CYBER PROVA NO DIREITO LUSO BRASILEIRO

José Alexandre Amaral Carneiro

Dissertação de Mestrado em Direito

Especialização em Ciências Jurídico-Políticas

Orientação: Prof. Ana Rita Alfaiate

Agosto, 2021

UNIVERSIDADE PORTUCALENSE

Do conhecimento à prática.

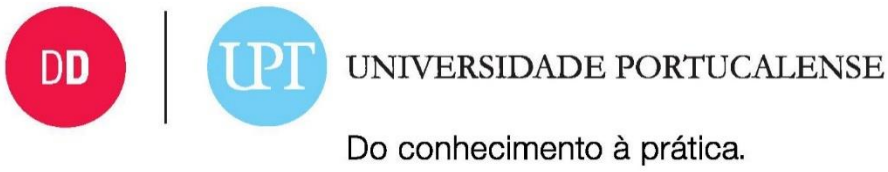
IMP.GE.84.1

José Alexandre Amaral Carneiro

CYBER PROVA NO DIREITO LUSO BRASILEIRO

Dissertação de Mestrado apresentada à Universidade Portucalense Infante D. Henrique para obtenção do grau de Mestre em Direito *especialização em Ciências Jurídico-Políticas*, sob a Orientação da Professora Doutora Ana Rita Alfaiate.

Departamento de Direito
Agosto, 2021



Dedico este trabalho à minha família, pelo incentivo e apoio incondicional de minha vida escolar e acadêmica.

AGRADECIMENTOS

Agradeço aos professores da licenciatura e do mestrado que me deram base e conhecimento científico, que estimularam a vontade de apreender, querer fazer melhor, propiciando a conclusão desse trabalho científico.

Agradeço minha orientadora Professora Ana Rita Alfaiate.

Agradeço meus familiares e esposa pelo apoio incondicional, carinho e sapiência.

Finalmente, agradeço a Deus que colocou no meu caminho seres tão especiais que me permitiram chegar até aqui, dar-me resiliência, manter a esperança e energia para conseguir finalizar a dissertação.

CYBER PROVA NO DIREITO LUSO BRASILEIRO

RESUMO

O presente estudo abordou a questão da cyber prova no direito português e brasileiro. Para tanto, empregou-se como procedimento metodológico pesquisa em materiais bibliográficos obtidos em repositórios como o Google Acadêmico e Scielo, além de sites institucionais e legislações e jurisprudências de ambos os países, empregando-se nesta busca os termos chaves principais: prova digital, prova eletrônica, cyber prova, crime digital, crime eletrônico, crime digital entre outros. Assim, iniciou-se o desenvolvimento do estudo elucidando o conceito de prova no tocante à sua natureza, função, finalidade e modalidades sob a luz do regramento legal dos países em estudo. Na sequência, descreveu-se os meios tradicionais pelos quais as provas são obtidas, tais como testemunhal, declarações de arguido, acareação entre outras. No capítulo seguinte abordou-se como ocorre a criminalidade informática por meio dos agentes hackers e crakers e principais casos registrados e, por fim, descreveu-se a prova digital no tocante à suas características, tipificação legal, princípios, legislação regulamentadora, obtenção e dificuldades enfrentadas no contexto contemporâneo. Desta forma, pode-se responder o objetivo geral do presente estudo que foi o de elucidar o papel e importância da cyber prova no contexto jurídico legal de Portugal e do Brasil, chegando-se à conclusão que há inúmeras formas de crimes informáticos, os quais são perpetrados por indivíduos denominados de hackers, phreakers, crackers, lammers entre outros que causam instabilidade na ordem social e econômica por meio de atividades ilícitas, as quais somente poderão ser eficientemente combatidas com instrumentos específicos como o da prova digital, a qual obtém evidências através da busca e preservação de dados, sendo esta possível desde que seja legal e moralmente válida. Neste sentido, legislações específicas foram criadas, mas, ainda assim falta regras de procedimentos que melhor conduzam sua ação, sendo o regime de prova digital ou ausente ou fragmentado, fragilizando a punição dos criminosos. Assim, os operadores legais devem ter celeridade no alinhamento jurídico dos instrumentos necessários para que se investigue e puna esses contraventores, inclusive com cooperação internacional pautada em procedimentos padronizados tendo em vista a transnacionalidade dessas práticas.

Palavras-chave: Direito comparado; Cyber prova; Criminalidade informática; Crime digital.

CYBER PROOF IN BRAZILIAN LUSO LAW

ABSTRACT

This study addressed the issue of cyber proof in Portuguese and Brazilian law. Therefore, a methodological procedure was used to search bibliographic materials obtained from repositories such as Academic Google and Scielo, as well as institutional sites and legislation and jurisprudence from both countries, using the main key terms in this search: digital proof, proof electronics, cyber proof, digital crime, electronic crime, digital crime among others. Thus, the development of the study began, elucidating the concept of evidence regarding its nature, function, purpose and modalities in light of the legal regulations of the countries under study. Next, the traditional means by which evidence is obtained were described, such as testimonials, defendants' statements, confrontation, among others. The following chapter discussed how computer crime occurs through hackers and crackers and the main registered cases and, finally, the digital evidence was described in terms of its characteristics, legal classification, principles, regulatory legislation, procurement and difficulties faced in the contemporary context. In this way, one can answer the general objective of this study, which was to elucidate the role and importance of cyber evidence in the legal legal context of Portugal and Brazil, reaching the conclusion that there are numerous forms of computer crimes, which are perpetrated by individuals called hackers, phreakers, crackers, lammers, among others that cause instability in the social and economic order through illicit activities, which can only be efficiently fought with specific instruments such as digital proof, which obtains evidence through search and preservation of data, which is possible as long as it is legally and morally valid. In this sense, specific legislation was created, but even so, there is a lack of procedural rules that better guide their action, with the system of digital evidence being either absent or fragmented, weakening the punishment of criminals. Thus, legal operators must swiftly align the legal instruments needed to investigate and punish these offenders, including international cooperation based on standardized procedures, bearing in mind the transnationality of these practices.

Keywords: Comparative law; Cyber proof. Computer Crime. Digital Crime.

SUMÁRIO

INTRODUÇÃO **10**
METODOLOGIA **14**
1 CONCEITO DE PROVA (A SUA NATUREZA/ FUNÇÃO) **15**
1.1 PROVA PESSOAL E PROVA REAL 20
1.2 PROVA DIRECTA (IMEDIATA) E INDIRECTA (MEDIATA/REPRESENTATIVA) 20
1.2.1 Prova representativa e prova indiciária **21**
1.3 PROVA PRÉ-CONSTITUÍDA E PROVA CONSTITUENDA 22
1.4 PROVA LIVRE E PROVA LEGAL 23
1.5 NOVIDADE DA LEI N.º 41/2013, DE 26 DE JUNHO: PROVA POR VERIFICAÇÕES NÃO JUDICIAIS QUALIFICADAS 24
2 FUNÇÃO E FINALIDADE DA PROVA **26**
2.1 PROVA COMO ACTIVIDADE PROBATÓRIA (PROBATÓRIO) 27
2.2 PROVA COMO RESULTADO PROBATÓRIO 29
2.3 MEIOS DE PROVA 30
2.4 PROVA DIFÍCIL 31
3 OS MEIOS TRADICIONAIS DE OBTENÇÃO DE PROVA **33**
3.1 PROVA TESTEMUNHAL (ART.º 128.º DO CPP) 33
3.2 DECLARAÇÕES DO ARGUIDO (ART.º 140.º E 141.º DO CPP) 37
3.3 PROVA POR ACAREAÇÃO (ART.º 146.º DO CPP) 39
3.4 PROVA POR RECONHECIMENTO (ART.º 147.º A 149 DO CPP) 40
3.5 PROVA PERICIAL (ART.º 151.º DO CPP) 42
3.6 PROVA DOCUMENTAL (ART.º 164.º DO CPP) 45
3.7 ESCUTAS TELEFÓNICAS (ART.º 187.º DO CPP) 48
4 A CRIMINALIDADE INFORMÁTICA **52**
4.1 HACKERS 57
4.2 OS CRACKERS 59
4.3 ATAQUES REGISTRADOS 61
5 A PROVA DIGITAL / PROVA ELECTRÓNICA **64**
5.1 CARACTERÍSTICAS 65
5.2 TIPIFICAÇÃO 66
5.3 PRINCÍPIOS 67
5.4 LEIS REGULADORAS 68
5.4.1 Código de Processo Penal **70**

5.4.2 Lei nº 32 / 2008, de 17 de Junho 72
5.4.3 Lei nº 109 / 2009, de 15 de setembro 28 (Lei do Cibercrime) 73
5.5 OBTENÇÃO DAS PROVAS DIGITAIS E BOAS PRÁTICAS 76
5.6 AS DIFICULDADES COLOCADAS PELA PROVA DIGITAL 80
5.7 SITUAÇÕES ONDE PODE SER UTILIZADA 81
CONCLUSÃO 83
REFERÊNCIAS 86

INTRODUÇÃO

A sociedade moderna está em constante mudança. Isso é especialmente verdadeiro no tocante ao uso de novas tecnologias. As distâncias físicas estão sendo revisadas porque não fazem mais sentido.

Transformações do século XX, como internet e correio eletrônico, mensagens curtas e redes sociais, não foram bem explorados e tiveram pouca relevância para a comunidade e o crime em particular. No entanto, graças à adaptabilidade e ao uso cada vez maior das Tecnologias da Informação e da Comunicação (TICs), esses contatos tornaram-se parte integrante da vida cotidiana e estão influenciando todos os seus aspectos.

A comunicação privada é uma das áreas mais revolucionadas da tecnologia. As comunicações eletrônicas são o método preferido de comunicação porque oferecem velocidade, baixo custo e fácil acesso, o que é representado por instrumentos como o correio eletrônico, SMS, e mensagens instantâneas a exemplo do WhatsApp e Messenger.

Nesse contexto os crimes informáticos tornaram-se mais comuns do que nunca, graças aos avanços tecnológicos. Necessário seria, portanto, que as leis de muitos países fossem atualizadas, modificadas ou criadas com o objetivo de combater o crime cibernético, utilizado principalmente pelo crime organizado e por terroristas.

Assim sendo, enquanto atividade probatória, a prova passou a ser elemento fundamental nesta tarefa, pois demonstra os fatos necessários para comprovar a existência do crime, a punição do réu e a pena ou medida de segurança cabível. Todos os atos ilícitos perpetrados no ambiente digital estão sujeitos à prova. A prova, resultante de atividades probatórias, é a razão que leva o órgão decisório a condenar sobre a ocorrência de fatos relevantes. Esta condição deve ser satisfeita se a motivação estiver de acordo com as regras da ciência, experiência e lógica.

A prova é, portanto, uma ferramenta, um resultado e uma atividade. Seus elementos objetivos são a prova. O resultado final da prova, que é a verdade dos fatos tal como são alegados, e a atividade probatória que corresponde ao conjunto dos atos processuais destinados a comprovar a veracidade do delito cometido.

Nesse contexto, é importante destacar que nem todas as provas podem ser acatadas no processo. No entanto, devem ser considerados os casos em que as provas podem ou não ser admissíveis, tendo em vista sua finalidade de demonstrar os fatos.

Nesse contexto, a produção da prova deve ocorrer em função de seu objetivo, respeitando desta forma os probandos fatos a respeito dos quais produzir-se-á os meios de prova que os sujeitos processuais indicarão.

A prova por si só é incapaz de comprovar qual é a sua função demonstrativa dos fatos (juridicamente relevantes), exigindo, assim, um meio de torná-la válida e eficaz.

Por ser o direito de prova uma garantia constitucional, não se pode falar em ação contraditória efetiva se não incluir a faculdade de usar todos os meios de prova possíveis e suficientes para reconstruir o que está sendo dito. Isso ocorre porque o direito à prova é um componente inevitável do princípio do contraditório. Faz-se necessário, portanto, sua revisão à luz da garantia constitucional do instrumento adequado para a solução de conflitos.

Hoje em dia, com os avanços tecnológicos, grande parte da população passou a ter acesso às Tecnologias da Informação e Comunicação, eles podem usá-los em sua vida cotidiana de maneira comum e difundida. O uso crescente de TICs pode levar ao cometimento ou vestígios de infrações criminais semelhantes. Existem muitos crimes que podem ser cometidos em um ambiente virtual, incluindo aqueles que envolvem provas digitais. Isso não é apenas cibercriminalidade.

Devido aos avanços tecnológicos, a evidência literal pode incluir arquivos de vídeo ou áudio digital. A investigação criminal pode (e não deve) priorizar as provas digitais nas investigações criminais, pois isso pode levar à perda da prova final que exonera ou condena um suspeito (acusado), ou provas impossíveis de obter por outros métodos tradicionais.

Os investigadores precisam lembrar que os dispositivos eletrônicos podem conter muitas informações que podem ser úteis em suas investigações. Essas informações podem ser encontradas na internet, telefones celulares e computadores, ou qualquer outro dispositivo que armazene bits e bytes. Este contexto revela o conceito central de todo este trabalho - Prova Digital (PD). São informações que podem ser extraídas de qualquer dispositivo eletrônico, seja local, remoto ou virtual. Também inclui redes de comunicação. A PD também pode ser interpretada como informação que possui valor probatório e é armazenada ou transmitida em formato binário. Essa perspectiva é baseada em fontes internacionais.

A prova digital agora é um tema de grande valor, uma vez que dispositivos eletrônicos ou a própria internet são as ferramentas mais populares para armazenar dados e informações. A coleta e análise de evidências digitais de PD tem se tornado uma importante ferramenta na solução de crimes devido aos significativos avanços tecnológicos das últimas duas décadas.

Acredita-se, portanto, que este novo método de prova, que agora está incluído na lista de crimes cibernéticos das principais preocupações sobre a taxa de criminalidade no país, é um passo necessário na busca por soluções jurídicas.

A evidência digital é crucial para descobrir a verdade por trás do número crescente de crimes. No entanto, deve-se alertar que pode representar um risco se os limites para sua obtenção não forem claros e que não esteja sujeito a um controle rigoroso devido à sua natureza, como se apresenta ou ao método de apreensão.

Foi face à necessidade de tratamento específico, a Lei do Cibercrime foi criada em resposta à esta urgência, principalmente em relação à obtenção de provas digitais. Estabelece aspectos substantivos, mas também regulamenta medidas que buscam descobrir a verdade material e preservar as evidências digitais.

Apesar de sua atual relevância e de algumas regulamentações legais, no entanto, o tratamento de evidências digitais e evidências com essas características (especificamente correio eletrônico e evidências de mensagens curtas) continuam a ser um tema para discussões interessantes e controversas em doutrinas e jurisprudência.

Essa realidade digital também confronta a realidade jurídica. É importante lembrar que os agentes criminosos permanecem invisíveis e indetectáveis pelas agências de aplicação da lei. Muitas vezes, é difícil encontrar a identidade do autor do crime devido ao anonimato e ao fato de o crime cibernético ser praticado online, o que dificulta a coleta rápida de evidências. É claro que o combate ao crime cibernético tem grandes desafios. Isso ocorre porque os agentes criminosos estão cada vez mais se voltando para a internet para praticar crimes. Eles podem ser anônimos e não deixar rastros.

Espera-se que isso torne a Lei mais necessária do que nunca para garantir a ordem e a harmonia social em uma sociedade mundial em constante mutação. Mesmo que se trate de uma previsão, é claro que a prova é o cerne do processo declaratório. A dificuldade da prova dependerá dos fatos a serem comprovados ou do local onde se realiza (dificuldade objetiva), podendo ser devido a uma das partes ter mais dificuldades relativas (dificuldade subjetiva). Cada tema é mais complexo e frequente. A dificuldade (ou mesmo impossibilidade) de provar certos fatos pela onerada parte processual passa a chamar a atenção de doutrinas e jurisprudências.

A interpretação e aplicação da Lei da Cibercriminalidade em Portugal e outras normas relevantes na área têm suscitado questões na jurisprudência portuguesa. Estas incluem dúvidas quanto à articulação da Lei do Cibercrime com o Código de Processo Penal e também a compatibilidade entre o regime jurídico de conservação

dos dados gerados no âmbito das comunicações eletrônicas (Lei n.º 32/2008, de 17 de julho), com a Lei da União Europeia.

Assim, a necessidade de ser eficiente na busca por provas é um indicativo de uma sociedade onde a informação flui em um fluxo constante, graças a todos os avanços científicos e tecnologias de ponta. A informação está disponível com um clique, todos os cidadãos têm acesso e a mudança é constante. A sociedade da informação de hoje é marcada pela rápida modificação e distribuição de informações. Isso permite romper com o que era irrefutável e certo.

Nesse sentido, a presente dissertação tem por objetivo tratar do tema da prova digital no contexto Portugal-Brasil através das normas que regulam essa matéria, bem como apresentar as principais problemáticas de compatibilização e interpretativas delas decorrentes, utilizando-se da doutrina e jurisprudência dos países de modo a encontrar a melhor forma de investigação e combate a cyber criminalidade sem prejudicar de forma abusiva os direitos fundamentais das pessoas em prol da busca da verdade e punição dos culpados.

METODOLOGIA

O procedimento metodológico de pesquisa para elaboração do presente estudo foi o bibliográfico com pesquisa em materiais secundários compostos por livros, sites institucionais, legislação, jurisprudências, teses, dissertações e artigos encontrados em repositórios acadêmicos como o Scielo, Google Acadêmico, Google Books e banco de teses digitais de diversas faculdades que possibilitaram responder o objetivo proposto.

Para localizar acertadamente os materiais foram empregados os termos de busca: prova, prova digital, cyber prova, crime informático, crime digital, crime eletrônico, hacker, cracker, pericial, perícia, meios de obtenção de prova, prova documental, expedita de dados e injunção para apresentação. Foi dado prioridade para materiais com não menos de 10 anos de publicação, os quais compuseram 84% dos referenciais pesquisados.

1 CONCEITO DE PROVA (A SUA NATUREZA/ FUNÇÃO)

Seja pela presença na realidade dos indivíduos, seja pela relevância nos processos, o Direito tem nas discussões sobre a prova um dos temas mais importantes de seu campo de conhecimento.

O termo “prova” vem do latim “*proba*”, representando um conceito de múltiplos significados nas linguagens corrente e jurídica. Nesta última, prova geralmente se refere a três entendimentos: 1) atividade, isto é, o desejo de se provar algo; 2) resultado, ou seja, algo que já foi provado; e 3) meio, no sentido da forma com que a prova vai ser realizada. A partir desses três sentidos, fala-se em atividade probatória, em resultado advindo da atividade e da forma pela qual ela foi elaborada (Oliveira, 2014).

De maneira empírica, entende-se do verbo “provar” o ato de certificar a veracidade de um acontecimento ou fato. Já etimologicamente, o termo substantivo de origem latina significa “correto”, “honesto”, e o seu verbo – “*probare*”, em latim” – diz sobre “provar honestamente” (J. J. M. Martins, 2015).

Segundo João José Marques Martins (2015), a prova traz os fatos em sua realidade, desenhando o contexto da circunstância, servindo também como base para formar convicções. De um lado, há a realidade demonstrada dos fatos e, do outro, há a aceitação crítica dessa demonstração conforme os acontecimentos são evidenciados. Portanto, são dois destinos que caminha para uma única função.

Em uma concepção de atividade probatória, o direito processual entende a prova como uma série de ações cujo objetivo é verificar e demonstrar evidências que auxiliem a concluir a veracidade dos acontecimentos. Desse modo, o conceito de prova abarca a produção dos meios e atos realizados no processo com a intenção de convencer o juiz sobre a verdade ou inverdade de uma alegação mediante aos fatos relevantes para a solução do caso em questão (Lima, 2013).

Santos (2017) complementa explicando que, muito embora o Código Civil, em seu segundo capítulo – que trata das provas – não abarca a prova por presunções. O art. 341º do referido documento estabelece que a função das provas é demonstrar a realidade dos fatos.

Entende-se, então, que no campo judicial, a discussão ultrapassa o enquadramento jurídico do caso concreto, sendo que o esforço das partes é comprovar os fatos que compõem o seu direto, ou, de modo contrário, provar os fatos

que impedem, modificam ou extinguem o seu direito, de modo a demonstrar a procedência, no primeiro caso, ou a improcedência de uma ação, no segundo caso.

É de conhecimento generalizado a necessidade de, em juízo, se produzir provas que sustentem a pretensão das partes envolvidas, compreendendo que a verdade não basta, demandando uma demonstração competente da mesma para que se consiga alcançar uma conclusão favorável e a efetivação dos direitos (Fidalgo, 2015).

Como discorrido anteriormente, o conceito de prova pode apresentar mais de um sentido, sendo distintas as formas pela qual a prova surge, quais sejam como actividade probatória, como resultado probatório ou como meio de prova (Guerra, 2016).

Sobre esta última forma, Santos (2017) explica que seria tudo aquilo que se mostra útil para se alcançar um resultado específico, seja por meio de uma coisa, uma atividade ou um fato. Desse modo, o entendimento do meio de prova é um tanto quanto vago, não estabelecendo muito rigor no conceito de prova.

O já mencionado art. 341º do Código Civil recorre ao entendimento da prova como resultado, entendendo-a a partir daquilo que se almeja alcançar por meio da produção de prova em um grau específico de verdade a depender dos padrões sociais estabelecidos. A função da prova-resultado é muito significativa na fundamentação da decisão do juiz (C. B. C. H. Martins, 2015).

Retornando à definição de prova, Mendes (2014a) a entende a partir de duas noções: 1) a de atividade probatória; e 2) a de resultado dessa atividade. Soares (2014) complementa afirmando a importância de diferenciar o conceito de prova nesses dois entendimentos, já que a finalidade desta é demonstrar a realidade dos fatos.

Nessas perspectivas, a prova enquanto atividade probatória é a forma pela qual os fatos relevantes para a determinação de uma ocorrência, para a punição do responsável e para o estabelecimento de sanções são demonstrados (Mendes, 2014a). Desse modo, todos os fatos que se enquadrem nessa noção constituem objeto de prova. Já a prova como resultado da atividade probatória, segundo o mesmo autor, refere-se aos motivos da convicção que dão base às decisões da entidade responsável, desde que tal convicção esteja fundamentada nos elementos apresentados no processo e siga os princípios da experiência, da ciência e da lógica (Mendes, 2014a).

Vê-se, portanto, a polissemia do conceito de prova, sendo que, para alguns processualistas, pode até mesmo ter interpretações equivocadas. Ao falar de prova, pode-se referir à atividade probatória, isto é, como o conjunto de ações que buscam estabelecer a veracidade ou a inverdade dos fatos. Pode-se também tratar do

resultado ou do meio de prova, este último muito difundido na doutrina, vendo-a como fonte, ou seja, documentos, inspeções, exames etc. (Marques, 2015).

Manuel de Andrade (2004) discorre que todo elemento que pode dar base à convicção da entidade decisora acerca dos fatos de uma causa pode ser entendido como prova. Alguns autores a veem apenas como as coisas corpóreas, isto é, as testemunhas, o perito, os documentos e demais corpos físicos que possibilitam ao magistrado uma percepção direta ou indireta sobre os ocorridos. Há também, na doutrina, o entendimento da prova como a própria percepção do juiz sobre o material probatório, como os conteúdos dos documentos, as afirmações dos peritos e as alegações em depoimentos.

As provas que foram apresentadas contra o arguido são avaliadas pela autoridade judiciária a fim de definir a culpabilidade ou a inocência do agente que será declarada em julgamento, estabelecida a partir da suficiência dos indícios reunidos para determinar se a conduta se enquadra nos elementos típicos da norma incriminadora e, em caso positivo, o arguido se tornará alvo de sanções (Pina, 2015).

De um lado, portanto, está a verdade do material apresentado vinculada ao objetivo do processo, sendo a produção de provas, a avaliação dessa verdade e o poder do juiz os alimentos da investigação. Do outro lado, estão a verdade formal e a conclusão do processo, entendendo que não há possibilidade da reconstrução absoluta da realidade. Desse modo, o processo apresentará um resultado que tem como base a verdade possível a partir da análise das evidências apresentadas (Carnelutti, 2005).

Compreende-se, assim, a multiplicidade e a possível controvérsia nos entendimentos do conceito de prova na doutrina. Contudo, para a definição de um conceito atual, é fundamental que perspectivas já superadas sejam excluídas a fim de que o entendimento seja compatível às percepções contemporâneas do direito (Marinoni & Arenhart, 2013).

Afirma-se, então, a impossibilidade de se enxergar a prova como um meio para a formação de uma certeza dos acontecimentos ou para alcançar a verdade absoluta dos fatos, já que se entende que a apresentação de provas processuais não é capaz de reconstituir uma situação em sua completa realidade, de modo a eliminar quaisquer dúvidas acerca da convicção formulada (Debona, 2017).

Nesse sentido, Marinoni e Arenhart (2013) explanam que a prova se resume em caráter argumentativo e retórico, no entendimento de que ela justifica a opção por uma das teorias defendidas no processo. Em outras palavras, a prova é um meio pelo qual o juiz constrói sua convicção acerca da causa.

A importância em se entender esse cenário está no fato de que a estrutura do processo penal é acusatória, mas demanda que se embase no princípio da verdade material ou da investigação. A entidade acusadora, portanto, não é a mesma que julga, cabendo à acusação definir o objeto do julgamento. Não existe um verdadeiro ônus da prova no processo penal (Jesus, 2011).

Por outro lado, Germano Marques Silva (2000) apresenta a definição do princípio de prova presente no art. 32 da CRP, que trata da presunção de inocência. Nesse documento, argumenta-se que quaisquer condenações devem ser advindas de uma atividade probatória por parte da acusação, sendo que a responsabilidade do arguido deve ser comprovada de forma sólida, sendo que não cabe ao acusado a necessidade de provar sua inocência. Não se deve, portanto, desconsiderar o direito do arguido à presunção de inocência de modo a prejudicá-lo moralmente ou socialmente. O processo penal, desse modo, exige a apresentação de todos os meios de prova suficientes para demonstrar a existência do delito e a necessidade de determinação de sanções aplicáveis em crimes comprovados.

Nesse cenário, tem-se que o momento de produção de provas se dá na fase processual da instrução, quando as partes podem apresentar em juízo todos os elementos probatórios que demonstrem a veracidade dos fatos relevantes ao caso (Carreira, 2016).

O Novo Código de Processo Civil (NCPC) regulamenta em sua Parte Geral, Livro II, Título V, os atos de instrução de modo a estabelecer a dinâmica do processo em primeira instância. O processo é apresentado em seu conteúdo mínimo e, então, os sujeitos da instância devem preencher o processo concreto com os elementos fundamentais para a sua conclusão (Faria & Loureiro, 2013).

A fase instrutória tem seu início assim que a lei prevê a indicação dos meios de prova como pertinente e, com base no NCPC, estes devem ser apresentados juntamente aos articulados (Valles, 2014).

No entanto, existe a possibilidade de o início da atividade instrutória venha antes do momento da instrução, o que ocorre em situações em que há produção antecipada de prova, conforme previsto no art. 419º do NCPC, ou nas quais as partes apresentem as provas documentais ainda na fase dos articulados, segundo o art. 423º, n.º 1, do mesmo documento. Cabe ressaltar que, embora essas situações evidenciem atos introdutórios fora da fase de instrução, não se dispensa o vínculo entre eles (Carreira, 2016).

