de aeronaves, rastreamento de voos, dentre outras. A plataforma de imagem de satélite, é gerida pelo Instituto Nacional de Pesquisas

Espaciais (INPE) do Brasil, e disponibiliza acesso a dados e informações sobre o meio ambiente e o clima, provenientes de missões e projetos espaciais conduzidos pelo INPE. O Radarbox é uma ferramenta de radar de aeronaves conveniente e acessível para monitorar voos em tempo real, sendo fácil de utilizar e proporcionando informações precisas e atualizadas acerca da localização de aeronaves em todo o globo. Já o *Flightradar24* é um serviço global de rastreamento de voos que oferece dados em tempo real sobre milhares de aeronaves em todo o mundo. O *Plane Finder*, por sua vez, é uma ferramenta online que permite aos usuários coletar informações de aviões em tempo real em escala global, incluindo a posição da aeronave, altitude, velocidade e número de voo.

Em artigo publicado por Sousa e Campos (2015), destaca que com o avanço da tecnologia, a cartografia convencional evoluiu da apresentação estática de mapas em papel para a exibição digital de mapas dinâmicos, tridimensionais e enriquecidos com recursos multimídia. De modo que afirma os autores que a transição da cartografia para o meio digital tornou-se ainda mais significativa com a disseminação da Internet e a popularização dos Sistemas de Informações Geográficas na Web (SIGWeb).

Explicam em termos gerais, que os SIGWeb são caracterizados por interfaces simples e intuitivas, oferecendo funcionalidades básicas para a manipulação e controle do conteúdo do mapa. Bem como, a ferramenta se destaca pela facilidade de uso para usuários não especializados, juntamente com o poder de compartilhamento de dados geográficos, são os principais impulsionadores da popularização desses sistemas.

Atualmente, há diversos SIGWeb disponíveis, tanto comerciais quanto livres, oferecendo uma variedade de serviços e recursos. Um exemplo de iniciativa livre é o *Open Street Map* (OSM), que visa construir uma malha viária global por meio da contribuição voluntária dos usuários. O projeto OSM permite ao público consultar sua base de dados por meio de um SIGWeb, possibilitando a visualização detalhada do sistema viário de várias cidades ao redor do mundo. A base de dados do OSM também é disponibilizada para desenvolvedores que desejam incorporá-la em seus próprios SIGWeb.

Por outro lado, existem os SIGWeb privados que oferecem serviços de mapas e roteamento, que se destacam-se o *Bing Maps* e o *Google Maps*. Apesar de serem serviços privados, esses sistemas não cobram pelos serviços básicos, como o roteamento, mas oferecem a opção de adquirir licenças comerciais para usuários e empresas interessados em explorar recursos avançados. O *Google Maps*, por exemplo, disponibiliza gratuitamente o serviço *Google Street View*, que enriquece a visualização cartográfica por meio de imagens fotográficas em nível do solo, capturadas por veículos equipados com sofisticados dispositivos de

imageamento. Antes de serem disponibilizadas, as imagens passam por um processo de turvação de regiões que possam permitir a identificação de pessoas e veículos. Posteriormente, as imagens são armazenadas e indexadas em um banco de dados espacial para facilitar a rápida recuperação e apresentação da visão panorâmica de 360 graus de qualquer ponto do mapa.

As provas digitais de georreferenciamento constituem elementos essenciais em diversas áreas, fornecendo uma base sólida para análises espaciais e uma documentação precisa de informações geográficas. Esse tipo de prova é particularmente significativo no âmbito judicial, dada a exatidão das coordenadas geográficas que desempenha um papel de importância.

A utilização de tecnologias como o Sistema de Posicionamento Global (GPS) e softwares especializados possibilita a coleta de coordenadas precisas, gerando uma documentação digital que pode ser empregada como prova em processos judiciais capaz de validar e demonstrar os limites territoriais e espaciais.

2.7 Da cadeia de Custódia

Através da legislação denominada “pacote anticrime” pela Lei nº 13.964/2019, houve um aprimoramento em diversos aspectos do código de processo penal. Dentre as significativas mudanças introduzidas por essa nova lei, destaca-se a inclusão dos artigos 158-A a 158-F, que regulamentaram o instituto da cadeia de custódia:

> “Art. 158-A do Código de Processo Penal (BRASIL, 1940): Considera-se cadeia de custódia o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte”.

Inicialmente, a cadeia de custódia foi concebida com base na jurisprudência norte-americana, visando preservar a integridade das provas e garantir a autenticidade entre a evidência e os fatos reconstruídos. Conforme afirmado por Badaró (2021, p.511), a cadeia de custódia é a "história cronológica escrita, ininterrupta e testemunhada, que acompanha a evidência desde o momento da coleta até sua apresentação em tribunal".

Deve-se ressaltar a expressão "cadeia de custódia", referindo-se à "documentação da cadeia de custódia", pois o procedimento de documentação da cadeia de custódia implica essencialmente em garantir a autenticidade e a integridade da prova desde o momento em que é colhida, assegurando que a evidência apresentada posteriormente nos autos seja genuína e autêntica em relação à sua origem.

Nesse contexto, Aury Lopes (2019, p.408) enfatiza que a preservação das fontes de prova é fundamental, especialmente quando se trata de provas coletadas fora do processo, como, por exemplo, no caso da coleta de DNA ou de interceptações telefônicas.

Além disso, justifica-se a importância de garantir a autenticidade e originalidade das provas, uma vez que isso evita possíveis manipulações indevidas, tanto para incriminar quanto para absolver, resultando em decisões judiciais de melhor qualidade e evitando injustiças.

Sob um enfoque doutrinário, é introduzida a abordagem da doutrina espanhola, da qual se originou o princípio da "mesmidade", destacando a necessidade de observar certas garantias formais no tratamento e procedimento das evidências da cadeia de custódia, com o objetivo de evitar quaisquer alterações indevidas.

Ao apresentar a documentação da cadeia de custódia ao magistrado, deve-se garantir que os elementos de prova apreciados e valorados sejam os mesmos originalmente coletados, conforme defendido por Aury Lopes (2019, p.413), para evitar que alguém seja julgado com base no “mesmo”, mas em provas selecionadas pela acusação.

2.7.1 Etapas da cadeia de Custódia

Conforme previsto no artigo 158-B do Código de Processo Penal, o rastreamento do vestígio abrange dez etapas, que são: reconhecimento, isolamento, fixação, coleta, acondicionamento, transporte, recebimento, processamento, armazenamento e descarte.

A etapa de reconhecimento consiste em identificar um elemento como potencialmente relevante para a produção de prova pericial (art. 158-B, I). De acordo com as definições do artigo, esses elementos podem ser quaisquer objetos, materiais brutos, visíveis ou latentes, constatados ou coletados, que estejam relacionados à infração penal (art. 158-A, § 3º).

O isolamento, por sua vez, tem o propósito exclusivo de evitar qualquer alteração nos elementos potencialmente selecionados, sendo o ato de preservar e isolar o ambiente imediato, mediato e relacionado aos vestígios e ao local do crime (art. 158-B, II).

A fixação, como terceira etapa, consiste na descrição detalhada do vestígio tal como encontrado no local do crime ou no corpo de delito. Essa descrição pode ser complementada por fotografias, filmagens ou croquis, e é indispensável que seja acompanhada de laudo pericial elaborado pelo perito responsável pelo atendimento (Art.158-B, III).

No que diz respeito à etapa da coleta dos elementos, essa deve ser realizada de preferência por um perito oficial, que encaminhará os vestígios para a central de custódia (art. 158-C).

A fase do acondicionamento, por sua vez, é o procedimento em que cada vestígio coletado é devidamente acondicionado de forma individualizada, levando em conta suas características físicas, químicas e biológicas, para posterior análise. Nesse processo, é necessário registrar a data, hora e o nome do responsável pela coleta e acondicionamento (art. 158-B, V).

Assim como a coleta, o acondicionamento também possui especificações detalhadas conforme descrito no art. 158-D, caput, tais como: i) o uso de recipientes adequados à natureza do material, preservando suas características; ii) a selagem dos recipientes com lacres numerados individualmente, garantindo a inviolabilidade e integridade dos vestígios durante o transporte; iii) o lacre só pode ser aberto pelo perito responsável pela análise, ou por pessoa autorizada mediante justificativa (art. 158-D, §3º).

Após a delicada etapa de preservação dos vestígios, segue-se a fase do transporte, que consiste no ato de transferir o vestígio de um local para outro, utilizando as condições adequadas para garantir a preservação de suas características originais, levando-o até a central de custódia (art. 158-B, VI).

A fase do recebimento é o ato formal de transferência da posse do vestígio, que deve ser devidamente documentado. Esse registro deve conter, no mínimo, informações como o número de procedimentos e unidade de polícia judiciária, local de origem, nome do responsável pelo transporte do vestígio, código de rastreamento, natureza do exame, tipo do vestígio, protocolo, assinatura e identificação de quem o recebeu (art. 158-B, VII).

A etapa mais extensa e crucial é a do processamento, que envolve o exame pericial propriamente dito, com a manipulação do vestígio de acordo com a metodologia apropriada para suas características biológicas, físicas e químicas. Para a realização desse procedimento, devem ser rigorosamente seguidas outras instruções, visto que implica na abertura do primeiro lacre colocado na fase de acondicionamento. Após o rompimento do lacre, o perito responsável deve registrar na ficha de acompanhamento do vestígio o nome e a matrícula do responsável, a data, o local e a finalidade, bem como informações sobre o novo lacre utilizado. Além disso, é necessário acondicionar o antigo lacre rompido no novo recipiente (art. 158-D, §5º).

Quando o vestígio requer provas de laboratório, o procedimento da cadeia de custódia é dividido em duas fases. A primeira é a "custódia externa", que abrange o controle do contato com a amostra desde o local de origem da coleta até sua chegada ao laboratório. A segunda fase, denominada "etapa interna", fica a cargo do registro do recebimento da amostra pelo laboratório, detalhes de transferência, armazenamento e sua destinação final.

Assim como ocorre em muitos laudos periciais, na documentação da cadeia de custódia é necessário incluir informações sobre a preparação da amostra para os testes realizados, bem como as condições do material após a perícia, como mudanças em suas características, peso, quantidade, entre outros detalhes.

Após o processamento minucioso, o material passa para a fase de armazenamento, que envolve a guarda apropriada do material a ser processado. Esse armazenamento deve ser realizado com vínculo ao número do laudo correspondente, possibilitando futuras contra perícias, descarte ou transporte de acordo com a legislação vigente (art. 158-F).

Por fim, a décima e última fase do procedimento, conforme previsto pela lei, é a fase do descarte, que consiste na liberação do vestígio, seguindo a legislação vigente e, quando necessário, mediante autorização judicial (art. 158-B, X).

É importante ressaltar que, embora o descarte represente a destinação final da custódia, os elementos probatórios devem ser mantidos armazenados na central de custódia, com os devidos registros, a fim de assegurar a autenticidade no caso de necessidade de repetição da perícia ou realização de contraprova.

Portanto, fica evidente a importância de seguir detalhadamente todo o procedimento estabelecido na lei referente à documentação da cadeia de custódia, garantindo que os operadores do direito possam exercer seus direitos de defesa e acusação, alcançando uma paridade de armas e assegurando a autenticidade dos elementos probatórios, promovendo, assim, a justa prolação de decisões.

2.7.2 Quebra da cadeia de Custódia - *Break on the chain of custody*

Sobre o tema da quebra da cadeia de custódia, Gustavo Badaró argumenta que, do ponto de vista terminológico, não é possível violar a própria cadeia de custódia de provas, uma vez que esta se limita a verificar se uma pessoa teve ou não contato com a fonte de prova.

O autor defende que o que realmente se viola é a integridade ou adulteração da fonte de prova, conforme previsto no §3º do art. 158-A do CPP. Segundo ele, falsificar a fonte original de prova não implica em violar a cadeia de custódia, mas sim consiste em fraudar ou adulterar essa própria fonte. Em outras palavras, a violação não diz respeito à sucessão de pessoas que tiveram contato com a prova, mas sim à documentação que atesta essa realidade.

Na visão de Badaró (2021, p.517), a quebra da cadeia de custódia ocorre quando a documentação da cadeia de custódia não é registrada integralmente, ou seja, quando o registro das pessoas que tiveram contato e acesso à fonte e ao material de provas é feito de forma parcial, em desacordo com o detalhamento exigido pela lei.

Essa situação leva a duas possibilidades: a primeira seria considerar a prova como ilegítima e, portanto, não admiti-la no processo; a segunda seria atribuir um valor probatório reduzido à prova produzida a partir de fontes cuja cadeia de custódia foi violada.

No entanto, Aury Lopes (2019, p.414) discorda desse posicionamento e defende que a única consequência aceitável em caso de quebra da cadeia de custódia deve ser a proibição da valoração probatória, resultando na exclusão física da prova principal e de todas as suas derivadas. Para Lopes, a importância de respeitar estritamente as regras do jogo está na necessidade de criar um efeito dissuasório – *deterrent Effect* -, desestimulando as agências repressivas de recorrerem a práticas ilegais para obter punições.

Em relação ao tema, o legislador não estabeleceu as consequências processuais específicas em caso de quebra da cadeia de custódia, deixando a discussão contemporânea entre a admissibilidade e a valoração da prova, ficando a critério das fontes hermenêuticas, dogmáticas e jurisprudenciais encontrar a melhor abordagem sobre o assunto.

2.7.3 A Prova digital na Cadeia de Custódia

Conforme a definição apresentada por Furlaneto Neto, Santos e Gimenez (2018), “as provas digitais compreendem os arquivos informáticos que podem estar em posse do investigado ou de terceiros, contendo informações relevantes para a busca da verdade. Essas provas abrangem todos os dados ou informações armazenadas em dispositivos informáticos”.

De acordo com a conceituação trazida por Greco, os dispositivos informáticos englobam aparelhos capazes de receber dados, processá-los e transmitir os resultados, tais como computadores, smartphones, *IPads*, *tablets*, entre outros.

A legislação recente trata sobre a cadeia de custódia das provas digitais, tema em questão, que envolvem provas obtidas por meio de interceptação do fluxo de comunicações telemáticas, quebra de dados ou por meio de infiltração policial virtual. Essa área exige uma metodologia padronizada para a coleta e análise das evidências digitais, pois o ambiente digital, como mencionado anteriormente, é volátil e sofisticado. As informações frequentemente se apresentam codificadas, exigindo o uso de dispositivos físicos para seu processamento e revelação de conteúdo, além do respeito às exigências detalhadas contidas na cadeia de custódia.

A prova digital, devido à sua própria natureza, é caracterizada por sua volatilidade e mutabilidade, podendo ser adulterada e/ou contaminada. Por esse motivo, é de extrema importância considerar os princípios informáticos para garantir o uso adequado de instrumentos técnicos, a fim de preservar e constituir uma prova válida para a persecução penal.

De acordo com as lições de Badaró (2021, p.522), os princípios constitucionais a serem resguardados na cadeia de custódia da prova digital abrangem os seguintes passos: i) identificar o suporte informático que contém os dados; ii) obter os dados através de técnicas de interceptação, como no caso da interceptação do fluxo de comunicações telemáticas, ou por meio de sequestro, cópia ou espelhamento do suporte que contém o arquivo de dados; iii) realizar a análise dos dados, que consiste em examinar a cópia do suporte informático relevante; e, por fim, iv) apresentar os resultados em juízo.

Diante do exposto, é perceptível que o legislador promoveu a cadeia de custódia visando ao garantismo no processo penal e à paridade de armas, embora tenha descrito as normas de forma genérica. No entanto, existe uma lacuna em relação ao tratamento específico da cadeia de custódia das provas digitais.

A partir disso, especialistas defendem o uso da Norma ABNT NBR ISSO/IEC 27037:2012 (ABNT, 2013) como uma forma de padronizar o tratamento das evidências digitais. Essa norma foi publicada em 2013 e está em vigor desde 2020.

Em artigo escrito por Furlaneto Neto e Santos (2020) sobre a norma mencionada acima, é explicado que “essa norma define e descreve diretrizes para a identificação, coleta, aquisição e preservação de evidências digitais. Embora não seja obrigatória por falta de reconhecimento legal, é a única norma elaborada por órgãos competentes e reconhecida no Brasil para tratar desse assunto. Além disso, em sua versão internacional (ISO), a norma descreve os procedimentos adotados em diversos países.

Nesse contexto, Badaró (2021, p.522) lista alguns métodos procedimentais, como fazer uma cópia ou espelhamento do bitstream da imagem do disco rígido ou suporte de memória em que o dado digital está registrado. Outro método é a utilização de um cálculo de algoritmo hash para verificar a identidade da cópia em relação ao arquivo original.

É de extrema importância que o método utilizado – sejam as melhores práticas ou a normatização da ABNT - garanta a integridade e autenticidade das evidências digitais, assegurando, assim, a força probatória das provas admitidas nos autos.

3 INFILTRAÇÃO POLICIAL VIRTUAL

3.1 Contexto histórico no Brasil e no direito comparado

Segundo o livro Números (13:1-16) do antigo testamento, Moisés recrutou doze homens para infiltrá-los na região, a fim conquistar a terra de Canaã, observar e colher informações importantes que auxiliassem no intento de dominação de terra. Diante disso, ter-se-á, o primeiro indício de surgimento da primeira figura de agente infiltrado (Kanda; Pigozzi; Santos, 2022, p.215).

Mais adiante, sob outra perspectiva, a maioria dos autores refere-se ao surgimento da figura do agente infiltrado durante a era do absolutismo francês do rei Luís XIV, tornando-se um referencial teórico comparativo significativo porque, posteriormente, o instituto da infiltração foi paulatinamente, introduzido em várias jurisdições legais[27].

No esforço para fortalecer o *Ancien Règime*[28], estabeleceu-se o papel do "*agent provocateur"*, assim como dos agentes delatores, que eram recrutados secretamente pela polícia e instruídos a se infiltrar na sociedade francesa para desmascarar os inimigos do Rei em troca de favores.

Sobre o assunto, *Foucault*, descreve em 1987, a evolução do uso de criminosos para fins de espionagem, denúncia e provocação, e enfatiza que seu uso era frequentemente empregado bem antes do século XX. Segundo consta, que após a Revolução Francesa essa prática foi abandonada devido ao fato de que a infiltração passou a se centrar em núcleos de partidos políticos e associações operacionais, fazendo com que o recrutamento desses indivíduos afete diretamente na mobilização de greves. Como resultado, têm-se uma organização subpolítica que trabalha em estreita colaboração com a polícia legal se desenvolveu, tornando-se uma forma de exército paralelo (Foucault, 1987).

---

[27] A respeito disso, Eduardo Araújo da Silva aponta "A origem do instituto pode ser buscada no período do absolutismo francês, sobretudo nos tempos de Luís XIV, no qual para reforçar o regime foi criada a figura do "delator" composta por cidadãos que descobriram na sociedade os inimigos políticos, em troca de favores do príncipe. Nessa época, sua prática limitava-se a espionar e levar os fatos ao conhecimento das autoridades, sem qualquer atividade de provocação. Contudo com o passar do tempo, a atividade de vigiar os suspeitos não foi suficiente para neutralizar a oposição ao regime, passando a atividade da mera espionagem para a provocação de condutas consideradas ilícitas" (Silva, 2009, p.75)".

[28] Antigo regime

A figura do uso de criminosos para tal mister é tão citada, que na literatura cita-se o exemplo de *Eugène-François Vidocq*[29] que ficou conhecido como o primeiro agente infiltrado no mundo:

> A morte de *Vidcoq* ocorrida em 1857, não o impediu de permanecer vivo ao longo da história, ele serviu de inspiração para muitos autores famosos, como por exemplo, *Vautrin de Balzac*, em seu personagem *Jean Valjean "Les Misérables*" (1862), por Hugo e *Jackal des Mohicans* de Paris, por *Dumas* (1854-59). Ele tornou-se o herói de muitos romances, quadrinhos e filmes, do século XIX ao XXI. É verdade que a sua vida parece torná-lo um personagem fictício, mas também é preciso lembrar que ele foi um criador de ficção, depois de ter sido um falsificador, condenado, espião e policial, ele também se tornou escritor. E entre essas ficções, ele se dedicou especialmente à sua (tradução nossa)[30].

Nota-se que *Vidcoq* também foi mencionado por *Focault*, que fez uma crítica bem-vinda, que recria a cena do início da infiltração naquele momento. O que por si só, serve para demonstrar que *Vidcoq* foi objeto de inúmeros estudos acadêmicos em sua legislatura patriarcal.

> Mas a importância quase mítica que ele teve aos próprios olhos de seus contemporâneos não se deve a esse passado, talvez enfeitado demais; não se deve sequer ao fato de que, pela primeira vez na história, um antigo forçado, alforriado ou comprado, se tenha tornado chefe de polícia, mas antes ao fato de que nele a delinquência assumiu verdadeiramente seu estado ambíguo de objeto e instrumento para um aparelho de polícia que trabalha contra ela e com ela (Focault, 1987).

Posteriormente a infiltração policial se tornou forte protagonista no cenário europeu, com a regulamentação do uso especial de investigação em diversos ordenamentos jurídicos.

Os países da Europa continental vêm desenvolvendo formas de cooperar na luta contra o crime desde o final da década de 1950, mas essa cooperação realmente decolou na década de 1980 como resultado do aumento do crime internacional.

---

[29] *Eugène-François Vidocq* (1775-1857) foi um criminoso e criminalista francês que inspirou muitos autores. Foi o fundador da *Sûreté Nationale* (segurança Nacional), polícia especializada em investigações criminais. *Vidcoq* sendo o primeiro homem a ter uma agência de detetives particulares, e ficou conhecido como o "pai da criminologia moderna".

[30] Leia-se no original: *La mort d'Eugène-François Vidocq le 11 mai 1857 ne l'a pas empêché de demeurer bien vivant. Inspiration du Vautrin de Balzac, du Jean Valjean des Miserábles (1862) d'Hugo et du Jackal des Mohicans de Paris de Dumas (1854-59), il est aussi le héros de nombreux romans, bandes dessinées et films, du XIX au XXI siècle. Il est vrai que sa vie rocambolesque semble en faire un personnage de fiction mais il convient également de rappeler qu'il fut créateur de fiction : après avoir été faussaire, forçat, mouchard et policier, il se fit aussi ècrivain. Et, parmi ces « fictions », il se consacra particulièrement à la sienne*. (GAUTHIER, Nicolas. Eugène-François Vidocq, penseur de l'espace social criminel. Romantisme: 2017/1. nº 175. p.29).

Para isso, a maioria dos países da união europeia adotaram como instrumento que adveio da Convenção de *Shengen*, que regulamentou e detalhou as formas de cooperação entre as autoridades policiais dos países subscritores.

Dada a complexidade do tema, e suas implicações para os direitos, liberdades e garantias dos cidadãos, os organismos internacionais têm deixado ao legislador nacional a decisão de como regulamentar a atuação do agente infiltrado. Desse modo, as normas surgem de acepções diversas, de acordo com o contexto histórico-cultural de cada país. A título de exemplo, em alguns países como o reino unido, a infiltração policial é de domínio público, de forma que o país distribui gratuitamente à população um Código de Conduta, enquanto em outros países, o instituto é levado à nível de Segurança de Estado, portanto privativo.

Sobre as diferenças na positivação legal dos institutos entre os países, Isabel Oneto (2005, p.96), acrescenta que o instituto da infiltração policial da forma como conhecemos, advinda da legislação alemã, em seu §110a do StPO – *StrafprozeBbuch*, encontra-se nos Estados Unidos e na maior parte da Europa, com exceção de Luxemburgo.

A autora cita como exemplo que na Holanda, a formação de grupos engajados na "*pseudo-achat*[31]" começou em 1985. O governo austríaco estabeleceu uma unidade especial para combater crimes envolvendo o tráfico de substâncias entorpecentes, dentro da qual estavam sendo planejadas “operações encobertas”. Na Suíça, as autoridades responsáveis pela persecução criminal, utilizou como recurso “agentes infiltrados privados” nas operações de narcotráfico, de modo que estes agentes simulam potenciais compradores em ação conjunta com os agentes das forças policiais.

