**DEPARTAMENTO DE DIREITO**

**MESTRADO EM DIREITO**

**ESPECIALIDADE EM CIÊNCIAS JURÍDICAS**

**UNIVERSIDADE AUTÓNOMA DE LISBOA**

**“LUÍS DE CAMÕES”**

**A OFENSA AOS DIREITOS FUNDAMENTAIS DO INVESTIGADO EM FACE DA PRODUÇÃO DE PROVA DIGITAL NO PROCESSO PENAL**

 Dissertação para a obtenção do grau de Mestre em Direito.

Autor**:** Thiago Chaves de Melo

Orientadores**:** Manuel Monteiro Guedes Valente e Armando Reis Dias Ramos

Número do candidato: 30002013

**Março de 2022**

**Lisboa**

**DEDICATÓRIA**

Essa dissertação é dedicada, primeiramente, ao Nosso Senhor Jesus Cristo, a quem deposito toda a minha fé e esperança; à minha adorável esposa Cibele e aos meus filhos, Enzo e Benício, pela compreensão, união, conforto e carinho; aos meus pais, Jales e Silvânia, esteios do meu caráter e da minha formação como ser humano; às integrantes da De Melo Assessoria Jurídica, Maria e Priscilla, pelo auxílio na lida diária; à Diretora do Centro Universátiro Mário Palmério, Kelma Gomes Mendonça Ghelli, pelo incentivo e motivação constantes.

Ao Dr. Hamilton Pires Ribeiro, a minha eterna gratidão pelas orientações, ensinamentos e oportunidades conferidos à época do estágio universitário, os quais foram pilares na formação do meu caráter profissional.

**RESUMO**

O presente trabalho tem como objetivo analisar a ofensa aos direitos e garantias fundamentais do investigado em face da produção de prova digital no processo penal no ordenamento jurídico brasileiro, bem como no ordenamento jurídico português. Não obstante trouxe à baila a compatibilização do processo penal com a nova realidade tecnológica brasileira com a análise do direito à intimidade e sigilo das comunicações na persecução penal, buscando-se elencar o equilíbrio entre o interesse estatal na prossecução dos investigados e a tutela dos direitos e garantias da pessoa. Para tanto, utilizou-se como metodologia o tipo de pesquisa bibliográfico, como método dedutivo, por meio da análise textual, temática e interpretativa de obras jurídicas sobre o tema, assim como o tipo de pesquisa documental, enquanto método indutivo, tendo como objeto a Constituição Federal brasileira e portuguesa como fonte primária de estudo para a exploração do controle de constitucionalidade e convencionalidade.

**Palavras-chave:** Direitos Fundamentais. Prova Digital. Processo Penal.

**ABSTRACT**

The present work aims to analyze the offense to the fundamental rights and guarantees of the investigated in the face of the production of digital evidence in the criminal process in the Brazilian legal system, as well as in the Portuguese legal system. Nevertheless, it brought up the compatibility of the criminal procedure with the new Brazilian technological reality with the analysis of the right to privacy and secrecy of communications in criminal prosecution, seeking to list the balance between the state interest in the prosecution of the investigated and the protection of the rights and guarantees of the person. To this end, the type of bibliographic research was used as a methodology, as a deductive method, through textual, thematic and interpretive analysis of legal works on the subject, as well as the type of documentary research, as an inductive method, having as object the Brazilian and Portuguese Federal Constitution as a primary source of study for the exploration of constitutionality and conventionality control.

**Keywords:** Fundamental Rights. Digital Evidence. Criminal proceedings.

**RESUMEN**

El presente trabajo tiene como objetivo analizar la ofensa a los derechos y garantías fundamentales del investigado frente a la producción de prueba digital en el proceso penal en el ordenamiento jurídico brasileño, así como en el ordenamiento jurídico portugués. No obstante, planteó la compatibilidad del proceso penal con la nueva realidad tecnológica brasileña con el análisis del derecho a la intimidad y al secreto de las comunicaciones en la persecución penal, buscando enumerar el equilibrio entre el interés estatal en el enjuiciamiento de los investigados y la protección de los derechos y garantías de la persona. Para ello se utilizó como metodología el tipo de investigación bibliográfica, como método deductivo, a través del análisis textual, temático e interpretativo de obras jurídicas sobre el tema, así como el tipo de investigación documental, como método inductivo, teniendo como objetar la Constitución Federal brasileña y portuguesa como fuente primaria de estudio para la exploración del control de constitucionalidad y convencionalidad

**Palabras clave:** Derechos Fundamentales. Prueba digital. Procedimientos criminales.

**ÍNDICE**

[INTRODUÇÃO 9](#_Toc99963757)

[CAPÍTULO I – AS NOVAS TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO E SUAS INFLUÊNCIAS 11](#_Toc99963758)

[1. As novas tecnologias de informação e comunicação e os direitos fundamentais 11](#_Toc99963759)

[2. As novas tecnologias de informação e comunicação e o direito processual penal 16](#_Toc99963760)

[3. Da Inexistência de definição concreta de Crimes Cibernéticos ou Cibercrimes 23](#_Toc99963761)

[4. Da previsão legal dos Cibercrimes 27](#_Toc99963762)

[CAPÍTULO II – DA PROVA DIGITAL 32](#_Toc99963763)

[1. Introdução 32](#_Toc99963764)

[2. Atividade Probatória e Prova 34](#_Toc99963765)

[3. Conceito de Prova Digital 36](#_Toc99963766)

[4. Características da Prova Digital 39](#_Toc99963767)

[5. Da recolha da Prova Digital 44](#_Toc99963768)

[6. Da Obtenção da Prova Digital 48](#_Toc99963769)

[7. As vantagens e os inconvenientes da prova digital 57](#_Toc99963770)

[8. A autenticidade da prova digital 59](#_Toc99963771)

[9. Valoração da prova digital 60](#_Toc99963772)

[CAPÍTULO III – INVESTIGAÇÃO CRIMINAL NA ERA DIGITAL 64](#_Toc99963773)

[1. Introdução 64](#_Toc99963774)

[2. Do uso da tecnologia na Investigação Criminal 67](#_Toc99963775)

[3. Dos métodos ocultos de Investigação Criminal: 68](#_Toc99963776)

[4. Aplicação dos Princípios Constitucionais como limitadores dos métodos ocultos de investigação criminal 75](#_Toc99963777)

[5. A Investigação Criminal e suas implicações face aos Direitos Fundamentais do Investigado 80](#_Toc99963778)

[CAPÍTULO IV – A PROVA DIGITAL E AS SUAS IMPLICAÇÕES NOS DIREITOS FUNDAMENTAIS DO INVESTIGADO 82](#_Toc99963779)

[1. Introdução 82](#_Toc99963780)

[2. A Investigação Criminal e o Direito à Privacidade do Investigado 82](#_Toc99963781)

[2.1. Breves considerações 82](#_Toc99963782)

[2.2. Evolução da proteção à intimidade 84](#_Toc99963783)

[2.3. A Inviolabilidade das comunicações e o Direito à intimidade 88](#_Toc99963784)

[2.4. Sigilo das comunicações e processo penal 94](#_Toc99963785)

[2.5. A Proteção dos Dados Pessoais do Investigado em Portugal e no Brasil 99](#_Toc99963786)

[3. Da Afronta aos direitos fundamentais pelas provas digitais 106](#_Toc99963787)

[CONCLUSÃO 111](#_Toc99963788)

[REFERÊNCIAS 114](#_Toc99963789)

# INTRODUÇÃO

As Novas Tecnologias de informação e comunicação (doravante, NTICs) mudaram e continuam a mudar a sociedade em todo o mundo: melhorando a produtividade industrial, revolucionando os processos de trabalho e fazendo com que tanto os capitais quanto as informações sejam transmitidos em uma velocidade impensável há algumas décadas.

No entanto, toda essa tecnologia também tem sido usada para fins menos louvável desencadeando novas formas de crime, tal como o delito informático, cujo conceito é de difícil elaboração devido ao grande catálogo de condutas que podem ser cometidas através dele.

A sociedade da informação, a ausência de fronteiras e empregos massivos de comunicações imateriais por meio de dispositivos eletrônicos entre quaisquer ponto cardeal do planeta, fazem os limites temporais e espaciais, que tanto caracterizam o Direito Penal, colocados em xeque. A delinquência informática supõe um tipo especial de criminalidade devido aos meios através dos quais materializam seus comportamentos.

Os avanços tecnológicos representam desafios jurídicos significativos em termos de investigação e prova dos crimes executados através da rede, e em geral, de qualquer conduta ilícita que faça uso da evolução da ciência e tecnologia, seja para o cometimento do delito ou para evitar sua descoberta.

Nesse sentido, diversos processos de comunicação e armazenamento de dados e informações tem se intensificado nos meios eletrônicos, impulsionando sobremaneira as relações entre as pessoas, de modo que os avanços tecnológicos implicam seus efeitos diretamente na vida privada e na esfera processual penal.

Nessa perspectiva, esse trabalho trouxe como eixo principiológico estruturante o princípio da proporcionalidade, uma vez que as restrições aos direitos à intimidade, à privacidade e o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas só podem ser introduzidas se forem estritamente necessárias e corresponderem efetivamente a objetivos de interesse geral ou à necessidade de proteção dos direitos e liberdades de terceiros.

Nessa senda, o presente trabalho abordou no primeiro capítulo a relação entre as denominadas Novas Tecnologias de informação e comunicação e os direitos fundamentais.

Ainda nesse capítulo, verificou-se a influência concreta das Novas Tecnologias de informação e comunicação no direito processual penal, bem como a afirmação de que não há uma definição concreta de crimes cibernéticos ou cibercrimes. E, por fim, nesse capítulo foi tratada a previsão legal dos chamados cibercrimes tanto no Brasil quanto em Portugal.

No segundo capítulo, houve uma abordagem ampla sobre a prova digital, sendo que foram analisados os aspectos da atividade probatória, conceito, características, recolha, obtenção, vantagens e inconveniências, autenticidade e, por fim, a valoração da prova digital.

No terceiro capítulo houve uma extensa análise do uso da tecnologia na investigação criminal, bem como a verificação e a implicação dos métodos ocultos de investigação criminal no processo penal brasileiro e português. Em razão disso, foi necessário tratar dos princípios constitucionais como elementos limitadores do uso dos métodos ocultos de investigação criminal, e, ao final, fora realizada uma análise das implicações da investigação criminal, com a utilização dos métodos ocultos, nos direitos e garantias fundamentais do investigado.

Finalmente, no quarto e derradeiro capítulo, tem-se o estudo do objeto central da presente dissertação, qual seja, as implicações e influências das provas digitais nos direitos e garantias fundamentais do investigado. Para tanto, passou-se pela observação da investigação criminal frente ao direito à privacidade do investigado, a evolução legislativa da proteção à intimidade, a inviolabilidade das comunicações e o direito à intimidade, o sigilo das comunicações e o processo penal, a proteção dos dados pessoais do investigado em Portugal e no Brasil, e, por fim, as razões e motivos que levam à afronta aos direitos fundamentais pelas provas digitais.

Para tanto, será utilizada como metodologia o tipo de pesquisa bibliográfico, enquanto método dedutivo, realizando a análise textual, temática e interpretativa de obras relacionadas ao tema, assim com o tipo de pesquisa documental, por meio da análise de conteúdo da Constituição Federal brasileira e portuguesa; além de Convenções e Tratados Internacionais no que tange às normas inerentes ao tema.

Enfim, o presente ensaio se dedicará a investigar a questão da ofensa aos direitos fundamentais do investigado em face da produção de prova digital no processo penal no ordenamento jurídico brasileiro e português.

# CAPÍTULO I – AS NOVAS TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO E SUAS INFLUÊNCIAS

# 1. As novas tecnologias de informação e comunicação e os direitos fundamentais

O homem vem a alterar, continuamente, de forma substancial o seu modo como se desloca de um lugar para o outro, como pensar, modificando-se conforme o grau de competitividade a que a sociedade o sujeita, tornando-o mais produtivo.

Na sociedade atual existe uma imensa massificação e expansão das tecnologias de informação e comunicação. Está-se perante de uma utilização totalmente globalizada destas novas tecnologias por qualquer pessoa independentemente da idade, preferência, localidade, entre outros.

Armando Dias Ramos, com a acuidade que lhe é peculiar, muito bem descreve a influência da tecnologia na sociedade contemporânea afiançando que “a informática há muito que entrou nas nossas vidas e com ela uma catadupa de acontecimentos têm surgido nas últimas décadas, as quais nos afetam direta ou indiretamente. Os desenvolvimentos operados, quer a nível de *hardware* quer a nível de *software*, nas redes de informação e comunicação têm produzido alterações no *modus vivendi* das sociedades a nível global. Criamos uma dependência de tal ordem que hoje somos quase incapazes de viver sem as tecnologias de informação e comunicação”[[1]](#footnote-1).

Desde o surgimento dessas novas tecnologias, em meados do século XX, elas têm-se penetrado em cada um dos diferentes setores da sociedade como a indústria, a economia, o comércio, o lazer e a educação a ponto de serem essenciais para a vida cotidiana.

Mais especificamente a partir da década de 1980, passou-se a afirmar que a sociedade atual é uma sociedade da informação ou da comunicação, uma que vez estas seriam nos dias atuais não só um nascedouro de riquezas, mas também causas principais das modificações e transformações econômicas, culturais, políticas e sociais.

A evolução e a proliferação das tecnologias de informação e comunicação, em especial os canais de comunicação, dos sistemas informáticos e dos dispositivos eletrônicos, aliadas à rapidez e à facilitação do anonimato em ambiente digital, acabaram também por estimular o desenvolvimento de novas atividades criminais[[2]](#footnote-2).

Nesta oportunidade, impende relatar que as aludidas tecnologia de informação e de comunicação sugiram quando da implementação do denominado processo de globalização.

Os grandes avancos tecnológicos impulsionaram sobremaneira as relações entre as pessoas, e tal fato não pode ser ignorado no mundo jurídico, em razão da instantaneidade do processo de comunicação decorrente da utilização dos meios eletrônicos.

O autor português Renato Lopes Militão[[3]](#footnote-3) demonstra ser descrente sobre os benefícios que as novas tecnologias da informação e da comunicação veio a proporcionar à sociedade.

Não é por demais apropriado ingressar no âmbito desta dissertação o aprofundamento e apreciação da presente perspectiva, ou seja, se as denominadas novas tecnologias da informação e da comunicação concedeu à sociedade benefícios ou malefícios.

Entretanto, para o aludido autor, o cenário apresentado por aqueles que defendem os benefícios trazidos pelas tecnologias da informação e da comunicação está na existência de uma nova economia com predominância de bens imateriais, cujas características são o crescimento econômico, expansão do emprego no domínio dos serviços relacionados com aquelas tecnologias, não passaria de mito radicalmente ideológico construido para o efeito[[4]](#footnote-4).

Para contrariar o que foi propagado pelos expoentes da chamada *nova economia*, o citado autor assevera que desde o início das novas tecnologias da informação e da comunicação, a taxa de crescimento econômico tem sido visivelmente reduzida, mormente se analisada com a que se registrou nas décadas anteriores[[5]](#footnote-5).

Ainda de acordo com o autor portugues, os benefícios de produtividade oriundos da utilização das novas tecnologias da informação e da comunicação são declaradamente inferiores aos que se têm observado nos setores e atividades que não se utilizam de tais tecnologias, além disso o percentual de empregos gerados pelas novas tecnologias dista léguas daqueles que se verifica em atividades semelhantes[[6]](#footnote-6).

Com o respeito devido ao posicionamento acima mencionado, não se olvida que, de fato, pode-se afirmar que as novas tecnologias de informação ou da comunicação influenciaram, em âmbito global, uma nova metodologia de economia, cujas características se afigura na introdução dos bens imateriais ou impalpáveis.

Os ganhos propocionados pelas novas tecnologias concederam à sociedade inegáveis benefícios, entretanto, tais benefícios proporcionaram também o surgimento de novos delitos, denominados de delitos informáticos, tornando-os mais comuns e acessíveis.

Feito esse pequeno contraponto, porém necessário, impende ressaltar que em tempos hodiernos, diversos processos de comunicação e armazenamento de dados e informações tem se intensificado nos meios eletrônicos, de maneira que os avanços tecnológicos implicam seus efeitos diretamente na vida privada e na esfera processual penal.

O que está em apreciação, é o emprego das novas tecnologias da informação e da comunicação para a prática delitiva e o uso de materiais advidos de sua utilização como prova – prova digital - no processo penal com infringência aos direitos fundamentais e garantias processuais do investigado.

Depois da abordagem sobre as denominadas novas tecnologias da informação e da comunicação, faz sentido no que se refere à disposição estrutural desta dissertação, versar algumas palavras sobre os direitos fundamentais.

Num formato conceitual, e a despeito dos demais conceitos análogos, direito fundamental é uma proposição jurídica positivada que ampara o indivíduo e a sociedade em relação ao Estado.

Diante desse panorama, pode-se afirmar que os direitos fundamentais não são absolutos ou ilimitados, na verdade, estão sujeitos a uma série de restrições ou limitações que fazem com que seu titular não possa exercer livremente certo direito em determinadas circunstâncias, em prol do bem comum.

E, na mesma direção de que os direitos fundamentais não são absolutos, muito bem assevera o jurisconsulto português Manuel Monteiro Guedes Valente, em seu artigo “Os direitos e garantias dos cidadãos investigados na era digital” que afirma que “hoje as pessoas pensam que podem escrever e dizer tudo nas redes sociais por considerarem que estão em um Estado de [total] liberdade de expressão, olvidando, assim, que os limites se extinguem com a afirmação de cada um dos nossos [seus] direitos fundamentais pessoais. O direito de liberdade de expressão e o direito de e à informação não são ilimitados. Aceção que muitas vezes os seres digitais esquecem e embarcam na onda que todos pensam conseguir surfar”[[7]](#footnote-7).

Em virtude do exposto, restou demonstrado que os benefícios que as novas tecnologias de informação e comunicação proporcionaram à sociedade são inegáveis, entretanto, tais benesses têm um outro lado, que foi a porta de entrada para a prática do denominado Crime informático, tornando-o mais atingível.

Concordando com a afirmativa acima, Armando R. Dias Ramos assevera que “contemporâneo deste avanço científico foi também o aproveitamento realizado por indivíduos que se dedicam à criminalidade, tirando partido das mesmas para realizarem delitos criminais à distância de um *click.* Surgiu, assim, uma nova forma de cometimento de crimes*”[[8]](#footnote-8)*.

Assim, para a assegurar a vigência e eficácia dos direitos fundamentais, os quais possuem um limite inexorável[[9]](#footnote-9), é mister equilibrar a produção de provas na a apuração das infrações digitais com a tutela e proteção daqueles.

Este tema tem grande relevância jurídica, não só no Brasil, como também nos demais países do mundo, tendo em vista as grandes dificuldades econtradas quando o assunto é a utilização das provas digitais como meio de prova no processo penal.

É sabido que uma das funções específicas da fase investigativa do processo penal consiste na realização dos atos de investigação destinados a apurar a existência e tipicidade do ato e sua autoria. Esses atos são construídos em pressupostos materiais imprescindíveis para que as partes possam fazer e comprovar suas acusações.

A coleta de provas do ambiente digital afeta diretamente, direitos fundamentais e garantias processuais asseguradas ao cidadão e, como consequência da evolução tecnológica é possível afirmar que quase todas as infrações penais contam com suporte virtual.

Neste contexto, a utilização pela polícia de tecnologias modernas constitui uma ferramenta de trabalho essencial para obter provas digitais do crime e neutralizar os meios sofisticados de que se utilizam os grupos criminosos organizados, bem como o caráter internacional de sua atividade.

Nesse aspecto dual entre os direitos fundamentais e a produção probatória virtual a Constituição da República Federativa do Brasil de 1988 trouxe em seu artigo 5º, incisos X e XII[[10]](#footnote-10) os direitos à intimidade, à privacidade e o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas.

Já em Portugal, através dos ensinamentos de Jorge Miranda e Rui Medeiros, tem-se que o “artigo 26º da Constituição da República Portuguesa[[11]](#footnote-11) constitui expressão direta do postulado básico da dignidade humana que a Constituição consagra logo no nº 1 como valor logicamente anteiror à própria ideia de Estado de Direito democrático e que constitui a referência primeira em matéria de direitos fundamentais”[[12]](#footnote-12).

Asseveram ainda os citados autores que, o direito da personalidade abarca a proteção “de todos os bens de personalidade independentemente de estarem ou não tipicamente consagrados”[[13]](#footnote-13), incluindo aqui o direito à palavra e à imagem que são considerados como “expressões típicas da autonomia pessoal” bem como “o direito a que não sejam registradas ou divulgadas palavras ou imagens da pessoa sem o seu consentimento”[[14]](#footnote-14).

Também impende realçar a tutela que o artigo 32º n.º 8 da Constituição da República Portuguesa[[15]](#footnote-15) confere ao sigilo das comunicações quando declara como nulas todas as provas obtidas mediante a intromissão abusiva nas mesmas.

No mesmo viés, a Carta dos Direitos Fundamentais da União Européia elenca em seus artigos 7º, n° 1 do artigo 8º e n° 1 do artigo 52º[[16]](#footnote-16) o direito à vida privada e também à proteção dos dados de caráter pessoal.[[17]](#footnote-17).

Por todo o exposto alhures, no próximo trecho da presente dissertação serão feitas análises sobre as possíveis influências das novas tecnologia da informação e da comunicação sobre a produção de provas digitais no direito processual penal.

# 2. As novas tecnologias de informação e comunicação e o direito processual penal

Todas as investigações criminais têm como principal objetivo obter o máximo possíveis de informações sobre a prática de um ato criminoso (o que aconteceu, quem interveio, quando e onde ocorreu) assim, devido a essa onipresença das novas tecnologias de informação e comunicação, em especial a *internet,* em nossas vidas, bem como o uso diário de múltiplos dispositivos eletrônicos, as autoridades responsáveis ​​pela investigação criminal mostrou um enorme interesse em poder acessar e analisar toda essa abundante informações digitais com as quais lidamos diariamente e as usamos para a investigação de todas classe de crimes.

Como visto uma das funções específicas da fase investigativa do processo penal consiste em realizar os atos de investigação destinados a apurar a preexistência e tipicidade do ato e sua autoria. Esses atos são erigidos em patamares materiais essenciais para que as partes possam preparar e fundamentar suas acusações e posteriormente, a defesa.

Assim, a primeira e principal garantia do investigado é estabelecida pelo princípio da legalidade que constitui pressuposto comum a todos os atos processuais limitantes de qualquer direito fundamental.

Por mandato expresso das Constituições Federais – brasileira[[18]](#footnote-18) e portuguesa[[19]](#footnote-19), qualquer ingerência estatal no campo dos direitos fundamentais e das liberdades públicas que afeta diretamente o seu desenvolvimento ou limita ou condiciona o seu exercício, requer autorização legal para tanto.

Os direitos fundamentais garantem aos indivíduos, um *status* jurídico ou liberdade no âmbito de sua existência. Portanto, é competência do legislador habilitar os órgãos persecutórios com meios legais e adequados de investigação. O artigo 8.2 da Convenção Europeia de Direitos Humanos[[20]](#footnote-20) prevê expressamente que qualquer interferência do poder público na esfera privada deve ser "previsto por lei".

Este princípio geral deve ser afirmado, especialmente enfaticamente, em âmbito do processo penal, pois, a ação do poder do Estado em sua forma mais extrema -punição criminal- implica uma profunda interferência na liberdade do acusado e no mais sagrado núcleo de seus direitos fundamentais – a liberdade.

Por isso, a importância de aumentar a capacidade das autoridades para usar qualquer medidas de pesquisa tecnológica destinadas a obter essas informações em um formato digital parece ser um pilar essencial em qualquer investigação criminal na atual sociedade informatizada em que vivemos, sem que isso implique em violação de seus direitos fundamentais.

De fato, a principal vantagem de usar estas novas medidas de investigação tecnológica reside na sua operacionalidade para obter provas de qualquer tipo de crime, seja ou não dos crimes de informática, uma vez que são uma ferramenta eficaz na investigação de qualquer tipologia criminal em que tais dispositivos eletrônicos constituem uma valiosa fonte de evidência, devido às suas atuais capacidades de armazenamento de informações e seu uso para todos os tipos de comunicações

A garantia do direito fundamental à privacidade é um dos grandes desafios dos sistemas jurídicos na atualidade e, portanto, também do direito processual penal, uma vez que uma das consequência do progresso da ciência no campo das telecomunicações, quase todas as infrações penais hoje contam com suporte tecnológico.

Essa proteção é de intenso interesse público: a repressão legal à conduta criminosa. No exercício desta função essencial do Estado, deve estar sempre presente a defesa adequada dos direitos e liberdades das pessoas envolvidas, o que acontencerá com o emprego legal e adequado do direito processual penal.

Neste contexto, a utilização por parte do Estado de tecnologias modernas constitui uma ferramenta de trabalho essencial para obter a provas digitais do crime e contrariar os meios sofisticados de que servem os grupos criminosos organizados, bem como o caráter internacional sua atividade.

No entanto, a investigação criminal derivada da utilização destas tecnologias coloca novos desafios que requerem uma resposta do legislador, pois há a necessidade de buscar um equilíbrio adequado entre a garantia segurança pública e a proteção da privacidade dos investigados, ponderação esta que se dará através da efetivação do direito processual penal.

Sobre a importância da efetivação do direito processual penal, a autora portuguesa Rosa Vieira Neves afiança que “a efetivação do processo penal visa essencialmente a realização da justiça e a descoberta da verdade material, a protecção dos direitos fundamentais e o restabelecimento da paz jurídica, através da aplicação de uma sanção penal ao arguido que violou específicos bens jurídicos que ascenderam à discursividade penal”[[21]](#footnote-21).

Nas lições de Guedes Valente, para quem o “direito processual penal é por excelência o Direito dos inocentes”[[22]](#footnote-22), tem-se que tal ciência “encontra-se em conflito permanente com a ânsia e o clamor de um povo que reclama justiça imediata e ou “a justiça do já”. Esta dinâmica da sociedade internético-personocêntrica derruba barreiras e limites, que se impuseram ao longo da história e que se devem impor como inultrapassáveis no campo da obtenção da prova penal, em especial no campo da investigação criminal *stricto sensu*, ou seja, aquela que se destina a recolher vestígios e indícios probatórios, elementos de prova reais e pessoais para o processo-crime para que, em sede de julgamento, se produza a prova fundante da decisão judicial”[[23]](#footnote-23).

E, como bem salientou o consagrado autor português Jorge de Figueiredo Dias “as soluções concretas dos problemas básicos do Direito Processual Penal dependam fundamentalmente do estádio de evolução e desenvolvimento social e cultural de uma certa comunidade, do grau de maturidade logrado pela sua consciência jurídica, das conceções jurídicas de base e das concretas formas de atuação estadual que aí vigoram, enfim, na tradição histórica nela vivente (…). O direito processual penal é o produto de uma longa evolução dirigida à escolha dos meios conducentes à realização ótima das tarefas próprias da administração da justiça penal”[[24]](#footnote-24).

A informática e a telecomunicação é gradativamente utilizada em todos os setores da sociedade, da defesa da soberania nacional, trafegando pela atividade financeira, econômica, científica, na saúde, na educação, à administração pública.

Entretanto, ao lado dessa “evolução” aparecem também práticas criminosas, possibilitando o surgimento da criminalidade organizada, colocando em perigo alguns setores importantes da comunidade, tais como transportes, serviços de telecomunicações e de urgências, entre outros.

Como mencionado, o crime organizado também tem aproveitado os avanços da ciência no campo das telecomunicações para expandir sua infraestrutura e para a consecução da prática criminosa, que se manifesta cada vez mais violenta e mais sofisticada nos meios e técnicas que usa, agindo de forma rápida, massiva e contínua.

Na verdade, quase todas as infrações criminais têm atualmente um suporte tecnológico. Para dar uma resposta às formas de delinquência ligadas ao uso de novas tecnologias, juntamente com a “delinquência tradicional”, surgiram outras que exigem buscar um equilíbrio adequado entre segurança e privacidade.

De um lado, tem-se a capacidade do Estado para enfrentar esta nova fenomenologia criminal, e de outro, a garantia da inviolabilidade dos direitos fundamentais assegurados constitucionalmente. É necessário ponderar cautelosamente a interferência na esfera dos direitos fundamentais para que seu conteúdo essencial não seja distorcido.

Como apontou o autor argentino Eduardo Juan Couture nesse sentido, configurado como garantia individual, *"el proceso (civil o penal) ampara al individuo y lo defiende del abuso de la autoridad del juez, de la prepotencia de los acreedores o de la saña de los perseguidores*".[[25]](#footnote-25)

O surgimento de novas tecnologias na investigação criminal não deve tornar-se, consciente ou inconscientemente, causa justificadora da manutenção de deficiências no sistema penal ou para corroer garantias historicamente consolidadas.

Também no novo ambiente tecnológico toda restrição de direitos fundamentais necessita de autorização judicial embasada em ditames legais, não podendo ser considerada legítima aquela decisão com fundamentação genérica. Isso se reveste de particular importância quando analisado sob o aspecto da proteção dos direitos e garantias pessoais.

No entanto, o interesse público inerente ao estado *ius puniendi* é constrangido pelo dever de respeitar os demais interesses públicos presentes no processo: não é senão a expressão da chamada garantia jurisdicional (e processual) na imposição de penalidades.

Se o processo judicial é concebido como garantia, é devido ao risco do Estado ultrapassar no exercício das suas atribuições de único titular do direito/dever de julgar o crime, por isso que os ordenamentos jurídicos brasileiro e português reconhecem limitações ao exercício da atividade probatória no processo penal, pois a verdade não pode ser apurada a qualquer preço.

Diante de tais circunstâncias, José Francisco de Faria Costa assinalou para a necessidade de o Direito Penal e Processual Penal regulamentar os crimes informáticos, asseverando para tanto que “a informação automatizada é uma realidade tão essencial que se, por hipótese - e não se está, por certo, a entrar no domínio da ficção científica -, se bloqueasse, totalmente e à escala mundial, o fluxo informacional automatizado, ainda que por breves horas, todos convêm em considerar que o caos se institucionalizaria. Ora, uma realidade tão importante, tão essencial para se empregar a expressão exata, que gera e suporta interesses materiais de somas astronómicas, rapidamente se impõe, repete-se, como uma questão a que o direito penal, se bem que em *ultima ratio*, não pode ficar indiferente”[[26]](#footnote-26).

Considerando o surgimento das novas necessidades ao direito penal e ao processo penal, necessidades que são resultantes da globalização, instou o legislador a elaborar instrumentos que objetivam diminuir constrangimentos e ilegalidades ocasiondas pela investigação criminal.

Ante tal panorama, é imperioso mencionar que foi aprovada no Brasil a Lei 9.296/1996 que regulamenta as interceptações telefônicas, com caráter processual penal, uma vez que dispôs sobre a persecução criminal em todas as suas fases, na hipótese de indícios razoáveis da autoria ou participação em infração penal, a prova não puder ser feita por outros meios disponíveis e quando o fato investigado constituir infração penal punida com pena de reclusão, conforme estabelece em seu artigo 2º.[[27]](#footnote-27)

Mais recentemente, ocorreram alterações significativas tanto no Código Penal e quanto no Código de Processo Penal brasileiros oriundas da vigência da Lei 14.155, de 27 de maio de 2021, a qual tornou mais graves os crimes de violação de dispositivos informáticos, futo e estelionato cometidos de forma eletrônica ou pela internet, e definiu a competência em modalidade de estelionato[[28]](#footnote-28).

Além disso, é necessário cumprir o requisito constitucional atinente à ordem do juízo competente, conforme descrição no inciso XII do artigo 5° da Constituição Federal Brasileira.

Impende ressaltar que no que tange às provas, não é, em termos gerais, um objetivo incondicional ou isento de limitações e, portanto, é possível estabelecer (e, de fato, há) limites ao seu exercício, por se tratar de uma garantia individual.

A Lei Fundamental Portuguesa disciplina em seu artigo 26º, sob a nomeclatura “Outros Direitos Pessoais” que “a todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à protecção legal contra quaisquer formas de discriminação”.

Nessa mesma toada, o número 2 do mesmo dispositivo constitucional dispõe que “a lei estabelecerá garantias efectivas contra a obtenção e utilização abusivas, ou contrárias à dignidade humana, de informações relativas às pessoas e famílias”.

Como observado, a Constituição da República Portuguesa, preserva em si, incontáveis formas de tutelar os direitos e garantias fundamentais, haja vista a imposição limites necessários à validade dos meios de prova e de sua obteção.

Seguindo os quadros europeus de regulamentação da denominada criminalidade informática – Resolução n.º 09/1989, o legislador português inseriu no ordenamento jurídico a Lei da Criminalidade Informática n.º 109/1991, de 17 de agosto, que muito embora tem prerscrutado uma gama de delitos, equivocou-se ao não contemplar meios de recolha de prova no ambiente digital.

Já em 15 de setembro de 2009 ingressou no ordenamento jurídico português a Lei n.º 109/2009 – Lei do Cibercrime – a qual além de revogar a Lei 109/1991, veio a estabelecer disposições penais materiais e processuais, bem como disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte eletrônico[[29]](#footnote-29).

Como observado, tanto o ordenamento jurídico brasileiro como o português se atentaram para com a tutela dos direitos fundamentais, constando em suas respectivas Constituições meios e instrumentos para a sua proteção.

Também é de se mencionar que em ambos os ordenamentos jurídicos há leis que disciplinam o assunto referente à denominada cibercriminalidade, sendo tratado como mais profundidade e acuidade em Portugal.

Diante da análise das influências das novas tecnologias de informação e de comunicação no direito processual penal, é mister, no próximo tópico, verificar o conceito de crimes cibernéticos ou cibercrimes tanto no Brasil quanto em Portugal.

# 3. Da Inexistência de definição concreta de Crimes Cibernéticos ou Cibercrimes

A premissa maior que se tem no presente assunto é que não há consenso entre os autores sobre uma definição concreta do conceito de crimes cibernéticos ou cibercrimes. Aliás, não há sequer um acordo sobre a nomeclatura a ser utilizada ao se tratar dos aludidos crimes.

Diante de tais constantações é imperioso referir que no dia 23 de novembro de 2001 a Convenção sobre o Cibercrime foi subscrita em Budapeste, a qual passou a ser denominada de Convenção de Budapeste[[30]](#footnote-30) e entrou em vigor em 1º de julho de 2004.

O objetivo da Convenção foi dar conformidade à lei penal material atinente à seara do cibercrime, principalmente o dano e sabotagem informática; produção, posse e distribuição de material pornográfico infantial na rede mundial de computadores; além de explicitar instruções de natureza processual, principalmente referente aos poderes e instrumentos de investigação para o combate desta criminalidade.

Em razão da dificuldade na recolha de prova digital e também motivado pela característica de transnacionalidade do cibercrime, Armando R. Dias Ramos indica outro objetivo da Convenção de Budapeste, qual seja a de uniformizar “a legislação internacional, mormente a nível europeu, sobre a temática – cibercrime – que é transversal a todos os países”[[31]](#footnote-31).

Oportuno ressaltar que o Brasil não é subscrevente da Convenção de Budapeste, ainda que ela esteja inspirando nitidamente a legislação sobre os crimes cibernéticos bem como nos instrumentos de investigação adequadas para enfrenta-los[[32]](#footnote-32).

Já em Portugal, através do Decreto do Presidente da República n.º 91/2009, a Convenção sobre o Cibercrime[[33]](#footnote-33) fora ratificada em 15 de setembro de 2009.

Como salientado acima, são diversos os vocábulos empregados com frequência e de forma aleatória para conceituar os crimes cibernéticos, quais sejam: crime informático; crime informático-digital; crime digital; cibercrimes; crime de alta tecnologia, etc,. Aliás, a autora e advogada portuguesa Vera Elisa Marques ao citar Silva Rodrigues assevera que “não há consenso quanto à expressão, à definição, nem quanto à tipologia e classificação destes crimes”[[34]](#footnote-34).

A Comissão das Comunidades Europeias, em 22 de maio de 2007, publicou a Comunicação da Comissão ao Parlamento Europeu, ao Conselho e ao Comité das Regiões, oportunidade em que afirmou ser o cibercrime, para os efeitos da citada comunicação, “actos criminosos praticados com recurso a redes de comunicações electrónicas e sistemas de informação ou contra este tipo de redes e sistemas”[[35]](#footnote-35).

Garcia Marques e Lourenço Martins, citados por Pedro Dias Venâncio, advertem para a circunstância de inexistir uma conceituação concreta para cibercrimes, e informam que “é frequente encarar a criminalidade informática como todo o acto em que o computador serve de meio para atingir um objectivo criminoso ou em que o computador é alvo simbólico desse acto ou em que o computador é objecto do crime”[[36]](#footnote-36).

O próprio autor acima referido ao comentar e anotar sobre a Lei do Cibercrime informa que “persiste a inexistência de um conceito de “criminalidade informática” expressamente consagrado na legislação, ou uniformemente sedimentado na doutrina e jurisprudência”[[37]](#footnote-37).

Entretanto, este autor nos oferece um conceito de cibercrime em duas vertentes. A primeira diz respeito ao conceito amplo de cibercrime consistente em “toda a panóplia de atividade criminosa que pode ser levada a cabo por meios informáticos, ainda que estes não sejam mais que um instrumento para a sua prática, mas que não integra o seu tipo legal, pelo que o mesmo crime poderá ser praticado por recurso a outros meios”[[38]](#footnote-38).

Deste conceito amplo de cibercrime é possível concluir que são todas as condutas ou atividades que podem ou não ser praticadas através dos meios informáticos, sendo certo que para a consumação do delito aqueles não são necessários.

Têm-se aqui os casos em que o meio informático não faz parte do tipo legal da infração penal, haja vista que estas podem ser praticadas por outros meios, tais como os crimes contra a honra.