Há distinção entre o conceito de prova ou elemento de prova e o indício para os efeitos de normas relacionadas ao inquérito e instrução. A prova é um fato que se difere do fato a ser provado, no entanto o releva de maneira direta ou indireta, sendo,

portanto, os vestígios da ocorrência do fato. Elas são analisadas a partir das regras e leis específicas que asseguram a verificação e a certeza judiciária (Tonini, 2000). Isto posto, cabe ressaltar que, no caso de suficiência de indícios, são classificadas três posições, conforme Pina (2015):

- A probabilidade mínima de condenação, com acusação ou pronúncia manifestamente fundadas, sendo um critério sem acolhimento da jurisprudência na atualidade;
- A probabilidade maior de condenação se comparada à probabilidade de absolvição, quando a primeira tem manifestação de mais de 50%. Nesse critério, entendem-se como indícios suficientes a admissão de provas no processo que possibilita o estabelecimento de sanções ao arguido;
- A probabilidade forte, quando a possibilidade de condenação do arguido é elevada. Ocorre quando, a partir dos indícios levantados pela acusação, é possível considerar como muito provável a condenação do acusado, sendo muito inferiores as possibilidades de absolvição.

No sistema acusatório brasileiro e português, a atividade probatória é de responsabilidade dos participantes do processo, quais sejam, o Tribunal, o Ministério Público, o arguido, os assistentes e as partes civis e há a ressalva de que ela não pode ser desenvolvida a qualquer custo. Em outras palavras, isso significa que não é de natureza absoluta o direito à prova, visto que esse é um direito que convive com demais direitos e, por isso, apresenta limitações. Nesse sentido, não são admitidos meios ilegais (quando vão contra às normas do direito processual) ou ilícitos (quando contrariam regras de direito material) para a obtenção de provas (Silva, 2015).

Inclusive, conforme explica Fidalgo (2009), em Portugal, o Ministério Público, no decorrer da etapa de inquérito, não só tem que recolher provas relacionadas à prática do crime mas decidir qual será a determinação da concreta medida da pena, assim como se fosse o juiz e estivesse na etapa do julgamento. Assim, é possível observar que o Minitério Público, para que consiga fazer a aplicação desta forma de processo especial, acaba tendo um trabalho muito maior do que apenas o de investigar a ocorrência do crime e seus respectivos agentes, de forma que consiga posteriormente fazer o arquivamento ou acusão.

Não é intenção deste estudo encerrar a discussão sobre os tipos de prova e suas classificações. Admite-se, aqui, os critérios determinados pela doutrina majoritária, que as categorizam segundo o sujeito, o objeto e a forma. São quatro critérios, sendo aqueles relacionados 1) às provas real e pessoal; 2) às provas direta e indireta; 3) às provas literal, testemunhal e material – que se dividem em provas pré-constituídas ou constituenda –; e 4) às provas livre e legal.

1.1 Prova pessoal e prova real

Há, por parte da doutrina, uma diferenciação entre a prova real e a prova pessoal, sendo que, na real, o elemento usado para firmar uma convicção está em uma coisa e, na pessoal, a fonte de prova é uma pessoa. Nos dois casos, há o objetivo de influenciar a instância de decisão a um entendimento da causa (Correia, 2015).

Como prova pessoal, enquadram-se os meios que recorrem a pessoas para falar sobre fatos relevantes para a determinação da verdade, como se vê em depoimentos indiretos e em testemunhos. Como prova real, entendem-se os objetos utilizados para estabelecer a realidade dos acontecimentos (Gíria, 2017).

Nesses tipos de prova, são admitidos, portanto, os testemunhos e depoimentos, documentos elaborados por pessoas, como perícias e declarações, bem como elementos orgânicos, como amostras sanguíneas, DNA, exames físicos dentre outros (Assis, 2019).

1.2 Prova directa (imediata) e indirecta (mediata/representativa)

Quando entre o fato a ser analisado e o juiz não existe nenhum elemento que se interpõe, tem-se a prova direta (ou imediata); já no caso contrário, quando há algo ou alguém entre o juiz e o fato, fala-se em prova indireta (ou mediata ou representativa). Em outras palavras, as primeiras são aquelas que demonstram diretamente o fato a ser apresentado ao juiz, e as segundas são aquelas que não representam por si o fato a ser comprovado e, portanto, demandam mediação de outros fatos.

As provas indiretas, desse modo, se apresentam como indícios, também sendo denominadas provas críticas, nas quais predominam as presunções, em que se parte de um fato conhecido para comprovar um fato desconhecido. Elas são chamadas de representativas ou históricas quando o fato analisado pelo tribunal representa o fato que almeja ser provado (Rodrigues, 2020).

De maneira resumida, pode-se dizer que, em provas imediatas, o juiz recorre à sua própria percepção de forma direta e, para as provas mediatas, a percepção não basta, sendo necessários instrumentos outros, como as regras da experiência e o raciocínio (Nogueira, 2016).

Alberto dos Reis (2012) acrescenta que na prova direta, não há elementos entre o fato a ser apurado e a instância de decisão, isto é, há contato direto entre o juiz e o objeto da prova. É o caso, por exemplo, da insperação judicial, prevista em lei, na qual o juiz recorre à sua própria percepção para a análise dos fatos.

Esses dois tipos de prova demandam a percepção e raciocínio do juiz para a conclusão da existência ou não de uma ocorrência, no entanto há variação no uso desses elementos entre as provas mediatas e imediatas (Correia, 2015).

Vê-se, portanto, a parte do exposto anteriormente, que as fontes de prova também podem ser diferenciadas entre as representativas, ou históricas, e indiciárias, ou críticas, ambas incluídas no rol das provas indiretas.

1.2.1 Prova representativa e prova indiciária

Aquelas fontes de prova das quais é possível retirar uma dedução sobre a realidade do fato reportado na história são as chamadas provas representativas. Nelas, o fato a ser provado está representado, registrado ou reproduzido, referindo-se a uma representação de um acontecimento do passado relevante ao crime, a qual se busca demonstrar a partir da análise do conteúdo histórico registrado em algum tipo de documento. De modo resumido, entende-se a prova histórica, ou representativa, como aquela que recai não sobre o fato que se pretende provar, mas sobre o fato que o representa (Correia, 2015).

Sobre a prova indiciária, diz-se que é nela, mais do que nas demais, que a lógica e a inteligência do juiz se faz mais presente. Essa prova pressupõe um fato apresentado a partir de uma prova direta e, a ele, associam-se as regras da experiência, da ciência ou do senso comum. Por meio do fato indiciante, há o desenvolvimento de um fato consequente, estabelecido pela racionalização e pela lógica (Cabral, 2012).

A diferença entre as provas direta e indiciária está no grau de confiança transmitido por cada uma. Predominantemente, a doutrina entende que a prova indiciária, quando aplicada corretamente, permite o estabelecimento de uma condenação. No Ac. TRG de 19/01/200925, Cruz Bucho discorre que este tipo de prova tem se mostrado muitas vezes como o único meio de esclarecer os fatos em situações de criminalidade organizada, o que tem se visto em diversos países que seguem um ordenamento jurídico próximo ao de Portugal (E. L. R. Gomes, 2017).

A admissão de recurso a este meio de prova já era prevista no Ac. TRC de 11/05/2005, quando se constatava a ausência de prova direta. Nesse mesmo caminho, o Ac. TRC de 21/03/201227 determina que, apesar de não haver referências a requisitos especiais na lei processual no que se refere aos requisitos da prova indiciária, o estabelecimento de sua credibilidade é determinado pela convicção do juiz que, mesmo sendo de caráter pessoal, deve estar sempre fundamentada na objetividade. Contudo, a consideração da prova indireta exige a obediência a requisitos indispensáveis, como a existência de diversos dados indiciários

comprovados e credíveis e a racionalidade da inferência alcançada, de modo que o fato consequente advenha de uma racionalização lógica dos fatos que o embasam (E. L. R. Gomes, 2017).

Observa-se nos casos espanhol e italiano, que a jurisprudência e a doutrina desses países trazem solução parecida no que diz respeito à prova indiciária. Na jurisprudência espanhola, inclusive, lê-se requisitos aos quais é necessário dar relevância, como a obrigação de os indícios estarem comprovados por provas diretas, a necessidade de haver uma pluralidade de indícios que apontem para um sentido equivalente, a exigência por um nexo de causalidade entre os indícios comprovados e os fatos deles deduzidos e, principalmente, a obrigatoriedade de que a sentença exposta pelo Tribunal apresente por completo o raciocínio que levou à condenação do arguido, sendo este o chamado dever de fundamentação (E. L. R. Gomes, 2017).

Também preveem o recurso a presunções que levem a conclusões sobre os fatos, havendo exceção apenas quando se tratem de questionar os fatos de natureza duradoura existentes na própria fonte de prova. Nesses casos, a prova indiciária atua como fonte de prova direta.

Portanto, o juiz pode atribuir valor a todas as provas produzidas no processo, sendo elas diretas ou não. Cabe a essa autoridade, então, dar bases sólidas para a sua decisão, evidenciando o raciocínio lógico utilizado para determinar suas decisões.

1.3 Prova pré-constituída e prova constituenda

Entende-se como prova pré-constituída aquela que precede ao processo, sendo sua origem desprendida do surgimento do litígio. Desse modo, ela não está diretamente vinculada ao processo, mas dele passará a fazer parte quando apresentada por uma das partes envolvidas.

Portanto, em outras palavras, esse tipo de prova é anterior ao momento da necessidade de sua apresentação em juízo, sendo produzidas antecipadamente, ou sendo provas documentais ou *adperpetuam rei memoriam*. Já as provas constituendas são, ao contrário, aquelas produzidas em juízo, elaboradas e apresentadas quando se tem a necessidade de demonstrar a veracidade de um fato. Entre elas, estão a prova pericial, a prova testemunhal e a prova por inspeção judicial (Rodrigues, 2020).

Lucinda Maria Duarte Dias da Silva (2017) contribui esclarecendo que as provas pré-constituídas são caracterizadas por não serem produzidas na ação pendente. Desse modo, a sua produção não demanda nenhum tipo de atividade preparatória na instância, apenas a regulação da forma e do momento em que será apresentada e incluída no processo. Ou seja, a instrução desse tipo de prova consiste, sobretudo, na atividade de apresentação ou incorporação da mesma na ação em curso.

Nesta senda, caso à parte atingida pela prova pré-constituída apresentada não foi possibilidata a oportunidade de impugnação de admissibilidade da mesma, poderá esta ser considerada invalidamente constituída (Carreira, 2016).

Carreira (2016) ainda acrescenta que tratam-se de provas obtidas legal ou ilegalmente e que levantam questionamentos sobre a admissibilidade de seu uso devido à própria natureza delas, pois há a possibilidade de ferirem direitos fundamentais quando exibidas nos processos, como no caso da exposição de cartas pessoais e diários íntimos, por exemplo.

Por outro lado, a prova constituenda é produzida ao longo do processo, isto é, só se forma o meio de prova após constatada a necessidade de se comprovar determinado fato. A prova testemunhal é o caso paradigmático desse tipo de prova, pois sua produção só se dá a partir do testemunho, não existindo antes desse a prova, somente o meio de prova (Oliveira, 2014).

Então, é a partir da necessidade da prova que surge o meio de prova neste último tipo, sendo, então, resultante de pendência do processo em sua atividade probatória. Em comparação entre a prova pré-constituída e a prova constituenda, o mecanismo de inclusão desta é mais complexo (Marques, 2015).

1.4 Prova livre e prova legal

A diferenciação entre as provas livre e legal diz respeito ao modo pelo qual a convicção do juiz acerca da prova produzida ou incluída no processo se forma. A origem do sistema de prova legal é germânica, sendo sua vigência até o século XIX. Trata-se de prova legal quando sua força e valorização se fundamental em critérios taxados e formalizados pelo legislador, não restando ao juiz possibilidade de valoração discricionária. Nesse caso, não há contestação ao êxito da prova (Marques, 2015).

A primeira aparição do sistema de prova livre, por sua vez, foi no direito romano e retornando apenas com a ascensão do processo civil moderno, já no final do século XIX. Esse tipo de prova se caracteriza pelo fundamento do julgador em suas convicções pessoais para a valoração e apreciação da prova. Ou seja, de modo oposto ao tipo de prova legal, esta é analisada em plena liberdade pelo juiz, em um contexto que privilegia mais a justiça do que a certeza. Muito embora esse seja o modelo vigente no ordenamento jurídico-processual, ainda se encontram manifestações do sistema de prova legal (Marques, 2015).

Sousa (1995) se dedica a comparar esses dois tipos de prova e, a partir de seus estudos, apresenta uma diferenciação que pontua que a prova legal desvia a administração da justiça da verdade material, contudo estabelece uma decisão de fácil verificação, já que, nesse caso, o juiz assume a função de verificar formalidades;

enquanto a prova livre afasta administração da justiça e verdade formal, mas demanda meios estabelecidos de controle da decisão. No entanto, há casos em que o sistema de provas livres precisa abrir espaço para o princípio da prova legal, como em situações de prova por confissão ou por documento autêntico, por exemplo (A. M. Silva, 2019).

Compreende-se, então, que aquela prova cuja apreciação em juízo é feita em completa liberdade é a chamada prova livre, não podendo esta ser entendida como uma prova arbitrária. A liberdade em excesso é contida a partir de uma fundamentação da decisão. Não há uma lei que delimite o valor de cada prova, cabendo ao juiz valorar e edificar sua convicção, no entanto esta deve ser embasada em experiência, em conhecimentos técnicos e científicos e nas regras da razão e da lógica, elementos que devem indicar a motivação da decisão tomada.

1.5 Novidade da lei n.º 41/2013, de 26 de junho: prova por verificações não judiciais qualificadas

O Código de Processo Civil sofreu diversas alterações. A Lei n.º 41, de 26 de junho de 2013 trouxe inovações que despertaram certas perplexidades e curiosidades. Os questionamentos em torno das referidas inovações dizem respeito, sobretudo, aos novos meios probatórios, quais sejam, à prova por declarações de parte e às verificações não judiciais qualificadas (Cabral, 2017).

De acordo com o NCPC, a parte pode se propor a oferecer declarações acerca dos fatos envolvidos na causa dos quais tenha conhecimento ou contato direto. Conforme o documento, essas afirmações entram na regra da livre apreciação da prova pela autoridade de decisão, exceto nas situações em que tais declarações assumam caráter de confissão, as quais demandam cumprimento dos termos referentes às provas por confissão (C. B. C. H. Martins, 2015).

Cabe mencionar que a possibilidade de declaração em juízo pelas partes foi tema de diversas análises doutrinárias e jurisprudenciais antes desta ser estabelecida como alteração no NCPC, o que pode ser motivo para um consenso sobre a questão (Fidalgo, 2015). Importa ressaltar ainda que, anteriormente, essa possibilidade não só não era legalmente prevista como também se caracterizava como uma controvérsia doutrinal e jurisprudencial (C. B. C. H. Martins, 2015).

Como mencionado no início deste tópico, a prova por declarações de parte (também chamada de prova por confissão das partes) se estabeleceu em 2013 a partir de uma reforma legislativa. É uma alteração que se mostrou interessante por seu caráter inovador e pelo intenso campo de debates que proporcionou, demonstrando a

relevância que assumiu esse processo de reformulações no processo civil que alterou o paradigma jurídico em vigência.

Muito embora a prova por declarações de parte tenha sido aprovada, prevista no art.º 466 do referido documento, os motivos que levam aos questionamentos dessa possibilidade não foram esquecidos, sendo este um dos maiores obstáculos para que tal inovação não seja vista como uma solução controversa e alvo de críticas (P. A. F. M. A. Martins, 2015).

Por fim, Gonçalves (2018) complementa que há uma subdivisão em dois meios de prova para o regime processual de produção de prova oral pelas partes, sendo elas o meio de prova por depoimento de parte e o meio de prova por declaração de parte. O primeiro objetiva alcançar a confissão, sendo que não foi um meio concebido pela legislação a fim de versar sobre fatos favoráveis àquele que depõe, prevendo-se, para esta situação, os meios de declaração. Geralmente, o que se constata é que o depoente, além de negar os fatos que o prejudicam, ainda inclui a versão que o favorece.

A divergência quanto ao aproveitamento desse tipo de produção de prova foi acentuada pelas recentes modificações na legislação. Desde a inclusão da possibilidade de depoimento e declaração de parte, tem-se debatido quanto ao aproveitamento de todo depoimento como prova, mesmo quando da parte favorável, a partir de uma interpretação sistemática conjugada. Esse fato indica que a prova por depoimento de parte pode ser ultrapassado a sua finalidade específica de caráter confessório (Gonçalves, 2018).

Tais controvérsias sobre a aplicação do regime de prova por depoimento de parte e por declarações de parte incumbiu a jurisprudência e a doutrina a missão de criar meios que proporcionem soluções às questões encontradas.

2 FUNÇÃO E FINALIDADE DA PROVA

Compreendendo que o objetivo maior da prova é convencer o juiz quanto aos fatos apresentados pelas partes, entende-se o magistrado como principal destinatário da prova. Desse modo, o processo deve ser visto como destino e não como destinatário, adotando o sentido de destino como local e de destinatário como pessoalidade (Melo Junior, 2016).

Ainda nesse sentido, pondera-se que, portanto, a demonstração da realidade seja o mesmo que a demonstração da verdade alcançável pelo juízo humano, isto é, uma certeza que terá como base a opinião, a convicção.

Nesse caso, sabendo-se que o convencimento do juiz é a finalidade da prova, quando isso não ocorre, a prova terá se mostrado inútil ao processo, no sentido de que não atingiu seu propósito (Debona, 2017).

No entanto, importa destacar que não se pode permitir que, na livre convicção do juiz, a certeza objetiva seja substituída pela certeza subjetiva, esta que é desvinculada as regras da lógica e das leis (Guerra, 2016). Desse modo, quando, no contexto do Direito, fala-se em convicção do juiz, diz-se da convicção objetiva como finalidade da prova, que segue a experiência e as normas legais que constituem o conteúdo de um direito probatório substantivo (P. A. F. M. A. Martins, 2015).

Não há uma definição concreta e direta de prova nas legislações penal e processual, sendo que o Código de Processo Penal, em seu art. 124º, se limita a definir o seu objeto, abarcando não apenas os elementos fundamentais do crime, mas todo o objeto do processo, o que significa que se considera tudo o que for alegado pelas partes (P. A. F. M. A. Martins, 2015).

Além disso, Debona (2017), discorrendo acerca da natureza jurídica da prova, explica sua divisão em duas categorias de prova: as materiais e as processuais. Essa classificação indica sentidos diferentes para cada categoria, sendo que a prova processual se refere de forma direta à atividade jurisdicional, no sentido da intenção de convencer o juiz acerca dos fatos.

Aqueles que defendem essa perspectiva da finalidade da prova argumentam que devem ser admitidos e valorados no decorrer do processo todos os meios de prova que podem ajudar a descobrir a verdade material, não importando, nesse sentido, se as provas se mostrem ilícitas, sendo mais interessante a sua relevância para a causa. Os que assim se posicionam entendem que a exclusão dessas provas do processo resultaria na rejeição de elementos necessários para a construção de uma convicção e, consequentemente, impedindo uma conclusão justa ao caso (Dinis, 2019).

É uma percepção, portanto, que assume a descoberta da verdade como finalidade maior da prova e, então, se uma prova ilícita não tiver seu valor lógico impactado por este fato, ela deve ser considerada, mesmo que não possa ser admitida em julgamento (Oliveira, 2014).

Segundo esse entendimento, a descoberta da verdade deve predominar em detrimento da proibição da obtenção de provas ilícitas, haja visto que essa ação é assegurada de sanções civis ou criminais ao responsável. Nesse sentido, defende-se que a prova ilícita deve ser incluída no processo e, em outro âmbito, a parte lesionada terá provido o seu direito de buscar os meios legais para defender os seus interesses (Dinis, 2019).

Desse modo, José Abrantes (1986) dispõe que o objetivo da prova é levar os fatos ao juiz, sendo que os resultados destas devem ser medidos a partir da noção da verdade, e não da moralidade. Por isso, no entendimento do autor, a meta da justiça deve ser prezar pela honestidade dos meios de prova, mas isso não deve impedir a utilização de provas alcançadas por determinados meios ilícitos. O valor violado para a obtenção desses resultados deve, sim, ser defendido, mas por meio das sanções legalmente estipuladas para tais ilicitudes, não admitindo, para essa defesa, o desenvolvimento de um julgamento falso.

Contudo, a descoberta da verdade por si só não basta para que provas ilícitas sejam admitidas em um processo. Os direitos, liberdades e garantias assegurados em um Estado de Direito não podem ser feridos em nome da busca da verdade, esta que deve se limitar aos princípios fundamentais do direito (Dinis, 2019).

2.1 Prova como actividade probatória (probatório)

Tanto no sentido comum quanto no sentido jurídico, provar algo significa levar à construção de uma convicção da verdade daquilo que é alegado. Em um processo civil, portanto, provar refere-se a expor à autoridade de decisão os elementos que lhe permitam a formação de um juízo de convicção sobre a veracidade dos fatos alegados ou contestados. Nesse sentido, entende-se a atividade probatória como um ato de convencimento.

Inicia-se, então, referindo-se à prova enquanto atividade probatória, ou, em outras palavras, como um conjunto de ações conectadas entre si que buscam conduzir à formação de determinada convicção pelo juiz.

Nesse cenário, portanto, qualquer campo do direito processual tem como característica pilar a atividade probatória em juízo relacionada aos direitos invocados. É uma atividade diretamente vinculada à busca por demonstrar a realidade dos fatos que cercam a matéria em discussão de modo a surtir em efeitos almejados pelas

partes a partir do estabelecimento de uma corrêspondência entre as verdades processual e material. Nessa linde, intenta-se que, por meio da realidade comprovada no processo, seja relatada a realidade ocorrida, o que alguns estudiosos nomeiam como princípio da verdade material (Santos, 2018).

Na atividade probatória, a prova assume o papel de garantir um juízo que se baseie na realidade assegurada por ela. A decisão final irá escrever a intervenção judicial, os juízos de fato e os juízos de direito, sendo que, por regra, o estabelecimento da sentença será determinado pelas provas produzidas e apresentadas no processo (P. A. F. M. A. Martins, 2015).

Ademais, a função garantística da prova não é a única, que também se presta a refutar a presunção de inocência, prescrita na Lei Fundamental, art. 32º, n.º 2. A sentença final será talhada a partir de um processo no qual a autoridade decisora revive e sente os acontecimentos apresentados (Beleza & Pinto, 2014). Uma sentença justa está necessariamente atrelada à verdade, que depende da melhor reconstrução dos fatos que seja possível alcançar por meio de provas. Nesse sentido, a decisão final se fundamenta na certeza dos fatos e na convicção do juiz a partir desta. Chama-se de prova, então, o conjunto dos motivos que geram tal certeza (Lima, 2009).

Outra visão da atividade probatória é apresentada por Lima (2009), que define o ato de provar como o processo de induzir a autoridade decisora a um convencimento da ocorrência de um fato história de modo ou forma determinados.

Então, é desenvolvida uma série de atos que possibilitem a formação de uma convicção pelo julgador a partir das demonstrações realizadas e, consequentemente, o estabelecimento de uma certeza sobre a realidade dos fatos por meio daquilo que é permitido concluir pelos meios de prova produzidos. A decisão do juiz deve, portanto, ser baseada sempre na apreciação das provas partindo de critérios objetivos e controláveis que justifiquem a motivação da sentença (Guerra, 2016).

Caso as partes não se empenhem em um mínimo de atividade probatória, não parece correto que os pressupostos no art. 411º, bem como em suas ramificações, serão preenchidos. Isso porque não há como a autoridade de decisão estipular diligências se não houver resultados nos autos que edifiquem sua convicção a respeito de uma causa. Nessa hipótese, impossibilita-se um critério lógico do juiz, visto que este só poderar ter dúvidas acerca da ocorrência de um fato quando se tenta demonstrá-lo. Entende-se que do vazio probatório não nascem dúvidas, mas da dialética das provas (Quintas, 2017).

Então, a vigência da autorresponsabilidade das partes determina que estas devem assumir o apontamento de elementos que convençam o juiz sobre a necessidade de se esclarecer um fato. Caso as partes não apresentem provas, cabe

ao juiz convidá-las a exercer a atividade probatória e, se isso não for suficiente, a autoridade deverá seguir a decisão de ônus da prova, ou seja, aquela que expõe a consequência da ausência de provas (Quintas, 2017).

Reafirma-se, nesta linde, que a busca da verdade material está estritamente vinculada ao princípio da descoberta da verdade material e da investigação, que diz que os elementos de fato imbutidos no processo por outros sujeitos processuais não limitam a atividade investigatória do tribunal, podendo este acrescentar ao processo circunstâncias outras que se mostrem relevantes (Eiras, 2008).

Desse modo, a atividade probatória se apoia nos fatos-base (factum probans), assumindo o papel de assentar os anseios do beneficiado pelo efeito de presunção a partir das provas que lhe competem, conforme precrito no Código Civil, art. 342º, n.º 1.

2.2 Prova como resultado probatório

A convicção construída pela autoridade decisora no processo que discute a existência ou inexistência de uma determinada situação de fato é a chamada prova como resultado (Manuel, 2015).

O resultado probatório prescrito legalmente é feito em vácuo, advindo os fatos comprovados não porque correspondem, de fato, à realidade, mas porque o legislador pretendeu dessa forma. Não se questiona sobre a função do juiz pela busca da verdade material e, a partir dela, decidir em conformidade, não se pretendendo aos dispostos legais, mas motivado pelo convencimento da verdade (Rodrigues, 2020).

Sendo o resultado probatório obtido pelo juiz na análise dos fatos motivados, então isso se mostra suficiente para argumentar pela solução justa, mesmo que esta não siga a força probatória legal dos meios de prova. Contudo, essa liberdade só é beneficiada à entidade decisora em situações de conflitos positivos de meios de prova, o que significa que fatos contraditórios são revelados por meios distintos, mas de valor equivalente, de prova (Rodrigues, 2020).

Portanto, a verdade formal se refere ao entendimento de que aquilo que não consta nos autos, não consta no mundo, o que significa dizer que a verdade, nesse sentido, resulta da atividade probatória contida no processo, mesmo que não correspondam àquilo que ocorreu historicamente. Já a verdade real é aquela que corresponde aos fatos apresentados materialmente com os acontecidos. Esta última é a verdade pretendida pelo processo civil moderno (Miotto, 2015).

Assim, o que é previsto pelo ônus subjetivo é que cada parte é atribuída do ônus de comprovar no processo a matéria que cabe provar conforme determinado legalmente (Miotto, 2015). Vale pontuar que, no caso da obtenção de um resultado

mesmo sem o mínimo de atividade probatória, o ônus da prova é dispensado. Nessa situação, há liberação pelo legislador da demonstração de um fato (Beirão, 2017).

Nesse sentido, a verdade processual se apresenta como o resultado probatório do processo válido, ou seja, trata-se da convicção de que determinada alegação tem sua aceitabilidade justificada como motivação da decisão, sobretudo por ter sido produzida a partir de meios válidos. Importa ressaltar que não se vê a verdade processual como absoluta, mas como uma verdade judicial.

2.3 Meios de prova

No que se refere ao valor ou força probatórios, os meios de prova legal podem apresentar várias gradações, que variam entre provas pleníssima, plena e bastante conforme o grau de destrutibilidade do resultado alcançado pelos meios.

No tocante aos meios de prova, Fidalgo (2006) explica que estes "caracterizam-se pela sua aptidão para serem por si mesmos fontes do convencimento do juiz; são elementos que o juiz pode usar de modo imediato para fundamentar a sua decisão" (p. 134). Já no tocante aos meios para obtenção de prova, a autora explica que se tratam de instrumentos cujo objetivo é servir às autoridades judiciárias tanto para a própria investigação como para recolher os meios de prova.