Por fim, a infiltração foi aprimorada para ser mais eficaz em derrubar e erradicar o crime organizado, e esse desenvolvimento começou nos Estados Unidos da América com as ações de dois policiais infiltrados, *Donnie Brasco* e *Bob Musella*.

Nos anos de 1976 e 1981, *Brasco*, pseudônimo fictício do agente chamado *Joseph Pistone*, se infiltrou na máfia de *Nova York*, juntando-se à família *Bonanno* e por meio de sua infiltração, *Brasco* foi capaz de construir relacionamentos de confiança com os principais membros da família, a ponto de intencionalmente, “se tornar um deles”, o que levou à acusação e condenação de centenas de pessoas.

Importante frisar que a instituição foi usada anteriormente como ferramenta de controle e repressão monárquica, antes de se tornar parte da própria força policial. A história demonstra que a instituição se tornou uma das formas mais eficazes de combater e desmantelar organizações altamente especializadas e compartimentalizadas (Wolff, 2018, p.21).

---

[31] Traduzido do Francês, pseudo-compra (tradução nossa).

A evolução do instituto não somente se deu na parte europeia e norte americana, o uso dos agentes infiltrados foi implementado em diversas legislações e jurisprudência de vários países, como ver-se-á a título de contextualização.

O desenvolvimento do instituto da infiltração policial não se originou apenas na Europa e América do Norte; como pode ser visto, o uso de agentes infiltrados foi implementado em várias nações através de leis e acórdãos jurisprudenciais.

3.2 Infiltração policial no direito estrangeiro

É cediço afirmar que o uso da infiltração policial tem angariado perspectivas positivas de resultados, sendo implementada nos diversos ordenamentos vinculados à *civil law*. Sendo importante analisar - ainda que superficialmente - as legislações acerca da tônica no ordenamento jurídico de alguns países e suas dicotomias, se houver.

A título introdutório, convém citar a Convenção de Palermo, ocorrida no ano de 2000, em Nova York, que em seu artigo 20, prevê a utilização de meios especiais de investigação de provas, dentre as quais a figura da infiltração de agentes. A convenção traça conceitos e delimitações a fim de que os países signatários possam introduzir a medida em seus ordenamentos legais[32].

A infiltração de agentes nos Estados Unidos da América é frequentemente adotada, em decorrência das diversas agências especializadas no método, como por exemplo, FBI (*Federal Bureau of Investigations*), criado em 1908, por *Theodore Roosevelt,* e DEA (*Drug Enforcement Administration*). Nos Estados Unidos, as legislações sobre a infiltração são esparsas, tendo assim, diversas regulamentações gerais, das quais se destaca o Título 28, da parte 2, capítulo 33, do Código de Processo Judicial, que estabelece diretrizes acerca das situações em que se pode utilizar a adoção da medida, bem como, o título 22, parágrafo 2º, item 11, do Código de Regramentos Federais (*Code of Federal Regulations*). E as orientações de formas e limites de atuação dos agentes, são encontradas em manuais próprios das respectivas agências, *FBI* e *DEA*.

No capítulo que trata da "Unidade de Contra-Inteligência em Departamento e Agências Federais Comunitárias Não-Inteligência" estabelece as unidades e departamentos, previstos no item a) "O Diretor do *Federal Bureau of Investigation* estabelecerá unidades de

[32] No Brasil, as determinações trazidas pela Convenção de Palermo, foram comtempladas pelo decreto Lei nº 5.014/2004.

contra-espionagem nos departamentos e agências descritos na subseção (b). Essas unidades serão compostas por oficiais da Divisão de Contra-espionagem do *Federal Bureau of Investigation"*.

Quanto as obrigações, estas estão disciplinadas no mesmo título no item "(c) Obrigações", que declina quais são as funções que deverão ser presididas por todas as agências de contra-espionagem do país:

> (c) Obrigações - O Diretor do *Federal Bureau of Investigation* deve assegurar que cada unidade de contra-espionagem estabelecida na subseção (A) em um departamento ou agência descrita na subseção (b) desempenhe as seguintes funções:
> (1) Realiza avaliações, em coordenação com a liderança do departamento ou agência, para determinar a postura de contra-espionagem do departamento ou agência, incluindo quaisquer componentes do mesmo.
> (2) Informa e consulta a liderança do departamento ou agência, incluindo quaisquer componentes do mesmo, e fornece recomendações com relação a quaisquer ameaças de contra-espionagem identificadas pela comunidade de inteligência.
> (3) Fornece o apoio administrativo e técnico necessário para desenvolver, em coordenação com a liderança do departamento ou agência, um plano para eliminar ou reduzir as ameaças descritas no parágrafo (2).
> (4) Serve como o principal ponto de contato para o departamento ou agência com relação à contra-espionagem para a comunidade de inteligência.

No que toca o uso da infiltração policial, o Estados Unidos permite a utilização da técnica especial de investigação e coordena diversas diretrizes que ficam a cargo e liberdade dos Estados legislarem de acordo com as particularidades próprias de cada um.

A infiltração policial virtual já foi admitida nos Estados Unidos à exemplo da operação emblemática conhecida como "Operação Torpedo[33]" largamente divulgada, e ficou conhecida pela utilização do *malware* CIPAV (*Computer and Internet Protocol Address Verifier)* pelas autoridades norte-americanas, os agentes ao utilizarem o *software* de rotina a fim de detectar IP's de indivíduos que conectam ou compartilham pornografia infantil em outros sistemas de compartilhamento de arquivos (ex: torrents). Em 2012, o FBI lançou sua primeira grande operação contra crianças e sites de pornografia usando uma técnica de investigação de rede NIT (*Network Investigative Technique*), termo cunhado pelo FBI para sua ferramenta de *hacking*.

A "Operação Torpedo" deu início com a prisão de *Aaron McGrath*, suposto anfitrião de três sites que incluíam pornografia infantil, acessíveis através da rede TOR. O FBI expediu uma

[33] *United States Attorney's Office District of Nebraska 2015 - Annual Report*. Disponível em: https://www.justice.gov/usao-ne/file/830846/download#page=25. Acesso em: 30 mai 2023.

busca para autorizar a instalação de um NIT (*Network Investigative Technique)* em um dos websites de *McGrath*, que após a concessão da autorização ficou permitido que a agência dos investigadores utilizassem a ferramenta por três semanas a fim de monitorar as atividades, como resultado, a operação "desanonimizou" vinte e cinco indivíduos e resultou em dezenove condenações.

A operação é detalhada na publicação anual de 2015 do "*United States Attorney's Office District of Nebraska 2015 - Annual Report* (Escritório de Advogado dos Estados Unidos Distrito de Nebraska relatório anual 2015), p.21[34]:

> O FBI foi alertado sobre a presença de servidores de computador em *Nebraska* hospedando três sites de pornografia infantil. Os sites *PedoBook*, *PedoBoard* e TB2 foram servidores ocultos na rede Tor.
> A Operação Torpedo foi uma investigação pioneira projetada para penetrar na capa de anonimato concedido aos indivíduos que usam o Tor para acessar, visualizar e comentar sobre o abuso sexual de bebês, lactentes e crianças pré-adolescentes. O uso de Técnicas de investigação de rede, interceptações do Título III e outros métodos utilizados pela primeira vez na Operação Torpedo tornou-se o protótipo de outro baseado em investigações da rede Tor.
> O administrador dos sites e outros cinco integrantes receberam sentenças que vão de 12 a 25 anos de prisão por seus papéis. Três indivíduos, *Aaron McGrath*, *Timothy DeFoggi* e *Jason Flanary*, foram os primeiros indivíduos no Oitavo Circuito a ser condenado por se envolver em uma empresa de exploração infantil carregando um obrigatória pena mínima de 25 anos de prisão. Treze indivíduos que eram visitantes, mas não membros dos sites, foram condenados de acessar com a intenção de ver pornografia infantil. Eles receberam sentenças variando de quatro a dez anos. Os promotores e agentes envolvidos na investigação foram reconhecidos pelo Diretor do *Federal Bureau of Investigation* com o prêmio de Destaque de Investigação Criminal. A equipe também recebeu em 2015 o prêmio de "Assistant Attorney General's" Prêmio de Serviço Excepcional (tradução nossa).

A previsão legal na Itália é estabelecida em três diplomas, no artigo 97 do Decreto Presidencial 309/1990, no artigo 12-*quater* do Decreto-Lei nº 306/1992 que posteriormente foi ratificado pela Lei nº 146/2006, de 16 de março de 2006 (Ratificação e implementação da Convenção e Protocolos das Nações Unidas contra o Crime Organizado Transnacional, adotados pela Assembléia Geral em 15 de novembro de 2000 e 31 de maio de 2001); no artigo 14 da Lei nº 269/1998 e *articolo 51 del Codice Penale*.

A alteração trazida pela *Legge* nº 146/2006 inseriu em seu artigo 9º, a disciplina acerca da "*Operazioni sotto cobertura*" que introduziu novos dispositivos recomendados pela Convenção e Protocolos das Ações Unidas, adotados pela Itália.

---

[34] *United States Attorney's Office District of Nebraska 2015 - Annual Report*. Disponível em: https://www.justice.gov/usao-ne/file/830846/download#page=25. Acesso em: 30 mai 2023.

A novel legislativa detalha de forma minuciosa os crimes que permitem a utilização da "*operazioni sotto copertura*"; a título de exemplo, temos a incidência do uso da técnica para fins unicamente de obtenção de provas relativas aos crimes contra a administração pública, dos crimes de particulares contra a administração pública, dos crimes contra a fé pública como por exemplo a moeda falsa, falsificações de documentos públicos das diversas formas de corrupção e dos crimes contra o patrimônio, bem como aos crimes relativos à armas, munições, explosivos, etecetera (art.9, alínea a, da *Legge* n º 146/2006).

Os policiais que podem participar das operações, como agentes especiais, são os policiais judiciários da Polícia Estadual, dos *carabinieri*, e do Corpo de Guardas da Finança, pertencentes às estruturas especializadas ou à Diretoria De Investigações Anti-máfia. A estes policiais, a legislação prevê o uso de documentos, identidades ou indicações de "cobertura/disfarce," emitidos pelos órgãos competentes, assim como para acionar ou entrar em contato com assuntos e sites nas redes de comunicações, devendo informar o Ministério Público dentro de quarenta e oito horas, a partir do início das atividades (art.9, 2, da *Legge nº 146/2006).*

A execução das operações são ordenadas pelos órgãos superiores de direção, por delegação destes, e por seus respectivos chefes. A entidade que ordenar a execução da operação deve notificar, previamente, a autoridade judiciária competente para a diligência. E se tratando de execução de atividades antidrogas, deve ser imediatamente e detalhadamente comunicada à Direção Central dos Serviços Antidrogas e ao Ministério Público competente para as investigações. Se a operação versar sobre crimes que envolvam associação do tipo mafiosa, o órgão responsável pela operação, além do cumprimento dos demais trâmites, deverá, especialmente, comunicar o Procurador Nacional Anti Máfia.

Ainda sobre o órgão do Ministério Público, em quaisquer casos, a este deve ser informado pelo mesmo órgão que ordenou a execução, e durante toda a operação, de todos os métodos aplicados, dos sujeitos participantes da operação, bem como dos resultados (art.9, 4, da *Legge* nº 146/2006).

Infere-se do exposto que não há pedido de requerimento por parte do órgão que irá executar a "*operazione sotto copertura"*, portanto, não demanda autorização judicial, mas sim, de comunicação tanto ao órgão do Ministério Público, que atua como uma espécie de fiscal, quanto da autoridade judicial através de relatórios pormenorizados.

De igual modo, a legislação não fala sobre a possibilidade, ou legitimidade de o órgão do Ministério Público requerer ou requisitar a "*operazione sotto copertura*", o que leva a crer, ao menos, em uma primeira análise, que a legitimidade de propositura de operação sobrevém do corpo de polícia.

De igual modo aos demais ordenamentos legais, os agentes de polícia não são punibilizados, e esta garantia de "exclusão de punibilidade" estão também estendidas aos demais agentes, auxiliares e intermediários que forem necessários à operação. É o que se extrai da leitura do artigo 51, do Código Penal italiano:

> Artigo 51, do Código Penal (Exercício de um direito ou cumprimento de um dever);
> O exercício de um direito ou o cumprimento de um dever imposto por norma legal ou por ordem legítima da autoridade pública exclui a punição.
> Se um fato constitutivo de crime for cometido por ordem da Autoridade, o agente público que deu a ordem é sempre o responsável pelo crime.
> Responde também pelo crime quem executou a ordem, salvo se, por erro de facto, tiver decidido obedecer a ordem legítima.
> Quem executa a ordem ilegítima não é punível quando a lei não lhe permite qualquer controle sobre a legitimidade da ordem (tradução nossa).

Uma questão de interesse trazida pela legislação italiana é o tratamento dado aos materiais ou bens apreendidos em custódia judicial, que são cedidos aos próprios órgãos de polícia judiciária para uso, ou cumprimento dos deveres institucionais.

Ainda difere a legislação italiana ao prever a punição de qualquer um dos envolvidos na operação de infiltração, caso divulgarem ou revelarem a identidade dos agentes infiltrados, com pena de 2 (dois) a 6 (seis) anos.

A legislação italiana dedicou uma lei especialmente ao que se refere "às normas contra a exploração da prostituição, pornografia e turismo sexual infantil" no que toca ao seu combate, através da Lei nº 269/1998 em seu art.14, que posteriormente, com a nova reformulação foram inseridos os artigos: *14-bis, 14-ter; art.14-quater e art. 14-quinquies* que tratam, especificamente, do combate à pornografia infantil em rede de *internet*.

Ainda no Ministério do Interior, foi criado um "Centro Nacional de Combate à Pornografia infantil na internet", denominado como "CENTRO", que possui a função de recolher todos e quaisquer relatórios provenientes das corporações policiais estrangeiras e entidades públicas e privadas, engajadas no combate à pornografa infantil, sobre sites que divulgam material sobre o uso de sexo de menores utilizando a *internet* e outras redes de comunicação, bem como os gestores e quaisquer beneficiários dos pagamentos relacionados.

Os agentes são obrigados a fazer os relatórios acima mencionados sem prejuízo das iniciativas e as determinações da autoridade judiciária e em caso de constatação positiva o site é relatado assim como os nomes dos gerentes, gestores e beneficiários dos pagamentos relacionados são inseridos em uma lista constantemente atualizada.

O “Centro” comunica à “Presidência do Conselho de Ministros - Informações e dados do Departamento, para a igualdade de oportunidades estatísticas relativas à pornografia infantil na *internet*”, por conta da predisposição do plano nacional de combate e prevenção à pedofilia.

Outra medida adotada foi das “Obrigações para os prestadores de serviços da empresa de informações prestadas através de redes de comunicações eletrônicas”, que obriga os fornecedores de serviços de redes de comunicação eletrônica a comunicação de informações encontradas nas redes sobre o tema.

É o que dispõe o texto do art. 14-ter, 1, da *Legge* nº 269/1998:

> Fornecedores de serviços prestados através de redes de comunicação eletrônicas, sem prejuízo do disposto em outros leis ou regulamentos do setor, para relatar ao Centro, se tomem conhecimento, de empresas ou de indivíduos que, a qualquer titulo, “*disseminar, distribuir ou comercializar, também via telemática, de material de pornografia infantil, bem como para se comunicar sem demora ao Centro, que o solicita, qualquer informação relacionados a contratos com tais empresas ou indivíduos”* (art.14-ter, 1, da Legge nº 269/1998).

A disposição prevê ainda que a empresa de rede de telecomunicações mantenha sob custódia os materiais apreendidos por pelo menos quarenta e cinco dias. E quaisquer violações das obrigações impostas implicam em sanção administrativa pecuniária no valor de 250.000 (duzentos e cinquenta mil euros).

Como o diploma legal versa sobre o combate à exploração da prostituição, pornografia, turismo sexual em detrimento de menores, foi necessário inserir a obrigação do “Uso de ferramentas técnicas para impedir o acesso a sites que disseminar pornografia infantil”, disciplinados no art. *14-quater*, que dispõe:

> Artigo 14-quater
> (Uso de ferramentas técnicas para impedir o acesso a sites que disseminar pornografia infantil).
> 1. Os provedores de conectividade à rede INTERNET, a fim de impedir o acesso a sites informados pelo Centro, são obrigados a usar ferramentas de filtragem e suas soluções tecnologias compatíveis com os requisitos identificados pelo decreto de Ministro das Comunicações, em acordo com o Ministro da Inovação e Tecnologias e transmite as associações representantes dos provedores de conectividade de rede de INTERNET. O mesmo decreto também indica o prazo para que os provedores de conectividade à rede INTERNET devem adotar de ferramentas de filtragem.
> 2. A violação das obrigações referidas no n.º 1 é punida com uma sanção pecuniária administrativa de 50.000 euros para 250.000 euros. O Ministério da Educação prevê a imposição da sanção comunicações.

E ainda, o mesmo diploma legal balizou ainda medidas financeiras para combater a comercialização de pornografia infantil:

> 1. O Centro transmite ao *Italian Exchange Office* (UIC), para a posterior comunicação aos bancos, às instituições monetárias, correio, à *Poste Italiane Spa* e aos intermediários financeiros que prestarem serviços de pagamento, as informações referidas no artigo *14-bis* relativo a beneficiários de pagamentos feitos para a comercialização de material relacionado ao uso sexual de menores na *INTERNET* e outras redes de comunicação.
> 2. Bancos, instituições de dinheiro eletrônico, correios italianos *Spa* e os intermediários financeiros que prestam serviços de pagamento comunicar à UIC qualquer informação disponível relativas a relacionamentos e às transações atribuíveis aos sujeitos indicados de acordo com o parágrafo 1.
> 3. Para efeitos de aplicação deste artigo e do artigo *14-bis*, a UIC transmite ao "Centro" as informações obtidas nos termos do art. do parágrafo 2.
> 4. Os contratos celebrados pelos bancos são automaticamente rescindidos, por instituições de dinheiro eletrônico, por *Poste Italiane Spa* e por intermediários financeiros que prestam serviços de pagamento com os assuntos indicados de acordo com o parágrafo 1º, relativos à aceitação, de parte deste último, de cartões de pagamento.
> 5. O "Centro" transmite qualquer informação relativa ao titular do cartão de pagamento que o utilizou para a compra de material sobre o uso sexual de menores na Internet INTERNET ou em outras redes de comunicação, ao banco, ao instituto de dinheiro eletrônico, à *Poste Italiane Spa* e ao intermediário de instituição financeira emissora do mesmo cartão, que pode solicitar informações aos titulares e revogar a autorização de uso do cartão ao respectivo titular.
> 6. Bancos, instituições de dinheiro eletrônico, *Poste Italiane Spa* e os intermediários financeiros que prestam serviços de pagamento, de acordo com as disposições emitidas pelo Banco da Itália, devem relatar os casos de revogação referidos no parágrafo 5, no contexto de notificações fornecidas para cartões de pagamento revogadas de acordo com o artigo 10-bis da lei de 15 de dezembro de 1990, n. 386.
> 7. Bancos, instituições de dinheiro eletrônico, *Poste Italiane Spa* e os intermediários financeiros que prestam serviços de pagamento comunicam à UIC a aplicação das proibições, os casos de cessações referido no n.º 4 e qualquer outra informação disponível relativa às relações e operações imputáveis aos sujeitos indicados de acordo com o n.º 1. A UIC transmite a informação assim adquirida ao Centro.
> 8. Por regulamento adotado nos termos do artigo 17, parágrafo 3, da lei 23 de agosto de 1988, n. 400, dos Ministros do Interior, do justiça, economia e finanças, comunicações, para o igualdade de oportunidades e para inovação e tecnologias, de acordo com o Banco de Itália e a UIC, ouvidos o Gabinete do Fiador do proteção de dados pessoais, procedimentos e regras são definidos modalidade a ser aplicada para transmissão confidencial, por meio de ferramentas informáticas e telemáticas, das informações exigidas pela Este artigo.
> 9. O Banco da Itália e a UIC verificam o cumprimento do disposições referidas neste artigo e no regulamento previsto do parágrafo 8 por bancos, instituições monetárias correio, *Poste Italiane Spa* e intermediários financeiros que fornecem serviços de pagamento. Em caso de infração, ao responsável, será aplicada multa para 500.000 euros. O Banco prevê a imposição da sanção da Itália em casos relativos ao uso de dinheiro eletrônico, ou o Ministro da

> Economia e Finanças, por recomendação do Banco da Itália ou da UIC, nos demais casos. Aplica-se, como compatível, o procedimento previsto no artigo 145 do texto consolidado referido no decreto legislativo de 1 de setembro de 1993, n. 385, e depois modificações.
> 10. As importâncias decorrentes da aplicação das sanções referidas no n.º parágrafo 9 são pagos na receita do orçamento do estado a ser reafetados ao fundo a que se refere o n.º 2 do artigo 17.º, e são destinados a financiar iniciativas de combate à pornografia infantil na INTERNET.

Andou bem o legislador italiano ao adotar práticas que envolvam a ordem monetária, de modo que a instituição do "Centro" e as instituições bancárias, e afins, andam juntas, de forma a se interligarem através da comunicação imediata umas às outras sobre qualquer atividade financeira, com total autonomia, uma vez que para a disponibilização da identificação das contas e das titularidades, é feita diretamente ao "Centro", sem a necessidade de autorização judicial para isso.

Em que pese no ordenamento jurídico italiano, a utilização da técnica de infiltração policial por meio virtual não estar expressamente admitida, através de uma interpretação hermenêutica, adota-se no sistema processual penal italiano a "permissão de realização de diligências processuais para a obtenção de provas atípicas e não tipificadas", previstas no artigo 189 do *Codice de Procedura Penale (CPPenale)* que traz a seguinte disposição:

> Artigo 189.
> Provas não disciplinadas pela lei
> 1. Quando for exigida prova não regulamentada por lei, o juiz pode contratá-la se ela for adequada para segurar apuração dos fatos e não prejudica a liberdade moral do pessoa. O juiz procede à admissão, ouvidas as partes no método de fazer o teste (tradução nossa)[35].

O sistema processual italiano, permite, portanto, o uso de provas não regulamentadas por lei, devendo ser requerida ao juiz a diligência ou meio de prova, desde que o meio seja idôneo e que não fira a liberdade moral da pessoa envolvida. A inteligência do artigo prevê ainda que o juiz decida especificamente sobre o pedido de admissão do meio de prova requerido por quaisquer das partes. Com a disposição do artigo 189º do *CPPènale*, vislumbra-se a possibilidade do uso da técnica de infiltração policial por meio virtual.

---

[35] No texto original: Art. 189. Prove non disciplinate dalla legge 1. *Articole* 189º*: Quando e' richiesta una prova non disciplinata dalla legge, il giudice puo' assumerla se essa risulta idonea ad assicurare l'accertamento dei fatti e non pregiudica la liberta' morale dela persona. Il giudice provvede all'ammissione, sentite le parti sulle modalita' di assunzione della prova.* Disponível em: https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.del.presidente.della.repubblica:1988-09-22;447. Acesso em: 30 mai. 2023. .