A segunda vertente é referente ao conceito em sentido estrito de cibercrime que seria aquele cujo tipo penal exige o denominado elemento informático ou digital para a sua configuração. Ou seja, para a configuração do cibercrime a presença dos componentes informáticos se faz necessária.

Nesta senda, pode-se citar como pertecente a essa tipologia, os crimes tipificados na Lei do Cibercrime – Lei 109/2009.

Para finalizar a análise do conceito de cibercrime levado a efeito por autores portugueses, é necessário antes, vislumbrar a catologação feita por Rita Coelho Santos[[39]](#footnote-39), para quem os “crimes tipicamente informáticos”, são aqueles ligados eminentemente à informática, os “crimes essencialmente informáticos”, os que possuem o bem jurídico ofendido de natureza informática, e, por fim, os crimes “acidentalmente informáticos”, aqueles em que o computador é apenas instrumento para a prática delitiva, não sendo, portanto, elemento integrante do tipo penal.

No Brasil, Dario José Kist assevera que “a incipiente doutrina sobre a cibercriminalidade ainda nao foi capaz de conduzir a uma uniformidade na sua designação, havendo referência a crimes virtuais, crimes cibernéticos, crimes de Internet, crimes de computador, crimes de informática ou informáticos, crimes digitais e cibecrimes”[[40]](#footnote-40).

Ainda, para o citado autor brasileiro “a tendência, ao que parece, caminha no sentido de estabilizar a denominação crimes ou delitos informáticos, perspectiva denunciada pela opção legislativa feita com a Lei n.º 12.737/12 (Lei Carolina Dieckmann), cum cujo enunciado consta que ela dispoe “sobre a tipificação criminal de delitos informáticos”[[41]](#footnote-41).

Mesmo diante de tais inconsistência na definição de cibercrimes, tem-se que o mesmo pode ser conceituado como aquele crime cujos sistemas digitais ou informáticos podem servir de instrumento para a prática criminosa, ou cujos aparelhos informáticos são alvo da conduta criminosa, sendo certo que a infração penal praticada por meio de instrumentos informáticos terá semelhanças com aquelas previstas tradicionalmente pelo legislador penal.

A despeitos das classificações e conceitos referidos acima, não se pode negar o que é idubitável, que esta natureza de criminalidade é uma realidade e encontra-se em franca e permanente expansão.

Corroborando com este entendimento, Armando R. Dias Ramos acrescenta que esta forma de criminalidade “é a de todas a mais grave e a que acarreta maiores dificuldades de identificação dos seus autores”[[42]](#footnote-42).

Como já fizemos referência, a principal circunstância de diferença neste modelo de criminalidade, é justamente a utilizaão dos instrumentos tecnológicos ou informáticos. À vista do exposto, em razão do seu alto grau de complexidade (a extensão e dimensão da realidade virtual) a cibercriminalidade torna bastante custosa a identificação e qualificação dos agentes infratores.

Diante do exposto, é sabido que obter o conhecimento das origens e das causas da infração penal, possibilita que providências seguras e eficazes sejam efetivadas para combate-las, tais como identificar as ameaças, com o menor tempo de reação e o com o mínimo de dano.

Com isso, nasce a prioridade em antever a prática delitiva, de modo que a prevenção seja estabelecida e adaptada à nova realidade tecnológica, sem a necessidade de se perquirir a forma com a qual o delito será praticado.

Novamente, utilizando os ensinamentos de Armando Dias Ramos é possível “afirmar que os crimes são velhos, as condutas é que são praticadas de um modo novo, as quais se nao estiverem tipificadas passam incólumes à ação da justiça”[[43]](#footnote-43).

Visto o tratamento legal e doutrinário dado sobre o conceito e classificação do crime cibernético ou informático, no próximo tópico ingressar-se-á à análise de sua tipificação no Brasil e em Portugal.

# 4. Da previsão legal dos Cibercrimes

Objetivamente, é possível notar que há diferenças no modo de tipificar a cibercriminalidade. Em Portugal está em vigor a Lei n.º 109/2009[[44]](#footnote-44), de 15 de setembro, denominada de “Lei do Cibercrime”, onde no Capítulo II, sob a rubrica de “Disposições penais materiais” constam a previsão legal para os seguintes tipos penais: art. 3º - falsidade informática[[45]](#footnote-45); art. 4º - o dano relativo a programas ou outros dados informáticos[[46]](#footnote-46); art. 5º - a sabotagem informática[[47]](#footnote-47); art. 6º - o acesso ilegítimo[[48]](#footnote-48); art. 7º - a interceptação ilegítima[[49]](#footnote-49) e art. 8º - a reprodução ilegítima de progrma protegido[[50]](#footnote-50).

Recentemente, o Capítulo II da Lei n.º 109/2009 fora profundamente alterada pela Lei n.º 79/2021[[51]](#footnote-51), de 24 de novembro, para inserir diversar outras figuras típicas, quais sejam: art. 3.º-A - Contrafação de cartões ou outros dispositivos de pagamento; art. 3.º-B - Uso de cartões ou outros dispositivos de pagamento contrafeitos; art. 3.º-C - Aquisição de cartões ou outros dispositivos de pagamento contrafeitos; art 3.º-D - Atos preparatórios da contrafação; art 3.º-E - Aquisição de cartões ou outros dispositivos de pagamento obtidos mediante crime informático.

Já no Brasil, o tratamento dado aos crimes informáticos não seguiu o modelo português, uma vez que não há uma lei especial e própria para catalogar os cibercrimes, sendo que estes estão situados em leis esparsas, merecendo atenção as seguintes: arts. 72[[52]](#footnote-52) e 73[[53]](#footnote-53) da Lei n.º 8.078/90, que dispõe sobre “a proteção do consumidor e dá outras providências”[[54]](#footnote-54); art. 2º[[55]](#footnote-55), inciso V, da Lei 8.137/90, que “define crimes contra a ordem tributária, econômica e contra as relações de consumo, e dá outras providências”[[56]](#footnote-56); art. 241-A[[57]](#footnote-57) (inserido pela alteração provocada pela Lei n.º 11.829/1998) da Lei n.º 8.069/90, que dispõe sobre “o Estatuto da Criança e do Adolescente e dá outras providências”[[58]](#footnote-58); art. 10[[59]](#footnote-59) (alterado recentemente pela Lei n.º 13.869/2019) da Lei 9.296/96[[60]](#footnote-60), que regulamenta a parte final do inciso XII do art. 5º da Constituição Federal; art. 72[[61]](#footnote-61) da Lei n.º 9.504/97, que “estabelece normas para as eleições”; art. 12[[62]](#footnote-62) da Lei n.º 9.609/98, que dispõe sobre “a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências”[[63]](#footnote-63).

O Código Penal brasileiro também traz em seu bojo algumas condutas criminosas catalogadas como cibercrimes, e merecem destaques as seguintes: art. 153, §1º-A[[64]](#footnote-64) – Divulgação de segredo; art. 154-A[[65]](#footnote-65) – Invasão de dispositivo informático (recentemente alterado pela Lei n.º 14.155/2021); art. 155, §4º-B[[66]](#footnote-66) – Furto qualificado mediante uso de dispositivo informático ou eletrônico (recentemente alterado pela Lei n.º 14.155/2021); art. 171, §2º-A[[67]](#footnote-67) – Fraude eletrônica; art. 313-A[[68]](#footnote-68) – Inserção de dados falsos em sistema de informações; art. 313-B[[69]](#footnote-69) – Modificação ou alteração nao autorizada de sistema de informações; art. 325, §1º[[70]](#footnote-70) - violação de sigilo funcional.

Diante do aludido, é observável que no Brasil, mesmo que de forma dispersa, tem-se um rol de tipos penais para abranger certa área da cibercriminalidade, quais sejam fraudes bancárias, uso indevido das redes sociais para a prática de crimes contra a honra, acesso ou uso não autorizado de sistemas ou dados, entre outros.

Segundo Dario José Kist[[71]](#footnote-71) em razão da intensidade da cibercriminalidade, é possível verificar que de forma paulatina a tipificação das condutas estão a ser inseridas nos ordenamentos jurídicos dos mais variados países.

Informa ainda o autor que “a importância ou mesmo a imprescindibilidade dessa medida situa-se em dois campos: um é o âmbito do princípio da legalidade penal – somente pode ser objeto de persecução penal conduta humana previamente definida em lei como crime; a outra diz respeito ao caráter transnacional da cibercriminadade, que demanda esforços conjugados entre os países por ela concretamente afetados para a punição dos agentes, em especial no campo da obtenção de prova”[[72]](#footnote-72).

Analisada a previsão legal do cibercrime tanto no Brasil quanto em Portugal, chegou-se o momento de adentrarmos no campo da denominada prova digital ou prova eletrônica.

# CAPÍTULO II – DA PROVA DIGITAL

# 1. Introdução

Como visto acima, as novas tecnologias de informação e comunicação, especialmente a *internet,* está revolucionando os pilares tradicionais da sociedade, trazendo novos conceitos e uma infraestrutura para prestação de uma ampla gama de serviços de comunicações eletrônicas.

O autor português Pedro Dias Venâncio aponta que o impacto das novas tecnologias de informação e comunicação na sociedade é gigantesca, haja vista que se constitui caminho exclusivo que permita a ocorrência de variadas relações econômicas, sociais, culturais, que de outro modo não existiram[[73]](#footnote-73).

Neste mesmo sentido, o preâmbulo da Convenção sobre o Cibercrime descreve os cuidados e riscos provocados pelas novas tecnologias de informação e comunicação ao afirmar que “conscientes das profundas mudanças provocadas pela digitalização, pela convergências e pela globalização permanente das redes informáticas; preocupados com o risco de que as redes informáticas e a informação electrónica sejam igualmente utilizadas para cometer infracções criminais e de que as provas dessas infracções sejam armazenadas e transmitidas através dessas redes”[[74]](#footnote-74).

Atualmente, como consequência do fenômeno da *Internet*, existem muitas pessoas que vivem no ambiente virtual, pois é por meio dele que se espalham cultura, se pode desfrutar de lazer sem nenhum tipo de limitações, pode se estabelecer relações entre as pessoas, uma vez que surgem inúmeras formas de ócio e de comunicação *online*, as compras são feitas de forma rápida e fácil através do comércio eletrônico etc,. Em suma, são numerosos os aspectos da vida cotidiana que se desenvolvem diariamente no dito ambiente virtual.

Como consequência desta realidade cada vez mais predominante, é necessário articular uma efetiva tutela jurisdicional do ambiente virtual, uma vez que os avanços advindos das novas tecnologias (como análise de DNA, câmeras de vídeo, programas rastreadores de computador, telefones celulares, acústica forense, etc.) vem aumentando proporcionalmente as infrações penais cometidas por este meio.

Para servir de exemplo, o *hacker* que espalha um vírus (cavalo de tróia) na rede, aquele que faz ameaças a outra pessoa através de uma rede social, ou que espalha pornografia infantil em determinados fóruns, ou que comete fraude por meio de dos portais de *internet*, são alguns dos comportamentos que têm ocorrido como consequência das novas tecnologias.

Sem dúvida, pode-se dizer que a *Internet* tem se tornado um novo instrumento para a prática de atos criminosos.

Tem-se por um lado, o aumento do uso de novas tecnologias e, por outro, o aumento das condutas criminosas realizadas por meio delas, e, essa nova realidade também conduz a uma transformação no processo de investigação criminal.

Manuel Monteiro Guedes Valente ressaltando a necessidade de adequar os meios persecutórios no combate a cibercriminalidade aos princípios constitucionais, com clareza assenta que “esta nova era e a necessidade de prevenção e repressão da criminalidade que recorre aos meios digitais para desenvolver a sua atividade ilícita – a era da criminalidade digital – exige uma reflexão sobre a necessidade de reforçar ou de relembrar os princípios constitucionais regentes da intervenção penal, em especial processual, no mundo digital”[[75]](#footnote-75).

Especificamente, em Portugal a Lei n.º 109/2009, de 15 de setembro[[76]](#footnote-76), para o reforço das garantias processuais e a regulamentação de medidas persecutórias, contempla a partir do seu Capítulo III, uma série de medidas investigativas na fase de instrução, como o uso de dispositivos técnicos para capturar o imagem, rastreamento e localização, o uso do agente disfarçado de computador, bem como a informação exaustiva sobre a apreensão de equipamentos informáticos ou dispositivos de armazenamento de dados.

Por sua vez, no Brasil está em trâmite na Câmara dos Deputados, de autoria do Deputado Federal Hugo Leal – PSD/RJ, o Projeto de Lei n.º 4.939/2020, o qual tem por escopo dispor sobre “as normas de obtenção e admissibilidade de provas digitais na investigação e no processo, além de outras providências”[[77]](#footnote-77).

Em suma, verifica-se que os ordenamentos jurídicos, português e brasileiro, este ainda é incipiente, têm por objetivo dar fundamento legal às mencionadas diligências de investigação dos crimes cometidos por meio eletrônico e com uso das novas tecnologias e, assegurar que as mesmas sejam realizadas de maneira garantista.

# 2. Atividade Probatória e Prova

Em primeiro lugar, para se poder compreender corretamente em que consiste a prova digital é importante coloca-la dentro de uma estrutura de qualquer processo para entendermos a sua importância. Tanto a prova digital como qualquer outro tipo de prova clássica ou tradicional enquadram-se na chamada fase probatória do processo. Portanto, é necessário de um ponto de vista geral esclarecer o que se entende por atividade probatória e, consequentemente, pela prova.

Iniciando-se com a atividade probatória por ser um conceito mais claro e sobre o qual não geram demasiadas dúvidas, no contexto processual penal tal atividade visa a acreditar ou convencer-se da veracidade de determinado fato por meio de percepções sensoriais fornecidas por pessoas ou coisas que constituem fontes materiais ou instrumentos probatórios, tendo todos eles como destinatários o juiz ou tribunal responsáveis pelo caso em julgamento[[78]](#footnote-78).

Portanto, provar é a atividade levada a cabo pelas partes no processo, cujo objetivo é convencer o juiz ou o tribunal daquilo que foi alegado, sendo uma fase essencial e de indiscutível importância em qualquer processo. Nesta atividade realizada pelas partes, tem-se a prova como um elemento essencial, justamente por ser o meio empregado para tanto.

Jeremy Bentham considerava que a prova é “um fato supostamente verdadeiro, o qual deve servir de motivo de credulidade sobre a existência ou inexistência de outro fato. Assim, toda prova compreende pelo menos dois fatos distintos: aquele que podemos chamar de fato principal, e aquele que está tentando provar que existe ou que não existe, o outro o fato probatório, que serve para comprovar o sim ou não do fato principal”[[79]](#footnote-79).

Por sua vez, em sua obra “A prova civil”, Franceso Carnelutti fixa seu escopo de aplicação ao afirmar que “a prova é usada como verificação, da verdade de uma proposição; só se fala de prova quando algo que foi afirmado e cuja exatidão se busca provar; não pertence à prova o procedimento pelo qual uma verdade não afirmada é descoberta”[[80]](#footnote-80).

Assim, podemos definir prova como a atividade processual das partes - demonstração e do juiz -de verificação- através do qual se busca o convencimento psicológico do magistrado sobre a veracidade dos dados relativos ao processo.

A prova pode ser um fim e um meio. A prova como fim é aquela que visa a demonstração da existência e do conteúdo de um fato do qual depende um direito. Como meio é o conjunto de recursos que podem ser usados ​​para obter a referida demonstração, o fim da prova.

Os princípios que regem o processo penal e suas diferenças com outros processos/procedimentos são aplicadas ao campo probatório sendo que para estabelecer os elementos típicos da prova no processo penal devemos levar em conta: a presunção de inocência como garantia processual sobre culpabilidade que determinará o conteúdo da sentença que conduz à absolvição se a culpa do infrator não puder ser provada e a livre apreciação da prova ou e do livre convencimento.

Nesta oportunidade, é de bom alvitre citar as lições de Nicola Framarino dei Malatesta para quem afiança que “o movimento histórico gradualmente ascendente da humanidade conduz, em matéria probatória, à preponderância da substância da prova, com critérios fixos, por parte da legislação, determinando em que condições probatórias se estará certo e quem quais outras não: teríamos, assim, as provas legais. E, falamos em provas legais como de um progresso histórico, porque substituiram as ordálias[[81]](#footnote-81) e os duelos judiciários, sistema probatório barbaramente taumatúrgico, atingido pelos anátemas do quarto Concílio Lateranense”[[82]](#footnote-82).

Diante do exposto, realizada essa abordagem inicial sobre atividade probatória e o conceito em sentido amplo de prova, é mister iniciarmos a análise de uma prova específica, qual seja, as provas digitais.

# 3. Conceito de Prova Digital

Ao longo da história, a transmissão de informações evoluiu do papiro para os sistemas de computador, passando pelo papel, como o conhecemos hoje. As informações geradas ao longo da história foram armazenadas e suportadas ao longo do tempo neste material.

No último século ocorreram grandes avanços na humanidade. Graças ao rádio, ao telefone ou à televisão, a vida de muitas pessoas em torno do conceito de informação mudou radicalmente.

Com o tempo, essa informação, que a princípio era pelo rádio ou televisão, passou a ser transmitida pelo telefone, até atingir um caráter multidirecional ou global, graças ao surgimento do computador, mais especificamente graças à Internet e sua rede mundial de computadores.

Por meio das novas tecnologias, todas as informações podem ser transferidas de ponta a ponta do mundo, em milésimos de segundo.

Além disso, o surgimento de novas tecnologias transformou a guarda e o armazenamento de documentos. A tecnologia digital permitiu que uma quantidade enorme de informações pudesse ser comutada e passasse a ser acondicionadas, principalmente em razão do desenvolvimento na comunicação e transações na sociedade globalizada que migraram para o mundo digital, simbolizando comodidades, facilidades na mobilidade de dados.

Fernanda Teixeira Souza Domingos e Priscila Costa Schreiner Röder asseveram que os “documentos virtuais passam a fazer parte das relações sociais, tanto com referência às transações reais quanto às transações plenamente virtuais. Acompanhando essa tendência, a investigação dos ilícitos do mundo atual depende de evidências digitais, independentemente de terem ocorrido, total ou parcialmente, no mundo real ou no mundo virtual”[[83]](#footnote-83).

Nos dias que correm, a obtenção de provas digitais torna-se de extrema importância para desvendar delitos, deparando-se esta questão, porém, com a necessidade de conceituar provas no ambiente digital.

Inicialmante é mister ressaltar que a necessidade em conceituar provas digitais se origina do avanço tecnológico à presença cada vez mais reiterada das chamadas tecnologias de informação e comunicação em praticamente todos os âmbitos da vida cotidiana das pessoas, o que tem provocado, de maneira inevitável, a aparição de novos meios de provas conhecidos como prova eletrônica ou digital.

Nesta oportunidade, é importante asseverar que não há uma unanimidade entre os autores especialistas, sobre a nomeclatura – se prova digital ou eletrônica. David Silva Ramalho informa que há uma identificação de uma relação de gênero e espécie entre prova eletrônica e prova digital, aquela sendo o gênero e esta a espécie[[84]](#footnote-84).

Dario José Kist informa que “o conceito de prova eletrônica é mais amplo do que o da prova digital: engloba todas as formas de dados, sejam produzidos por dispsotivo analógico, ou de forma digital. Mas, ainda que relacionadas, as duas formas não podem ser confundidas, nomeadamente porque para a produção de cada uma delas devem ser observados normas e procedimentos específicos”[[85]](#footnote-85).

Também é imperioso afirmar que na atualidade, não contamos com nenhum corpo normativo a nível nacional – Brasil - e nem internacional que nos ofereça um conceito claro e único do que devemos entender por prova digital.

Por isso, é necessário nos acudir de conceitos oferecidos por diversos autores para podermos fixar uma noção mais aproximada possível do que vem a ser prova digital. E, uma das opções disponíveis para poder compreender o conceito de prova digital é coloca-la em relação com as ditas provas clássicas ou tradicionais, oferecendo assim uma definição geral e em sentido negativo, segundo a qual poderíamos afirmar que são todos aqueles meios de prova que não encaixam dentro daqueles já conhecidos e regulados pela lei.

O fato de que a prova digital tenha sua origem na evolução e aplicação da novas tecnologias de informação e comunicação na realidade que vivemos hoje em dia, faz-se necessário um conceito muito mais específico e autônomo, separando-a dos meios probatórios ja conhecidos.

Neste sentido e seguindo uma linha de concepção independente, é possível considerar as provas digitais como aquela informação obtida a partir de um dispositivo eletrônico ou meio digital, o qual serve para adquirir convencimento da certeza de um fato[[86]](#footnote-86); como aquele meio eletrônico que permite credenciar fatos relevantes para o processo, sejam eles fatos físicos ou mesmo eletrônico, e que é composto por dois elementos necessários à sua existência, os quais determinam a sua especialidade de prova eletrônica em relação a outros meios probatórios: um elemento técnico ou hardware e um elemento lógico ou software[[87]](#footnote-87).

Diante de tal espectro, devemos destacar que a prova digital tem um caráter polifacético em razão dela ser objeto de prova ou meio de prova, isto é, pode ser objeto de prova, e aí falamos em prova um fato eletrônico, ou pode ser um meio de prova, assim aludimos a provar eletronicamente um fato, ou pode, simultaneamente, se objeto e meio de prova quando se trata de provar eletronicamente um fato eletrônico[[88]](#footnote-88).

Também pode-se definir prova digital “como qualquer tipo de informação, com valor probatório, armazenada em repositório electrónico-digital de armazenamento ou transmitida em sistemas e redes informáticas ou redes de comunicações electrónicas, privadas ou publicamente acessíveis, sob a forma binária ou digital”[[89]](#footnote-89).

O orientador na presente dissertação, Armando Dias Ramos propõe uma definição de prova digital, em consideração ao fato de que o legislador português não positivou a sua definição na Lei 109/2009, a conceitua como toda e qualquer “informação passível de ser obtida ou extraída de um dispositivo eletrónico (local, virtual ou remoto) ou de uma rede de comunicações, razão pela qual esta prova digital, para além de ser admissível, deve ser também autêntica, precisa e concreta”[[90]](#footnote-90).

Eoghan Casey sustenta que a prova digital “é um tipo de evidência, cujo conteúdo se encontra em algum dispositivo construído de campos eletrônicos, magnéticos e pulso eletrônicos, os quais pondem ser extraídos, coletados e analizados por um conjunto de especialistas chamados de peritos, quem com instrumentos tecnológicos especiais podem converter-la em prova científica”[[91]](#footnote-91).

Ocorre que a prova digital ainda não possui a sua autonomia, carecendo da analogia ou da interpretação extensiva de normas e regulamentos atinentes à outras espécies probatórias.

Em que pese não haver nenhuma legislação conferindo à prova digital uma certa autonomia, há, entretanto, normatização referente às regras de conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrônicas no direito português, como por exemplo as regras previstas na Lei n.º 32/2008, de 17 de julho, e as regras processuais existentes na Lei do Cibercrime (Lei n.º 109/2009, de 15 de Setembro), mas, a verdade é que estas leis não criaram uma sistemática própria, autônoma da prova digital.

Portanto, é possível verificar que a especificidade da prova digital consiste em como é arquivada a informação e bem como em suas características respectivas. Essas peculiaridades conduz a procedimentos e cautelas especiais na produção e obtenção dessa prova, o que estabelece efeito de sua caracterização.

Cumprido o mister de apresentar os múltiplos conceitos de provas digitais, se faz necessário, agora, analisar as suas principais características.

# 4. Características da Prova Digital

A sociedade como um todo é testemunha diária do lado positivo das novas tecnologias de informação e comunicação. No entanto, não se pode olhar para o outro lado quando diariamente também fica evidente a face negativa das mesmas, pois são protagonistas em novos tipos infrações penais que até pouco tempo eram inexistentes.

Como visto anteriormente, estas novas formas de transgressão da lei são denominados de ciberdelitos, crime cibernéticos, ciberdeliquência, etc. Na maioria das ocasiões, para que os delitos cibernéticos possam ser investigados, é necessária uma prova distinta, que até pouco tempo não existia, qual seja, a prova digital.

E é neste ponto onde as diligências de investigação tecnológica assume um papel fundamental ao se apresentar como a principal fonte de obtenção das aludidas provas digitais.

Assim, se não houver gravação capturada por câmeras de vídeo, conversas gravadas eletronicamente e interceptada pelos agentes, histórico de páginas da *web* obtido por registro remoto de um computador, ou conversas do WhatsApp coletadas em um celular, muitas delas ilícitas, incontáveis infrações penais estariam sem apuração e isentas de punições.

Dito isto e já analisado o conceito de prova digital acima, se faz necessário o estudo de suas caractéristicas predominantes, iniciando com a constatação de que no dia 06 de março de 2020 o Conselho da Europa editou o Guia Eletrônico de Provas – Um guia básico para policiais, promotores e juízes.

Constata-se no aludido guia que “a prova digital está hoje presente na generalidade dos processos de natureza criminal. Encontra-se em computadores, *tablets, smartphones,* dispositivos de armazenamento USB, câmaras fotográficas e/ou de vídeo digitais, aparelhos periféricos, gravadores de áudio, sistemas de videovigilância, consolas de videojogos, servidores, *routers, access points*  ou em movimento por redes de comunicações electrónicas, entre outros locais”[[92]](#footnote-92).

Cada uma destas fontes de prova digital pode conter várias categorias de prova e, por força da sua especificidade, pode impor diferentes meios de recolha. Meios de recolha que, naturalmente, em nada são comparáveis com os utilizados para recolha de prova física[[93]](#footnote-93).

Em consequência, devido à sua natureza virtual a prova digital é indispensável a sua documentação que é feita através de dispositivos de armazenamento das informações que comprovam a sua existência e a origem dos fatos. No entanto, para que a prova digital seja admitida no processo judicial deve atender a três requisitos essenciais, quais sejam:

A Legalidade, no caso de obtenção de prova digital, deve ser dentro dos limites do respeito aos princípios constitucionais e dos direitos fundamentais, ou seja, o direito ao sigilo das comunicações, à privacidade pessoais, à inviolabilidade do domicílio, aos segredos financeiros entre outros. Em caso de violação de um dos direitos, será considerado como prova ilícita, ou seja, inconstitucional, portanto, sua exclusão do processo judicial será imediata.

A Integridade, devido à volatilidade das provas digitais para garantir a imutabilidade do meio digital, é importante que a evidência eletrônica seja submetida à perícia informática forense, para que um profissional especializado emite um laudo sobre a sua integridade para sua avaliação no processo judicial.

A Autenticidade, consiste em garantir que a amostra ou evidência sobre a qual se faz a pesquisa seja idêntica à amostra original, que é preservada e é guardada através da Cadeia de Custódia, garantindo que as provas digitais não sofram nenhuma modificação, manipulação ou alteração em sua recolha, transferência e/ou armazenamento.

Esta é a primeira etapa de acesso às fontes de provas eletrônicas ou digitais; ou seja, obter a prova digital pelas partes no processo ou pela autoridade judiciária no processo penal, refere-se ao momento anterior ao fornecimento da prova digital ao processar; isto é, o acesso às informações dos fatos armazenados em um dispositivo eletrônico, ou em qualquer caso transmitido por meio de mensagens eletronicamente, seja por meio de redes, via internet, site, redes sociais, WhatsApp, informações em nuvem disco rígido, USB, CD, DVD, pen drive ou outro. Ou seja, é a comprovação das evidências que existiam nas fontes de prova.

Benjamim Silva Rodrigues reconhece as seguintes características da prova digital: (i) efemeridade, temporalidade, precariedade e não durabilidade; (ii) fragilidade e fácil alterabilidade; (iii) volatilidade ou instabilidade, diante da possibilidade de desaparecimento e alteração; (iv) aparente imaterialidade ou invisibilidade; (v) complexidade ou codificação, pela necessidade de “uso/conhecimento de palavras-chave ou técnicas de desencriptação”; (vi) dispersão, disseminação ou pulverização; (vii) dinamismo e mutabilidade[[94]](#footnote-94).

Por sua vez, Denise Provasi Vaz descreve quatro características da prova digital, quais sejam “(i) imaterialidade e desprendimento do suporte físico originário; (ii) volatilidade; (iii) suscetibilidade de clonagem; e (iv) necessidade de intermediação de equipamento para ser acessada”[[95]](#footnote-95).

No aspecto imaterial, a prova digital possui a natureza impalpável, haja vista a impossibilidade de vê-los, os dados informáticos consistem em impulsos elétricos[[96]](#footnote-96). Diante de tal característica, possibilita-se aos sistemas informáticos o arquivamento de gigantesca quantidade de informações, haja vista que os dados não ocupam ambiente físico relevante. E, essa circunstância possibilita acúmulos de informações e de dados, em capacidade extremamente superior aos documentos tradicionais.

Em relação à volatilidade, as provas digitais se mostram frágeis no sentido de que estão propensas às variações e dissipação com facilidade. E, com isso é possível perder as informações ou dados armazenados digitalmente e, assim, haver modificações ou alterações que possam prejudicar a sua credibilidade ou confiabilidade[[97]](#footnote-97).

O fato de não ser possível afirmar se somente uma pessoa é que teve acesso ao *login –* palavra-chave, com certeza é uma das fragilidades da prova digital, haja vista que no Direito Penal hipóteses e ilações não são suficientes para responsabilizar o acusado.

Atinente à característica de suscetibilidade de clonagem, a prova digital por ser imaterial, os dados informáticos possibilitam a sua cópia a outros dispositivos eletrônicos, em sua completude.

Por fim, em relação à característica de intermediação de equipamentos eletrônicos para o acesso à prova digital, tem-se a necessidade de utilização de um dispositivo eletrônico para que se possa processar e acessar as informações e disponibiliza-la de maneira compreensível pelo o homem[[98]](#footnote-98).

David Silva Ramalho também nos apresenta como características da prova digital a imaterialidade ou invisibilidade e fragilidade e volatilidade. Segundo este autor português, a característica de imaterialidade da prova digital “apesar de precisar de estar incorporada num suporte material, é, no essencial, composta por sua sequência de *bits,* e existe independentemente do tipo de suporte físico no qual é incorporada. A prova digital precisa de um transportador, mas não se resume a ele”[[99]](#footnote-99).

Atinente à característica de fragilidade e volatilidade da prova digital, David Silva Ramalho ainda assevera que “a prova digital resulta na necessidade de uma resposta célere e tecnicamente qualificada, não só, como se referiu, para preservação da cadeia de custódia, mas também para tornar possível o acesso a dados de outro modo dificilmente acessíveis, como sejam dados cifrados ou dados, em geral, invisíveis ao utilizador comum”[[100]](#footnote-100).

Dario José Kist ao disciplinar sobre as características da prova digital, além daquelas que foram levadas a efeito por David Silva Ramalho, acrescenta a dispersão como atributo das provas digitais.

Para o autor brasileiro, a dispersão da prova digital consiste na situação em que a prova de determinado fato pode estar localizada em “vários locais diferentes próprio sistema informático, ou que os dados que compõem a prova digital podem estar situados em diferentes locais geográficos, o que é determinado pelo fato de os fornecedores de serviços, terem suas sedes dispersas pelo globo terrestre”[[101]](#footnote-101).

Analisadas as caraterísticas e requisitos essenciais da prova digital, o próximo passo é o estudo das fases de sua obtenção.

# 5. Da recolha da Prova Digital

Os dados obtidos por uma das partes litigantes são enquadrados em três possibilidades: primeira, os dados ou evidências digitais são encontrados armazenados no mesmo dispositivo eletrônico do interessado (acusado).

Nesta fase, para acessar o conteúdo do sistema ou equipamento de *hardware*, é necessário deter a posse física do material, ou seja, o infrator ou o Ministério Público deve receber o dispositivo eletrônico que contém as informações e dados provenientes da infração penal. Ter o dispositivo e o conteúdo das informações é poder garantir a integridade da prova digital.

Neste caso, a dificuldade está na forma de incorporar a prova ao processo judicial, especialmente o credenciamento da sua autenticidade e integridade são as dificuldades mais destacadas, uma vez que a parte lesada não tem este meio de prova.

Como segunda possibilidade, a prova digital encontrada arquivada em um dispositivo eletrônico de terceiros. Nesta situação, as informações ou provas podem ser fornecidas por decisão do magistrado que poderá determinar o seu depósito em juízo.

E, no terceiro caso, o acesso às informações pode ter sido obtido em violação aos direitos constitucionais, e, se assim fosse, tal recolhe seria inconstitucional, por violar os limites e princípios constitucionais, o que enseja a exclusão da prova digital ilícita.

Diante de tais constatações, é imperioso mencionar a lição proferida por David Silva Ramalho quando afirma que “não existe consenso sobre a metodologia a adoptar no processo de recolha, preservação e apresentação de prova digital. Os vários autores que se pronunciam sobre a importância de um modelo de ciência forense digital uniforme e alargado (...), tendem a apresentar modelos distintos, com diferentes etapas, procedimentos e sequências”[[102]](#footnote-102).

Dario José Kist, no mesmo sentido, assevera que “não há uniformidade, também, sobre as etapas, os procedimentos e a sequência ideal ou adequada para a recolha, preservação e apresentação da prova digital. Não obstante, parece haver aceitação da premissa de que, como em qualquer investigação criminal, também relativamente à prova digital devem ser observadas fases subsequentes e progressivas, caa uma destinada a finalidades específicas”[[103]](#footnote-103).

Entretanto, em que pese a ausência de consenso sobre as estapas de recolha da prova digital, o Instituto Nacional de Padrões e Tecnologias[[104]](#footnote-104) (*National Institute for Standards an Technology –* NIST) apresenta quatro fase ou etapas na investigação em ambiente digital, quais sejam: a recolha *(collection),* o exame *(examination),* a análise *(analysis)* e o relatório *(reporting).*

A recolha é a etapa inicial do procedimento apresentado pelo NIST, consistente em atos de identificação das evidências digitais, a sua recolha propriamente dita, sua rotulagem e seu registro, bem como demais atos destinados a garantir a integridade dos dados.

Estes atos poderão revistir-se de variadas formas, tendo em conta as variáveis, ou seja, a categoria de dados a recolher e o grau de urgência na recolha; tratando-se de dados dinâmicos, em trânsito por conta de ligações ativas, em que o risco de perda é muito maior do que em relação aos dados estáticos, o procedimento poderá se simplificado, assim como nos casos em que se detecta a iminente perda da fonte do sistema informático[[105]](#footnote-105).

A segunda etapa de recolha da prova digital é o exame que consiste no processamento das informações coletadas na fase anterior, cujo escopo é retirar, do conjuto de informações e dados que estão em posse do perito forense, aqueles que possuem importância para trâmite probatório.

Após a coleta de dados, a próxima fase é examinar os dados e informações, que de acordo com o Guia para a Integração de Técnicas Forenses na Resposta à Incidentes, o exame consiste no processamento forense de dados recolhidos utilizando um conjunto de métodos manuais e automatizados, incluindo ferramentas forenses e técnicas adequadas à tipologia de dados visados, avaliando e extraindo informações relevantes a partir dos dados recolhidos, assegurando sempre, porém, a sua integridade[[106]](#footnote-106).

Esta fase também pode contornar ou mitigar os recursos do sistema operacional ou do aplicativo que obscurecem dados e códigos, como compactação de dados, criptografia e mecanismos de controle de acesso.

Um disco rígido adquirido pode conter centenas de milhares de arquivos de dados; identificar os arquivos de dados que contêm informações de interesse, incluindo informações ocultada por meio de compactação de arquivos e controle de acesso, pode ser uma tarefa assustadora[[107]](#footnote-107).

Uma vez extraída a informação relevante do dispositivo eletrônico, o perito digital deve estudar e analisar os dados para extrair conclusões deles. A base da perícia é usar uma abordagem metódica para alcançar conclusões embasadas nos dados disponíveis ou determinar que nenhuma conclusão ainda pode ser extraída.

A análise deve incluir a identificação de pessoas, lugares, itens e eventos, e determinar como esses elementos são relacionados para que se possa chegar a uma conclusão. Muitas vezes, esse esforço incluirá dados correlacionados entre várias fontes[[108]](#footnote-108).

David Silva Ramalho assevera que o “processo de análise pressupoe a interpretação dos elementos objectivos disponíveis e o seu confronto com a tese da acusação e, quando aplicável, com a tese do arguido. A partir da conjugação de informação jacente em ambiente digital, extrapolar-se-á uma conduta materialmente ocorrida no mundo físico”[[109]](#footnote-109).

A fase final é o relatório, que é o processo de preparação e apresentação das informações resultantes da fase de análise. O modelo proposto pelo NIST consiste na confecção de um relatório, onde os peritos ou analistas expõem as conclusões advindas do estudo das informarções e dados informáticos coletados nas fases anteriores.

Ainda de acordo com o modelo de ciência forense digital apresentado pelo NIST, há muitos fatores que afetam os relatórios, incluindo os seguintes: Exposição de explicações alternativas; Consideração dos interessados e Informações obtidas.

Em relação à exposição de explicações alternativas, tem-se que quando a informação relativa a um evento estiver incompleta, pode não ser possível chegar a uma explicação definitiva do que aconteceu.

Quando um evento tem duas ou mais explicações plausíveis, cada uma deve receber a devida consideração no processo de relatório. Os analistas devem usar uma abordagem metódica para tentar provar ou refutar cada explicação possível que se propõe[[110]](#footnote-110).

Conhecer o público para o qual os dados ou informações serão mostrados é importante. Um incidente que exige o envolvimento da aplicação da lei requer relatórios altamente detalhados de todas as informações coletadas, podendo também exigir cópias de todos os dados probatórios obtidos[[111]](#footnote-111).

O relatório também inclui a identificação de informações acionáveis ​​obtidas a partir de dados que podem permitir que um analista colete novas fontes de informação.

Como visto acima, um cuidado principal que deve nortear as etapas referidas é garantir meios e instrumentos para revelar a conservação da cadeia de custódia, preferivelmente por meio de confecção de procedimentos ou de pequenos relatórios de cada etapa.