Nesse contexto, o valor da prova pleníssima é indestrutível por quaisquer que sejam os demais meios. Então, depois de verificado o fato-base da presunção, não mais se admitem provas que contrariem o fato presumido verificado, ou seja, a denominada prova do contrário, prevista no CC, art. 350º, n.º 2, não obstante o fato-base ser atacável a partir da demonstração de incoerência. Desse modo, vê-se esse grau de prova como uma presunção irrefutável (Vaz, 2020).

Nessa gradação, estão incluídas as presunções *júris et de jure*, como, por exemplo, quando se presume de má-fé a posse adquirida por violência. Nesse caso, não há possibilidade de se refutar a presunção, no entanto é possível fazê-lo à sua base, sendo que a presunção é ilidida ao se provar que não se adquiriu a posse para violência (Rodrigues, 2020).

Nesse tipo de presunção, obedecendo às máximas da experiência, o legislador raciocina convictamente que, frente a determinadas situações, exclui-se a admissão de prova contrária. A consequência de impossibilitar o refuto da presunção é que o fato presumido argumentado pela parte beneficiada ganha valor jurídico de certeza mesmo quando não existem provas sobre o mesmo, assumindo o status de prova pleníssima. Então, uma vez que o fato-base é demonstrado, a própria lei, sem a exigência de quaisquer demonstrações críticas, dá por adquirido um outro fato (Santos, 2018).

A prova plena, por sua vez, permite a demonstração de outros meios de prova que contestem o fato presumido, ou seja, cede frente a apresentação de alegações da não veracidade do fato objeto, conforme previsto no CC, art. 347º, admitindo a prova do contrário. Excetuam-se os casos de restrição da referida demonstração, como constituem as provas plenas qualificadas. O Código Civil, em seu art. 344º, n.º 1, refere à prova plena, estabelecendo a inversão do ônus da prova em situações de existência de presunção legal, dando a essa prova a presunção ilidível (CC, art. 350º, n.º 2) (Vaz, 2020).

Então, no caso da prova plena, cabe à parte contrária demonstrar que a presunção já legalmente apresentada a partir de prova plena é falsa, atuando, assim, na inversão do ônus da prova. Entende-se, desse modo, que o que implica a inversão não é a presunção judicial, o que se diferencia é o fato objeto de prova (Santos, 2017).

A distribuição entre as partes do risco de que certo fato não seja provado é definido juridicamente pelas regras do ônus da prova, que imputa às partes o dever de comprovar os fatos que assim demandarem para que se alcance resultado satisfatório na causa. Diante de uma prova legal plena, esse ônus sofre uma inversão, tendo a parte atingida a responsabilidade de demonstrar de contradizer o fato apresentado. Vale destacar que é preciso convencer o julgador da não veracidade do fato em análise, não sendo suficiente apenas gerar dúvidas sobre ele (Santos, 2017).

Por fim, aquela que cede mediante simples contraprova é a denominada prova bastante. Nesse caso, apenas a dúvida do juiz quanto à realidade apresentada por prova confrontada com outros elementos é o suficiente, conforme destaca o art. 346º do CC. É, então, uma presunção legal que não resulta em inversão do ônus da prova (Vaz, 2020).

Apesar de serem constatadas diversas congruências entre os sistemas processuais observados quanto ao valor e avaliação das provas, o sistema português concede maior atenção às especificidades das provas e dos fatos, promovendo maior profundidade nas caracterizações realizadas nas decisões da justiça sobre os fatos da demanda e nas provas elaboradas. Há, no caso de Portugal, melhor detalhamento dos conceitos dos três tipos de provas apresentados neste tópico – provas bastante, plena e pleníssima. No contexto brasileiro, via de regra e não por falta de menção na legislação processual, é comum que essas distinções sejam feitas de forma genérica pelos juízes trabalhistas (Assis, 2019).

2.4 Prova difícil

Diante de uma prova difícil, restarão dúvidas impossíveis de esclarecimento. Nesse caso, ao se afirmar que a prova de um fato é difícil aponta a dificuldade de se

alcançar um grau elevado de persuasão no julgador sobre a realidade de um fato (Silva & Reis, 2013). O NCPC dispõe a teoria da distribuição dinâmica, cujo objetivo é solucionar a questão da prova diabólica, que não encontrou solução na distribuição estática, que reparte a prova entre as partes de forma rígida, entendendo que a prova é daquele que a alega. Dependendo do caso concreto, então, o ônus da prova é dinamizado ou invertido quando se torna demasiadamente difícil para uma das partes.

A relevância concedida ao tema prova se justifica pela importância e pela dificuldade da discussão. Nesse sentido, Silva e Reis (2013) afirmam que se, por regra, os temas de prova são difíceis, ainda mais o é o tema da prova difícil, pois envolve preocupações que se refletem tanto nas partes atingidas pelas regras rígidas do ônus da prova quanto no juiz que se vê diante de uma alegação não plenamente provada, mas sem razoabilidade para se exigir uma prova.

Em algumas ocasiões, será bilateralmente diabólica a comprovação do fato, o que significa que será impossível ou extremamente difícil para ambas as partes conseguirem prová-lo. Sobre isso, Bessa e Leite (2016) discorrem que essa situação é problemática, pois elimina a possibilidade de distribuição dinâmica do ônus da prova. Nesses casos, o juiz não deve manter o ônus da prova com quem alegou o fato, bem como não cabe a ele inverter o ônus na fase probatória. Didier Jr., Braga e Oliveira (2015) complementam que é possível que, em situações como essa, pode o juiz chegar ao fim da instrução sem atingir um grau mínimo de convicção e, portanto, sendo vedado o *non liguet*, tal dúvida levará uma das partes a arcar com as consequências desse estado.

3 OS MEIOS TRADICIONAIS DE OBTENÇÃO DE PROVA

Distinguir o direito probatório formal do direito probatório material é fundamental para se bem compreender a prova em sua totalidade. O Código Civil apresenta o direito probatório material, estabelecendo uma definição de prova, regrando a repartição de ônus da prova, definindo o objeto da prova e versando sobre a admissibilidade dos meios de prova, bem como sobre os critérios para valorar ou analisar as provas. Os meios de prova prescritos nesse documento são os típicos: a confissão, descrita nos arts. 352º ao 361º; a prova documental, versada entre os arts. 362º e 387º; a prova pericial, presente nos arts. 388º e 389º; a prova por inspeção, regulada pelos arts. 390º e 391º; e, por fim, a prova testemunhal, apresentada na redação dos arts. 392º ao 396º. São meios de prova que servem, excetuando alguns casos, para comprovar quaisquer fatos, configurando o denominado princípio da equivalência ou substituição mútua (Rodrigues, 2020).

Maia (2019) acrescenta a centralidade da vítima como fonte de prova relevante, visto que se vê como suporte do processo o depoimento por ela oferecido, ainda que lhe seja garantida a possibilidade de rejeição à prestação de depoimento, conforme descrito CPP, em seu art. 134º. Para tentar superar progressivamente isso, sempre que possível, o Ministério Público deverá cuidar do recolhimento de acervo probatório complementar com o recurso às provas indiciária ou indireta. Desse modo, acrescenta-se a prova pericial – com destaque às declarações das partes civis, do arguido e do assistente e à prova médica –; a prova por reconhecimento; a prova por acareação; a prova documental; e a reconstituição do fato, todos previstos no CPP. Importa dizer que, não importando o meio ou os meios de prova escolhidos, o recolhimento e a intervenção destes deverá ser realizada da forma mais ágil possível, de modo a atender ao seu caráter de crime prioritário, respeitando o que procede da Lei n.º 96/2017, em seus arts. 2º e 3º (Maia, 2019).

3.1 Prova testemunhal (art.º 128.º do CPP)

Primordialmente, a produção dos meios de prova se dá em audiência de julgamento, sendo a admissão de valoração de meios de prova produzidos anteriormente permitida apenas em casos excepcionais, conforme disposição do CPP, em seu art. 355º (M. V. P. Silva, 2017).

No que se refere às providências cautelares, o CPP, em seu art. 249º, n.º 2, atribui ao PSP a responsabilidade de coletar informações das pessoas que permitam a

reconstituição do crime e a revelação dos agentes envolvidos. As informações podem ser recolhidas em momentos e locais determinados, caso contrário, o êxito da investigação poderá ser comprometido (Sá, 2015).

A prova testemunhal se insere nesse contexto. O previsto no art. 128, n.º1 do CPP assevera que “a testemunha é inquirida sobre factos de que possua conhecimento direto e que constituam objeto da prova”. Nesse sentido, Francisco Marcolino de Jesus (2011) argumenta que a prova testemunhal se configura enquanto prova pessoal, na qual a ação é de uma pessoa que declara ou narra os fatos dos quais possui conhecimento. O modo de ação, nesses casos, é, portanto, a declaração. Segundo Sousa (2016), a prova testemunhal pode ser descrita como a declaração de conhecimento de alguém alheio à lide, cujo objeto da narração juramentada é um fato atual ou do passado do qual sabe o declarante direta ou indiretamente.

Então, observa-se a fundamental importância da prova testemunhal ao processo penal, pois é difícil que infrações sejam comprovadas unicamente com outros elementos de prova. Silva F. (2009) defende que a Justiça tem nas testemunham os seus ouvidos e olhos, pois é por elas que a autoridade de decisão ouve e vê os fatos analisados. Essa é uma realidade, principalmente, em casos de abuso sexual, em que, predominantemente, o único meio de prova é a testemunha e, justamente por isso, é preciso atentar de forma mais profunda aos riscos de falibilidade da declaração, haja visto que, em certas circunstâncias, a fragilidade humana frente aos seus interesses materiais e pessoais se mostra mais forte do que os princípios da verdade e da justiça (Silva, F., 2019).

Os fatos juridicamente relevantes em posse da testemunha são o objeto da prova testemunhal, como descrito no CPP, em seu art. 128º, n.º 1. Via de regra, o declarante tem posse de tais conhecimentos por ter visto ou escutado algo, mas não se eliminam os testemunhos obtidos a partir de outros sentidos, quando adequados ao que se pretende provar (Silva, 2009).

Há possibilidade do testemunho direto ou indireto, variando conforme àquilo a que se reporta, aos fatos probandos ou aos seus meios de prova, sendo este último caso informalmente chamado de ouvir dizer. A prova testemunhal abarca, portanto, o depoimento indireto, que é regulado no regime legal de prestação de prova testemunham como a declaração de uma testemunha sobre algo que ouviu de outro declarante (Albuquerque, 2009).

Em princípio, não há permissão para o depoimento indireto, entendendo-o como contradizente às exigências do princípio de imediação da prova e da contraditoriedade que caracterizam um processo penal de sistema acusatório. O depoimento indireto, então, só se justifica em casos extraordinários, como em circunstâncias de morte,

desaparecimento ou anomalia psíquica da testemunha (Albuquerque, 2009), fazendo com que a natureza do descrito no art. 129º seja excecional.

Nesse caminho, Sá (2015) acrescenta que o depoimento indireto, seja ele sobre aquilo que se ouviu de pessoas determinadas, como disposto no CPP, art. 129º, n,º 1, seja em reprodução de rumores ou vozes públicos, vide art. 130º, n.º 1 do mesmo documento, é proibido. No caso em que a testemunha ouviu alguém dizer alguma coisa relevante, há a possibilidade de o julgador convidar a pessoa a depor, mas, caso não o faça, não poderá o depoimento reproduzido atuar como meio de prova, com salvas exceções, conforme já mencionado. O art.º 131 do CPP discorre sobre a incapacidade de testemunhar em determinados casos, diferente do que dispõe o art.º 133 do mesmo documento, que trata do impedimento de declaração como testemunha em situações específicas.

Observa-se, portanto, que o CPP, a partir do seu art. 128º, apresenta um catálogo dos meios de prova cujo objetivo é assegurar a credibilidade à demonstração dos fatos em âmbito jurídico, impedindo, por exemplo, os testemunhos de ouvi dizer, bem como as declarações acerca do caráter, personalidade, condições pessoais e condutas passadas do arguido, como se vê no art. 291, n.º 4, acrescentado no CPP a partir da Lei n.º 59, de 1998. No entanto, há quem defenda o deferimento desse último tipo de testemunho, sobretudo em casos de crimes sexuais, entendendo que as inquirições referentes à personalidade dos arguidos podem indicar tendências que melhor evidenciem o caso e assegure de forma mais eficiente os direitos fundamentais das vítimas (Dias, 2014).

São aspectos fundamentais na fase de julgamento, que determinam o estabelecimento da sanção ou de medidas de segurança, de coação ou de garantia patrimonial. Por outro lado, não é necessário produzir-se prova com essa relevância ainda no momento indiciário, quando ainda se está decidindo se o arguido irá a julgamento.

Nesse sentido, o CPP, em seu art. 128º, n.º 2, estabelece que:

> [...] salvo quando a lei dispuser diferentemente, antes do momento de o tribunal proceder à determinação da pena ou da medida de segurança aplicáveis, a inquirição sobre factos relativos à personalidade e ao carácter do arguido, bem como às suas condições pessoais e à sua conduta anterior, só é permitida na medida estritamente indispensável para a prova de elementos constitutivos do crime, nomeadamente da culpa do agente, ou para a aplicação de medida de coacção ou de garantia patrimonial.

Cardoso (2015) complementa que, as provas coletadas no decorrer do processo são lidas e avaliadas nas fases do inquérito e da instrução, contudo elas podem ser descartadas no momento da audiência. Por exemplo, pode-se imaginar uma situação

em que uma testemunha tenha deposto na fase da instrução, mas se nega a testemunhar em audiência. É uma situação prevista pelo CPP, em seu art. 356º, n.º 6, que proíbe, nesses casos, a leitura do depoimento já realizado.

Os princípios descritos a seguir são aqueles que devem ser obedecidos no momento do recolhimento da prova testemunhal:

- Princípio da legalidade ou da legitimidade da prova, o qual está descrito no CPP de S. Tomé e Príncipe, no art. 198º, que admite quaisquer provas que não forem legalmente proibidas. De acordo com Alves (1997), tal princípio admite a inclusão de toda prova que não seja impedida por lei, mesmo que esta não esteja legalmente prevista ou que se mostre atípica;
- Princípio da investigação ou da verdade material, descrito no CPPSTP, art. 322°, sob o seguinte texto: “o tribunal ordena, oficiosamente ou a requerimento, a produção de todos os meios de prova cujo conhecimento se lhe afigure necessário à descoberta da verdade e à boa decisão da causa”. Em sentido equivalente, o art. 299º, n.º 3, do mesmo documento trata dos poderes e deveres atribuídos ao presidente de audiência do tribunal, cujo objetivo é descobrir a verdade. O princípio também é explanado nas redações dos arts. 33º, 231º, 250º n.º 1, e 283º n.º 3 (Boa Morte, 2017);
- Princípio da livre apreciação da prova, disposto no CPPSTP, art. 200º, in verbis: “Salvo quando a lei dispuser diferentemente, a prova é apreciada segundo as regras de experiência e a livre convicção da entidade competente”. Para Castanheira Neves (1968 citado em M. A. M. Silva, 2000), a liberdade mencionada nesse princípio não equivale a uma decisão irracional, pautada na emoção e impressão do julgador, visto que ela precisa ser fundamentada;
- Princípio da presunção de inocência, abordado no CRSTP, art. 40º, n.º 2, na Convenção Europeia para a Proteção dos Direitos e Liberdades Fundamentais, art. 6º, n.º 2, bem como na Declaração Universal dos Direitos dos Homens, em seu art. 11º (Silva, 2008). Além disso, também se dispõe sobre o referido princípio no Pacto Internacional de Direitos Civis e Políticos, em seu art. 14º, n.º 2, que versa que “toda a pessoa acusada de crime tem direito a que se presuma a sua inocência enquanto não se prove a sua culpabilidade, em conformidade com a lei”; “é um verdadeiro princípio de prova, diretamente vinculativo de todas as autoridades”.

Ademais, com o estabelecimento do novo CPPSTP, torna-se imperioso o uso de provas outras no processo de investigação criminal, ao passo que, atualmente, a sociedade assiste ao surgimento de tipos outros de crimes, bem como de novos *modus operandi*, fazendo que apenas a utilização da prova testemunhal torne a tarefa mais complexa (Boa Morte, 2017).

Maia (2019) realizou um estudo no qual verificou que, em 66,9% dos casos de violência doméstica, a prova testemunhal se mostra vantajosa, apresentando média de ocorrência de 2,64 por processo, com variação de 1 a 6 testemunhas. Foram 131 declarantes observados, sendo que, destes, o incidente foi presenciado por 40%, 30% viu marcas de agressão e 57% teve conhecimento indireto. Entretanto, nota-se ambiguidade no papel da testemunha, haja visto que se trata de uma declaração de um indivíduo que, por não fazer parte da ação, compõe a narrativa dos fatos passados de forma subjetiva, sendo impossível que as imagens narradas consigam retratar fielmente a realidade. Avaliando a credibilidade do testemunho de violência doméstica, uma procuradora destaca o pudor daquele que depõe ao se "intrometer", por assim dizer, na vida familiar de outrem:

> Não foi possível fazer prova dos factos constantes da acusação pública uma vez que o arguido não prestou declarações em audiência e julgamento, prescindiu da prova testemunhal por si arrolado e, de igual modo, a ofendida usou da faculdade concedida por lei de se recusar a depor. Assim, a fundamentação da matéria de facto provada resultou do afirmado pelo arguido e pela ofendida por ocasião da sua identificação e respostas aos costumes, do relatório médico e do registo criminal." O arguido estava acusado de agredir com várias pancadas de mão aberta na face, de mão fechada na zona do olho, socos na cabeça e puxões de cabelo, pontapés nas pernas, dos quais resultaram dores e hematomas, de ameaças de morte e insultos, de controlo do conteúdo das comunicações no telemóvel e redes sociais da vítima contra a sua vontade (síntese da decisão n° 35) (Maia, 2019, p. 88).

Dessa forma, o valor assumido pela prova testemunhal ao processo é incontornável, sobretudo ao se tratar de um processo penal, que tem nesta uma ferramenta importante para se atingir a verdade material, diferente, por exemplo, do processo civil, cuja relevância maior recai sobre as provas pericial e documental (Fonseca, 2018).

3.2 Declarações do arguido (art.º 140.º e 141.º do CPP)

O Direito admite como meio de prova as declarações do arguido, desde que respeitado o princípio que trata da não obrigatoriedade de contribuir. O que determina a valoração das referidas declarações no decorrer do processo é, principalmente, a estrutura adotada aos trâmites legais. Em Portugal, com a constitucionalização da

estrutura acusatória, alguns princípios passaram a prevalecer no que diz respeito à valoração da prova em geral (E. L. R. Gomes, 2017).

O CPP, em seu art. 140º, estabelece que, mesmo que detido, sempre que o arguido fizer declarações, ele deve se encontrar livre. Muito embora essas declarações apontem controvérsias, não há nada que impeça que o arguido ofereça declarações sobre algo de que tenha conhecimento direto e que seja relevante para a causa. Não se trata, portanto, de uma prova proibida, conforme as previstas nos arts. 125º e 126º do referido documento (Moreira, 2019).

Sobre isso, Eva Lídia Ribeiro Gomes (2017) discorre acerca da natureza bicéfala das declarações do arguido, já que são, ao mesmo tempo, meios de prova e de defesa. Faz ainda uma consideração quanto ao primeiro interrogatório judicial, afirmando que, apesar de contido na etapa processual, sob o domínio do Ministério Público, esse interrogatório de arguido detido se mostra como um ato jurisdicional cujo papel não é o de investigar ou de coletar provas, mas sim de caráter garantístico. Então, como meio de defesa, ao arguido é oferecida a possibilidade de ir contra os alegados que decretam a sua coação.

Importa relembrar que o Código Processual Penal, em seu art. 357º, previa um regime restritivo de leitura e reprodução das declarações do arguido desenvolvidas antes do julgamento, impossibilitando que, sem autorização do arguido, fosse designado recurso a esse meio de prova. A possibilidade de admissão desse meio de prova foi ampliada a partir das modificações na legislação, dando ao julgador a oportunidade de sua valoração mesmo em situações em que o arguido faça o uso de seu direito ao silêncio (E. L. R. Gomes, 2017).

Portanto, antes, somente era alvo de valoração a confissão do arguido realizada em audiência de discussão e julgamento, entretanto, com as modificações no CPP advindas da Lei n.º 20, de 2013, as declarações do arguido fornecidas antes do julgamento passaram a ser aceitas como meio de prova. Assim como Sousa Mendes (2013), defende-se que a estrutura acusatória do direito penal é posta em causa, juntamente aos princípios jurídicos da oralidade, da imediação, do contraditório e da igualdade de armas, o que pode resultar na opção pelo silêncio pelo arguido antes mesmo do julgamento, mostrando-se como uma limitação na coleta de provas pela investigação.

Sobre o direito ao silêncio, José António Barreiro (2005) explica que ele se fundamenta na finalidade das declarações do arguido, sendo estas não apenas um meio de prova, mas também um meio de defesa, em que sua prática é opcional. Pelo viés objetivo, facilita o ato de mentir impunemente. Sob o ponto de vista da iniciativa, esta pode surgir do conselho de defesa ou do próprio arguido, podendo ser ampliada a

todas as etapas do processo, não se limitando à fase do julgamento. No que se refere ao âmbito, seu exercício pode ser parcial ou total. O autor ainda afirma que, desse direito, decorre a possibilidade de o arguido alterar a sua versão dos fatos sem que isso incorra em punições.

Paulo de Sousa Mendes (2014b) levanta questionamento sobre o que motiva a valoração como prova documental em julgamento de declarações do arguido obtidas por escutas telefônicas, alegando ser esta uma fragilidade axiológica do sistema processual, haja visto que ao arguido é impedido o direito de argumentar sobre o que foi dito em tais provas, supondo que, por conta da proteção assegurada em lei aos segredos das comunicações e da privacidade, estas até deveriam se beneficiar de tutela reforçada. No caso, o autor argumenta em favor dessa possibilidade unicamente em situações nas quais tais declarações não sejam abarcadas pelo princípio contra a autoincriminação.

Sobre a natureza do interrogatório do arguido, a semelhança da prática e o entendimento atual, vale mencionar que o CCP de 1929 já o previa em duas naturezas. Adriana Ristori (2007), quanto ao entendimento de hoje sobre o propósito do interrogatório no processo penal, constata a evidenciação deste como um meio de natureza dupla, perspectiva já mencionada, quais sejam, a de defesa e a de prova.

Por fim, Sousa (2018) argumenta que as declarações do arguido devem ser somadas ao recolhimento de sangue, saliva ou ar expelido em uma tentativa de qualificação da pessoa como “coisa”, observando tais declarações como parte do ser humano, estas que não podem ser recolhidas sem o consentimento do titular.

3.3 Prova por acareação (art.º 146.º do CPP)

O CPP, em seu capítulo III, art. 146º, n.º 1, possibilita a acareação dos coarguidos nos casos de evidentes contradições nas declarações, em que essa prática se mostre necessária para a busca da verdade. A partir desse meio de prova, o tribunal pode determinar as versões dos fatos que merecem credibilidade. Geralmente, o coarguido delator apresentará uma narrativa que diverge daquela fornecida pelo coarguido incriminado, contudo a intenção não é dar mais valor às declarações do coarguido, e sim observar as contradições nas versões e analisar qual se mostra mais credível (F. A. A. Silva, 2019).

Sempre que forem constatadas controvérsias entre as declarações fornecidas, poderá o juiz colocar os agentes em confronto de modo a buscar a verdade, haja visto que o objetivo maior do processo é descobrir a verdade material (Verónico, 2015).

3.4 Prova por reconhecimento (art.º 147.º a 149 do CPP)

A lei francesa não diz nada sobre a prova por reconhecimento, diferente do que se observa no sistema de Portugal. Neste último, é admitida a criação de equipas mistas, o que não se permite na França. No contexto francês, há regulação legal do recurso às compras simuladas e à geolocalização, quesitos nos quais se omite a lei portuguesa, resultando em interpretações distintas na doutrina e jurisprudência quanto à sua utilização (T. J. Mendes, 2018).

A prova por reconhecimento consta entre os diversos meios de prova mencionados no CPP, sendo ela um meio de prova típico previsto nos arts. 147º e 149º do referido documento. No mesmo capítulo, está disposto o reconhecimento de pessoas e o de coisas (ou objetos), podendo estes ser em duas vertentes, o reconhecimento pessoal e o fotográfico (Ribeiro, 2019).

Na lei portuguesa, esse meio de prova está previsto no CPPP, tratando do reconhecimento de pessoa o art. 147º, e do reconhecimento de coisas o art. 148º. Já o art. 150º do mesmo documento é consagrada a reconstituição do fato, meio de prova realizado quando for preciso determina a possibilidade de certo fato ter ocorrido de forma específica.

Por outro lado, seguindo o princípio da necessidade, adequação e proporcionalidade, disposto no CPPP, em seu art. 193, n.º 1, a aplicação de medidas de garantia patrimonial e de coação devem estar em conformidade com as exigências cautelares requeridas pelo caso, assim como também devem ser proporcionais à gravidade do delito e às punições passíveis de aplicação (Arrone, 2018).

Desse modo, conforme disposto no CPP, a prova por reconhecimento é um meio caracterizado pela confirmação de uma coisa ou pessoa conhecida antes do ato. Então, é um meio de prova que confirma – e não que cria – um elemento de prova cuja admissibilidade processual já tenha se efetivado ou uma percepção sensorial prévia ao ato em comparação a percepção atual da pessoa.

Silva (2002), discorrendo sobre o entendimento do CPP, afirma o reconhecimento enquanto meio de prova que busca a confirmação de uma percepção sensorial anterior, o que faz a partir do estabelecimento de uma identidade entre esta e a percepção presente da pessoa que procede ao ato. O autor ainda diz que o intuito desse meio de prova não é acrescentar elementos, mas confirmar aquele que já foi admitido. Para Seiça (2003), o reconhecimento é um meio de reconstrução dos fatos passados passível de diversos fatores de distorção. Mesquisa (2018) também participa da discussão, acrescentando que a prova por reconhecimento apresenta

especificidades, já que o fato probando é a identidade da coisa ou da pessoa a partir do confronto de percepções do passado e do presente, a primeira se referindo ao fato probatório, e a segunda, à experiência processual.

Ressalta-se que, devido à sua autonomia e irrepetibilidade, é um meio de prova que se destaca dos demais, muito embora tenha em comum com a prova testemunhal o aspecto de ser elaborada por fontes pessoais e a partir das percepções destas (MESQUISA, 2018). O que a afasta do regime de prova testemunhal é a disposição de um capítulo específico no CPP e, no que se refere à estrutura, garantias e requisitos, apresentar singularidades dispostas no art. 147º, n.º 7 do CPP, que, em casos de inobservância, o meio probatório faz-se ineficaz.

Ainda debatendo essa distinção, Garret (2007) argumenta que a prova por reconhecimento se distingue da testemunhal porque está sujeita a um formalismo legal e a circunstâncias de realização que impedem essa aproximação. No entanto, muito embora haja diferenças, não há impedimentos para que uma mesma pessoa seja fonte para esses dois tipos de meios de prova em um mesmo processo (Mesquita, 2018).

Segundo a lei, existem quatro tipos de reconhecimento: por descrição, no qual há uma identificação que a descreva; por fotografia, gravação ou filme; presencial, quando um dos presentes é reconhecido; e com resguardo, sem que a pessoa identificada veja quem a identificou (Albuquerque, 2009).