Com avanço, por meio da "Reforma de Orlando" de 2016, e aprovada em 2017, regulamentou, expressamente, a utilização do *malware* como meio de obtenção de provas. A previsão permitiu ao Estado ferramentas modernas e mais sofisticadas para o enfrentamento de uma criminalidade em constante avanço. Conforme disposição dada no no Cap. IV, relativo à "*intercettazioni di conversazioni o* comunicazioni" , inserindo no art. 266, n. 2 e n. *2-bis*, do *CPPenale*, inserindo o uso de "*inserimento di captatore informático*" (inserção de coletor informático):

> 2. Nos mesmos casos, a interceptação de comunicações entre os presentes, que também podem ser realizadas por meio de a **inserção de um sensor de computador** em um dispositivo eletrônico portátil. No entanto, se estes ocorrerem em locais indicado pelo artigo 614 do código penal, a interceptação é permitida apenas se houver razão para acreditar que ele ali está para a realização de atividade criminosa. (253) (260) (263) (267) (275). 2-bis. A interceptação de comunicações entre os presentes através de **inserção de um sensor de computador** em um dispositivo eletrônico portátil é sempre admitido nos processos pelos crimes referidos no artigo 51, parágrafos 3º-bis e 3º-quarto, e, mediante indicação de razões que justifiquem a sua utilização mesmo nos locais indicados pelo artigo 614 do código penal, por crimes contra a ordem pública oficiais ou pessoas encarregadas do serviço público contra a administração pública para a qual não está prevista a pena de prisão inferior a cinco anos determinados nos termos da lei do Artigo 4. (253) (260) (263) (267) (270) ((275) (grifo nosso e tradução nossa)[36].

A Alemanha introduziu as "operações encobertas" no seu ordenamento jurídico após a aprovação do *OrgK – Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität* (Lei contra o Tráfico Ilícito de Estupefacientes e Outras Manifestações de Criminalidade) de 22 de setembro de 1992, com previsão legal nos artigos nos artigos 110-A e 110-B.

Na legislação alemã, o uso de agente infiltrado é restrito, pelo princípio da subsidiariedade, que só permite a realização da operação em situações em que, de outra forma,

---

[36] No texto original: "*Negli stessi casi e' consentita l'intercettazione di comunicazioni tra presenti, che puo' essere eseguita anche mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile. Tuttavia, qualora queste avvengano nei luoghi indicati dall'articolo 614 del codice penale, l'intercettazione e' consentita solo se vi e' fondato motivo di ritenere che ivi si stia svolgendo l'attivita' criminosa. (253) (260) (263) (267) ((275); 2-bis. L'intercettazione di comunicazioni tra presenti mediante inserimento di captatore informatico su dispositivo eletrônico portatile e' sempre consentita nei procedimenti per i delitti di cui all'articolo 51, commi 3-bis e 3-quater, e, previa indicazione delle ragioni che ne giustificano l'utilizzo anche nei luoghi indicati dall'articolo 614 del codice penale, per i delitti dei pubblici ufficiali o degli incaricati di pubblico servizio contro la pubblica amministrazione per i quali e' prevista la pena della reclusione non inferiore nel massimo a cinque anni, determinata a norma dell'articolo 4"* (Tradução Nossa).

a investigação fracassaria. A outra limitação prevê que a infiltração só deve ser autorizada quando, no caso concreto, existirem indícios suficientes de que o crime cometido é de natureza grave, e nos seguintes domínios: do tráfico de entorpecentes ou de armas; de falsificação de moeda; de documentos ou valores; de segurança do Estado ou quando se tratar de grupos organizados (§ 110ª, 1, do StPO).

Os investigadores disfarçados - nomenclatura atribuída pela legislação alemã -, são os oficiais de polícia, e a estes, a lei também confere o uso de identidade permanente e alterada (fictícia), de forma que os documentos necessários podem ser produzidos, modificados e utilizados, desde que sejam essenciais para a operação.

No que se refere a parte procedimental, o uso do investigador infiltrado (operações encobertas) só será permitido com a aprovação do Ministério Público, e esta aprovação deve ser feita de forma escrita e delimitada. Se no caso, não houver o consentimento do Ministério Público em até três dias úteis, a operação deve ser encerrada.

Uma dissociação feita na legislação alemã corresponde ao procedimento e preconiza que a medida deve ser dirigida contra um suspeito específico, imposição esta não registrada pelos demais ordenamentos jurídicos.

Quanto à identidade do investigador infiltrado, deve ser mantida em sigilo até depois do término da operação. Entretanto, a identidade pode ser revelada a pedido do Ministério Público e do Tribunal Competente para decidir pela autorização da operação.

Na data de 15 de março foi publicada uma Diretiva da União Europeia DIRETIVA (UE) 2017/541 do "Parlamento Europeu e do Conselho da União Europeia", datada de 15 de março de 2017, relativa à luta contra o terrorismo que substitui a Decisão-Quadro 2002/475/JAI do Conselho, e que altera a Decisão 2005/671/JAI, EM SUA DIRETIVA (21), e dispõe:

> (21) A fim de investigar e processar com êxito infrações terroristas, infrações relacionadas com um grupo terrorista ou infrações relacionadas com atividades terroristas, os responsáveis pela investigação ou repressão dessas infrações deverão poder utilizar instrumentos de investigação eficazes, tais como: são utilizados para combater o crime organizado ou outros crimes graves. A utilização destes instrumentos de acordo com a legislação nacional deve ser orientada, tendo em conta o princípio da proporcionalidade, a natureza e a gravidade das infrações objeto de investigação e deve respeitar o direito à proteção dos dados pessoais. Quando apropriado, essas ferramentas devem incluir, por exemplo, revista em todos os bens pessoais, interceptação de comunicações, vigilância encoberta, incluindo vigilância eletrônica, gravação e armazenamento de gravações de som em veículos públicos ou privados ou em locais privados ou públicos e gravação de

> imagens de pessoas em veículos de lugares públicos e em lugares públicos, e investigações financeiras[37].

Conforme o dispositivo colacionado, é permitido, portanto, utilizar instrumentos de investigação eficazes, dentre os quais a vigilância eletrônica, às infrações relacionadas com um grupo terrorista ou infrações relacionadas com atividades terroristas.

Na Espanha a infiltração é disciplinada no artigo 282-*bis* da *Ley de Enjuiciamiento Criminal España,* que também restringe e delimita a infiltração aos crimes enquadrados dentro do conceito de crime organizado. Posteriormente, em 05 de outubro de 2015, a *Ley de Enjuiciamiento* foi alterada pela Lei Orgânica nº 13/2015, que alterou a Lei de Processo Penal para o reforço das garantias processuais e a regulamentação das medidas de investigação tecnológica.

A legislação espanhola apresenta um rol taxativo quanto aos crimes que permitem o uso da técnica de infiltração, sendo aplicável aos crimes graves e de grande ofensa à sociedade e enquadrados dentro do conceito de crime organizado.

No que concerne ao procedimento, segundo a legislação espanhola, é a polícia que faz o requerimento *ex officio* ao juiz competente, demonstrando, o caso concreto, se enquadrar nas atividades típicas de crime organizado, contido no rol taxativo. Quanto à autorização, será realizada por meio de resolução (decisão) fundamentada e deverá especificar a necessidade da medida (infiltração). Ainda no mesmo inciso, consta a obrigatoriedade de que as informações que forem sendo obtidas com a investigação "*sejam levadas imediatamente, ou o mais rápido possível*", ao conhecimento daquele que autorizou a utilização do agente infiltrado.

---

[37] Na disposição original: "*Damit die Ermittlungen bei und die Verfolgung von terroristischen Straftaten, Straftaten im Zusammenhang mit einer terroristischen Vereinigung oder Straftaten im Zusammenhang mit terroristischen Aktivitäten erfolgreich durchgeführt werden können, sollten die für die Ermittlung oder Verfolgung dieser Straftaten verantwortlichen Personen die Möglichkeit haben, wirksame Ermittlungsinstrumente einzusetzen, wie sie zur Bekämpfung der organisierten Kriminalität oder sonstiger schwerer Straftaten verwendet werden. Der Einsatz dieser instrumente im Einklang mit dem nationalen Recht sollte gezielt erfolgen und dem Grundsatz der Verhältnismäßigkeit sowie der Art und Schwere der untersuchten Straftaten Rechnung tragen und sollte das Recht auf den Schutz personenbezogener Daten achten. Falls angezeigt, sollten diese Instrumente beispielsweise die Durchsuchung jeglichen persönlichen Eigentums, die Überwachung des Kommunikationsverkehrs, die verdeckte Überwachung einschließlich elektronischer Überwachung, die Aufnahme und Aufbewahrung von Tonaufnahmen in privaten oder öffentlichen Fahrzeugen oder an privaten oder öffentlichen Orten sowie Aufnahmen von Bildmaterial von Personen in öffentlichen Fahrzeugen und an öffentlichen Orten sowie Finanzermittlungen umfassen*". (Tradução Nossa) Disponível em: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32017L0541:DE:HTML. Acesso em 30 mai 2023.

Posteriormente, tais informações deverão constar no processo em sua totalidade para serem avaliadas de modo criterioso pelo órgão judicial competente.

A lei espanhola prevê isenção criminal para os crimes cometidos pelo agente infiltrado, guardando a proporcionalidade. No mesmo molde, adotado por outras legislações pátrias, o agente infiltrado está amparado pelo exercício regular do direito, se caso precisar praticar algum crime durante a operação, desde que o agente não tenha provocado por si próprio o delito.

Quanto ao prazo de duração da infiltração policial, a legislação espanhola foi omissa, apenas fazendo referência ao período máximo que o policial poderá utilizar-se da identidade falsa, sendo autorizada por um período de seis meses. De sorte que, o período de duração da infiltração deva ficar a cargo do juiz competente.

Importante destacar, na legislação espanhola, que a identidade fictícia é assegurada até a duração do julgamento, para salvaguardar a identidade real do agente infiltrado nos termos do art. 282-bis, 2, da *Ley de Enjuiciamiento Criminal*.

Participam da infiltração os funcionários da polícia judiciária, que incluem os *funcionarios del Cuerpo Nacional de la Policía y Miembros de la Guardia civil.*

Anteriormente, a *Ley de Enjuiciamiento Criminal* não contemplava a figura da infiltração por meio virtual ou tecnológico, conforme a expressão dada pelo país, e urgia uma reforma legislativa para regulamentar a prática de forma expressa. Quando em março de 2015, o Conselho de Ministros, aprovou o projeto de Lei Orgânica incorporando dois novos incisos ao referido artigo *282-bis LECrim*:

> a. A regulamentação do agente infiltrado da informática em comunidades fechadas da rede usando material ilegal.
> b. A regulamentação do regime jurídico a que estão sujeitas as gravações efetuadas pelo agente secreto em suas conversas com o suspeito.

Portanto, a infiltração policial tecnológica pôde se concretizar diante de duas inovações: *Ley Orgánica 13/2015, de 5 de octubre de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica*.

O projeto de reforma da *Ley de Enjuiciamiento Criminal* ampliou os poderes do agente infiltrado na *Internet* e a inclusão dos incisos 6º e 7º do art. *282-bis do LECrim* se deu diante da necessidade "*de combater a emigração de pedófilos para redes de comunicação privada*", a fim de impedir que a troca de pornografia infantil ocorra em fóruns mais restritos e de difícil

controle pela polícia. E para esse nível de investigação seria necessário o uso da infiltração por meio virtual.

Merecem atenção dois trechos extraídos do Preâmbulo, da reforma legislativa e colacionados abaixo:[38]

> No que se refere aos procedimentos de investigação tecnológica, a reforma contempla a ordem de conservação de dados como medida de segurança, cujo objetivo é garantir a preservação de dados e informações específicas de todo tipo que estejam armazenados em sistema até a correspondente autorização judicial […] Desta forma, a sua posterior contribuição como meio de prova ou, se for o caso, a sua análise forense não será frustrada pelo desaparecimento, alteração ou deterioração de elementos inerentemente voláteis […] Esta norma toma como referência o artigo 16 da Convenção sobre Delitos Cibernéticos, de 23 de novembro de 2001, ratificada pela Espanha em 20 de maio de 2010, e estabelece um prazo máximo de vigência da ordem de noventa dias, prorrogáveis até que sejam autorizados cento e oitenta dias. No mesmo capítulo, é permitida a gravação de imagem em espaço público sem necessidade de autorização judicial, desde que não afete nenhum dos direitos fundamentais do art. 18 de nosso texto constitucional […].

E sobre a regulamentação do agente infiltrado da informática:

> […] regulamenta-se a figura do agente infiltrado da informática, que carece de autorização judicial para atuar em canais fechados de comunicação (já que em canais abertos, por sua própria natureza, não é necessário) e que, por sua vez, necessitará de autorização especial (seja na mesma resolução judicial, com motivação distinta e suficiente, ou em outra diferente) para trocar ou enviar arquivos ilegais devido ao seu conteúdo no curso de uma investigação.

Para concluir, os dispositivos que versam sobre o tratamento e armazenamento de dados acima citados, foram redigidos conforme a orientação declinada pela Convenção de Budapeste de 23 de novembro de 2001, ratificada pela Espanha em 20 de maio de 2010.

O Código Processual Penal Francês ao dispor do instituto da infiltração em sua tônica legislativa o fez de forma minuciosa, em seus artigos 706-81 a 706-87 – e de forma parecida com as demais legislações estrangeiras -; o ordenamento jurídico francês também delimita a utilização da infiltração aos delitos enquadrados no conceito de organização criminosa através do rol taxativo do art. 706.º-73 e 706.º-73.º-1, *du Code de Procédure Pénale*.

---

[38] ESPANHA. *Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimento de las garantias procesales y la regulación de las medidas de investigación tecnológica* Disponível em: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10725. Acesso em: 04 jun 2023.

A legislação francesa cuidou de trazer um conceito acerca da infiltração policial em seu artigo 706-81, segunda parte:

> A infiltração consiste, por oficial ou agente da polícia judiciária especialmente autorizado em condições fixadas por decreto e a cargo de oficial de polícia judiciária encarregado de coordenar a operação, proceder à vigilância de pessoas suspeitas da prática de crime ou delito por pretensão. a essas pessoas como um de seus co-autores, cúmplices ou destinatários. Para o efeito, o oficial ou agente de polícia judiciária fica autorizado a usar de identidade falsa e a praticar, se necessário, os actos referidos no artigo 706.º-82.º. Sob pena de nulidade, esses atos não podem constituir incitação à prática de delitos". (tradução nossa)[39].

Desde que justificada a necessidade do uso da infiltração nos crimes abrangidos pela lei, o Procurador da República faz o requerimento ao juiz de instrução, que após autorizar a realização da operação encoberta, irá supervisioná-la dentro das condições previstas nos art. 706-83, primeira parte. Esta autorização deve ser feita por escrito e expressamente motivada, sob pena de nulidade, nos termos do artigo 706.º-81.º do mesmo diploma legal.

Com relação ao tempo de duração da operação, a autorização concedida fixa a duração da operação de infiltração, que não pode ultrapassar os quatro meses. A operação pode ser renovada nas mesmas condições de forma e duração. E ainda, o magistrado que autorizou a operação pode, a qualquer momento, ordenar a sua interrupção antes do termo do prazo fixado. (706-83, parte final).

Se decorrido o prazo fixado na autorização, ou em caso de decisão de interrupção da operação pelo magistrado, e não havendo prorrogação, o agente infiltrado poderá continuar as atividades, acobertado sob a isenção de responsabilidade penal, pelo tempo estritamente necessário que lhe permita cessar a atividade em segurança, devendo o magistrado ser informado com brevidade. Outra situação ocorre se no caso de findo o prazo de quatro meses e o infiltrado não puder cessar as atividades com segurança, o magistrado autoriza a prorrogação pelo período máximo de quatro meses.

---

[39] No texto original: *L'infiltration consiste, pour un officier ou un agent de police judiciaire spécialement habilité dans des conditions fixées par décret et agissant sous la responsabilité d'un officier de police judiciaire chargé de coordonner l'opération, à surveiller des personnes suspectées de commettre un crime ou un délit en se faisant passer, auprès de ces personnes, comme un de leurs coauteurs, complices ou receleurs. L'officier ou l'agent de police judiciaire est à cette fin autorisé à faire usage d'une identité d'emprunt et à commettre si nécessaire les actes mentionnés à l'article 706-82. A peine de nullité, ces actes ne peuvent constituer une incitation à commettre des infractions»* (Tradução Nossa).

A legislação aponta ainda da obrigatoriedade de relatório elaborado pelo agente da polícia judiciaria e devem constar os elementos que dizem respeito estritamente à infração, de forma que este relatório não deve pôr em risco a segurança do agente infiltrado.

A isenção de responsabilidade da polícia judiciaria (agente) é prevista no art. 706-82, ao destacar "*Os agentes da polícia judiciária ou agentes autorizados a realizar operação de infiltração podem, em todo o território nacional, sem responsabilidade criminal por esses atos (...)*", a título de exemplo: adquirir, deter, transportar, dentre outros.

No que diz respeito à identidade real do infiltrado, a legislação francesa inova, ao proibir que a identidade verdadeira do agente infiltrado conste em qualquer fase procedimental, e se descumprida a proibição, implica em pena de prisão e multa de 75 mil até 150 mil euros, se da revelação de identidade resultar em morte do infiltrado, cônjuges filhos e ascendentes diretos.

Na França a infiltração também está prevista em mais um diploma legal, o "*Code des adouanes*" que segundo ao art. 67 bis, inciso I, permite a infiltração para apuração de infrações relacionadas à alfândega aduaneira:

> […] para a apuração de infrações aduaneiras, se a pena incorrida for igual ou superior a dois anos de prisão, os despachantes autorizados pelo ministro das Alfândegas nas condições fixadas por decreto podem proceder em todo o território nacional, após comunicação ao Ministério Público e salvo oposição deste magistrado, à vigilância de pessoas contra as quais existam um ou mais motivos plausíveis de os suspeitar de serem autores de uma infração aduaneira ou de nela terem participado como cúmplices ou interessados na fraude […].[40]

De igual modo, com a legislação anterior o código aduaneiro trouxe uma espécie de conceito categorizando a infiltração policial por agentes devidamente habilitados para o mister, conforme se infere do texto de lei colacionado:

> […] A infiltração consiste, para um despachante aduaneiro especialmente autorizado nas condições fixadas por decreto, agindo sob a responsabilidade de um agente da categoria A responsável pela coordenação da operação, no acompanhamento de pessoas suspeitas da prática de uma infracção aduaneira, passando, a essas pessoas, como um dos seus co-autores, cúmplices ou

[40] No original: *Sans préjudice de l'application des dispositions des articles 60,61,62,63,63 bis, 63 ter et 64, afin de constater les délits douaniers, si la peine encourue est égale ou supérieure à deux ans d'emprisonnement, les agents des douanes habilités par le ministre chargé des douanes dans des conditions fixées par décret peuvent procéder sur l'ensemble du territoire national, après en avoir informé le procureur de la République et sauf opposition de ce magistrat, à la surveillance de personnes contre lesquelles il existe une ou plusieurs raisons plausibles de les soupçonner d'être les auteurs d'un délit douanier ou d'y avoir participé comme complices ou intéressés à la fraude au sens de l'article 399*.

> interessados na fraude. Para o efeito, o funcionário aduaneiro está autorizado a usar uma identidade falsa e praticar, se necessário, os atos abaixo mencionados. Sob pena de nulidade, esses atos não podem constituir incitação à prática de delitos.

No código aduaneiro francês, a infiltração segue procedimento idêntico da legislação do código de processo penal quanto ao tempo de duração, quanto à legitimidade em operacionalizar a infiltração, autorização judicial motivada e expressa, sigilo quanto a identidade real do agente até o julgamento, excludente da responsabilidade penal do agente e é aplicada aos crimes previstos em rol taxativo na legislação aduaneira.

A única diferença no tipo de infiltração a que se refere o código aduaneiro, está na colaboração entre países estrangeiros, caso haja a necessidade de dar continuidade na operação de infiltração, fora do território nacional francês, com o consentimento do ministro da justiça, após requerimento feito pelo Ministério Público.

Por outro lado, tratando-se de infiltração por meio digital, para apuração de crimes digitais, a legislação pátria não mencionava a sua aplicação de forma expressa nas legislações até então apresentadas e vigentes no país. Isto mudou no dia 26 de janeiro de 2023, quando entrou em vigor no código de processo penal o artigo 230-46:

> Com o único fim de registar crimes e contravenções puníveis com pena de prisão praticados por meio de comunicações eletrônicas, e quando as exigências do inquérito ou inquérito o justifiquem, os oficiais ou agentes da polícia judiciária que intervêm no inquérito ou em carta rogatória podem, se estejam afetos a serviço especializado e especialmente autorizados para o efeito nas condições fixadas por despacho do Ministro da Justiça e do Ministro do Interior, proceder sob pseudónimo aos atos seguintes sem responsabilidade criminal
> 1° Participar de trocas eletrônicas, inclusive com pessoas susceptíveis de serem os autores desses delitos;
> 2° Extrair ou armazenar por este meio dados sobre pessoas susceptíveis de serem os autores destes delitos e quaisquer provas;
> 3° Adquirir qualquer conteúdo, produto, substância, amostragem ou serviço ou transmitir qualquer conteúdo em resposta a uma solicitação expressa. [Disposições declaradas inconstitucionais por decisão do Conselho Constitucional n.º 2022-846 DC, de 19 de janeiro de 2023] a operação seja autorizada pelo Ministério Público ou pelo juiz de instrução apreendido dos factos;
> 4° Após autorização do Ministério Público ou do juiz de instrução apreendidos os factos, com vista à aquisição, transmissão ou venda por pessoas susceptíveis de serem os autores destes delitos de qualquer conteúdo, produto, substância, afastamento ou serviço, incluindo ilícitos, colocar à disposição dessas pessoas meios jurídicos ou financeiros, bem como meios de transporte, depósito, alojamento, conservação e telecomunicação.

> Sob pena de nulidade, a autorização prevista nos n.º 3.º e 4.º, que pode ser dada por qualquer meio, é mencionada ou juntada aos autos do processo e os atos autorizados não podem constituir incitação à prática desses delitos.
> Os atos referidos neste artigo são praticados sob a tutela do Ministério Público ou do juiz de instrução.

Isto porque, em artigo publicado por Gojkovic-Lette, aborda o cibercrime e ampliação da investigação sob um pseudônimo autorizada expressamente na referida legislação, e decorre que a prática não pode ser exercida por quaisquer OPJ's (*officiers de police judiciaire*), somente àqueles especializados e devidamente autorizados, de forma que:

> […] Assim, e de acordo com o mesmo paralelismo ligado à autorização do magistrado e à não incitação à prática destas infrações, os funcionários públicos podem efetuar uma operação de (*coup d'achat*)[41] compra na Internet, considerada como uma compra de confiança.[42]

Infere-se do exposto que o art. 230-46 do *Code de Procédure Pénale* é suscinto, ao disciplinar somente sobre a designação de "proceder sob pseudônimo" e quanto à forma de extração e armazenamento destes dados e demais provas. Da leitura poder-se-á concluir que o artigo permite a infiltração policial por meio virtual por descrever "os oficiais ou agentes da polícia judiciária que intervêm (…) podem, se estejam afetos a serviço especializado e especialmente autorizados para o efeito nas condições fixadas por despacho do Ministro da Justiça (…)" e também é permitida no ordenamento jurídico pátrio através de votos jurisprudenciais, mesmo que ainda suscinta a determinação expressa no referido texto legal.

Outra alteração importante foi dada pela *Loi d'orientation et de programmation pour la performance et la 136 sécurité intérieure* Lei n.º 2011-267, de 14 de Março de 2011 que promoveu a alteração nos artigos 706-102-1 a 9 para a utilização de dispositivos de *malware*:

> Artigo 706-102-1 Versão em vigor desde 01 de junho de 2019
> Alterada pela LEI n 2019-222 de 23 de março de 2019 - art. 46
> Pode ser necessária a instalação de um dispositivo técnico que tenha por finalidade, sem o consentimento dos interessados, aceder, em qualquer lugar,

---

[41] "*Coup d'achat"*, refere-se à prática de um policial comprar algo ilícito em benefício de sua investigação, quando os policiais se fazem passar por potenciais compradores para permitir prisões, ou quando usam um informante para a compra, são "pseudo-compradores."