Para Dario José Kist “o relatório destina-se à exposição das conclusões que o analista alcançou na manipulação das evidências digitais acerca das hipóteses de investigação”[[112]](#footnote-112).

David Silva Ramalho também manifesta sobre o relatório emitido na recolha de prova afirmando que “uma vez concluída a investigação, deverá ser elaborado um relatório final no qual conste uma explicação dos procedimentos adoptado, dos dados relevantes e da valoração que dos mesmos é feita. O grau de densificação e detalhe do relatório será inversamente proporcional ao nível de especificação e âmbito de abrangência da informação constante dos autos, designadamente em outros relatórios, e, quando o haja, o relatório pericial”[[113]](#footnote-113).

Analisada a recolha da prova digital, em sequência, apresenta-se com uma análise sucinta, os principais meios de obtenção da prova digital oferecidos pela Convenção de Budapeste sobre a Cibercriminalidade.

# 6. Da Obtenção da Prova Digital

Como já mencionado alhures, o Brasil não é signatário[[114]](#footnote-114) da Convenção de Budapeste sobre o Cibercrime, em que pese ela influenciar a doutrina nacional sobre os pontos atinentes à cibercriminalidade. Assim, como o ordenamento jurídico brasileiro não possui norma específicas atinentes à obtenção da prova digital, faz-se necessário o uso da anologia para a fase probatória.

No âmbito internacional, tem-se a Convenção sobre a Cibercriminalidade do Conselho da Europa que fora firmada na cidade Budapeste, em 23 de novembro de 2001, onde em seu artigo 16 dispõe que os “Estados signatários adotem as medidas legislativas e outras que se revelem necessárias para permitir à suas autoridades competentes exigir ou obter de uma outra forma a conservação expedita de dados informáticos específicos, incluindo dados relativos ao tráfego, armazenados por meio de um sistema informático, nomeadamente nos casos em que existem motivos para pensar que os mesmos sao suscetíveis de perta ou alteração”[[115]](#footnote-115).

Diante de tal cenário legislativo, Portugal, em 15 de setembro de 2009 ratificou a Convenção sobre o cibercrime, através do Decreto do Presidente da República de n.º 91/2009 e em seguida promulgou a Lei n.º 109/2009, de 15 de setembro.

Sendo assim, hodiernamente em Portugal, a prova digital e sua obtenção está regulada em três diplomas legais diferentes: a Lei nº 32/2008, de 17 de julho, que dispõe sobre a conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrônicas; a Lei nº 109/2009, de 15 de setembro que prevê disposições processuais aplicáveis a crimes informáticos, crimes cometidos por meio de um sistema informático e, quaisquer crimes em relação aos quais seja necessário proceder à recolha de prova em suporte eletrônico; e o Código de Processo Penal (artigos 171º a 190º) .

Atento ao tema ora proposto, a Convenção sobre a Cibercriminalidade apresenta os principais meios de obtenção da prova digital, quais sejam: (art. 16) o uso de meios para a preservação expedita de dados; (art.17) a conservação e revelação expedita de dados informáticos; (art.18) a injunção sobre terceiros para a apresentação de dados ou concessão de acesso; (art.19) a pesquisa e a apreensão de dados informáticos; (art.20) a interceptação em tempo real de dados informáticos e, (art.21) as ações encorbertas em meio digital.

A lei portuguesa n.º 109/2009, de 15 de setembro, também trás um catálogo de meios de obteção de provas digitais: (art. 12.º) Preservação expedita de dados; (art. 13º) Revelação expedita de dados de tráfego; (art. 14º) Injunção para apresentação ou concessão do acesso a dados; (art. 15º) Pesquisa de dados informáticos; (art.16º) Apreensão de dados informáticos; (art. 17º) Apreensão de correio electrônico e registos de comunicações de natureza semelhante; (art. 18º) Intercepção de comunicações; (art. 19º) Acções encobertas.

Para não extrapolar o objetivo da presente dissertação, os aludidos meios de obtenção de prova digital serão vistos em seus aspectos legais e conceituais.

Assim, atinente à preservação expedita de dados, tem-se que a mesma se identifica como uma determinação de conservação das provas, encaminhada a quem tenha o controle ou a disponibilidade das informações ou dos dados informáticos arquivados ou armazenados em sistema operacional, para que os conserve até uma segunda ordem das autoridades.

De acordo com o Relatório Explicativo da Convenção[[116]](#footnote-116), mais especificamente nos itens 158[[117]](#footnote-117) e adiantes, verifica-se que a palavra ‘preservação’ significa que os dados, existentes e arquivados, sejam conservados e protegidos de tudo que possa ocasionar a deterioração ou alteração de sua qualidade ou de seu estado, devendo-se mantê-los protegidos de qualquer forma de modificação, exclusão ou danos.

Consta ainda deste mesmo relatório que o artigo 16º da Convenção de Budapeste não especifica a forma segundo a qual os dados deverão ser preservados, pelo que caberá a cada Parte estipular a forma mais adequada de preservação e, nalguns casos particulares, determianr se a preservação dos dados deverá ou nao implicar o seu “congelamento”[[118]](#footnote-118).

Observa-se, entretanto, que a citada medida de obtenção de prova digital consiste em meio de relevante valor quando há razões para acreditar que as informações ou dados informáticos são frágeis e passíveis de intervenção de terceiros, tais como o próprio acusado, servindo-se para a sua preservação.

Em Portugal, o dispositivo legal que prevê a preservação expedita de dados é o artigo 12º, da Lei 109/2009, a Lei do Cibercrime[[119]](#footnote-119).

De acordo com Dario José Kist, a medida de preservação expedita de dados “tem a natureza instrumental para outra medida posterior, que é o acesso, conhecimento e utilização de dados informáticos como prova em processo penal. Seu objetivo, é preservar dados que, de acordo com as autoridades que estão investigando determinado fato, possam ser necessários para a “descoberta da verdade” e que se suspeita possam ser alterados ou destruídos”[[120]](#footnote-120).

No mesmo trilho, Duarte Rodrigues Nunes assevera que “a preservação nao se confunde com o arquivamento dos dados, compreendido este como o processo de guardar e manter na sua posse, para o futuro, dos dados que estão sendo produzidos; a medida de preservação de dados, ora em análise, refere-se apenas àqueles que já existem por haverem sido recolhidos pelo detentor, e nao abrange a obtenção de dados em tempo real e, muito menos, o acesso ao conteúdo das comunicações”[[121]](#footnote-121).

Em relação à preservação e à revelação expedita de dados de tráfego, o artigo 17º[[122]](#footnote-122) da Convenção de Budapeste dispõe que cabe a cada Estado adotarem medidas legais aos forncedores de serviços que tenham participado na transmissão da comunicação, a divulgação destes dados à autoridade competente.

Importante ressaltar que o item 133[[123]](#footnote-123) do Relatório Explicativo da Convenção de Budapeste após demonstrar que o artigo 17º prevê obrigações relativamente à preservação de dados de tráfego e a sua expedita divulgação, informa que um dos maiores desafios que se tem no combate à cibercriminalidade é a dificuldade de identificação do infrator.

Essa medida de obtenção de prova digital, em Portugal, restou prevista no artigo 13º[[124]](#footnote-124) da Lei 109/2009 – Lei do Cibercrime, com a nomeclatura “revelação expedita de dados de tráfego”.

Verifica-se que esse meio de obtenção de prova detém o objetivo de identificar todos os fornecedores de serviço usado na transmissão, pois é por esse meio que se pode conseguir as informações e dados informáticos produzidos durante todo o percurso da comunicação.

Um outro meio de obtenção de prova digital é a chamada injunção para apresentação ou concessão do acesso a dados. No artigo 18[[125]](#footnote-125) da Convenção de Budapeste tem-se a autorização aos Estados para adotarem medidas legislativas para permitir que as autoridades ordenem a apresentação ou permita o seu acesso às informações ou aos dados informáticos que estejam na posse ou no controle de terceiros.

A Lei do Cibercrime – Lei n.º 109/2009 – dispõe sobre a injunção para apresentação ou concessão de acesso a dados no seu artigo 14º[[126]](#footnote-126).

Diante dos elementos apresentados nos dispositivos legais acima referenciados, é possível afirmar que a injunção para apresentação ou concessão do acesso a dados consiste em uma determinação da autoridade encaminhada a quem tenha o controle ou a disponibilidade de dados informáticos ou informação específicos arquivados em dispositivo eletrônico, para que os informe às autoridades investigativas ou para que permita o seu acesso ao sistema eletrônico onde se encontram.

Um outro meio de obtenção de provas digitais é a busca e apreensão de dados informáticos armazenados. Está previsto no artigo 19º[[127]](#footnote-127) da Convenção de Budapeste, e trata-se de uma importante medida de natureza instrumental, a qual habilita as autoridades competentes a procederem à buscas ou apreensões de sistemas informáticos ou a outro suporte que permita o armazenamento dos dados informáticos.

Consoante o item 184 e seguintes do Relatório Explicativo da Convenção de Budapeste, o citado dispositivo legal visa a modernização e a harmonização das legislações nacionais relativamente à busca e apreensão de dados informatizados armazenados, para fins de obtenção de provas relacionadas com investigações criminais ou ações penais específicas e tem por objetivo estabelecer um poder equivalente relativo aos dados armazenados[[128]](#footnote-128).

Por sua vez, Portugal orientou-se normativamente sobre esse meio de obtenção de prova com a presença de três artigos na Lei de Cibercrimes, quais sejam: o artigo 15º, cuja nomeclaratura constante é “pesquisa de dados informáticos”; artigo 16º que trata da “apreensão de dados informáticos”; e o artigo 17º que cuida da “apreensão de correio electrónico e registos de comunicações de natureza semelhante”.

Ao analisar o artigo 15º da Lei de Cibercrimes, Armando Dias Ramos preceitua que “a razão de ser deste artigo prende-se com o facto de, por vezes, ser impossível apreender um sistema informático na sua totalidade para o sujeitar a exame pericial. Não só pela sua dimensão, tanto em tamanho físico como em termos de alocação de espaço digital, mas, na maioria das vezes, porque a sua apreensão poderia causar danos irreparáveis, fazendo, por exemplo, que outros sistemas informáticos, dependente deste, deixem de funcionar”[[129]](#footnote-129).

Também, ao comentar os citados dispositivos legais, Manuel Monteiro Guedes Valente assevera que “as polícias criminais detém instrumentos jurídicos suficientes para procederem à aquisição, conservação e tratamento da prova obtida no meio digital. Sendo que atuam sob a égide das designadas medidas cautelares e de polícia, extraordinárias, urgentes e *periculum in mora*, cabendo-lhes comunicar de imediato a sua atividade às autoridades judiciárias: Ministério Público e Juiz das Liberdades. O mesmo se passe no quadro das apreensões digitais, como decorre do artigo 16º da Lei do Cibercrime, com exceção de apreensões que tenham ou visam como foco a atividade ilícita de advocacia, médica, bancária e jornalística ou conflitem com estas atividades”[[130]](#footnote-130).

Verifica-se que este meio de obtenção de prova digital na Convenção de Budapeste sobre a Cibercriminalidade foi tratado em apenas um dispositivo legal, enquanto que na Lei de Cibercrime de Portugal teve seu tratamento separado em três artigos.

A interceptação em tempo real de dados informáticos é um outro meio de obtenção de prova digital prevista tanto na Convenção de Budapeste sobre a Cibercriminalidade e na Lei 109/2009 – Lei do Cibercrime, em Portugal.

Os artigos 20[[131]](#footnote-131) e 21[[132]](#footnote-132) da Convenção de Budapeste se dedicam a este meio de obtenção de provas digitais. Por sua vez, o Relatório Explicativo da aludida Convenção, nos itens 205 a 215, em suma, constam que as disposições contidas nos artigos 20 e 21 da Convenção de Budapeste tratam da questão sobre a recolha e a interceptação em tempo real, de dados informáticos por parte das autoridades competentes, bem como de recolha e interceptação de dados pelos fornecedores de serviços.

Por seu turno, Portugal trata essa matéria na Lei 109/2009, de 15 de setembro de 2009, sobre a rubrica “intercepção de comunicações” em seu artigo 18º[[133]](#footnote-133).

Finalmente, a obtenção de meios de provas digitais com recurso de ações encobertas no meio digital, impende ressaltar que a Convenção de Budapeste sobre a Cibercriminalidade não faz referência sobre tal mecanismo. Apesar disso, diversos países europeus introduziram em seu ordenamento jurídico a possibilidade de utilizar tal instrumento na recolha da prova digital.

Em Portugal, as ações encobertas encontram-se previstas no artigo 19º da Lei 109/2009, donde é possível vislumbrar que o legislador expandiu tais procedimentos à Cibercriminalidade, através das ações já dispostas na Lei n.º 101/2001, de 25 de agosto, que preve o chamado regime jurídico das ações encobertas.

Ao analisar este meio de obtenção de provas digitais, Armando Dias Ramos assinala que o legilador portugues não elaborou norma específica para esta modalidade nova de apuração de crimes, e muito menos regulamentou os meios técnicos a utilizar, direcionando apenas esse dispositivo legal ao regime jurídico das ações encobertas[[134]](#footnote-134).

Diante de tudo que foi exposto acima, é possível afirmar que não há um regime jurídico próprio e autônomo atinente à prova digital, isto é, quando o magistrado analisa o meio probatório que fora coletado no âmbito digital, cujo objetivo é a busca da verdade material, o julgador aplicará os dispositivos legais constantes do Código de Processo Penal, local em que há diversos meios de obtenção de provas.

Entretanto, refutando a necessidade de um regime processual penal próprio, autônomo e eficiente para a obtenção da prova digital, Renato Lopes Militão assevera que “as ‘medidas tradicionais’, nomeadamente o regime processual penal geral referente à obtenção de prova, são suficientes também em relação à prova digital. Sem prejuízo, naturalmente, de carecerem de algumas adaptações, que respondam a certas especificidades desta prova. Deste modo, atrevemo-nos a prever que um regime autónomo e eficientista no domínio da prova digital nem sequer irá conduzir a resultados particularmente significativos. A menos que, como adiante hipotisaremos, entretanto se degradem também os critérios do julgamento da matéria de facto”[[135]](#footnote-135).

Analisados os meios de obtenção de prova digital previstos na Convenção de Budapeste sobre a Cibercriminalidade e na Lei n.º 109/2009, de 15 de setembro de 2009, resta-nos a reafirmar que o Brasil não é ainda signatário da citada Convenção, contudo, impende mencionar que há no ordenamento jurídico brasileiro fundamentos para a utilização de algum dos meios de obtenção de prova digital acima visto.

É possível afirmar que além das previsões constantes no Código de Processo Penal, há ao menos outros três diplomas legais específicos que possibilitam o manejo de alguns desses meios de obtenção de prova digital, quais sejam: a Lei n.º 9.296/96, que dispõe sobre a interceptação telefônica e telemática; a Lei n.º 12.965/14, denominada de Marco Civil da Internet; e a Lei n.º 13.441/17, que modificou o Estatuto da Criança e do Adolescente – Lei n.º 8.069/90.

No próximo tópico da presente dissertação, serão vistas os empencilhos apresentados na utilização da prova digital.

# 7. As vantagens e os inconvenientes da prova digital

O direito penal contemporâneo, apesar de aceitar e preservar em grande medida as diretrizes substanciais clássicas e a filosofia jurídica que o orientam, é, por um lado, necessário atualizar o rol de infrações penais e de penas, como estratégia de política criminal diante das novas formas, métodos e espaços criminais originados das novas tecnologias de informação e comuncicação.

Por outro lado, está amplamente comprometido o processo como cenário para a articulação dos institutos jurídicos, para atuar em meio às encruzilhadas que são geradas pela incidência processual das garantias de ordem convencional e constitucional, para modernizar e executar novas metodologias e instrumentos de pesquisa, especialmente nos tempos atuais em que o chamado cibercrime e outras fontes de desestabilização trazem consigo novos paradigmas ou desafios de justiça

Em razão do que foi analisado acima, é possível apontar quatro importantes vantagens advindas das provas digitais. A primeira é que, sempre e enquanto o material não for adulterado, essas provas oferecem informações mais objetivas, claras, precisas, completas e neutras do que outros meios provas, como depoimentos de testemunhas, que sempre podem ser contraditórias.

A segunda é que a revolução tecnológica trouxe consigo uma nova onda de atividades – lícitas e ilícitas - que são apoiadas nas novas tecnologias de informação e comunicação e que exigem provas digitais nos diferentes graus jurisdicionais como elemento-chave no desenvolvimento do processo.

A terceira vantagem da prova digital é que o seu tratamento processual é relativamente simples porque em quase todos os casos, os peritos forenses obtém facilmente as informações e por meio de laudos periciais é possível concluir sobre sua veracidade, mesmo existindo casos em que não será necessária a sua colaboração.

A quarta é que com o passar do tempo essas provas digitais acabaram levando a uma redução no custo total do processo, bem como simplificá-lo reduzindo os custos processuais de impressão de milhares de páginas e a burocracia dedicada à gestão e tramitação dos autos.

Essas vantagens acima apontadas, ajudará a reforçar os princípios da economia processual, da concentração e unidade de atos e da publicidade, dando lugar a processos mais céleres convertendo-se em uma justiça moderna, ágil e mais próxima do cidadão.

Entretanto, é imperioso também apontar os invonvenientes advindos da utilização da prova ditigal, que são de caráter legal e técnico. O principal obstáculo de natureza jurídica é que, apesar das boas intenções dos legisladores europeus e nacionais – Portugal e Brasil - não há regulamentação suficiente e isso traz insegurança jurídica em torno das provas digiais.

As desvantagens técnicas podem ser agrupadas em três. A primeira refere-se à realidade cotidiana dos tribunais, ou seja, a falta de meios aliada à exclusão digital nos profissionais do setor judiciário - o que seria resolvido com a oferta de treinamento especializado para profissionais para familiarizá-los com o novo ambiente digital[[136]](#footnote-136).

A segunda dificuldade na utilização da prova digital está na complexidade do assunto que implica a necessidade de recorrer a profissionais técnicos para a elaboração da prova pericial, devido à dificuldade técnica implícita de um material provas relacionadas com as tecnologias de informação e comunicação, e que o juiz, regra geral, não tem – complexidade que também ocorre em outros casos em que o juiz precisa da ajuda de profissionais de outras áreas (médicos, engenheiros, arquitetos...)-.

O último inconveniente, e que se torna o ‘calcanhar de aquiles’ da prova digital é a sua volatilidade ou facilidade em sua manipulação.

Assim, as características específicas da prova digital, em particular, o fato de ser alterável, frágil, volátil, imateral, tranformam-na em prova complexa tecinicamente e ausente de estudos especializados.

Benjamim Silva Rodrigues assevera que a prova digital é “fragmentária, dispersa, frágil, volátil, alterável, instável, apagável e manipulável, invi´sivel e espacialmente dispersa. Sendo, por isso, extremamente difícil, complexo e, até, aleatório detectar, preservar, apreender, analisar, garantir a fiabilidade, assegurar a compreensibilidade e apresentar em julgamento as provas digitais”[[137]](#footnote-137).

# 8. A autenticidade da prova digital

O que muitas vezes é esquecido como resultado desta crescente conveniência com a prova digital é que os documentos eletrônicos no sentido mais estrito e outras informações armazenadas na mídia eletrônica são não apenas ideologicamente, mas também materialmente vulneráveis.

Uma sequência de dados armazenados em um meio eletrônico pode ser alterada se o meio contiver uma nova gravação ou o a informação é transportada para outro meio, que pode ser difícil ou mesmo impossível de reconhecer devido a características especiais do utilizador “não há bits falsos. Isto equivale a afirmar que, enquanto no mundo físico, a materialidade do meio em que se propagam as mensagens permite uma série de mecanismos de verificação de sua autenticidade (exame grafotécnico, análise da tinta, do papel em que impressa a mensagem, como papel-moeda, marca d’água, etc.), no meio virtual isto é impossível”[[138]](#footnote-138).

Imagens na tela de um computador ou telefone celular podem ser criadas sem nenhum conhecimento especial em programas de edição de imagens ou mesmo em sites que permitem visualmente a criação de uma reprodução totalmente nova. São numerosos aplicativos na internet e podem ser facilmente encontrados em qualquer mecanismo de pesquisa.

Os regulamentos legais não são de forma alguma exaustivos e devem ser conciliados na jurisdição penal com a necessidade de uma investigação pericial dos fatos do caso, mas mostra que para a atribuição de valor probatório a documentos eletrônicos e outras informações extraído da mídia digital, “é fundamental avaliar o grau de segurança e de certeza que se pode ter, sobretudo quanto à sua autenticidade, que permite identificar a sua autoria, e à sua integridade, que permite garantir a inalterabilidade do seu conteúdo”[[139]](#footnote-139).

A autenticidade e integridade estão previstos na legislação brasileira, no Código de Processo Civil (Lei nº 13.105, de 16 de março de 2015) nos artigos 193 e seguintes, para os registros dos atos processuais eletrônicos, podendo ser utilizada a analogia a todos os registros eletrônicos que se pretendem usar com valor probatório no processo.

No entanto, se a informação for gerada exclusivamente de forma eletronica, por exeemplo preenchendo um formulário digital, que se vincula ao seu autor, como é o caso da contabilidade eletrônica de transações financeiras, ou mesmo automaticamente por sistemas assistidos por computador, para gravação ou como resultado de seu uso - de chamadas telefônicas, troca de mensagens, acesso a aplicativos da internet para dados de localização recebidos por dispositivos móveis usados ​​para acesso, etc. - não há nenhuma outra evidência e as informações devem ser retiradas do banco de dados digital.

Em tal situação, podem existir dúvidas sobre a precisão das informações contidas no banco de dados, e dessa forma é necessário o operador responsável pela base de dados esclarecer sobre a operação e consequentemente sobre o seu funcionamento; e portanto quanto ao valor dos dados obtidos.

No entanto, por vezes são juntadas na investigação criminal, imagens da tela do computador documentos ou mesmo reprodução de má qualidade sem qualquer esclarecimento acerca da criação e armazenamento dos dados, sobre o tipo de acesso à base de dados ainda responsável por esta atividade.

Desta forma, o valor probatório do banco de dados digitais se deteriora completamente, uma vez que não pode ser garantido que a informação tem fonte confiável, nem que o que é reproduzido nos registros corresponde ao que aparece na origem (autenticidade) e não foi alterado desde extração (integridade).

# 9. Valoração da prova digital

A tecnologia incorporada aos aspectos da vida vem modificando profundamente as interações sociais, reformulando a comunicação, substituindo-se o papel amplamente pelos sistemas de informática; não sendo mais necessário o contato presencial, transmitindo-se um volume imenso de informação, com a celebração de negócios jurídicos e também atos ilícitos.

Devido ao uso diário da internet e outros meios de comunicação, um dos procedimentos investigativos quase indispensáveis ​​para a resolução dos crimes geralmente são o acesso às comunicações feitas pelo suposto autor dos crimes seja simplesmente por telefone, chamadas, sms ou dados de geolocalização, como eletrônico, páginas da web visitadas, e-mails, mensagens enviadas ou recebidos através de programas de computador ou aplicativos de mensagens, etc.

Os avanços tecnológicos representam desafios jurídicos significativos em termos de investigação e prova dos crimes executados através da rede, e em geral, de qualquer conduta ilícita que faça uso da evolução da ciência e tecnologia, seja para o cometimento do delito ou para evitar sua descoberta.

Os comportamentos criminosos mais perigosos enfrentados atualmente, como terrorismo, crime organizado, tráfico de drogas e armas, exploração sexual de menores e pornografia infantil, crime econômico e corrupção e, claro, o cibercrime; se adaptaram muito rapidamente às mudanças na ciência e tecnologia, em sua tentativa de explorar ilegalmente e difundir os valores e a prosperidade da sociedade.

É então que surgem dificuldades importantes na admissão de novas medidas tecnológicas de investigação e novas fórmulas de interferência no conteúdo das comunicações cibernéticas, restando, basicamente como solução para tanto a interceptação de comunicações telefônicas.

Contudo, tal medida limitativa dos direitos fundamentais e liberdades do investigado alude a requisitos essenciais para garantir a sua constitucionalidade e princialmente segurança jurídica.

O juiz competente deverá levar em consideração para a correta avaliação do prova digital a sua integridade e autenticidade, a posição processual que tiveram as partes, isto é, se foi contestado ou não e a avaliação conjunta de todas as provas do processo penal. É evidente que “a confiabilidade da prova documental – e a importância singular que os ordenamentos processuais lhe emprestam – assenta-se, exatamente, na estabilidade do suporte em que a informação é registrada”[[140]](#footnote-140).

Como é sabido um documento produzido em meio eletrônico pode, em regra, ser modificado facilmente, em meios de armazenamento aptos a realizar regravação. Na movimentação de dados na internet, a informação armazenada em meio eletrônico “assume caráter temporário, é fungível e de grande volatilidade”[[141]](#footnote-141) em visível incoerência com a natureza e a própria utilidade da prova documental.

Qualquer reprodução de um documento, seja no mesmo ou em outro suporte que corresponda ao transportado, pode ser idêntica e, portanto, indistinguível do original para fins de prova. Portanto, manter o original com atributos próprios pode ultrapassar a vida útil de um dispositivo de armazenamento e aumentar a estabilidade do documento. Por outro lado, a transferência para outro meio, como a materialização em papel, sempre transformará em uma cópia, com a restrição de que a reprodução, devido à possível necessidade de confrontar o original, esteja no meio em que se encontra produzido.

Historicamente, a estabilidade que os documentos fornecem como evidências pré-constituídas e que podem preservar a memória de atos e acontecimentos sem inclinações subjetivas lhes valeram tratamento especial na legislação brasileira e estrangeira, que inclusive lhes conferiu pleno reconhecimento como os únicos idôneos para provar certos fatos, como determinava o art. 401 do Código de Processo Civil instituído pela Lei n.º 5.869, de 11 de janeiro de 1973.

Esta relevância única dos documentos explica o tratamento cuidadoso de sua produção e valoração jurídica, desde a prova documental, embora inerentemente mais segura em comparação com outras mídias, que se expõem ao erro, falsificação, perecimento e de uso indevido.

Em relação à valoração, a lei também teve o cuidado de esclarecer alguns termos intuitivos, que, na ausência de uma disposição normativa, poderiam ser facilmente derivadas de regras gerais, como, por exemplo, a declaração contida em documento o considerada verdadeiro apenas em relação ao signatário, ou para evitar o uso de documentos pré-datados para violar direitos, a data do documento específico não é aplicável a terceiros até que seja verificada por dados externos e objetivos - como a morte de um dos Assinantes ou a inscrição no cartório - a impossibilidade de outra data.

As premissas levantadas em relação às provas físicas não se desviam do que se deve buscar em relação às provas digitais. Se a adequada decomposição analítica dos documentos for assumida em seu aspecto intrínseco correspondente ao conteúdo e seu suporte material como manifestação concreta e sensível, pode-se afirmar que o desenvolvimento tecnológico sempre tende a favorecer o uso de novos suportes, sem, no entanto, desnaturar a essência ou registro um fato que caracteriza o conteúdo da prova e, portanto, requer o mesmo cuidado ao reconhecer sua eficácia.

No caso da prova digital, em função do avanço legislativo ocorrido desde os primeiros alertas sobre a obsolescência do direito processual frente à tecnologia, a renúncia ao esforço de interpretação necessário para o reconhecimento das informações armazenadas em meio eletrônico como provas e valoradas pelo seu conteúdo.

# CAPÍTULO III – INVESTIGAÇÃO CRIMINAL NA ERA DIGITAL

# 1. Introdução

O adjetivo comumente usado para designar o atual estágio em que vivemos é o da ‘sociedade da informação e do conhecimento’, vista como a sucessora da sociedade industrial ou pós-moderna e caracterizada pelo papel transcendental desempenhado pelas tecnologias de informação e comunicação nas atividades sociais, culturais e econômicas[[142]](#footnote-142).

Se somarmos a esse desenvolvimento tecnológico a redução de custos de fabricação e venda de todos os tipos de dispositivos eletrônicos, é fácil verificar a universalização do uso da tecnologia da informação por qualquer cidadão, em qualquer lugar do mundo e em todas as áreas de nossas vidas, o que deu origem a uma nova forma de relação entre humanos e máquinas através da coleta e troca de *bytes* para qualquer atividade “um novo comportamento baseado no ‘consumo tecnológico’ gerador de um verdadeiro ambiente digital do indivíduo, que seria composto por todas as informações em formato eletrônico que, voluntária ou involuntariamente, consciente ou inconscientemente, o homem gera com sua atividade, não importa onde os arquivos de computador que o contêm estejam localizados ou os canais de comunicação por onde passa”[[143]](#footnote-143).

Com tal transformação na sociedade e com o aumento dos canais de comunicação disponíveis, com a proliferação dos sistemas e dispositivos eletrônicos, unidos à velociade e à ausência de obstáculos ao anonimato na seara digital, acabaram por incentivar o desenvolvimento de novas condutas criminosas.

A ausência de obstáculos para a prática de crimes digitais é inversamente proporcional aos óbices encontrados pelos órgãos de persecução penal na investigação criminal, principalmente referente à identificação dos agentes envolvidos no fato criminoso.

 Eduardo Bolsoni Riboli argumenta que “os novos obstáculos apresentados à investigação pela criminalidade tecnologicamente engajada decorrem mais das tecnologias utilizadas pelos criminosos do que das novas práticas ilícitas – exclusiva ou maioritariamente em ambiente digital – criadas. São os novos dispositivos eletrônicos e sistemas informáticos assimilados pela criminalidade que obstaculizam a persecução penal, mas que também podem a facilitar”[[144]](#footnote-144).

Este mesmo autor assevera que os tradicionais meios de obtenção de prova são cada vez mais ineficazes e inadequados ao combate dos crimes digitais, exigindo-se aperfeiçoamento e assimilação de tecnologias de investigação pelo Estado no exercício do seu *ius puniendi*[[145]](#footnote-145).

Corroborando com o aludido acima, Manuel Monteiro Guedes Valente salientando o atual ‘quadro’ da justiça criminal, assinala que a “opção por meios de investigação ou meios de obtenção de prova com uma dinâmica tecnológica, digital ou intra-social, assentes numa lógica de celeridade incontrolável e de negação do tempo da norma, que é substituído pela norma do tempo, é uma caraterística da justiça dos nossos dias”[[146]](#footnote-146).

Assim diante da premente necessidade de suplantar as dificuldades e inadequações reveladas pelos convencionais meios de obtenção de provas, fez com que surgissem novos meios e instrumentos de investigação criminal adequados e hábeis ao combate dos crimes digitais, como os que serão analisados abaixo.

O adjetivo comumente usado para designar o atual estágio em que vivemos é o da ‘sociedade da informação e do conhecimento", vista como a sucessora da sociedade industrial ou pós-moderna e caracterizada pelo papel transcendental desempenhado pelas tecnologias de informação e comunicação nas atividades sociais, culturais e econômicas[[147]](#footnote-147).

Se somarmos a esse desenvolvimento tecnológico a redução de custos de fabricação e venda de todos os tipos de dispositivos eletrônicos, é fácil verificar a universalização do uso da tecnologia da informação por qualquer cidadão, em qualquer lugar do mundo e em todas as áreas de nossas vidas, o que deu origem a uma nova forma de relação entre humanos e máquinas através da coleta e troca de bytes para qualquer atividade: um novo comportamento baseado no “consumo tecnológico" gerador de um verdadeiro ambiente digital do indivíduo, que seria composto por todas as informações em formato eletrônico que, voluntária ou involuntariamente, consciente ou inconscientemente, o homem gera com sua atividade, não importa onde os arquivos de computador que o contêm estejam localizados ou os canais de comunicação por onde passa[[148]](#footnote-148).

Com tal transformação na sociedade e com o aumento dos canais de comunicação disponíveis, com a proliferação dos sistemas e dispositivos eletrônicos, unidos à velociade e à ausência de obstáculos ao anonimato na seara digital, acabaram por incentivar o desenvolvimento de novas condutas criminosas.

A ausência de obstáculos para a prática de crimes digitais é inversamente proporcional aos óbices encontrados pelos órgãos de persecução penal na investigação criminal, principalmente referente à identificação dos agentes envolvidos no fato criminoso.

 Eduardo Bolsoni Riboli argumenta que os “novos obstáculos apresentados à investigação pela criminalidade tecnologicamente engajada decorrem mais das tecnologias utilizadas pelos criminosos do que das novas práticas ilícitas – exclusiva ou maioritariamente em ambiente digital – criadas. São os novos dispositivos eletrônicos e sistemas informáticos assimilados pela criminalidade que obstaculizam a persecução penal, mas que também podem a facilitar”[[149]](#footnote-149)*.*

Este mesmo autor assevera que os tradicionais meios de obtenção de prova são cada vez mais ineficazes e inadequados ao combate dos crimes digitais, exigindo-se aperfeiçoamento e assimilação de tecnologias de investigação pelo Estado no exercício do seu *ius puniendi*[[150]](#footnote-150).

Corroborando com o aludido acima, Manuel Monteiro Guedes Valente salientando o atual ‘quadro’ da justiça criminal, assinala que a “opção por meios de investigação ou meios de obtenção de prova com uma dinâmica tecnológica, digital ou intra-social, assentes numa lógica de celeridade incontrolável e de negação do tempo da norma, que é substituído pela norma do tempo, é uma caraterística da justiça dos nossos dias”[[151]](#footnote-151).

Assim diante da premente necessidade de suplantar as dificuldades e inadequações reveladas pelos convencionais meios de obtenção de provas, fez com que surgissem novos meios e instrumentos de investigação criminal adequados e hábeis ao combate dos crimes digitais, como os que serão analisados abaixo.

# 2. Do uso da tecnologia na Investigação Criminal

Todas as investigações criminais têm como principal objetivo obter o máximo de informações possíveis sobre a prática de um fato criminoso (o que aconteceu, quem interveio, quando e onde ocorreu) assim, devido a essa presença massiva da *internet* na vida cotidiana, bem como o uso diário de múltiplos dispositivos eletrônicos, as autoridades responsáveis ​​pela investigação criminal mostraram um enorme interesse em poder acessar e analisar todas essas inumeras informações digitais e as utilizar para a investigação de todas as classes de crimes.

A importância de aumentar a capacidade das autoridades para usar qualquer medidas de pesquisa tecnológica destinadas a obter essas informações em um formato digital parece ser um pilar essencial em qualquer investigação criminal na atual sociedade informatizada.

De fato, a principal vantagem de usar estas novas medidas de investigação tecnológica reside na sua operacionalidade (transversalidade) para obter provas de qualquer tipo de crime, seja ou não dos chamados "crimes de informática", uma vez que são uma ferramenta eficaz na investigação de qualquer tipologia criminal em que tais dispositivos eletrônicos constituem uma valiosa fonte de evidência, devido às suas atuais capacidades de armazenamento de informações e seu uso para todos os tipos de comunicações.

A exemplo disso, imagina-se as células terroristas que se comunicam por meio de mensagens criptografada e postada em blogs; o assassino que carrega em sua agenda eletrônica uma lista de seus clientes ou de suas futuras vítimas; ou o chefe de um grupo criminoso que salva documentos eletrônicos sobre a contabilização de suas operações, datas e locais de recebimento e entrega de mercadorias e detalhes de contato de outras gangues criminosas.

Nenhum destes exemplos conduz à delitos cibernéticos propiamente ditos, entretanto, criam dados digitais e informações que configuram fatos puníveis.

Da mesma forma, a atual moda juvenil de gravar com um aparelho celular todos os tipos de delitos (condução de veículo de forma imprudente, assédio de colegas em sala de aula, espionar provadores femininos, etc.) e depois disponibiliza-los nas redes sociais, são a melhor amostra de como a obtenção dessas informações em formato ditigal podem ajudar, enormemente, os órgãos de investigação na resolução de delitos que não são em absoluto delitos digitais ou cibernéticos.

Assim, dada a alta taxa de criminalidade observada nos últimos anos, surgiu a necessidade de gerar conhecimento sobre o *modus operandi* dos criminosos e os vestígios deixados pela infração penal, em especial àqueles cometidos em ambiente digital.

Desde que os criminosos inventaram novas formas de cometer crimes, usando tecnologia e métodos muitos sofisticados que lhes permitem fugir à justiça, por isso, tornou-se essencial a utilização de métodos eficazes e eficientes que respondam às exigências da administração da justiça.

Portanto, os órgãos de persecução penal em apoio ao sistema judiciário tem implementado o uso de métodos tecnológicos modernos para facilitar e aprimorar a função que é desempenhada; conseguir o descongestionamento do trabalho nos órgãos judiciais e facilitar a coleta e registro de provas digitais.

Neste momento é importante mencionar a importância da investigação criminal levada a efeito pelo Manuel Monteiro Guedes Valente para quem “a investigação criminal tem como fim último a realização do direito nas prossecuções de defesa da sociedade, do colectivo, que tem o direito de viver em segurança e numa ordem social e internacional que lhe garanta a efectivação plena dos seus direitos e liberdades”[[152]](#footnote-152).

Diante das contatações da real necessidade de instrumentalizar os órgãos de investigação para o combate dos delitos cibernéticos, tem-se por oportuno a análise de algumas questões sobre os chamados métodos ocultos de investigação criminal em ambiente digital.

# 3. Dos métodos ocultos de Investigação Criminal:

Em razão da junção entre a evolução do crime organizado com o aumento de ameaças terroristas, a globalização bem como a disseminação de novas tecnologias, foram acontecimentos aptos ao desenvolvimento de crimes e à redução da possibilidade de descoberta dos mesmos.

Manuel Augusto Meireis assevera que “já não é o furto, o rapto isolado, ou mesmo o homicídio que preocupam as mais altas instancias com competência para definir modelos de prevenção e investigação criminal; para esta criminalidade, os métodos e as técnicas tradicionais, vao dando ainda resposta satisfatórias. De facto, o que hoje constitui o principal motivo as suas preocupações, sao as novas formas emergentes da criminalidade: os atentaos ao ambiente à escala planetátia; as grandes redes internacionais de tráfego de droga; de tráfego de armas, de tráfico de substâncias radioactivas, de tráfico de capitais. Mas são ainda, e também, os crimes de natureza económica e financeira e, sempre com eles coligadas, cifras negras; e o incontornável terrorismo”[[153]](#footnote-153).