No reconhecimento de pessoas, antes mesmo de proceder ao reconhecimento físico, o indivíduo que procede à identificação precisa descrever todos os detalhes na descrição do identificando, assim como deve indicar se já havia visto a pessoa reconhecida anteriormente e as condições em que isso aconteceu, além de fornecer informações outras que possam assegurar credibilidade à identificação (Sá, 2015).

No reconhecimento por fotografias, gravações ou vídeos, é necessário que se apresente à pessoas diversos registros com imagens de indivíduos que apresentem características semelhantes a quem se quer reconhecer, de modo a garantir maior fiabilidade a esse meio de prova. Do mesmo modo, deve-se ampliar a quantidade de pessoas que compõem o painel de reconhecimento; exigir que aquele responsável por conduzir o reconhecimento não tenha conhecimento sobre a identidade do suspeito; informar previamente a testemunha ocular que existe a possibilidade de o suspeito não estar entre os indivíduos que integram o painel de reconhecimento; formar um painel composto de pessoas que apresentem todas as características informadas anteriormente pela testemunha, sem que nenhuma delas tenha atributos destoantes; apresentar previamente à testemunha um primeiro painel de reconhecimento no qual

não consta o suspeito a fim de verificar se ela tende a fazer um julgamento relativo (Sá, 2015).

Marques (2019) observou uma prova por reconhecimento em que se pedia às testemunhas que descrevessem o identificado em todas as suas peculiaridades das quais se lembrasse. Pediu-se que alguns traços identificativos fossem reconhecidos nomeadamente, como o sexo, a etnia, a altura, a idade, o cabelo, o vestuário, traços faciais, postura e modo de andar e até mesmo a voz. Além disso, demandou-se das testemunhas que relatasses ao tribunal a natureza de sua relação com o identificado, questionando-as se antes mesmo da data dos fatos em análise elas já o conheciam, bem como perguntou-se se havia elementos outros que poderiam ser incluídos por serem relevantes à busca pela verdade, conforme determina o CPP, art. 147º, n.º 1.

Marques (2019) ainda presenciou situações em que o Ministério Público ou o tribunal solicitou o confronto com várias fotografias recolhidas pela PSP no decorrer da investigação. Essa era uma ação costumeira em audiências de discussão e julgamento, sobretudo quando se tratavam de crimes de tráfico de estupefacientes. Geralmente, recorria-se ao reconhecimento fotográfico em situações nas quais o arguido não estava presente, colaborando, a partir de sua identificação, com o depoimento da testemunha. Cabe ressaltar que, na etapa de julgamento, só se utiliza o reconhecimento quando nas fases de inquérito e de instrução ele foi inexistente, mediante a uma iniciativa das autoridades de investigação, à nulidade probatória do ato ou à nulidade processual.

Entende-se como complexo o ato de reconhecimento de pessoas, que envolve etapas de descrição prévia do indivíduo identificado pela fonte e de confronto visual desta com o identificando, sendo o legislador o responsável por definir os meios usados para o efeito.

Pontua-se ainda que, caso conclusivo, essa fase narrativa se configura como um tipo de reconhecimento autônomo, ou, não seguindo dela da fase da prova por reconhecimento o confronto visual, conformará uma prova testemunhal de caráter narrativo.

3.5 Prova pericial (art.º 151.º do CPP)

O CPP prevê diligências de prova às quais podem se sujeitar o arguido, quais sejam, a disposta no art.º 151 e conseguintes – perícia – e a consagrada no art. 171º e posteriores – o exame (Fernandes, 2017).

Nesse sentido, Fidaldo (2006) explica que a perícia representa uma interpretação frente aos factos realizada por meio de indivíduos com conhecimento científicos, técnicos ou artísticos específicos, analisando-se vestígios pelos quais

esses profissionais podem alcançar certas conclusões periciais, as quais são disponibilizadas as autoridades para que sejam apreciadas, constituindo desta forma meios de prova. Estas autoridades, nos exames, se apercebe de forma directa dos meios de prova, através dos quais investiga indícios e vestígios através inspecção das coisas, pessoas, e do local, sendo o exame uma forma dos vestígios serem obtidos (meios de prova) ou, de forma indirecta, por meio do auto cuja elaboração será feita por autoridade judiciária ou ainda por um órgão de polícia criminal, os quais descreverão os vestígios deixados pelo crime bem como os relativos indícios de onde e como foi praticado.

A responsabilidade jurídica sobre o comportamento ilícito varia conforme o entendimento do agente responsável pelo crime sobre o seu ato e as consequências dele decorrentes. A perícia, nesse sentido, auxilia na avaliação da personalidade do autor do ato, sendo demandada quando a apreciação dos fatos carece de conhecimentos técnicos, científicos ou artísticos específicos. O objeto de análise da perícia é esse fato, portanto, que pode assumir caráter de pessoa, coisa ou lugar. Geralmente, o propósito da perícia é determinar a ilicitude e/ou a punibilidade de um determinado comportamento e seus efeitos, definir a autoria desse comportamento ou consequência, estabelecer o tipo de crime e verificar circunstâncias que se mostrem atenuantes ou agravantes do ato. Cabe ao juiz solicitar a perícia, seja a de personalidade ou a psiquiátrica quando houver dúvidas quanto à personalidade ou comportamento da pessoa, conforme disposto nos arts. 159º e 160º do CPP (Verónico, 2015).

Então, pode-se dizer que o regime da prova pericial trata da matéria de fato, sobre a qual recai o parecer do especialista e que está submetida à livre avaliação do julgador. Por outro lado, a declaração da ciência ou juízo científico, está que ampara o referido parecer, mostra-se como alvo possível de discussão em um plano científico e, portanto, não entra nesse poder de descrição (Verónico, 2015).

O valor da prova pericial está descrito no art. 163º do CPP, que aponta que deve haver justificativa dos motivos quando o juiz discordar do parecer apresentado pelo perito (Antunes, 2010). Tal presunção pode ser afastada a partir da prova do contrário pelo julgador, esta que precisa ser fundamentada de modo a apontar as razões que levam à divergência. Ribeiro (2015) explica que essa discordância é permitida desde que o juiz possua ele mesmo conhecimentos de valor científico ou técnico equivalente ao do perito, sendo, desse modo, capaz de indagar as conclusões apresentadas no relatório pericial.

Além disso, é fundamental que em qualquer ocasião o juízo técnico se mostre em uma afirmação categórica, sobre a qual não pairem dúvidas acerca do assunto

tratado, não abrindo, assim, possibilidade para suposições de probabilidades e opiniões. No caso de o perito emitir uma probabilidade, uma opinião ou demonstrar dúvidas ao invés do solicitado juízo técnico-científico, cabe ao tribunal decidir sobre a matéria de fato, não sendo limitado por qualquer restrição probatória (Afonso, 2016).

Os chamados *first responders* são aqueles que primeiro tiveram acesso ao local do crime e, por isso, se mostram extremamente relevantes para o desenrolar da preservação das provas, auxiliando a tomada de decisão do juiz, que deve ter o mínimo de dúvidas possível em sua análise. Seguindo a importância desses elementos, virão a coleta de provas, a investigação criminal, a gestão técnica forense e a fase pericial, todos itens fundamentais para assegurar o êxito do processo (Vasco, 2018).

Aliás, não é raro que os peritos sejam os responsáveis pela descoberta de indícios. Nesse sentido, o CPP, em seu art. 151º, explica que a prova pericial age não apenas na apreciação dos fatos como também em sua percepção, como ocorre, por exemplo, em situações que se coleta material biológico para análise de DNA. Isso porque, geralmente, o conhecimento do perito permite que esse indivíduo perceba a existência de material biológico em uma mancha, por exemplo, bem como será ele a pessoa capaz de realizar o recolhimento adequado desse material para a análise. Entende-se, então, que a perícia se faz presente em várias etapas do processo (Branco, 2017).

Também compõem o processo as diversas áreas laboratoriais especializadas na produção de prova pericial, isto é, prova técnico-científica, o que faz a partir de análises dos vestígios produzidos na ação de um delito e posteriormente encontrados. Por meio do estudo minucioso dos elementos materiais vinculados ao crime auxiliam a determinar a ocorrência do fato e a estabelecer o modo que aconteceu. Assim, mesmo em casos de confissão do responsável pelo ato ilícito, a prova pericial se faz indispensável, mostrando-se como principal fonte para a determinação de punições (Vasco, 2018).

Em processos sobre crimes sexuais, não pode haver limitação à identificação de vestígios ou sinais traumáticos, já que, sobretudo nesses casos, o exame pericial se apresenta como meio de prova importante. Em tais situações, é função da perícia interpretar e registrar elementos de agressão de natureza sexual. O exame deve ser feito rapidamente e de forma completa, sendo que a coleta das informações sobre o eventual crime será feita por meio de uma entrevista que buscará identificar fatores de vulnerabilidade da vítima (Verónico, 2015).

O art. 159º do CPP regulamenta os conhecimentos forenses e médico-legais quanto à avaliação dos danos nos arguidos e nas vítimas, sejam eles danos físicos, mentais ou físicos (Brito, 2019).

Na pesquisa de Brito (2019), ficou evidente que, em casos de violência médica, as provas periciais mais recorrentes foram o relatório de exame forense e o médico-legal, seja em fase de julgamento, seja em fase de inquérito. Mas não existem apenas essas, podendo haver, também, as perícias a armas de fogo e armas brancas apreendidas na investigação. Outro ponto levantado no referido estudo é acerca da relevância ínfima que o sistema judicial concede ao dano psíquico provocado à vítima, bem como aos aspectos psicológicos do réu, haja visto que se observou a não solicitação desses exames durante esse processo.

Em uma observação comparativa, Brito (2019) também constatou diferença da pena estabelecida entre os casos em que há apresentação de prova pericial no julgamento, sobretudo referindo-se aos exames forense e médico-legal da vítima, sendo que, quando da existência dessa prova, a pena é consideravelmente maior (18,2 meses); os casos em que esse tipo de prova não constou em julgamento atingiram média de pena de 11,72 meses. O que se percebe, portanto, é que quando o juiz se depara com um relatório pericial, ele toma conhecimento mais detalhado sobre o risco envolvido na questão, e isso influencia no estabelecimento de penas, demonstrando, assim, uma relação importante entre a prova pericial e a pena concreta.

José António Barreiros (2014), nesse sentido, argumenta sobre a elevada importância da prova pericial frente às demais provas no processo penal contemporâneo, explicando que, no mundo atual, com mudanças constantes e sofisticação da criminalidade, determinadas ações só podem ser plenamente compreendidas a partir de um conhecimento especializado. Por isso, ele entende que tal meio de prova atende ao objetivo do processo, e mais, objetivo este que apenas com a prova pericial será alcançado – o que antes era atribuído à confissão do arguido –, oferecendo ao juiz conhecimentos objetivos alcançados por terceiros e permitindo conclusões probatórias fundamentadas não em seu próprio juízo.

Portanto, a prova pericial se mostra de significativa importância ao processo penal, funcionando o perito como meio de descobrir, apreender e apreciar provas por meio de métodos científicos específicos (Afonso, 2016).

3.6 Prova documental (art.º 164.º do CPP)

O Código Civil, em seu art. 362º, entende a prova documental como aquela que decorre de um documento, assumindo como tal quaisquer objetos produzidos por

pessoas a fim de representar ou reproduzir algo, alguém ou um fato. Os documentos autênticos são aqueles elaborados por entidade pública de autoridade em sua produção, já os demais são denominados documentos particulares. Estes podem ser simples, assinados pelo autor, ou autenticados, quando reconhecidos por advogado ou notário (Escola Prática da Guarda, 2008). Os documentos simples, se reconhecida a autoria, podem servir como prova plena, no entanto, se nele forem constatadas irregularidades, caberá ao juiz determinar de que forma elas afetam a capacidade probatória do documento, tal como dispõe o art. 376º do Código Civil (J. P. V. B. Silva, 2017).

O CPP também apresenta uma definição à prova documental, constatada em seu art. 164º, n.º 1, conceituando-a como declaração, notação ou sinal escrito ou em quaisquer meios técnicos, nos termos da lei penal. Segundo o documento, esse tipo de material só não é admissível enquanto meio de prova quando as informações são anônimas, conforme se observa no art. 164º (Ferrão, 2018).

Imagens e sons, portanto, podem ser enquadrados como prova documental admissível, de acordo com o CPP (Cunha, 2017). Registros em vídeo, fotográficos, listagens de valores e de locais de uso de cartões, talões de pagamento etc. são elementos que poderão ser utilizados em processo e se mostrar como meios importantes para produção de provas (Alves, 2019).

Ramos (2015a) acrescenta que a prova digital também pode ser classificada como prova documental quando aquela puder ser corporizada por escrito ou por outro meio técnico ao processo, como no caso de impressões de mensagens ou fotografias, por exemplo.

Paulo Dá Mesquita (2011) explica sobre a abrangência da categoria da prova documental, que demanda ações de adequação da dogmática da divisão sistemática das provas centralizada nos mediadores, elaborada em um contexto politicamente pouco sensível à interpretação da componente funcional dos atos de comunicação. Ademais, ele pondera que ainda é escasso o empenho da doutrina e da jurisprudência no estudo desse tipo de prova.

Deve-se destacar dois aspectos quando se trata desse meio de prova: 1) os termos em que sua admissibilidade é aferida; e 2) o seu valor probatório no processo. O já mencionado art. 164º do CPP admite o uso do documento enquanto meio de prova e, a partir dessa disposição, entende-se que o emprego da prova documental não se faz obrigatório, podendo ser utilizado em seu lugar outro meio de prova, desde que favoreça o objetivo que se almeja atingir (Afonso, 2016).

É responsabilidade da autoridade da concorrência listar as provas documentais que constam nos autos e que se classificam como confidenciais, podendo o visado

interferir nessa classificação bem como na relevância probatória final a ela atribuída. Tal listagem das provas documentais confidenciais precisa ser pormenorizada, bem detalhada, de modo que se assegure o direito de defesa, com vista à elaboração de solicitações de acesso concretas e bem fundamentadas pelos visados (Sousa, 2015).

Se no regime de prova testemunhal a testemunha se configura como meio de prova e suas declarações, a prova, no regime de prova documental, o meio de prova é o papel e o seu respectivo conteúdo se apresenta como sendo a prova (Jesus, 2015). Do mesmo modo, o Acórdão do Tribunal da Relação do Porto, de 01-06-2016 pondera que, nas escutas telefônicas, estas são meios de coleta de prova, os meios de prova são os diálogos recolhidos a partir delas, que, transcritos e incluídos no processo, os conteúdos se tornarão prova documental (Tribunal da Relação do Porto, 2016).

Faz-se importante, também, traçar os limites entre a prova documental e a prova testemunhal. No que se refere aos documentos que apresentam declarações, a questão se faz mais complexa, uma vez que se valorada sem qualquer tipo de restrição pelo julgador, mostra-se prejudicial ao princípio do contraditório, ao menos no que tange o contraditório para a prova. Portanto, leva a derrogação de certas normas probatórias, sobretudo aquelas referentes às provas testemunhais e ao princípio do contraditório, já que não permite às partes a possibilidade de apresentar provas outras que tratem dos fatos ali apresentados (Ferrão, 2018).

Iolanda Calamendrei (1995 citado em Ferrão, 2018) evidencia as semelhanças entre os documentos que trazem declarações e o depoimento indireto, inserido na categoria de prova testemunhal. Contudo, ela destaca que nas situações em que as declarações se baseiem nas percepções do próprio responsável pela autoria do documento, tais semelhanças são excluídas.

Cabe ressaltar que, no cenário da criminalidade tributária, a prova documental se faz a mais recorrente, sobretudo aqueles documentos recolhidos em inspeção tributária, possíveis de serem utilizados em processo penal tributário por meio da intercomunicabilidade probatória. É, nesse contexto, um mecanismo que, desde que obedeça a proibição do excesso e não desrespeitando a redação do CPP, art. 126º, configura-se como um mecanismo de garantia processual. Destaca-se que, ocorrendo a inspeção tributária fora dos dispostos em lei, não haverá possibilidade de valoração dos documentos (Moreira, 2018).

Por fim, Fonseca (2018) discorre que a prova documental, assim como a pericial, assume relevância significativa no processo civil, assim como a prova testemunham se evidencia enquanto meio de prova importante no processo penal em comparação aos demais.

3.7 Escutas telefónicas (art.º 187.º do CPP)

As escutas telefônicas não se apresentam unicamente como meio de coleta de informações em busca da verdade, mas também como instrumento mediato de recolhimento de provas e meios de prova (Santos, 2015).

Elas estão incluídas no rol de métodos ocultos de investigação, isto é, entre aqueles que possibilitam que provas sejam recolhidas sem que o investigado saiba conscientemente que está se incriminando (Santos, 2015).

Entende-se que o objetivo do uso das escutas telefônicas seja recolher provas reais e provas pessoais para posterior análise e interpretação jurídica. Cabe destacar que, como provas reais, enquadram-se os elementos materiais e factuais do delito, e, as pessoais são aquelas que localizam agentes e testemunhas relevantes para o decorrer do caso (Santos, 2015).

Sua utilização depende do julgador, que deve realizar um despacho fundamentado que demande o uso dessas escutas, sendo aceitável em situações nas quais se evidenciem razões que levem a acreditar que são indispensáveis para se descobrir a verdade, no sentido de que outro meio de obtenção de prova seja difícil ou impossível. Desse modo, observa-se que o regime de escutas tem natureza excecional, devendo ser empregado em última opção (M. M. M. Silva, 2017).

Desse modo, esse é um regime admitido em matéria do processo penal, conforme consta na CRP, art. 34º, contrariando as proibições dispostas no art. 32º, n.º 8, do mesmo documento e no art. 126º do CPP, redações que destacam a nulidade de provas que tenham sido coletadas a partir de intromissão abusiva no domicílio, nas telecomunicações e correspondências e na vida privada (Batista, 2018).

Segundo Batista (2018), são elementos a serem observados:

- Fase do processo: seguindo plenamente a lei, a escuta telefônica só será permitida em casos de crimes já iniciados ou concluídos, não sendo admitida no propósito de prevenir delitos. Desse modo, não pode ser empregada em outra fase do processo sem a abertura do inquérito.
- Catálogo de crimes: O CPP, art. 187º, apresenta o catálogo de crimes, entre os quais estão os passíveis de pena superior à prisão de 3 anos; os referentes ao tráfico de armas e estupefacientes; a criminalidade violenta ou organizada e o terrorismo; o rapto, sequestro ou tomada de reféns; e os delitos que atacam a segurança do Estado.

- Catálogo de sujeitos: os potenciais alvos de escuta telefônica também estão descritos no mesmo artigo do CPP, sendo eles o suspeito ou o arguido, a vítima e o intermediário.
- Prazo de autorização: o CPP, ainda no art. 187º, em seu n.º 6, estabelece que "a interceção e a gravação de conversações ou comunicações são autorizadas pelo prazo máximo de três meses, renovável por períodos sujeitos ao mesmo limite, desde que se verifiquem os respetivos requisitos de admissibilidade". O início dessa contagem se dá no dia em que o despacho judicial permite a escuta.
- Procedimentos: o art. 32º, n.º 4, da CRP regula as formalidades referentes à reserva do juiz e ao uso ou conservação da prova (Batista, 2018).

Observa-se, portanto, conforme destaca Faria (2013), que o CPP, especificamente em seu art. 187º, atribui um regime restrito à admissibilidade das escutas telefônicas, destacando o seu uso ponderado e cauteloso. Paulo de Sousa Mendes (2018) complementa que diversos dos meios de obtenção de provas necessários só podem ser utilizados a partir de autorização do julgador, sendo a escuta telefônica um desses meios cuja admissibilidade depende de despacho do juiz. Nesse caso, então, a parte (MP) precisa enviar um requerimento à autoridade de decisão, que, verificada a real necessidade, procederá com um despacho fundamentado autorizando a utilização do meio de prova. Ademais, em situações de constatada urgência ou de perigo na demora, o requerimento ao juiz pode vir dos OPC. Carvalho (2012) ainda explica que não pode haver determinação de interceptação pelo julgador de escuta de outra pessoa ou de outro telefone do mesmo sujeito.

As formalidades são dispensadas quando o requerimento advém do Ministério Público ou de autoridade policial criminal, conforme dispõem os arts. 168º, n.º 3, e 269º, entretanto Valente (2010) argumenta que as razões de fato e de direito que assegurem a real necessidade da escuta para a busca da verdade também assim deveriam funcionar.

Leite (2004) pontua que a autorização das escutas depende de um elenco estabelecido de tipos legais de crime, não importando o grau de comparticipação. Conforme explicitado anteriormente, entre esse rol de crimes estão aqueles que indicam ação violenta ou em que a palavra é usada como ferramenta. Entretanto, o autor argumenta que, para reforçar o caráter de *ultima ratio* desse meio de prova, a alínea a) do art. 187º, n.º 1, que apresenta o catálogo de crimes, deveria passar por uma modificação, incluindo a previsão de uma moldura penal mais alta.

Inclusive, Santos (2015) relembra que, apresentando-se como alvo de imputação ou responsabilidade criminal, o defensor se mostra como sujeito passivo da medida de ingerência e, como há previsão legal do uso das escutas apenas em situações de razões evidentes para tanto, então, também se entende que não dispõe que pode ser aplicada unicamente contra o defensor; em outras palavras, não há impedimento para que esse meio seja empregado de forma desfavorável ao arguido.

Nesta linde, Andrade (2014) pondera que o regime das escutas telefônicas apresenta o que chama de danosidade polimórfica, ou seja, além de um meio complexo, é também invasivo e potencial violador dos direitos fundamentais dos indivíduos. Para ele, os danos dessa prática atingem as dimensões objetiva e subjetiva, haja visto que, a partir de seu emprego, são escutadas mais pessoas do que se pretendia e, consequentemente, são atingidos mais bens jurídicos do que os previstos; é nesse fato que mora a justificativa da cautela de seu uso.

Sabe-se que esse meio de prova traz impactos, sobretudo, aos direitos fundamentais vinculados aos direitos de personalidade e de intimidade, descritos nos arts. 80º do CC, 12º do DUDH, 26º da CRP e 8º do CEDH. Fere também os preceitos do sigilo dos meios de comunicação e da inviolabilidade do domicílio, conforme atestam os arts. 82º a 88º do CC, 12º do DUDH, 34º da CRP e 190º do CP. E envolve os direitos à palavra e a à imagem, ao silêncio e a não autoincriminação, ao status processual ativo e à liberdade de expressão, que podem ser encontrados nos arts. 26º, 32º, n.^{os} 1 e 2, e 37º da CRP e 192º, 194º e 199º do CP (Santos, 2016).

Ana Raquel Conceição (2009) ressalta que o erro do arguido não é induzido intencionalmente na escuta telefônica, pelo contrário, ele se encontra em erro espontâneo. Por isso, o juiz será responsável por definir, a partir dos requisitos de admissibilidade desse meio de prova, os limites pelos quais esse erro inquirirá a prova obtida.

Aqui, argumenta-se que as escutam são passíveis de valoração na comprovação de um crime novo de que se teve conhecimento e que esteja listado em lei, mesmo que o delito motivador da aplicação desse meio de prova não seja provado ou, por algum motivo, não seja perseguido. Por outro lado, não sendo o crime novo pertencente ao catálogo de delitos e se mostrando desvinculado do crime original investigado, o conhecimento adquirido sobre esse delito pode servir como notícia de um crime (H. S. G. Silva, 2019).

Por fim, compreendendo que o regime de escuta será empregado como último meio de obtenção de provas em um caso e que não há imposição de indícios seguros por lei, defende-se pela necessidade de que tais indícios sejam seguros, consistentes

e se mostrem fundamentais, ou seja, indispensáveis para a efetivação da investigação (Santos, 2015).

4 A CRIMINALIDADE INFORMÁTICA

Tanto os estudos científicos quanto a imprensa pública, sobretudo a internacional, já mencionavam os crimes informáticos ainda na década de 1960. Esses delitos também são conhecidos a partir de outras nomenclaturas, tais como “criminalidade de informática”, “infrações realizadas por meio de computador”, “criminosos de computador”, fraude de informática”, “delinquência informática”, entre outras, sendo algumas delas utilizadas de forma equivocada, conforme pontua Euzébio (2014). A imprensa especializada veiculava questões referentes a esses crimes, como casos de manipulação e sabotagem de computadores, uso ilegais de sistemas informáticos e espionagem por meios digitais. A partir da década de 1980, começaram a aparecer os casos de vírus, *hackers*, piratarias etc., temas que levantaram os debates acerca da segurança e controle desses delitos (Silva, 2016).

O primeiro país a apresentar normas relacionadas à violação de bens informáticos foi a Suécia, entretanto os pioneiros no combate efetivo a esses crimes foram os Estados Unidos da América, que desde 1970 vem promovendo discussões acerca de atos ilícitos por meio da internet. Em 1986, promulgaram a *Computer Fraud and Abuse Act* e, em 1988, tal lei condenou Robert Morris, o primeiro hacker a ser penalizado por crimes cibernéticos (Jesus & Milagre, 2016).

Na Europa, o início do combate a esse tipo de delito se deu em meados da década de 1980, sob a responsabilidade do Conselho da Europa, que estabeleceu um comitê responsável por estudar as questões relacionadas ao crime informático e elaborar um relatório com as conclusões alcançadas (Mota, 2019).

No contexto brasileiro, a década de 1990 marca o início da popularização da internet e, consequentemente, o surgimento dos crimes virtuais (Ribeiro, 2017). O primeiro caso averiguado se deu em 1997, fazendo de vítima uma jornalista que recebia em sua caixa de e-mail materiais de cunho sexual e ameaças. A partir da investigação, identificou-se como autor do crime um analista de sistemas, que recebeu como pena a prestação de serviços à Academia de Polícia Civil para ensinar às autoridades policiais quanto ao uso de informática (Nogueira, 2008).

Jesus e Milagre (2016) ainda complementam que os primeiros crimes de *phising scam* bancário foram relatados no Brasil ainda em 1999. Mencionam também o famoso caso do empresário acusado de enviar, de Londres, mensagens de e-mail para o mercado financeiro apresentando informações falsas que previam a quebra de um determinado banco. Tal situação foi motivadora de grande alarde na época e, como resultado, gerou intensos debates sobre as questões relacionadas à

investigação de cibercrimes, cuja prática poderia se dar em qualquer lugar do mundo. Foi então que começou a se fortificar o entendimento da necessidade do estabelecimento de leis que abarcassem os crimes informáticos.

Introduzindo o tema, Lima (2017) descreve o crime virtual como quaisquer condutas ilícitas que busquem exclusivamente prejudicar sistemas físicos ou técnicos bem como os componentes de computadores. Há também o crime virtual misto, que utiliza a internet como meio indispensável para o ato, mas visa agir sobre bem jurídico que não o informático, como, por exemplo, nos ilícitos que envolvem transferências ilegais de valores de contas correntes.

Ribeiro (2017) destaca que, na atualidade, o contexto de tais crimes tem se tornado ainda mais complexo, visto que, antes, apenas aqueles indivíduos com amplo conhecimento de informática eram capazes de cometê-los, mas, agora, com o crescimento do acesso a informações e métodos para agir delituosamente no meio digital, ampliou-se o leque de pessoas que podem praticar esses crimes.