[42] No original: (…) *Ainsi, et selon le même parallélisme lié à l'autorisation du magistrat et la non-incitation à commettre ces infractions, les fonctionnaires peuvent effectuer une opération de coup d'achat sur Internet, considéré comme un achat de confiance*. GOJKOVIC-LETTE. Colonel Johanne. *Le coup d'achat : Un instrument efficace dans la lutte la criminalité*. *In observatoire des criminalités internationales*. Juillet, 2021.p.6. Disponível em:https://www.iris-france.org/wp-content/uploads/2021/07/Obs-Criminalit%C3%A9s-internationales-Juillet-2021.pdf. Acesso em: 25 mai 2023.

> a dados informáticos, registrá-los, armazená-los e transmiti-los, de modo a que sejam armazenados num sistema informático, como eles são exibidos em uma tela para o usuário de um sistema automatizado de processamento de dados, à medida que ele os introduz digitando caracteres ou à medida que são recebidos e transmitidos por periféricos.
> O Ministério Público ou o juiz de instrução pode designar qualquer pessoa singular ou coletiva autorizada e inscrita numa das listas previstas no artigo 157.º, para efetuar as operações técnicas que permitam a realização do dispositivo técnico referido no primeiro parágrafo deste artigo. O Ministério Público ou o Juiz de Instrução podem ainda prescrever a utilização de recursos do Estado sujeitos a segredo de defesa nacional, de acordo com as formas previstas no Capítulo I do Título IV do Livro I.

No ordenamento português, a infiltração policial é prevista na Lei nº 101/2001 intitulada como "*Acções Encobertas*" e estabelece o "Regime Jurídico das ações encobertas para fins de prevenção e investigação criminal", tratando da admissibilidade e dos requisitos para a utilização da técnica de investigação. Nos anos seguintes, houve mais duas alterações legislativas, sendo a mais recente a Lei nº 61/2015, que incluiu delitos que envolvem organizações terroristas, terrorismo, terrorismo internacional e financiamento do terrorismo.

A legislação portuguesa em seu art. 1º, alínea 2, traça um conceito sobre ações encobertas e a qualificação de quem tem legitimidade para atuar como agente: "*Consideram-se acções encobertas aquelas que sejam desenvolvidas por funcionários de investigação criminal ou por terceiro actuando sob o controle da Polícia Judiciária para prevenção ou repressão dos crimes indicados nesta lei, com ocultação da sua qualificação e identidade*"

A fim de se evitar descontextualizações, importa fazer uma observação acerca da "acções encobertas," título da legislação ora apresentada, e a figura do agente infiltrado. Está relativamente pacificado na doutrina portuguesa que o agente encoberto, nada mais é que uma subespécie do agente infiltrado; esta é a visão da maioria dos doutrinadores que nega a existência de uma distinção entre os dois, mas sim, uma relação de subespécie.

Alves Meireis (1999, p.192) entende que o conceito de polícia à paisana é o conceito que melhor se aplica à figura do agente encoberto, de forma que "O agente encoberto é, assim, um agente da autoridade, ou alguém que com ele actua de forma concertada, que sem revelar a sua identidade ou qualidade, frequenta os meios conotados com o crime na esperança de descobrir possíveis delinquentes; não provoca ao crime, nem conquista a confiança de ninguém. A sua presença e a sua qualidade é indiferente para determinar o rumo dos acontecimentos; naquele lugar e naquele momento poderia estar qualquer outra pessoa e as coisas aconteceriam da mesma forma; aqui o risco corre, no todo, por conta do delinquente".

Quanto ao legislador nomear a lei nº 101/2001 de "acções encobertas", segundo opina Oneto (2005, p.141) "*Parece que o legislador optou pela expressão "agente encoberto" ao invés de utilizar o termo "agente infiltrado", nela se incluindo a realidade que pode comportar as duas figuras*".

Feito esse recorte introdutório, poder-se-á analisar a legislação partindo da premissa que as duas figuras apresentadas fazem parte da mesma categoria, portanto sujeitas igualmente ao mesmo procedimento e regras.

A ação encoberta também delimita os tipos legais que se aplicam a técnica de infiltração, através da taxatividade do rol, apresentado no artigo 2º "âmbito de aplicação", que permeia desde o crime de homicídio até crimes relativos ao mercado de valores mobiliários. Por mais que o rol seja taxativo, a gama de crimes que permitem o uso das ações encobertas é vasto.

Quanto aos requisitos para o uso da técnica especial de investigação, estão delimitados no artigo 3º, alínea 1, da Lei 101/2001 que dispõe que a ações encobertas devem ser utilizadas para fins de prevenção e repressão de determinados crimes identificados, e com o objeto da "descoberta de material probatório", ainda cuidou de tratar sobre a questão da voluntariedade do agente infiltrado em querer participar da operação.

No que toca à legitimidade e competência, o inciso 3º disciplina que a ação encoberta no âmbito do inquérito depende de prévia autorização do Ministério Público, sendo obrigatória a comunicação ao juiz de instrução. Feita a comunicação ao Juiz de instrução, e se este não proferir um despacho de recusa da operação nas setenta e duas horas seguintes, a autorização estará automaticamente validada.

Do mesmo modo que a legislação espanhola e francesa, também estão assegurados ao agente encoberto que atuou na operação, o sigilo da identidade real, podendo o agente utilizar-se da identidade fictícia até o julgamento.

A duração da autorização da identidade fictícia é de 5 meses, um mês a mais que a autorização dada pela legislação francesa (quatro meses), e um mês a menos da autorização dada pela legislação espanhola (seis meses).

No artigo 6º da Lei 101/2001, trata sobre a isenção da responsabilidade penal do agente encoberto. De modo semelhante nas demais legislações até aqui abordadas, "O agente infiltrado ficará isento de responsabilidade criminal pelos atos que forem consequência necessária do desenvolvimento da investigação, desde que mantenham a devida proporcionalidade com o objeto da investigação, desde que não constituam provocação ao crime".

Quando da alteração legislativa dada pela Lei nº 61/2015, de 24 de junho sobre a possibilidade do uso da infiltração por meio virtual, a legislação portuguesa não disciplinou

sobre o tema, inserindo apenas a alínea "f", que trata da inserção dos crimes de "Organizações terroristas, terrorismo, terrorismo internacional e financiamento do terrorismo" no rol taxativo de crimes disciplinados no art. 4º da Lei 101/2001.

Entretanto, a legislação portuguesa inseriu o uso das "*acções encobertas*", através do art. 19º da Lei nº 109/2009, de 15 de setembro de 2009, que "Aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa". A medida foi adotada após Portugal tornar-se signatário da Convenção de Budapeste e inserir em seu ordenamento pátrio as normativas e diretrizes concebidas na Lei do Cibercrime, conforme disposição trazida:

> Artigo 19.º
> Acções encobertas
> 1- É admissível o recurso às acções encobertas previstas na Lei n.º 101/2001, de 25 de agosto, nos termos aí previstos, no decurso de inquérito relativo aos seguintes crimes:
> a) Os previstos na presente lei;
> b) Os cometidos por meio de um sistema informático, quando lhes corresponda, em abstrato, pena de prisão de máximo superior a 5 anos ou, ainda que a pena seja inferior, e sendo dolosos, os crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes, a burla qualificada, a burla informática e nas comunicações, a discriminação racial, religiosa ou sexual, as infracções econômico-financeiras, bem como os crimes consagrados no título iv do Código do Direito de Autor e dos Direitos Conexos.
> 2 - Sendo necessário o recurso a meios e dispositivos informáticos observam-se, naquilo que for aplicável, as regras previstas para a intercepção de comunicações.

Com a inserção do artigo acima referido, depreende-se que a lei de forma sucinta inseriu duas tratativas, a primeira versa sobre os crimes que admitem o uso da técnica investigativa, que são os previsto no rol taxativo da lei nº 101/2001 e todos que forem cometidos por meio de um sistema informático, cuja pena de prisão em abstrato seja superior a 5 (cinco) anos e inferior, no caso de crimes dolosos contra a liberdade e autodeterminação sexual. A segunda, dispõe sobre meios e dispositivos informáticos, de modo que diante da necessidade de busca por estes meios deverão ser respeitadas as regras atinentes à interceptação de comunicações.

Por fim, a previsão legal da infiltração ou ação encoberta na Argentina, é trazida pela *Ley* nº 27.319/16 "*Delitos Complejos: Investigación, Prevención y lucha de los delitos complejos. Herramientas. Facultades*", que tem por objetivo, além de delimitar os instrumentos e poderes necessários para a aplicação na investigação, como prevenção e combate aos crimes complexos, ainda cuidou de regular a figura dos agentes encobertos e agente revelador, bem

como o legislador destaca que a referida lei deverá ser aplicada sob a égide do princípio da necessidade, princípio da razoabilidade e proporcionalidade.

Quanto aos crimes que permitem a aplicação das técnicas investigativas, estes são taxativos e estão delimitados no artigo 2º, tais como: crimes de tráfico, infrações previstas no código aduaneiro, crimes que envolvem organização criminosa, etc.

Quanto à infiltração policial, o legislador argentino trouxe uma conceituação acerca da figura do agente infiltrado, que dispõe:

> Artigo 3º- Será considerado agente infiltrado todo funcionário autorizado e altamente qualificado das forças de segurança que der seu consentimento e ocultar sua identidade, se infiltrar ou introduzir em organizações criminosas ou associações criminosas, com o objetivo de identificar ou prender os autores, participantes ou corretivos, para impedir a consumação de crime, ou para colher informações e provas necessárias à investigação, com autorização judicial.

Portanto, o texto de lei restringe a atuação dos agentes infiltrados aos funcionários das forças de segurança, não se restringindo a apenas um órgão específico de polícia e sim a toda a segurança nacional. No mesmo artigo, deixa evidenciado o consentimento e voluntariedade do agente infiltrado em submeter-se à espécie de investigação, a importância da voluntariedade do agente infiltrado vem reforçada novamente no artigo 11º da referida lei.

Quanto aos objetivos, consiste em identificar e efetuar a prisão dos autores, participantes ou "encobridores", proceder a colheita de informações e de provas necessárias à investigação, e também com o objetivo de impedir a consumação do crime. De todas as legislações apresentadas, a legislação argentina foi a única que trouxe em seu texto como objetivo o uso da infiltração para impedir a consumação do crime.

No que toca a parte procedimental, a técnica de infiltração pode ser disposta pelo juiz de ofício ou a pedido do ministério Público, e o controle operacional fica a cargo do Ministério da Segurança da Nação, que se encarrega de promover a seleção e treinamento do agente designado.

Toda a informação colhida através da operação deve ser imediatamente levada ao conhecimento do Juiz e do representante do Ministério Público. No âmbito judicial, precisamente na fase de instrução processual, o agente infiltrado só deve prestar depoimento se este for absolutamente indispensável, e deverão ser utilizados meios técnicos necessários a fim de evitar a revelação da identidade real do agente.

O artigo 9º da legislação cuida da isenção da responsabilidade penal do agente infiltrado: "*Não será punido o agente infiltrado ou revelador que, como consequência necessária da prática do ato que lhe foi confiado, tenha sido compelido à prática de crime* (…)".

Na regulamentação que trata acerca da identidade real ou em respeito à nova identidade, prevê a punição de pena de prisão até 4 (quatro) a oito (8) anos e multa equivalente em pesos ao valor de seis (6) unidades fixas a oitenta e cinco (85) unidades fixas[43] e inabilitação absoluta perpétua, ao funcionário que indevidamente revelar a identidade real do agente infiltrado. Da mesma forma será punido com pena de prisão de 1 (um) a 3 (três) anos, e multa equivalente em pesos no valor de 4 (quatro) unidades fixas a 60 (sessenta) unidades fixas e inabilitação especial de 3 (três) a 10 (dez) anos, o funcionário que, por imprudência, negligência ou inobservância dos deveres que lhe competem, permitir ou oportunizar que outrem conheça tal informação.

No caso de ser revelada a identidade do agente infiltrado e a segurança pessoal do agente estiver ameaçada, a legislação lhe garante o direito em lei de permanecer na ativa ou aposentar-se, independentemente do número de anos de serviço.

Nesta perspectiva, é de se observar que, para o efetivo cumprimento do devido processo legal e respeito às demais garantias constitucionais, em todas as resoluções legislativas ora abordadas, têm-se o controle exercido pelo judiciário, a fim de se evitar prejuízos nas operações e consequentemente na colheita e comprovação de provas, em razão de descumprimento aos preceitos legais.

3.3 Evolução Legislativa Brasileira

A figura do agente infiltrado foi abordada no Brasil foi no Projeto de Lei nº 3.516/1989. proposta de lei foi vetada pelo Exmo. Sr. Presidente da República Fernando Henrique Cardoso de forma que, além de não cogitar a submissão da operação à autorização judicial, a subcomissão do projeto de lei também rejeitou a ideia de que a instituição em questão havia dado ao agente infiltrado permissão expressa para a prática de crimes, sob o argumento de que tal permissão violaria a separação de poderes, motivo pelo qual a figura do agente infiltrado sofreu o veto, sendo retirada através do referido veto presidencial. Posteriormente, fora introduzida no ordenamento brasileiro com a edição da Lei nº 10.217/01, apesar de ainda carecer de aperfeiçoamento técnico.

---

[43] A própria legislação indica que 1 (uma) unidade fixa equivale a 1 (um) salário-mínimo, vital e móvel atualizado a época da sentença.

Em que pese a inserção no texto legal do regulamento que tratava da submissão à autorização judicial, ainda restava ausente a regulamentação quanto ao instituto da antijuricidade, de forma que o legislador deixou que a questão eventualmente fosse tratada através da via doutrinária e jurisprudencial.

Importante ressaltar que não houve regulamentação quanto ao estabelecimento da antijuridicidade, apesar de ter sido inserida no texto legal a regulamentação que trata da submissão à autorização judicial. Com isso, o legislador deixou que a doutrina e a jurisprudência resolvessem a questão em definitivo.

Nesse contexto legislativo, a lei ainda era extremamente vaga em relação à organização criminosa e não continha nenhuma definição normativa do que constituía organização criminosa. Quanto ao instituto da infiltração policial, essas questões foram tratadas de maneira pouco técnica, com os requisitos autorizadores para a operacionalização desse tipo único de investigação ausentes. Omissão que só foi apenas suprida com a introdução da Lei das Organizações Criminosas, Lei nº 12.850/2013.

No ano de 2002, entrou em vigor a Lei de Drogas (Lei nº 10.409/2002) que em seu artigo 33, inciso I, introduz o uso da infiltração policial no contexto do tráfico ilícito de Drogas, e, futuramente revogada pela atual Lei de Drogas, promulgada no ano de 2006, com a Lei nº 11.343/2006, artigo 53, inciso I.

Ainda fora editada a Lei 12.694/2012 que dispunha sobre o processo e o julgamento do colegiado em primeiro grau de jurisdição de crimes praticados por organizações criminosas e trazia, em seu artigo 2º, um primeiro conceito de organizações criminosas que mais tarde foi modificado com a promulgação da Lei de organizações criminosas no ano subsequente[44].

Não se olvida que de fato havia questões importantes acerca de uma regulamentação jurídica melhor amparada tecnicamente, principalmente no que toca ao uso da técnica especial de investigação. Definições e conceituações de extrema importância que somente seriam inseridas e definidas com a entrada da Lei nº 12.850/13, em 02 de agosto de 2013.

No cenário apresentado, com o advento da Lei nº 12.850/13, havia duas opções para o uso da técnica especializada de investigação infiltrada: i) quando uma organização, associação ou quadrilha estivesse envolvida na investigação e ii) os crimes listados estejam contidos na Lei de Drogas.

---

[44] Art. 2º da Lei 12.694/2012. "Para os efeitos desta Lei, considera-se organização criminosa a associação, de 3 (três) ou mais pessoas, estruturalmente ordenada e caracterizada pela divisão de tarefas, ainda que informalmente, com objetivo de obter, direta ou indiretamente, vantagem de qualquer natureza, mediante a prática de crimes cuja pena máxima seja igual ou superior a 4 (quatro) anos ou que sejam de caráter transnacional".

Importa reconhecer o avanço que a novel legislativa angariou ao compensar as omissões que impediam de se aplicar o instituto da infiltração, com atenção à segurança e respeito às garantias constitucionais, por meio da normatização delineada nos artigos 3º e 10 a 14.

Quanto à legislação mencionada, poder-se-á abordar os seguintes aspectos introduzidos na novel legislativa: i) Trouxe um novo conceito de organização criminosa (artigo 1º, §1º); ii) fez a equiparação da lei quanto às infrações penais previstas em tratado ou convenção internacional (artigo 1º, §2º); iii) conceituou o tipo penal de organização criminosa (artigo 2º); iv) estatuiu os meios de obtenção de prova (artigo 3º); v) regimentou a infiltração policial (artigo 3º, inciso VII, e 10 a 14); vi) delimitou a responsabilidade penal do agente infiltrado (artigo 13 e parágrafo único), e por fim, vii) tipificou os crimes ocorridos na investigação e obtenção de prova.

Em que pese, a legislação ter trazido à lume aspectos que supriram lacunas importantes, ainda assim, no que toca a parte de conceituar o instituto da infiltração até então, quedou-se inerte, ficando à cargo da doutrina e jurisprudência fazê-lo de modo hermenêutico.

Com a promulgação da Lei nº 13.441/17, que introduziu a figura da infiltração policial na internet com o fim de investigar os crimes previstos no (ECA), Estatuto da Criança e do Adolescente, alterou-se, portanto, o ECA, promovendo na seção V-A, inserção dos artigos 190-A, 190-B, 190-C, 190-D e 190-E. O novel legislativo estava atrelado ao fato de normatizar pela primeira vez a técnica excepcional investigativa em meio cibernético.

Dessa forma, a Lei nº 12.850/13 é a que mais ampara a técnica de infiltração policial, e após a publicação da Lei nº 13.441/17 e, principalmente, com a chegada do "pacote anticrime" através reformulação advinda da Lei nº 13.964/2019, que inseriu na antiga lei de organizações criminosas (Lei nº 12.850/13) os artigos 10-A ao artigo 14, a figura dos "agentes de polícia infiltrados virtuais", e de forma cirúrgica, normatizou e delimitou tanto os procedimentos, quanto contextualizou a responsabilidade penal do agente infiltrado.

Por consequência, têm-se que a infiltração policial por meio virtual se aplica nos crimes previstos no artigo 1º, da Lei 12.850/13, por força da inserção do §2º, do artigo 10, da Lei 12.850/13, ao dispor "*Será admitida a infiltração se houver indícios de infração penal que trata o art.1º e se a prova não puder ser produzida por outros meios disponíveis*". Portanto, a reformulação dada em 2019 ampliou as infrações que admitem o uso da técnica investigativa por meio virtual, não se restringindo apenas aos crimes previstos no (ECA) Estatuto da Criança e do Adolescente (Lei nº 13.441/17), bem como aos crimes previstos nas leis nº 11.343/06 – Lei de Drogas em seu art. 53, inciso I, e demais crimes de relevância para a sociedade.

3.4 Conceito doutrinário da infiltração policial

Henrique Hoffmann (2017) descreve em artigo publicado que a infiltração policial:

> Consiste em técnica investigativa especial e subsidiária, qualificada pela atuação dissimulada (com ocultação da identidade real) e sigilosa de agente policial, presencialmente ou virtualmente, frente a um criminoso ou grupo de criminosos, com o objetivo de localizar fontes de provas, identificando criminosos e obtendo elementos de condenação para elucidar o crime e desarticular associação ou organização. Por fim, define que a infiltração policial é gênero, do qual são espécie a infiltração física e a infiltração virtual.

Outra definição trazida por Antonio Scarance Fernandes (2009, p.18), conceitua a infiltração policial como:

> O ingresso de alguém, em uma organização criminosa, ocultando sua identidade com o objetivo de identificar seus membros, especialmente aqueles que têm papéis mais significativos na estrutura da organização, com a finalidade de coletar evidências para fundamentar a organização. O fato de alguém penetrar na organização e agindo como se a ele pertencessem, permite-lhes compreender o seu funcionamento e possibilita o acesso a informações e dados pertinentes.

Para Armando Dias Ramos (2022, p.54), de acordo com a conceituação trazida pela doutrina portuguesa, têm-se por agente infiltrado "aquele que não se limitando a ocultar a sua verdadeira identidade consegue granjear no suspeito uma aproximação de confiança e kde prova sem incitar ou precipitar o *actus delitual*."

Para Higor Vinícius Nogueira Jorge (2018, p. 33) "a infiltração é técnica aplicada nas hipóteses em que o policial ingressa em determinada organização criminosa para obter informações de interesse da investigação criminal".

Ainda sobre conceituação de infiltração policial na doutrina portuguesa e que guarda semelhança com a definição trazida pelos autores brasileiros, Pereira (2015, p.390) ao delimitar e classificar a infiltração leciona que:

> O agente infiltrado pode ser classificado como "meio extraordinário de investigação de determinados crimes graves cuja prática é parte da atividade de uma organização criminosa, que consiste em integrar ou incorporar na estrutura da referida organização um policial, a quem, para tais fins, é atribuída identidade assumida ou fictícia, a fim de coletar, a partir desse cargo e dadas as dificuldades de fazê-lo pelos meios ordinários de investigação, informações e dados sobre os atos criminosos investigados, bem como outras que possam levar ao conhecimento da estrutura, membros, financiamento e funcionamento

> da organização criminosa que possam conduzir ao seu desmantelamento ou à sua ineficácia (tradução nossa)[45].

Por outra ótica, mais poética, Manuel Monteiro Guedes Valente (2009, p.170), refere-se ao agente infiltrado como aquele que:

> […] convive e partilha da intimidade do suspeito, tem acesso a informações familiares e pessoais que nunca teria se não ganhasse sua confiança, partilha a mesa da comida, partilha e acede à vida privada e familiar do suspeito. De sorte que, há uma relação forçada e eticamente repreendida, pois caso não fosse a finalidade da investigação criminal de um crime típico do crime organizado, por exemplo, corrupção, tráfico de droga, tráfico de armas, branqueamento de capitais […] aquele agente não teria acesso à pessoa e à sua família.

Para Wolff (2018, p.20), agente infiltrado é "aquele policial que, ocultando sua verdadeira identidade e função através do uso de cobertura fictícia, aproxima-se de suspeitos da prática de determinados crimes para fazer prova de sua ocorrência".

Na doutrina espanhola, Pereira (2016, p.316-317) com base em um argumento politico-criminal acerca da atuação do agente infiltrado considera que:

> visa enfrentar processos criminais graves com respeito às garantias constitucionais, especialmente em relação aos problemas colocados pelo crime organizado em matéria de drogas, tráfico ilícito de pessoas, substâncias ou animais, ou crimes em matéria de propriedade intelectual e industrial, entre outros. Justifica-se pela ineficácia das técnicas tradicionais de investigação no combate ao crime organizado, dada a dimensão internacional destas organizações, a abundância de recursos de que dispõem e a dificuldade de conhecer sua estrutura e funcionamento dado a opacidade e relativa descrição de suas atividades[46].

---

[45] No original: "*el agente encubierto o se puede catalogar como un medio extraordinario de investigación de determinados delitos graves cuya comisión se encuadra en la actividad de una organización criminal, que consiste en integrar o incorporar a la estructura de dicha organización a un funcionario de policía, a quien, a tales efectos, se le otorga una identidad supuesta o ficticia, para poder recabar, desde esa posición y ante las dificultades de hacerlo mediante los medios de investigación ordinarios, información y datos sobre los hechos delictivos investigados, así como otros que puedan conducir a conocer la estructura, integrantes, financiación y funcionamiento de la organización criminal que puedan conducir a su desmantelamiento o a lograr su inoperância.* (PEREIRA, Flávio Cardoso. *El agente infiltrado desde el punto de vista del garantismo procesal penal*. 2. ed. Curitiba: Juruá, 2016. p.390).