De acordo com o pensamento de David Silva Ramalho, a preocupação com o aumento exponencial de crimes em âmbito digital traduz-se legítima e a situação de vigilância constante se faz necessário, entretanto a concepção do problema bem como as suas implicações são exarcebadas.

Ainda, segundo o autor português “independentemente do ocorre noutros ordenamentos jurídicos onde o referdio receio se afigura mais fundado, os métodos de investigação e de obtenção de prova até agora consagrados no ordenamento jurídico português, sem prejuízo das insuficiências e perplexidades de que padecem na sua regulação, quando devidamente aplicados nao permitem concluir pelo mérito desses alarmes”[[154]](#footnote-154).

Verifica-se, entretanto, que há um elo entre o processo penal e a infração criminal, isto é, a caracterização e aplicação prática do digesto processual está diretamente ligada à transformação e configuração do delito.

Deste modo, a excepcional gravidade das infrações penais e o aprimoramento do seu *modus operandi,* sendo inadequados os meios ou métodos convencionais para fazerem frente ao seu combate, ampara a adoção de métodos mais gravosos e aprimorados de investigação e de obtenção de provas.

A utilização destes meios de investigação criminal possui, em regra, como pressuposto a sua necessidade para sua efetividade ou eficácia da *persecutio criminis* em concreto somada à gravidade da infração penal.

Ou seja, não é suficiente que a perseguição criminal seja substancialmente difícil em razão dos métodos usados em sua prática, mas também é preciso que o grau de agressão do delito fundamente o uso dos meios mais gravosos.

Utilizando-se, mais uma vez dos ensinamentos de David Silva Ramalho, tem-se que o processo penal evolui para poer fazer face às novas realidades do crime, mas, quando essa evolução implique uma ingerência em direitos fundamentais, a mera adição dos correspondentes mecanismos processuais ao arsenal dos meios de investigação e obtenção de prova nao permite *per se* a sua utilização sem critérios[[155]](#footnote-155).

Diante do exposto, em razão da necessidade de equilibrar o processo penal com as novas formas de práticas criminosas (delitos cibernéticos) foram originados os denominados métodos ocultos de investigação, dentre eles pode-se citar o agente infiltrado; o agente encoberto e os que estão previstos na Lei n.º 109/2009, de 15 de setembro.

Para Manuel da Costa Andrade médotos ocultos de investigação seriam “uma intromissão nos processos de acção, interacção e comunicação das pessoas concretamente visadas, sem que estas tenham conhecimento do facto nem dele se apercebam. Que, por causa disso, continuam a agir, interagir, a expressar-se e a comunicar de forma ‘inocente’, fazendo ou dizendo coisas de sentido claramente auto-incriminatório ou incriminatório daqueles que com elas interagem ou comunicam. De forma simplificada e reducionista, os meios ocultos de investigação levam as pessoas atingidas – normalmente o suspeito – a ‘ditar’ inconscientemente para o processo ‘confissões’ não esclarecidas nem livres”[[156]](#footnote-156).

Como a própria denominação sugere, tais métodos são aqueles usados na investigação criminal sem que deles tenham conhecimento os investigados, sendo certo que essa ocultação é o que lhe dar eficiência na apuração delitiva.

Isso significa que os investigados ‘levam a vida’ e suas atividades contidianas normalmente, sem ter noção ou ciência que estão sendo averiguados, vigiados ou de que estejam convivendo, lado a lado, com agentes infiltrados, com quem poderá confiar informações que poderão ser usadas em seu desfavor em um processo criminal.

Manuel Monteiro Guedes Valente, com a maestria que lhe é peculiar, afiança que os meios ou métodos ocultos de obtenção de prova – investigação criminal –operacionalizados pelas polícias, configuram uma autêntica intrusão nos tempos e espaços operativos humanos de ação, interação e comunicação entre as pessoas visadas em concreto, bem como terceiros, com a instância investigativa.

O propósito é que os envolvidos não tenham qualquer conhecimento sobre essa intrusão e, simultaneamente, “produzam prova incriminatória contra si próprias com uma ausência plena de autodeterminação – liberdade de e em pensar, liberdade de e em decidir, e liberdade de e em agir (interagir e comunicar) – e com uma consequente ausência de autorresponsabilidade consciente”[[157]](#footnote-157).

Hans-Jörg Albrecht citado por David Silva Ramalho assevera que há ao menos quatro características entre as espécies de métodos ocultos de investigação criminal, quais sejam: “(i) são ocultados do visao e neutralizam alguns dos seus direitos processuais convencionais, *maxime* o direito à não-auto-incriminação; (ii) são abrangentes, na medida em que incidem sobre um número elevado de terceiros e permitem recolher informações que atravessam o passado, presente e futuro e nao se limitam ao período relativo aos factos sob investigação; (iii) neutralizam igualmente o direito de certas testemunhas nao prestarem declarações; (iv) e permitem recolher informações sem ter em atenção a intimidade e fiabilidade da comunicação”[[158]](#footnote-158).

Manuel da Costa Andrade tece duras críticas ao uso dos aludidos métodos ocultos, haja vista que tais recursos “acaba por deslocar o centro de gravidade das decisões da fase do julgamento, quase sempre público, para os resultados obtidos em sede de inquérito através de investigações ocultas. Assim se arrisca transformar o julgamento num mero ritual externo, no qual o juiz se vê desarmado e enfraquecido em face do Ministério Público e dos órgãos de polícia criminal, ao passo que o arguido é lentamente convertido de sujeito processual em objecto do processo”[[159]](#footnote-159).

Observa-se, portanto, que a utilização dos métodos ocultos de investigação criminal apresentam uma elevada e irrestrita gravidade em diversos âmbitos, inserindo-se a sua potencial anulação de bens jurídicos e direitos fundamentais de uma diversidade de pessoas, devendo-se encontrar um limite para o seu uso.

Com efeito, a consagração destes métodos ocultos não significa, de todo, a sua constante disponibilidade para o seu uso sem critérios no decorrer de qualquer investigação criminal. Uma vez que, o simples fato de um método de investigação ser oculto demonstra, por si só, um fator de lesividade a ter o cuidado de sua aplicação de forma proporcional.

Em Portugal os métodos ocultos de investigação criminal encontram-se espalhados em diversos diplomas normativos, sendo que alguns estão normativados no Código de Processo Penal, tal como as escutas telefônicas, e, outros como “os agentes encobertos” estão dispostos na Lei nº 101/2001; os registros fotográficos previstos na Lei nº 5/2002; a vídeo vigilância, Lei nº 1/2005; e, recentemente os métodos ocultos de investigação em ambiente digital previstos na Lei nº 109/2009, de 15 de setembro. Também, não se pode cair no esquecimento os denominados actos de colaboração ou instrumentais que estão dispostos no artigo 6º, da Lei n.º 36/94, de 29 de setembro, a qual estebelece medidas de combate à corrupção e criminalidade económica financeira.

Atinente ao ordenamento jurídico brasileiro, a repercussão mais categórica da aplicação dos métodos ocultos de investigação é a indiferença total com o contraditório durante a fase inquisitorial. Argumenta-se que a persecução penal somente pode ser seguida quando o sujeito é vigiado sem o seu conhecimento.

Soma-se a esse argumento, o arrazoado de que as provas ou elementos probatórios coletados no transcorrer da investigação inquisitorial são apenas informativos, os quais serão submetidos à apreciação do Ministério Público, que verificará a conveniência ou não de tais elementos para a propositura da ação penal.

Como resultado, no decorrer da fase inquisitorial, não se permite qualquer tipo de manifestação do investigado em relação às eventuais afrontas a seus direitos e garantias fundamentais, e isso ocorre em razão de total ignorância da existência da medida ou pela caracterísitica inquisitiva do momento ou de um contraditório inexistente ou procrastinado.

Na prática processual brasileira, é verificável a tolerância com o alastramento dos meios ocultos de investigação através da jurisprudência dos últimos anos, que rotineiramente manifesta sua preferência pelos interesses atinentes ao *ius puniendi* do Estado, mesmo que em prejuízo dos direitos e garantias fundamentais.

Para exemplificar, tem-se os constantes precedentes jurisprudenciais[[160]](#footnote-160) que, embasados nos argumentos de dificuldade e complexidade da investigação criminal, permitem renovações sucessivas e reiteradas de interceptações telefônicas, em que pese a exege de uma medida restritiva de direitos seja percepção de maior garantia.

Em relação a este ponto específico de renovações sucessivas e reiteradas de interceptações telefônicas, o Supremo Tribunal Federal decidiu, recentemente (17 de março de 2022), por maioria, que a Justiça poderá autorizar a prorrogação sucessiva de escutas telefônicas em investigações criminais, sem limite definido de prazo[[161]](#footnote-161).

O Tribunal, por maioria, apreciando o tema 661 da repercussão geral, deu provimento ao recurso extraordinário, para declarar a validade das interceptações telefônicas realizadas e de todas as provas delas decorrentes, nos termos do voto de Alexandre de Moraes, Redator para o acórdão, vencidos Gilmar Mendes (Relator), Dias Toffoli, Nunes Marques e Ricardo Lewandowski.

Em seguida, por unanimidade e nos termos do voto do Alexandre de Moraes, o Tribunal fixou a seguinte tese: “São lícitas as sucessivas renovações de interceptação telefônica, desde que, verificados os requisitos do artigo 2º da Lei nº 9.296/1996 e demonstrada a necessidade da medida diante de elementos concretos e a complexidade da investigação, a decisão judicial inicial e as prorrogações sejam devidamente motivadas, com justificativa legítima, ainda que sucinta, a embasar a continuidade das investigações. São ilegais as motivações padronizadas ou reproduções de modelos genéricos sem relação com o caso concreto”[[162]](#footnote-162).

Nathalie Fragoso e Gabriel Brezinski Rodrigues asseveram que “embora fundamental enquanto filtro do poder punitivo, as diretrizes acima defendidas somente operam efeitos práticos quando o dado colhido furtivamente é submetido à instrução processual penal, já que os métodos ocultos de investigação se desenvolvem ainda no âmbito da investigação preliminar, geralmente em medidas cautelares sigilosas, deferidas por um juiz, mas conduzidas pela polícia judiciária ou pelo aparato de apoio do Ministério Público”[[163]](#footnote-163).

Diogo Malan, seguindo o mesmo racíocinio acima exposto, afirma que no âmbito do processo penal brasileiro “a coleta de fontes reais de prova não é submetida a qualquer contraditório, já que o lugar-comum teórico é de que os elementos colhidos não servem diretamente à formação do convencimento do juiz, mas apenas como informe para estruturação do conjunto probatório que posteriormente será levado à instrução. Portanto, se o método oculto de investigação for realizado em completo descompasso com a legislação, sua consequência prática é a inadmissibilidade probatória do elemento colhido, e não a nulidade do ato”[[164]](#footnote-164).

Tal como ocorre em Portugal, no Brasil não teve a iniciativa em compilar todos os métodos ocultos de investigação criminal em um único diploma.

Somado a essa circunstância, tem-se que os métodos ocultos presentes no ordenamento jurídico brasileiro são compostos por requisitos e pressupostos diversificados, sendo certo que não são dotados de proporcionalidade e não guardam graus de lesividade e danosidade para serem autorizados de forma escalonada.

Mais uma vez valendo-se dos ensinamentos de Manuel Monteiro Guedes Valente “o processo legislativo de validação e legitimação jus normativo-constitucional dos meios de investigação criminal, os quais devem estar em consonância com os princípios constitucionais regentes das restrições de direitos e liberdades fundamentais pessoais. Pois, em um determinado tempo e espaço, leis podem ser criadas e aprovadas para o emprego de métodos ocultos de investigação pelo poder representativo do povo, o político-legislativo, como forma de legitimar o aniquilamento de direitos fundamentais e, assim, legitimar tiranias”[[165]](#footnote-165).

Como visto alhures, a inexistência de um regime geral, tanto em Portugal como no Brasil, tem-se que a utilização dos métodos ocultos de investigação criminal encontra limites em princípios e demarcada por pressupostos, sendo que a sua utilização fora de tais parâmetros a torna ilegal e abusiva.

# 4. Aplicação dos Princípios Constitucionais como limitadores dos métodos ocultos de investigação criminal

Como visto, os atos de investigação criminal que comprometam os direitos fundamentais em razão da inovação e impacto na vida cotidiana das nova tecnologias, devem estar fundados no princípio da legalidade, e é possível extrair deste princípio que “a lei deve especificar todos e cada um dos pressupostos e condições da intervenção e não deixar ao arbítrio dos investigadores e juízes a interpretação particular dos interesses e garantias prevalecentes em cada caso de busca ou recolha de informação das provas incriminatórias”[[166]](#footnote-166).

Dito isso, é mister questionar até que ponto é legal ou lícito ao Estado atingir direitos, garantias e liberdades das pessoas que se presumem inocentes na obtenção de prova para o exercício do seu direito de punir.

De acordo com David Silva Ramalho, os métodos ocultos de investigação criminal aparecem dendro de um equilíbrio, qual seja, de um lado a eficiência na defesa dos investigados na ação penal que produz bloqueios à investigação criminal, e de outro, a eficiência no plano da investigação criminal que legitima a restrição ou ablação de direitos fundamentais e processuais do investigado[[167]](#footnote-167).

Manuel da Costa Andrade mencionado por David Silva Ramalho disciplina que a ausência de critérios establecidos por via legislativa num regime geral unificado e da verficação de comprometedoras inconsistências e assistematicidades e despropocionadas assimetrias no direito positivo que regula esta matéria nao decorre a impossibilidade de se erigir um regime jurídico e uma teoria geral dos métodos ocultos[[168]](#footnote-168).

Verifica-se nas palavras acima empregadas, o que se busca em um regime geral unificado é identificar as categorias e definir os princípios de investigação e a sua ulterior aplicação, aberta às singularidades de cada uma delas[[169]](#footnote-169).

Ressaltando a importância de se reforçar ou relembrar os princípios constitucionais que regem a atividade investigatória em âmbito digital, Manuel Monteiro Guedes Valente afiança que a incapacidae de ação e de prevenção gerada *ab initio* por esta criminaliade não pode servir de catapulta para se promover um ataque aos direitos, liberdades e garantias fundamentais pessoais consagradas na Constituição[[170]](#footnote-170).

Diante do que foi lecionado acima, é mister tão somente mencionar quais são os princípios constitucionais regentes dos métodos ocultos de investigação criminal, para não fugir do objetivo principal da presente dissertação.

Valendo-me novamente dos ensinamentos do Manuel Monteiro Guedes Valente, tem-se que “é impossível olvidar que o recurso a meios de obtenção de prova digitais, como buscas no sistema digital, apreensões prejudiciais e preventivas diditais, reastreamento das comunicações efetuadas pelos sistemas operativos digitais, monitorização dessas comunicações, dos IMEI’s, dos IP’s e dos GPS’s, agente infiltrado digital, ação enconberta digital, representam, por si só e pela sua natureza, uma manifestação e uma elevada danosidade social e lesividade na restrição de direitos, liberdades e garantias fundamentais pessoais”[[171]](#footnote-171).

Ainda, em conformidade com os ensinamentos do Manuel Monteiro Guedes Valente, tais circustâncias é que “impõe ao legislador a concretização dos vetores da política criminal do ser humano, (...) assim como a aferição e amalgama de princípios éticos-jurídicos que devem reger a decisão política de aprovação em lei dos meios de obtenção de prova admissíveis e dos pressupostos estritos (materiais e formais) de admissibilidade de recurso aos meios ocultos de obtenção e prova”[[172]](#footnote-172).

O Livro III (Da Prova), Título I (Disposições gerais), artigo 125º (Legalidade da Prova) do Código de Processo Penal Português dispõe que “são admissíveis as provas que não forem proibidas por lei”[[173]](#footnote-173). Ou seja, a variedade de meio prova e de meio de obtenção de prova permitidos no processo penal não está limitado a um rol taxativo, ao contrário, compreende os meios de prova e meios de prova denominados de atípicos ou inominados, desde que não sejam legalmente proibidos.

David Silva Ramalho na análise deste dispositivo legal conclui que “a aparente simplicidae da formulação legal do citado artigo, conjugada com a sua inserção sistemática, não deve, porém, induzir o intérprete a concluir precipitadamente que toda a prova será válida, desde que o método da sua obtenção não preencha a factispécie do artigo 126º do CPP”.

Desta interpretação extrai-se que, observada a ausência de proibições legais devidamente previstas em lei que impedem ao uso de meio de prova ou de obtenção de prova atípico, passa-se à verificação de sua capacidade para cercear direitos fundamentais do investigado.

Trata-se, entretanto, da análise da verificação de “qualquer compressão do âmbito de protecção do direito, traduzida na desconsideração de elementos do objecto de protecção, ou na recusa da titularidade ou exercício de meios jurídicos destinados à respectiva fruição, operada por acto do poder público de natureza geral e abstracta ou individual e contreta, neste caso o recurso a métodos ocultos”[[174]](#footnote-174).

Tem-se aqui, portanto, o denominado Princípio da Reserva de Lei.

Em seu artigo “O Reforço dos Princípios Constitucionais na obtenção de prova no Mundo Digital”[[175]](#footnote-175), Manuel Monteiro Guedes Valente cita o Princípio da Reserva de Constituição nas restrições de direitos, liberdades e garantias fundamentais – n.º 2 do artigo 18 da CRP – e das garantias efetivas no âmbito do recurso ao meios ocultos de obtenção de prova.

Para o mencionado autor, os dispositivos constitucionais - artigos 26.º, n.ºs 1 e 2; 34.º, n.º 4 e 35.º da CRP, na linha do artigo 18.º, n.º 2 da CRP – impõem que a restrição de direitos, liberaes e garantias fundamentais pessoais, no âmbito de quaisquer meios de investigação criminal que com eles colidam, esteja prevista na Constituição[[176]](#footnote-176).

David Silva Ramalho ao dissertar sobre o Princípio da Proporcionalidade frente aos métodos ocultos de investigação criminal, utiliza-se dos ensinamentos de Jorge Reis Novais, para quem “a referência fundamental do controlo da actuação dos poderes públicos em Estado e Direito, assumindo, particularmente no âmbito dos limites aos direitos fundamentais, o papel de principal instrumento de controlo da actuação restritiva da liberdade individual e de chave sem a qual, integrada no recurso à metodologia da ponderação de bens, não seria possível decifrar os complexos problemas que aí vêm suscitados”[[177]](#footnote-177).

Frente a esse princípio, David Silva Ramalho conclui que “caberá ao legislador estabelecer, em função da gravidade do método, uma filtragem do tipo de crimes e das condições da sua prática susceptíveis de justificarem a cocnreta restrição abrangida pela sua previsão. Daí que, entre os critérios utilizados, se recorra frequentemente a um catálogo de crimes aptos a desencadearem o recurso a certo tipo de métodos, quer em função da sua gravidade, quer em função da sua absoluta indispensabilidade para a prova do ilícito”[[178]](#footnote-178).

Verifica-se, portanto, que pelo Princípio da proporcionalidade entende-se que devem ser levados em consideração todas as circunstâncias do caso e o sacrifício dos direitos e interesses afetado de forma que não seja superior ao benefício resultante de sua adoção para interesse público e terceiros.

Para a ponderação dos interesses em conflito, a avaliação do interesse público levará em consideração: a gravidade do evento, sua importância social ou o campo tecnológico de produção, a intensidade dos sinais existentes e a relevância do resultado perseguido com o restrição do direito.

Manuel Monteiro Guedes Valente ainda menciona os Princípios da Reserva de Código e da Segurança Jurídica, sendo que a opção, que os legisladores têm seguido, é de regular matéria tão sensível por leis avulsas que entram, quantas vezes, em contradição com o Código de Processo Penal e com as leis de valor reforçado e, por conseguinte, estão feridas de ilegalidade e de inconstitucionalidade material indireta[[179]](#footnote-179).

Em relação ao Princípio da Segurança Jurídica, Manuel Monteiro assevera que segurança jurídica não se afere apenas da codificação de todos os meios de obtenção de prova, sujeitos a um regime comum, mas também da determinabilidade normativa – os termos têm de ser suficientemente claros para que todos os cidadãos conheçam as circunstâncias e quesitos dos meios ocultos[[180]](#footnote-180).

Manuel da Costa Andrade ao dissertar sobre o Princípio da Subsidiariedade afiança que o mesmo está ligado intimamente com o Princípio da Proporcionalidade, sendo que a sua aplicação prática signfica que a autoridade judiciária competente, colcoada perante uma pluralidade de métodos abertos e ocultos de investigação criminal abstractamente aplicáveis, come, no plano extrínseco, por dar prioridade aos métodos abertos, e, caso estes nao sejam aptos a satisfazer os interesses da investigação, no plano intríseco, recorra ao método menos gravoso de entre aqueles que se afiguram idóneos[[181]](#footnote-181).

O outro princípio de que se trata neste trabalho é o Princípio da Reserva do Juiz. Por este princípio tem-se que quando há necessidade de recorrer a uma medida legalmente prevista que se prenda diretamente com direitos fundamentais, *maxime* um método oculto de investigação criminal, é geralmente ao juiz de instrução que cabe aferir do cumprimento dos pressupostos legais para a sua utilização, incluindo, no plano estritamente jurídico, da respectiva proporcionalidade à luz da circunstâncias do caso[[182]](#footnote-182).

Impende ressaltar que Manuel Monteiro Guedes Valente[[183]](#footnote-183) ainda indica outros príncipios aplicáveis ao tema métodos ocultos da investigação criminal, quais sejam: Princípios da Determinabilidade e da Certeza dos meios de obtenção de prova; Princípio do Catálogo; Princípio da excecionalidade de recurso ao meio em geral e em concreto; Princípio da irretroatividade das leis restritivas de direitos e liberdades fundamentais e de leis sanadoras supervenientes de meios de persecução penal; Princípio da (in) admissibilidade constitucional.

Analisados os limites e restrições à utilização dos métodos ocultos de investigação criminal na obtenção das provas digitasi, se faz oportuno verificar as implicações dessa investigação face aos direitos fundamentais do investigado.

# 5. A Investigação Criminal e suas implicações face aos Direitos Fundamentais do Investigado

Como vimos, o uso policial da tecnologia para investigação e resolução de crimes é o resultado de uma evolução contínua ligada ao desenvolvimento da humanidade. Portanto, da mesma forma que os avanços tecnológicos são aplicados em telemedicina ou engenharia biomédica, podem e devem ser também utilizados pelas autoridades responsáveis ​​pela aplicação da lei para solucionar crimes de forma mais rápida, eficiente e seguro.

Afinal, o uso da tecnologia pelas forças e corpos de Segurança Pública não significa outra coisa que amplificar esmagadoramente seus sentidos, seus conhecimentos e métodos de atuação.

No entanto, não podemos ignorar o impacto que o desenvolvimento das TIC’s pode ter na afetação aos Direitos Fundamentais, de modo que se faz necessário analisar os desafios éticos e jurídicos que os desenvolvimentos relacionados às novas tecnologias podem suscitar no processo de adaptação dos direitos constitucionais para dar respostas aos riscos e desafios impostos pelas inovações tecnológicas.

De fato, o uso de equipamentos de áudio e imagens térmicas que nos permitem ver e ouvir o que acontece dentro das paredes das casas é mais do que apenas "colocar o ouvido" e pode restringir o conceito atual de inviolabilidade domiciliar.

A possibilidade de escanear os corpos das pessoas para descobrir se elas carregam explosivos sob suas roupas ou substâncias proibidas dentro de seu corpo, e até mesmo evitar comportamentos suspeitos, graças aos programas informáticos de análise de conduta humana, também vai além do que constituiria uma busca policial por descobrir os pertences que a pessoa carrega que exige uma reflexão sobre o debate sobre o direito à privacidade e intimidade[[184]](#footnote-184). A comparação dos dados de posicionamento GPS de um terminal de aparelho celular para conhecer, em tempo real, o deslocamentos ou a posição geográfica de um determinado cidadão, excede o que poderia constituir um acompanhamento policial.

O autor português Paulo Dá Mesquita ao se manifestar sobre a investigação criminal com o uso das novas tecnologias e a sua afetação aos direitos fundamentais, assevera que “é fato inconteste que o surgimento e desenvolvimento da Internet, da informática e dos novos mecanismos de telecomunicação que as conjugam e são delas dependentes, bem como o aprimoramento de aparelhos e dispositivos utilizados, alterou completamente a comunicação a distância entre as pessoas; enquanto novas tecnologias de comunicação e informação, essas ferramentas permitiram uma circulação célere e massiva de informações, novas formas de comunicar e de interação social, ensejando uma verdadeira remodelação da sociedade, sendo fator decisivo para o fenômeno da globalização”[[185]](#footnote-185).

Dario José Kist também comentou sobre a afronta das provas digitais sobre os direitos fundamentais, asseverando que “se de um lado houve uma universalização no acesso às tecnologias de comunicação, esta mesma revolução potenciou novas formas de vulnerar a privacidade dos participantes dos processos de comunicação, pois os mecanismos de intromissão alheia em comunicações privadas experimentaram a mesma sofisticação dos próprios meios de comunicação”[[186]](#footnote-186).

Tais avanços tecnológicos são vistos com enorme desconfiança por certo setor doutrinário, mas também pelos próprios tribunais, preocupados principalmente com a insuficiência da regulação da lei sobre o uso de instrumentos tecnológicos na investigação criminal e a sua possível afetação desproporcional da intimidade e de outros direitos fundamentias dos sujeitos passivos das investigações. Posto isso, no próximo capítulo serão tecidas palavras sobre a implicação das provas digitais frente aos direitos fundamentais do investigado, objetivo principal da presente dissertação.

# CAPÍTULO IV – A PROVA DIGITAL E AS SUAS IMPLICAÇÕES NOS DIREITOS FUNDAMENTAIS DO INVESTIGADO

# 1. Introdução

Diante do que fora exposto acima, verifica-se que constantemente tem-se a necessidade em repensar qual é a ideia de liberdade, intimidade ou segurança, bem como os respetivos cruzamentos entre tais conceitos para redefinir as preferências, prioridades ou grau de tolerância.

Neste capítulo final, é imperioso asseverar sobre a conscientização necessária do conteúdo do direito fundamental à privacidade, aqui entendido no sentido mais amplo possível.

Por isso, nos tópicos abaixo serão analisadas algumas questões sobre a privaciade, intimidade, sigilo das comunicações e proteção dos dados pessoais, para ao final concluir, se em razão da obteção de prova digital por meio da investigação criminal há afronta aos direitos fundamentais.

# 2. A Investigação Criminal e o Direito à Privacidade do Investigado

# 2.1. Breves considerações

O autor espanhol Vicente Gimeno Sendra afirma que uma das funções específicas da fase investigativa do processo penal consiste na realização dos atos de investigação destinados a apurar a preexistência e tipicidade do ato e sua autoria. Esses atos tornam-se pressupostos materiais essencial para as partes prepararem e fundamentarem suas acusações[[187]](#footnote-187).

Como consequência do progresso da ciência no campo das telecomunicações, quase todas as infrações penais hoje têm um suporte tecnológico.

Nesse contexto, o uso pela Polícia de tecnologias modernas constitui uma ferramenta de trabalho essencial para obter as provas digitais do crime e contrariar os meios sofisticados que se servem os grupos criminosos, bem como o caráter internacional sua atividade.

Não obstante, a investigação criminal derivada do uso dessas tecnologias, coloca novos desafios que exigem uma resposta do legislador. Um destes consiste na necessidade de buscar um equilíbrio adequado entre a garantia de segurança pública e a proteção da privacidade dos investigados.

Não se desconhece a intensa interferência estatal na esfera privada dos cidadãos, que muitas destas medidas implicam. Até recentemente, as áreas em que a vida privada e familiar se desenvolvia, limitavam-se ao lar e à correspondência postal. Hoje, as novas tecnologias têm feito que muitos aspectos da vida privada se desenvolvam em novos espaços, não só no espaço físico, mas também no espaço virtual, que da mesma forma devem ser protegidos[[188]](#footnote-188).

Dito isso, há que se afirmar que o direito à privacidade teve sua origem no trabalho doutrinário, e que gradualmente fora confirmado em leis e decisões dos órgãos judiciais, e que nos dias atuais é detentor de proteção Constitucional[[189]](#footnote-189).

Certo disso, uma das questões mais controvertidas está na definição do campo de proteção do direito à privacidade, haja vista as inúmeras manifestações referentes a esse ponto.

Dario José Kist citando os ensinamentos de Samuel Warren e Louis Brandeis, assevera que inicialmente a construção teoria sobre o direito à privacidade “foi focada na prerrogativa de estar só, de não ser incomodado na intimidade, no sentido de definir uma área impenetrável à curiosidade alheia, resguardando alguns aspectos de vida das pessoas do conhecimento de outras, com o consequente direito ao sossego e à reclusão, e todo o raciocínio desenvolvido tinha por foco a salvaguarda da imagem como valor inerente à intimidade”[[190]](#footnote-190).

Considerando o conceito acima apresentado, tem-se que com a ampliação e disseminação das novas tecnologias de informação e comunicação, aumentou-se também o grau de exposição das pessoas, o que facilitou a intromissão no âmbito mais restrito de suas intimidades; por isso, se fez necessário criar meios e mecanismos protetivos da privacidade.

Novamente fazendo uso dos ensinamentos do autor brasileiro Dario José Kist, é necessário definir o conteúdo da intimidade para verificar em que situações a intervenção e ingerência nas comunicações, por certamente afrontá-las, será considerada abusiva, com a imprestabilidade consequente da prova digital produzida[[191]](#footnote-191), mas antes é preciso tecer algumas palavras sobre a proteção à intimidade[[192]](#footnote-192).

# 2.2. Evolução da proteção à intimidade

A evolução do direito torna necessária a aplicação de uma especificidade aos diversos novos direitos que surgem para se conseguir uma correta cobertura jurídica. A lei concede prioridade local às disciplinas especializadas, aplicáveis ​​para a sua proteção, de acordo com um conjunto de leis ou princípios de direito aplicáveis ​​a essas especialidades; isto é, leis específicas.

A história da humanidade conquistou grandes espaços em matéria de liberdade de informação e expressão e, aos poucos, veio ganhando espaço para a conquista de outros direitos e liberdades que florescem inesperadamente em razão da evolução da sociedade, como por exemplo, o direito à proteção de dados pessoais que surgem à luz do aprimoramento científico, tecnológico e dos direitos envolvidos.

A proteção de dados é um campo jurídico estreamente necessário para analisar o momento tecnológico em que se encontra a sociedade; a um passo da singularidade. É necessário rever o campo jurídico que não só está em ascensão, mas também será um dos eixos sobre os quais girará o futuro direito da inteligência artificial e da robótica avançada, de forma a poderem se adequar às necessidades sociais do direito.

A proteção de dados não pode ser menos, embora seja um campo relativamente novo, ainda mais quando se trata de um dos que mais evoluem no direito.

A origem mais clara do campo da proteção de dados é encontrada nos Estados Unidos no ensaio publicado como um artigo na *Harvad Law Review* como “*The Right to Privacy*” por Warren e Brandeis em 1890 (1), onde o que agora está estabelecido é considera a definição mais aceita de privacidade.

A privacidade é geralmente entendida como o direito de ser deixado em paz ou de não ser incomodado, "o direito de ser deixado em paz". Portanto, pode-se observar que a privacidade baseia-se no anonimato, no sigilo, tendo como pilares a autonomia, a individualidade, o desenvolvimento da personalidade e a inviolabilidade da dignidade pessoal[[193]](#footnote-193).

Em 1763, William Pitten o autor da citação do aforismo inglês "a casa de um homem como seu castelo", reivindica pela proteção pessoal do indivíduo contra o poder do monarca em qualquer lugar, inclusive na morada mais humilde.

Tal princípio básico do direito inglês concede a cada cidadão, como indivíduo, a proteção de seu domicílio como o lugar onde é concedida a máxima proteção pessoal. [[194]](#footnote-194).

Foi o juiz Thomas M. Cooley quem afirmou na primeira edição do Tratado de Direito Constitucional, sobre as limitações constitucionais que dependem do poder legislativo dos Estados Unidos da América em 1868. Estabeleceu a primeira referência jurídica de privacidade de dados ao indicar que as garantias da Terceira[[195]](#footnote-195), Quarta[[196]](#footnote-196) e Quinta[[197]](#footnote-197) Emendas da Constituição dos Estados Unidos constituem veículos para a proteção da privacidade individual[[198]](#footnote-198).

Thomas M. Cooley indicou que a máxima da *common law* de "a casa de um homem como seu castelo" citada em 1763 por William Pitten é a expressão jurídica que garante a imunidade do cidadão em seu domicílio contra a ação do governo. E por extensão da proteção à sua pessoa, propriedade e documentação pessoal, mesmo em face de um processo judicial.

Sendo assim, a Suprema Corte dos Estados Unidos, ao longo de uma ampla e flutuante jurisprudência, considerou a existência do direito à privacidade, implícita na liberdade de associação que protege a Primeira Emenda[[199]](#footnote-199) que protege qualquer cidadão contra qualquer obrigação legal de divulgar a associação a um grupo ou organização; da mesma forma, a Quarta Emenda, no que diz respeito às buscas arbitrárias, limita a intrusão do governo em pessoas, casas, documentos e bens pessoais e; também na Quinta Emenda em relação à incriminação contra si mesmo ou divulgação de dados pessoais[[200]](#footnote-200).

Mas foi só alguns anos depois, em 1905, que a Suprema Corte da Geórgia aplicou claramente o conceito de proteção de dados e privacidade de um ponto de vista jurídico pela primeira vez, no caso da Pavesick & New England Life Insurance Company[[201]](#footnote-201).

A partir daí se reconheceu a existência do direito à própria imagem e o direito à privacidade na vida privada; sob o fundamento jurídico de que esse direito é um direito inato que surge à luz das leis naturais.

A sentença indicou que a liberdade pessoal abrange tanto o direito à vida pública como um direito correlativo à privacidade no mesmo nível de proteção que o primeiro e de natureza inviolável.

Os países europeus que foram os precursores da proteção de dados na Europa foram o Reino Unido e a Alemanha principalmente, devido à sua data e conteúdo regulamentado. O primeiro foi o Reino Unido, que iniciou seu debate em 1961, quando Lord Mancroft apresentou um projeto de lei cujo objetivo era a regulamentação e a proteção da privacidade.

Mais tarde, houve outra tentativa em 1967 com o projeto Lyon apresentado por Alexander Lyon, embora também tenha falhado. Só em 1972, com a publicação do Younger Committee Report, é que se estabeleceu o sinal de partida para a legislação europeia em matéria de proteção de dados.

Os resultados desta comissão deram origem ao Livro Branco onde o conceito de proteção de dados pessoais derivado do processamento informatizado de dados foi introduzido em 1979. Após esse histórico, em 1984 foi aprovada a Lei de Proteção de Dados[[202]](#footnote-202).

Nesse viés, a Comunidade Europeia aprovou a Convenção para a Proteção de Pessoas com Relação ao Tratamento Automatizado de Dados Pessoais em 28 de janeiro de 1981.

Na Espanha, como em vários outros países da região e ao redor do mundo, o desenvolvimento do comércio eletrônico destacou a necessidade do aumento de proteção dos dados pessoais dos cidadãos, sem subestimar os grandes marcos normativos e jurisprudenciais que na época marcaram a história europeia e espanhola.

As primeiras referências importantes sobre o direito à proteção da intimidade na Península Ibérica são encontradas a partir dos trabalhos preparatórios do Artigo 18.4 da Constituição Espanhola de 1980, até a atual Lei Orgânica de Proteção de dados pessoais de 13 de dezembro de 1999.

A Constituição da República Portuguesa de 1976 foi a primeira da Europa a destinar um dispositivo à matéria de proteção de dados pessoais em seu artigo 35.º, acerca das normas gerais de tratamento de dados pessoais no âmbito da informática e aqueles constantes de ficheiros manuais.

O Brasil só decretou uma lei ampla acerca da proteção de dados em 2018, com a Lei n. 13.709, de 14 de agosto (Lei Geral de Proteção de Dados), inspirada no Regime Geral de Proteção de Dados europeu.

Insta mencionar que a lei portuguesa 67 de 26 de outubro de 1998, que atualmente foi revogada pela Lei 58/2019 de 08 de agosto, foi clara ao conceituar os dados pessoais; sendo considerado um conceito muito mais prescritivo e padronizador que a norma anterior.[[203]](#footnote-203)

Nessa normativa o legislador português já disciplinou acerca dos dados pessoais para fins de investigação policial, nesse momento limitando-se ao necessário para a prevenção de um perigo concreto ou repressão de uma infracção determinada, para o exercício de competências previstas no respectivo estatuto orgânico ou noutra disposição legal e ainda nos termos de acordo ou convenção internacional de que Portugal fosse parte, conforme disposição do artigo 8° da Lei 67/98.

# 2.3. A Inviolabilidade das comunicações e o Direito à intimidade

O sigilo das comunicações constitui uma das clássicas garantias dos direitos fundamentais que visa proteger a vida privada da pessoa, embora já seja, em última instância, um direito fundamental autônomo.

Seu estudo é de notável interesse, já que daquela concepção “clássica” ela teve que evoluir notavelmente e de forma acelerada, de certa forma paralela ao impressionante desenvolvimento que a técnica significa para a comunicação entre pessoas, em razão das novas tecnologias.

Da mesma forma, pode-se falar de um desenvolvimento jurídico, visando fortalecer a garantia de que a própria lei inclui, aumentando e detalhando os requisitos necessários para uma intervenção de comunicações legítima, e adaptando esses requisitos, que foram originalmente destinados à interceptação da correspondência postal, para o telefone, meio fixo ou móvel, para o correio eletrônico e as demais formas de comunicação que existem hoje.