Déborah Oliveira (2017) refere-se a uma fala do analista sênior da equipe Global de Investigação e Análises da Kaspersky Lab, Fábio Assolini, o qual explica a existência de dois perfis de criminosos nessa área. O primeiro é aquele com pouca habilidade técnica, havendo casos em que não possui nenhum conhecimento informático, mas que pratica os crimes a partir do que aprende em vídeos veiculados em plataformas *on-line* que ensinam algumas técnicas. Esses são os chamados script kiddies. O segundo perfil é o de conhecimento específico elevado, mostrando-se um superprofissional, capaz de criar códigos indecifráveis e promover ataques em série.

Portanto, ao se ignorar medidas preventivas ou de segurança no meio virtual, cresce a vulnerabilidade de sistemas, armazenamentos, dados e processos. Não é raro que as redes sejam atacadas por vírus que se alastram a outros computadores, prejudicando todo um sistema informático (Floriano & Rodrigues, 2017).

Informações de autoridades oficiais de Portugal asseguram que, em um futuro próximo, o país assistirá à elevação significativa da criminalidade informática e, por esse motivo, é fundamental que o Estado busque meios de garantir a segurança e a defesa no universo virtual, bem como aos cidadãos que a ele recorrem. Entende-se a ciberdefesa como um conceito que se refere às medidas que visam proteger o Estado de eventuais ataques; e a cibersegurança está relacionada à preservação da tranquilidade pública nesses meios, ou seja, diz sobre a segurança interna (Correia, Santos, & Correia, 2017).

A União Europeia traçou uma estratégia de cibersegurança que abrange a prevenção e a reação às perturbações e aos ataques que prejudiquem os sistemas de telecomunicações dos países-membro, protegendo os serviços de computação em

nuvem, os motores de pesquisa, as plataformas de pagamento em linha, as redes sociais e os *sites* de comércio eletrônico (Lopes, 2010).

No que se refere aos cibercriminosos, Costa (2011) entende que o responsável pela ação geralmente apresenta características que se divergem do criminoso comum. Geralmente, o criminoso é alfabetizado, culto, inteligente e raramente possui antecedentes criminais.

O crescimento da criminalidade digital se explica por três motivos. Primeiro, viu-se o aumento de usuários da internet e de outros meios eletrônicos, elevando, assim, o leque de vítimas para essas práticas criminosas. Segundo, a popularização da internet também fez crescer o número de criminosos que a utilizam. Por último, a ausência de segurança nesse meio, bem como de conscientização sobre ela, ao passo que a maioria dos usuários não pensa na possibilidade de se tornar alvo de um crime informático (Pinheiro, 2016).

O crime praticado por meios informáticos faz uso das características comuns dos delitos informáticos, sendo o anonimato a principal delas, mostrando-se valiosa para a ação criminosa. Alguns programas informáticos permitem a ocultação de identidade e da localização, no entanto eles demandam conhecimentos específicos não dominados pelo cidadão leigo, o que faz com que o criminoso dessa área seja munido de entendimento dos meios digitais (Ferraz, 2020).

Pode-se dizer que a criminalidade informática possui algumas especificidades. Sydow (2015) discorre que os crimes informáticos não demandam contato físico entre o praticante do delito e a vítima, bem como não exige visitação antecipada ao local em que o crime será realizado e nem planejamento, justamente por ocorrer em espaço virtual, sem território, governo ou povo, eximindo o agente responsável de altos riscos. É uma prática que não apresenta padrão e nem resulta na sensação de sofrimento ou exercício de violência. Além disso, existe a possibilidade de vários crimes serem cometidos concomitantemente e em diversos lugares, inclusive de forma transnacional. Por fim, os agentes criminosos contam com a vantagem de que são escassos os profissionais investigadores capacitados para o trabalho.

Silveira (2016) também aborda o caráter transfronteiriço do ambiente digital, explicando que computadores e sistemas informáticos podem ser conectados independentemente da localização no mundo. Não há barreiras para comunicações distribuídas pelo globo. Nesse sentido, ao dizer que, via ambiente digital, a atuação pode se dar de forma transnacional, refere-se à noção de ruptura de territórios, assumindo uma realidade virtual que se faz presente simultaneamente em todos os lugares e em lugar nenhum.

Então, rompe-se com a ideia da prática de um crime ligada a uma base física de território, eliminando-se também os limites impostos pelas fronteiras e distâncias. É uma situação que permite que um mesmo delito informático implique em dois ordenamentos jurídicos diferentes ou mais, o que torna ainda mais complexas a qualificação do crime e o estabelecimento de normas aplicáveis (Silveira, 2016). Fiorillo e Conte (2015) exemplificam essa possibilidade comentando que uma empresa situada no Canadá, por exemplo, pode ter seu sistema informático violado por um criminoso que se encontra no Chile, e os respectivos prejuízos desse ilícito serem presenciados no Japão.

A lei portuguesa que diz sobre o julgamento da responsabilidade civil na violação de direitos de personalidade, levando em conta a transnacionalidade da criminalidade informática estabelece que, nesses casos, deve ser aplicada a norma vigente no país do qual decorreu a atividade causadora do dano. Contudo, há que se ressaltar que, na maioria desses casos, são envolvidos os direitos transnacionais por meio da internet, criando barreiras à acusação criminal pela dificuldade de se definir o local de origem do delito. De outra forma, existe a possibilidade de se aplicar a lei da residência habitual da parte prejudicada, que garante maiores chances de levar o crime a julgamento, desde que autorizada maior flexibilidade para a aplicação de lei divergente (Freitas, 2018).

Costa (2011) narra um caso exposto pelo promotor Roberto Lyra, no qual um pedófilo brasileiro e investigado em seu país migrou para um *site* português, do qual enviou para um *hacker* fotografias de adultos fazendo sexo com menores de idade. O *hacker* em questão estava colaborando com as investigações do caso. No entanto, ao descobrir que era alvo de investigação, o referido pedófilo protestou que os investigadores não conseguiriam prendê-lo, pois estava em um provedor de fora do Brasil.

Sobre essa dificuldade, relata-se que, nos delitos praticados em provedores estrangeiros ou por agentes que estão fora do país, é preciso que haja uma expedição de rogatória, o que se mostra como um atraso para a investigação. Essa é uma dificuldade que poderia ser superada por meio de cooperação ou convênio internacional (Costa, 2011).

Nesse contexto, o Conselho da Europa elaborou a Convenção sobre o Cibercrime, que trata das obrigações dos Estados em criminalizar os crimes informáticos e cooperar com os demais países em casos como os citados anteriormente (Tavares, 2018). Já no caso do Brasil, Ribeiro (2017) explica que a norma nacional não será aplicada caso o crime for cometido fora do país, entretanto, tendo ele sido praticado por um brasileiro, estando a vítima no Brasil e sendo a

conduta considerada ilícita em ambos os países, a competência no caso será brasileira.

No que diz respeito à cooperação internacional, Jesus e Milagre (2016) discorrem que esta ainda se apresenta como um desafio no combate à criminalidade informática. Os provedores são os que mais possuem capacidade de apurar ocorrências que envolvam seus usuários e, segundo os autores, os serviços mais utilizados no Brasil não internacionais, sendo que alguns não têm nem filiais físicas em solo brasileiro. Por isso, sempre que há processos que demandem quebras de sigilos dos clientes desses provedores, eles alegam que não precisam seguir a jurisdição brasileira, mas sim as normas do país de sede. Na maioria dos casos, esse argumento não é considerado pelo judiciário, contudo não exclui a preocupação em relação à situação, fazendo-se relevante o efetivo desenvolvimento da cooperação entre os países.

Frente às dificuldades que envolvem essa questão, a criação de leis nacionais que busquem prevenir tais crimes poderiam resultar no surgimento de paraísos criminais, em referência aos conhecidos paraísos fiscais. Também chamados de *Computer crime heavens*, ou apenas *heavens*, seriam locais com legislações mais amenas nos quais os provedores fariam sede em busca da não punição aos delitos informáticos (Kerr, 2011).

No que se refere às características, Guerra (2019) argumenta que existem distinções entre os crimes informáticos e os demais crimes. Os primeiros são realizados a partir da utilização da tecnologia e demanda uma investigação que recolha elementos que sirvam de provas para o posterior processo penal. Nessa investigação, diversos recursos podem ser utilizados.

A velocidade da prática criminosa também se destaca como característica peculiar ao delito informático, normalmente efetivado em nanossegundos. Em muitas ocorrências, a vítima sequer nota o ataque, sendo comum que perceba (quando percebe) o fato apenas em eventos posteriores, como quando é notificada por e-mail, por exemplo (Albuquerque, 2006).

Há de se ressaltar, ainda, a íntima relação entre crimes informáticos e o financiamento do terrorismo. Esse tipo de crime se apresenta como um meio para o branqueamento de capitais, estes usados para financiar práticas e grupos terroristas. Além disso, assim como o branqueamento de capitais, os atos terroristas e delitos informáticos são organizados por grupos cujos membros possuem alto grau de conhecimento para a prática das ações, isto é, a organização é outra característica que estreita a ligação entre essas ações (Conceição, 2018).

Portugal tem registrados crimes que indicam o uso de criptomoedas para financiar grupos terroristas, bem como para a prática de crimes de extorsão, lavagem de dinheiro, evasão fiscal e delitos referentes à comercialização de material pornográfico, inclusive com conteúdo de pedofilia, e ao tráfico de drogas e armas. Desses ataques, o mais frequente é o ataque de Ramsonware, atingindo na maior parte vítimas no setor corporativo (Garnaeva, Sinitsyn, Namestnikov, Makrushin, & Liskin, 2016). Observa-se, contudo, que sempre existe a possibilidade de a acusação culminar no branqueamento de capitais, muito embora a tipologia do crime, já que o objetivo dos criminosos nesses atos é o, depois de consumados os crimes, converter as criptomoedas em dinheiro físico (Gaspar, 2018).

Denota-se, assim, o caráter violento e organizado dessa criminalidade, que é determinante na constatação de associação criminosa. É uma realidade que demanda a urgência da cooperação internacional não apenas na incriminação dos atos, mas também na repressão e prevenção dos mesmos. Desse modo, o combate a esses delitos deve se dar em parceria entre os Estados, seja no que se refere à cooperação entre eles, seja quanto à harmonização das leis que tratem do assunto (Conceição, 2018).

Dentre os usuários mais ameaçadores no mundo digital estão os crackers, que são os bandidos cibernéticos; os carders, especializados em fraudar cartões de crédito; os phreakers, que atuam no campo de eletrônica e telefonia; os warchalkers, ou wardrivers, que invadem redes wireless; e os insiders, estes que são os mais perigosos conforme o FBI, pois se tratam de funcionários ou ex-funcionários que possuem informações privilegiadas das empresas (J. Q. Gomes, 2017). Alguns desses usuários são abordados nos tópicos a seguir.

4.1 Hackers

Chamam-se de hackers os conhecidos como “piratas” de computador. É uma expressão que começou a ser utilizada nos laboratórios de computação do Massachusetts Institute of Technology (MIT), instituição na qual os alunos se dedicavam a aprender tudo o que era possível realizar com o computador (Silva & Silva, 2015).

Os hackers possuem amplo conhecimento em informática, sobretudo no que se refere à segurança dos sistemas operacionais e da informação e à linguagem de programação, o que confere a eles o domínio dos métodos de invasão mais efetivos. Quando o hacker atua com a intenção de invadir computadores e danificar ou subtrair informações, seja por motivos pessoais ou a serviço do crime organizado, ele é

chamado de cracker – como será mais aprofundado no próximo tópico –; então, o termo hacker refere-se ao gênero, e cracker, à espécie (Eufrásio, 2015).

Por meio de seus conhecimentos e práticas, o hacker pode acessar informações e dados, instalar programas, descobrir senhas, formatar o disco rígido e, até mesmo, ver a tela, assistir a vídeos e ouvir a voz do alvo, caso o equipamento conte com câmera e microfone, ou seja, ele é capaz de fazer escutas clandestinas, prática muito corriqueira entre criminosos que objetivam descobrir segredos industriais (Gimenes, 2013).

Contudo, há de se ressaltar que, muitas vezes, atribui-se uma percepção equivocada ao hacker. Esses indivíduos geralmente seguem um código ética e não empregam seus conhecimentos técnicos para o mal, mesmo que possam seus atos não corresponder aos dispostos legais (Oliveira, 2012). Sobre isso, Macedo (2015) explica que normalmente se utiliza a nomenclatura hacker para dizer daqueles que dominam plenamente os conhecimentos sobre computador e internet e que os utilizam para ações prejudiciais, no entanto nem sempre atuam contra equipamentos e/ou pessoas, mas utilizam aquilo que sabem para alertar os responsáveis pelos equipamentos e sistemas quanto às brechas na segurança, por exemplo.

É muito comum que organizações contratem hackers para que eles desenvolvam mecanismos de segurança que protejam o banco de dados e o sistema da empresa. Nesses casos, eles buscam as vulnerabilidades no sistema e indicam onde e como precisam ser aprimorados (Euzébio, 2014).

O *site* Alldas.de realizou um estudo que indica que, na atualidade, o Brasil é o país com a maior quantidade de hackers no mundo. Dos atos realizados por esses indivíduos, o estudo destaca invasões a IBM americana, ao Pentágono e à Microsoft. São vários os grupos brasileiros de hackers, sendo os mais famosos o Brazil Hackers Sabotage, o Silver Lords, o Demônios, o Prime Suspectz e o Tty0, conhecidos pela velocidade com que realizam seus ataques. O referido site classificou esses grupos como os mais ativos no planeta no que se refere a ataques a instituições governamentais e a grandes empresas (Gimenes, 2013). Inclusive, alguns hackers brasileiros estão abrindo fóruns e portais de discussão que tratam de segurança e atuam quando administradores expõem as vulnerabilidades de seus sistemas, invadindo as redes frágeis (L. R. Santos, 2011).

Cabe destacar que, assim como nas comunidades das ciências da computação, na sociedade a denominação hacker passou a ganhar novos sentidos, sobretudo a partir do surgimento do cibercrime, quando o termo começou a designar sujeitos que praticavam atos ilícitos a partir de meios informáticos. O hacker passou a ser visto como aquele que viola a segurança de sistemas para quaisquer finalidades, sendo que

a motivação de sua ação é o que estabelece o caráter ético ou antiético de sua conduta. A partir dessas motivações, nasceram três designações: 1) White hat hacker; 2) grey hat hacker; e 3) black hat hacker (J. L. A. Santos, 2011).

Os white hat hackers são os hackers que agem para aprimorar sistemas informáticos de terceiros, oposto do que fazem os black hat hackers. Agora, quando as características dos white e dos blach hat hackers são combinadas, tem-se o grey hat hacker. Ele pode acessar o sistema legítima ou ilegitimamente para identificar as vulnerabilidades existentes, oferecendo aos proprietários a oportunidade de reparar os erros. Se o serviço desse indivíduo para a reparação das falhas for oferecido em troca de dinheiro ou de cargo na empresa, então ele passa a ser classificado como black hat hacker. Mas, apesar de geralmente esse indivíduo não agir para a obtenção de benefícios ilícitos, as práticas por ele promovidas poderão contrariar os dispostos legais e o código de conduta ao qual estão submetidos os hackers (Heitor, 2015).

No caso brasileiro, é necessário a comprovação da existência de uma finalidade na ação, isto é, precisa haver dolo. Em uma situação de invasão não concedida, não haverá crime se não objetivar o que é proibido em lei. Essa situação permite as mencionadas atuação em que hackers violam sistemas para descobrir as vulnerabilidades e auxiliar no aperfeiçoamento da segurança dos mesmos (J. Q. Gomes, 2017).

Por fim, Vieira (2019) destaca que a forma mais adequada de se proteger a ataques de hackers é a partir do uso de softwares anti-hacking, que protegem os usuários contra vírus, spyare, malware, ramsoware, entre outros perigos.

4.2 Os Crackers

Como discutido no tópico anterior, muito embora seja atribuído ao hacker o caráter criminoso na atuação no meio digital, muitas vezes esses indivíduos atuam auxiliando a descobrir os crackers, estes sim criminosos. Os crackers usam seus conhecimentos para prejudicar bens jurídicos de terceiros a fim de obter vantagens (Silva & Silva, 2015). Nesse sentido, o termo “crackers” se empenha em denominar as pessoas que violam sistemas para invadir, roubar e danificar informações (Silva, Guariento, Queiroz, Resende, & Silva, 2013).

Na categoria crackers, há os chamados carders, especializados na fraude de cartões de crédito e boletos bancários. A ação dos carders se baseia na violação de portais virtuais de comércio eletrônico, na instalação sem autorização de programas em equipamentos alheios e na criação de sites comerciais falsos (Dantas, 2014).

As especificidades dos crimes informáticos mostram-se como barreiras ao trabalho no do legislador, pois dificultam sua previsão. A dinamicidade do meio digital

é uma das características mais relevantes nesse sentido, pois o surgimento de novas tecnologias é constante (J. Q. Gomes, 2017).

Recentemente, observou-se uma inovação denominada botnet, referente ao aluguel de controle de redes infectadas e controladas remotamente para suporte a quaisquer atividades ilícitas. Para coletar dados da maior quantidade de computadores possível, os hackers recorrem a instrumentos de scanning e, então, as informações obtidas são arquivadas em bases de dados. As vulnerabilidades identificadas nos softwares se mostram aos criminosos como possibilidades de ataques a milhares de computadores, portanto, estando esses equipamentos ao serviço dos agentes mal-intencionados. A botnet, dessa forma, serve para hackers e organizações criminosas como base para ataques.

Um desses ataques possíveis é o *Distributed Denial of Service Attack* (DDoS attack), que muito tem representado em prejuízos para organizações, que após as ações criminosas, perdem por determinado tempo o acesso ao seu sistema. Nesse ataque, ao contrário da grande maioria, a vítima não tem seu sistema invadido, a ação se dá por meio de uma sobrecarga de acesso simultâneo em seus recursos, e o resultado são prejuízos na casa dos milhares. Em 2012, inclusive, *sites* das instituições bancárias Bradesco e Banco do Brasil, como das empresas GOL e TAM sofreram com o DDoS attack (J. Q. Gomes, 2017).

Discorrendo sobre os benefícios financeiros alcançados pelos crackers, Costa (2011) destaca:

- Comercialização de informações de cartão de crédito;
- Aluguel de botnets (há registros de botnets que possuem mais de 1,5 milhão de computadores sobre seu controle. A partir deles, pode-se realizar o mencionado ataque DDoS.
- Comercialização de proxys abertos, que permitem o envio de spam e a comunicação entre agentes do crime;
- Furto de dados pessoais para chantagem;
- Roubo de valores de contas bancárias;
- Comercialização de seriais de programas proprietários.

A proliferação de robôs por meio das botnets é justificada pela sua eficiência de infecção; quando um computador é infectado, os demais equipamentos da rede também se tornam vulneráveis (Costa, 2011).

Crespo (2011) acrescenta que, entre os crackers, também existem os phreakers, aqueles que atuam na área da telefonia. Esses indivíduos fraudam o sistema de operação das ligações para captar as conversas de terceiros e, também, utilizar o telefone de outras pessoas em benefício próprio. A partir dessa ação de invasão aos

sistemas telefônicos, podem utilizar outras linhas para ligações, cujo pagamento será efetuado por outro usuário. Sobre os phreakers, Nogueira (2008) os descreve como o "terror das companhias telefônicas" devido à capacidade desses sujeitos de burlar seus sistemas, sejam eles de telefonia móvel ou fixa, cujas condutas resultam em prejuízos imensos.

Importa destacar que todo indivíduo que use tecnologias informáticas é possível alvo de crimes virtuais, estando o usuário conectado ou não à internet e independente do equipamento que utiliza. Nota-se, então, que não existe equilíbrio na relação entre sujeitos passivo e ativo, sendo que qualquer pessoa pode ser vítima, ao passo que, para atuar como agente ativo, é necessário amplo conhecimento para a prática desses crimes. Cabe dizer, ainda, a persistente desigualdade no acesso à informática a nível mundial, o que também corrobora o desequilíbrio aqui mencionado (Dantas, 2014).

4.3 Ataques registrados

A Europa assiste ao crescimento da criminalidade informática, seja esse crescimento no que se refere à quantidade, seja no que se refere à complexidade. Do mesmo modo, tem se tornado cada vez mais recorrente o uso de provas digitais e de ferramentas de anonimização e encriptação com o objetivo de cometer atos ilícitos. Dentre as ferramentas mais comuns nos ataques informáticos, está o software do tipo ransomware.

O mencionado ransomware é um tipo de software malicioso, isto é, um malware, cujo objetivo é invadir ilicitamente um sistema informático alheio. O que o distingue dos outros tipos de malwares é que ele não apenas causa danos ao sistema invadido, mas também o bloqueia ou aos seus dados para fins de solicitar valor de resgate à vítima; daí vem o seu nome: em inglês, "ransom" quer dizer "resgate". Os tipos mais modernos desse software são os crypto-ransomwares, que atuam na encriptação de determinados sistemas ou arquivos (Brito, 2016).

Em 2017, no dia 12 de maio, um ataque de hackers repercutiu a nível mundial, pois afetou quase 300 mil computadores de quase 100 países, dentre eles o Brasil, a Espanha, a Rússia, o Reino Unido, a Ucrânia e a Turquia. O instrumento de ataque foi um tipo de ransomware, que ficou popularmente conhecido como WannaCry, ou, na tradução, "vontade de chorar" (Carneiro, 2017).

Inclusive, o princípio básico da legalidade, previsto no Código Penal, fez com que os ataques informáticos específicos não fossem criminalizados pelo legislador europeu e português, sob a justificativa de que esses malwares ficam ultrapassados de forma rápida por conta da velocidade do desenvolvimento tecnológico. Desse modo, preferiu-se por punir o acesso ilegítimo em vez de especificar o tipo de ataque.

De modo igual, a danificação de dados por encriptação também é mencionada por outro tipo legal (Freitas, 2018).

Portanto, observa-se que o aumento da criminalidade informática nos últimos anos se mostra uma realidade mundial. Como exemplo, pode-se citar a estimativa de que esse tipo de crime cause um prejuízo de aproximadamente USD $ 3 trilhões em todo o globo, superando as expectativas para os danos causados pelo tráfico de drogas, que é de USD $ 1 trilhão. Os continentes serão mais afetados na seguinte ordem: primeiro a Ásia, seguida da Europa, depois as Américas do Norte e Sul. Com uma representação de mais de 75% dos ataques, o setor mais impactado por esses delitos é o financeiro, seguido do governamental, sendo atingido por 10,56% dos crimes. As indústrias de comunicação, de energia, setor industrial e o do comércio aparecem na sequência, com 8,41%, 3,71%, 1,98% e 0,05%, respectivamente (Freitas, 2018).

Ao tratar dos crimes informáticos e as suas características específicas, vê-se que algumas destas dificultam as investigações das ações ilícitas, sendo que podem ser destacadas a volatilidade e a efemeridade das informações arquivadas e transmitidas, que podem ser utilizadas de forma direta ou indireta no crime. Um meio de garantir a segurança e integridade de provas dos crimes, bem como preparar as autoridades policiais à dinamicidade com que os delitos informáticos acontecem, seria promover uma investigação preliminar guiada por unidades especializadas nesse tipo de ação criminosa (Dias, 2014).

Das diversas questões envolvidas na investigação desse tipo de crime, pode-se destacar como principais empecilhos a ausência de um método que contemple as particularidades do cibercrime, os sistemas ultrapassados e a falta de cooperação entre as entidades envolvidas. Somando-se as características específicas desse crime, a elevada quantidade de ocorrências, o grau técnico que compreendem, o seu caráter extraterritorial e as dificuldades de investigação, tem-se como resultado a morosidade no tratamento dos casos (Simas, 2014).

Importa ressaltar que o crime informático não se caracteriza como um crime fim, pois é uma ação que se dá apenas em ambiente virtual, excetuando as práticas de hackers que por vezes podem se enquadrar nos crimes de extorsão, falsidade ideológica, estelionato, fraude etc. Por isso, o comportamento criminoso pode ter o virtual como elemento de materialização, contudo nem sempre ocorre o mesmo com o crime (Lima, 2017).

Por fim, entende-se que o acesso não autorizado a um sistema ou rede informáticos caracteriza o crime de acesso ilegítimo, um delito informático técnico que tem o domicílio informático como o bem jurídico violado. Ribeiro (2015), discorrendo

sobre a segurança dos bens informáticos enquanto bem jurídico tutelado, explica as suas três dimensões: 1) a confiança no uso dos sistemas, a qual será abalada a partir da invasão aos mesmos; 2) os danos nos bens informáticos, possível consequência do ato criminoso, com malefícios aos programas, aos itens arquivados e ao próprio equipamento informático; 3) a tutela dos conteúdos, esses que, ao serem acessados ilegalmente, sofrem a violação do princípio da privacidade.

O pleno funcionamento das entidades públicas, das indústrias, do comércio e diversos serviços, hoje, dependem das plataformas informáticas, isto é, a sobrevivência da economia está atrelada a elas, assim como a descredibilização das atividades on-line pelos usuários consumidores também não é desejável. O bem jurídico em questão, portanto, é vocacionado nas esferas coletiva e individual (Ribeiro, 2015).

5 A PROVA DIGITAL / PROVA ELECTRÓNICA

As evoluções nas tecnologias de informação e comunicação vieram acompanhadas de novos desafios referentes à segurança e defesa nesses ambientes (cibersegurança e ciberdefesa) para impedir a ocorrência dos crimes informáticos. Mas não apenas isso, também foram apresentadas novas necessidades no que se refere à investigação judiciária e à prova digital (Gonçalves, 2017).

Em uma apresentação inicial, Ramalho (2017) explica que ainda não existe uma definição legal para a prova digital, o que não significa que esse tipo de prova foi esquecido pela legislação, haja visto que a lei menciona provas “em suporte eletrônico” e “em suporte digital”.

A forma como ela aparece nos dispostos levou à equivalência dos conceitos de prova eletrônica e prova digital, o que se sabe ser equivocado, ao passo que, em termos de amplitude, a prova digital está inserida no rol das provas eletrônicas. Esta última traz dados digitais e analógicos passíveis de manipulação, armazenamento ou transmissão entre redes e sistemas informáticos semelhantes. Por exemplo, as provas analógicas são digitalizáveis, mas não possuem origem no formato digital, como é o caso da revelação de fotos ou das gravações de fita de vídeo ou áudio (Sousa, 2018).

Nesse sentido, entende-se que prova digital é toda aquela que não é analógica. David Silva Ramalho (2017) explica que “digital” abarca diversas realidades tecnológicas e os sistemas não eletrônicos de comunicação, incluindo a internet. Por isso, segundo o autor, o termo mais adequado para tratar deste tipo de prova seria “prova eletrônico-digital”, que abrangeria a prova digital enquanto um dos elementos da prova eletrônica.

Uma definição mais simples e objetiva é apresentada pelo *Scientific Working Group on Digital Evidence*, que entende essa prova como uma informação arquivada e/ou transmitida de forma binária cujo valor é probatório (Scientific Working Group on Digital Evidence, 2016). Entretanto, o entendimento mais claro é o que define a prova digital como dados ou informações transmitidos ou armazenados na forma binária e que podem valer como prova, este que foi formulado na ISSO/IEC 270372.

De modo geral, portanto, quaisquer informações ou dados transmitidos ou arquivados em um dispositivo eletrônico se configuram como prova digital, mas, de forma mais específica, importa explicar que o termo “digital” indica que o dado armazenado ou enviado/recebido é repartido em sequência de números binários (0 e 1), cujo reconhecimento e tradução são feitos por aparelhos informáticos (Militão, 2012).