[46] "No texto original: *Téngase presente, además, que el argumento político-criminal es bastante significativo, puesto que la actuación del infiltrado tiene por objeto afrontar actuaciones criminales graves, con respecto a las garantías constitucionales, especialmente en lo relativo a problemas que plantea la delincuencia organizada en materia de drogas, tráficos ilícitos de personas, sustancias o animales, o delitos en materia de propiedad intelectual e industrial, entre otros. Se justifica por la ineficacia de las técnicas de investigación tradicionales en la lucha contra la criminalidad organizada, ante la dimensión internacional de estas organizaciones, la abundancia de recursos con*

E ainda de acordo com o Supremo Tribunal Federal Espanhol, conceitua a infiltração policial como "um procedimento investigativo que é realizado de forma anônima, sem revelar a identidade ou condição do policial para uma vez introduzido no ambiente criminal, poder descobrir os planos e assim abortá-los, bem como descobrir os autores do ato e conseguir sua prisão[47] (tradução nossa)".

Outro ponto importante acerca da infiltração policial é a distinção entre agente infiltrado e agente provocador, que segundo Sônia Brito (2016, p.94), é quando "*alguém (particular ou autoridade policial), de forma insidiosa, instiga o agente à prática do delito com o objetivo de prendê-lo em flagrante, ao mesmo tempo em que adota todas as providências para que o delito não se consuma*."

Wolff (2018, p.218) discorre sobre a diferença do agente infiltrado com à paisana, ao lecionar que:

> A diferença entre o agente infiltrado e o à paisana decorre do fato de o último não utilizar identidade fictícia. Sua conduta se caracteriza por uma postura de mera observação. O primeiro, por outro lado, atua ativamente para criar uma relação de confiança que lhe permita desvendar a prática de crime ou introduzir-se no universo de organização criminosa, para melhor entender seu funcionamento. Para alcançar tal desiderato, o agente infiltrado se utiliza do ardil, o que inocorre com o à paisana. Por essas diferenças, é imprescindível a autorização judicial apenas para a infiltração[48].

Apesar das principais objeções levantadas, é consenso de todos que o uso da infiltração como técnica investigativa especializada está relacionado com a investigação de diversos crimes de natureza grave, não apenas na legislação brasileira, mas também nos mais variados ordenamentos pátrios, tratado brevemente pelo direito comparado.

---

los que cuentan, y la dificultad de conocer su estructura y funcionamiento dado la opacidad y relativa discreción de sus actividades". (PEREIRA, Flávio Cardoso. *El agente infiltrado desde el punto de vista del garantismo procesal penal*/2ª Edição. Curitiba: Juruá, 2016, p.390).

[47] No texto original: "*El Tribunal Supremo español también ha conceptuado la infiltración de un agente encubierto policial como un procedimiento de investigación que se realiza de incógnito, sin revelar la identidad ni condición de policías con el fin de, una vez introducido en el ambiente criminal, poder conocer los planes y así abortarlos, y también para poder descubrir a los autores del hecho y procurar su detención*" PEREIRA, Flávio Cardoso. *El agente infiltrado desde el punto de vista del garantismo procesal penal*. Coimbra: Juruá Editorial, 2016, p.330.

[48] Vide. SILVA, Ângelo Roberto Ilha da; SHIMABUKURO, Adriana. et al. Crimes Cibernéticos. 2ª ed. De acordo com a Lei nº 13.441/17 (Lei de Infiltração Virtual) e a Lei nº 13.260/16 (Lei Antiterrorismo). Porto Alegre: Livraria do Advogado, 2018.

De outro lado, vale ressaltar, que o uso da técnica especial de investigação, por restringir direitos fundamentais, só deve ser usada como *última ratio*. E apesar disso, é necessária para combater uma criminalidade cada vez mais sofisticada tecnologicamente.

3.4.1 Agente Infiltrado e Agente Provocador

Segundo Oneto (2005), a recente autonomização conceitual do agente infiltrado, motivada pela necessidade político-criminal de sua consagração legal, demandou uma análise comparativa com o agente provocador, uma figura doutrinária que, devido à falta de tipificação legal, tem desfrutado de impunidade. Até a efetiva separação dogmática das duas figuras, a distinção entre elas era meramente nominal, referindo-se indiscriminadamente à mesma realidade, ambas historicamente designadas como "*agent provocateur*".

Essa origem comum tem suas raízes na literatura francesa e remonta ao período do *Ancien Régime*. Alves Meireis menciona que os "*primeiros agentes provocadores da história europeia*" foram contratados por inspetores da polícia parisiense no final do século XVIII. A polícia fazia uma distinção entre aqueles que trabalhavam secretamente, na clandestinidade, chamados eufemisticamente de "*observateurs*", e aqueles que eram contratados abertamente, denominados popularmente como "mouches", "sous-inspecteurs", "commis" ou "préposés" (Oneto, 2005).

Dentro dos contratados, "muitos são mesmo reclusos que negociam sua liberdade em troca de cooperação, especialmente através da infiltração em locais considerados 'perigosos'; outros, no entanto, vêm de níveis sociais mais elevados; tudo dependia do "*milieu*" onde o sub-inspetor deveria se infiltrar, facilitando assim o trabalho de seguir, escutar, informar, mas também de provocar e prender os criminosos sob vigilância".

Portanto, naquele tempo a figura do agente provocador condensava diferentes formas de intervenção: o agente poderia ser contratado para se infiltrar (agente infiltrado) ou ser pago para seguir, escutar e informar, bem como para provocar a comissão do crime (agente provocador), além daquele que negociava sua liberdade em troca de cooperação (informador).

Para a autora, outra dificuldade surgida na delimitação conceitual do "agente provocador" está relacionada ao fato de que, desde então, sua utilização ocorre tanto para fins de prevenção e repressão criminal quanto para fortalecer estratégias políticas de poder. Isso resulta em um conceito desmedidamente amplo para um contexto que se deseja regulamentado por critérios jurídico-criminais, dentro de um Estado de Direito (Oneto, 2005).

Merece destaque especial a opinião de Flávio Cardoso Pereira sobre a definição e consequência jurídica do agente provocador, que ao instigar ou induzir outra pessoa a cometer um crime com o propósito de prendê-la e levá-la à justiça, não tem a capacidade de invocar para si a possibilidade de suscitar uma causa de justificação, ao contrário do "agente secreto". Isso implica que o agente provocador, representado por uma pessoa física que busca induzir ou instigar o suspeito a cometer atos criminosos pelos quais será responsabilizado criminalmente, com o principal objetivo de obter provas que o incriminem, acaba por violar as garantias essenciais de um Estado de Direito social e democrático. Como resultado, essa forma de investigação policial enfrenta considerável rejeição tanto no âmbito jurídico quanto doutrinário e jurisprudencial (Pereira, 2016).

Como visto, o agente infiltrado recebe autorização judicial para se integrar a uma organização criminosa com o intuito de reunir informações que possibilitem desmantelar o grupo, sendo necessário que sua atuação seja predominantemente passiva, sem induzir os outros membros a cometerem qualquer delito.

Entretanto, se os agentes policiais ou de inteligência possuem evidências suficientes da presença de uma organização criminosa e decidem se infiltrar nela em busca de informações que possam revelar as diversas infrações cometidas por seus membros, não se pode alegar a ocorrência de crime impossível. Isso se deve ao fato de que a intenção de cometer delitos já estava firmemente estabelecida nos sujeitos que estavam praticando as infrações penais, por meio de uma decisão livre e anterior à intervenção do agente infiltrado (Lima, 2016).

Por outro lado, a ação do agente provocador ("*entrapment doctrine*" ou teoria da armadilha), comumente conduzida sem autorização judicial prévia, se configura pela indução de alguém a cometer um determinado ilícito, mesmo que essa pessoa não tivesse originalmente a intenção de fazê-lo. Nesse cenário, ocorre a violação do direito fundamental de não se autoincriminar e do direito à ampla defesa, comprometidos pela manipulação promovida pelo agente infiltrado.

Em conclusão, a principal distinção entre agente infiltrado e agente provocador se baseio no fato de o agente provocador ser um membro policial ou civil que induz ou provoca outrem a delinquir de forma a facilitar a recolha de provas da ocorrência do fato criminoso, e muitas com o fim de obter a prisão do agente. Enquanto o agente infiltrado limita-se a a alçar laços de confiança com o investigado a fim de colher informações, planos, confidencias e provas de autoria e materialidade.

3.5 Requisitos e Aspectos Operacionais

O cumprimento de determinados requisitos previstos nos artigos 10 e 11 da Lei das Organizações Criminosas, Lei nº 12.850/13, é de extrema importância para manter a legalidade da operação. O primeiro requisito mais importante é a autorização judicial que deve ser devidamente justificada, motivada e sigilosa, sendo de suma importância que a decisão decline os limites da operação.

Primeiramente, cumpre destacar que a própria legislação brasileira cuidou de separar o instituto da infiltração policial (art. 10) como gênero, da qual é espécie a infiltração policial virtual (art.10-A). Conforme redação dada aos artigos:

> Art. 10. A infiltração de agentes de polícia em tarefas de investigação, representada pelo delegado de polícia ou requerida pelo Ministério Público, após manifestação técnica do delegado de polícia quando solicitada no curso de inquérito policial, será precedida de circunstanciada, motivada e sigilosa autorização judicial, que estabelecerá seus limites.

Ao passo que admitiu a "ação de agentes de polícia infiltrados virtuais", dada pela seguinte redação:

> Art. 10-A. Será admitida a ação de agentes de polícia infiltrados virtuais, obedecidos os requisitos do caput do art. 10, na internet, com o fim de investigar os crimes previstos nesta Lei e a eles conexos, praticados por organizações criminosas, desde que demonstrada sua necessidade e indicados o alcance das tarefas dos policiais, os nomes ou apelidos das pessoas investigadas e, quando possível, os dados de conexão ou cadastrais que permitam a identificação dessas pessoas.

É de suma importância ressaltar a divisão – gênero e espécie –, feita no instituto, porque em determinados momentos a legislação prevê requisitos diferentes a ambos, como no caso da renovação do prazo de autorização do uso da técnica de investigação que difere um do outro.

Os institutos do *fumus comissi delecti* e do *periculum in mora* estão previstos nos artigos 10º, parágrafo 2º, art. 10-A, parágrafo 3º e art.11º, ambos da Lei 12.850/13, respectivamente. Isto significa que a infiltração depende da presença de indícios ou elementos incendiários dos crimes descritos no art. 1º, § 1º, da Lei 12.850 /13.

> Art. 10, § 2º. Será admitida a infiltração se houver indícios de infração penal de que trata o art. 1º desta Lei e se as provas não puderem ser produzidas por outros meios disponíveis

> Art.10-A, §3º. Será admitida a infiltração se houver indícios de infração penal de que trata o art. 1º desta Lei e se as provas não puderem ser produzidas por outros meios disponíveis.
> Art. 11. O requerimento do Ministério Público ou a representação do delegado de polícia para a infiltração de agentes conterão a demonstração da necessidade da medida, o alcance das tarefas dos agentes e, quando possível, os nomes ou apelidos das pessoas investigadas e o local da infiltração.

É parte fundamental destacar que os parágrafos 2º do artigo 10, e parágrafo §3º do artigo 10-A da legislação não menciona indícios de autoria, mas sim indícios de infração penal. Assim, a autoria será confirmada por meio do uso da infiltração policial, que auxiliará a identificar o *modus operandi* da organização criminosa, bem como de seus integrantes, finalizando com a verificação da autoria e identificação de membros.

Já o instituto do *periculum in mora,* encontra amparo legislativo no art. 11 da referida lei, ao impor a demonstração da necessidade da técnica investigativa através da infiltração. Essa necessidade mencionada refere-se ao risco ou dano potencial, em detrimento à persecução penal, se a infiltração não for realizada em tempo hábil.

No que toca a parte doutrinária e jurisprudencial, a indispensabilidade da infiltração ou comumente conhecida como a expressão *ultima ratio* é o requisito que assume a maior importância em ser preenchido a fim de manter a legalidade da técnica. Disciplinada na segunda parte do artigo 10, parágrafo 3º, a infiltração só será permitida quando não houver outros meios disponíveis para produzir a prova. O requisito para a admissibilidade da técnica investigativa decorre do princípio da proporcionalidade, que estabelece que o juiz deve primeiramente buscar medidas investigatórias que causem menor quantidade de restrições à liberdade pessoal do agente.

Quanto ao prazo de duração da infiltração, a legislação brasileira em cotejo com as legislações do direito comparado abordadas, é a que mais amplia o prazo de duração, que consiste no prazo de 6 (seis) meses, “sem prejuízo de eventuais renovações”, comprovada a necessidade da medida.

Quanto à renovação, a lei faz duas distinções, no que toca à quantidade de renovações permitidas. No art. 10, § 3º, a legislação não menciona o período ou quantidade de renovação permitida, o que pode implicar como um lapso do legislador, ou que o mesmo fez a supressão do tempo de renovação, de sorte que fica adstrito à discricionariedade do juiz. Ao contrário, no art.10-A que trata da infiltração policial virtual, o legislador permite a renovação do instituto, e delimita expressamente que a renovação não exceda à 720 (setecentos e vinte) dias.

Assim como demais ordenamentos jurídicos que citam a existência de relatório da infiltração, a legislação brasileira inseriu dois tipos de relatórios. O primeiro, trata de relatório circunstanciado, previsto nos art. 10, §4º e art. 10-A, §5º que deverá ser apresentado ao juiz competente e posteriormente deverá dar ciência ao Ministério Público. O segundo relatório chamado de "relatório da atividade de infiltração" em ambos os casos, refere-se à operação propriamente dita, com previsão nos art. 10, §5º e art.10-A, §6º.

Quanto ao relatório circunstanciado, segunda definição dada pelo texto legal, presume-se uma obrigação imposta, ao dispor "*findo o prazo previsto (...) os relatórios circunstanciados deverão/será apresentado ao juiz competente, que imediatamente cientificará o Ministério Público*". Em sentido inverso, a legislação tratou de modo diferente a respeito do "relatório de atividade de infiltração" disposto nos art. 10, §5º e art.10-A, § 6º, dos quais dispõem:

> Art.10, § 5º - No curso do inquérito policial, o delegado de polícia **poderá** determinar aos seus agentes, e o Ministério Público **poderá** requisitar, a qualquer tempo, relatório da atividade de infiltração (grifo nosso).
> Art.10-A - § 6º - No curso do inquérito policial, o delegado de polícia **poderá** determinar aos seus agentes, e o Ministério Público e o juiz competente **poderão** requisitar, a qualquer tempo, relatório da atividade de infiltração (grifo nosso).

Infere-se de ambos os textos legais a expressão "poderá" ou "poderão", de forma que o legislador deixou claro a faculdade dos legitimados a solicitação do relatório, por determinação feita pelo Delegado de Polícia, ou por requisição feita pelo juiz ou Ministério Público do "relatório de atividade de infiltração" ao agente infiltrado. Entretanto, a legislação não especificou detalhes de como seria a apresentação desse relatório, limitando-se apenas a especificar o registro, gravação e armazenamento dos atos eletrônicos praticados no âmbito da infiltração por meio virtual.

Outra diferença dada pela legislação é quanto aos legitimados, enquanto no art. 10, §5º, a lei deixa claro que quem pode determinar ou requisitar a apresentação do relatório é apenas o delegado de polícia e o ministério publico, no art. 10-A, §6º, o legislador incluiu o juiz como legitimado a requisitar o relatório de atividade de infiltração.

Quanto ao procedimento, previsto no art.12, o pedido de infiltração deve ser distribuído sigilosamente, omitindo informações que possam indicar a operação ou que identifique o agente infiltrado. Contudo, as informações a respeito da necessidade da operação de infiltração deverão ser dirigidas diretamente ao juiz competente, que decidirá no prazo de 24 (vinte e quatro) horas, após manifestação do Ministério Público, se o pedido for feito por representação

do delegado de polícia, guardando as medidas necessária para o êxito das investigações e a segurança pessoal do agente infiltrado nos termos do parágrafo 1º, do art.12.

O paragrafo 1º, do art.12, trata do trâmite do pedido de infiltração feito pelo delegado de polícia, mas quedou-se inerte, quanto ao procedimento quando versar o pedido de infiltração a partir de requisição feita pelo Ministério Público, lacuna que pode ser preenchida com subsunção à norma prevista no art.10, da referida legislação "*A infiltração de agentes de polícia em tarefas de investigação, representada pelo delegado de polícia ou requerida pelo Ministério Público, após manifestação técnica do delegado de polícia quando solicitada no curso de inquérito policial* (…)". Do exposto, o Ministério Público deve requisitar o pedido de infiltração ao juiz competente, atendendo os requisitos do art. 12 *caput* e art. 12, §1º, e após a manifestação técnica do delegado de polícia, o juiz decidirá no prazo estabelecido pela lei de 24 (vinte e quatro) horas.

Posteriormente, nos termos do artigo 14, inciso I, da Lei nº 12.850, têm-se a exigência da anuência do agente policial. Importante notar que este requisito se refere especificamente aos direitos inerentes ao agente, antes de qualquer outra coisa, de forma que a recusa ou decisão de interromper o trabalho a qualquer momento não configura desobediência e nem chega perto de uma violação dos deveres funcionais.

Ainda, o pacote anticrime inclui na lei de organização criminosa a ocultação de identidade do policial (art. 10-C), para uso na operação de infiltração policial e no parágrafo único discorreu sobre a obrigação do agente policial se ater a estrita finalidade da operação, respondendo pelos excessos praticados (art.10-C, parágrafo único).

Por último, mas não menos importante, a lei trata a respeito da proporcionalidade e da excludente de responsabilidade penal do agente infiltrado. A proporcionalidade está inserida na previsão estabelecida pelo art.13 *caput*, nos seguintes dizeres: "*O agente que não guardar, em sua atuação, a devida proporcionalidade com a finalidade da investigação, responderá pelos excessos praticados*". E no parágrafo único, o legislador prevê a excludente da responsabilidade penal do agente que no âmbito da infiltração pratica crime no curso da investigação, quando inexigível conduta diversa está amparado pela excludente de punibilidade.

Em seu aspecto operacional, principalmente no que toca a infiltração policial virtual, preleciona Stanguerlin e Petean (2021, p. 50):

> Frisa-se que a infiltração exige uma adequada e devida preparação por parte do agente, especialmente na modalidade virtual, na qual o indivíduo deverá possuir o domínio da ciência da computação, o conhecimento de softwares e outras técnicas essenciais para o sucesso na investigação. Dessa maneira, se

> não estiverem presentes agentes de polícia judiciária aptos para tal tarefa, o procedimento não deverá se desenvolver, porque ocorrerá o risco de comprometer a produção de informações visando ao correto exercício do direito de punir pertencente ao Estado.

Quanto sua modalidade, a infiltração policial pode ser dividida em duas modalidades, a *light cover* e *deep cover*, permitidas pela Lei de Organizações Criminosas. A *light cover,* ou infiltração leve, requer envolvimento mínimo do agente e não dura mais de seis meses; já a *deep cover,* ou infiltração profunda, dura mais de seis meses e envolve a imersão completa no ambiente da organização criminosa, sem manter qualquer comunicação externa.

3.6 Ambiente de atuação da infiltração policial

Em meio à Guerra Fria, os americanos criaram a internet para se proteger e agilizar as trocas de informações que, em caso de ataques nucleares, a comunicação efetiva seria essencial para a sobrevivência do país.

O escritor *Manuel Castells* (2003, p.13) define o período de início, criação e desenvolvimento como:

> As origens da internet podem ser encontradas na Arpanet, uma rede de computadores montada pela Advanced Research Projects Agency (ARPA) em setembro de 1969. A ARPA foi formada em 1958 pelo Departamento de Defesa dos Estados Unidos com a missão de mobilizar recursos de pesquisa, particularmente do mundo universitário, com o objetivo de alcançar superioridade tecnológica militar em relação à União Soviética na esteira do lançamento do primeiro Sputnik em 1957.

Mais tarde, no ano de 1974, engenheiros da ARPANET começaram a delinear um projeto para solucionar o problema decorrente da proliferação de redes de comunicação com protocolos diferentes. O programa desenhado foi chamado de "*Internet Transmission Control Program"* (Programa de Controle de Transmissão Entre Redes), que se tornou o precursor do TCP/IP (*Transfer Control Protocol – Internet Protocol*), conhecido atualmente.

Segundo explica Santos e Barreto (2019, p. 2):

> Em 1981, a especificação TCP/IP foi finalizada, publicada e adotada pelos diferentes tipos de redes de computadores. E em 1982, as conexões da ARPANET, já utilizando o protocolo TCP/IP, avançaram além do solo estadunidense, dando origem à internet. Todavia, a partir de 1989 que a internet tomou a forma que hoje conhecemos.

No cenário brasileiro, a internet surgiu em 1995, ano em que o Ministério das Comunicações e Ciência e Tecnologia, por portaria, cunhou o conceito de “provedor privado de acesso à internet” e consentiu a operação comercial da rede no Brasil. A partir deste momento, um processo de inclusão tem-se estabelecido, ainda que paulatinamente, mas acelerado significativamente nos últimos anos (Viana, 2014, p.127).

Embora a internet tenha sido desenvolvida com o intuito de facilitar e ampliar a comunicação, ela evoluiu e adquiriu novas características, algumas das quais, em particular, a tornaram um ambiente fecundo e inovador para as mais diversas atividades criminosas.

Nesse sentido, temos o uso da *surface web*, que envolve indexadores de pesquisa universais aproveitados por todos os cidadãos. Conjuntamente a *deep web*, que consiste em páginas que só podem ser acessadas por meio dos mecanismos de busca adequados e possuem uma série de ferramentas que dificultam o acesso, foi desenvolvido com a intenção de manter o anonimato durante pesquisa em atividades militares e governamentais.

Portanto, a *dark web*, que usa a criptografia como principal aliada, é atualmente o maior obstáculo para que as autoridades identifiquem condutas criminosas e seus agentes. A *dark web* é um ambiente ainda mais misterioso e profundo, em razão da segurança no sigilo e integridade das informações, bem como da autenticação de usuários, remetentes e destinatários, a *dark web* é um ambiente ainda mais misterioso e profundo.

3.6.1 *Surface web*, *Deep web* e *Darknet*

Segundo conceito trazido por Barreto e Silva (2019, p.06) A *surface web* é composta por páginas, sites e conteúdos que utilizam a arquitetura de redes cliente-servidor e fazem uso de computadores "especializados" que são responsáveis por prover serviços aos seus usuários. Essas máquinas hospedam páginas web, serviços de e-mail, bancos de dados, documentos e diversos serviços que pessoas e empresas usam diariamente.

Já o conceito de *deep web*, tem origem desde a década de 90, conhecida anteriormente pela expressão de “rede escondida” (*hidden web)*. De forma similar, no ano de 1994, foi utilizada a expressão “rede invisível” pelo Dr. *Jill Ellsworth*, referindo-se ao conteúdo invisível de informação para os mecanismos de busca convencionais (Barreto; Santos, 2019, p. 6).

Para os autores a definição de *deep web* baseia-se em:

> […] redes de computadores que têm como características o anonimato, a criptografia, a descentralização e a codificação aberta, e cujo conteúdo não é

> visível pelas ferramentas de busca convencionais. A arquitetura de redes predominantes é a ponto a ponto (P2P), ou seja, dispensa um servidor central, cenário no qual todos os componentes (pontos ou nós) funcionam ora como cliente, ora como servidor.

Conforme apresentado, a *deep web* é composta de quatro características ou requisitos que a definem (descentralização, anonimato, criptografia, codificação-aberta). A título de exemplo, temos a rede *Tor*, que guarda as quatro características acima listadas, bem como, as redes utilizadas para *download* de arquivos como o *torrents*, que mesmo apresentando apenas uma ou outra característica, deve ser classificada como deep web, ou nomeadas como "redes descentralizadas", mas não enquadradas no âmbito da *surface web*, uma vez que seus conteúdos, além de não estarem indexados na *surface web*, a principal característica da *torrents* é a descentralização.