Sendo assim, é notório que existe uma garantia que protege as comunicações entre as pessoas, de forma que qualquer suposição admissível de interceptação de comunicações é apresentada como excepcional e cercada de limites, requisitos e garantias, visto que esta prática afeta um direito fundamental, e somente o cumprimento desses requisitos e garantias permitirá que essa afetação não se torne uma violação.

Como direito fundamental, o sigilo das comunicações é reconhecido na Declaração Universal dos Direitos Humanos de 10 de dezembro de 1948 em seu art. XII, que estabelece que “ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferencias ou ataques”[[204]](#footnote-204).

O direito à privacidade é consideravelmente novo no mundo jurídico, fruto de produção doutrinária, sendo constantemente reconhecido nas decições judiciais, legislações e hoje possui status de direito fundamental em várias localidades, a exemplo do Brasil que elencou na Constituição Federal em seu artigo 5 inciso X a vida privada e a intimidade como invioláveis, uma vez que a abrangem a vida particular da pessoa natural.

Segundo Carlos Alberto Bittar[[205]](#footnote-205), “o elemento fundamental do direito à intimidade, manifestação primordial do direito à vida privada, é a exigibilidade e respeito ao isolamento de cada ser humano, que não pretende que certos aspectos de sua vida cheguem ao conhecimento de terceiros”.

A expressão direito à privacidade, em sentido amplo, é adotada por José Afonso da Silva[[206]](#footnote-206) elencando o que envolve o íntimo, privado e atinente à personalidade, consagradas pelo texto constitucional, e define a privacidade como sendo “o conjunto de informação acerca do indivíduo, que ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em que condições, sem a isso poder ser legalmente sujeito”.

O direito à intimidade, abarcado pelo direito à privacidade, necessita de amparo para que a dignidade da pessoa seja mantida e efetivada, sendo este um direito básico e fundamental inato ao ser humano com amparo constitucional.

A inviolabilidade das comunicações é uma questão fundamental contemplada nas principais convenções internacionais de direitos humanos. Na América Latina, a maioria de seus países reconhece o nível constitucional de inviolabilidade das comunicações como uma questão fundamental e, portanto, só pode ser suspensa em casos excepcionais e nas condições estabelecidas em lei.

Dada a sua natureza de direito fundamental, a regra geral é que o direito à inviolabilidade das comunicações só pode ser limitado nos casos e circunstâncias expressamente previstos na lei, o que ocorre geralmente no âmbito de investigações criminais ou por razões de segurança do Estado.

A Constituição brasileira possui diversos dispositivos que podem ser utilizados no contexto de investigações criminais usando tecnologias de informação, principalmente aqueles que protegem a privacidade do indivíduo.

O artigo 5º, inciso X, da Constituição da República Federativa do Brasil dispõe sobre a proteção da privacidade de uma forma genérica. Esse dispositivo é complementado por outro imediato, o art. 5º, XII, CF, que dispõe sobre a inviolabilidade da correspondência e das comunicações em geral, com exceção das situações abrangidas por ordem judicial, nas hipóteses e na forma que a Lei nº 9.296 / 96 estabelece para fins de investigação criminal ou instrução processual penal.

A proteção é concedida a todos os mecanismos de comunicação digital, independentemente do formato usado. A realidade tecnológica apresenta um amplo leque de opções como programas de mensagens instantâneas, videoconferência ou telefonia sobre IP, etc.

No Brasil, o direito à privacidade é regido principalmente pelo Código Civil e pela Lei Geral de Proteção de Dados Pessoais do Brasil. O artigo 21 do Código Civil Brasileiro estabelece que “a vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma”.

O referido dispositivo também permite que qualquer pessoa possa requerer o pagamento de indenização pelos danos civis advindos da divulgação não autorizada de escritos, transmissão de discursos, ou publicação, exibição ou uso de imagem de uma pessoa, a menos que seja necessário para fins judiciais.

Em outras palavras, os direitos da personalidade incluem o uso da voz e da imagem humanas e, como regra geral, permitem que as pessoas busquem compensação pelo uso não autorizado de tais gravações de conversas privadas.

Já a Lei 13.709, de 14 de agosto de 2018, alterada pela Lei 13.853 de 2019 e definida como Lei Geral de Proteção de dados (LGPD), entrou em vigor em setembro de 2020 e reforça as proteções constitucionais e legais existentes para o direito à privacidade, com ênfase nos direitos dos indivíduos.

A LGPD rege o processamento de dados pessoais em qualquer tipo de meio de comunicação (incluindo mídia digital) para proteger a liberdade, a privacidade e o livre desenvolvimento de personalidades.

De forma breve, é de suma importância definir acerca da terminologia sobre os tipos de dados consagrada internacionalmente, caracterizando cada um dos elementos necessários ao acesso à rede e para a utilização dos serviços, classificados de forma tripartida, quais sejam, os dados cadastrais, os dados de tráfego e os dados de conteúdo.

Os dados cadastrais constituem as informações fornecidas pelo usuário, que são essenciais à comunicação e relacionam-se à ligação à rede, contudo, não integram o processo de comunicação e, portanto com o seu acesso tem-se a menor intrusão na privacidade.

Diferentemente dos dados de tráfego, que surgem da transmissão de mensagens pela rede e, portanto, são gerados pelo processo de comunicação eletrônica.[[207]](#footnote-207)

E por fim, os dados de conteúdo, que se caracterizam pela mensagem em si, o teor do que fora transmitido entre emitente e destinatário, classificados como os de maior intrusão na privacidade no caso de acesso.

A definição dos dados é de suma importância para a compreensão de qual regime jurídico deverá ser adotado para o acesso a eles, considerando os direitos fundamentais em pauta.

A LGPD estabelece expressamente certas bases jurídicas para o tratamento válido e legal de dados pessoais (incluindo o seu registo e transmissão), que incluem: cumprir uma obrigação legal ou regulamentar do responsável pelo tratamento; servir os interesses legítimos do responsável pelo tratamento ou de terceiros; fazer cumprir um contrato ou outros procedimentos preliminares relacionados com um contrato de que o titular seja parte, a pedido do titular dos dados; e, com o consentimento do titular dos dados.

A inviolabilidade das comunicações implica um espaço de abstenção do Estado quanto às comunicações interpessoais, cujo conteúdo não pode ser internalizado, salvo no caso de ter consequências fora da esfera íntima do titular, como nos casos em que constitui um elemento de prova de crime ou produz efeitos a terceiros.

Como é sabido o direito à privacidade caaracteriza-se como sendo o direito de se excluir, afastar ou obstar a intromissão de terceiros nos assuntos que pertencem ao íntimo do indivíduo ou ao seu círculo de convivência, podendo, inclusive, impedir a divulgação dessas informações, devidamente assegurado pelo artigo 5º, inciso X, da Constituição Federal de 1988, sob pena de indenização pelo dano material e/ou moral decorrente da violação.

Além da protecão constitucional, consigna-se a Lei 12.965/14 que dispõe sobre a proteção dos registros, dados pessoais e às comunicações privadas, que em seu artigo 10[[208]](#footnote-208) elenca a obrigação geral de preservação da intimidade, da vida privada, honra e a imagem das partes envolvidas na comunicação.

Realizada uma análise do texto legislativo supramencionado ainda é possivel aferir o nível de afetação do direito fundamental que permite o acesso aos dados cadastrais conforme disposto no § 3º no artigo 10, enquanto que nos outros tipos de dados esse acesso pode ser condicionado à requisição judicial.

Interessante é que ainda que o acesso seja condicionado à requisição judicial, tamanha é a relevância do direito de intimidade e da vida privada; restando estabelecidas condições para a solicitação de fornecimento de registros de conexão ou de registros de acesso a aplicações de internet, quais sejam; fundados indícios da ocorrência do ilícito, justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória, e período ao qual se referem os registros; sem prejuizo dos demais requisitos legais, sob pena de inadmissibilidade do pedido.[[209]](#footnote-209)

À semelhança de outros países, a Constituição de Portugal regula no seu artigo 34.º a inviolabilidade da correspondência, do domicílio e demais meios de comunicação privada. No mesmo texto legal, o artigo 26 regulamenta o direito à privacidade.

No artigo 32.8 do texto constitucional português, estabelece que todas as provas obtidas por meio de interferência abusiva na correspondência são declaradas nulas. Posteriormente, o artigo 35º estabelece regras detalhadas sobre a utilização das tecnologias de informação.

Por outro lado, o artigo 37 relativo à liberdade de expressão e informação indica que haverá total liberdade para expressar pensamentos por vários meios, bem como o direito de informar, ser informado e ser informado sem impedimentos ou discriminação, mas que as infrações que estão comprometidos no exercício destes direitos, estarão sujeitos aos princípios do direito penal e a sua avaliação ficará a cargo dos tribunais judiciais.

A legislação portuguesa criminaliza o acesso indevido às comunicações, uma vez existem disposições legais que impedem o acesso aos seus conteúdos, a exemplo da Lei 109/91 sobre Crimes Informáticos (revogada pela Lei 109/2009) em seu artigo 8[[210]](#footnote-210) que regula a interceptação ilegítima das comunicações.

Insta mencionar que o conteúdo das mensagens do correio eletrônico era estritamente de caráter privado, não se permitindo que fossem conhecidas por terceiros, sendo a interceptação por agentes do Estado uma interferência na vida privada.

Ademais, foi decretada a Lei 32 de 17 de julho de 2008 relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrônicas publicamente disponíveis ou de redes públicas de comunicações que estabeleceu que é proibida a conservação de dados que revelem o conteúdo das comunicações, sem prejuízo do disposto na Lei n.º 41/2004, de 18 de Agosto, e na legislação processual penal relativamente à intercepção e gravação de comunicações.

Resta disciplinado no artigo 9º número 1 da Lei 32/2008 a possibilidade de transmissão de dados, que somente será autorizada por despacho fundamentado do juiz de instrução, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter no âmbito da investigação, detecção e repressão de crimes graves.

A Lei nº 32/2008 tem um regime processual próprio da matéria por si regulada, firme na existência de dados conservados nos termos do artigo 4.º, nº 1 pelos fornecedores de serviços.

No que tange às disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte eletrônico foi aprovada a Lei 109 em 15 de setembro de 2009, conhecida como Lei do Cibercrime, adaptando o direito interno à Convenção sobre Cibercrime do Conselho da Europa.

Além disso, para a prova de comunicações preservadas ou conservadas em sistemas informáticos deve-se observar o sistema processual penal, previsto nos artigos 11º a 19º da Lei 109 de 15 de setembro de 2009, coadjuvado pelos artigos 3º a 11º da Lei nº 32/2008.

Sobre isso, a Convenção de Direitos Humanos estabeleceu critérios para examinar a "interferência", determinando se são arbitrárias ou abusivas quanto ao alcance do seu artigo 11.2, indicando como requisios a previsão em lei; a perseguição de um propósito legítimo; ser adequado, necessário e proporcional. Ausente qualquer um desses requisitos implica que a interferência é contrária à Convenção.

As escutas telefônicas representam um impacto direto na vida privada das pessoas, devendo; portanto, ser expressamente previsto em lei, que deve estabelecer com clareza e precisão detalhes sobre os procedimentos e âmbito da medida de intervenção, as circunstâncias em que eles podem ser usados, o procedimento a seguir entre outros elementos que detalhem sua execução, monitoramento e utilização.

# 2.4. Sigilo das comunicações e processo penal

A privacidade é um atributo da pessoa. Uma sociedade democrática não se concebe sem respeitar o âmbito em que cada pessoa decide de acordo com sua moralidade privada.

No processo penal, a intervenção das comunicações telefônicas e da interceptação de comunicações escritas ou telegráficas, tornou-se uma ferramenta útil em investigações criminais, tornando-se uma intromissão por parte do Ministério Público e do Judiciário contra vários direitos fundamentais da pessoa previstos na Constituição, a fim de descobrir a verdade e a relação das pessoas sujeitas à restrição com os fatos criminosos.

O direito à inviolabilidade das comunicações privadas configura-se como garantia formal, ou seja, que essas comunicações sejam protegidas independentemente do seu conteúdo. Neste contexto, não é necessário analisar de forma alguma o conteúdo ou as circunstâncias, para determinar a sua proteção pelo direito fundamental.

Em 30 de novembro de 2012, a Lei 12.737 de 2012, que define alguns crimes informáticos, incorporou ao Código Penal novas infrações penais brasileiras, como o artigo 154-A que disciplina a invasão de dispositivo informático; e o artigo 266, § 1º e 2º acerca da interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública.

Além disso, o artigo 151 do Código Penal disciplina sobre a violação de correspondência e impõe pena de 1 a 6 meses, ou multa, para quem intervier indevidamente no conteúdo da correspondência fechada, dirigida a outra pessoa, uma vez que o conteúdo das correspondências é inviolável em decorrência de norma constitucional.

Existem outras referências à tecnologia da informação na legislação brasileira, como a Lei 9.296 de 1996 que regulamenta as interceptações de comunicações telefônicas de qualquer natureza; a Lei 9.609 de 1998 que dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e outras providências; a Lei 9.983 de 2000 que faz a alteração do Código Penal, disciplinando crimes relacionados ao acesso aos sistemas informáticos da Administração Pública e a Lei 12.034 de 2009, que regulamenta o uso da internet no sistema eleitoral brasileiro.

Embora a finalidade da restrição de comunicações geralmente tenha um propósito positivo, isso não pode justificar um propósito excessivo, como uma forma de “obter a verdade real a qualquer preço”, uma vez que só é lícito descobrir a verdade quando isso for feito compatível com o respeito e garantia dos direitos fundamentais[[211]](#footnote-211).

Nesse sentido, essas restrições podem ser compatíveis com o respeito à dignidade e intimidade ou vida privada da pessoa humana, quando permitido intromissões, em princípio legítimas, na vida privada, se e somente se houver proporcionalidade entre o direito violado e a restrição feita, além da motivação da restrição, levando ao não estabelecimento de um poder aberto à intervenção das comunicações, que não podem ser permanentes, muito menos desmotivadas.

O principal mecanismo de controle da afetação aos direitos fundamentais em estudo é a autorização judicial prévia e, no caso do Brasil, uma vez realizado o procedimento de interceptação, o juiz deve decidir se os resultados são relevantes para a investigação.

Fala-se da ilegalidade da intervenção das comunicações telefônicas e interceptação de comunicação escrita, quando as disposições normativas estabelecidas para tais casos e que constituem resultados do mesmo como prova não são respeitadas, estaria diante de um comportamento que em muitos países foi reconhecido como crime dentro seus códigos penais.

Em relação à possibilidade de limitação de direitos fundamentais, Peces Barba[[212]](#footnote-212) destaca os limites dos fatos e os limites juridicos, sendo os operadores jurídicos responsáveis por incorporá-los ao ordenamento jurídico, considerando para cada caso o limite de cada direito, que em primeira ordem são encontrados no texto constitucional e na legislação com amparo constitucional, e os limites dos direitos em particular serão encontrados em resoluções judiciais.

Em um estado de direito, todos os tipos de investigação tem como limite o respeito aos direitos fundamentais das pessoas, que não são absolutos e permitem restrições, desde que dita restrição responde a um propósito superior, à investigação de ato criminoso que ameace a coexistência e a paz social, levando em consideração a proporcionalidade da medida restritiva.

Na esfera criminal, durante o processo de investigação que se utiliza de escutas telefônicas e escutas de comunicações escritas e telégrafos requeridas pelo Ministério Público, estas serão viáveis ​​na medida em que buscar a proteção de interesse superior ao direito afetado, tendo em mente que não é possível obter a verdade real a qualquer preço, uma vez que só é lícito descobrir a verdade quando isso for feito compatível com o respeito à dignidade, privacidade e vida privada da pessoa, sendo que a motivação defendida pelo juiz deve responder a tais critérios, influenciando a restrição de cada um dos direitos indicados.

Nessa esteira, fala-se em ilegalidade da intervenção das comunicações telefônicas e a interceptação de comunicações escritas ou telégrafos, em razão do não cumprimento dos dispositivos que regulam tal restrição e, em segundo lugar, quando não há motivação adequada e a argumentação do juiz que autorizou tal intervenção.

Com o fito de regular os excessos nas medidas de intervenção ao direito de dignidade, privacidade e vida privada da pessoa, no âmbito doutrinal e jurisprudencial estabeleceu princípios gerais que devem ser considerados na decisão judicial, que deve considerar a legalidade, motivação, proporcionalidade, necessidade, utilidade e adequação.

Nos princípios indicados, caberá ao juiz determinar a origem da medida de intervenção, devendo estabelecer como requisito principal o período de início e término da referida intervenção, que deve ser dentro de um período determinado razoável.

Quando o assunto em pauta são os crimes praticados no meio eletrônico, automaticamente há uma relação com os direitos e liberdades individuais da pessoa.

O ordenamento jurídico português, assim como no Brasil é fruto de uma evolução legislativa cautelosa. A princípio a Constituição portuguesa disciplina acerca dos dados informatizados no seu artigo 35, resguardando as pessoas quanto à utilização dos dados, restando disciplinada a proibição de acesso aos dados pessoais de terceiros, salvos em casos excepcionais previstos em lei.

Em razão da extrema necessidade de proteção dos direitos dos cidãdão o legislador teve que “transpor estes direitos para leis ordinárias, combinando a evolução tecnológica operada e os direitos dos cidadãos”[[213]](#footnote-213).

Com a revolução informática, aqueles crimes tipificados no Código Penal vigente na época (Decreto-Lei nº 400/82 de 23-09-1982) no Capítulo IV intitulado dos crimes contra a reserva da vida privada, passaram a ser insufucientes levando o legislador português a aprovar a Lei 10 de 29 de abril de 1991, a Lei da Proteção de Dados Pessoais face à Informática para abarcar as garantias asseguradas na Constituição.[[214]](#footnote-214)

Posteriormente, foi decretada a Lei 67 de 26 de outubro de 1998, conhecida como Lei de Proteção de dados pessoais, que trouxe em seu bojo tratamento dos dados pessoais e à livre circulação desses dados.

Nítida proteção aos direitos foi disciplinada no artigo 8° em seu n° 2 que permitia o tratamento dos dados pessoais relativos a suspeitas de atividades ilícitas e infrações penais poderia ser autorizado pela Comissão Nacional de Proteção de Dados, observadas as normas de proteção de dados e de segurança da informação, desde que não prevaleçam os direitos, liberdades e garantias do titular dos dados. Insta mencionar que esse diploma somente foi revogado pela Lei 58 de 08 de agosto de 2019.

No que tange à proteção da vida privada, destacou-se ainda a Lei 41 de 18 de agosto de 2004, alterada pela Lei 46 de 29 de agosto de 2012, que disciplina sobre o tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas e em seu artigo 4º resguardando os direitos dos cidadãos garantindo a inviolabilidade das comunicações e respetivos dados de tráfego realizadas através de redes públicas de comunicações e de serviços de comunicações eletrônicas acessíveis ao público.

Por fim, foi decretada em 17 de julho de 2008 a Lei n.º 32 com o objetivo de regular a conservação e a transmissão dos dados de tráfego e de localização relativos a pessoas singulares e a pessoas colectivas, bem como dos dados conexos necessários para identificar o assinante ou o utilizador registado, para fins de investigação, deteção e repressão de crimes graves por parte das autoridades competentes, sendo um ícone em matéria de obtenção da prova digital. A mencionada lei foi atualizada pela Lei 79 de 24 de novembro de 2021.

Sendo assim, cabe ao Estado garantir os direitos das pessoas, como a privacidade e a segurança, quando na utilização das tecnologias de comunicação e informação tais direitos forem ameaçados.

Pedro Dias Venâncio trouxe a conceituação da criminalidade informática abrangendo “toda a panóplia de atividade criminosa que pode ser levada a cabo por meios informáticos, ainda que estes não sejam mais que um instrumento para a sua prática, mas que não integra o seu tipo legal, pelo que o mesmo crime poderá ser praticado por recurso a outros meios” .[[215]](#footnote-215)

A Lei 109 de 17 de agosto de 1991 trouxe em seu bojo os crimes ligados à informática e suas respectivas penas. A mencionada lei foi revogada pela Lei 109 de 15 de setembro de 2009 que aprovou a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, adaptando o direito interno à Convenção sobre Cibercrime do Conselho da Europa.

Nesse sentido, a evolução da criminalidade lado a lado com as inovações tecnológicas evidencia a necessidade de o ordenamento jurídico, especificamente o direito processual penal a evoluir e passar por constantes alterações, criando normas legais e procedimentos para utilização das provas digitais nas investigações criminais, além de criminalizar os delitos praticados virtualmente e; garantindo ao mesmo tempo os direitos fundamentais dos cidadãos e a integralidade e força probatória quando da obtenção da prova digital.

# 2.5. A Proteção dos Dados Pessoais do Investigado em Portugal e no Brasil

Inicialmente, é imperioso afirmar que o direito à proteção de dados pessoais não é um direito absoluto; pode limitar-se, se necessário, para atingir um objetivo de interesse geral ou para proteger os direitos e liberdades dos outros.

Tanto o sistema organizacional português quanto o brasileiro têm por base, de forma aberta ou distretamente, a disponibilidade de informações de todo tipo e o volume de dados pessoais são recolhidos nas mais diversas áreas, que provavelmente vão além de qualquer ideia que se possa pré-conceber.

Esta (relativa) novidade corresponde à imposição de uma espécie de contrapoder atribuído de forma generalizada a todos os sujeitos particulares (se bem com a intervenção de órgãos públicos).

A Europa é a área geográfica onde a proteção da privacidade é maior e isso não se deve pelo fato de coletarem menos dados do que em outros lugares, mas sim pela simples razão de que pelo menos tem-se vindo a ganhar um poder de disposição sobre os dados que merecem mais atenção e preocupação, isto é, pode-se determinar as condições em que as informações pessoais se torna disponível para os outros[[216]](#footnote-216). Ou em outros termos, teoricamente as pessoas devem ser capazes de saber sobre si mesmas.

A proteção de dados não se refere, portanto, apenas à reserva com que devem ser tratados determinadas informações, mas caracteriza-se fundamentalmente pelo reconhecimento a todos os cidadãos de um poder de controle sobre seus próprios dados, a qualquer hora e em qualquer lugar.

Isso permite se falar em um poder de controle que do ponto de vista ativo tem um caráter individualizado, mas também difuso, e do ponto de vista passivo é dirigido contra todos os sujeitos que tenham dados pessoais.

Quando se tratar de mecanismos de persecução criminal, entre os quais incluímos o processo penal, parece evidente que essa faculdade de disposição deve ser enfraquecido, pois estar-se-á na presença de um interesse maior.

Lidar com a questão da proteção de dados na investigação criminal, obriga-se, portanto, a combinar dois elementos que, podem parecer antitéticos, pois compartilham a característica de serem fatores determinantes da aparência de implicações legais relevantes.

Da aparente luta entre estes dois elementos, mas também de suas implicações mútuas, deve-se extrair algumas conclusões que aspiram à validade geral, quais sejam: (i) a proteção de dados pessoais em sua dimensão de autodeterminação informativa, isto é, entendida como a faculdade de um sujeito de decidir o que é que outros saibam sobre ele; e (ii) a investigação criminal entendida como buscar o maior volume possível de informações sobre fatos (dados objetivos) e sobre seu suposto autor (dados pessoais).

O conflito entre ambos fica claro se for considerado que enfatizar o primeiro será necessariamente prejudicial para a segunda, uma vez que a fase de investigação criminal e obtenção da prova digital constituem ingerências contínuas no âmbito da tutela que promove todos os regulamentos de proteção de dados pessoais.

Assim, quando a polícia obtém as fontes de provas por meio de escutas telefônicas de conversas entre indivíduos sujeitos a investigação criminal, poderá ter sido violado o direito ao sigilo das comunicações regulamentado no artigo 5º, inciso XII[[217]](#footnote-217) da Constituição da República Federativa do Brasil de 1988 e no artigo 34º, 1[[218]](#footnote-218), da Constituição da República Portuguesa.

Por outro lado, com o acesso e visualização das informações mantidas em um aparelho telefônico, um disco de armazenamento portátil ou qualquer outro dispositivo eletrônico, poderia interferir com o direito à privacidade pessoal regulamentado nos dispositivos acima citados.

O acesso aos dados contidos em dispositivos eletrônicos afeta, sem dúvida, o direito à privacidade pessoal, mas também pode afetar o sigilo das comunicações, quando há um processo de comunicação, ou seja, quando dispositivos são usados ​​para transmitir informações entre um transmissor e um receptor através de redes de comunicação, como mensagens instantâneas ou por correio eletrônico.

Feitas essas breves ponderações sobre a proteção dos dados pessoais, é mister verificar como que cada ordenamento jurídico – Portugal e Brasil – se comportam na lida com tal direito fundamental.

Em Portugal, de forma vanguardista, consagrou no art.º 35.º da CRP, no texto de 1976, sob a rubrica “Utilização da informática”[[219]](#footnote-219), o direito à proteção dos dados pessoais informatizados.

Neste aspecto, em conformidade com o artigo 35º, n.º 3 tem-se que “a informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis”.

Assim sendo, os dados pessoais apurados e colhidos com estrita observação dos princípios da proporcionalidade e finalidade, o ordenamento jurídico português - n.º 1, do art.º 35.º da CRP- garante ao titular dos dados o direito de conhecer os propósitos a que se destina a sua recolha, devendo o processamento de recolha dos mesmos observar o cumprimento de três regras essenciais: o dever de informação, o dever de adequação e o dever de obtenção de consentimento prévio e esclarecido do interessado[[220]](#footnote-220).

Deste modo, passando-se ser mais considerável a existência de garantias contra o método e uso abusivo de dados pessoais informatizados, e a sua conciliação com diversos direitos, liberdades e garantias, o direito à autodeterminação informacional, previsto no artigo 35.º da CRP, aparece como o direito que cada indivíduo tem de controlar a informação disponível a seu respeito nas fases e obtenção, arquivamento, utilização e transmissão dos seus dados pessoais.

Após a previsão pioneira na Constituição da República Portuguesa, em 1991 adveio a primeira lei que tratou da proteção de dados pessoais face à informática, qual seja a Lei n.º 10/1991[[221]](#footnote-221), de 27 de abril.

E, por meio da Diretiva 95/46/CE, de 24 de outubro de 1995, do Parlamento Europeu e do Conselho, os princípios fundamentais da proteção de dados, que figuravam na Convenção n.º 108 do Conselho da Europa, seriam também previstos nesta Diretiva. Visava essa Diretiva conciliar o direito sobre a informação com o direito à circulação da informação, tendo influenciado o panorama do direito interno de todos os paíse da União Europeia, obrigando à adoção de legislação interna em matéria de proteção de dados pessoais, estimulando a uniformização do nível de proteção concedido por todos os Estados membros, visando alcançar um patamar de segurança comum[[222]](#footnote-222).

Com o passar do tempo, a matéria atinente à proteção de dados passou a ser prevista pela Lei n.º 67/98, de 26 de outubro, denominada de “Lei de Proteção aos Dados Pessoais” a qual revogou a Lei n.º 10/91, de 27 de abril, e transpôs para a ordem jurídica portuguesa a Directiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados[[223]](#footnote-223).

Importante mencionar que a Lei n.º 67/98, de 26 de outubro trouxe para o seu bojo o conceito de dados pessoais[[224]](#footnote-224) em seu artigo 3.º, alínea. a), como sendo “qualquer informação, de qualquer natureza e independentemente do respectivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável a pessoa que possa ser identificada directa ou indirectamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social”[[225]](#footnote-225).

Além das mencionadas leis, o ordenamento jurídico português ainda contempla outra no sentido de ampliar a proteção dos dados pessoais, onde é possível citar Lei n.º 41/2004, de 18 de agosto, que transpôs para a ordem jurídica nacional a Diretiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12/07, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas[[226]](#footnote-226); Lei n.º 5/2004, de 10 de fevereiro, denominada de Lei das Comunicações Eletrónicas, que estabelece o regime jurídico aplicável às redes e serviços de comunicações eletrónicas e aos recursos e serviços conexos, definindo as competências da autoridade reguladora nacional neste domínio[[227]](#footnote-227), no âmbito do processo de transposição das Directivas n.os 2002/19/CE, 2002/20/CE, 2002/21/CE, e 2002/22/CE, todas do Parlamento Europeu e do Conselho, de 7 de Março, e da Directiva n.º 2002/77/CE, da Comissão, de 16 de Setembro; Lei n.º 32/2008, de 17 de julho, que, transpondo a Diretiva n.º 2006/24/CE126, do Parlamento Europeu e do Conselho, de 15 de março, veio regular a conservação e transmissão dos dados de tráfego e localização, e os dados relevantes para a identificação do assinante ou o utilizador, garantindo a investigação e repressão de crimes graves, consagrando-se, desde logo, no n.º 2, do art.º 1.º, deste diploma, a proibição de conservação de dados que revelem o conteúdo das comunicações, sem prejuízo das exceções previstas na Lei[[228]](#footnote-228); e, por fim, tem-se o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, que é o novo Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia (UE), e estabelece as regras relativas ao tratamento, por uma pessoa, uma empresa ou uma organização, de dados pessoais relativos a pessoas na UE. Para além do reforço da proteção jurídica dos direitos dos titulares dos dados, o RGPD define novas regras e procedimentos do ponto de vista tecnológico[[229]](#footnote-229).

Diante deste quadro normativo de proteção de dados são consagradas alterações de fundo no que respeita ao tratamento de dados pessoais, contemplando-se, para além de um novo conceito de dados pessoais, um avolumado número de medidas com vista à proteção da privacidade pessoal, como é o caso do reforço dos direitos do titular dos dados, designadamente, o aprofundamento do direito à transparência e do direito de informação e acesso aos dados pessoais, consubstanciado na exigência de maior rigor no tipo de informações a prestar ao titular dos dados e pelo incremento dos requisitos do consentimento, prevendo-se regras especiais de tutela de dados de menores[[230]](#footnote-230).

No Brasil, a proteção dos dados pessoais caminha ‘a passos lentos’. Iniciando-se com a Lei n.º 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet. Esta lei também instituiu especificamente dois meios de obtenção de provas, a conservação expedita de dados e a injunção sobre terceiros para a apresentação de dados.

Em seguida, adveio a Lei n.º 13.709, de 14 de agosto de 2018, denominada de Lei Geral de Proteção de Dados Pessoais. Esta lei representa um marco histórico na regulamentação sobre o tratamento de dados pessoais no Brasil, tanto em meios físicos quanto em plataformas digitais.

Além de mudar a maneira como instituições privadas coletam, armazenam e disponibilizam informações de usuários, a LGPD é destinada às instituições públicas – portanto, deve ser seguida por União, estados, Distrito Federal e municípios[[231]](#footnote-231).

E, somente em 10 de março de 2022, o Congresso Nacional brasileiro promulgou a Emenda Constitucional n.º 115, que inclui a proteção de dados pessoais entre os direitos e garantias fundamentais, além disso restou fixada a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

Restou assim disposta a proteção de dados na CRB: “art. 5º, inciso LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais”[[232]](#footnote-232). Como se vê, somente agora é que o Brasil alçou a proteção de dados pessoais à positivação constitucional.

Verifica-se, portanto, em Portugal e no Brasil, há mecanismos que facilitam a troca de informações durante a investigação criminal[[233]](#footnote-233), com o objetivo de alcançar uma maior eficácia no combate ao crime, no entanto, estes mecanismos não foram acompanhados, paralelamente, por novos instrumentos de proteção de dados pessoais que garantem que esta troca de informações é realizada com total respeito à privacidade das pessoas.

Em outras palavras, houve uma evolução para aumentar a eficácia da investigação criminal, mas não evoluiu ou aumentou, da mesma forma, a proteção de dados pessoais que são tratados de maneira diferentes pelos ordenamentos jurídicos.

# 3. Da Afronta aos direitos fundamentais pelas provas digitais

Apesar de nas seções expostas ter sido feita referência à obtenção de informações contidas em dispositivos eletrônicos por meio do exame dos mesmos com a correspondente perícia, se for o caso, bem como obter informações através do agente disfarçado, ou do exame dos dados arquivados em dispositivos eletrônicos, fica evidente que não são as únicas formas de acessar as informações ou dados que puderem ter especial relevância para a investigação criminal.

Assim, existem outros meios de investigação criminal, como a intercepção de comunicações, a gravação direta de comunicações orais, bem como a captura da imagem ou uso de dispositivos de rastreamento e geolocalização, igualmente adequados para a realização investigação criminal.

Nesta seção, examinar-se-á a possibilidade das provas digitais advindas de medidas de investigação criminal poderem violar os direitos fundamentais do investigado. Para chegarmos a este ponto da dissertação foi necessário passar pela análise das novas tecnologias de informação e comunicação e os direitos fundamentais; verficar a previsão legal dos denominados cibercrimes; tivemos que manifestar sobre a prova digital, e, por fim analisar a questão do uso da tecnologia na investigação criminal, passando-se pelo estudo dos chamados métodos ocultos de investigação criminal.

Coerentemente, Manuel Monteiro Guedes Valente afiança que “a criminalidade digital exige uma especial atenção por parte do sistema e justiça criminal. Mas impõe que essa atenção não abdique dos valores cuja conquista custaram sangue, porque nem sempre os fins fustificam os meios”[[234]](#footnote-234).

Tanto no ordenamento jurídico brasileiro quanto no português, há entendimento de que os direitos fundamentais poderão ser restringidos de forma excepcional, sendo certo que tais restrições deverão partir de normas legais.

Dito isso, é imperioso afirmar que a prova digital assume uma situação de agressividade e de lesividade aos direitos fundamentais, pois, ao utiliza-la como meio de prova ou como instrumento para sua obtenção, tem-se o risco de ofensa ou restrição aos ditos direitos.

Benjamim Silva Rodrigues afirma categoricamente que ao fazer uso da prova digital há um risco imenso de ofender direitos constitucionalmente salvaguardados, tais como o direito à palavra, o Direito à imagem, (Art. 26º da CRP) o Direito à autodeterminação informacional e da comunicação, o Direito à inviolabilidade do domicílio informático (Art. 34.º da CRP), o direito à reserva da intimidade da vida privada e familiar, e muitos outros que em resultado da utilização da prova digital, são ofendidos[[235]](#footnote-235).

Verifica-se, portanto, um choque de interesses, pois, de um lado tem-se os direitos fundamentais da pessoa e de outro os objetivos e finalidades do processo penal e o *ius puniendi* do Estado.

Neste mesmo caminho, se faz necessária a retomada dos ensinamentos de Manuel Monteiro Guedes Valente, para quem:

(...) o desejo de uma justiça célere e veloz, que satisfaça o clamor dos cidadãos, que se encontram em estado paneónico – medo esquizofrénico – perante os fenómenos da criminalidade económico-financeira [v. g., crimes tributários (fiscais e previdenciários), manipulação de mercado, corrupção, branqueamento], do crime organizado transnacional [v. g., crime de tráfico de armas, de droga, de seres humanos e de órgãos humanos] e do terrorismo, conduziram os decisores políticos a implementar meios de obtenção de prova especializados, especiais e excecionais: ampliação do âmbito das interceções telefónicas, registo de voz off e imagem, gravações ambientais, gravações e fotografias por meio de câmaras de videovigilância, agentes infiltrados física e digitalmente, rastreios e persecuções digitais, localizações celulares, controlo e monitoramento concreto de IP, IMEI e GPS, recurso a IMSI-Carther (IMEI), buscas e apreensões preventivas no sistema digital a nível nacional, regional e internacional sem qualquer conhecimento do visado, e a admissibilidade e utilização como meios de prova os relatórios elaborados pelos serviços secretos[[236]](#footnote-236).

Diante de tais constatanções, o citado autor português conclui que “por essa razão, consideramos que o recurso a meios excecionais de investigação criminal ou a metodologias de obtenção de informação e prova criminal deve estar previsto e legislado, mas submetido desde logo ao princípio da excecionalidade. O que é excecional não é nem pode ser vulgar”[[237]](#footnote-237).

Existe uma similitude entre as Constituições Federais – Brasil[[238]](#footnote-238) e Portugal[[239]](#footnote-239) – pertinente às inúmeras formas de garantir a defesa dos direitos e garantias fundamentais, inclusive inserindo limites à validade dos meios de prova e de obtenção de prova.

Desta forma, é totalmente possível verificar a presença de diversos limites e tutelas constitucionais previstos, à qualquer tipo de procedimentos ou instrumentos, suscetíveis de violar ou agredir os direitos fundamentais.

Atinente às restrições dos direitos fundamentais, é importante mencionar que estes são uma posição jurídica positivada que buscam tutelar e proteger a sociedade e o indíviduo das forças do Estado.

Em outras palavaras, os direitos fundamentais possibilitam aos cidadãos possuir uma garantia de que determinada proposta legislativa, medida judicial ou ação criminal, não poderá se materializar, caso venha afrontar um ou mais direitos fundamentais.

Entrentanto, como visto acima, os direitos fundamentais não são de todos absolutos, haja vista que possuem limitações internas, isto é, uma garantia de igualdade entre os cidadãos, de forma que, todos tenham o mesmo acesso e tenham protegidos os seus direitos.

Jorge Gouveia Bacelar assevera com acuidade que “não seria de todo possível a vida colectiva e em sociedade, caso não fossem previstos mecanismos de limitação material dos direitos fundamentais genericamente proclamados, com o propósito originário de garantir a própria permanência da respectiva tipologia no seu conjunto”[[240]](#footnote-240).

Então, para a ocorrência de restrição aos Direitos Fundamentais, se faz necessária competência especial para se concretizar. Em se tratando dos direitos, liberdades e garantias, o artigo 165º 1) b) da CRP, com a rubrica “Reserva relativa da competência legislativa”, que é da exclusiva competência da Assembleia da República legislar, salvo autorização do governo, em matéria de Direitos, Liberdades e Garantias.

Nesta oportunidade, se faz imperioso argumentar sobre os riscos da utilização da prova digital sem o devido controle.