Contudo, conforme esclarece Gonçalves (2017), por não se apresentar ainda como uma categoria completamente autonomizada, para assimilar a prova digital faz-se necessário à recorrer à ampliação de interpretação de normas que tratam de outros tipos de prova, seguindo o CPP, art. 189º, que foi modificado em 2007 pela Lei n.º 47.

Mas é sabido que a prova digital merece um tratamento diferenciado, que seja com mais cautela, haja visto que ela pode ser anulada por quaisquer descuidos (Ramos, 2014). Nesse sentido, Fernandes (2017) esclarece que, por ser uma informação digital, sempre há a possibilidade de a referida prova ser alterada ou mesmo destruída, e isso sem deixar vestígios. Por esse motivo, é fundamental que a prova seja obtida e recolhida de forma rápida, o que determina o sucesso da investigação.

Então, esse é um tipo de prova que merece prioridade nos inquéritos, sendo que pode ser alcançada em um vasto espectro de tipologias criminais competentes à GNR. Além disso, acrescenta-se que as autoridades ainda têm muito a se desenvolver para se mostrar completamente apta a obter a prova digital, demonstrando a necessidade de capacitá-las nesse sentido, haja visto o maior desenvolvimento nessa área por alguns Comandos Territoriais (Mateus, 2016).

5.1 Características

Como a prova digital é um documento eletrônico, ou seja, uma sequência de números binários, não há como realizar a apreensão material da mesma, pois não é impressa ou assinada fisicamente e a sua autenticidade é comprovada em sua forma eletrônica, o que, por vezes, exige tecnologias e conhecimentos específicos, como ressalta Militão (2012). Rodrigues (2011) ainda contribui dizendo que, por se apresentar como uma prova instável, volátil, dispersa, fragmentada, invisível e facilmente manipulável e/ou apagável, são materiais que se mostram em grande nível de dificuldade de obtenção e manutenção.

Segundo explica Gonçalves (2017), a preservação da prova é indispensável, e as características específicas da prova digital a dificultam, justamente por ser passível se alteração ou destruição, um claro obstáculo para a manutenção de sua integridade e para o seu não repúdio.

Desse modo, no que diz respeito às especificidades da prova digital, compreende-se que o caráter tridimensional dos dados mostrados pelos ecrãs dos computadores aponta a invisibilidade desses materiais, e é justamente essa imaterialidade desse tipo de prova que a torna vulnerável e volátil, ao passo que é passível de manipulação e de destruição. Ademais, por estar contida em sistemas ou

em outros espaços virtuais, é indispensável que o acesso a esse material seja veloz e recorra a técnicas altamente qualificadas (Sousa, 2018).

Tendo a prova digital uma natureza instável e frágil, falar dela demanda destacar as inúmeras especificidades que ela traz consigo. Primeiro, importa destacar que a obtenção desse tipo de prova se diferencia do método de obtenção de provas físicas de outros tipos de delito. Por exemplo, nem sempre é preciso se deslocar até o local de realização do crime para colhê-la, sobretudo quando o delito cometido se configura como um cibercrime, isso porque a sua natureza é remota, assim como pode ser a sua forma de obtenção (Rodrigues, 2011).

Além disso, acrescenta-se que é possível hierarquizar algumas divisões de categorias de prova digital por ordem de relevância para a investigação criminal: 1) internet, por meio da qual se recolheu em sites de comunicação as primeiras provas digitais em investigações. Existem alguns softwares que recorrem internet exclusivamente para ocultação de identidade e localizar sujeitos que utilizam e compartilham informações. 2) computadores, por meio dos quais se faz o acesso à internet e nos quais ficam registrados os históricos e os arquivos temporários de navegação, elementos que podem servir de material probatório. 3) dispositivos eletrônicos portáteis, estes que podem ser os mais importantes e que recebem maior atenção dos investigadores; referem-se aos tablets, smartphones e telemóveis, dos quais podem ser recolhidos diversos tipos de provas materiais, como vídeos, mensagens de texto e áudio, fotos, localização GPS etc. (Goodison, Davis, & Jackson, 2015).

5.2 Tipificação

De acordo com Ramos (2014), a prova digital precisa ser incluída no rol de provas periciais, uma das classificações probatórias já tipificadas, isso porque ela exige de quem as recolhe uma qualificação técnica. Além disso, argumenta também que pode-se enquadrar a prova digital como prova documental, apesar de sua imaterialidade, ao passo que pode ser corporizada em meio físico, quando, por exemplo, se imprime uma mensagem de e-mail ou uma fotografia. Assim, demanda-se do investigador responsável pelo recolhimento da prova digital o conhecimento específico para lidar com esse material, e não apenas na recolha e manuseio, como também na análise posterior. A partir desse entendimento, nasceu a Lei n.º 32, de 17 de julho de 2008, que trata da conservação de dados produzidos ou tratados no cenário da oferta de serviços de comunicações eletrônicas, a ser tratada mais adiante.

A LC, em seu art. 2º, alínea b), estabelece dados informáticos como “qualquer representação de factos, informações ou conceitos sobre uma forma suscetível de

processamento num sistema informativo, incluindo os programas aptos a fazerem um sistema informático executar em função". Então, consideram-se como dados informáticos programas de sistemas informáticos, documentos eletrônicos e dados pessoais, de localização ou de tráfego (A. T. S. Oliveira, 2017).

Estes são divididos em quatro categorias, conforme descrição de Ana Teresa Seabra Oliveira (2017):

- Dados de localização, caracterizados por indicarem a localização geográfica do equipamento terminal dos utilizadores de serviços de comunicação eletrônica que sejam disponíveis publicamente. Além disso, esses dados também apontam o destinatário de uma comunicação;
- Dados de tráfego, que são informações técnicas ou informáticas referentes a comunicações dadas por meio de tecnologias de informação e comunicação, que contêm dados quando à origem, à hora, à duração, aos trajetos e aos serviços subjacentes da comunicação;
- Dados de base, os pessoais relacionados à conexão à rede de comunicações. Compõem esta categoria a identidade do assinante, bem como o número e a morada deste;
- Dados de conteúdo, cujas informações dizem respeito ao conteúdo de uma mensagem ou comunicação (A. T. S. Oliveira, 2017).

A partir dessa distinção, é possível afirmar que as categorias de localização, base e conteúdo são sustentadas pelos dados de tráfego. Ademais, importa destacar que, em uma investigação, os dados de localização e de tráfego podem ser requisitados pelas autoridades judiciária ou policial e, no caso de rejeição a esse pedido, como ocorre em determinados meios de obtenção de prova, os operadores de telecomunicações que não obedecerem ao requerimento incorrerão em crime de desobediência. Quanto aos dados de base, ressalta-se que a única situação em que o acesso a eles não é permitida se dá quando o respectivo tutelar das informações se apresenta contrário à publicação das mesmas, prerrogativa esta disposta em contrato quanto da contratação de um serviço de telecomunicação. Por fim, explica-se que o tratamento concedido aos dados de conteúdo segue os preceitos estabelecidos no CPP, arts. 187º e 189º, que dispõem sobre as escutas telefônicas (A. T. S. Oliveira, 2017).

5.3 Princípios

Os princípios que estabelecem os limites e restrições às provas digitais, independentemente de sua categoria específica, são os mesmos que regem os demais meios de obtenção de prova. Assim, por exemplo, por meio do princípio da

verdade material, ou da investigação, o tribunal é incumbido de competência para ordenar os meios de prova imprescindíveis para a busca da verdade, ao passo que os excessos na procura da verdade material são impedidos pelo princípio da verdade processual. Também é possível mencionar o princípio da livre apreciação de prova, que, segundo a redação do art. 127º do CPP, impõe que a prova deve ser avaliada conforme as regras da experiência e a livre convicção do julgador, com exceção dos casos em que a lei preveja atuação distinta (Gonçalves, 2017).

Não se pode deixar de mencionar que, para Rodrigues (2009), não apenas os princípios referentes à prova dispostos no processo penal devem ser aplicáveis à obtenção da prova digital, como também aqueles apresentados na *International Hi-Tech Crime and Forensics Conference*, de 1999.

5.4 Leis reguladoras

Buscando contemplar os novos riscos advindos da era digital e em uma tentativa de cumprir com os deveres internacionais, promoveu-se uma atualização na legislação portuguesa de modo a regular a prova digital. Nessa busca, optou-se por criar uma legislação avulsa com diversos meios de obtenção desse material (Matias, 2020). Nasceu, assim, em 2009, a Lei n.º 109, conhecida como Lei do Cibercrime.

A Lei do Cibercrime surgiu como consequência do ato de ratificação de Portugal à Convenção sobre Cibercrime de Budapeste, passando a ser uma lei bom abrangência bastante grande, uma vez que criou tipos penais novos específicos sobre crimes praticados na esfera digital, dispondo também sobre regras processuais penais novas, a exemplo da obtenção de provas feitas através de meios especificamente voltados para o ambiente digital (Fidalgo, 2019).

Antes da promulgação dessa lei, Portugal não contava com um regime que regulamentasse a obtenção da prova digital de forma detalhada e específica. Diferente do que se vê na Alemanha, por exemplo, cuja referida regulação existe desde 1968, em disposições do Código de Processo Penal do país e pela denominada Lei de Restrição do Segredo Postal, de Correspondência e das Comunicações à Distância (Marques, 2014).

O ordenamento jurídico português ganhou sua primeira referência aos dados informáticos em 1976, quando o art. 35º da Constituição mencionou a proteção aos indivíduos contra tratamentos informáticos de dados privados. A interpretação dessa redação foi ampliada a partir de revisões posteriores no texto constitucionais, chegando a abordar o acesso não autorizado de terceiros a dados informáticos pessoais (Venâncio, 2011).

Como esse tipo de prova se mostrava uma novidade para a qual o ordenamento jurídico ainda não apresentava regulamentações, duas propostas foram apresentadas: o Projeto de Lei n.º 208/IX, que dispunha sobre a "proteção dos dados pessoais e a privacidade das comunicações eletrônicas na sociedade de informação, procedendo à transposição da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2012"; e outra, que tratava do "Regime Jurídico da obtenção de prova digital eletrônica na Internet", apresentada no Projeto de Lei n.º 217/IX. Muito embora nenhuma dessas propostas tenham vigorado, elas inspiraram a elaboração da Lei n.º 32, de 17 de julho de 2008, que dispôs acerca da conversação de dados produzidos ou tratados no contexto da oferta de serviços eletrônicos de comunicação (Monteiro, 2016).

Dias (2015) ainda destaca que, considerando as evoluções na legislação, os Projetos de Lei n.^{os} 217/X, 240/X e 367/X e a Proposta de Lei n.º 155/IX, muito embora proponham soluções importantes no que se refere à obtenção da prova digital, não se fizeram relevantes na ordem jurídica de Portugal, o que se explica por um cenário de instabilidade política.

Importa destacar também que são visíveis algumas debilidades nas opções legislativas da LC e da Reforma do CPP. Por exemplo, a referida reforma demonstrou não ponderar acerca da diversidade de dados no que se refere à recolha de prova eletrônica, bem como não dispôs sobre o acesso a comunicações eletrônicas por meios telemáticos em uma adaptação deste ao regime da apreensão da correspondência, de modo a assegurar proteção a bens jurídicos em diversos âmbitos (Mesquita, 2010a). Já na LC, vê-se a opção por uma via sistemática não vinculada ao CPP.

Nesse contexto da prova digital e considerando a regulamentação internacional, três diplomas merecem destaque pelo efeito que causaram: 1) a Convenção sobre o Cibercrime, de 2001; 2) a Decisão Quadro 2005/222/JAI, do Conselho, de 2005; e 3) a Diretiva 2006/24/CE, do Conselho e do Parlamento Europeu, de 2006 (Pratas, 2018).

Paulo Dá Mesquita (2010b) explica que duas linhas problemáticas no âmbito processual decorreram do desenvolvimento tecnológico, no sentido de que impactaram no modelo tradicional de se tratar os materiais probatórios. A primeira diz respeito à intromissão em comunicações que só dessa maneira podem ser recolhidas; a segunda trata da fixação do acontecimento, dado que os meios tecnológicos registram as informações para o futuro. Andrade (2013) complementa que esses métodos de investigação intrusivos, os quais, ao menos na etapa de recolhimento da prova digital, não precisa ser escondido do visado.

5.4.1 Código de Processo Penal

Ao longo do tempo, o atual CPP sofreu diversas modificações em seus dispostos. Em sua versão inicial, de 1987, a disposição sobre as escutas telefônicas vinha no art. 190º, que atribuía as comunicações ou conversações realizadas por meio de qualquer meio técnico que não o telefone o mesmo tratamento previsto pelos arts. 187º ao 189º. Isso significa que aos demais meios técnicos aplicava-se o regime das escutas telefônicas (Pratas, 2018).

O meio de obtenção de prova do qual discorrem os arts. 187º ao 189º do CPP, como explicado outrora, é entendido como a última opção a ser adotada em um processo de investigação, justamente por não haver meio de limitar os atingidos por essa prática, que pode recair sobre terceiros e objetos outros que não são alvos de investigação, bem como por violar diversos direitos fundamentais. Para exemplificar, pode-se imaginar uma situação em que um criminoso é alvo de escuta telefônica por conta de seu envolvimento com o tráfico de drogas. O emprego desse meio de prova poderá descobrir, também, os parceiros de negócio desse indivíduo, assim como seus clientes e as ações vinculadas às ações ilícitas do referido crime. Também existem casos em que as informações segregadas pelas comunicações se mostram mais relevantes que o conteúdo mesmo da comunicação, entretanto importa destacar que a ordem jurídica não protege todos os dados obtidos na comunicação (Andrade, 2009).

Vera Marques Dias (2012) explana que as evoluções tecnológicas e informacionais invadiram todos os âmbitos das vidas dos indivíduos, não deixando de chegar nas práticas criminosas, que com elas se aperfeiçoaram, o que demandou alterações dos preceitos legais vigentes.

Nesse sentido, mudanças importantes decorreram da reforma do CPP em 2007, tais como a inversão na ordem dos arts. 189º e 190º, quando o primeiro passou a tratar da abrangência do regime das escutas telefônicas, e o segundo do efeito de nulidade (Pratas, 2018).

A partir da mencionada reforma, o art. 189º, em seu n.º 1, estabelece à interceção das comunicações a aplicação do regime das escutas, conforme mencionado, além de ressaltar a interceção de correio eletrônico e demais formas de envio/recebimento de dados por meios telemáticos, ainda que estes estejam armazenados em suportes digitais. O n.º 2 desse mesmo artigo afirma ainda a aplicação do regime de escuta aos dados de tráfego e de localização de celular (Pratas, 2018).

No entanto, Paulo Dá Mesquita (2011) revela que esse processo de reforma apresenta uma grande lacuna, ao passo que ele entende que as modificações dela

advindas indicam um pensamento que não corresponde à exigências necessárias frente ao desenvolvimento tecnológico e seus efeitos na interação comunicacional e nos registros de dados.

No contexto português, além do CPP, a já mencionada Lei n.º 32/2008 também trata da prova digital, discorrendo sobre a conservação dos dados gerados ou tratados nos meios de comunicações eletrônicas. Assim também o faz a também já referida Lei do Cibercrime (Pratas, 2018).

No entendimento de João Conde Correia (2014), a soma desses três documentos corrobora, na verdade, uma incoerência nas regulamentações desse tema, bem como prejudica a boa prática nos casos que o envolvem. Nesse sentido, o autor vê que a questão da prova digital ainda apresenta lacunas, especialmente no campo normativo. Pinho (2012) também argumenta que articulação das três mencionadas leis resulta em problemáticas, sobretudo no que envolve a compreender como aplicá-las de forma conjugada e o regime que advém da combinação delas.

Armando Dias Ramos (2015b) afirma que a Convenção do Cibercrime, de 2001, inspirou a Lei do Cibercrime vigente em Portugal. No entanto, ressalta que o desenvolvimento da tecnologia nos anos que se passaram desde então foi enorme. Silveira (2016) destaca a fala de Joana Marques Vidal, procuradora-geral da República, que, em conferência realizada em 2016, ressaltou os desafios impostos pela criminalidade na internet, pontuando a urgência em avaliar a legislação existente no sentido de identificar as modificações necessárias para que essa questão seja plenamente coberta. O indivíduo que pratica delitos digitais, sobretudo se membro de grupos organizados, geralmente apresenta conhecimentos informáticos altamente qualificados e detém os meios tecnológicos mais atualizados, fato este que vem sendo desconsiderado pela legislação.

A dispersão do tema da prova digital em vários documentos legais impõe obstáculos na aplicação coerente do regime e, para assegurar uma centralidade normativa adequada, é preciso que tal matéria seja incluída no CPP (Campos, 2019).

Frente a esse cenário, encontram-se diversas opiniões e propostas que buscam solucionar a questão. Por exemplo, Renato Lopes Militão (2012) defende a integração das normas regulamentadoras da obtenção da prova digital ao CPP; enquanto Manuel Da Costa Andrade (2009) argumenta em favor da elaboração de um regime mais amplo no próprio CPP acerca dos meios de intromissão nas telecomunicações, entendendo a insuficiente dos dispostos no art. 189º desse documento.

Assim, vendo o CPP como defasado no que se refere à atualidade eletrônica e digital, esta que demanda alterações nos deveres internacionais do Estado de Portugal, dois novos regimes passaram a compor o ordenamento jurídico do país, os

quais apresentam disposições acerca da obtenção de prova digital. São, desse modo, três regimes que regulamentam a questão, sendo eles o próprio CPP, em seus arts. 187º ao 190º, a Lei n.º 32, de 17 de julho de 2008, e a Lei do Cibercrime (Freitas, 2017).

5.4.2 Lei nº 32 / 2008, de 17 de Junho

A partir da promulgação da Lei n.º 32, em 2008, o ordenamento jurídico passou a obedecer à Diretiva n.º 2006/24/CE, do Conselho e do Parlamento Europeu, esta que se refere à conservação de dados produzidos ou tratados no contexto da oferta de serviços eletrônicos de comunicação de redes públicas ou publicamente disponíveis, conforme explanado anteriormente.

Desse modo, tornando ainda mais complexas as dificuldades na interpretação advinda, principalmente, das modificações do CPP, a referida lei passou a regular a conservação e a transmissão de dados de localização e de dados, além de outros relevantes para a identificação do usuário com objetivos investigativos.

A redação dessa norma diz que só serão admissíveis os dados transmitidos em casos que evidenciem motivos que os demonstrem como imprescindíveis para a descoberta da verdade, em despachos fundamentados do JIC e em alguns crimes específicos, sempre obedecendo aos princípios da necessidade, da adequação e da proporcionalidade.

Além disso, também impõe que os dados transmitidos podem ser referentes unicamente ao arguido ou ao suspeito, incluindo aqueles a quem recai a suspeita de transmitir ou receber mensagens provenientes ou destinadas a aquele. Os dados da vítima só podem ser transmitidos quando houver autorização dela.

Vê-se, então, que muito embora o legislador convoque requisitos de acesso próximos, os regimes foram duplicados sem que houvesse algum motivo técnico para tanto, resultando nas normas especiais dispostas na Lei n.º 32/2008 e nas normas gerais do CPP.

Vale destacar, assim como faz Ribeiro (2015), que apesar de a Diretiva 2006/24/CE prever um período máximo de dois anos para a conservação dos dados, a mencionada lei de 2008 estabelece um ano a esse limite. Ressalta-se, entretanto, que a investigação, descoberta e repressão de crimes graves serão as finalidades exclusivas da conservação de dados, esta cuja autorização advém de despacho fundamentado da autoridade julgadora, conforme dispõe a Lei de Retenção de Dados, nos n.^{os} 1 e 3 do art. 3º).

Pontua-se que o regime jurídico do cibercrime aqui em vigor se estabelece sob influência europeia, sobretudo da Convenção do Cibercrime.

5.4.3 Lei nº 109 / 2009, de 15 de setembro 28 (Lei do Cibercrime)

Diante dos vazios legislativos no que se refere à prova digital, publicou-se, em Portugal, a Lei n.º 109, de 15 de setembro de 2009, também chamada de Lei do Cibercrime, que entrou em vigor a partir de outubro daquele ano. Essa lei, assim como a Resolução da Assembleia da República n.º 88/2009 e o Decreto do Presidente da República n.º 92/2009, foram publicadas oito anos após a Convenção sobre o Cibercrime. A referida resolução aprovava a Convenção, e o decreto a ratificava; enquanto a Lei do Cibercrime veio para adaptar o ordenamento jurídico do país à Convenção e à decisão do Conselho referente a violações a sistemas de informação, a Decisão Quadro n.º 2005/222/JAI (Fernandes, 2017).

Os tipos penais incluídos pela Lei n.º 10, de 1991, que tratava da criminalidade informática, foram mantidos na Lei n.º 109/2009, entretanto esta apresentou outros tipos. Mas as inovações mais significativas para o direito interno de Portugal dizem respeito aos meios de prova, ao passo que esse diploma foi o pioneiro no país a abranger um regime próprio de obtenção da prova digital, superando, desse modo, as lacunas existentes a partir da lei anterior (Mann, 2018).

Sob um olhar sistemático, a estrutura da Lei do Cibercrime se mostra tripartida, com disposições processuais, materiais e acerca da cooperação entre os Estados no que se refere à matéria penal e às equivalências ao que se estabeleceu na Convenção sobre o Cibercrime. Importa dedicar maior atenção ao Capítulo III da referida lei, que traz disposições processuais, tais como da preservação e da revelação de dados, da injunção para a concessão de acesso ou preservação dos dados, a análise e a apreensão de dados informáticos, do correio eletrônico e dos registros comunicacionais de natureza semelhante e da intercepção de comunicações, itens dispostos, respectivamente, entre os arts. 12º e 18º (Fernandes, 2017).??

De forma resumida, quanto ao recolhimento e conservação da prova digital, pode-se dizer que a Lei do Cibercrime foi inovadora, pois apresentou meios ainda não existentes de obtenção de provas, contidos nos arts. 12º ao 14º do LCC. Além disso, regulou algumas legislações já previstas, mas que, antes, não se enquadravam nos crimes informáticos e no ambiente digital, como se vê no LCC, arts. 15º ao 19º (Pereira, 2019).

A regulação das relações entre as autoridades judiciárias e os fornecedores de serviços está prevista entre os arts. 12º e 14º, principalmente no que se refere à obtenção, revelação e preservação de dados. De modo mais específico, o art. 12º dispõe que, quando se mostrar necessária a obtenção de determinados dados

informáticos arquivados em um sistema informático, o MP deve entrar com requerimento para que o juiz de instrução criminal demande a um fornecedor de serviço de comunicação a disponibilidade ou o controle desses dados. A justificativa para essa necessidade se mostra quando comprovado o receio de alteração, manipulação ou exclusão desses dados (Silveira, 2016).

No entanto, não se pode excluir a possibilidade de que os dados almejados pela ordem da autoridade judiciária se percam antes mesmo que os fornecedores de serviço de comunicação consigam resguardá-los, haja vista que uma das características do crime informático é o alto conhecimento técnico e informático dos agentes envolvidos na prática ilícita. Ademais, o nível de prática dos cibercriminosos pode resultar em um cenário no qual o MP sequer tenha conhecimento desses dados (Silveira, 2016).

Já os arts. 15º e 16º tratam da pesquisa e apreensão de dados informáticos encontrados e que se mostrem de relevância probatória. A redação desses dispostos indicam que se trata de um regime em que a obtenção de dados em tempo real não se torna possível, tampouco se pode realizar a pesquisa ou a apreensão de dados remotamente, exigindo que estas sejam feitas fisicamente no sistema visado (Silveira, 2016).

O art. 19º, por sua vez, não abrange a prova digital de forma específica, discorrendo sobre as ações encobertas e admitindo o uso destas no decurso de inquérito conforme as disposições na Lei n.º 101/2001. Alguns crimes não mencionados no Regime Jurídico sobre as Ações Encobertas são adicionados no n.º 1 do referido artigo, fato que se mostra alvo de crítica por parte de alguns doutrinadores, sob o argumento de que a ampliação desse rol de crimes figura uma associação entre os crimes informáticos e aqueles cometidos pelo computador e de que acaba por prever medida de caráter excepcional a uma quantidade extensa de crimes, mas sem, para tanto, se aprofundar nos princípios da necessidade e da proporcionalidade (Marques, 2014).

A Lei 101, de 2001, mencionada no parágrafo anterior, de acordo com o seu art. 1º, entende como ações encobertas “aquelas que sejam desenvolvidas por funcionários de investigação criminal ou por terceiro atuando sob o controle da Política Judiciária para prevenção ou repressão dos crimes indicados nesta Lei, com ocultação da sua qualidade e identidade”. O artigo seguinte apresenta o leque de crimes sobre o qual essa técnica de investigação será admitida, e ao qual são incluídos os crimes dispostos na Lei do Cibercrime. A ação encoberta é permitida por esse regime jurídico com o fim de prevenir e repreender a criminalidade, no entanto, exige-se a comprovação de indícios mínimos que indiquem o delito (dentre os dispostos no

catalogo do art. 2º da referida lei e no art. 19º da Lei do Cibercrime) ou a preparação para ele (Marques, 2014).

A infiltração também poderá ser empregada enquanto instrumento de prevenção de crime e como meio de recolhimento de provas em investigação criminal ocorrida depois da consagração do fato. Não há, na Lei da Infiltração, distinção entre agente infiltrado, encoberto e civil, o que, como consequência, permite a interpretação de uma equivalência entre essas formas de atuação, o que não seria correto. Tendo a Lei n.º 101/2001 uma aproximação lógica com a atuação do agente infiltrado, vê-se que não existe adequação entre esta e a atuação policial nas formas de encoberto e civil (Marques, 2014).

No entendimento de Militão (2012), quanto à obtenção de prova digital, diversos meios processuais foram consagrados pela Lei n.º 109, de 2009. Mais que isso, estabeleceu também obrigações de terceiros, mecanismos agressivos, perigosos e intrusivos de cooperação internacional. Neves e Correia (2014) e Pereira (2019), por sua vez, pontuam que, muito embora tenha previsto as buscas tradicionais, a Lei do Cibercrime não admitiu as buscas on-line por tratar-se de uma forma oculta de investigação e recolhimento de dados informáticos, da qual não se teria conhecimento em casos cuja notificação não fosse obrigatória.

Assim, pode-se dizer que o espectro de utilização das ferramentas dispostas na Lei do Cibercrime tem maior amplitude do que a própria lei em si, isso porque, provando-se necessário o recolhimento de prova digital, ela pode ser aplicada em investigações de qualquer crime previsto na lei – já que as disposições dos arts. 12º, 13º, 14º, 15º, 16º e 17º são de aplicação geral. Contudo, importa ressaltar que a aplicabilidade dos arts. 18º e 19º é restringida pelo art. 11º, haja visto o caráter intrusivo dessas previsões (Marques, 2014).

No entanto, alguns pontos despertam incertezas, sobretudo quando se fala em uma visão conjunta das leis n.os 32/2008 e 109/2009 e do CPP. Hoje, a obtenção de dados é prevista tanto pela Lei n.º 32/2008 quanto pelo CPP, art. 189º, n.º 2. Mas é possível constatar que as duas leis aqui citadas acabam por revogar o art. 189º do CPP, pois, segundo esclarece João Conde Correia (2014), elas se sobrepõem ao regime geral, que acaba por sobreviver somente naquilo que não foi regulamentado especificamente em momento posterior.