Quanto à *dark web* ou *darknet*, é a rede da *deep web* que constitui as seguintes características, apresentada pelos autores (Barreto; Santos, 2019, p. 8):

> A *dark web*, ou darknet, é a rede da *deep web* ou parte dela com características de um alto grau de anonimato e segurança exigido e é utilizada, como regra, para o cometimento de ilícitos criminais e práticas escusas. É empregada por usuários da internet, ativistas políticos, hackers e criminosos, notadamente por garantir a privacidade nas comunicações e/ou a não aplicação da lei penal.

O conceito de *dark web* não se restringe apenas sobre o conteúdo obscuro, ilícito e imoral, mas também, leva em consideração o alto grau de segurança e anonimato. Uma rede que serve para ilustrar o conceito de *dark web*, é a rede *Freenet*, que só é acessada por usuários de confiança através de convite para integrar à "comunidade" da rede.

3.6.2 Características da *Deep Web*

A arquitetura de rede principal da *deep web* é a ponto a ponto (P2P), isto é, descentralizada, pois um servidor central não é necessário. Os componentes (sejam eles pontos ou nós) trabalham juntos para estabelecer um verdadeiro canal de comunicação bidirecional.

Para ilustrar como acontece a transmissão de um arquivo, no decorrer da transmissão cada nó pode prover porções menores de um arquivo; no entanto, ao final, a transmissão do arquivo será montada e apresentado em sua totalidade. Ao longo da transmissão; no entanto, caso um dos nós se desconecta da rede como resultado dessa transferência, a solicitação do ponto receberá a parte que falta de outro que nó que esteja conectado à rede. Esse tipo de

funcionalidade é normalmente usado por redes ponto a ponto de compartilhamento de arquivos e documentos.

Quanto às características mencionadas, os autores Barreto e Santos (2019, p. 10) definem as principais:

> a) Anonimato: O objetivo principal da utilização de redes cujo conteúdo não é indexado na Surface Web é proporcionar anonimato a seus usuários. Nesse cenário, podemos destacar: pessoas comuns em busca de conteúdo com garantia de privacidade; blogueiros, ativistas e jornalistas, para a publicação de suas opiniões, ideias, críticas e denúncias, principalmente em regiões do globo onde a censura governamental, política e de grupos extremistas não permite que certos conteúdos sejam levados ao conhecimento das pessoas de outros países, além dos criminosos que buscam meios para não serem alcançados pela aplicação da lei penal.
>
> b) Segurança: essa peculiaridade decorre da conexão criptografada entre os nós componentes da rede. No *handshake*, ou seja, durante o fechamento da conexão entre os nós componentes da rede, é criado um canal de comunicação (túnel) criptografado ponto a ponto. Por conseguinte, mesmo que os pacotes sejam interceptados em algum momento da conexão, permanecerão cifrados totalmente ilegíveis para aqueles que estão tentando identificar o conteúdo daquela comunicação.
>
> c) Código aberto: relaciona-se com o poder de mutação e constante melhoramento dos mecanismos de anonimato e segurança das redes que operam na *deep web*. Um software de código aberto ou Open source ou software é aquele que pode ser manipulado por um usuário/programador de forma a eliminar suas vulnerabilidades e/ou problemas e propor novas funcionalidades e melhoramentos, a fim de beneficiar a comunidade de usuários. Essa característica não é peculiar apenas de redes que operam na *Deep Web*, sendo muito utilizada por programadores de software da *Surface Web*, principalmente aqueles utilizadores de sistemas operacionais baseados em Linux.

Logo, a doutrina de escol balizou-se por essas quatro características para classificar uma rede no "conceito de *deep web*": descentralização, anonimato, segurança e código aberto.

3.6.3 Rede *Tor* e Rede *Freenet*

Segundo definição dada pela *Eletronic Frontier Foundation*[49] a conceituação da rede Tor é:

[49] No original: *Tor is free software and an open network that helps you to circumvent Internet censorship and aids in protecting your anonymity online. The Tor network provides the foundation for a range of applications that allow organizations and individuals to share information over public networks without compromising their privacy.* ELETRONIC FRONTIR FOUNDATION. How to

> Tor é um *software* livre e uma rede aberta que ajuda você a contornar a censura na Internet e auxilia na protegendo seu anonimato online. A rede Tor fornece a base para uma variedade de aplicações que permitem que organizações e indivíduos compartilhem informações em redes públicas sem comprometer sua privacidade (tradução nossa).

Quanto ao procedimento para acesso da rede, Barreto e Santos (2019, p.14-15) descrevem:

> O acesso a ela é realizado através do navegador de mesmo nome e seu funcionamento é totalmente descentralizado, por meio da criação de um circuito formado, por padrão, de três relés/nós (clientes Tor) escolhidos aleatoriamente e distribuídos ao redor do mundo, os quais se comunicam, ponto a ponto através de um túnel criptografado. Cada nó só conhece o conteúdo dos pacotes de seus vizinhos imediatos; caso um pacote seja interceptado, a criptografia garantirá o princípio da segurança. O protocolo de internet requisitante de uma página web será sempre do último nó (o relé de saída), e não do usuário que de fato solicitou a página, o que garante, assim, o princípio do anonimato.
>
> Os usuários se interligam através de uma série de túneis virtuais, semelhante a uma VPN, diferentemente da navegação convencional, em que o cliente deve se conectar diretamente a um servidor (a chamada arquitetura cliente/servidor, já que permite a organizações e a indivíduos capturar e compartilhar informações dos usuários). Na rede Tor, por sua vez, a arquitetura cliente/servidor não se configura, em razão da navegação anônima, ainda que o acesso a sites tenha ocorrido através de redes públicas.

Quanto a rede *Freenet* também é uma rede ponto a ponto que funciona por meio de conexões fechadas através de nós, sem a presença de servidores centralizados. Barreto e Santos (2019, p.32) detalham melhor a sua arquitetura:

> A Freenet é uma rede de arquitetura ponto a ponto (P2P) projetada especificamente para atuar na *deep web* e que tem como objetivo principal prover anonimato e segurança a seus usuários, permitindo uma comunicação sem censura. Diferentemente da rede Tor, a *Freenet* não possui um navegador próprio. Para utilizá-la, o internauta deve instalar o software Freenet, programa que funciona casado com um *browser* da preferência do usuário (*Chrome*, *Firefox*, etc.).
>
> Quando da instalação, deve-se indicar uma porção do *hard disk* (disco rígido) que servirá aos demais componentes dessa rede no armazenamento de conteúdos. A totalidade das informações e dos dados contidos na rede *Freenet* instalada pode ser, assim, totalmente criptografada. Além disso, essa rede possui um cliente P2P chamado *Frost*, o qual possibilita aos usuários o compartilhamento de arquivos, assim como na *BitTorrent*, porém de forma

---

help protect your online anonymity using tor. Disponível em: https://www.eff.org/files/filenode/basic_tor_intro_guide_fnl.pdf. Acesso em 13 jun 2023.

> totalmente anônima. Seus principais diretórios de *links* são: *EnzoHidex* e *Nerdageddon*.

Comparando a rede *Freenet* e a rede Tor, ressalta-se uma distinção entre ambas, de forma que a rede Tor é composta por três nós para a obtenção de uma requisição ou resposta de conteúdo, e ser o*utproxy*, o que significa dizer, que a rede permite seu uso na *surface web*. Ao contrário da rede *Freenet*, cujos conteúdos percorrem um circuito sem número de nós definidos de modo que, quanto maior o número de nós, melhor é a sua funcionalidade, principalmente no que diz respeito à velocidade da resposta da rede. E diferentemente, da rede *Tor*, a rede *Freenet* é *inproxy*, isto significa que a rede não permite nenhum acesso de forma externa, devendo o usuário ser primeiramente "parte dela" para posteriormente, poder acessá-la.

3.6.4 Os crimes digitais na *Deep Web*

Conforme mencionado, em virtude dos avanços tecnológicos e a propagação da internet de modo geral, o ambiente virtual se caracteriza como um vasto e fértil terreno para o cometimento de crimes dos mais variados tipos, cometidos por quaisquer indivíduos que se julgam com a expertise e habilidades suficientes para esquivar-se dos olhos da justiça, acreditando estarem abarcados sob o manto do anonimato.

Há um dissenso tanto na doutrina quanto no meio acadêmico acerca da conceituação de crimes digitais, não existindo uma terminologia pacificada. Alguns autores denominam os crimes praticados por meio da rede mundial de computadores com a terminologia de "delitos informáticos", como por exemplo, denominação adotada por Rossini (2004, p. 110); por outro lado, Gouvêia (1997, p.54) adota a denominação de "crimes por meio da informática", de forma que o computador se caracteriza como o único meio para a prática dos crimes. Outra denominação apontada refere-se ao termo de "crime informático", terminologia adotada por Sydow (2015, p.55).

Entretanto, algumas dessas denominações ou terminologias acabam limitando o próprio conceito de crimes digitais atrelado ao uso de um computador especificamente. O que, na prática, tal denominação não convém, em razão de o cometimento de crimes praticados por meio da rede mundial de computadores não prescindir de um computador, podendo existir outros meios que sirvam de instrumentalização, de modo que há crimes praticados por meio de computador e crimes praticados contra o computador.

Nesse sentido, Furlaneto Neto e Santos (2018, p.28) citando Luiz Flávio Gomes (2000) destaca:

> Como fator criminógeno, há delitos cometidos por meio do computador (*the computer as a tool of a crime*) e outros contra o computador (*the computer as the object of a crime*), isto é, os cometidos contra "as informações e programas nele contidos". Assim, a informática seria meio para a prática de novas condutas delituosas, como potencializaria crimes tradicionais, já previstos na legislação em vigor, citando, como exemplo, o estelionato e o furto mediante a fraude.

Por outro lado, de forma mais ampla, Marcelo Xavier de Freitas Crespo, em artigo publicado, define de forma menos limitada ao conceituar crimes digitais como:

> crimes digitais são tanto os crimes tradicionais, já previstos na legislação, contra os valores que tradicionalmente reconhecemos como merecedores de proteção, praticados com auxílio da mais moderna tecnologia, bem como as condutas ilícitas passíveis de penas que se voltem contra os sistemas informatizados e os dados (CRESPO, 2015).

Portanto, hodiernamente, não há uma terminologia pacificada e majoritária acerca de uma conceituação sobre os crimes praticados pela internet, conforme ressalta Santos (2014, p. 237):

> Como se pode perceber, não existe um único conceito definitivo para o que seja um crime praticado pela Internet, ou um cibercrime. Alguns apresentam um conceito amplo, abrangendo qualquer conduta que implica o uso da tecnologia informática, enquanto outros de forma mais específica entendem ser a criminalidade desse tipo apenas aquela que envolve um computador.

Enquanto no campo da conceituação há significativa discordância, no campo que concerne aos crimes praticados por meio da internet há uma uniformidade. De forma que há certos tipos de crimes que são mais usuais de serem praticados por meio da internet: violação de direitos autorais; crimes contra a honra, como calúnia, difamação e injúria; crimes de ameaça; invasão de dispositivo informático; furto e furto mediante fraude praticado por meio da internet; estelionato; extorsão e muitos outros crimes mais graves e prejudiciais para a sociedade com um todo, cometidos, principalmente, através do uso da *deep web*, tais como, o tráfico de drogas, tráfico de armas; abuso e exploração sexual infantil; os chamados *black markets* (mercado negro) de produtos ilegais e falsificados, dentre outros.

3.7 Responsabilidade Penal do agente infiltrado, Proporcionalidade e Limites de atuação

Partindo do conceito apresentado de infiltração policial, conclui-se que a infiltração visa a inserção de agente policial, altamente treinado seja em ambiente físico ou digital, objetivando a colheita de indícios de autoria e materialidade. Utilizando-se de uma identidade falsa, e, não se limitando apenas em ocultar a sua verdadeira imagem, vai além, ao granjear junto ao suspeito uma aproximação de laços de confiança e solidariedade.

Isto posto, é impossível que o agente infiltrado não cometa crimes para garantir tanto o sucesso da infiltração e a sua viabilidade, como para garantir sua segurança física a fim de cumprir com o seu intento. De modo que para alçar laços de confiança junto ao suspeito, em determinados momentos, é apresentado ao policial infiltrado situações em que este deve cometer o ilícito penal para conquistar a confiança e garantir o prosseguimento e sucesso da operação de infiltração.

Resta evidente, que existe uma disputa entre valores, com a eficiência e eficácia da investigação e da persecução penal de um lado, e a moralidade e a legalidade dos métodos de investigação adotados pelo Estado de outro. Tanto no Brasil quanto na maioria do mundo, a ponderação desses valores resultou na escolha da eficácia estatal, permitindo o uso de agentes infiltrados, especialmente por razões de política criminal, devido ao aumento significativo da criminalidade organizada e dos delitos cometidos na Internet.

Dessa forma, a necessidade de o agente infiltrado cometer ou participar na prática de delitos é clara, seja para viabilizar a própria infiltração, seja para assegurar tanto sua continuidade e êxito quanto sua segurança pessoal. Tornando-se crucial definir a possibilidade de exclusão da responsabilidade desse agente pelos crimes cometidos.

Portanto, um agente que se infiltra fisicamente numa determinada organização criminosa, é instado a cometer atos de traficância, por exemplo, cometendo o crime previsto no art. 33, da Lei 11.343/2006 (Brasil, 2006) que criminaliza: "*Importar, exportar, remeter, preparar, produzir, fabricar, adquirir, vender, expor à venda, oferecer, ter em depósito, transportar, trazer consigo, guardar, prescrever, ministrar, entregar a consumo ou fornecer drogas, ainda que gratuitamente, sem autorização ou em desacordo com determinação legal ou regulamenta"*, não deve ser responsabilizado, em razão de que a sua conduta foi necessária para garantir a confiança do investigado e o sucesso da operação.

Do mesmo modo, não deve sofrer responsabilização penal um agente que se infiltra no âmbito virtual, principalmente, na *deep web*, se caracterizando por um pedófilo, deve provar

que faz parte daquele meio, e para isso, fornecer, compartilhar e armazenar conteúdos de pornografia infantil, incindido assim, no crime previsto no art. 241, do Estatuto da Criança e do Adolescente (Brasil, 1999), que criminaliza a conduta de: "*Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente*". Sem esquecermos que ainda deve o policial, antes de tudo, ser visto como um membro aceito e ativo nas comunidades da *dark web*.

Em vista disso, a legislação não foi omissa e procurou regulamentar a exclusão da responsabilidade penal do agente infiltrado, e o respeito da proporcionalidade, promovendo inserção de ambos nas legislações especiais que tratam do assunto.

Em primeiro lugar, conforme anteriormente já dito, sabe-se que a utilização da técnica de investigação de infiltração de agentes necessita da observação dos requisitos autorizadores para adoção da medida, dos quais, um deles refere-se ao requisito da autorização judicial prévia, que deve estabelecer os limites da atuação do agente infiltrado. Isso inclui a descrição dos métodos investigativos que podem ser empregados, como por exemplo, constar autorizado a gravação ambiental ou escuta telefônica do investigado, bem como a especificação dos delitos que o agente pode cometer para facilitar a investigação, sem ser responsabilizado por eles.

No entanto, é impraticável para o magistrado antecipar todas as situações que possam surgir durante a infiltração, razão pela qual as leis pertinentes exigem a responsabilização do agente caso ele não atue conforme a autorização recebida, e com o objetivo estrito da investigação guardando a devida proporcionalidade, bem como os limites de atuação.

Ao se imiscuir no terreno que versa sobre a excludente de responsabilidade penal do agente infiltrado, se torna necessário apresentar o tema sob duas perspectivas, a primeira trata-se de um recorte sobre as quatro correntes doutrinárias estabelecidas na doutrina de escol que versam sobre o assunto, e a segunda aborda as disposições legislativas pátrias que positivaram a excludente de responsabilidade penal do instituto no ordenamento pátrio.

Em sede doutrinária importa mencionar que existem quatro abordagens na doutrina nacional em relação à natureza jurídica dessa exclusão, abrangendo a escusa absolutória com base na política criminal; a atipicidade da ação por falta de dolo; a excludente de ilicitude pelo estrito cumprimento do dever legal e a causa supralegal de exclusão da culpabilidade por inexigência de conduta diversa.

A corrente doutrinária que propõe a exclusão da responsabilidade do agente infiltrado, com base na ideia de escusa absolutória, argumenta que o agente infiltrado não será

responsabilizado por eventuais delitos cometidos durante a infiltração como uma escolha de política criminal, representando uma causa pessoal para a exclusão da aplicação da pena. É importante notar que a escusa absolutória não elimina a tipicidade ou a ilicitude do ato, nem a culpabilidade do indivíduo, mas apenas impede o julgamento de reprovação pessoal daquele agente que cometeu o delito, conforme delineado por Sales (1993).

Nesse sentido, a justificativa para a atuação do agente infiltrado implicaria a impunidade de um eventual delito por ele praticado. No caso de o delito ser cometido em conjunto com os investigados, a escusa absolutória se aplicaria apenas a ele, sem se estender às condições pessoais dos demais indivíduos que participaram na prática do delito.

Por outro lado, a perspectiva que se baseia na ideia de atipicidade da conduta por falta de dolo fundamenta-se na compreensão de que, para que uma ação seja típica, não basta que ela esteja prevista como tal no ordenamento jurídico. Em outras palavras, a tipicidade formal da conduta não é suficiente, sendo necessário analisar também a tipicidade material, baseada no princípio da lesividade ao bem jurídico protegido, e a antinormatividade da conduta. Nesse contexto, considerando que o agente não age com a intenção de cometer o delito, mas sim com o objetivo de fomentar investigações, angariar laços de confiança a fim de garantir a persecução penal dos investigados, de modo que a tipicidade penal ficaria descaracterizada devido à ausência de imputação subjetiva, ou seja, diante da ausência de dolo.

No que toca a corrente doutrinária que defende a exclusão da responsabilidade penal com base na excludente de ilicitude do estrito cumprimento do dever legal argumenta que, quando o agente infiltrado comete um delito para facilitar a infiltração ou que seja crucial para o êxito da operação, desde que esteja agindo conforme a autorização recebida e dentro dos limites da proporcionalidade, está cumprindo uma obrigação estabelecida por lei, ou seja, a de investigar crimes, tornando sua conduta não ilícita.

Para essa corrente, a autorização judicial concedida para a utilização da infiltração de agentes constitui uma cláusula geral que exclui a ilicitude das ações do agente, desde que sua atuação esteja relacionada com a atividade de infiltração e respeite os princípios da proporcionalidade, legalidade e os direitos fundamentais dos investigados.

Quanta a última corrente apresentada, argumenta pela exclusão da culpabilidade do agente policial infiltrado pela inexigibilidade de conduta diversa, descaracterizando o delito. Para essa corrente, o agente infiltrado se enquadra em uma causa supralegal de excludente de culpabilidade, uma vez que se encontra em uma situação extraordinária, na qual é obrigado a cometer delitos não apenas para ganhar a confiança dos investigados e, assim, viabilizar a infiltração, mas também para garantir o sucesso da operação e sua própria incolumidade física.

No que toca às disposições legislativas, o *caput* do art.13 da Lei 12.850/13 dispõe que: "*o agente que não guardar, em sua atuação, a devida proporcionalidade com a finalidade da investigação, responderá pelos excessos praticados*". Infere-se da leitura que o dispositivo contempla a responsabilização do agente quando não guardar a devida proporcionalidade e a finalidade da investigação em sua atuação, deduz-se que, caso ele cometa um delito que não esteja relacionado com a investigação em andamento, que não seja essencial para o êxito da operação, ou cujo dano ou risco causado por ele seja excessivo em relação àquele que se procura proteger, será responsabilizado.

Já o parágrafo único desse dispositivo especifica que: "*Não é punível, no âmbito da infiltração, a prática de crime pelo agente infiltrado no curso da investigação, quando inexigível conduta diversa*". Portanto, constata-se da leitura do dispositivo que no contexto da infiltração, o cometimento de crime pelo agente infiltrado durante a investigação não será passível de punição, desde que seja inexigível conduta diversa. Dessa forma, fica claro, que o legislador adotou o entendimento de que a exclusão da responsabilidade do agente infiltrado possui natureza jurídica de causa supralegal de excludente de culpabilidade.

Nesse sentido, quando o agente é instado ou induzido a praticar determinado ato ilícito, de modo que se o não fizer colocaria em prejuízo a eficácia e sucesso da infiltração, não deve ser responsabilizado, uma vez que não poderia exigir deste outra conduta diferente. Entretanto, quando o delito for cometido em conluio com os demais investigados, essa excludente de ilicitude não se estende a eles, de modo que serão responsabilizados e posteriormente punidos de acordo com a teoria da acessoriedade limitada.

Outra legislação apontada é a Lei nº 13.964/19, comumente conhecida como "pacote anticrime" que aperfeiçoou a legislação penal e processual penal, e também contemplou a excludente de ilicitude da conduta do agente com a inserção do art. 10-C na Lei de organizações criminosas (Lei nº 12.850/13) ao dispor que: "*Não comete crime o policial que oculta a sua identidade para, por meio da internet, colher indícios de autoria e materialidade dos crimes previstos no art. 1º desta Lei*".

Depreende-se do exposto que nesse dispositivo, especificamente, o legislador optou pela excludente de ilicitude da conduta do agente em razão do estrito cumprimento do dever legal, tendo em vista, que a ocultação de sua identidade é item primordial para garantir a eficiência e eficácia da infiltração.

Na mesma vertente dos demais dispositivos, através do parágrafo único do art.10-C, o legislador cuidou de positivar o princípio da proporcionalidade, ao estabelecer que o agente que

não guardar a estrita finalidade da investigação e a proporcionalidade responderá pelos excessos praticados.

Por fim, a exclusão da responsabilidade penal do agente infiltrado, no contexto digital, está regulamentada pelo artigo 190-C da Lei 13.441/2017. Este dispositivo estipula que não configura crime a conduta do policial que oculta sua identidade para, por meio da Internet, coletar indícios de autoria e materialidade dos crimes contra a dignidade sexual de crianças e adolescentes, conforme previsto no Estatuto da Criança e do Adolescente (BRASIL, 1990), ou para investigar delitos como invasão de dispositivo informático, estupro de vulnerável, corrupção de menores, satisfação da lascívia mediante presença de criança ou adolescente, favorecimento da prostituição ou de outra forma de exploração sexual de criança, adolescente e/ou vulnerável.

E também em seu parágrafo único, positivou a responsabilização penal do agente que não guardar a estrita finalidade da investigação e a proporcionalidade, devendo responder pelos excessos praticados. Entretanto, a recente legislação não abordou, da mesma forma que a Lei 12.850/2013, a situação em que o agente infiltrado em meio virtual pratica, eventualmente, um crime não previsto no plano operacional autorizado judicialmente, utilizando a excludente de culpabilidade da inexigibilidade de conduta diversa.

Para o autor, a omissão ocorreu porque a infiltração virtual não proporcionará tantas situações imprevisíveis quanto a infiltração "*in loco*", onde o agente está, de fato e fisicamente, próximo aos criminosos, aumentando, naturalmente, as possibilidades de ele cometer comportamentos delituosos não autorizados antecipadamente pelo magistrado. De qualquer maneira, existe a possibilidade dos artigos 10 a 14 da Lei 12.850/2013 serem aplicados de forma subsidiária às infiltrações virtuais, uma vez que tratam do mesmo instituto jurídico, que é a infiltração de agentes policiais (Zanella, 2020).

Nesse sentido, em recente dissertação publicada por Lígia Bueno Asperti, aborda o assunto ao tecer considerações de que a Lei 12.850/2013, que regulamenta o instituto da infiltração policial como gênero, sendo portanto, aplicada de forma subsidiária, para preencher possíveis lacunas existentes na Lei 13.441/2019, que trata da modalidade digital de infiltração policial, entende-se, assim como no caso do artigo 10-C, adicionado à Lei das Organizações Criminosas (Brasil, 2013) pela Lei 13.964/2019 (Brasil, 2019) a possibilidade de utilização da modalidade digital nas investigações dos crimes ali mencionados, que a exclusão da responsabilidade do agente infiltrado ocorre devido à escusa supralegal de culpabilidade por inexigibilidade de conduta diversa. E isso se aplica nos casos em que restar demonstrado que o policial não tinha outra opção a não ser cometer o delito, de modo que sua atuação está de

acordo com a autorização judicial, a finalidade da investigação e os princípios da proporcionalidade.