Como visto, a prova digital é fundamental para elucidação de determinados crimes, em especial os chamados cibercrimes, sendo ela um elemento imprescindível, sendo certo também, que ela poderá se apresentar como um risco aos direitos fundamentais quando utilizada sem o devido controle.

Foi possível verificar nas páginas anteriores, seja em razão da natureza ou do formato da prova digital, a sua recolha – apreensão – que muito provavelmente ocorra em ambientes privados, tem este a proteção da lei.

Desta forma, a recolha da prova digital para a investigação criminal que não tenha o devido controle ou que não obedece às determinadas regras, possibilitará que incontáveis pessoas tenham acesso às informações privilegiadas, violando-se desta maneira, os direitos e garantias fundamentais tutelados constitucionalmente.

Para finalizar, importante citar os ensinamentos de Joaquín Delgado Martín, o qual afirma que um dado incontestável é que as provas digitais são potencialmente vulneradora de direitos fundamentais, tais como o direito à intimidade, o direito de imagem, o sigilo das comunicações, a proteção de dados, entre outros[[241]](#footnote-241).

Segue o autor espanhol asseverando que a doutrina tem alcançado um certo consenso na inexistência de um determinismo tecnológico, de modo que, hoje se entende que as provas digitais não são más ou boas *por si,* sendo que dependerá do uso que ser fará das mesmas[[242]](#footnote-242).

Para concluir que realmente os direitos fundamentais estão vulneráveis perante as provas digitais, é mister afirmar que o fato de se ampliar, agilizar e amparar os meios de investigação criminal na consecução da prova digital, mostra-se ainda mais ofensivo, lesivo e temerário do que realiza-lo em relação às provas clássicas.

Neste mesmo sentido, tem-se a afirmação levada a efeito por Renato Lopes Militão de que “pelas pelas próprias características e potencialidades das NTIC, a concretização de tais medidas ofende, acrescida e gravemente, múltiplos direitos, liberdades e garantias, não só dos agentes dos crimes mas também, pelo menos em boa parte dos casos, de suspeitos inocentes ou terceiros acidentais”.

Vale a pena mencionar aqui, para finalizar esse ponto da dissertação, os ensinamentos de Benjamim Silva Rodrigues, para quem “o direito à palavra, o direito à imagem, o direito à autodeterminação informacional, o direito à reserva da intimidade da vida privada e familiar, o «direito à inviolabilidade do domicílio informático (artigo 34.º, da CRP) que nos surge como uma garantia imprescindível da afirmação do direito à autodeterminação informacional e comunicacional e tantos outros direitos pessoalíssimos são em regra enormemente lesados por aquelas acções. Mas também o podem ser, e são-no bastas vezes, direitos patrimoniais, desde logo o direito de propriedade”[[243]](#footnote-243).

Como visto acima, há uma série de princípios norteadores para que sejam observados ao se adotar qualquer diligência de investigação que, na prática possa prejudicar os direitos fundamentais da pessoa, sendo que os ordenamentos jurídicos brasileiro e português autorizam a possibilidade de restringir esses direitos fundamentais, desde que cumpram uma finalidade legítima e que, graças a esta limitação, se obtém um interesse socialmente benéfico relevante.

Não se olvida que, qualquer limitação de direitos deve ser adotada em relação às garantias mínimas que garantem a confiabilidade do meio, a saúde e a integridade da pessoa investigada.

#

# CONCLUSÃO

A Constituição Brasileira e a Constituição Portuguesa possuem diversos pontos comuns no que se refere aos direitos fundamentais, em que restaram reconhecidas prerrogativas básicas inerentes ao homem (como a vida, liberdade, educação, saúde); embora existam algumas divergências doutrinárias em alguns pontos.

O objetivo da discussão foi mostrar que a tecnologia abriu caminho para evidências na mídia eletrônica antes mesmo da disciplina legislativa, uma vez que as provas são grandes pontos de contato entre o processo e a realidade externa, cujo desenvolvimento segue necessariamente.

 A produção das provas digitais depende, se os direitos disputados não estiverem disponíveis, também no processo penal, ou se a reprodução for contestada, da garantia de uma prova correta, de autenticidade e integridade por meios técnicos apropriados, caso contrário, a prova obtida de uma fonte digital não tem valor probatório.

No caso específico de extratos digitais de bases de dados, a garantia de autenticidade e integridade depende na observância da formação do conteúdo na fonte em um processo de extração documentado que pode ser autenticado pelo editor, sob pena de responsabilidade civil e criminal; não se permitindo que imagens digitais sejam coletadas sem qualquer esclarecimento, cuidado ou segurança.

Em relação à fonte das provas, não é dispensada a necessidade de técnica pericial para a sua produção, quando apreendidos materiais durante a investigação para a verificação da autenticidade, garantia da integridade por meio do monitoramento da tecnologia utilizada e da observação da cadeia de custódia, para o manuseio do material para fins probatórios, resguardados os direitos e garantias individuais da pessoa investigada.

Conforme mencionado, a prova digital caracteriza-se, dentre outras formas, por sua volatilidade e fragilidade, ou seja, requer manuseio técnico qualificado para que seja produzida, sob pena de alteração ou perda de todos os dados ou informações captadas e de relevância para a prova do fato.

Portanto, o processo penal, como um sistema que tem por fundamento e limite, a dignidade da pessoa humana, principalmente à integridade da pessoa; na tentativa de amenizar a desigualdade das armas entre o Estado e o indivíduo busca o equilíbrio (entenda-se justa ponderação) entre o interesse do Estado na prossecussão penal dos culpados e ao mesmo tempo, a tutela adequada dos direitos fundamentais e garantias processuais da pessoa.

Diante disso, especificamente as interceptações telefônicas, prova digital de grande impostância nas investigações criminais, por representarem um impacto direto na vida privada das pessoas, devem; portanto, ser expressamente prevista em lei, que deve estabelecer com clareza e precisão detalhes sobre os procedimentos e âmbito da medida de intervenção, as circunstâncias em que eles podem ser usados, o procedimento a seguir entre outros elementos que detalhem sua execução, monitoramento e utilização, sob pena de nulidade, em razão da ofensa aos direitos e garantias individuais do investigado.

Finalmente, conforme observado na pesquisa o Brasil só veio a decretar uma lei ampla sobre a proteção de dados em 2018, com a Lei n. 13.709, de 14 de agosto (Lei Geral de Proteção de Dados),

Restou evidenciado que os principais países europeus possuem suas legislações sobre proteção de dados há tempos, atualizadas de acordo com os progressos alcançados pela União Europeia.

Não obstante, notou-se ainda que Portugal é um dos pioneiros no que se refere à proteção de dados pessoais, com a Constituição da República de 1976, que foi de grande influência para a Constituição da República Federativa do Brasil de 1988, quando estabeleceu ampla proteção à privacidade e intimidade, ao domicílio, às comunicações pessoais e aos dados pessoais.

No que se refere à colisão de normas acerca das investigações criminais, as regras da ponderação permitem orientar racionalmente a busca da solução mais correta para o caso concreto, utilizando-se ainda dos princípios contitucionais, como o da proporcionalidade que assume importante função como norteador pelo aplicador do direito, uma vez que concilia dois valores primordiais: a segurança jurídica e a justiça.

A Constituição da República Portuguesa prevê o princípio da proibição do excesso, devendo-se observar os critérios da adequação, necessidade e proporcionalidade, não podendo as normas restritivas dos direitos, liberdades e garantias “diminuir a extensão e o alcance do conteúdo essencial dos preceitos constitucionais que os consagram”, conforme disciplina os artigos 17 e 18. Insta salientar que, essas limitações de direitos somente se darão em situações de clara e indispensável necessidade.

Ora, a investigação criminal aliada à inovação tecnológica, que está em constante mudança e desenvolvimento, implica diretamente na lesão de direitos, liberdades e garantias dos suspeitos, sejam eles criminosos ou inocentes, e até de terceiros. Caberá ao Estado-Juiz defender o direito dos cidadãos, que ficarão completamente expostos em eventual investigação criminal.

Em suma, a LGPD inovou no ordenamento jurídico brasileiro, tratando-se, de enorme avanço jurídico no Brasil, ao disciplinar normas específicas para o tratamento de dados. Contudo é evidente que Portugal possui um aparato normativo bem mais amplo, com uma infinidade de legislações e dispositivos que regulamentam o tema e que melhor protegem o cidadão.

# REFERÊNCIAS

ABEL LLUNCH, Xavier; PICÓ I JUNOY, Joan, et al. **La prueba electrónica**. Barcelona: Bosch, 2011. ISBN: 978-84-7698-955-5.

ALVES. Nadia Castro. Colisão de direitos fundamentais e ponderação. **Meritum.** Belo Horizonte, v. 5, n. 1, p. 25-48, jan./jun. 2010.

ANDRADE, Manuel da Costa. **Bruscamente no Verão passado – A reforma do Código de processo penal.** Coimbra: Coimbra Editora, 2009. ISBN 9789723217261.

AZEVEDO, Camilo Chianca de Oliveira. **Proteção constitucional à privacidade em face da liberdade de informação: aplicação imediata dos direitos fundamentais nas relações privadas.** 2009. 83 f. TCC (Graduação) - Curso de Direito, Ciências Sociais Aplicadas, Universidade Salvador, Salvador, 2009. Cap. 3. Disponível em: http://www.conteudojuridico.com.br/monografia-tcctese,prote cao-constitucional-a-privacidade-em-face-da-liberdade-de-informacao-aplicacao-imediata-dos-direitosfund,5523 1.html>. [Consult. 30 abr. 2021].

BENGER, Vincent. **Jurisprudencia de la Cour Européenne des Droit de L´Homme.** 5.ed. Sirey: Francia, 1996.

BENTHAM, M. Jeremías. **Tratado de las Pruebas Judiciales**. París: Bossange Frerres, 1825, p 19. Antônio Pereira Gaio Júnior, Bruno Augusto Sampaio Fuga, William Santos Ferreira (orgs). ISBN 978-65-86300-86-4. Disponível em: http://cdigital.dgb.uanl.mx/la/1080045433\_C/1080045433\_T1/1080045433\_MA.PDF

BITTAR, 1994, p.107 apud GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. **Novo curso de direito civil**. 11ª ed. São Paulo: Saraiva, 2009, volume 1. ISBN 978-6555594461.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**: promulgada em 5 de outubro de 1988. [Em linha] [Consult. 22 Mar. 2022]. Disponível em: http://www.planalto.gov.br/ccivil\_03/constituicao/constituicao.htm

\_\_\_\_\_\_\_\_\_\_\_. Supremo Tribunal Federal. Habeas Corpus n° 91.867/PA. Relator Min. Gilmar Mendes. Acórdão de 24 de abril de 2012. **Diário de Justiça Eletrônico**. Brasília, 2012. [Consult. 17 dez 2019] Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=27923

\_\_\_\_\_\_\_\_\_\_\_. Supremo Tribunal Federal. **Recurso Extraordinário 625263/PR**. Relator Gilmar Mendes. [Em linha] Brasília, 13 de junho de 2013. [Consult. 23 Mar. 2022] Disponível em: https://redir.stf.jus.br/paginadorpu b/paginador.jsp?docTP=TP&docID=4472381.

BRAVO, Rogério, **As Tecnologias de Informação e a Compressão dos Direitos, Liberdades e Garantias: os efeitos das regras “10/10” e “1/1”.** [Em linha] Lisboa, 2012. [Consult. 20 jan. 2021]

BRENNER, S., “At light speed: attribution and response to cybercrime/terrorism/Warfare”, **Journal of Criminal Law & Criminology**, 2007, nº97, p. 379.

BUENO DE MATA, Federico. **Prueba electrónica y proceso 2.0.** Valencia: Tirant lo Blanch, 2014. ISBN: 978-84-9053-483-0.

CABRAL, Antonio do Passo. A eficácia probatória das mensagens eletrônicas. **Revista de Processo,** São Paulo, v. 31, n. 135, p. 97-131, 2006, p. 102.

CARNELUTTI, Francesco; AUGENTI, Giacomo P. **A prova civil.** Lisa Pary Scarpa (trad). Campinas: Bookseller, 2005. ISBN: 8574683515, 9788574683515.

CARTA dos Direitos Fundamentais da União Europeia. **Jornal Oficial da União Europeia**. [Em linha]. [Consult. 26 nov. 2020]. Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:12016P/TXT>.

CASEY, Eoghan. **Digital evidence and computer crime: forensic science, computers and the internet.** 3rd ed. [s.l] Elsevier, 2011. ISBN 978-0-12-374268-1, p. 191.

CASTRO, Catarina Sarmento e. **Direito da informática, privacidade e dados pessoais**. Coimbra: Almedina, 1ª ed. 2005. ISBN-13: 978-9724024240.

CASTROVERDE, Córdoba Diego; GIMÉNEZ, Ignácio Diez-Picazo. Reflexiones sobre los retos de la protección de la privacidad en un entorno tecnológico. In: **El derecho a la privacidad en un entorno tecnológico.** [Em linha] Madrid, 2016. [Consult. 19 Mar. 2022] Disponível em: https://www.tribunalconstitucional.es/es/publicaciones/Publicaciones/ALTC-Jornada-20.pdf

CRATO, Nuno Teixeira. **The Walking Virtually Dead: Entre uma Algoritmocracia Jus Constituendum e um Homem Virtual Transparente, Existe Espaço para o Direito a uma Identidade Informacional?** Lisboa: Universidade de Lisboa, 2016. 136 f. Tese de Mestrado em Segurança da Informação e Direito no Ciberespaço, p. 34.

CLÍMACO VALIENTE, Ernesto. **Génesis histórico-normativa del derecho a la protección de los datos personales desde el derecho comparado a propósito de su fundamento.** [Em linha] 2012 [Consult. 18 Mar. 2022] Disponível em: https://e-archivo.uc3m.es/handle/10016/18785#preview.

COMISSÃO das Comunidades Europeias. **Comunicação da Comissão ao Parlamento Europeu, ao Conselho e ao Comité das Regiões: Rumo a uma política geral de luta contra o cibercrime.** [Em linha] Bruxelas, 22 Mai. 2007 [Consult. 29 Jan 2022] Disponível em https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX:52007DC0267.

CONDE, Francisco Muñoz. **Em búsqueda de la verdade em el processo penal**. Buenos Aires: Hammurabi, 2007.

CONVENÇÃO para a Protecção dos Direitos do Homem e das Liberdades Fundamentais. [Em linha] Roma, 2022. (4 Nov. 1950) [Consult. 08 Mar. 2022] Disponível em https://www.echr.coe.int/documents/convention\_por.pdf.

CONVENÇÃO sobre o cibercrime. [Em linha] Budapeste, 23 de Nov. 2001 [Consult. 12 Fev. 2022] Disponível em: https://rm.coe.int/16802fa428.

COOLEY, Thomas McIntyre. **A Treatise on the Constitutional Limitations which rest upon the legislative power of the States of the American Union.** Little, Brown & Co: Boston, 1868. [Em linha] [Coonsult. 17 Mar. 2022] Disponível em: https://repository.law.umich.edu/books/10/.

COSTA, José Francisco de Faria, **Algumas reflexões sobre o estatuto dogmático do chamado “Direito Penal Informático”, Direito Penal da Comunicação, alguns escritos**. Coimbra Editora, 1998. ISBN 972-32-0850-4

COUTURE, Eduardo Juan. **Fundamentos del Derecho Procesal Civil.** 4.ed. Buenos Aires: B de F, 2002. ISBN 987-10-890-58.

DECLARAÇÃO Universal dos Direitos Humanos. 10 de dezembro de 1948. [Em linha] [Consult. 19 Mar. de 2022]. Disponível em: https://brasa.org.br/declaracao-universal-dos-direitos-humanos/?gclid=Cj0KCQjw1PSDBhDbARIsAPeTqrfRLDqHzL\_deuqOryQjJHC2jl\_ 93jSN2Zme\_t-QDig0gFBQxMaor84aAm12EALw\_wcB.

DELGADO, Joaquín Martín. La prueba del whatsapp. **Diario La Ley**, núm. 8605, Sección Tribuna, 15 Sep.2015, Ref. D-331, Editorial LA LEY [Em linha] [Consult. 23 Mar. 2022] Diisponível em: https://docplayer.es/25786992-La-prueba-del-whatsapp-joaquin-delgado-martin-magistrado-de-la-audiencia-pr ovincial-de-madrid-doctor-en-derecho.html.

DIAS, Jorge de Figueiredo, **Clássicos Jurídicos: Direito Processual Penal.** Coimbra: Coimbra Editora, 2004, ISBN 972-32-1250-1.

DIAS, Vera Elisa Marques. **A problemática da investigação do Cibercrime.** [Em linha] [Consult. 29 Jan. 2022] Disponível em <http://www.datavenia.pt/ficheiros/edicao01/datavenia01_p063-088.pdf>.

DIDIER JÚNIOR, Fredie; BRAGA, Paula Sarno; OLIVEIRA, Rafael Alexandria de. **Curso de direito processual civil.** 11. ed. Salvador: Jus Podivm, 2016. v. 2. ISBN 978-85-442-0663-8.

DOMINGOS, Fernanda Teixeira Souza; RÖDER, Priscila Costa Schrenir. Obtenção de provas digitais e jurisdição na Internet. **Investigação e prova nos crimes cibernéticos**. São Paulo: EMAG, 2017. ISBN 978-85-98004-04-4.

FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito da Universidade de São Paulo**, v. 88, p. 439-459, 1993.

FRAGOSO, Nathalie; RODRIGUES, Gabriel Brezinski. Dossiê: Privacidade e proteção de dados pessoais na segurança pública e no processo penal. **Revista Direito Público**, Brasília, Volume 18, n. 100, 581-605, out./dez. 2021. ISSN 2236-1766.

FROTA, Hidemberg Alves da. **A proteção da vida privada, da intimidade e do segredo no Direito brasileiro e Comparado**. Anuario de Derecho Constitucional Latinoamericano, Montevideo, v. 13, n. 1, t. 2, p. 459-495, ene.-dic. 2007. Disponível em: <https://revistas- colaboracion.juridicas.unam.mx/index.php/anuarioderecho-constitucional/article/download/30 386/27425 >. [Consult. 30 abr. 2021].

GARCIA, Jesús Maria González. El proceso penal español y la prueba ilícita: Spanish criminal procedure and the illegal evidence. **Revista de Derecho**, vol. XVIII, n° 2, (Diciembre 2005), p. 187-211. ISSN 0718-0950.

GOUVEIA, Jorge Bacelar. **Manual de Direito Constitucional**. Coimbra: Almedina, 2016. ISBN 978-9724067964.

GONZÁLEZ, Nicolás Cuéllar Serrano. Garantías constitucionales en la persecución penal en el entorno digital. In: **Derecho y Justicia penal en el Siglo XXI. Liber amicorum en homenaje al Profesor Antonio González-Cuéllar García**. Madrid: Colex, 2006. ISBN 84-8342-047-3.p. 887-916.

GRANCE, T.; CHEVALIER, S.; SCARFONE, K..; DANG, H. **Guia para Integração de Técnicas Forenses em Resposta a Incidentes, Publicação Especial.** Instituto Nacional de Padrões e Tecnologia. [Em linha]. Gaithersburg, MD, 2006 [Consult. 12 Mar. de 2022] Disponível em: https://tsapps.nist.gov/publication/get\_pdf.cfm?pub\_id=50875

INSA MÉRIDA, Fredesvinda; LÁZARO HERRERO, Carmen; GARCÍA GÓNZALEZ, Nuria. **Pruebas electrónicas ante los tribunales en la lucha contra la cibercriminalidad. Un proyecto europeo.** [Em Linha] [Consult. 28 Fev. 2022] Disponível em: http://www.scielo.org.ve/scielo.php?script=sci\_arttext&pid=S1690-75152008000200009.

JONES, M. Jackson. **The Fourth Amendment and Search Warrant Presentment: Is a Man's House Always his Castle.** [Em linha] 2011 [Consult. 17 Mar. 2022] Disponível em: https://heinonline.org/HOL/LandingPage?handle=hein.journals/amjtrad35&div=37&id=&page=

KENT JR, Michael B. **Pavesich, Property and Privacy: The Common Origins of Property Rights and Privacy Rights.** [Em linha] 2009 [Consult. 17 Mar 2022] Disponível em: https://scholarship.law.campbell.edu/cgi/viewcontent.cgi?article=1077&context=fac\_sw.

KIST, Dario José. **Prova digital no processo penal**. Leme: JH Mizuno, 2019, p. 384. ISBN 978-85-7789-430-7.

LEI n.º 05/04. **Diário da República Série I**-A n.º 34/2004 (10-02-2004), p. 788 – 821 [Em linha] [Consult. 21 Mar. 2022]. Disponível em: https://dre.pt/dre/detalhe/lei/5-2004-581061.

LEI n.º 32/08. **Diário da República Série I**-A n.º 137/2008 (17-07-2008), p. 4454 – 4458 [Em linha] [Consult. 21 Mar. 2022]. Disponível em: https://dre.pt/dre/detalhe/lei/32-2008-456812

LEI n.º 41/04. **Diário da República Série I**-A n.º 194/2004 (18-08-2004), p. 5241 – 5245 [Em linha] [Consult. 21 Mar. 2022]. Disponível em: https://dre.pt/dre/detalhe/lei/41-2004-480710.

LEI n° 79 de 24 de novembro de 2021. [Em linha] **Diário da República Eletrónico n° 228/2021. Série** I de 2021-11-24. p. 09-38. [Consult. 20 jan.2022] Disponível em: https://data.dre.pt/eli/lei/109/2009/p/cons/2021112 4/pt/html.

LEI n.º 67/98. **Diário da República Série I**-A n.º 247/1998 (26-10-1998), p. 5536 – 5546 [Em linha] [Consult. 21 Mar. 2022]. Disponível em: https://data.dre.pt/eli/lei/67/1998/10/26/p/dre/pt/html https://dre.pt/dre/detalhe/lei/67-1998-239857.

LEI n° 109 de 15 de setembro de 2009. [Em linha] **Diário da República Eletrónico n°179/2009. Série** I de 2009-09-15. [Consult. 20 jan.2022] Disponível em: https://data.dre.pt/eli/lei/109/2009/p/cons/20211124/pt/html

LEI nº 8078 de 11 de setembro de 1990. [Em linha] **Diário Oficial da União**. Brasil, 2022. [Consult. 22 jan.2022] Disponível em: http://www.planalto.gov.br/ccivil\_03/leis/8078compilado.htm

LEI nº 8137 de 27 de dezembro de 1990. [Em linha] **Diário Oficial da União**. [Consult. 22 jan.2022] Disponível em: http://www.planalto.gov.br/ccivil\_03/leis/l8137.htm

LEI nº 9296 de 24 de julho de 1996. [Em linha] **Diário Oficial da União.** Seção 1 – 25/7/1996, p. 13757. [Consult. 20 jan.2021] Disponível em: [https://www2.camara.leg.br/legin/fed/lei/1996/lei-9296-24-julho-1996-349049-publicacaoori ginal-1-pl.html](https://www2.camara.leg.br/legin/fed/lei/1996/lei-9296-24-julho-1996-349049-publicacaoori%20ginal-1-pl.html)

LEI nº 9609 de 19 de fevereiro de 1998. [Em linha] **Diário Oficial da Uni**ão. Brasil, 2022 [Consult. 24 jan.2022] Disponível em: http://www.planalto.gov.br/ccivil\_03/leis/l9609.htm

LEI n°13.709 de 14 de agosto de 2018. [Em linha] **Diário Oficial da União.** [Consult. 22 jan.2022] Disponível em: de http://www.planalto.gov.br/ccivil\_03/\_ato2015-2018/2018/lei/l13709.htm

LEI n° 14155 de 27 de maio de 2021. [Em linha] **Diário Oficial da União**. [Consult. 20 jan.2022] Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/Lei/L14155.htm>

MALAN, Diogo. Métodos ocultos, devido processo e o enfrentamento à criminalidade organizada. In: **Direitos fundamentais e processo penal na era digital: doutrina e prática em debate.** [Em linha] São Paulo: InternetLab, v. 4, 2021. [Consul. 21 Mar. 2022] ]Disponível em: https://congresso.internetlab.org.br/livros/.

MALATESTA, Nicola Framarino dei. **A lógica das provas em matéria criminal.** Campinas:Russell Editores, 2009, ISBN 978-85-89251-75-4.

MARINONI, Luiz Guilherme; ARENHART, Sérgio Cruz. **Prova.** 2. ed. São Paulo: Revista dos Tribunais, 2011. ISBN 9788520340165.

MARQUES, José Frederico. **Elementos de direito processual penal.** 2.ed. Campinas: Millennium, 2000. ISBN 858-6833-142.

MARQUES, Garcia; MARTINS, Lourenço. **Direito da Informática**. 2ª ed. Coimbra: Almedina, 2006. ISBN 978-9724028590.

MARTINEZ, Gregorio Peces-Barba. **Curso de Derechos Fundamentales.** Universidad Carlos III, Boletín del Estado, Madrid, 1995. ISSN 0213-9995.

MEIREIS, Manuel Augusto. Homens de confiança. Será o caminho? In: **II Congresso de processo penal. Memórias.** Manuel Monteiro Guedes Valente (coord). Coimbra: Almedina, 2006, p. 81-101. ISBN 972-40-2814-3.

MILITÃO, Renato Lopes. A propósito da prova digital no processo penal. **Revista da Ordem dos Advogados**, Lisboa, Ano 72, vol. 1 (Janeiro-Março 2012), p. 247-285.

MINUTA do Relatório Explicativo da Convenção sobre o cibercrime. [Em linha] [Consult. 18 Mar. 2023] https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Docum ents/Convention%20and%20protocol/ETS\_185\_Portugese-ExpRep.pdf

MIRANDA, Jorge; MEDEIROS, Rui. **Constituição Portuguesa Anotada**. 2.ed. Wolter Kluwer: Coimbra Editora, 2010. ISBN: 978-97-2321-82-2-0.

NEVES, Rosa Vieira. **A Livre Apreciação da Prova e a Obrigação de Fundamentação da Convicção (na Decisão Final Penal)** 1.ª ed. Coimbra: Coimbra Editora, 2011, ISBN 978-972-32-1929-6.

NIEVES Saldaña, M. The Right to Privacy. La génesis de la protección de la privacidad en el sistema constitucional norteamericano: el centenario legado de Warren y Brandeis. **Revista De De-recho Político**, 85, 195-240, 2012.

NUCCI, Guilherme de Souza. **Manual de Processo Penal.** 8.ed. São Paulo: Revista dos Tribunais, 2011. ISBN 978-852-034-07-52.

NUNES, Duarte Rodrigues. **Os meios de prova previstos na Lei do Cibercrime**. Coimbra: Gestlegal, 2018, ISBN 9789898951847.

PASTORE, Guilherme de Siqueira. Considerações sobre a autenticidade e a integridade da prova digital. **Cadernos Jurídicos**, São Paulo, ano 21, nº 53, p. 63-79, Janeiro-Março/2020.

PECES-BARBA MARTINEZ, Gregorio. **Curso de Derechos Fundamentales**. Universidad Carlos III, Boletín.

PEREA, Inmaculada Lopez-Barajas. Garantias Constitucionales en la Investigacion Tecnológica del delito: previsión legal y calidad. **Revista de derecho político**, Madrid, n 98, enero-abril, p. 91-119, 2017. ISSN 0211-979X.

PORRAS, Andrés José González. **A. Privacidad en Internet: Los derechos fundamentales de privacidad e intimidad en internet y su regulación jurídica: La vigilancia masiva**. [Em linha] 2015 [Consult. 18 Mar. 2022] Disponível em: https://dialnet.unirioja.es/servlet/tesis?codigo=80236.

PORTUGAL. Decreto-Lei n° 78/87. Código de Processo Penal. **Diário da República I Série**, n° 40, 17-02-1987. [Em Linha] Lisboa, 1987. [Consult. 03 Mar. 2022] Disponível em: https://dre.pt/dre/legislacao-consolidada/decreto-lei/1987-34570075-50539675.

PROJETO de Lei n° 4939 de 15 de outubro de 2020. [Em linha] **Câmara dos Deputados**. [Consult. 20 jan.2022] Disponível em: https://www.camara.leg.br/proposicoesWeb/prop\_most rarintegra?codteor=1936366&filename

RAMALHO, David Silva. **Métodos Ocultos de Investigação Criminal em Ambiente Digital.** Coimbra: Almedina, 2017. ISBN 978-97-2407-00-0-1.

RAMOS, Armando Dias. **A Prova Digital em Processo Penal: O correio eletrónico.** Chiado Editora, 2014. ISSBN 978-969-51-2384-1.

\_\_\_\_\_\_\_\_\_\_\_. A novíssima diretiva relativa ao cibercrime. In SOUSA, Constança Urbano de (coord.). **O espaço de liberdade, segurança e justiça da UE: desenvolvimentos recentes - The EU area of freedom, security and justice: recent developments.** Lisboa: Ediual, 2014, p. 176-192. ISBN: 978-989-8191-61-8.

\_\_\_\_\_\_\_\_\_\_\_. Do periculum in mora da atuação da autoridade judiciária ao fumus boni iuris da intervenção policial: contributo para o estudo das medidas cautelares e de polícia na cibercriminalidade económica. In: **IV Congrresso de Processo Penal**, 2016. Manuel Monteiro Guedes Valente (coord.) [Em Linha] p. 10. [Consult. 19 Mar. 2022] Disponível em: https://www.academia.edu/8696142/Medidas\_cautelares\_e\_de\_pol%C3%ADcia\_na\_cibercriminalidade\_econ%C3%B3mica

REGULAMENTO Geral de Proteção de Dados. **Jornal Oficial da União Europeia**, 04-05-2016. [Em linha] 59º Ano. Edição em língua portuguesa. [Consult. 22 Mar. 2022] Disponível em: https://www.sg.pcm.gov.pt/sobre-nos/regulamento-geral-de-prote%C3%A7%C3%A3o-de-dados.aspx#:~:text=O%20Regulamento%20(UE)%202016%2F,relativos%20a%20pessoa s%20na%20UE.

REVORIO, Francisco Javier Díaz. La constitución ante los avances científicos y tecnológicos: breves reflexiones al hilo de los recientes desarrollos en materia genética y en tecnologías de la información y la comunicación. [Em linha**]. Revista de Derecho Político de la UNED**, nº 71-72, 2008. p. 87-110. [Consult. 17 Mar. 2022]. Disponível em <https://revistas.uned.es/index.php/>derechopolitico/article/view/9040. ISSN 0211-979X.

RIBOLI, Eduardo Bolsoni. A utilização de novas tecnologias no âmbito da investigação criminal e as suas limitações legais: a interceptação de comunicações em massa e os softwares de espionagem. **Galileu – Revista de Direito e Economia,** Volume XIX, (Dezembro 2018), e‑ISSN 2184‑1845. p. 49-77.

RODOTÀ, Stefano. Democracia y protección de datos. [Em Linha] **Cuardenos de Derecho Publico,** 1997/2007, n° 19-20. [Consult. 21 Mar. 2022] ISSN 1989-8967 Disponível em: https://revistasonline.inap.es/index.php/CDP/article/view/690/745.

RODRIGUES, Benjamim Silva. Contributo para a fundamentação da sua autonomia dogmática e científica à luz do novo paradigma de investigação criminal: A ciência forense digital e a prova digital. In **Direito Penal Parte Especial: Direito Penal Informático-Digital**, [sl]. Coimbra, 2009. ISBN 978-989-95779-5-4.

\_\_\_\_\_\_\_\_\_\_\_. **Da prova penal: Tomo IV – Da prova-electrónico digital e da criminalidade informático-digital.** Lisboa: Rei dos Livros, 2011. ISBN: 9789898305183.

RUIZ, Estrella, Entrada y registro, interceptaciones de comunicaciones postales, telefónicas, etc., en: **Medidas restrictivas de los derechos fundamentales**. CDJud: Madrid, 1996.

SALDAÑA, Maria Nieves. The Right to Privacy. La génesis de la protección de la privacidad en el sistema constitucional norteamericano: el centenario legado de Warren y Brandeis. [Em linha] **Revista De Derecho Político**, 85, p. 195-240, 2012. [Consult. 17 Mar. 2022] Disponível em: https://www.researchgate.net/publication/256544041\_THE\_RIGHT\_TO\_PR IVACY\_LA\_GENESIS\_DE\_LA\_PROTECCION\_DE\_LA\_PRIVACIDAD\_EN\_EL\_SISTEMA\_CONSTITUCIONAL\_NORTEAMERICANO\_EL\_CENTENARIO\_LEGADO\_DE\_WARREN\_Y\_BRANDEIS\_The\_Right\_to\_Privacy\_The\_Genesis\_of\_the\_Protecti

SANTOS, Rita Coelho. **O Tratamento Jurídico-Penal da Transferência de Fundos Monetários Através da Manipulação Ilícita dos Sistemas Informáticos**, Coimbra: Coimbra Editora, 2005. p. 320. O presente estudo corresponde à dissertação de mestrado em Ciências Jurídico-Criminais apresentada em outubro de 2001 e defendida em novembro de 2003 na Faculdade de Direito da Universidade de Coimbra. ISBN 972-32-1300-1.

SENDRA, Vicente Gimeno. **Derecho Procesal Penal**. Civitas. Navarra. Ediciones Jurídicas Castillo de Luna. S.L.; 1ª edição. 2015. ISBN 978-8494276446.

SILVA, José Afonso da. **Curso de direito constitucional positivo**. 43ª ed. São Paulo: Malheiros, 2020. ISBN: 978-85-392-0462-5.

SIMAS, Diana Viveiros de. **O Cibercrime**. Dissertação apresentada no âmbito do 2.º Ciclo de Estudos em Direito, no Curso de Mestrado em Ciências Jurídico-Forenses, conferido pela Universidade Lusófona de Humanidades e Tecnologias, sob orientação do Prof. Dr. José Sousa Brito, Lisboa, 2014.

TEIXEIRA, Angelina. A Chave para a Regulamentação da Proteção de Dados. **Data Venia Revista Jurídica Digital**, n.º 6. Novembro 2016. ISSN 2182-6242. p. 6-32.

VALENTE, Manuel Monteiro Guedes. O Reforço dos Princípios Constitucionais na Obtenção de Prova no Mundo Digital. **Corpus Delicti Revista de Direito de Policia Judiciária**, Brasília. ISSN 2526-4265 e-ISSN: 2526-9623, Ano 2, n° 3 (Janeiro-Junho 2018), p. 11-25

\_\_\_\_\_\_\_\_\_\_\_. Editorial dossiê “Investigação preliminar, meios ocultos e novas tecnologias”. **Revista Brasileira de Direito Processual Penal**, Porto Alegre, vol. 3, n. 2, p. 473-482, mai./ago. 2017. ISSN 2525-510x. [Consult. 10 Mar. 2022] Disponível em https://doi.org/10.22197/rbdpp.v3i2.82.

\_\_\_\_\_\_\_\_\_\_\_. Os direitos e garantias dos cidadãos investigados na era digital. In: ANTONIALLI, Dennys; FRAGOSO, Nathalie (eds.). **Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate.** Vol. II. São Paulo. InternetLab, p. 26, 2019. ISBN 978-85-92871-02-4

\_\_\_\_\_\_\_\_\_\_\_. Meios ocultos de investigação: Contributo mínimo para uma reflexão maior. [Em linha] **Revista Brasileira de Ciências Criminais**, São Paulo-SP, 21 de Agosto de 2015 [Consult. 22 Mar. 2022]. Disponível em https://www.ibccrim.org.br/noticias/exibir/6323/

\_\_\_\_\_\_\_\_\_\_\_. **Teoria Geral do Direito Policial.** 6.ed. Coimbra: Almedina, 2019. ISBN 978-972-40-8078-9.

VAZ, Denise Provasi. **Provas digitais no processo penal: Formulação do conceito, definição das características e siatematização do processo probatório**. 2012. Tese (Doutorado em Direito) – Programa de Pós graduação em Direito. Universidade de São Paulo São Paulo, 2012.

VENÂNCIO, Pedro Dias. **Lei do Cibercrime Anotada e Comentada**. Coimbra: Coimbra Editora, 2011. ISBN: 9789723219067.