Inclusive, uma das críticas mais recorrentes no que concerne à relação entre CPP e Lei do Cibercrime refere-se à assimilação do correio eletrônico em curso ao regime das escutas telefônicas ao rol de crimes previstos no art. 187º do CPP, o que, como resultado, acabaria por impor restrições relevantes ao acesso a esses materiais

pela investigação de cibercrimes e, consequentemente, ao recolhimento de provas digitais (Monteiro, 2016).

Nesse contexto, Fidalgo (2019) explica que a utilização cada vez maior da prova digital no processo penal, fundamentalmente das mensagens enviadas por correio eletrônico e análogos, se faz merecedora de destaque dentre os demais meios de prova, dispostos de forma natural no diploma legal português em matéria de Direito Processual Penal. Continua hoje sem saber as razões pelas quais o legislador omitiu essas processuais diligências de em prol do recolhimento de provas digitais do Código de Processo Penal, talvez evitando assim que houvesse dificuldade na harmonia com as normas existentes no próprio código (art. 179.º e 189.º) e já agora aproveitando para revogar formalmente o art. 189.º do CPP, uma vez que foi substituído pelo art. 17.º.

Apesar disso, amplia-se o âmbito de aplicação a partir da disposição do art. 17º da Lei 109, de 2009, que admite a obtenção do correio eletrônico nas situações em que se investigam crimes efetivados por meio de um sistema informático ou, conforme art. 11º, n.º 1, em que se comprove a relevância de recolhimento de prova em ambiente digital (Monteiro, 2016).

De qualquer forma, uma vez que regras especiais foram introduzidas em prol da recolha de provas eletrônicas, esta mostrou ser uma inovadora lei no ordenamento jurídico de Portugal, visto que anteriormente ao seu vigor, os crimes da esfera digital eram investigados tendo por base as regras gerais instituídas no CPP (Fidalgo, 2019), uma vez que, mesmo existindo uma lei denominada de Lei de Criminalidade Informática, só constavam dela normas substantivas as quais não contribuíam na específica investigação dos crimes tipificados.

5.5 Obtenção das provas digitais e boas práticas

Mesmo com as adaptações necessárias, os meios de obtenção da prova digital se mostram as tradicionais previstas no CPP, ou seja, buscas, apreensões, revistas, exames ou intercepção de comunicação (Nogueira, 2016).

Ressalta-se que não pode existir relação física entre o dado digital gerado, arquivado e compartilhado entre os dispositivos e a pessoa enquanto indivíduo que pode ser proprietário das referidas informações. Isso, diversas vezes, mesmo não se tratando de uma situação geral e abstrata, mostra-se como um obstáculo para conseguir a autorização de acesso a determinados meios de obtenção de prova. Mas, certamente, essa não é a única dificuldade na obtenção da prova digital (A. T. S. Oliveira, 2017).

A Lei do Cibercrime consagra, em seu art. 15º, a pesquisa de dados informáticos enquanto meio de obtenção de prova e, sobre isso, pode-se dizer que, interligando com os dispostos nos dois artigos seguintes do mesmo documento, que tratam, respectivamente, da apreensão de dados informáticos e da apreensão de correio eletrônico e registos de comunicação de natureza semelhante, enquadram-se na previsão da Conversão do Cibercrime, art. 19º (Sousa, 2018).

Primeiro, o art. 15º da Lei do Cibercrime prevê que, objetivando alcançar a verdade, a autoridade judiciária poderá autorizar ou despachar ordem para a pesquisa de dados informáticos arquivados em sistema informático específico (cujos termos para essa pesquisa estão indicados no n.º 4 desse artigo), atentando ao fato de que isso será admissível quando a ação for imprescindível para a produção de prova. No entanto, essa autorização antecipada do juiz é dispensado nas situações apresentadas no n.º 3, alíneas a) e b), do art. 15º (Sousa, 2018).

Assim, é possível dizer que, conforme as disposições do artigo citado acima, a pesquisa de dados informáticos se configura como uma busca realizada em um ambiente informático ou digital, mas cuja efetivação deve acontecer de forma presencial, obedecendo ao princípio da legalidade, já que não existe nenhuma previsão que admita buscas on-line (Morais, 2012).

Rogério Bravo (2013), professor e inspetor-chefe da Polícia Judiciária de atuação na área da criminalidade informática, explica que, resumidamente, o direito penal da criminalidade informática tutela a confidencialidade, a integridade e a disponibilidade dos dados, assim como, nas diversas etapas de integração tecnológica, também protege a confidencialidade, a integridade e a disponibilidade do processamento eletrônico, possibilitando a busca, o armazenamento e a transmissão dessas informações.

No que diz respeito à aquisição ou recolhimento de prova, a palavra “prova” indica que o tribunal deve reconhecer o responsável por essa recolha, de modo que esse processo siga a lei no que concerne à produção de prova. Já no que se refere às peculiaridades, aos requisitos e aos princípios de validade da prova digital, compreende-se que esta também precisa respeitar os paradigmas legais para sua admissibilidade. Além disso, a prova precisa ser apresentada em uma linguagem mais simples, entendendo que os operadores judiciários nem sempre compreenderão a linguagem técnica; precisa ser durável e, portanto, demanda-se cuidado no recolhimento e conservação desta; e precisa ter um padrão uniforme na produção de prova, o que significa que as regras para tal devem ser as mesmas em todas as suas formas de apresentação e em todos os níveis de investigação forense digital (Rodrigues, 2011).

Cabe dizer, também, que são raras as situações em que esse tipo de prova é encontrado no local de realização do crime e a apreensão só se faz de forma imaterial, exigindo um conhecimento informático qualificado, sujeita, portanto, a erros humanos e/ou das máquinas (Freitas, 2017). Armando Dias Ramos (2017) ainda acrescenta que, por essas particularidades, o sucesso da investigação depende diretamente da velocidade e da qualidade na obtenção da prova.

Apesar de a Lei do Cibercrime se mostrar inovadora e representar relevância significativa no combate à criminalidade informática, há de se constatar sua potencial força para violar direitos, liberdades e garantias. Por isso mesmo, o uso das ferramentas nela dispostas demanda cautela, de modo a evitar ao máximo afetar os direitos fundamentais dos indivíduos. Nesse sentido, Militão (2012) argumenta que, aplicando os meios de obtenção de prova previstos na referida lei, corre-se o risco de degradar as garantias processuais do arguido e do suspeito, e essa degradação é um dos principais elementos de um Estado punitivo.

Então, defende-se que as OPC e JIC devem utilizar de forma apropriada os recursos em ordem da busca da verdade material e da autoria de um crime, unicamente quando esses se mostrarem realmente necessários, respeitando os princípios da necessidade e da proporcionalidade, sem extrapolar os limites para se alcançar a prova, tal como dispõe o art. 18º da CRP, em seu n.º 2. Ademais, há necessidade obrigatória de se justificar sempre quando se fizerem presentes as restrições aos direitos fundamentais, de modo que essa justificativa assegure outros direitos e interesses constitucionais. Justamente por isso, quaisquer meios de obtenção de prova só pode ser utilizado quando houver autorização judicial ou do visado, independentemente se a prova buscada seja tradicional ou digital (Rodrigues, 2010).

Vale ressaltar que os meios de obtenção de prova como, por exemplo, escuta telefônica ou acesso a dados de localização de celular e de tráfego, devem mirar um suspeito específico, nunca sendo admitida o recolhimento de informações de quantidades abstratas de indivíduos; nesse sentido, sem a determinação de um suspeito, impõe-se uma barreira aos meios de obtenção de prova digital. A Lei n.º 32/2008 destaca apenas uma ressalva a essa norma, estabelecendo que as informações privadas produzidas ou armazenadas em serviço de comunicação eletrônica ou em uma comunicação eletrônica a partir das redes públicas de comunicações eletrônicas estão à ordem do Estado Português por um grande intervalo de tempo (Rodrigues, 2009).

Desse modo, observa-se que o combate à criminalidade informática pelo Estado tem como um dos principais entraves os próprios direitos fundamentais. O que se tem

assistido é a um processo penal neoliberal que se mostra demasiadamente intrusivo, imediatista, desleal e secretista. São muitos os casos de investigação criminal nos quais informações ora confidenciais alcançam números indiscriminados de pessoas, o que representa um risco significativo de que tais informações sejam utilizadas com objetivos distintos do que se pretendia originalmente (Pereira, 2019).

Renato Lopes Militão (2012), por sua vez, propõe uma forma mais ampla e simples de regime processual penal para a prova digital a partir do entendimento da necessidade de mudanças que atendam a realidade da investigação na atualidade. Além disso, também propõe uma especificação no que diz respeito aos meios de obtenção desse tipo de prova, ressaltando que esse processo deve ocorrer de maneira rápida e eficaz, o que, muitas vezes, não tem acontecimento.

Comparando o processo de recolhimento da prova digital à recolha de material biológico, Ramalho (2017) comenta que a atuação do especialista no que se refere ao primeiro tipo deve ser semelhante à do especialista que realiza o recolhimento de material biológico para análise posterior. Então, o que se argumenta é que o responsável pela detecção de vestígios e o recolhimento desses deve ser munido de conhecimentos técnicos qualificados, bem como devem ser distinguidas as etapas de identificação da prova e a da perícia.

Quando a obtenção de provas se dá em smartphones, o dispositivo deve ser recolhido e, em seguida, os conteúdos guardados no equipamento devem ser apreendidos pelas autoridades judiciárias com o objetivo de buscar provas incriminatórias. Contudo, como muito já se mencionou, são várias as ocasiões em que os investigadores se deparam com materiais com encriptação, o que dificulta o acesso aos dados ali armazenados, tornando mais complexo o processo de obtenção de prova digital (Fernandes, 2017).

Outra situação possível é a da danificação da informação e a consequente alteração do material probatório. O armazenamento inadequado pode ser responsável isso, já que radiação ultravioleta e umidade podem causar esse tipo de prejuízo e, como resultado, inviabilizar o uso do meio de descoberta da verdade (A. T. S. Oliveira, 2017).

Em Portugal, os métodos de obtenção de prova digital decorrem da norma internacional acerca das tecnologias de informação, técnicas de segurança e diretrizes para a identificação, aquisição, recolhimento e preservação da prova digital, nomeada ISO/IEC 27037, de 2012. Além dela, no mesmo ano, uma recomendação foi elaborada pelo CERT.PT, a qual apresentava de forma genérica os cuidados necessários no recolhimento de provas, aconselhando especificidades e ferramentas conforme o tipo de crime (Marques, 2013).

A obtenção de prova digital conta com três categorias mais relevantes, segundo o *Scientific Working Group on Digital Evidence*: 1) as equipas de primeira resposta, nas quais estão inseridos os responsáveis pelo recolhimento desse tipo de prova no que se refere à cena do crime e às buscas; 2) os examinadores e analistas, cujas atribuições são a recuperação e a análise de vestígios digitais; e 3) os técnicos, incumbidos de coletar e preparar esses vestígios para exame e análise subsequentes (Scientific Working Group on Digital Evidence, 2004).

O emprego as práticas adequadas e específicas na obtenção de provas digitais se mostra determinante. Silva (2018), em sua pesquisa por meio de entrevistas e questionários com militares investigadores, verificou que esses profissionais não se consideravam plenamente aptos para trabalhar com a prova digital, o que evidencia a urgência de uma formação mais aprofundada nesse quesito.

Para que as novas tecnologias amparem a Justiça, é fundamental que o investigador criminal saiba lidar com os instrumentos tecnológicos de modo a conseguir enfrentar os desafios impostos pelas peculiaridades do ambiente informático. É determinante também que esses profissionais contem com formação e treinos que os capacitem para essa tarefa, fornecendo-lhes os conhecimentos científicos e técnicos exigidos para o bom uso das ferramentas informáticas, o que contribuiria de forma efetiva com o êxito do processo de obtenção de provas digitais (Silveira, 2016).

5.6 As dificuldades colocadas pela prova digital

As especificidades técnicas da prova digital a tornam um material delicado, passível de inutilização por conta de simples descuido. Sobre isso, Ramos (2015a) afirma que vários fatores tornam esse tipo de prova vulnerável e também diferente das demais, dando-a um caráter temporário, volátil e fungível.

A investigação e a responsabilização dos criminosos tem a prova digital como tema de grande relevância, sobretudo quando se destaca que o desenvolvimento da tecnologia possibilitou o surgimento de novos meios de obtenção de provas, tais como as gravações de vídeo e áudio, as escutas telefônicas, as fotografias, as análises genéticas etc. (Mesquisa, 2010b). Por outro lado, Militão (2012) acrescenta que a prova digital se apresenta como frágil, instável, destrutível, dispersa, fragmentada, manipulável e invisível, cuja identificação, apreensão, preservação, análise e tratamento sejam extremamente complexos, assim como também o é conseguir assegurar sua compreensibilidade e fiabilidade. Isso é um entrave para as investigações no cambo da criminalidade informática, demandando a regulação da recolha de provas pelo CPP, assim como foi feito na Lei n.º 109/2009.

Sobre o caráter temporário da prova digital, Ramos (2015a) esclarece que algumas informações podem estar disponíveis apenas por um determinado intervalo de tempo ou podem até mesmo desaparecer com o passar dos dias, como o que ocorre, por exemplo, com os dados de tráfego, sendo que os ISP's devem, por lei, armazenar por um ano. Nesse caso, a investigação conta com apenas um ano para seu percurso de produção de prova, período esse cuja contagem inicia no momento da prática do fato.

Aliás, considera-se que, devido aos mencionados atributos da prova digitais, sobretudo sua volatilidade e temporalidade, em situações de urgência, a medida de acesso às mesmas pode ser autorizada pelo próprio MP, sem que isso acarrete em prejuízo à sua admissibilidade. A não autorização do mesmo, bem como a ausência de fundamentação no que se refere ao enquadramento em um dos crimes dispostos no catálogo, resulta na ilegalidade da medida e na nulidade do meio de prova. Acrescenta-se que a legalidade da autorização do julgador deve obedecer aos conhecimentos disponíveis quando ela é concedida, independendo dos conhecimentos posteriores (Campos, 2019).

Ainda sobre as dificuldades relacionadas ao tema da prova digital, Costa (2017) também discorre que, mais do que as outras, esse tipo de prova apresenta grande potencial de violar direitos, liberdades e garantias constitucionais, especialmente se o meio de prova não seguir as determinações legais. Ainda completa que os direitos violados, nesse caso, também são tutelados no campo processual-penal. Portanto, a utilização da prova digital enquanto ferramenta da busca da verdade se encontra em uma linha tênue que limita essa descoberta e a ofensa a direitos fundamentais, estes que, por isso, mostram-se como barreiras para a validade dos meios e métodos de obtenção da prova digital.

5.7 Situações onde pode ser utilizada

Observa-se que um dos crimes nos quais a prova digital se faz mais presente é o crime de violência doméstica, sobretudo quando os envolvidos são pessoas de gerações mais novas, geralmente mais adeptos dos dispositivos eletrônicos e do uso da internet. Sabe-se que uma das características desse tipo de situação é a dificuldade de se encontrar meios de prova, além de que a porcentagem de inquéritos findos por acusação é pouco expressiva. Por isso, justifica-se a necessidade de se recorrer a todos os meios de prova possíveis para a continuidade do inquérito para a etapa de acusação. Nesse caso, a prova digital tem se mostrado como um meio relevante na resolução dos casos desse tipo de violência (Silva, 2018).

Em pesquisa, Ministério da Administração Interna (2016) constatou que, entre os anos de 2012 e 2015, foram abertos 33.841 inquéritos de violência doméstica, sendo que, deles, a grande maioria foi arquivada, uma representação de 77,8% dos casos. Além disso, 4,7% resultou em suspensão provisória do processo e apenas 17,5% chegou em fase de acusação. Dos arquivados (um total de 26.313 casos), verifica-se que parte significativa teve como motivo as disposições do n.º 2 do art. 277º do CPP, referente à insuficiência de provas; outros arquivamentos se abrigaram na redação do n.º 1 do mesmo artigo, que diz sobre a ausência de crime ou a não prática do crime pelo arquivo. Há também uma parcela de arquivados justificada nas atribuições do art. 282º, n.º 3, do mesmo documento, sobre a finalização do inquérito pro suspensão provisória do processo.

CONCLUSÃO

Este estudo mostra que é possível executar crimes clássicos usando tecnologia moderna, e nesse cenário a prova digital permite métodos mais rápidos de obtenção de informações, incluindo a preservação, divulgação e buscas de dados expeditas, o que facilita as investigações.

A lei prevê que a prova pode ser criada por qualquer meio legal e moralmente válido, ou seja, incluindo-se neste rol todo rastro digital deixado no ambiente virtual.

Foi interessante ver que havia diferentes tipos de agentes de intrusão. Nesse contexto, os Hackers são aqueles que obtêm acesso aos sistemas de informação sem autorização, por vezes empregando vírus de computador para alcançar seus propósitos. Os phreakers usam linhas telefônicas para manipular as redes de comunicação (blackboxing - isso envolve fazer com que as linhas telefônicas sejam obstruídas a fim de impedir ou reduzir o pagamento à operadora. Os crackers descomplicam ou removem as proteções do programa para obter acesso irrestrito. Já os Lammers possuem pouco conhecimento e acabam fazendo ataques com instrumentos desenvolvidos por outros.

Neste cenário de crimes virtuais, a prova teve que evoluir no tocante à como é obtida. Nesse sentido, a Lei 109/2009 é uma inovação legislativa significativa no sistema jurídico português. Regula uma realidade que até então não era reconhecida pelo legislador português: o cometimento de crimes por meio de sistemas digitais ou ainda em situações em que a colheita de provas em meio a um ambiente digital fosse necessária. Frente a esta realidade, a referida lei criou um conjunto de disposições processuais para a prova digital em Portugal.

A Lei de Crimes Cibernéticos incluiu uma nova lei substantiva e um conjunto de disposições processuais relacionadas a provas digitais. Portugal passou a contar com mecanismos processuais como a preservação expedita de dados (artigo 12.º), revelação expedita de dados de tráfego (artigo 13.º), injunção para apresentação ou concessão do acesso a dados (artigo 14.º), pesquisa de dados informáticos (artigo 15.º), apreensão de dados informáticos (artigo 16.º), apreensão de correio eletrónico e registos de comunicações de natureza semelhante (artigo 17.º), interceção de comunicações (artigo 18.º) e ações encobertas (artigo 19.º). Exceto nos artigos 18.º e 19.º, pode-se utilizar todos os mencionados mecanismos processuais não somente quando se investiga os crimes previamente previstos na Lei do Cibercrime, assim como nos processos de ordem criminal onde se praticou tal delito com uso de sistema

digital ou em função da necessidade de se recolher indícios de prova em base eletrônica, por força do art. 11.º, n.º1 da Lei do Cibercrime.

Essa lei, apesar de ter sido uma inovação no ordenamento jurídico de Portugal, não estabelece regras de procedimento, pondo em risco a avaliação das provas obtidas nestes. Ainda assim, estas foram uma inovação na legislação portuguesa e ajudaram a proteger uma realidade que não tinha regulamentação legal.

Apesar de toda evolução legal, cabe dizer que o regime de prova digital é fragmentado e ausente, o que leva a áreas cinzentas, aplicação inconsistente e falta dos regulamentos necessários. Embora fosse de se esperar que todas as lacunas fossem preenchidas, o legislador destacou a inconsistência do regulamento.

Embora as evidências digitais possam ser cruciais para determinar a verdade de certos crimes e uma ferramenta inestimável para resolver casos que de outra forma não poderiam ser resolvidos, é importante que se tenha em mente que isso ainda pode ser novo. A evidência digital também pode prejudicar a segurança do sistema de justiça criminal se não for usada de acordo com as regras.

Portanto, é importante analisar os arquivos digitais tendo em mente três coisas: autoria, autenticidade e integridade. É importante que a análise do documento possa revelar por quem ele foi escrito. A autenticidade refere-se ao fato de o conteúdo ter sido criado pelo signatário. Integridade é o conteúdo do documento e garante que não foi alterado em sua forma original.

A trilogia jurídica existente exige uniformidade do direito internacional no crime cibernético. Isso busca harmonizar as estruturas normativas. Só então a cooperação internacional pode ser eficaz na extinção de ciber-paraísos. Os ciberataques só podem ser combatidos de forma eficaz se houver coordenação e cooperação internacional, levando em consideração a característica de transnacionalidade.

No entanto, é imprescindível dispor de ferramentas processuais, nomeadamente, meios de obtenção de provas especificamente concebidos para o combate ao crime informático. A Lei dos Crimes Cibernéticos estabeleceu um procedimento de prova digital, mas é importante que o legislador leve em consideração o constante progresso científico e adapte os mecanismos de coleta de provas às realidades tecnológicas.

A cooperação internacional no combate ao crime cibernético é fundamental, pois este não conhece fronteiras geográficas. O Brasil pode aderir à convenção do crime cibernético (também conhecida como Convenção de Budapeste em referência à sua assinatura de 2001). A convenção está atualmente em vigor com 66 países. Ele lista os tipos de crimes relacionados à tecnologia da informação e estabelece procedimentos para cooperação internacional e acesso a evidências por países fora de sua jurisdição.

O Brasil, por ser participante do protocolo de evidências eletrônicas, passaria a ser reconhecido por sua conformidade com os padrões internacionais, o que fortaleceria sua imagem como parceiro de confiança. O Brasil seria participante do protocolo de evidências eletrônicas, facilitando a atualização na convenção e o padrão para trocas de informações.

REFERÊNCIAS

Abrantes, J. J. (1986). Prova ilícita: Da sua relevância no processo civil. *Revista Jurídica da Associação Académica da Faculdade de Direito de Lisboa*, nova série, (7).

Afonso, M.C. C. (2016). *A reconstituição informática e as provas atípicas em processo penal.* (Dissertação de Mestrado). Universidade Nova de Lisboa.

Albuquerque, P. P. (2009). *Comentário do código de processo penal: À luz da Constituição da República Portuguesa e da Convenção Europeia dos direitos do homem*. (3ª ed.). Universidade Católica.

Albuquerque, R. C. (2006). Os objetos intangíveis na era da criminalidade informática. *Espaço Jurídico Journal of Law*, *7*(2), 165-178. https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/8794

Alves, M. J. (1997). Processo Penal IV: meios de prova. *Revista Polícia Portuguesa*, *60*(108), 14-19.

Alves, R. M. L. (2019). Crime de abuso de cartão de garantia ou de crédito: Enquadramento jurídico, prática e gestão processual. In *O Crime de abuso de cartão de garantia e crédito e o crime de burla informática*. (pp. 217-248). Centro de Estudos Judiciários.

Andrade, M. C. (2004). *Direito penal médico - SIDA*: Testes arbitrários, confidencialidade e segredo. Coimbra.

Andrade, M. C. (2009). *Bruscamente no verão passado, a reforma do código de processo penal*: Observações críticas sobre uma lei que podia e devia ter sido diferente. Coimbra.

Andrade, M. C. (2013). *Sobre as proibições de prova em processo penal*. Coimbra.

Andrade, M. C. (2014). O regime dos conhecimentos da investigação em processo penal: Reflexões a partir das escutas telefónicas. *Revista Brasileira de Ciências Criminais, 22*(110), 259-296.

Antunes, M. J. (2010). *Código Penal*. (17ª ed.). Coimbra.

Arrone, I. S. (2018). *A investigação criminal em Moçambique*: Gestão e cadeia de custódia da prova. (Dissertação de Mestrado). Instituto Superior de Ciências Policiais e Segurança Interna.

Assis, B. C. (2019). *A oralidade no processo do trabalho*. (Dissertação de Mestrado). Universidade de Lisboa.

Barreiros, J. A. (2014). Prova pericial: uma oportunidade perdida. In Leite, A. L. (Org.). *As alterações de 2013 aos códigos penal e de processo penal*: Uma reforma "cirúrgica"? (pp. 203-216). Coimbra.

Batista, L. J. (2018). *O malware como meio de obtenção de prova em processo penal.* (Dissertação de Mestrado). Universidade de Lisboa.

Beirão, J. M. M. (2017). *Da distribuição do ónus da prova no direito processual civil português*: Contributo para o estudo da possibilidade de flexibilização através de uma distribuição dinâmica. (Dissertação de Mestrado). Universidade de Lisboa.

Beleza, T. P., & Pinto, F. C. (2014). *Prova criminal e direito de defesa, estudos sobre teoria da prova e garantias de defesa em processo penal*. Almedina.

Bessa, L. R., & Leite, R. R. (2016). A inversão do ônus da prova e a Teoria da Distribuição Dinâmica: Semelhanças e incompatibilidades. *Revista Brasileira de Políticas Públicas*, *6*(3), 140-155.

Boa Morte, R. S. D. (2017). *A prova testemunhal*: *A razão antropológica da sua força processual*. (Dissertação de Mestrado). Instituto Superior de Ciências Policiais e Segurança Interna.

Branco, P. M. A. (2017). *O exame neurológico p300 – (in)viabilidade no processo penal português.* (Dissertação de Mestrado). Universidade de Coimbra.

Bravo, R. (2013). As tecnologias de informação e a compressão dos direitos, liberdades e garantias: Os Efeitos das regras "10/10" e "1/1". *Terra de Lei*, 2(3), 1-8. https://www.academia.edu/2047039/As_Tecnologias_de_Informacao_e_a_Compressaao_dos_Direitos_Liberdades_e_Garantias_os_efeitos_das_regras_10_10_e_1_1_

Brito, D. R. (2016). *Combatendo a ameaça ransomware aplicando a norma ISO/IEC 27001:2013 na gestão da segurança da informação*. (Trabalho de Conclusão de Curso). Universidade Tecnológica Federal do Paraná.

Brito, I. (2019). *Violência doméstica*: *O contributo das ciências forenses*. (Dissertação de Mestrado). Universidade do Porto.

Cabral, J. R. P. (2017). *A prova por declarações de parte no código de processo civil*. (Dissertação de Mestrado). Universidade de Lisboa.

Cabral, J. S. (2012). Prova Indiciária e as novas formas de criminalidade. *Revista Julgar*, 17, 1-21.

Campos, J. F. S. (2019). *O malware como meio de obtenção da prova em processo penal*. (Dissertação de Mestrado). Universidade de Coimbra.

Cardoso, J. Y. C. (2015). *Princípio do nemo tenetur se ipsum accusare no contexto da sujeição a exames*. (Dissertação de Mestrado). Universidade de Lisboa.

Careiro, C. R. D. (2017). *Interceptação telemática no processo penal*. (Trabalho de Conclusão de Curso). Universidade Federal Fluminense.

Carnelutti, F. (2005). *A prova civil*. (L. P. Scarpa, trad.). Bookseller.

Carreira, T. R. (2016). *As provas ilícitas no processo civil*. (Dissertação de Mestrado). Universidade de Coimbra.

Carvalho, N. V. (2012). As escutas telefónicas. O Controlo judicial da realização de escutas - problemas do atual regime processual. *Revista de Ciências Empresariais e Jurídicas, 21*(21), 167-199.

Conceição, A. R. (2009). *Escutas telefónicas: Regime processual penal*. Quid Juris.

Conceição, A. R. O. P. (2018). *O branqueamento de capitais e o estatuto do arrependido colaborador: as novas exigências investigatórias no (ainda) admirável mundo novo*. (Tese de doutoramento). Universidade Lusíada.

Conte, C. P., & Fiorillo, C. A. P. (2015). *Crimes no meio digital*. Saraiva.

Correia, J. C. (2014). Prova digital: As leis que temos e a lei que devíamos ter. *Revista do Ministério Público*, *35*(139), 29-59.

Correia, P. M. A. R., Santos, S. I. S., & Correia, M. C. A. R. F. (2017). Percepções sobre cibersegurança e privacidade em Portugal: Evidências estatísticas de igualdade e desigualdade homem-mulher. *Revista Latino-Americana de Geografia e Género*, *8*(1), 35-50.