Conclui o tema, ao lecionar que a regulamentação legal da infiltração policial estabelece duas formas de isenção de responsabilidade penal para o agente policial infiltrado. No contexto da infiltração tradicional, há a exclusão de ilicitude do crime de ocultação da identidade na infiltração na Internet, conforme previsto no artigo 10-C. Além disso, existe a causa supralegal de exclusão de culpabilidade por inexigibilidade de conduta diversa nos demais delitos, desde que cometidos dentro dos limites estabelecidos pela autorização judicial, em conformidade com o princípio da proporcionalidade e finalidade da investigação, como delineado no parágrafo único do artigo 10-C e no artigo 13, todos da Lei 12.850/2013 (Asperti, 2021).

De igual modo no contexto da infiltração digital, como uma espécie do gênero infiltração policial, as escusas se repetem, incluindo a exclusão da ilicitude da conduta de ocultação da identidade para se infiltrar na Internet, conforme disposto no artigo 190-C da Lei 13.441/2017 (Brasil, 2017). Além disso, há a escusa supralegal de culpabilidade por inexigibilidade de conduta diversa, conforme estabelecido no parágrafo único do mesmo dispositivo (Asperti, 2021).

Quanto ao princípio da proporcionalidade, a legislação dispôs que será norteado pelo instituto da inexigibilidade de conduta diversa, conforme disposto no art. 13 "*caput*": "*O agente que não guardar, em sua atuação, a devida proporcionalidade com a finalidade da investigação, responderá pelos excessos praticados".* Ao passo que no parágrafo único, disciplinou sobre a inexigibilidade de conduta diversa: "*Parágrafo único. Não é punível, no âmbito da infiltração, a prática de crime pelo agente infiltrado no curso da investigação, quando inexigível conduta diversa".*

Por outro lado, quanto à lei nº 13.441/2017 (Brasil, 2017), o legislador não mencionou de forma expressa a causa de excludente de responsabilidade penal, apenas cuidou de resguardar em seu dispositivo a proporcionalidade. Depreende-se do exposto que em ambas as legislações, quanto à análise de eventual excesso praticado pelo agente infiltrado será decidida pelo juiz à luz da revelação do caso concreto.

Quanto ao estabelecimento de fixação de limites pelo magistrado, estão previstos tanto no art. 10 da Lei 12.850/13, ao estabelecer que: "art. 10: *A infiltração de agentes de polícia (...) será precedida de circunstanciada, motivada e sigilosa autorização judicial, que estabelecerá seus limites*", quanto no art. 190-A do ECA: art. 190-A, inciso I: "*será precedida de autorização judicial devidamente circunstanciada e fundamentada, que estabelecerá os limites da infiltração para obtenção de prova, ouvido o Ministério Público*". Entretanto, as disposições

legislativas limitaram-se apenas a atribuir ao juízo o dever de estabelecer e fixar os limites da infiltração policial, restando omissas em explanar as balizas norteadoras desta limitação. Dessa forma, compete ao juiz, com base no artigo 3º do Código de Processo Penal (CPP), suprir essa lacuna. É importante destacar que, ao estabelecer os limites para o agente infiltrado, o magistrado deve observar o princípio da proporcionalidade.

Da mesma maneira, ao definir esses limites, o juiz precisa considerar as disposições do artigo 369 do Novo Código de Processo Civil (CPC), equivalente ao artigo 332 do CPC/73, que, por força do artigo 3º do CPP, é aplicável ao processo penal. Esse artigo estipula que a prova, para ser aceitável, deve ser moralmente legítima. Portanto, o agente infiltrado não deveria, por exemplo, se aproximar da filha do investigado e simular envolvimento emocional com ela para se aproximar do alvo da operação. Isso ocorre porque não seria moralmente aceitável atingir terceiros inocentes para desvendar a prática de crimes de uma pessoa específica, especialmente quando existem outros meios para alcançar esse objetivo. É importante ressaltar que a prova que ultrapassa os limites da proporcionalidade e moralidade será considerada nula (Wollf, 2018, p.88).

Insta mencionar igualmente, outro limite à atuação do agente infiltrado, que é a possibilidade do flagrante preparado. Nesse caso, não se trata da anulação da prova, como ocorre quando a conduta do agente é desproporcional ou imoral, mas sim porque não haverá crime por parte do investigado. Essa conclusão decorre da aplicação da Súmula 145 do Supremo Tribunal Federal (STF) ao caso específico. Conforme dispõe: "*Não há crime, quando a preparação do flagrante pela polícia torna impossível a sua consumação*".

Assim, não ocorrerá crime se: i) houver preparação por parte da polícia e, ii) ao mesmo tempo, o crime não se concretizar ou sua consumação for inviável devido à atuação policial. Esse enunciado é resultado do artigo 17 do Código Penal, que trata do crime impossível: Art.17: "*Não se pune a tentativa quando, por ineficácia absoluta do meio ou por absoluta impropriedade do objeto, é impossível consumar-se o crime*".

Nas lições trazidas por Wolff (2018) embasadas nos ensinamentos de Lafave (2003), salienta que a preocupação em evitar a atuação do agente provocador não é exclusiva do direito nacional. De sorte que nos Estados Unidos da América, a jurisprudência estabeleceu a "*entrapment defense*" como uma maneira de restringir e limitar a atividade policial que incentiva a prática de crimes para posteriormente efetuar prisões. Conforme decidido pela Suprema Corte dos Estados Unidos da América no caso *Sorrels* v. *U.S.* (1932), "*entrapment*" seria, em uma tradução livre, "a concepção e o planejamento de um crime por um agente, e a

viabilização de sua prática por ato de terceiro que não o teria perpetrado senão pelos truques, pela instigação ou por fraude por parte deste agente".

Para o autor, tanto na abordagem subjetiva, que avalia se a prática decorreu exclusivamente da provocação, quanto na objetiva, que se concentra nos limites objetivos ao incentivar a prática de crimes, a teoria da "*entrapment defense*" fundamenta-se na instigação estatal como estímulo à prática do ato ilícito, que não poderia ser aceito (Wolff, 2018).

É assunto inconteste que a legislação pátria estabeleceu uma escusa de responsabilidade para todas as ações consideradas infrações penais, realizadas pelo agente infiltrado, quer fisicamente ou digitalmente, contanto que se comprove serem necessárias para a efetiva infiltração policial ou sua continuidade. De sorte que essas ações devem observar a finalidade da investigação e ser proporcionais aos objetivos perseguidos.

3.8 Da materialização das provas obtidas por meio da infiltração policial

A materialização das provas digitais representa um marco crucial na legislação brasileira, refletindo a adaptação necessária para lidar com a crescente importância da tecnologia na sociedade contemporânea. Com a ascensão da era digital, tornou-se imperativo estabelecer diretrizes e parâmetros legais que permitam a utilização eficaz e confiável das evidências obtidas a partir de meios eletrônicos.

O advento das provas digitais implicou uma reconfiguração nos conceitos tradicionais de evidência e sua produção. O ordenamento jurídico brasileiro, ao reconhecer a relevância das tecnologias da informação, estabeleceu na Lei nº 11.419/2006, que dispõe sobre a informatização do processo judicial. Essa legislação promoveu uma transição significativa ao possibilitar a tramitação de processos de forma eletrônica, permitindo a criação e apresentação de documentos digitais como evidências nos procedimentos legais.

Posteriormente, a Lei nº 12.965/2014, conhecida como o Marco Civil da Internet, reforçou a importância da autenticidade das provas digitais ao estabelecer diretrizes para a proteção dos dados e a privacidade dos usuários na rede. Essa legislação preconiza a necessidade de preservar a integridade das informações e reconhece a validade dos documentos eletrônicos como meios de comprovação legal.

É crucial ressaltar que a materialização das provas digitais na legislação brasileira não implica uma renúncia aos princípios de autenticidade e integridade. Pelo contrário, representa um avanço na capacidade do sistema jurídico de acompanhar as transformações tecnológicas e

de assegurar que as evidências apresentadas sejam confiáveis e estejam em conformidade com os preceitos legais.

A materialização das provas digitais na legislação brasileira é uma resposta necessária e progressista à evolução tecnológica. Ao estabelecer parâmetros para a utilização e autenticação de evidências eletrônicas, o sistema legal brasileiro demonstra seu compromisso em garantir a eficácia e a confiabilidade dos processos judiciais na era digital. Essa adaptação é essencial para preservar a justiça e a segurança jurídica em um contexto cada vez mais digitalizado.

A obtenção de provas digitais por meio da infiltração policial representa um avanço significativo no combate à criminalidade na era digital. Esse método envolve a inserção de um agente policial disfarçado em grupos criminosos ou em ambientes virtuais onde atividades ilícitas são suspeitas de ocorrer. O objetivo é coletar informações e evidências que possam subsidiar a persecução penal.

Essa estratégia tornou-se especialmente relevante diante do aumento das atividades criminosas online, que abrangem desde fraudes financeiras e ciberataques até a disseminação de conteúdo ilegal, como pornografia infantil e tráfico de drogas. A infiltração policial em ambientes digitais permite um acesso direto e discreto a esses grupos, possibilitando a obtenção de provas concretas e valiosas para a investigação e persecução criminal.

No entanto, a utilização desse método requer um cuidadoso equilíbrio entre a eficácia na obtenção de provas e o respeito aos direitos individuais e à privacidade. Para isso, é essencial que a infiltração policial seja autorizada judicialmente, sendo conduzida dentro de parâmetros legais estritamente definidos.

Além disso, a atuação do agente policial infiltrado deve ser pautada por princípios éticos e jurídicos, evitando a incitação ou participação ativa em atividades criminosas. O objetivo é obter informações de forma passiva, sem comprometer a integridade da investigação ou a segurança do agente infiltrado.

As provas digitais obtidas por meio da infiltração policial são frequentemente utilizadas em processos judiciais como evidências válidas, desde que sua coleta tenha sido realizada em conformidade com as leis e os procedimentos estabelecidos. A precisão e a autenticidade dessas evidências são fundamentais para garantir a justiça e a eficácia do sistema legal.

Destarte, a infiltração policial em ambientes digitais representa uma importante ferramenta para a obtenção de provas em casos de crimes digitais. Quando realizada de forma legal e ética respeitando os princípios e garantias fundamentais, a utilização deste instituto contribui para o fortalecimento das investigações e a promoção da segurança cibernética,

permitindo que os responsáveis por atividades criminosas online sejam devidamente responsabilizados perante a lei.

4 CONCLUSÃO

No primeiro capítulo foram abordados os princípios do devido processo legal e da proibição da prova ilícita, princípios fundamentais que garantem ao indivíduo a segurança e o respeito por suas garantias individuais. Em seguida, foi discutida a prova no processo penal, incluindo sua definição abrangente e suas principais categorizações: provas documentais, testemunhais e periciais. Também foram apresentados os métodos estabelecidos na legislação para obtenção de provas, garantindo que estes estejam em conformidade com os direitos e garantias fundamentais, como o direito à intimidade, à privacidade e à inviolabilidade do domicílio. Além disso, foram exploradas as orientações doutrinárias relacionadas à busca pela verdade real e substancial, destacando que esta é alcançada por meio dos procedimentos baseados nos princípios do contraditório, da ampla defesa e do devido processo legal.

Depreende-se do exposto que na produção de provas conforme disciplinadas na legislação pátria, são aceitos os meios de obtenção de prova que não infrinjam os direitos e garantias fundamentais, incluindo o direito à intimidade, à privacidade e a inviolabilidade do domicílio. Além disso, são apresentadas a admissibilidade das provas e as restrições estabelecidas por lei, permitindo assim a exploração das orientações doutrinárias relacionadas à busca pela verdade real e substancial. Isso serve como um exemplo da perspectiva doutrinária de que essa verdade é estabelecida por meio de procedimentos baseados nos princípios do contraditório, da ampla defesa e do devido processo legal.

No segundo capítulo, foram apresentadas as provas digitais definindo-as como "*dados armazenados ou transmitidos por dispositivos eletrônicos*". Foram detalhadas suas características peculiares, como imaterialidade, volatilidade, suscetibilidade de clonagem e facilidade de dispersão, exigindo a aplicação de procedimentos técnicos na obtenção, armazenamento e posterior introdução no processo penal. Foi ressaltado que, apesar de não estarem explicitamente previstas na legislação, as provas digitais se tornaram fontes importantes de provas devido à evolução tecnológica.

Analisando as particularidades da prova digital em comparação com as outras formas de evidência aceitas pela legislação brasileira, observa-se que a prova digital apresenta certos traços distintivos, como a ausência de materialidade, a facilidade de ser copiada, a capacidade de se dissipar rapidamente e a necessidade de um dispositivo para a sua transmissão. Isso implica na necessidade de adotar procedimentos técnicos tanto ao obtê-la quanto ao armazená-la e posteriormente introduzi-la no processo penal. Além disso, no que diz respeito à classificação da prova digital, ela se assemelha à prova documental, porém possui uma natureza e características próprias devido às suas peculiaridades distintas.

Em relação à busca pela verdade e à eficiência do processo, é necessário conduzir a obtenção e produção de provas digitais por meio de procedimentos específicos, guiados pelos objetivos de preservação, autenticidade, durabilidade e acessibilidade dos dados digitais. Isso é particularmente crucial devido à volatilidade e fragilidade dessas provas, as quais podem se tornar frágeis se manuseadas de maneira negligente, comprometendo suas características ou até mesmo levando ao desaparecimento.

Esses procedimentos devem respeitar as garantias do devido processo legal, protegendo os direitos fundamentais para assegurar a validade e legitimidade das provas. A aplicação do instituto da cadeia de custódia é fundamental, assim como o respeito às normas que delineiam os procedimentos adequados para a aquisição, conservação, análise e produção de dados digitais. Isso garante a confiabilidade na coleta e preservação da cadeia de custódia, considerando as peculiaridades do ambiente digital.

Embora o ordenamento jurídico brasileiro atual apresente parca legislação específica sobre a obtenção e produção de provas digitais, é possível encontrar fundamentos no Código de Processo Penal e em leis específicas, como a Lei nº 9.296/96, Lei nº 12.965/14 (Marco Civil da Internet), e Lei nº 13.441/17 (alteração no Estatuto da Criança e do Adolescente). Entretanto, a falta de normalização específica não deve ser vista como uma proibição do método de obtenção e produção probatória, primeiramente, em razão do princípio da liberdade probatória, e depois, em decorrência da adesão do Brasil ao Tratado Internacional da Convenção de Budapeste.

Isto porque, conforme foi destacado, o processo penal brasileiro não se limita aos meios de prova mencionados expressamente na legislação. A doutrina prevalecente considera que as partes têm liberdade probatória, desde que não violem as garantias constitucionais ou que sejam irrelevantes ou ilícitas. Por outro lado, sendo as provas digitais espécie das provas tradicionais entendidas como gênero, sempre o julgador e os demais operadores de direito poderão fazer uso da analogia e a hermenêutica.

Em segundo lugar, com a adesão do Brasil a Convenção de Budapeste, sinaliza que em um futuro próximo o poder legislativo deverá fazer a inserção das normativas e diretrizes propostas pelo tratado internacional, tendo em vista o cuidado dos redatores da Convenção de Budapeste em discutir aspectos cruciais, como o direito substantivo, processual e a jurisdição. Assim, a convenção foi elaborada não apenas para introduzir novos tipos de crimes, mas também para estabelecer regulamentos de procedimento penal que conciliam práticas do direito penal internacional, bem como, para estipular acordos relacionados à tecnologia da informação.

No que diz respeito à busca e apreensão da prova digital, as regras existentes no Código de Processo Penal podem ser aplicadas, mas é essencial estabelecer normas específicas que exijam a presença de perito na diligência, determinem a forma do procedimento e os requisitos do registro da apreensão.

Quanto à busca e apreensão da prova digital, é possível conduzi-las de acordo com as normas vigentes no Código de Processo Penal. Entretanto, é fundamental a implementação de normas específicas que incluam a necessidade de um perito na diligência, estabeleçam a metodologia a ser seguida no procedimento e determinem os requisitos para o registro da apreensão.

Também foi abordado o instituto da cadeia de custódia, crucial para garantir os princípios e garantias fundamentais. Por fim, a pesquisa tratou da importância da cooperação internacional na obtenção de provas, por meio da ratificação da Convenção de Budapeste sobre cibercrime.

No último capítulo, foram apresentadas as especificidades do instituto da infiltração policial, incluindo sua definição, modalidades e requisitos de admissibilidade, além dos aspectos operacionais. Em seguida, foi analisado o uso da infiltração policial virtual, introduzida no ordenamento jurídico brasileiro pelas Leis 12.850/2013 e nº 13.441/2017. Foram destacadas as particularidades desse instituto no Brasil e no direito comparado, como Estados Unidos, Itália, Alemanha, Espanha, França, Portugal e Argentina.

No que diz respeito ao último capítulo, é relevante destacar a análise legislativa realizada em países estrangeiros, da qual podemos inferir que, nos ordenamentos jurídicos nacionais examinados, todos optaram por normatizar expressamente as provas digitais. Essa abordagem é justificada pela importância do assunto no contexto atual, considerando os avanços tecnológicos e a sofisticação dos crimes praticados no meio cibernético.

Outro aspecto que merece especial atenção refere-se ao uso de softwares maliciosos, conhecidos como *malware*. Algumas legislações estrangeiras admitem, de maneira explícita, o emprego de programas informáticos ocultos destinados a obter informações processadas por dispositivos informáticos, sendo úteis para a investigação de cibercrimes. Destacam-se, nesse contexto, as legislações relacionadas à prova eletrônica e digital, que contemplam esse recurso. Nestes casos, o juiz competente pode autorizar a instalação de software que permita, de forma remota e telemática, o exame a distância e sem o conhecimento do titular ou usuário, do conteúdo de um computador, dispositivo eletrônico, sistema informático, instrumento de armazenamento de dados ou base de dados. Exemplos notáveis dessas legislações incluem os Estados Unidos, Itália e França.

O assunto abordado é de extrema complexidade e controvérsia. Nos países que autorizam esse recurso, nota-se que as justificativas se baseiam na necessidade de dotar as instâncias de investigação com recursos tão eficientes quanto os disponíveis para os perpetradores de cibercrimes. Essa abordagem visa priorizar o interesse público na prevenção e repressão dessas práticas criminosas, cada vez mais presentes no cenário global.

No entanto, surge a preocupação com a preservação da privacidade e intimidade do indivíduo sob investigação, uma vez que esses recursos são extremamente invasivos, sendo capazes de capturar e revelar praticamente todos os aspectos da vida digital da pessoa investigada. Portanto, nos casos em que o uso de *malware* é permitido em investigações criminais, são estabelecidos limites, como por exemplo, a definição de um rol taxativos de crimes, e seu alto teor de periculosidade, sem se esquecer da necessidade de autorização judicial e outros controles que atuam como condicionantes da legalidade da prova obtida.

Até o momento, no Brasil, não há discussões significativas acerca da utilização do malware. Seria prudente implementar uma regulamentação legal específica, trazendo benefícios evidentes para ambas as partes: os agentes de investigação teriam à disposição uma ferramenta com inegável capacidade probatória quando necessário e em conformidade com as condições legais, enquanto os direitos fundamentais dos investigados seriam restringidos apenas na medida permitida por essa legislação específica.

Outro aspecto crucial a ser examinado ao abordar a infiltração policial refere-se à responsabilidade penal do agente infiltrado e ao Princípio da Proporcionalidade. Pode-se concluir que a exclusão da responsabilidade penal do agente infiltrado no ambiente digital tem uma natureza jurídica de causa supralegal de excludente de culpabilidade devido à inexigibilidade de conduta diversa.

Essa determinação proporciona segurança jurídica tanto aos investigados, que têm a garantia de que a atuação policial será devidamente supervisionada, seja pelo Delegado responsável pela investigação, pelo Ministério Público e/ou pelo magistrado que autoriza a medida, quanto aos agentes infiltrados. Estes últimos podem desempenhar suas funções com tranquilidade, cientes de que estão respaldados pela legislação quando se encontram em situações em que não têm alternativa senão cometer o delito.

Quanto ao princípio da proporcionalidade, é indiscutível que a legislação nacional estabeleceu uma isenção de responsabilidade para todas as ações que possam ser consideradas infrações penais, seja realizada pelo agente infiltrado de maneira física ou digital, desde que fique comprovada a necessidade para a efetiva infiltração policial ou sua continuidade. Essas

ações devem, portanto, estar alinhadas com a finalidade da investigação e ser proporcionais aos objetivos perseguidos.

Inicialmente dito, nos últimos anos, observamos uma significativa transformação na execução e repressão de delitos, impulsionada pelos avanços tecnológicos que deram origem aos cibercrimes. A sociedade contemporânea enfrenta desafios complexos e em constante evolução. Nesse cenário dinâmico, os crimes assumiram novas formas, como roubo de informações, fraudes online, ataques cibernéticos e pornografia infantil, desafiando os sistemas processuais a se adaptarem e responderem eficazmente.

A criminalidade transcende fronteiras geográficas e temporais, escapando ao controle estatal. As abordagens tradicionais de controle penal mostram-se ineficazes diante da criminalidade cibernética, que opera globalmente, explorando as brechas entre sistemas legais e regulatórios. Diante disso, surgem novos métodos de investigação de provas, incluindo a infiltração policial virtual, foco deste estudo.

Diante da insuficiência dos meios tradicionais, a infiltração policial virtual emerge como um meio legítimo de investigação em crimes cibernéticos, desde que respeite os limites dos direitos fundamentais dos indivíduos. Este procedimento, regulamentado pelo ordenamento jurídico, deve ser excepcional, autorizado apenas para investigar delitos específicos listados no rol taxativo autorizador, evitando o uso do agente infiltrado como facilitador genérico das ações de investigação.

A aplicação da infiltração policial virtual deve obedecer ao princípio da proporcionalidade, sendo determinada por decisão fundamentada de um juiz competente. A medida só é justificada quando atende aos requisitos de adequação, necessidade e proporcionalidade em sentido estrito. Portanto, é essencial garantir o equilíbrio entre o garantismo e a eficiência na repressão da criminalidade cibernética, buscando aprimorar a legislação nacional para especificar e ampliar os recursos tecnológicos disponíveis para a obtenção efetiva de provas digitais.

REFERÊNCIAS

ALEMANHA. ***StrafprozeBordnung* (StPO). *Verdecketer Ermittler***. Código de Processo Penal Alemão. Disponível em: https://dejure.org/gesetze/StPO/110a.html. Acesso em: 23 jun. 2021.

ALEMANHA. ***StrafprozeBordnung. Verdeckter Ermittler***. Que permite o uso dos "investigadores proibidos" para investigar ofensas criminais no campo de narcóticos ilícitos, tráfico de armas, organização criminosas, dentre outros. Disponível em: https://dejure.org/gesetze/StPO/110a.html. Acesso em: 23 jun. 2021.

ALEMANHA. ***StrafprozeBordnung. Verfahren beim Einsatz eines Verdeckten Ermittlers***. Artigo que traça e delimita o procedimento ao usar um agente secreto. Disponível em: https://dejure.org/gesetze/StPO/110b.html. Acesso em 26 jun. 2021.

ANDRADE, Manuel da Costa. Bruscamente no verão passado, a reforma do código de processo penal: observações críticas sobre uma lei que podia e devia ter sido diferente. Coimbra: Coimbra Editora, 2009.

ARGENTINA. ***Ley* nº 27.319/16, de 22 de novembro de 2016**. *Investigación, Prevención y Lucha de los delitos complejos. Herramientas. Facultades*. Disponível em: https://www.argentina.gob.ar/normativa/nacional/ley-27319-268004/texto. Acesso em: 26 jun. 2021.