1. RAMOS, Armando R. Dias. A novíssima diretiva relativa ao cibercrime. In SOUSA, Constança Urbano de (coord.). **O espaço de liberdade, segurança e justiça da UE: desenvolvimentos recentes - The EU area of freedom, security and justice: recent developments**. Lisboa: Ediual, 2014, ISBN: 978-989-8191-61-8. p. 176. [↑](#footnote-ref-1)
2. RIBOLI, Eduardo Bolsoni. A utilização de novas tecnologias no âmbito da investigação criminal e as suas limitações legais: a interceptação de comunicações em massa e os softwares de espionagem. **GALILEU – REVISTA DE DIREITO E ECONOMIA,** e‑ISSN 2184‑1845, Volume XIX, (Dezembro 2018), p. 49-77. [↑](#footnote-ref-2)
3. MILITÃO, Renato Lopes. A propósito da prova digital no processo penal. **Revista da Ordem dos Advogados**, Lisboa, Ano 72, vol. 1 (Janeiro-Março 2012). p. 247-285. [↑](#footnote-ref-3)
4. *Ibid*., p. 248. [↑](#footnote-ref-4)
5. *Ibid*., p. 249. [↑](#footnote-ref-5)
6. *Ibid*., p. 248. [↑](#footnote-ref-6)
7. VALENTE, Manuel Monteiro Guedes. Os direitos e garantias dos cidadãos investigados na era digital. In: ANTONIALLI, Dennys; FRAGOSO, Nathalie (eds.). **Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate.** Vol. II. São Paulo. InternetLab, p. 26 2019, ISBN 978-85-92871-02-4. p. 26. [↑](#footnote-ref-7)
8. RAMOS, Armando R. Dias. A novíssima diretiva relativa ao cibercrime. In SOUSA, Constança Urbano de (coord.). **O espaço de liberdade, segurança e justiça da UE: desenvolvimentos recentes - The EU area of freedom, security and justice: recent developments**. Lisboa: Ediual, 2014, ISBN: 978-989-8191-61-8. p. 176-177. [↑](#footnote-ref-8)
9. Ao argumentar que os direitos fundamentais possuem limitações, Manuel Monteiro Guedes Valente em seu artigo publicado na Revista Direitos Fundamentais e Processo Penal na Era Digital afiança que: “A afirmação de cada um dos nossos direitos fundamentais pessoais tem, *ab initio*, um limite inexorável: o direito dos demais seres humanos que, como valores vitais e essenciais à vida em comunidade [bem jurídico] não podem ser lesados ou colocados em perigo de lesão. O exercício de direitos deve ocorrer em plena harmonia e em equilíbrio – equidade – sob pena de negarmos o sistema assente na construção de garantia, de segurança e de coesão social”. [↑](#footnote-ref-9)
10. Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...] X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; [...] XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; [...]. [↑](#footnote-ref-10)
11. Artigo 26.º Outros direitos pessoais: 1. A todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à proteção legal contra quaisquer formas de discriminação. [↑](#footnote-ref-11)
12. MIRANDA, Jorge; MEDEIROS, Rui. **Constituição Portuguesa Anotada**. 2.ª ed. Wolter Kluwer: Coimbra Editora, 2010, ISBN: 978-97-2321-82-2-0. p. 603. [↑](#footnote-ref-12)
13. *Ibid*., p 607. [↑](#footnote-ref-13)
14. *Ibid*., p 618. [↑](#footnote-ref-14)
15. Artigo 32.º Garantias de processo criminal: 8. São nulas todas as provas obtidas mediante tortura, coação, ofensa da integridade física ou moral da pessoa, abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações. [↑](#footnote-ref-15)
16. Artigo 7º Respeito pela vida privada e familiar: Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações. Artigo 8º Proteção de dados pessoais: 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. Artigo 52º Âmbito dos direitos garantidos: 1. Qualquer restrição ao exercício dos direitos e liberdades reconhecidos pela presente Carta deve ser prevista por lei e respeitar o conteúdo essencial desses direitos e liberdades. Na observância do princípio da proporcionalidade, essas restrições só podem ser introduzidas se forem necessárias e corresponderem efetivamente a objetivos de interesse geral reconhecidos pela União, ou à necessidade de proteção dos direitos e liberdades de terceiros. [↑](#footnote-ref-16)
17. CARTA dos Direitos Fundamentais da União Europeia. **Jornal Oficial da União Europeia**. [Em linha]. [Consult. 26 nov. 2020]. Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex>: 12016P/TXT. [↑](#footnote-ref-17)
18. Exemplo da necessidade de autorização judicial para limitar ou condicionar o exercício dos direitos fundamentais encontra-se no inciso LXI do artigo 5º da Constituição da República Federativa do Brasil, o qual dispoe que “ninguém será preso senão em flagrante delito ou por ordem escrita e fundamentada de autoridade judiciária competente, salvo nos casos de transgressão militar ou crime propriamente militar, definidos em lei”. [↑](#footnote-ref-18)
19. Na Constituição da República Portuguesa encontramos também exemplos de exigência de autorização ou manifestação judicial para limitar ou condicionar o exercício dos direitos fundamentais, é o que consta no artigo 27, no item 2, o qual dispõe que “ninguém pode ser total ou parcialmente privado da liberdade, a não ser em consequência de sentença judicial condenatória pela prática de acto punido por lei com pena de prisão ou de aplicação judicial de medida de segurança”. [↑](#footnote-ref-19)
20. CONVENÇÃO para a Protecção dos Direitos do Homem e das Liberdades Fundamentais. [Em linha] Roma, 2022. (4 Nov. 1950). [Consult. 08 Mar. 2022]. Disponível em <https://www>.echr.coe.int/documents/con vention\_por.pdf. [↑](#footnote-ref-20)
21. NEVES, Rosa Vieira. **A Livre Apreciação da Prova e a Obrigação de Fundamentação da Convicção (na Decisão Final Penal)** 1.ª ed. Coimbra: Coimbra Editora, 2011, ISBN 978-972-32-1929-6. p. 79. [↑](#footnote-ref-21)
22. VALENTE, Manuel Monteiro Guedes. Editorial dossiê “Investigação preliminar, meios ocultos e novas tecnologias”. **Revista Brasileira de Direito Processual Penal**, Porto Alegre, vol. 3, n. 2, p. 473-482, mai./ago. 2017. ISSN 2525-510x. [Consult. 10 Mar. 2022]. p. 473. Disponível em <https://doi.org/10.22197/rbdpp.v3i2.82>. [↑](#footnote-ref-22)
23. *Ibid*., 473. [↑](#footnote-ref-23)
24. DIAS, Jorge de Figueiredo. **Clássicos Jurídicos, Direito Processual Penal**, Coimbra Editora, 2004, ISBN 972-32-1250-1. p. 59-60. [↑](#footnote-ref-24)
25. COUTURE, Eduardo Juan. **Fundamentos del Derecho Procesal Civil.** 4ª ed. Buenos Aires: B de F, 2002, ISBN 987-10-890-58. p. 119. [↑](#footnote-ref-25)
26. COSTA, José Francisco de Faria, **Algumas reflexões sobre o estatuto dogmático do chamado “Direito Penal Informático”, Direito Penal da Comunicação, alguns escritos**. Coimbra Editora, 1998. ISBN 972-32-0850-4. p. 116. [↑](#footnote-ref-26)
27. LEI nº 9.296 de 24 de julho de 1996. [Em linha] **Diário Oficial da União**. Seção 1 – 25/7/1996, p. 13757.[Consult. 20 Jan. 2022]. Disponível em: https://www2.camara.leg.br/legin/fed/lei/1996/lei-9296-24-julho-1996-349049-publicacaooriginal-1-pl.html [↑](#footnote-ref-27)
28. LEI n° 14.155 de 27 de maio de 2021. [Em linha] **Diário Oficial da União**. [Consult. 20 Jan. 2022] Disponível em: http://www.planalto.gov.br/ccivil\_03/\_ato2019-2022/2021/Lei/L14155.htm [↑](#footnote-ref-28)
29. LEI n° 109 de 15 de setembro de 2009. [Em linha] **Diário da República Eletrónico n°179/2009. Série** I de 2009-09-15. [Consult. 20 Jan.2022] Disponível em: <https://data.dre.pt/eli/lei/109/2009/p/cons/20211124/pt/html> [↑](#footnote-ref-29)
30. Armando R. Dias Ramos em seu artigo “A novíssima diretiva relativa ao cibercrime”, a denomina de Ciberconvenção. [↑](#footnote-ref-30)
31. RAMOS, Armando R. Dias. A novíssima diretiva relativa ao cibercrime. In SOUSA, Constança Urbano de (coord.). **O espaço de liberdade, segurança e justiça da UE: desenvolvimentos recentes - The EU area of freedom, security and justice: recent developments**. Lisboa: Ediual, 2014, ISBN: 978-989-8191-61-8. p. 177. [↑](#footnote-ref-31)
32. É imperioso ressaltar que no dia 15 de dezembro de 2021, o Senado Federal aprovou a adesão do Brasil à Convenção sobre o Crime Cibernético, celebrada em Budapeste, na Hungria, em novembro de 2001 (Projeto de Decreto Legislativo 255/2021). A matéria, que teve como relator o senador Nelsinho Trad (PSD-MS), será encaminhada à promulgação. (https://www12.senado.leg.br/noticias/materias/2021/12/15/aprovada-adesao-do-brasil-a-convencao-sobre-o-crime-cibernetico) [↑](#footnote-ref-32)
33. A versão em português da Convenção sobre o Cibercrime fora obtida no seguinte endereço eletrônico: <https://data.dre.pt/eli/decpresrep/91/2009/09/15/p/dre/pt/html> [↑](#footnote-ref-33)
34. DIAS, Vera Elisa Marques. **A problemática da investigação do Cibercrime**. [Em linha] [Consult. 29 Jan. 2022] Disponível em http://www.datavenia.pt/ficheiros/edicao01/datavenia01\_p063-088.pdf. [↑](#footnote-ref-34)
35. COMISSÃO das Comunidades Europeias. **Comunicação da Comissão ao Parlamento Europeu, ao Conselho e ao Comité das Regiões: Rumo a uma política geral de luta contra o cibercrime.** [Em linha] Bruxelas, 22 Mai. 2007 [Consult. 29 Jan 2022]. Disponível em <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX:52007DC0267>. [↑](#footnote-ref-35)
36. VENÂNCIO, Pedro Dias. **Lei do Cibercrime, anotada e comentada**. Coimbra: Coimbra Editora, 2011. ISBN: 9789723219067. p. 16. [↑](#footnote-ref-36)
37. *Ibid*, p. 16 [↑](#footnote-ref-37)
38. *Ibid*, p. 17. [↑](#footnote-ref-38)
39. SANTOS, Rita Coelho. **O Tratamento Jurídico-Penal da Transferência de Fundos Monetários Através da Manipulação Ilícita dos Sistemas Informáticos**, Coimbra: Coimbra Editora, 2005. p. 320. ISBN 972-32-1300-1. p.32. [↑](#footnote-ref-39)
40. KIST, Dario José. **Prova digital no processo penal**. Leme: JH Mizuno, 2019, p. 384. ISBN 978-85-7789-430-7. p. 63-64. [↑](#footnote-ref-40)
41. *Ibid*., p. 63-64. [↑](#footnote-ref-41)
42. RAMOS, Armando R. Dias. A novíssima diretiva relativa ao cibercrime. In SOUSA, Constança Urbano de (coord.). **O espaço de liberdade, segurança e justiça da UE: desenvolvimentos recentes - The EU area of freedom, security and justice: recent developments**. Lisboa: Ediual, 2014. ISBN: 978-989-8191-61-8. p. 177. [↑](#footnote-ref-42)
43. *Ibid*., p. 177. [↑](#footnote-ref-43)
44. LEI n° 109 de 15 de setembro de 2009. [Em linha] **Diário da República Eletrónico n°179/2009. Série** I de 2009-09-15. [Consult. 20 jan.2022]. Disponível em: <https://data.dre.pt/eli/lei/109/2009/p/cons/20211124/pt/html> [↑](#footnote-ref-44)
45. 1 - Quem, com intenção de provocar engano nas relações jurídicas, introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos, com a intenção de que estes sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem, é punido com pena de prisão até 5 anos ou multa de 120 a 600 dias. 2 - Quando as ações descritas no número anterior incidirem sobre os dados registados, incorporados ou respeitantes a qualquer dispositivo que permita o acesso a sistema de comunicações ou a serviço de acesso condicionado, a pena é de 1 a 5 anos de prisão. 3 - Quem, atuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiro, usar documento produzido a partir de dados informáticos que foram objeto dos atos referidos no n.º 1 ou dispositivo no qual se encontrem registados, incorporados ou ao qual respeitem os dados objeto dos atos referidos no número anterior, é punido com as penas previstas num e noutro número, respetivamente. 4 - Quem produzir, adquirir, importar, distribuir, vender ou detiver qualquer dispositivo, programa ou outros dados informáticos destinados à prática das ações previstas no n.º 2, é punido com pena de prisão de 1 a 5 anos. 5 - Se os factos referidos nos números anteriores forem praticados por funcionário no exercício das suas funções, a pena é de prisão de 2 a 5 anos. [↑](#footnote-ref-45)
46. 1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, apagar, alterar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis ou não acessíveis programas ou outros dados informáticos alheios ou por qualquer forma lhes afectar a capacidade de uso, é punido com pena de prisão até 3 anos ou pena de multa. 2 - A tentativa é punível. 3 - Incorre na mesma pena do n.º 1 quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas nesse número. 4 - Se o dano causado for de valor elevado, a pena é de prisão até 5 anos ou de multa até 600 dias. 5 - Se o dano causado for de valor consideravelmente elevado, a pena é de prisão de 1 a 10 anos. 6 - Nos casos previstos nos n.os 1, 2 e 4 o procedimento penal depende de queixa. [↑](#footnote-ref-46)
47. 1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, entravar, impedir, interromper ou perturbar gravemente o funcionamento de um sistema informático, através da introdução, transmissão, deterioração, danificação, alteração, apagamento, impedimento do acesso ou supressão de programas ou outros dados informáticos ou de qualquer outra forma de interferência em sistema informático, é punido com pena de prisão até 5 anos ou com pena de multa até 600 dias. 2 - Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no número anterior. 3 - Nos casos previstos no número anterior, a tentativa não é punível. 4 - A pena é de prisão de 1 a 5 anos se o dano emergente da perturbação for de valor elevado. 5 - A pena é de prisão de 1 a 10 anos se: a) O dano emergente da perturbação for de valor consideravelmente elevado; b) A perturbação causada atingir de forma grave ou duradoura um sistema informático que apoie uma actividade destinada a assegurar funções sociais críticas, nomeadamente as cadeias de abastecimento, a saúde, a segurança e o bem-estar económico das pessoas, ou o funcionamento regular dos serviços públicos. [↑](#footnote-ref-47)
48. 1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo aceder a um sistema informático, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias. 2 - Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no número anterior. 3 - A pena é de prisão até 2 anos ou multa até 240 dias se as ações descritas no número anterior se destinarem ao acesso para obtenção de dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento. 4 - A pena é de prisão até 3 anos ou multa se: a) O acesso for conseguido através de violação de regras de segurança; ou b) Através do acesso, o agente obtiver dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento. 5 - A pena é de prisão de 1 a 5 anos quando: a) Através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei; ou b) O benefício ou vantagem patrimonial obtidos forem de valor consideravelmente elevado. 6 - A tentativa é punível, salvo nos casos previstos nos n.os 2 e 3. 7 - Nos casos previstos nos n.os 1, 4 e 6 o procedimento penal depende de queixa. [↑](#footnote-ref-48)
49. 1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, e através de meios técnicos, interceptar transmissões de dados informáticos que se processam no interior de um sistema informático, a ele destinadas ou dele provenientes, é punido com pena de prisão até 3 anos ou com pena de multa. 2 - A tentativa é punível. 3 - Incorre na mesma pena prevista no n.º 1 quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no mesmo número. [↑](#footnote-ref-49)
50. 1 - Quem ilegitimamente reproduzir, divulgar ou comunicar ao público um programa informático protegido por lei é punido com pena de prisão até 3 anos ou com pena de multa. 2 - Na mesma pena incorre quem ilegitimamente reproduzir topografia de um produto semicondutor ou a explorar comercialmente ou importar, para estes fins, uma topografia ou um produto semicondutor fabricado a partir dessa topografia. 3 - A tentativa é punível. [↑](#footnote-ref-50)
51. LEI n° 79 de 24 de novembro de 2021. [Em linha] **Diário da República Eletrónico n° 228/2021. Série** I de 2021-11-24. p. 09-38. [Consult. 20 Jan. 2022]. Disponível em: [https://data.dre.pt/eli/lei/ 109/2009/p/cons/2021 112 4/pt/html](https://data.dre.pt/eli/lei/%20109/2009/p/cons/2021%20112%204/pt/html). [↑](#footnote-ref-51)
52. Art. 72. Impedir ou dificultar o acesso do consumidor às informações que sobre ele constem em cadastros, banco de dados, fichas e registros: Pena Detenção de seis meses a um ano ou multa. [↑](#footnote-ref-52)
53. Art. 73. Deixar de corrigir imediatamente informação sobre consumidor constante de cadastro, banco de dados, fichas ou registros que sabe ou deveria saber ser inexata: Pena Detenção de um a seis meses ou multa. [↑](#footnote-ref-53)
54. LEI nº 8078 de 11 de setembro de 1990. [Em linha] **Diário Oficial da União**.[Consult. 22 Jan. 2022] Disponível em: http://www.planalto.gov.br/ccivil\_03/leis/l8078compilado.htm [↑](#footnote-ref-54)
55. Art. 2° Constitui crime da mesma natureza:  (...). V - utilizar ou divulgar programa de processamento de dados que permita ao sujeito passivo da obrigação tributária possuir informação contábil diversa daquela que é, por lei, fornecida à Fazenda Pública. Pena - detenção, de 6 (seis) meses a 2 (dois) anos, e multa. [↑](#footnote-ref-55)
56. LEI nº 8137 de 27 de dezembro de 1990. [Em linha] **Diário Oficial da União**.[Consult. 22 Jan. 2022] Disponível em: http://www.planalto.gov.br/ccivil\_03/leis/l8137.htm [↑](#footnote-ref-56)
57. Art. 241-A.  Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.  § 1 oNas mesmas penas incorre quem: I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo;  II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo. § 2 oAs condutas tipificadas nos incisos I e II do § 1 odeste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo. [↑](#footnote-ref-57)
58. LEI nº 8.137 de 27 de dezembro de 1990. [Em linha] **Diário Oficial da União**. Brasil, 2022 [Consult. 24 Jan. 2022] Disponível em: http://www.planalto.gov.br/ccivil\_03/leis/l8137.htm [↑](#footnote-ref-58)
59. Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, promover escuta ambiental ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei: Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa. Parágrafo único. Incorre na mesma pena a autoridade judicial que determina a execução de conduta prevista no caput deste artigo com objetivo não autorizado em lei. [↑](#footnote-ref-59)
60. LEI nº 9.296 de 24 de julho de 1996. [Em linha] **Diário Oficial da União**. Brasil, 2022 [Consult. 24 Jan. 2022] Disponível em: http://www.planalto.gov.br/ccivil\_03/leis/l9296.htm [↑](#footnote-ref-60)
61. Art. 72. Constituem crimes, puníveis com reclusão, de cinco a dez anos: I - obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem de votos; II - desenvolver ou introduzir comando, instrução, ou programa de computador capaz de destruir, apagar, eliminar, alterar, gravar ou transmitir dado, instrução ou programa ou provocar qualquer outro resultado diverso do esperado em sistema de tratamento automático de dados usados pelo serviço eleitoral; III - causar, propositadamente, dano físico ao equipamento usado na votação ou na totalização de votos ou a suas partes. [↑](#footnote-ref-61)
62. Art. 12. Violar direitos de autor de programa de computador: Pena - Detenção de seis meses a dois anos ou multa. § 1º Se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente: Pena - Reclusão de um a quatro anos e multa. § 2º Na mesma pena do parágrafo anterior incorre quem vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral. § 3º Nos crimes previstos neste artigo, somente se procede mediante queixa, salvo: I - quando praticados em prejuízo de entidade de direito público, autarquia, empresa pública, sociedade de economia mista ou fundação instituída pelo poder público; II - quando, em decorrência de ato delituoso, resultar sonegação fiscal, perda de arrecadação tributária ou prática de quaisquer dos crimes contra a ordem tributária ou contra as relações de consumo. § 4º No caso do inciso II do parágrafo anterior, a exigibilidade do tributo, ou contribuição social e qualquer acessório, processar-se-á independentemente de representação. [↑](#footnote-ref-62)
63. LEI nº 9.609 de 19 de fevereiro de 1998. [Em linha] **Diário Oficial da União**. Brasil, 2022 [Consult. 24 Jan. 2022]. Disponível em: http://www.planalto.gov.br/ccivil\_03/leis/l9609.htm [↑](#footnote-ref-63)
64. § 1o-A. Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública: Pena – detenção, de 1 (um) a 4 (quatro) anos, e multa. § 2o Quando resultar prejuízo para a Administração Pública, a ação penal será incondicionada.  [↑](#footnote-ref-64)
65. Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. § 1o Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput. § 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico. § 3o  Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa. [↑](#footnote-ref-65)
66. § 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo. [↑](#footnote-ref-66)
67. § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo. [↑](#footnote-ref-67)
68. Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa.  [↑](#footnote-ref-68)
69. Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente: Pena – detenção, de 3 (três) meses a 2 (dois) anos, e multa. Parágrafo único. As penas são aumentadas de um terço até a metade se da modificação ou alteração resulta dano para a Administração Pública ou para o administrado. [↑](#footnote-ref-69)
70. Art. 325 - Revelar fato de que tem ciência em razão do cargo e que deva permanecer em segredo, ou facilitar-lhe a revelação: Pena - detenção, de seis meses a dois anos, ou multa, se o fato não constitui crime mais grave. §1o Nas mesmas penas deste artigo incorre quem: I – permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública; II – se utiliza, indevidamente, do acesso restrito. § 2o Se da ação ou omissão resulta dano à Administração Pública ou a outrem: Pena – reclusão, de 2 (dois) a 6 (seis) anos, e multa. [↑](#footnote-ref-70)
71. KIST, Dario José. **Prova digital no processo penal**. Leme: JH Mizuno, 2019, p. 384. ISBN 978-85-7789-430-7. p. 75. [↑](#footnote-ref-71)
72. *Ibid*., p. 75-76. [↑](#footnote-ref-72)
73. VENÂNCIO, Pedro Dias. **Lei do Cibercrime: Anotada e Comentada.** Coimbra: Coimbra Editora, 2011. ISBN: 9789723219067. p. 14-15. [↑](#footnote-ref-73)
74. CONVENÇÃO sobre o cibercrime. [Em linha] Budapeste, 23 de Nov. 2001 [Consult. 12 Fev. 2022] Disponível em: https://rm.coe.int/16802fa428. [↑](#footnote-ref-74)
75. VALENTE, Manuel Monteiro Guedes -O Reforço dos Princípios Constitucionais na Obtenção de Prova no Mundo Digital. **Corpus Delicti** **Revista de Direito de Policia Judiciária**, Brasília. ISSN 2526-4265 e-ISSN: 2526-9623, Ano 2, n° 3 (Janeiro-Junho 2018), p. 11-25. [↑](#footnote-ref-75)
76. LEI n° 109 de 15 de setembro de 2009. [Em linha] **Diário da República Eletrónico n°179/2009. Série** I de 2009-09-15. [Consult. 21 jan.2022] Disponível em: <https://data.dre.pt/eli/lei/109/2009/p/cons/20211124/pt/html> [↑](#footnote-ref-76)
77. PROJETO de Lei n° 4.939 de 15 de outubro de 2020. [Em linha] **Câmara dos Deputados.** [Consult. 20 jan.2022] Disponível em: https://www.camara.leg.br/proposicoesWeb/prop\_mostrarintegra?codteor=1936366&f ilename [↑](#footnote-ref-77)
78. BUENO DE MATA, Federico. **Prueba electrónica y proceso****2.0.**Valencia: Tirant lo Blanch, 2014. ISBN 978-84-9053-483-0, p. 93. [↑](#footnote-ref-78)
79. BENTHAM, M. Jeremías. **Tratado de las Pruebas Judiciales. París:** Bossange Frerres, 1825, p 19. Antônio Pereira Gaio Júnior, Bruno Augusto Sampaio Fuga, William Santos Ferreira (orgs). ISBN 978-65-86300-86-4. Disponível em: http://cdigital.dgb.uanl.mx/la/1080045433\_C/1080045433\_T1/1080045433\_MA.PDF. [↑](#footnote-ref-79)
80. CARNELUTTI, Francesco; AUGENTI, Giacomo P. **A prova civil**. Lisa Pary Scarpa (trad). Campinas: Bookseller, 2005. ISBN: 8574683515, 9788574683515, p. 121. [↑](#footnote-ref-80)
81. Ordália ou ordálio, consistia na prova judiciária produzida com a concorrência de elementos da natureza, destacando-se o fato de o julgamento ser decorrente de interpretação divina do caso em si. Era um juízo de Deus. [↑](#footnote-ref-81)
82. MALATESTA, Nicola Framarino dei. **A lógica das provas em matéria criminal.** Campinas:Russell Editores, 2009, ISBN 978-85-89251-75-4, p. 45. [↑](#footnote-ref-82)
83. DOMINGOS, Fernanda Teixeira Souza; RÖDER, Priscila Costa Schrenir. Obtenção de provas digitais e jurisdição na Internet. **Investigação e prova nos crimes cibernéticos**. São Paulo: EMAG, 2017, ISBN 978-85-98004-04-4. p. 57 [↑](#footnote-ref-83)
84. RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital**. Coimbra: Almedina, 2017. ISBN 978-972-40-7000-1, p. 99-100. [↑](#footnote-ref-84)
85. KIST, Dario José. **Prova digital no processo penal**. Leme: JH Mizuno, 2019, p. 384. ISBN 978-85-7789-430-7, p. 109. [↑](#footnote-ref-85)
86. INSA MÉRIDA, Fredesvinda; LÁZARO HERRERO, Carmen; GARCÍA GÓNZALEZ, Nuria. **Pruebas electrónicas ante los tribunales en la lucha contra la cibercriminalidad. Un proyecto europeo.** [Em Linha] [Consult. 28 Fev. 2022] Disponível em: http://www.scielo.org.ve/scielo.php?script=sci\_arttext&pid=S1690-75152008000200009. [↑](#footnote-ref-86)
87. BUENO DE MATA, Federico. **Prueba electrónica y proceso 2.0**. Valencia: Tirant lo Blanch, 2014. ISBN: 978-84-9053-483-0, p. 103. [↑](#footnote-ref-87)
88. ABEL LLUNCH, Xavier; PICÓ I JUNOY, Joan, et al. **La prueba electrónica**. Barcelona: Bosch, 2011. ISBN: 978-84-7698-955-5, p. 26. [↑](#footnote-ref-88)
89. RODRIGUES, Benjamim Silva. Contributo para a fundamentação da sua autonomia dogmática e científica à luz do novo paradigma de investigação criminal: A ciência forense digital e a prova digital. In **Direito Penal Parte Especial: Direito Penal Informático-Digital**, [sl]. Coimbra, 2009, p. 722. ISBN 978-989-95779-5-4. [↑](#footnote-ref-89)
90. RAMOS, Armando Dias. **A Prova Digital em Processo Penal: O correio eletrónico.** Chiado Editora, 2014. ISSBN 978-969-51-2384-1, p. 97. [↑](#footnote-ref-90)
91. CASEY, Eoghan. **Digital evidence and computer crime: forensic science, computers and the internet.** 3rd ed. [s.l] Elsevier, 2011. ISBN 978-0-12-374268-1, p. 191. [↑](#footnote-ref-91)
92. CONSELHO DA EUROPA. **Eletronic Evidence Guide – A basic guide for police officers, prosecutors and judges. Cybercrime Division. Directorate General of Human Rights and Rule of Law.** Strasbourg, France. Data: 06 de março de 2020, p. 41-44. [Consult. em 20 Fev. de 2022]. Disponível em: https://rm.coe.int/c-proc-electronic-evidence-guide-2-1-en-june-2020-web2/16809ed4b4. [↑](#footnote-ref-92)
93. KIST, Dario José. **Prova digital no processo penal**. Leme: JH Mizuno, 2019, p. 384, ISBN 978-85-7789-430-7, p. 102. [↑](#footnote-ref-93)
94. RODRIGUES, Benjamim Silva. **Da prova penal: Tomo IV – Da prova-electrónico digital e da criminalidade informático-digital.** Lisboa: Rei dos Livros, 2011. ISBN: 9789898305183, p. 41-44. [↑](#footnote-ref-94)
95. VAZ, Denise Provasi. **Provas digitais no processo penal: Formulação do conceito, definição das características e siatematização do processo probatório**. 2012. Tese (Doutorado em Direito) – Programa de Pós graduação em Direito. Universidade de São Paulo São Paulo, 2012, p. 66. [↑](#footnote-ref-95)
96. *Ibid*, p. 68. [↑](#footnote-ref-96)
97. Renato Lopes Militão doutrina sobre a fragilidade da prova digital que “é certo que o legislador português, através do Dec. Lei n.º 290-D/99, de 02/08, entretanto alterado pelo Dec. Lei n.º 62/2003, de 03/04, regulou a validade, eficácia e valor probatório dos documentos electrónicos, bem como a assinatura electrónica. Porém, as referidas dúvidas sobre a autoria e genuinidade dos documentos digitais resultam de causas técnicas inultrapassáveis, não podendo ser colmatadas por lei, pelo que sempre subsistirão”. [↑](#footnote-ref-97)
98. VAZ, Denise Provasi. **Provas digitais no processo penal: Formulação do conceito, definição das características e siatematização do processo probatório**. 2012. Tese (Doutorado em Direito) – Programa de Pós graduação em Direito. Universidade de São Paulo São Paulo, 2012, p. 69. [↑](#footnote-ref-98)
99. RAMALHO, David Silva. **Métodos Ocultos de Investigação Criminal em Ambiente Digital**. Coimbra: Almedina, 2017, ISBN 978-97-2407-00-0-1, p. 105-106. [↑](#footnote-ref-99)
100. *Ibid*. [↑](#footnote-ref-100)
101. KIST, Dario José. **Prova digital no processo penal**. Leme: JH Mizuno, 2019, p. 384. ISBN 978-85-7789-430-7, p. 120. [↑](#footnote-ref-101)
102. RAMALHO, David Silva. **Métodos Ocultos de Investigação Criminal em Ambiente Digital.** Coimbra: Almedina, 2017. ISBN 978-97-2407-00-0-1, p.111. [↑](#footnote-ref-102)
103. KIST, Dario José. **Prova digital no processo penal**. Leme: JH Mizuno, 2019, p. 384. ISBN 978-85-7789-430-7, p. 125. [↑](#footnote-ref-103)
104. GRANCE, T.; CHEVALIER, S.; SCARFONE, K..; DANG, H. **Guia para Integração de Técnicas Forenses em Resposta a Incidentes, Publicação Especial**. Instituto Nacional de Padrões e Tecnologia. [Em linha]. Gaithersburg, MD, 2006 [Consult. 12 Mar. de 2022] Disponível em: [https://tsapps.nist.gov/publication /get\_pdf.cfm](https://tsapps.nist.gov/publication%20/get_pdf.cfm)?pub\_id =50875 [↑](#footnote-ref-104)
105. RAMALHO, David Silva. **Métodos Ocultos de Investigação Criminal em Ambiente Digital.** Coimbra: Almedina, 2017. ISBN 978-97-2407-00-0-1, p. 118. [↑](#footnote-ref-105)
106. GRANCE, T.; CHEVALIER, S.; SCARFONE, K..; DANG, H. **Guia para Integração de Técnicas Forenses em Resposta a Incidentes, Publicação Especial**. Instituto Nacional de Padrões e Tecnologia. [Em linha]. Gaithersburg, MD, 2006 [Consult. 12 Mar. de 2022] Disponível em: <https://tsapps.nist.gov/publication/get> \_pdf.cfm?pub\_id=50875, p. ES-1, 2-2 e 3.1. [↑](#footnote-ref-106)
107. *Ibid* , p. ES-1, 3-2 e 3.6 [↑](#footnote-ref-107)
108. *Ibid*, p. ES-1, 3-3 e 3.6 [↑](#footnote-ref-108)
109. RAMALHO, David Silva. **Métodos Ocultos de Investigação Criminal em Ambiente Digital.** Coimbra: Almedina, 2017. ISBN 978-97-2407-00-0-1, p. 129. [↑](#footnote-ref-109)
110. GRANCE, T.; CHEVALIER, S.; SCARFONE, K..; DANG, H. **Guia para Integração de Técnicas Forenses em Resposta a Incidentes, Publicação Especial**. Instituto Nacional de Padrões e Tecnologia. [Em linha]. Gaithersburg, MD, 2006 [Consult. 12 Mar. de 2022] Disponível em: https://tsapps.nist.gov/publication/get\_pdf.cfm?pub\_id=50875, p. ES-1, 3-3 e 3.6. [↑](#footnote-ref-110)
111. *Ibid*, p. ES-1, 3-3 e 3.7 [↑](#footnote-ref-111)
112. KIST, Dario José. **Prova digital no processo penal.** Leme: JH Mizuno, 2019, p. 384. ISBN 978-85-7789-430-7, p.135. [↑](#footnote-ref-112)
113. RAMALHO, David Silva. **Métodos Ocultos de Investigação Criminal em Ambiente Digital.** Coimbra: Almedina, 2017. ISBN 978-97-2407-00-0-1, p. 145-146. [↑](#footnote-ref-113)
114. A adesão do Brasil à Convenção sobre o Crime Cibernético, conhecida como Convenção de Budapeste, por ter sido celebrada na capital da Hungria, em novembro de 2001, foi aprovada pelo Senado no 15 de dezembro de 2021. O Projeto de Decreto Legislativo (PDL) 255/2021 foi relatado pelo senador Nelsinho Trad (PSD/MS) e aguarda promulgação pelo Congresso Nacional. A Convenção de Budapeste tem como objetivo facilitar a cooperação internacional para combater o cibercrime. Elaborado pelo Comitê Europeu para os Problemas Criminais, com o apoio de uma comissão de especialistas, o documento lista os principais crimes cometidos por meio da rede mundial de computadores e foi o primeiro tratado internacional sobre crimes cibernéticos. A Convenção já foi assinada por mais de 60 países e é utilizada por outros cerca de 160 como orientação para as legislações locais. (informação constante em <http://www.mpf.mp.br/pgr/noticias-pgr/brasil-aprova-adesao-a-convencao-de-budapeste-que-facilita-cooperacao-internacional-para-combate-ao-cibercrime#:~:text=O%20Proje to%20de%20Decreto%20Legislativo,internacional%20para%20combater%20o%20cibercrime>.) [↑](#footnote-ref-114)
115. CONVENÇÃO sobre o cibercrime. [Em linha] Budapeste, 23 de Nov. 2001 [Consult. 20 Mar. 2022] Disponível em: https://rm.coe.int/16802fa428. [↑](#footnote-ref-115)
116. MINUTA do Relatório Explicativo da Convenção sobre o cibercrime. [Em linha] [Consult. 18 Mar. 2022]. Disponível em <https://www.coe.int/t/dg1/legalcoope>ration/economiccrime/cybercrime/Documents/Convention% 20and%20protocol/ETS\_185\_Portugese-ExpRep.pdf [↑](#footnote-ref-116)
117. O objectivo das disposições contidas no Artigo 16º é o de assegurar que as autoridades competentes, ao nível nacional, dispõem da capacidade necessária para emitir uma ordem ou, de forma semelhante, obter a preservação expedita dos dados informatizados, armazenados, especificados, relativamente a uma investigação criminal ou acção penal específica. [↑](#footnote-ref-117)
118. MINUTA do Relatório Explicativo da Convenção sobre o cibercrime. [Em linha] [Consult. 18 Mar. 2022]. Disponível em https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Convention %20and%20protocol/ETS\_185\_Portugese-ExpRep.pdf [↑](#footnote-ref-118)
119. Artigo 12.º - Preservação expedita de dados: 1 - Se no decurso do processo for necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos armazenados num sistema informático, incluindo dados de tráfego, em relação aos quais haja receio de que possam perder-se, alterar-se ou deixar de estar disponíveis, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados, designadamente a fornecedor de serviço, que preserve os dados em causa. 2 - A preservação pode também ser ordenada pelo órgão de polícia criminal mediante autorização da autoridade judiciária competente ou quando haja urgência ou perigo na demora, devendo aquele, neste último caso, dar notícia imediata do facto à autoridade judiciária e transmitir-lhe o relatório previsto no artigo 253.º do Código de Processo Penal. 3 - A ordem de preservação discrimina, sob pena de nulidade: a) A natureza dos dados; b) A sua origem e destino, se forem conhecidos; e c) O período de tempo pelo qual deverão ser preservados, até um máximo de três meses. 4 - Em cumprimento de ordem de preservação que lhe seja dirigida, quem tenha disponibilidade ou controlo sobre esses dados, designadamente o fornecedor de serviço, preserva de imediato os dados em causa, protegendo e conservando a sua integridade pelo tempo fixado, de modo a permitir à autoridade judiciária competente a sua obtenção, e fica obrigado a assegurar a confidencialidade da aplicação da medida processual. 5 - A autoridade judiciária competente pode ordenar a renovação da medida por períodos sujeitos ao limite previsto na alínea c) do n.º 3, desde que se verifiquem os respectivos requisitos de admissibilidade, até ao limite máximo de um ano. [↑](#footnote-ref-119)
120. KIST, Dario José. **Prova digital no processo penal**. Leme: JH Mizuno, 2019, p. 384. ISBN 978-85-7789-430-7, p. 139 [↑](#footnote-ref-120)
121. NUNES, Duarte Rodrigues. **Os meios de prova previstos na Lei do Cibercrime***.* Coimbra: Gestlegal, 2018, ISBN 9789898951847. p. 35. [↑](#footnote-ref-121)
122. Artigo 17 – Conservação expedita e divulgação parcial de dados de trânsito: 1 Cada Parte adotará, em relação aos dados de tráfego que devem ser preservados nos termos do Artigo 16, tais e outras medidas que possam ser necessárias para: a) garantir que essa preservação expedita de dados de tráfego esteja disponível, independentemente de um ou mais prestadores de serviços estiveram envolvidos na transmissão dessa comunicação; e b) assegurar a divulgação expedita à autoridade competente da Parte, ou a uma pessoa por ela designada autoridade, de uma quantidade suficiente de dados de tráfego para permitir à Parte identificar os prestadores de serviços e os caminho pelo qual a comunicação foi transmitida. 2 Os poderes e procedimentos referidos neste artigo estarão sujeitos aos artigos 14 e 15. [↑](#footnote-ref-122)
123. Um dos maiores desafios que se colocam, no contexto do combate ao crime praticado no seio de redes informáticas, é a dificuldade de identificação do infractor, bem como de avaliação da extensão e do impacto dessa mesma infracção. [↑](#footnote-ref-123)
124. Artigo 13.º - Revelação expedita de dados de tráfego: Tendo em vista assegurar a preservação dos dados de tráfego relativos a uma determinada comunicação, independentemente do número de fornecedores de serviço que nela participaram, o fornecedor de serviço a quem essa preservação tenha sido ordenada nos termos do artigo anterior indica à autoridade judiciária ou ao órgão de polícia criminal, logo que o souber, outros fornecedores de serviço através dos quais aquela comunicação tenha sido efectuada, tendo em vista permitir identificar todos os fornecedores de serviço e a via através da qual aquela comunicação foi efectuada. [↑](#footnote-ref-124)
125. Artigo 18 – Ordem de produção: 1 Cada Parte adotará as medidas legislativas e outras que sejam necessárias para capacitar seus autoridades para ordenar: a) uma pessoa em seu território para enviar dados de computador especificados em sua posse ou controle, que são armazenados num sistema informático ou num suporte informático de armazenamento de dados; e b) um provedor de serviços que oferece seus serviços no território da Parte para apresentar informações do assinante relacionados a tais serviços na posse ou controle desse provedor de serviços. 2 Os poderes e procedimentos referidos neste artigo estarão sujeitos aos artigos 14 e 15.