Correia, T. M. (2015). *A prova no processo civil: Reflexões sobre o problema da (in)admissibilidade da prova ilícita*. (Dissertação de Mestrado). Universidade de Coimbra.

Costa, C. R. S. (2017). *As proibições de prova e a prova digital: Aproximação aos lugares-comuns de um instituto clássico em face de uma nova realidade.* (Dissertação de Mestrado). Universidade do Minho.

Costa, F. J. (2011). *Locus delicti nos crimes informáticos*. (Tese de doutoramento). Universidade de São Paulo.

Crespo, M. X. F. (2011). *Crimes digitais*. Saraiva.

Cunha, J. R. F. (2017). *As imagens da videovigilância como meio de prova penal*. (Dissertação de Mestrado). Instituto Superior de Ciências Policiais e Segurança Interna.

Dantas, B. B. S. (2014). *A ineficácia da lei 12.737/2012 em face do avanço da criminalidade de informática*. (Trabalho de Conclusão de Curso). Universidade Federal de Campina Grande.

Debona, P. O. (2017). *A distribuição dinâmica do ônus da prova à luz do processo justo e da cooperação processual*. (Dissertação de Mestrado). Universidade de Coimbra.

Dias, C. B. A. (2015). *Crimes virtuais*: As Inovações jurídicas decorrentes da evolução tecnológica que atingem a produção de provas no processo penal. (Trabalho de Conclusão de Curso). Centro Universitário de Brasília.

Dias, J. E. M. V. (2014). *Considerações sobre a prova e contraditório na fase de instrução no processo penal*. (Dissertação de Mestrado). Universidade Portucalense.

Dias, V. M. (2012). A problemática da investigação do cibercrime. *Data Venia Revista Jurídica Digital*, *1*(1), 63-88. https://www.datavenia.pt/ficheiros/edicao01/datavenia01_p063-088.pdf

Didier Junior, F., Braga, P. S., & Oliveira, R. A. (2015). *Curso de direito processual civil*: Teoria da prova, direito probatório, ações probatórias, decisão precedente, coisa julgada e antecipação dos efeitos da tutela. (10ª ed., Vol. 2). Jus Podivm.

Dinis, Y. E. A. (2019). *A prova ilícita e o princípio da proporcionalidade*: *Análise sobre a sua admissibilidade em Processo Civil.* (Dissertação de Mestrado). Universidade de Lisboa.

Eiras, H. (2008). O princípio da livre apreciação da prova. In: Eiras, H. *Processo penal ementar*. (7ª ed.). Quid Juris.

Escola Prática da Guarda. (2008). *Manual da prova da escola prática da GNR*. EPG.

Eufrásio, E. T. L. (2015). *O cibercrime e a violação dos direitos fundamentais de natureza pessoal dos menores – o caso da CPLP*. (Dissertação de Mestrado). Universidade Fernando Pessoa.

Euzébio, G. A. (2014). *O crime de invasão de dispositivo informático acrescido pela lei Carolina Dieckmann sob a perspectiva do princípio da proporcionalidade*. (Trabalho de Conclusão de Curso). Universidade do Sul de Santa Catarina.

Faria, N. S. (2013). Acesso ao registo das escutas telefónicas: Os poderes de destruição do juiz de instrução. In Fidalgo, A. R. et al. *Prova criminal e direito de defesa*: *Estudos sobre teoria da prova e garantias de defesa em processo penal* (pp. 38-66). Almedina.

Faria, P. R., & Loureiro, A. L. (2013). *Primeiras notas ao novo código de processo civil*. Almedina.

Fernandes, V. (2017). *A necessidade de desencriptação de smartphones para obtenção de prova no processo penal*: *Restrições ao princípio de não-autoincriminação na era digital*. (Dissertação de Mestrado). Universidade de Lisboa.

Ferrão, A. (2018). *A prova documental: Regime e principais questões*. (Dissertação de Mestrado). Faculdade Católica de Direito.

Ferraz, A. B. S. (2020). *O crime de tráfico de pessoas: As insuficiências do artigo 160º do código penal à luz do atual contexto social*. (Dissertação de Mestrado). Universidade Católica Portuguesa.

Fidalgo, M. (2015). *A Instrução no novo código de processo civil*: A prova por declarações de parte. (Dissertação de Mestrado). Universidade de Lisboa.

Fidalgo, S. (2006). Determinação do perfil genético como meio de prova em processo penal. *Revista Portuguesa de Ciência Criminal*, *16*(1),115-148.

Fidalgo, S. (2009). O processo sumaríssimo na revisão do Código de Processo Penal. *Separata da Revista CEJ de Lisboa*, (9)*,* 297-319.

Fidalgo, S. (2019). A recolha de prova em suporte electrónico: em particular, a apreensão de correio eletrónico. *Revista Julgar*, (38),151-160.

Fidalgo, S. (2019). Apreensão de correio eletrónico e utilização noutro processo das mensagens apreendidas, *Revista Portuguesa de Ciência Criminal*, (1), 59-74.

Floriano, A. L., & Rodrigues, C. H. V. P. (2017). *Crimes informáticos*: Dos delitos e dos infratores. *Diálogo e Interação*, *11*(1), 244-268.

Fonseca, I. S. V. (2018). *Prova testemunhal*: *A justiça penal*. (Dissertação de Mestrado). Instituto Superior de Ciências Policiais e Segurança Interna.

Freitas, J. C. J. (2018). *A proteção dos dados pessoais de pagamento utilizados no comércio eletrónico, em Portugal*. (Dissertação de Mestrado). Universidade do Minho.

Freitas, J. P. C. B. (2017). *Os meios de obtenção de prova digital na investigação criminal: O regime jurídico dos serviços de correio eletrônico e de mensagens curtas*. (Dissertação de Mestrado). Universidade do Minho.

Garnaeva, M., Sinitsyn, F., Namestnikov, Y., Makrushin, D., & Liskin, A. (2016). *Kaspersky security bulletin: Overall statistics for 2016*. Kaspersky Lab, dec. https://go.kaspersky.com/global_security_bulletin_2016_stats_soc_2016.html

Garret, F. A. (2007). *Sujeição do arguido a diligências de prova e outros temas*. Fronteira do Caos.

Gaspar, J. N. F. (2018). *Estudo da criptomoeda*: *Análise aos desafios de substância criminal*. (Dissertação de Mestrado). Academia Militar de Lisboa.

Gimenes, E. A. S. G. (2013). Crimes virtuais. *Revista de Doutrina TRF4*, (55), 1-19.

Gíria, J. F. O. C. (2017). *Do informador de polícia ao agente provocador*: *O contributo dos homens de confiança para a produção de prova e a sua perigosidade*. (Dissertação de Mestrado). Universidade Nova de Lisboa.

Gomes, E. L. R. (2017). *A leitura e a reprodução das declarações do arguido no âmbito do processo penal e a sua valoração como meio de prova*. (Dissertação de Mestrado). Universidade do Minho.

Gomes, J. Q. (2017). *Sociedade da informação e a criminalidade informática*: *As Correlações entre a legislação brasileira e a convenção de Budapeste sobre cibercrime.* (Trabalho de Conclusão de Curso). Universidade Federal do Ceará.

Gonçalves, A. B. M. (2018). *A produção de prova oral pelas próprias partes*. (Dissertação de Mestrado). Universidade Nova de Lisboa.

Gonçalves, J. G. (2017). *A prova digital em 2017 – reflexões sobre algumas insuficiências processuais e dificuldades da investigação*. (Dissertação de Mestrado). Universidade Nova de Lisboa.

Goodison, S. E., Davis, R. C., & Jackson, B. A. (2015). Digital evidence and the U.S. criminal justice system. *NCJRS*. https://www.ojp.gov/pdffiles1/nij/grants/248770.pdf.

Guerra, G. G. A. (2019). *Infiltração virtual dos agentes policiais: Como meio de investigação de prova na persecução penal*. (Trabalho de Conclusão de Curso). Universidade Evangélica de Anápolis.

Guerra, J. L. G. (2016). *A livre apreciação da prova em processo penal*: *Em especial a prova pericial.* (Dissertação de Mestrado). Universidade Lusíada de Lisboa.

Heitor, P. L. V. O. (2015). *Contributo para a compreensão das causas de exclusão de ilicitude e da culpa no crime de acesso ilegítimo*. (Dissertação de Mestrado). Universidade do Minho.

Jesus, D., & Milagre, J. A. (2016). *Manual de crimes informáticos*. Saraiva.

Jesus, F. M. (2011). *Os meios de obtenção da prova em processo penal*. (Vol. 2). Almedina.

Jesus, F. M. (2015). *Os meios de obtenção da prova em processo penal*. (2ª ed.). Almedina.

Kerr, V. K. S. (2011). *A disciplina, pela legislação processual penal brasileira, da prova pericial relacionada ao crime informático praticado por meio da Internet*. (Dissertação de Mestrado). Universidade de São Paulo.

Leite, A. L. (2004). As escutas telefónicas: Algumas reflexões em redor do seu regime e das consequências processuais derivadas da respectiva violação. *Revista da FDUP*, *1*, 9-58.

Lima, G. P. (2017). *Crimes virtuais*: *Aspectos legais e validade das provas e documentos gerados nas redes sociais, uma revisão integrativa*. (Trabalho de Conclusão de Curso). Universidade Federal Rural de Pernambuco.

Lima, M. P. (2009). *Manual de Processo Penal*. (4ª ed.). Lumen Juris.

Lima, R. B. (2013). *Curso de Processo Penal.* Ímpetus.

Lopes, F. (2010). *Gestão do conhecimento – modelação dos incidentes e das respostas*. (Dissertação de Mestrado). Universidade Católica Portuguesa.

Macedo, P. A. (2015). *Crimes virtuais frente a falta de legislação e educação digital*. (Trabalho de Conclusão de Curso). Uni-Anhanguera Centro Universitário de Goiás.

Maia, A. S. M. (2019). *O silêncio do arguido, a culpa da vítima*: *Uma proposta sociológica no domínio do crime de violência doméstica*. (Dissertação de Mestrado). Universidade do Porto.

Mann, D. C. (2018). *Infiltração digital*: *A validade como meio de prova e os limites éticos do estado-investigador*. (Dissertação de Mestrado). Instituto Superior de Ciências Policiais e Segurança Interna.

Manuel, H. (2015). *A investigação criminal no estado de direito democrático*: *Autonomia e dependência da polícia de investigação criminal em Moçambique*. (Dissertação de Mestrado). Instituto Superior de Ciências Policiais e Segurança Interna.

Marinoni, L. G., & Arenhart, S. C. (2013). *Curso de Processo Civil*: Processo de conhecimento. (11ª ed., Vol. 2). Revista dos Tribunais.

Marques, A. C. F. (2019). *Relatório de Estágio Curricular no Tribunal Judicial Comarca de Lisboa, Juízo Central Criminal*. (Dissertação de Mestrado). Universidade Nova de Lisboa.

Marques, D. S. M. (2015). *O processo civil e a colaboração de terceiros*. (Dissertação de Mestrado). Universidade de Coimbra.

Marques, M. J. X. B. (2014). *Os meios de obtenção de prova na lei do cibercrime e o seu confronto com o código de processo penal*. (Dissertação de Mestrado). Universidade Católica Portuguesa.

Marques, P. P. L. C. (2013). *Informática forense*: *Recolha e preservação de prova digital.* (Dissertação de Mestrado). Universidade Católica Portuguesa.

Martins, C. B. C. H. (2015). *Declarações de parte*. (Dissertação de Mestrado). Universidade de Coimbra.

Martins, J. J. M. (2015). *Prova por presunções judiciais na responsabilidade civil aquiliana*. (Tese de doutoramento). Universidade de Lisboa.

Martins, P. A. F. M. A. (2015). *Nemo tenetur se ipsum accusare e a obrigação de sujeição a exames*. (Dissertação de Mestrado). Instituto Superior de Ciências Policiais e Segurança Interna.

Mateus, M. A. T. (2016). *Crimes em ambiente digital*: *Investigação da GNR para a obtenção de prova*. (Dissertação de Mestrado). Academia Militar de Lisboa.

Matias, M. I. A. V. (2020). *Apreensão de correio eletrônico e registros de comunicações de natureza semelhante*. (Dissertação de Mestrado). Universidade de Coimbra.

Melo Junior, J. E. (2016). *A repartição do ônus da prova no processo coletivo*: *Controvérsias nos sistemas probatórios do Brasil e de Portugal*. (Dissertação de Mestrado). Universidade de Lisboa.

Mendes, P. S. (2013). *Lições de direito: Processo penal*. Almedina.

Mendes, P. S. (2014a). O processo penal entre a eficácia e as garantias. In Mendes, P. S. *Direito da investigação criminal e da prova, de AA. VV*. (pp. 67-80). Almedina.

Mendes, P. S. (2014b). *Lições de Direito Processual Penal*. Almedina.

Mendes, P. S. (2018). *Lições de direito processual penal*. (5ª ed.). Almedina.

Mendes, T. J. (2018). *Liberdade, segurança e justiça*: *O modelo português e francês na investigação do contrabando de tabaco*. (Dissertação de Mestrado). Academia Militar de Lisboa.

Mesquita, P. D. (2010a). *Processo penal: Prova e sistema judiciário*. Coimbra.

Mesquita, P. D. (2010b). Prolegómenos sobre prova eletrônica e intercepção de telecomunicações no Direito Processual Penal Português – O Código e a Lei do Cibercrime. In: Mesquita, P. D. *Processo penal, prova e sistema judiciário*. (pp. 83-129). Coimbra: Coimbra.

Mesquita, P. D. (2011). *A prova do crime e o que se disse antes do julgamento*: *Estudo sobre a prova no processo penal português, à luz do sistema norte-americano*. Coimbra.

Mesquita, P. D. (2018). *Comentário judiciário do código processo penal*. (Tomo II). Coimbra: Almedina.

Militão, R. L. (2012). A propósito da prova digital no processo penal. *Revista da Ordem dos Advogados*, *72*(1), 247-283.

Ministério da Administração Interna. Secretaria Geral do MAI. (2016). Violência Doméstica: Relatório anual de monitorização. *SGMAI*. https://www.sg.mai.gov.pt/Noticias/Documents/Rel%20VD%202015.pdf

Miotto, C. C. (2015). *Ônus da Prova*: *Uma análise da distribuição estática e dinâmica do ônus da prova e a sua previsão legislativa nos sistemas processuais civis português e brasileiro*. (Dissertação de Mestrado). Universidade do Minho.

Monteiro, V. L. A. (2016). *Os meios de obtenção de prova no ambiente digital*: *O correio eletrônico.* (Dissertação de Mestrado). Universidade Católica Portuguesa.

Morais, I. L. S. (2012). *A apreensão de correio electrónico em processo penal*: *Dos direitos fundamentais às ingerências, constitucional e legalmente legitimadas, nas comunicações*. (Dissertação de Mestrado). Universidade de Lisboa.

Moreira, J. R. B. V. (2019). *A (in)admissibilidade e valoração das declarações de um co-arguido em prejuízo de outro co-arguido*. (Dissertação de Mestrado). Universidade do Minho.

Moreira, S. M. D. (2018). *A privatização da investigação na criminalidade tributária e a obtenção de meios de prova*: *Reflexões sobre a sua valoração em julgamento.* (Dissertação de Mestrado). Universidade do Minho.

Mota, P. L. R. (2019). Crime de burla informática e nas comunicações – enquadramento jurídico, prática e gestão processual. In Pereira, L. M. C. S. *et al*. (Org.) *O crime de abuso de cartão de garantia e crédito e o crime de burla*

informática. (pp. 167-192). Centro de Estudos Judiciários. (Ministério Público, Coleção Formação)

Neves, R. C., & Correia, H. S. (2014). A lei do cibercrime e a colaboração do arguido no acesso aos dados informáticos. *Actualidad Jurídica Uría Menéndez*, (38), 146-149.

Nogueira, S. D. A. (2008). *Crimes de informática*. BH.

Nogueira, S. F. M. S. (2016). *A valorização e motivação do tribunal no âmbito da livre apreciação da prova*. (Dissertação de Mestrado). Universidade Lusíada do Porto.

Oliveira, A. T. S. (2017). *Obtenção de prova digital*: *Utilização de malware pelos órgãos da polícia criminal*. (Dissertação de Mestrado). Universidade do Minho.

Oliveira, D. (2017, 13 setembro). Qual o perfil dos cibercriminosos no Brasil? *It Forum*. https://itforum.com.br/noticias/qual-o-perfil-dos-cibercriminosos-no-brasil/

Oliveira, N. F. (2012). *O crime de violação de direito autoral da música na Internet*. (Trabalho de Conclusão de Curso). Centro Universitário Eurípedes de Marília.

Oliveira, S. F. (2014). *Admissibilidade da prova ilícita em processo civil*. (Dissertação de Mestrado). Universidade de Lisboa.

Pereira, M. O. C. (2019). *Prova digital problemas de compatibilização entre as leis nº 32/2008, nº 109/2009 e o código de processo penal*. (Dissertação de Mestrado). Universidade de Coimbra.

Pina, C. M. V. (2015). *A presunção de inocência nas fases preliminares do processo penal*: *Tramitação e actos decisórios*. (Dissertação de Mestrado). Universidade Nova de Lisboa.

Pinheiro, P. P. (2016). *Direito digital*. (6ª ed.). Saraiva.

Pinho, C. (2012). Os problemas interpretativos resultantes da Lei n.º 32/2008, de 17 de julho. *Revista do Ministério Público*, *33*(129), 63-93.

Pratas, R. M. C. S. (2018). *O correio eletrônico como meio de prova em processo penal*. (Dissertação de Mestrado). Universidade Católica Portuguesa.

Quintas, R. L. R. M. B. (2017). *Officium Iudicis Instrutório*: *A Indagação oficiosa da verdade no Processo Civil.* (Dissertação de Mestrado). Universidade de Coimbra.

Ramalho, D. S. (2017). *Métodos ocultos de investigação criminal em ambiente digital.* Almedina.

Ramos, A. D. (2014). *A prova digital em processo penal*. Chiado.

Ramos, A. D. (2015a). *A prova digital em processo penal: O Correio eletrónico*. (2ª ed.). Chiado.

Ramos, A. D. (2015b). *A prova digital na investigação do (ciber)terrorismo, Investigação Criminal, 9*. ASFIC/PJ.

Ramos, A. D. (2017). *A prova digital em processo penal: O Correio eletrônico*. (2ª ed.). Chiado.

Reis, J. A. (2012). *Código de processo civil anotado*. (3ª ed., Vol. 3). Coimbra.

Ribeiro, M. C. F. (2015). *Cibercrime e prova digital*. (Dissertação de Mestrado). Instituto Superior Bissaya Barreto.

Ribeiro, N. L. (2017). *Desafios enfrentados na repressão dos crimes informáticos à luz dos avanços tecnológicos*. (Trabalho de Conclusão de Curso). Universidade Federal de Campina Grande.

Ribeiro, N. S. (2019). *A prova por reconhecimento no processo penal*: *Do Reconhecimento fotográfico ao reconhecimento pessoal*. (Dissertação de Mestrado). Instituto Superior de Ciências Policiais e Segurança Interna.

Ristori, A. D. P. (2007). *Sobre o silêncio do arguido no interrogatório no processo penal português*. Almedina.

Rodrigues, A. M. (2020). *A valorização da prova em processo civil*: *Prova legal e livre apreciação da prova*. (Dissertação de Mestrado). Universidade Nova de Lisboa.

Rodrigues, B. S. (2009). *Direito penal parte especial*. (Tomo I). Coimbra. (Direito Penal Informático-Digital)

Rodrigues, B. S. (2010). *Da prova penal: Bruscamente… a(s) face(s) oculta(s) dos métodos ocultos de investigação criminal*. (Tomo II) Rei dos Livros.

Rodrigues, B. S. (2011). *Da prova penal: Da prova-electrónico-digital e da criminalidade*. (Tomo IV). Rei dos livros.

Sá, C. F. C. (2015). *Da prova*: *Na Atuação policial e no âmbito da infração tributária*. (Dissertação de Mestrado). Universidade do Minho.

Santos, J. L. A. (2011). *Contributos para uma melhor governação da cibersegurança em Portugal*. (Dissertação de Mestrado). Universidade Nova de Lisboa.

Santos, L. R. (2011). *Crimes virtuais e tutela penal*. (Trabalho de Conclusão de Curso). Universidade Estácio de Sá.

Santos, M. F. R. (2018). *Invocação e ilusão de presunções legais em processo civil*: *Análise às particularidades do seu regime probatório*. (Dissertação de Mestrado). Universidade de Lisboa.

Santos, M. S. (2015). *Escutas telefónicas a defensor e arguido*: *A Epidemia da devassa silenciosa*. (Dissertação de Mestrado). Universidade de Lisboa.

Santos, R. C. (2017). *Algumas considerações sobre a relevância da prova por presunções judiciais na responsabilidade civil extracontratual*. (Dissertação de Mestrado). Universidade de Coimbra.

Santos, T. C. P. (2016). *O regime das escutas telefónicas*: *Das suas particularidades aos seus limites*. (Dissertação de Mestrado). Universidade de Coimbra.

Scientific Working Group on Digital Evidence (2004, January 15). Guidelines & Recommendations for Training in Digital & Multimedia Evidence. *SWGDE*. https://www.swgde.org/documents/Archived%20Documents

Scientific Working Group on Digital Evidence (2016, June 23). SWGDE Digital & Multimedia Evidence Glossary Disclaimer. *LEVA*. https://www.leva.org/wp-content/uploads/2019/10/SWGDE-Glossary.pdf

Seiça, A. M. (2003). Legalidade da prova e reconhecimentos atípicos em processo penal: Notas à margem de jurisprudência (quase) constante. In Andrade, M. C. et al. Coimbra.

Silva, A. M. (2019). *Princípio do dispositivo versus princípio do inquisitório*: *Quem deve produzir as provas?* (Dissertação de Mestrado). Universidade do Minho.

Silva, E. M., Guariento, N., Queiróz, R. O., Resende, T., & Silva, C. K. (2013). Direito digital: Uma análise preponderante sobre o mais novo ramo do direito e suas transformações sócio-jurídicas. *Revista de Direito do Centro Universitário Newton Paiva*, *1*(20), 169-178.

Silva, F. A. A. (2019). *A revelação do crime do funcionário como condição expressa da suspensão provisória do processo aplicada ao arguido da corrupção ativa*. (Dissertação de Mestrado). Universidade de Lisboa.

Silva, G. M. (2000). *Curso de processo penal*. (Vol. 3). Editorial Verbo.

Silva, G. M. (2009). *Curso de processo penal*. (3ª ed., Vol. 2). Editorial Verbo.

Silva, H. F. G. (2019). *Investigação criminal*: *O Acesso a terminais de intercepção de comunicações pelos órgãos de polícia criminal*. (Dissertação de Mestrado). Instituto Superior de Ciências Policiais e Segurança Interna.

Silva, J. P. V. B. (2017). *A prova em medicina dentária forense*. (Dissertação de Mestrado). Instituto Superior de Ciências da Saúde Egas Moniz.

Silva, L. A. S. (2015). *O agente infiltrado*: *Estudo comparado da legislação da Alemanha, Brasil e Portugal*. (Dissertação de Mestrado). Universidade de Coimbra.

Silva, L. M. D. D. (2017). *Convenções de prova em processo civil*. (Tese de doutoramento). Universidade de Coimbra.

Silva, M. A. M. (2000). *Curso de processo penal*. Quartier Latin.

Silva, M. A. M. (2008). *Curso de processo penal*. Quartier Latin.

Silva, M. M. M. (2017). *As comunicações eletrónicas e a investigação criminal (rumo à compreensão do regime de ingerência no seu conteúdo)*. (Dissertação de Mestrado). Universidade do Minho.

Silva, M. V. P. (2017). *A prova do crime de abuso sexual de menores*: *Uma perspectiva crítica*. (Dissertação de Mestrado). Universidade do Minho.

Silva, P. C., & Reis, N. T. (2013). A prova difícil: Da *probatio levior* à inversão do ónus da prova. Revista de Processo, *38*(222), 149-171.

Silva, P. S., & Silva, M. P. (2015). *Direito e crime cibernético*: *Análise da competência em razão do lugar no julgamento de ações penais*. Vestnik.

Silva, T. A. M. (2018). *Recolha da prova digital nos processos-crime de violência doméstica*. (Dissertação de Mestrado). Academia Militar de Lisboa.

Silva, T. I. G. (2016). *A (in)eficácia do ordenamento jurídico brasileiro no combate à pornografia de vingança*. (Trabalho de Conclusão de Curso). Centro Universitário Tabosa de Almeida.

Silveira, M. A. B. M. (2016). *Da problemática da investigação criminal em ambiente digital - em especial, sobre a possibilidade de utilização de malware como meio oculto de obtenção de prova*. (Dissertação de Mestrado). Universidade Católica Portuguesa.

Simas, D. V. (2014). *O cibercrime*. (Dissertação de Mestrado). Universidade Lusófona de Humanidades e Tecnologia.

Soares, P. A. F. (2014). *Meios de obtenção de prova no âmbito das medidas cautelares e de polícia*. Almedina.

Sousa, A. F. A. P. (2018). *Direito à não auto-incriminação e cibercrime*: *Colaboração do arguido no acesso a dados informáticos.* (Dissertação de Mestrado). Universidade de Lisboa.

Sousa, L. F. P. (2016). *A prova testemunhal*. Almedina.

Sousa, M. T. (1995). *As partes, o objeto e a prova na ação declarativa.* Lex.

Sousa, S. M. P. (2015). Reflexões soltas sobre a jurisprudência do tribunal da concorrência, regulação e supervisão em matéria de confidencialidade e acesso à prova. *Revista de Concorrência e Regulação*, *9*(35), 113-122.

Sydow, S. T. (2015). *Crimes informáticos e suas vítimas*. Saraiva.

Tavares, J. D. (2018). Ordem internacional, crime organizado e direito penal. In Agra, C., & Torrão, F. (Coord.). Criminalidade: Organizada e económica (pp. 11-40). Universidade Lusíada.

Tonini, P. (2000). *La prova penale*. Giuffre.

Tribunal da Relação do Porto. (2016, 01 junho). *Acórdão TRP 1345/10.7JAPRT.P1 de 01-06-2016*. http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/1f85e373f004b9fd80257fd5004eda69?OpenDocument.

Valente, M. M. G. (2010). *Processo Penal*. (3ª ed., Tomo I). Coimbra: Almedina.

Valles, E. (2014). *Prática processual com o novo CPC*. (8ª ed.). Almedina.

Vasco, M. A. M. (2018). *Investigação criminal*: *Gestão do local do crime em Portugal e Angola*. (Dissertação de Mestrado). Instituto Superior de Ciências Policiais e Segurança Interna.

Vaz, M. S. C. (2020). *Os sistemas de vigilância à distância no contexto laboral*: *Alguns problemas*. (Dissertação de Mestrado). Universidade de Coimbra.

Venâncio, P. D. (2011). *Lei do cibercrime: Anotada e comentada*. Coimbra.

Verónico, M. S. B. (2015). *Agressores sexuais: Caracterização de uma amostra portuguesa*. (Dissertação de Mestrado). Universidade do Porto.

Vieira, E. S. (2019). *Gestão em investigação e inteligência privada*: *Crimes cibernéticos.* (Trabalho de Conclusão de Curso). Instituto de Ensino Superior de Minas Gerais Dias D'Ávila.