ASPERTI, Lígia Bueno. **A Responsabilidade penal do agente infiltrado na internet: análise das leis nº 12.850/2013 e 13.441/2017. 2021**. Orientador: Dr. Mário Furlaneto Neto. Dissertação (Mestrado em Direito e Estado na Era Digital) – Centro Universitário Eurípides de Marília, Marília, 2021.

BAUMAN, Zygmunt. **Modernidade Líquida**. Trad. Plínio Dentzien. Rio de Janeiro: Zahar, 2001.

BARRETO, Alessandro Gonçalves; SANTOS, Hericson dos. **Deep web: Investigação no submundo da internet**. Rio de Janeiro: Brasport, 2019.

BARROSO, Luís Roberto. Os princípios da razoabilidade e da proporcionalidade no Direito Constitucional. **Revista do Ministério Público do Rio de Janeiro** – nº 4, jul/dez. 1996. Disponível em: https://www.mprj.mp.br/servicos/revista-do-mp/revista-04. Acesso em 13 jan. 2024.

BOITEUX, Luciana. Crimes informáticos: Reflexões sobre a política criminal inseridas no contexto internacional atual. **Revista Brasileira de Ciências Criminais**. São Paulo: Revista dos Tribunais, 2004.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 21 jun. 2021.

BRASIL. **Decreto-Lei nº 3.689, de 03 de outubro de 1941**. Código de Processo Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em 01 out. 2019.

BRASIL. **Lei nº 13.964, de 24 de dezembro de 2019**. Aperfeiçoa a legislação penal e processual penal. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13964.htm. Acesso em: 10 fev. 2020.

BRASIL. **Lei Federal nº 9.099, de 26 de setembro de 1995**. Dispõe sobre os Juizados Especiais Cíveis e Criminais e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/leis_2001/l10217.htm. Acesso em: 01 de out. de 2019.

BRASIL. **Lei nº 10.217, de 11 de abril de 2011**. Altera os arts. 1o e 2o da Lei no 9.034, de 3 de maio de 1995, que dispõe sobre a utilização de meios operacionais para a prevenção e repressão de ações praticadas por organizações criminosas. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/leis_2001/l10217.htm. Acesso em: 15 jun. de 2021.

BRASIL, **Lei nº 10.409, de 11 de janeiro de 2002**. Dispõe sobre a prevenção, o tratamento, a fiscalização, o controle e a repressão à produção, ao uso e ao tráfico ilícitos de produtos, substâncias ou drogas ilícitas que causem dependência física ou psíquica, assim elencados pelo Ministério da Saúde, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10409.htm. Acesso em: 15 jun. de 2021.

BRASIL. **Lei nº 11.343, de 23 de agosto de 2006**. Institui o Sistema Nacional de Políticas Públicas sobre Drogas - Sisnad; prescreve medidas para prevenção do uso indevido, atenção e reinserção social de usuários e dependentes de drogas; estabelece normas para repressão à produção não autorizada e ao tráfico ilícito de drogas; define crimes e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11343.htm. Acesso em: 21 de jun. de 2021.

BRASIL. **Lei nº 12.694, de 24 de julho de 2012**. Dispõe sobre o processo e o julgamento colegiado em primeiro grau de jurisdição de crimes praticados por organizações criminosas; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 3.689, de 3 de outubro de 1941 - Código de Processo Penal, e as Leis nºs 9.503, de 23 de setembro de 1997 - Código de Trânsito Brasileiro, e 10.826, de 22 de dezembro de 2003; e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/L12694.htm. Acesso em: 21 de jun. de 2021.

BRASIL. **Lei nº 12.850, de 02 de agosto de 2013**. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei nº 9.034, de 3 de maio de 1995. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. Acesso em: 21 de jun. 2021.

BRASIL. **Lei nº 13.441, de 08 de maio de 2017**. Altera a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), para prever a infiltração de agentes de polícia na internet com o fim de investigar crimes contra a dignidade sexual de criança e de adolescente. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Lei/L13441.htm. Acesso em: 24 de jun. de 2021.

BRASIL. **Lei nº 11.690 de 2008**. Que alterou os dispositivos do Decreto-Lei nº 3.689, de 3 de outubro de 1941 – Código de Processo Penal, relativos à prova, e outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11690.htm. Acesso em: 04 jun 2023.

BRASIL. **Lei nº 4.898, de 09 de dezembro de 1965**. Regula o Direito de Representação e o processo de Responsabilidade Administrativa Civil e Penal, nos casos de abuso de autoridade. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l4898.htm. Acesso em: 24 jun. 2021.

BRASIL. **Lei nº 13.964, de 24 de dezembro de 2019**. Aperfeiçoa a legislação penal e processual penal. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm. Acesso em: 27 jun. 2023.

BRASIL. **Decreto nº 5.014, de 12 de março de 2004**. Promulga o protocolo adicional da Convenção de Palermo. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/decreto/d5016.htm. Acesso em: 27 jun. 2023.

BRITO. Sônia. **O agente infiltrado: o problema da legitimidade no processo penal so estado de direito e na experiência brasileira**. Coimbra: Almedina, 2016.

CARNELUTTI, Francesco. "***Lecciones sobre el Proceso Penal***". Trad. Espanhola, Vol. II. Buenos Aires: EJEA, 1950.

CARVALHO, Paulo Roberto de Lima. **Prova cibernética no processo**. Curitiba: Juruá, 2009.

CASEY, Eoghan. ***Digital Evidence and computer crime : forensic Science, computers and the internet.*** *Third edition/by Eoghan Casey ; with contributions from Susan W. Brenner [et al]*. San Diego: Elsevier, 2011.

CASTRO. Henrique Hoffmann Monteiro de. **Lei nº 13.441/2017 instituiu a infiltração policial virtual**. Disponível em: https://www.conjur.com.br/2017-mai-16/academia-policia-lei-1344117-instituiu-infiltracao-policial-virtual?. Acesso em: 15 de jun. de 2021.

CASTELLS, Manuel. **A galáxia da internet: Reflexões sobre a internet, os negócios e sociedade**. Tradução Maria Luiza de A. Borges. Rio de Janeiro: Jorge Zahar, 2003.

CRESPO, Marcelo Xavier de Freitas. Crimes digitais: do que estamos falando? 2015. Disponível em: https://canalcienciascriminais.com.br/crimes-digitais-do-que-estamos-falando/. Acesso em 20 jun. 2023.

DINAMARCO, Cândido Rangel. **Instituições de Direito Processual Civil** - Vol.3. São Paulo: Malheiros, 2001.

DIRETIVA DA UNIÃO EUROPEIA. **Directive (EU) 2017/541 of the European Parliament and of the Council** of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA. Disponível em: https://eur-lex.europa.eu/eli/dir/2017/541/oj. Acesso em 26 jun. 2023.

ESPANHA. ***Artículo 282-bis, Ley de Enjuiciamiento Criminal***. Título III. De la policía judicial. Disponível em: https://vlex.es/vid/ley-enjuiciamiento-criminal-real-septiembre-170233. Acesso em: 26 jun. 2021.

ESPANHA. **Ley de Enjuiciamiento Criminal**. Ley Orgánica 13/2015. Disposiciones generales. Disponível em: https://www.boe.es/eli/es/lo/2015/10/05/13. Acesso em 26 jun. 2021.

ESPANHA. ***Boletín Oficial de las Cortes Generales-Senado****, IX legislatura, 28 de marzo de 2011, núm 38, pág. 5.* Disponível em: https://www.senado.es/legis9/publicaciones/pdf/senado/bocg/BOCG_T_09_38.PDF. Acesso em 24 mai 2023.

ESTADOS UNIDOS DA AMÉRICA. *Title 28 -* ***Judiciary and Judicial Procedure****, Part II - Department of Justice, Chapter 33 – Federal Bureau of Investigation*. Traça e delimita as diretrizes da infiltração de agentes. Disponível em: https://uscode.house.gov/view.xhtml?path=/prelim@title28/part2/chapter33&edition=prelim. Acesso em 26 jun. 2021.

ESTADOS UNIDOS DA AMÉRICA. ***United States Attorney's Office District of Nebraska*** *2015 - Annual Report*. Disponível em: https://www.justice.gov/usao-ne/file/830846/download#page=25. Acesso em: 30 mai 2023.

ESTADOS UNIDOS DA AMÉRICA. *Murray v. United States*, 487 U.S 533 (1988). ***Justia U.S Supreme Court***. Disponível em : https://supreme.justia.com/cases/federal/us/487/533/. Acesso em: 18 jan. 2024.

ESTADOS UNIDOS DA AMÉRICA*: Nix v. Williams*, 467 U.S 431 (1984). **Justia U.S Supreme Court**. Disponível em: https://supreme.justia.com/cases/federal/us/467/431/. Acesso em: 18 jan. 2024.

FERRAJOLI. Luigi. **Direito e Razão**: Teoria do Garantismo Penal. São Paulo: Editora Revista dos Tribunais, 2002.

FERREIRA, Marco Aurélio Gonçalves. **Devido processo legal**: um estudo comparado. Rio de Janeiro: Lumen Juris, 2004, p. 60-61.

FILIOL, Eric. ***Computer viroses: From theory to applications***. Paris : Springer, 2004.

FOUCALT. Michel. **Vigiar e punir**: Nascimento da prisão. Trad. Raquel Ramalhete. Petrópolis: Vozes, 1987.

FURLANETO NETO. Mário. **Crimes na internet e inquérito policial eletrônico**/Mário Furlaneto Neto, José Eduardo Lourenço dos Santos, Eron Veríssimo Gimenes. 2. ed. São Paulo: Edipro, 2018.

FURLANETO NETO, Mário; DOS SANTOS, José Eduardo Lourenço. APONTAMENTOS SOBRE A CADEIA DE CUSTÓDIA DA PROVA DIGITAL NO BRASIL. **Revista Em Tempo**, [S.l.], v. 20, n. 1, nov. 2020. ISSN 1984-7858. Disponível em: <https://revista.univem.edu.br/emtempo/article/view/3130>. Acesso em: 25 jan. 2024. doi: https://doi.org/10.26729/et.v20i1.3130. Acesso em: 15 mai. 2023.

FRANÇA. ***Livre IV : De quelques procédures particulières***. *Titre XXV: De la procédure appicable à la criminalité et à la délinquance organisées et aux crimes.* Disponível em: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071154/LEGISCTA000006138138/#LEGISCTA000038311675. Acesso em: 26 jun. 2021.

FRANÇA. **Code des douanes**. Titre II: Organisation et fonctionnement du servisse des douanes (Articles 43 à 67F) Chapitre IV : Pouvoirs des agents des douanes (Articles 60 à 67 quinquies B). Section 7 : Procédures spécieles d'enquête douanière (Articles 67 bis à 67 bis-4). Disponível em : https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006071570/. Acesso em 25 mai. 2023.

FRANÇA. ***Code de Procédure Pénale****: Paragraphe 4: De la captation des données informatiques*. Article 706-102-1. Disponível em: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038311624. Acesso em 30 mai 2023.

FERREIRA, Marco Aurélio Gonçalves. **Devido processo legal: um estudo comparado**. Rio de Janeiro: Lumen Juris, 2004, p. 60-61.

GAUTHIER. Nicolas. ***Eugène-François Vidocq, penseur de l'espace social criminel***. *Romantisme*: 2017/1 (nº 175), p.29.

GOJKOVIC-LETTE. Colonel Johanne. ***Le coup d'achat : Un instrument efficace dans la lutte la criminalité. In observatoire des criminalités internationales***. Juillet, 2021.p.6. Disponível em: https://www.iris-france.org/wp-content/uploads/2021/07/Obs-Criminalit%C3%A9s-internationales-Juillet-2021.pdf. Acesso em: 25 mai 2023.

GIDDENS, Anthony. **As consequências da modernidade**. Trad. Raul Fiker. São Paulo: Editora Unesp, 1991.

GOUVÊA, Sandra. O direito na era digital: crimes praticados por meio da informática. Rio de Janeiro: Mauad, 1997.

GRINOVER, Ada Pellegrini. **Liberdades públicas e processo penal: as interceptações telefônicas**. 2. Ed. São Paulo: Revista dos Tribunais, 1982.

ITÁLIA: ***Legge nº nº 309/1990****, Capo III. Operazioni di Polizia e Destinazione di beni e valori sequestrati o confiscati. Articulo 97. Attivita' sotto copertura*. Traça e delimita diretrizes para as unidades especializadas antidrogas, que, exclusivamente, utiliza as técnicas, com o propósito de obter provas sobre os crimes previstos neste diploma. Disponível em: https://www.federserd.it/files/download/drp_309_9-10-90_aggiornato.pdf. Acesso em: 23 jun. 2021.

ITÁLIA. ***Legge nº* 306/1992**. 12-*Quater. Ricettazione di armi, riciclaggio e reimpiego simulati*. Dispõe sobre a Polícia Judiciária do serviço de Investigação Anti-máfia. Disponível em: https://direzioneinvestigativaantimafia.interno.gov.it/normative/d.l.306-1992.pdf. Acesso em 26 jun. 2021.

ITÁLIA. ***Legge nº* 268/1998**. *artigo 14. Attivita' di Contrasto*. Dispõe sobre polícia judiciária das estruturas especializadas para a repressão de crimes sexuais ou para a proteção de menores, ou aqueles instituídos para o confronto de infrações do crime organizado, podem, mediante autorização da autoridade judiciária, com o único objetivo de obter provas. Disponível em: https://www.camera.it/parlam/leggi/98269l.htm. Acesso em: 23 jun. 2021.

ITÁLIA. **Legge nº 269/1998**. *Norme contro lo sfruttamento dela prostituzione, dela pornografia, del turismo sessuale in danno di minori, quale nuove forme di reduzione in schiavitu*. Disponível em: https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:1998-08-03;269!vig=. Acesso em 23 jun. 2021.

ITÁLIA. ***Legge nº 146/2006***. *Ratifica ed esecuzione dela Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, adottati dall'Assemblea generale il 15 novembre 2000 ed il 31 maggio 2001*. Disponível em: https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2006-03-16;146. Acesso em 22 mai 2023.

ITÁLIA. ***Articolo 51 Del Codice Penale***. Disponível em: https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:codice.penale:1930-10-19;1398~art51. Acesso em 22 mai 2023.

JORGE. Higor Vinicius Nogueira. **Investigação criminal tecnológica: cont´rm informações so0bre inteligência policial, drones e recursos tecnológicos aplicados na investigação.** Volume 2. – Rio de Janeiro: Brasport, 2018.

JOSE. Maria Jamile. **A infiltração policial como meio de investigação de prova nos delitos relacionados à criminalidade organizada**. 2010. Dissertação (Mestrado). Universidade de São Paulo, São Paulo. Disponível em: https://teses.usp.br/teses/disponiveis/2/2137/tde-01122010-144008/pt-br.php. Acesso em: 21 mar. 2021.

KANDA, Bruna Bárbara Paiz Zeotti. Direito, **Novas tecnologias e Controle Social: O cenário do Direito Digital**/ Bruna Bárbara Paiz Zeotti Kanda, Michele Christina Martins Pigozzi da Silva, org; José Eduardo Lourenço dos Santos, coordenador – Curitiba: CRV, 2022.

KHALED JR. Salah H. **A busca da verdade no processo penal: para além da ambição inquisitorial**/ Salah H. Khaled Jr. – 4. Ed. – Belo Horizonte, MG: Letramento; Casa do Direito, 2023.

LIMA. Renato Brasileiro de. **Legislação Criminal Especial Comentada**. 5ª ed. Vol. Único. Salvador: Juspodvm, 2017.

MACIEL, Rafael Fernandes. **Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais** (Lei nº 13.709/18). 1ª ed. Goiânia: RM Digital Education, 2019.

MALATESTA. Nicola Framarino Dei. **A Lógica das provas em matéria criminal**. Tradução de J. Alves de Sá. 2 ed. Lisboa: A.M. Teixeira & C., 1927.

MALDONADO, Viviane Nóbrega. **LGPD – Lei Geral de Proteção de Dados Pessoais. Manual de Implementação**. 3ª Ed. São Paulo: Revista dos Tribunais, 2020.

MARQUES. José Frederico. **Instituições de Direito Processual Civil**. Campinas: Millenium – 1ª ed. Atualizada, 2000.

MARQUES. Maria Joana Xara-Brasil. **Os meios de obtenção de prova na lei do cibercrime e o seu confronto com o código de processo penal**. 2014. Dissertação (Mestrado) Universidade Católica Portuguesa, Lisboa, Portugal. Disponível em: https://repositorio.ucp.pt/bitstream/10400.14/17887/1/Dissertacao%20de%20Mestrado%20final%20-%20JoanaXaraBrasilMarques%20-%20Final.pdf. Acesso em: 13 abr. 2021.

MEIREIS, Manuel Augusto Alves. **O Regime Das Provas Obtidas Pelo Agente Provocador Em Processo Penal**. Coimbra: Almedina, 1999.

MINTO, Andressa Olmedo. **A Prova Digital no Processo Penal**. São Paulo: LiberArs, 2021.

PEREIRA, Flávio Cardoso. **Agente infiltrado virtual: primeiras impressões da Lei nº 13.441/2017**. Revista do Ministério Público de Goiás. Goiânia, p.97-117, 2017. Disponível em: http://www.mp.go.gov.br/revista/pdfs_12/8-ArtigoFlavio_Layout%201.pdf. Acesso em 12 mar. 2021.

PEREIRA. Flávio Cardoso. ***El agente infiltrado desde el punto de vista del garantismo procesal penal***. Coimbra: Juruá Editorial, 2016.
PORTUGAL. Lei nº 101, de 25 de agosto de 2001. Ações encobertas para fins de prevenção e investigação criminal. Disponível em: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=89&tabela=leis. Acesso em: 26 jun. 2021.

PORTUGAL. **Lei nº 61/2015, de 25 de agosto de 2015**. Que estabelece o regime jurídico das ações encobertas para fins de prevenção e investigação criminal, permitindo que nelas sejam incluídos todos os ilícitos criminais relacionados com o terrorismo. Disponível em: https://dre.pt/home/-/dre/67579528/details/maximized. Acesso em: 25 jun. 2021.

PORTUGAL. **Lei nº 109/2009, de 15 de setembro de 2009**. Aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa. Disponível em: https://dre.pt/dre/detalhe/lei/109-2009-489693. Acesso em: 29 mai. 2023.

RAMOS, Armando Dias. **O agente encoberto digital: meios especiais e técnicos de investigação criminal**. Coimbra: Almedina, 2022, p.54).

RODRIGUES. Benjamim Silva. **Da prova penal: Tomo IV – Da prova-electrónico-digital e da criminalidade informático-digital**. Coimbra: Coimbra Editora, 2009.

RAMOS, João Gualberto Garcez. **Evolução histórica do princípio do devido processo legal**. Revista da Faculdade de Direito da Universidade Federal do Paraná – UFPR. Curitiba, n 46, p.101-110, março, 2007. Disponível em: https://revistas.ufpr.br/direito/article/view/14975/10027. Acesso em: 26 jun. 2021.

ROSSINI. Augusto Eduardo de Souza. **Informática, telemática e direito penal**. São Paulo: Memória jurídica, 2004.

SALES, Sheila Jorge Selim de. **Do sujeito ativo na parte especial do código penal**. Belo Horizonte: Del Rey, 1993.

SANTOS, José Eduardo Lourenço dos. **A discriminação racial pela internet e o direito penal: o preconceito sob a ótica criminal e a legitimidade da incriminação**. Curitiba: Juruá, 2014.

SCARANCE FERNANDES, Antônio. Antônio. **O equilíbrio na repressão ao crime organizado**. *In*: *Crime organizado – aspectos processuais*. São Paulo: Revista dos Tribunais, 2009.

SCHWAB, Klaus. **A Quarta Revolução Industrial/Klaus Schwab**; tradução Daniel Moreira Miranda. – São Paulo: Edipro, 2016.

STANGUERLIN, Marina; PETEAN, Fabiano Augusto. **Agente infiltrado: sua natureza jurídica na produção digital de provas**. 1ª ed. – Curitiba: Appris, 2021.

SYDOW. Spencer Toth. **Crimes informáticos e suas vítimas**. 2. Ed. São Paulo: Saraiva, 2015.

SILVA, Ângelo Roberto Ilha da; SHIMABUKURO, Adriana... [et al.]. **Crimes Cibernéticos. 2ª ed. De acordo com a Lei nº 13.441/17 (Lei de Infiltração Virtual) e a Lei nº 13.260/16 (Lei Antiterrorismo)**. Porto Alegre: Livraria do Advogado, 2018.

SILVA, Eduardo Araújo da. **Crime organizado: procedimento probatório**. 2ª Edição. São Paulo: Atlas, 2009.

SOUSA, Marcos Silva, Jorge Campos. Construção de vídeos de rotas de veículos através da composição de segmentos de vídeos georreferenciados. **Revistas Unifacs – Universidade de Salvador.** v.14 (2015). Disponível em: https://revistas.unifacs.br/index.php/sepa/article/view/3848.

SOUZA, Bernardo de Azevedo. **Manual prático de provas digitais**/Bernardo de Azevedo e Souza, Alexandre Munhoz, Romullo Carvalho. – São Paulo: Thomson Reuters Brasil, 2023.

SUPREMO TRIBUNAL FEDERAL – STF. 2ª Turma, **RHC 90.376/RJ**, Rel. Min. Celso de Mello, DJe-018 17/05/2007. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=456098. Acesso em: 31 mar. 2022.

SUPREMO TRIBUNAL FEDERAL. 2ª Turma, **HC 69.912-0/130-RS**. Relator Ministro Néri da Silveira, 08/03/1996. Disponível em: https://jurisprudencia.stf.jus.br/pages/search?base=acordaos&pesquisa_inteiro_teor=false&sinonimo=true&plural=true&radicais=false&buscaExata=true&page=1&pageSize=10&queryString=69.912-0%2F130-RS&sort=_score&sortBy=desc. Acesso em 26 jun. 2023.

SUPREMO TRIBUNAL FEDERAL. "**Secretaria de Altos Estudos, Pesquisa e Gestão da Informação e Coordenadoria de Difusão de Informação – Jurisprudências Internacionais**". Pesquisa de jurisprudência internacional sobre "Admissibilidade de Prova Ilícita." Disponível em: https://www.stf.jus.br/arquivo/cms/jurisprudenciaInternacional/anexo/PJI52021AdmissibilidadedaprovailcitaV3.pdf. Acesso em: 04 jun 2023.

TARUFFO, Michele. ***La prueba de los hechos***. Madrid: Trotta, 2005.

TAVARES, Juarez. **Prova e Verdade**/ Juarez Tavares; Rubens Casara. São Paulo: Tirant lo Blanch, 2020.

VALENTE, Manuel Monteiro Guedes. **A investigação do crime organizado: Buscas domiciliares nocturnas, o agente infiltrado e intervenção nas comunicações**. *In*: VALENTE, Manuel Monteiro Guedes (coord). *Criminalidade organizada e criminalidade de massa. Interferêncioas e ingerências mútuas*. Coimbra: Almedina, 2009. p.159-184.

VAZ, Denise Provazi. **Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório**. Orientador: Antonio Scarance Fernandes, 2012. 198 f. Tese (Doutorado em Direito) – Faculdade de Direito da Universidade de São Paulo, São Paulo, 2012.

VIANA, Ulisses Scharz. Liberdade de expressão, comunicação e manifestação do pensamento como princípios fundamentais do marco civil. *In*. LEITE, George Salomão *et al*. *Marco Civil da Internet.* São Paulo: Atlas, 2014.

ZANELLA, Everton Luiz. **Infiltração de agentes**. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/442/edicao-1/infiltracao-de-agentes. Acesso em 23 jun. 2021.

WOLFF. Rafael. **Agentes Infiltrados: O magistrado como garantidor e ferramenta de aprimoramento deste meio especial de investigação**. 2ª ed. São Paulo: Almedina, 2018.