3 Para os fins deste artigo, o termo “informações do assinante” significa qualquer informação contida na forma de dados informáticos ou qualquer outra forma que seja detida por um prestador de serviços, relativa aos assinantes do seu serviços que não sejam dados de tráfego ou conteúdo e pelos quais podem ser estabelecidos:

a) o tipo de serviço de comunicação utilizado, as provisões técnicas tomadas e o tempo de serviço; b) a identidade do assinante, endereço postal ou geográfico, telefone e outros números de acesso, faturamento e informações de pagamento, disponíveis com base no contrato ou acordo de serviço; c) quaisquer outras informações no local de instalação dos equipamentos de comunicação, disponíveis com base em o contrato ou acordo de serviço.” [↑](#footnote-ref-125)
126. Artigo 14.º - Injunção para apresentação ou concessão do acesso a dados: 1 - Se no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados que os comunique ao processo ou que permita o acesso aos mesmos, sob pena de punição por desobediência. 2 - A ordem referida no número anterior identifica os dados em causa. 3 - Em cumprimento da ordem descrita nos n.os 1 e 2, quem tenha disponibilidade ou controlo desses dados comunica esses dados à autoridade judiciária competente ou permite, sob pena de punição por desobediência, o acesso ao sistema informático onde os mesmos estão armazenados. 4 - O disposto no presente artigo é aplicável a fornecedores de serviço, a quem pode ser ordenado que comuniquem ao processo dados relativos aos seus clientes ou assinantes, neles se incluindo qualquer informação diferente dos dados relativos ao tráfego ou ao conteúdo, contida sob a forma de dados informáticos ou sob qualquer outra forma, detida pelo fornecedor de serviços, e que permita determinar: a) O tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço; b) A identidade, a morada postal ou geográfica e o número de telefone do assinante, e qualquer outro número de acesso, os dados respeitantes à facturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços; ou c) Qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços. 5 - A injunção prevista no presente artigo não pode ser dirigida a suspeito ou arguido nesse processo. 6 - Não pode igualmente fazer-se uso da injunção prevista neste artigo quanto a sistemas informáticos utilizados para o exercício da advocacia, das actividades médica e bancária e da profissão de jornalista. 7 - O regime de segredo profissional ou de funcionário e de segredo de Estado previsto no artigo 182.º do Código de Processo Penal é aplicável com as necessárias adaptações. [↑](#footnote-ref-126)
127. Artigo 19 – Busca e apreensão de dados informáticos armazenados: 1 Cada Parte adotará as medidas legislativas e outras que sejam necessárias para capacitar seus autoridades para pesquisar ou acessar de forma semelhante: a) um sistema informático ou parte dele e dados informáticos nele armazenados; e b) um meio de armazenamento de dados de computador no qual os dados de computador podem ser armazenados em seu território. 2 Cada Parte adotará as medidas legislativas e outras que sejam necessárias para assegurar que, quando as autoridades pesquisam ou acessam similarmente um sistema de computador específico ou parte dele, de acordo com o parágrafo 1.a, e tenha motivos para acreditar que os dados solicitados estão armazenados em outro sistema informático ou parte dele em seu território, e esses dados estiverem legalmente acessíveis ou disponíveis para o sistema inicial, as autoridades poderão estender rapidamente a busca ou acesso similar ao outro sistema. 3 Cada Parte adotará as medidas legislativas e outras que sejam necessárias para capacitar seus

autoridades a apreender ou proteger de forma semelhante os dados de computador acessados ​​de acordo com os parágrafos 1 ou 2. medidas devem incluir o poder de: a) apreender ou igualmente proteger um sistema informático ou parte dele ou um meio de armazenamento de dados informáticos; b) fazer e conservar uma cópia desses dados informáticos; c) manter a integridade dos dados informáticos armazenados relevantes; d) tornar inacessíveis ou remover esses dados informáticos do sistema informático acedido. 4 Cada Parte adotará as medidas legislativas e outras que sejam necessárias para capacitar seus autoridades a ordenar a qualquer pessoa que tenha conhecimento sobre o funcionamento do sistema informático ou medidas aplicado para proteger os dados informáticos nele contidos para fornecer, conforme o razoável, as informações necessárias, para permitir

a realização das medidas referidas nos n.ºs 1 e 2. 5 Os poderes e procedimentos referidos neste artigo estarão sujeitos aos artigos 14 e 15. [↑](#footnote-ref-127)
128. MINUTA do Relatório Explicativo da Convenção sobre o cibercrime. [Em linha] [Consult. 18 Mar. 2022]. Disponível em <https://www.coe.int/t/dg1/legalcoope>ration/economiccrime/cybercrime/Documents/Convention% 20and%20protocol/ETS\_185\_Portugese-ExpRep.pdf [↑](#footnote-ref-128)
129. RAMOS, Armando Dias. **Do periculum in mora da atuação da autoridade judiciária ao fumus boni iuris da intervenção policial: contributo para o estudo das medidas cautelares e de polícia na cibercriminalidade económica**. In: IV Congresso de Processo Penal, 2016. Manuel Monteiro Guedes Valente (coord.) [Em Linha] p. 10. [Consult. 19 Mar. 2022] Disponível em: https://www. academia.edu/8696142/Medidas\_cautelares\_e\_de\_pol%C3%ADcia\_nacibercriminalidade\_econ%C3 %B3mica [↑](#footnote-ref-129)
130. VALENTE, Manuel Monteiro Guedes. Os direitos e garantias dos cidadãos investigados na era digital. In: ANTONIALLI, Dennys; FRAGOSO, Nathalie (eds.). **Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate**. Vol. II. São Paulo. InternetLab, p. 26, 2019. ISBN 978-85-92871-02-4. p. 34-35. [↑](#footnote-ref-130)
131. Artigo 20 – Coleta de dados de tráfego em tempo real: 1 Cada Parte adotará as medidas legislativas e outras que sejam necessárias para capacitar seus autoridades para: a) recolher ou registar através da aplicação de meios técnicos no território dessa Parte, e b) obrigar um prestador de serviço, dentro de sua capacidade técnica existente: i) coletar ou registrar por meio da aplicação de meios técnicos no território dessa Parte; ou ii) cooperar e auxiliar as autoridades competentes na coleta ou registro de, dados de tráfego, em tempo real, associados a comunicações especificadas em seu território transmitidas por meio de um sistema de computador. 2 Quando uma Parte, devido aos princípios estabelecidos de seu ordenamento jurídico interno, não puder adotar as medidas referido no n.º 1, alínea a), pode, em vez disso, adotar medidas legislativas e outras que sejam necessárias para garantir a coleta ou registro em tempo real de dados de tráfego associados a comunicações especificadas transmitida no seu território, através da aplicação de meios técnicos nesse território. 3 Cada Parte adotará as medidas legislativas e outras que sejam necessárias para obrigar um prestador de serviços manter em sigilo o fato da execução de qualquer poder previsto neste artigo e qualquer informação relativo a ele. 4 Os poderes e procedimentos referidos neste artigo estarão sujeitos aos artigos 14 e 15. [↑](#footnote-ref-131)
132. Artigo 21 – Interceptação de dados de conteúdo: 1 Cada Parte adotará as medidas legislativas e outras que sejam necessárias, em relação a uma série de delitos graves a serem determinados pelo direito interno, para habilitar suas autoridades competentes a: a) recolher ou registar através da aplicação de meios técnicos no território dessa Parte, e b) obrigar um prestador de serviço, dentro de sua capacidade técnica existente: i) coletar ou registrar por meio da aplicação de meios técnicos no território dessa Parte, ou ii) cooperar e auxiliar as autoridades competentes na coleta ou registro de, dados de conteúdo, em tempo real, de comunicações específicas em seu território transmitidos por meio de um computador sistema. 2 Quando uma Parte, devido aos princípios estabelecidos de seu ordenamento jurídico interno, não puder adotar as medidas referido no n.º 1, alínea a), pode, em vez disso, adotar medidas legislativas e outras que sejam necessárias para garantir a coleta ou gravação em tempo real de dados de conteúdo em comunicações especificadas em seu território através da aplicação de meios técnicos nesse território. 3 Cada Parte adotará as medidas legislativas e outras que sejam necessárias para obrigar um prestador de serviços manter em sigilo o fato da execução de qualquer poder previsto neste artigo e qualquer informação relativo a ele. 4 Os poderes e procedimentos referidos neste artigo estarão sujeitos aos artigos 14 e 15. [↑](#footnote-ref-132)
133. Artigo 18.º - Intercepção de comunicações: 1 - É admissível o recurso à intercepção de comunicações em processos relativos a crimes: a) Previstos na presente lei; ou b) Cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico, quando tais crimes se encontrem previstos no artigo 187.º do Código de Processo Penal. 2 - A intercepção e o registo de transmissões de dados informáticos só podem ser autorizados durante o inquérito, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter, por despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público. 3 - A intercepção pode destinar-se ao registo de dados relativos ao conteúdo das comunicações ou visar apenas a recolha e registo de dados de tráfego, devendo o despacho referido no número anterior especificar o respectivo âmbito, de acordo com as necessidades concretas da investigação. 4 - Em tudo o que não for contrariado pelo presente artigo, à intercepção e registo de transmissões de dados informáticos é aplicável o regime da intercepção e gravação de conversações ou comunicações telefónicas constante dos artigos 187.º, 188.º e 190.º do Código de Processo Penal. [↑](#footnote-ref-133)
134. RAMOS, Armando Dias. **A Prova Digital em Processo Penal: O correio eletrónico**. Chiado Editora, 2014. ISSBN 978-969-51-2384-1, p. 90-91. [↑](#footnote-ref-134)
135. MILITÃO, Renato Lopes. A propósito da prova digital no processo penal. **Revista da Ordem dos Advogados**, Lisboa, Ano 72, vol. 1 (Janeiro-Março 2012), p. 263. [↑](#footnote-ref-135)
136. BUENO DE MATA, Federico. **Prueba electrónica y proceso 2.0.** Valencia: Tirant lo Blanch, 2014. ISBN: 978-84-9053-483-0. p. 172-179. [↑](#footnote-ref-136)
137. RODRIGUES, Benjamim Silva. **Da prova penal: Tomo IV – Da prova-electrónico digital e da criminalidade informático-digital.** Lisboa: Rei dos Livros, 2011. ISBN: 9789898305183. p. 19. [↑](#footnote-ref-137)
138. CABRAL, Antonio do Passo. A eficácia probatória das mensagens eletrônicas. **Revista de Processo**, São Paulo, v. 31, n. 135, p. 97-131, 2006, p. 102. [↑](#footnote-ref-138)
139. DIDIER JÚNIOR, Fredie; BRAGA, Paula Sarno; OLIVEIRA, Rafael Alexandria de. **Curso de direito processual civil.** 11. ed. Salvador: Jus Podivm, 2016. v. 2. ISBN 978-85-442-0663-8. p. 221-222. [↑](#footnote-ref-139)
140. MARINONI, Luiz Guilherme; ARENHART, Sérgio Cruz. **Prova**. 2. ed. São Paulo: Revista dos Tribunais, 2011. ISBN 9788520340165. p. 563-564 [↑](#footnote-ref-140)
141. RAMOS, Armando Dias. **A Prova Digital em Processo Penal: O correio eletrónico.** Chiado Editora, 2014. ISBN 978-969-51-2384-1. p. 143. [↑](#footnote-ref-141)
142. GONZÁLEZ, Nicolás Cuéllar Serrano. Garantías constitucionales en la persecución penal en el entorno digital. In: **Derecho y Justicia penal en el Siglo XXI. Liber amicorum en homenaje al Profesor Antonio González-Cuéllar García**. Madrid: Colex, 2006. ISBN 84-8342-047-3.p. 887. [↑](#footnote-ref-142)
143. *Ibid*., p. 891. [↑](#footnote-ref-143)
144. RIBOLI, Eduardo Bolsoni. A utilização de novas tecnologias no âmbito da investigação criminal e as suas limitações legais: a interceptação de comunicações em massa e os softwares de espionagem. **Galileu – Revista de Direito e Economia**, Volume XIX, (Dezembro 2018), e‑ISSN 2184‑1845. p. 51. [↑](#footnote-ref-144)
145. *Ibid*., p. 51. [↑](#footnote-ref-145)
146. VALENTE, Manuel Monteiro Guedes. Editorial dossiê “Investigação preliminar, meios ocultos e novas tecnologias”. **Revista Brasileira de Direito Processual Penal**, Porto Alegre, vol. 3, n. 2, p. 473-482, mai./ago. 2017. ISSN 2525-510x. [Consult. 10 Mar. 2022] Disponível em <https://doi.org/10.22197/rbdpp.v3i2.82>. p. 474. [↑](#footnote-ref-146)
147. GONZÁLEZ, Nicolás Cuéllar Serrano. Garantías constitucionales en la persecución penal en el entorno digital. In: **Derecho y Justicia penal en el Siglo XXI. Liber amicorum en homenaje al Profesor Antonio González-Cuéllar García**. Madrid: Colex, 2006. ISBN 84-8342-047-3. p. 887. [↑](#footnote-ref-147)
148. *Ibid*., p.55. [↑](#footnote-ref-148)
149. RIBOLI, Eduardo Bolsoni. A utilização de novas tecnologias no âmbito da investigação criminal e as suas limitações legais: a interceptação de comunicações em massa e os softwares de espionagem. **Galileu – Revista de Direito e Economia**, Volume XIX, (Dezembro 2018), e‑ISSN 2184‑1845. [↑](#footnote-ref-149)
150. *Ibid*., p. 51. [↑](#footnote-ref-150)
151. VALENTE, Manuel Monteiro Guedes. Editorial dossiê “Investigação preliminar, meios ocultos e novas tecnologias”. **Revista Brasileira de Direito Processual Penal**, Porto Alegre, vol. 3, n. 2, p. 473-482, mai./ago. 2017. ISSN 2525-510x. [Consult. 10 Mar. 2022] Disponível em <https://doi.org/10.22197/rbdpp.v3i2.82>. p. 474. [↑](#footnote-ref-151)
152. VALENTE, Manuel Monteiro Guedes. **Teoria Geral do Direito Policial.** 6.ed. Coimbra: Almedina, 2019. ISBN 978-972-40-8078-9. p. 478. [↑](#footnote-ref-152)
153. MEIREIS, Manuel Augusto. Homens de confiança. Será o caminho? In: **II Congresso de processo penal. Memórias.** Manuel Monteiro Guedes Valente (coord). Coimbra: Almedina, 2006, p. 81-101. ISBN 972-40-2814-3. p. 84. [↑](#footnote-ref-153)
154. RAMALHO, David Silva. **Métodos Ocultos de Investigação Criminal em Ambiente Digital.** Coimbra: Almedina, 2017. ISBN 978-97-2407-00-0-1. p. 204. [↑](#footnote-ref-154)
155. RAMALHO, David Silva. **Métodos Ocultos de Investigação Criminal em Ambiente Digital.** Coimbra: Almedina, 2017. ISBN 978-97-2407-00-0-1. p. 205. [↑](#footnote-ref-155)
156. ANDRADE, Manuel da Costa. **Bruscamente no Verão passado – A reforma do Código de processo penal.** Coimbra: Coimbra Editora, 2009. ISBN 9789723217261. p. 105-106. [↑](#footnote-ref-156)
157. VALENTE, Manuel Monteiro Guedes. Meios ocultos de investigação: Contributo mínimo para uma reflexão maior. [Em linha] **Revista Brasileira de Ciências Criminais**, São Paulo-SP, 21 de Agosto de 2015 [Consult. 22 Mar. 2022]. Disponível em https://www.ibccrim.org.br/noticias/exibir/6323/ [↑](#footnote-ref-157)
158. RAMALHO, David Silva. **Métodos Ocultos de Investigação Criminal em Ambiente Digital.** Coimbra: Almedina, 2017. ISBN 978-97-2407-00-0-1. p. 209. [↑](#footnote-ref-158)
159. *Ibid*., p. 209. [↑](#footnote-ref-159)
160. A constitucionalidade das renovações sucessivas e, por conseguinte, a interpretação do termo “renovável por igual tempo” descrito no art. 5º da Lei nº 9.296/96 são temas do pendente Recurso Extraordinário nº 625263/PR, interposto pelo Ministério Público Federal e de relatoria de Gilmar Mendes. Vale notar que, em 13 de junho de 2016, o Supremo Tribunal Federal, por unanimidade, reconheceu a existência de repercussão geral do tema. [↑](#footnote-ref-160)
161. BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário 625263/PR**. Relator Gilmar Mendes. [Em linha] Brasília, 13 de junho de 2013. [Consult. 23 Mar. 2022] Disponível em: https://redir.stf.jus.br/paginadorpu b/paginador.jsp?docTP=TP&docID=4472381. [↑](#footnote-ref-161)
162. *Ibid*. [↑](#footnote-ref-162)
163. FRAGOSO, Nathalie; RODRIGUES, Gabriel Brezinski. Dossiê: Privacidade e proteção de dados pessoais na segurança pública e no processo penal. **Revista Direito Público**, Brasília, Volume 18, n. 100, 581-605, out./dez. 2021. p. 585. ISSN 2236-1766. p. 595. [↑](#footnote-ref-163)
164. MALAN, Diogo. Métodos ocultos, devido processo e o enfrentamento à criminalidade organizada. In: **Direitos fundamentais e processo penal na era digital: doutrina e prática em debate**. [Em linha] São Paulo: InternetLab, v. 4, 2021. [Consul. 21 Mar. 2022] ]Disponível em: https://congresso.internetlab.org.br/livros/. [↑](#footnote-ref-164)
165. VALENTE, Manuel Monteiro Guedes. Meios ocultos de investigação: Contributo mínimo para uma reflexão maior. [Em linha] **Revista Brasileira de Ciências Criminais**, São Paulo-SP, 21 de Agosto de 2015 [Consult. 22 Mar. 2022]. Disponível em https://www.ibccrim.org.br/noticias/exibir/6323/ [↑](#footnote-ref-165)
166. PEREA, Inmaculada Lopez-Barajas. Garantias Constitucionales en la Investigacion Tecnológica del delito: previsión legal y calidad. **Revista de derecho político**, Madrid, n 98, enero-abril, p. 91-119, 2017. ISSN 0211-979X. p. 11 [↑](#footnote-ref-166)
167. RAMALHO, David Silva. **Métodos Ocultos de Investigação Criminal em Ambiente Digital.** Coimbra: Almedina, 2017. ISBN 978-97-2407-00-0-1. p. 211. [↑](#footnote-ref-167)
168. *Ibid*., p. 212. [↑](#footnote-ref-168)
169. *Ibid*., p. 213. [↑](#footnote-ref-169)
170. VALENTE, Manuel Monteiro Guedes -O Reforço dos Princípios Constitucionais na Obtenção de Prova no Mundo Digital. **Corpus Delicti** **Revista de Direito de Policia Judiciária**, Brasília. ISSN 2526-4265 e-ISSN: 2526-9623, Ano 2, n° 3 (Janeiro-Junho 2018), p. 13. [↑](#footnote-ref-170)
171. *Ibid*., p. 15. [↑](#footnote-ref-171)
172. *Ibid*. [↑](#footnote-ref-172)
173. PORTUGAL. Decreto-Lei n° 78/87. **Diário da República I Série**, n° 40, 17-02-1987. [Em Linha] Lisboa, 1987. [Consult. 03 Mar. 2022] Disponível em: https://dre.pt/dre/legislacao-consolidada/decreto-lei/1987-34570075-50539675. [↑](#footnote-ref-173)
174. RAMALHO, David Silva. **Métodos Ocultos de Investigação Criminal em Ambiente Digital.** Coimbra: Almedina, 2017. ISBN 978-97-2407-00-0-1. p. 215. [↑](#footnote-ref-174)
175. VALENTE, Manuel Monteiro Guedes -O Reforço dos Princípios Constitucionais na Obtenção de Prova no Mundo Digital. **Corpus Delicti** **Revista de Direito de Policia Judiciária**, Brasília. ISSN 2526-4265 e-ISSN: 2526-9623, Ano 2, n° 3 (Janeiro-Junho 2018), p. 16. [↑](#footnote-ref-175)
176. *Ibid*. [↑](#footnote-ref-176)
177. RAMALHO, David Silva. **Métodos Ocultos de Investigação Criminal em Ambiente Digital.** Coimbra: Almedina, 2017. ISBN 978-97-2407-00-0-1. p. 227 [↑](#footnote-ref-177)
178. *Ibid*. [↑](#footnote-ref-178)
179. VALENTE, Manuel Monteiro Guedes - O Reforço dos Princípios Constitucionais na Obtenção de Prova no Mundo Digital. **Corpus Delicti Revista de Direito de Policia Judiciária**, Brasília. ISSN 2526-4265 e-ISSN: 2526-9623, Ano 2, n° 3 (Janeiro-Junho 2018), p. 17. [↑](#footnote-ref-179)
180. *Ibid*. [↑](#footnote-ref-180)
181. *Ibid*., p. 235*.* [↑](#footnote-ref-181)
182. RAMALHO, David Silva. **Métodos Ocultos de Investigação Criminal em Ambiente Digital.** Coimbra: Almedina, 2017. ISBN 978-97-2407-00-0-1. p. 236. [↑](#footnote-ref-182)
183. VALENTE, Manuel Monteiro Guedes -O Reforço dos Princípios Constitucionais na Obtenção de Prova no Mundo Digital. **Corpus Delicti** **Revista de Direito de Policia Judiciária**, Brasília. ISSN 2526-4265 e-ISSN: 2526-9623, Ano 2, n° 3 (Janeiro-Junho 2018), p. 17. [↑](#footnote-ref-183)
184. REVORIO, Francisco Javier Díaz. La constitución ante los avances científicos y tecnológicos: breves reflexiones al hilo de los recientes desarrollos en materia genética y en tecnologías de la información y la comunicación. [Em linha**]. Revista de Derecho Político de la UNED**, nº 71-72, 2008. p. 87-110. [Consult. 17 Mar. 2022]. Disponível em https://revistas.uned.es/index.php/derechopolitico/article/view/9040. ISSN 0211-979X. p. 105. [↑](#footnote-ref-184)
185. KIST, Dario José. **Prova digital no processo penal**. Leme: JH Mizuno, 2019, p. 384. ISBN 978-85-7789-430-7. p. 283. [↑](#footnote-ref-185)
186. *Ibid.*, p. 283. [↑](#footnote-ref-186)
187. SENDRA, Vicente Gimeno. **Derecho Procesal Penal**. Civitas. Navarra. Ediciones Jurídicas Castillo de Luna. S.L.; 1ª edição. 2015. ISBN 978-8494276446. p. 350-354. [↑](#footnote-ref-187)
188. CASTROVERDE, Córdoba Diego; GIMÉNEZ, Ignácio Diez-Picazo. Reflexiones sobre los retos de la protección de la privacidad en un entorno tecnológico. In: **El derecho a la privacidad en un entorno tecnológico.** [Em linha] Madrid, 2016. [Consult. 19 Mar. 2022] Disponível em: https://www.tribunalconstitucional.es/es/publicaciones/Publicaciones/ALTC-Jornada-20.pdf [↑](#footnote-ref-188)
189. É o caso da Constituição da República Portuguesa que prevê o direito à reserva da intimidade da vida privada no artigo 26, n.º 1: A todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à protecção legal contra quaisquer formas de discriminação. E, a Constituição brasileira que dispõe sobre o direito à privacidade no artigo 5º, inciso X: são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação. [↑](#footnote-ref-189)
190. KIST, Dario José. **Prova digital no processo penal**. Leme: JH Mizuno, 2019, p. 384. ISBN 978-85-7789-430-7. p. 290. [↑](#footnote-ref-190)
191. *Ibid*., p. 293. [↑](#footnote-ref-191)
192. Dario José Kist assevera que “nesta oportunidade é importante mencionar a existência da Teoria dos Círculos de Proteção, concebida por Heinrich Hubmann. Dario José Kist ao comentar essa teoria assevera que “essa teoria gravita em torno dos direitos da personalidade: cada indivíduo tem o direito ao livre desenvolvimento da sua personalidade, fundamentado juridicamente no direito geral de ação, que na Alemanha tem assento constitucional; e, no contexto, um dos elementos essenciais ligados à personalidade é a individualidade, a que garante a singularidade do indivíduo e que, dada essa relevante função, exige proteção contra a massificação e a curiosidade alheia; essa proteção, segundo o autor em questão, deve ser conferida em três níveis, círculos ou esferas: a esfera individual, a esfera privada e a esfera secreta ou íntima. E, na sua perspectiva, essas três esferas poderiam ser representadas por três anéis ou círculos concêntricos, exatamente para evidenciar a necessidade de maior proteção para o círculo, exatamente para evidenciar a necessidade de maior proteção para o círculo mais interno, o da esfera íntima, afrouxando-se, paulatinamente, o rigor da tutela em relação aos outros”. [↑](#footnote-ref-192)
193. PORRAS, Andrés José González. **A. Privacidad en Internet: Los derechos fundamentales de privacidad e intimidad en internet y su regulación jurídica. La vigilancia masiva.** [Em linha] 2015 [Consult. 18 Mar. 2022] Disponível em: https://dialnet.unirioja.es/servlet/tesis?codigo=80236. [↑](#footnote-ref-193)
194. JONES, M. Jackson. **The Fourth Amendment and Search Warrant Presentment: Is a Man's House Always his Castle.** [Em linha] 2011 [Consult. 17 Mar. 2022] Disponível em: https://heinonline.org/HOL/LandingPage?handle=hein.journals/amjtrad35&div=37&id=&page= [↑](#footnote-ref-194)
195. Nenhum soldado poderá, em tempo de paz, ser aquartelado em qualquer casa, sem o consentimento do proprietário, nem em tempo de guerra, mas de forma a ser prescrita pela lei. [↑](#footnote-ref-195)
196. A Quarta Emenda à Constituição dos Estados Unidos é uma das emendas feitas na Carta dos Direitos e refere-se à proteção contra buscas e apreensões arbitrárias e foi instituída como resposta aos abusos do controverso *writ of assistance*, um tipo de mandado geral de busca emitido pelo governo colonial britânico e que foi uma importante fonte de tensão na América pré-revolucionária. [↑](#footnote-ref-196)
197. A emenda traz a cláusula de devido processo legal, segundo a qual "ninguém pode ser privado de sua vida, liberdade ou propriedade sem o devido processo legal de todos os humanos" [↑](#footnote-ref-197)
198. COOLEY, Thomas McIntyre. **A Treatise on the Constitutional Limitations which rest upon the legislative power of the States of the American Union**. Little, Brown & Co: Boston, 1868. [Em linha] [Coonsult. 17 Mar. 2022] Disponível em: https://repository.law.umich.edu/books/10/ [↑](#footnote-ref-198)
199. O congresso não deverá fazer qualquer lei a respeito de um estabelecimento de religião, ou proibir o seu livre exercício; ou restringindo a liberdade de expressão, ou da imprensa; ou o direito das pessoas de se reunirem pacificamente, e de fazerem pedidos ao governo para que sejam feitas reparações de queixas. [↑](#footnote-ref-199)
200. SALDAÑA, Maria Nieves. The Right to Privacy. La génesis de la protección de la privacidad en el sistema constitucional norteamericano: el centenario legado de Warren y Brandeis. [Em linha] **Revista De De-recho Político**, 85, p. 195-240, 2012. [Consult. 17 Mar. 2022] Disponível em: <https://www>. researchgate. net/publication/256544041\_THE\_RIGHT\_TO\_PRIVACY\_LA\_GENESIS\_DE\_LA\_PROTECCION\_DE\_LA\_PRIVACIDAD\_EN\_EL\_SISTEMA\_CONSTITUCIONAL\_NORTEAMERICANO\_EL\_CENTENARIO\_LEGADO\_DE\_WARREN\_Y\_BRANDEIS\_The\_Right\_to\_Privacy\_The\_Genesis\_of\_the\_Protecti [↑](#footnote-ref-200)
201. KENT JR, Michael B. **Pavesich, Property and Privacy:** **The Common Origins of Property Rights and Privacy Rights**, [Em linha] 2009 [Consult. 17 Mar 2022] Disponível em: <https://scholarship.law>. campbell.edu/cgi/viewcontent.cgi?article=1077&context=fac\_sw. [↑](#footnote-ref-201)
202. CLÍMACO VALIENTE, Ernesto. **Génesis histórico-normativa del derecho a la protección de los datos personales desde el derecho comparado a propósito de su fundamento**. [Em linha], ano 2012 [Consult. 18 Mar. 2022] Disponível em: https://e-archivo.uc3m.es/handle/10016/18785#preview. [↑](#footnote-ref-202)
203. CASTRO, Catarina Sarmento e. **Direito da informática, privacidade e dados pessoais.** Coimbra: Almedina, 1ª ed. 2005. ISBN-13: 978-9724024240. p. 339 [↑](#footnote-ref-203)
204. DECLARAÇÃO Universal dos Direitos Humanos. 10 de dezembro de 1948. [Em linha] [Consult. 19 Mar. de 2022]. .Disponível em: https://brasa.org.br/declaracao-universal-dos-direitos-humanos/?gclid=Cj0KCQjw1PSD BhDbARIsAPeTqrfRLDqHzL\_deuqOryQjJHC2jl\_93jSN2Zme\_t-QDig0gFBQxMaor84aAm12EALw\_wcB. [↑](#footnote-ref-204)
205. BITTAR, 1994, p.107 apud GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. **Novo curso de direito civil**. 11ª ed. São Paulo: Saraiva, 2009, volume 1. ISBN 978-6555594461. p. 171. [↑](#footnote-ref-205)
206. SILVA, José Afonso da. **Curso de direito constitucional positivo**. 43ª ed. São Paulo: Malheiros, 2020. ISBN: 978-85-392-0462-5. p. 206. [↑](#footnote-ref-206)
207. KIST, Dario José. **Prova digital no processo penal**. Leme: JH Mizuno, 2019, p. 384. ISBN 978-85-7789-430-7. p. 110-111. [↑](#footnote-ref-207)
208. Art. 10. Lei 12.965/2014. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas. [↑](#footnote-ref-208)
209. Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet. Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade: I - fundados indícios da ocorrência do ilícito; II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e III - período ao qual se referem os registros. Art. 23. Cabe ao juiz tomar as providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, da vida privada, da honra e da imagem do usuário, podendo determinar segredo de justiça, inclusive quanto aos pedidos de guarda de registro. [↑](#footnote-ref-209)
210. Artigo 8º. Intercepção ilegítima. 1- Quem, sem para tanto estar autorizado, e através de meios técnicos, interceptar comunicações que se processam no interior de um sistema ou rede informáticos, a eles destinadas ou deles provenientes, será punido com pena de prisão até três anos ou com pena de multa. 2- A tentativa é punível. [↑](#footnote-ref-210)
211. RUIZ, Estrella. Entrada y registro, interceptaciones de comunicaciones postales, telefónicas, etc. In: **Medidas restrictivas de los derechos fundamentales**. CDJud: Madrid, 1996, p. 354. [↑](#footnote-ref-211)
212. MARTINEZ, Gregorio Peces-Barba. **Curso de Derechos Fundamentales**. Universidad Carlos III, Boletín

del Estado, Madrid, 1995. ISSN 0213-9995. p. 590. [↑](#footnote-ref-212)
213. SIMAS, Diana Viveiros de. **O Cibercrime**. Dissertação apresentada no âmbito do 2.º Ciclo de Estudos em Direito, no Curso de Mestrado em Ciências Jurídico-Forenses, conferido pela Universidade Lusófona de Humanidades e Tecnologias, sob orientação do Prof. Dr. José Sousa Brito, Lisboa, 2014. pág. 71. [↑](#footnote-ref-213)
214. MARQUES, Garcia; MARTINS, Lourenço. **Direito da Informática.** 2ª ed. Coimbra: Almedina, 2006. ISBN 978-9724028590. p. 663. [↑](#footnote-ref-214)
215. VENÂNCIO, Pedro Dias. **Lei do Cibercrime Anotada e Comentada**. Coimbra: Coimbra Editora, 2011. ISBN: 9789723219067. pág. 16. [↑](#footnote-ref-215)
216. RODOTÀ, Stefano. Democracia y protección de datos. [Em Linha] **Cuardenos de Derecho Publico**, 1997/2007, n° 19-20. [Consult. 21 Mar. 2022] ISSN 1989-8967. p.16. Disponível em: <https://revistasonline>.inap.es/index.php/CDP/article/view/690/745 . [↑](#footnote-ref-216)
217. XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; [↑](#footnote-ref-217)
218. Artigo 34.º - Inviolabilidade do domicílio e da correspondência: 1. O domicílio e o sigilo da correspondência e dos outros meios de comunicação privada são invioláveis. [↑](#footnote-ref-218)
219. Artigo 35 – Utilização da Informática: 1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei. [↑](#footnote-ref-219)
220. CASTRO, Catarina Sarmento e. **Direito da Informática, Privacidade e Dados pessoais**. Coimbra. Edições Almedina. 2005. ISBN: 9789724024240. p. 32. [↑](#footnote-ref-220)
221. A Lei 10/91, de 27 de abril, inseriu os princípios constantes na Convenção n.º 108, adotada pelo Conselho da Europa em 28 de janeiro de 1981, protegendo os dados informatizados pessoais das pessoas singulares. O objetivo desta Convenção era tutelar a intimidade e garantir o funcionamento do mercado interior e a livre circulação de dados pessoais entre os Estados-membros da União. [↑](#footnote-ref-221)
222. CRATO, Nuno Teixeira. **The Walking Virtually Dead: Entre uma Algoritmocracia Jus Constituendum e um Homem Virtual Transparente, Existe Espaço para o Direito a uma Identidade Informacional?** Lisboa: Universidade de Lisboa, 2016. 136 f. Tese de Mestrado em Segurança da Informação e Direito no Ciberespaço, p. 34. [↑](#footnote-ref-222)
223. LEI n.º 67/98. **Diário da República Série I-**A n.º 247/1998 (26-10-1998), p. 5536 – 5546 [Em linha] [Consult. 21 Mar. 2022]. Disponível em: https://data.dre.pt/eli/lei/67/1998/10/26/p/dre/pt/html https://dre.pt/dre/detalhe/ lei/67-1998-239857. [↑](#footnote-ref-223)
224. Também são considerados dados pessoais, entre outros, o nome, morada, residência, local de trabalho, endereço do correio eletrónico, o nº de telefone, n.º de cartão de cidadão, o n.º fiscal, o tipo sanguíneo, o IBAN da conta bancária, bem como demais elementos que, por estarem associados a uma pessoa, permitam identificá-la. [↑](#footnote-ref-224)
225. LEI n.º 67/98. **Diário da República Série I-**A n.º 247/1998 (26-10-1998), p. 5536 – 5546 [Em linha] [Consult. 21 Mar. 2022]. Disponível em: https://dre.pt/dre/detalhe/lei/67-1998-239857. [↑](#footnote-ref-225)
226. LEI n.º 41/04. **Diário da República Série I-**A n.º 194/2004 (18-08-2004), p. 5241 – 5245 [Em linha] [Consult. 21 Mar. 2022]. Disponível em: https://dre.pt/dre/detalhe/lei/41-2004-480710. [↑](#footnote-ref-226)
227. LEI n.º 05/04. **Diário da República Série I-**A n.º 34/2004 (10-02-2004), p. 788 – 821 [Em linha] [Consult. 21 Mar. 2022]. Disponível em: https://dre.pt/dre/detalhe/lei/5-2004-581061. [↑](#footnote-ref-227)
228. LEI n.º 32/08. **Diário da República Série I-**A n.º 137/2008 (17-07-2008), p. 4454 – 4458 [Em linha] [Consult. 21 Mar. 2022]. Disponível em: https://dre.pt/dre/detalhe/lei/32-2008-456812 [↑](#footnote-ref-228)
229. REGULAMENTO Geral de Proteção de Dados. **Jornal Oficial da União Europeia,** 04-05-2016. [Em linha] 59º Ano. Edição em língua portuguesa. [Consult. 22 Mar. 2022] Disponível em: [https://www.sg.pcm.gov.pt/sobre-nos/regulamento-geral-de-prote%C3%A7%C3%A3o-de-dados.aspx#:~:text=O%20 Regulamento%20 (UE)% 20 20](https://www.sg.pcm.gov.pt/sobre-nos/regulamento-geral-de-prote%C3%A7%C3%A3o-de-dados.aspx#:~:text=O%20 Regulamento%20  (UE)% 20 20)16%2F,relativos%20a%20pessoas%20na%20UE. [↑](#footnote-ref-229)
230. TEIXEIRA, Angelina. A Chave para a Regulamentação da Proteção de Dados. **Data Venia Revista Jurídica Digital,** n.º 6. Novembro 2016. ISSN 2182-6242. p. 6-32. [↑](#footnote-ref-230)
231. LEI n°13.709 de 14 de agosto de 2018. [Em linha] **Diário Oficial da União**. [Consult. 22 jan.2022] Disponível em: de http://www.planalto.gov.br/ccivil\_03/\_ato2015-2018/2018/lei/l13709.htm [↑](#footnote-ref-231)
232. BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil:** promulgada em 5 de outubro de 1988. [Em linha] [Consult. 22 Mar. 2022]. Disponível em: <http://www>. planalto.gov.br/ccivil\_03/ constituicao/constituicao.htm [↑](#footnote-ref-232)
233. Contexto y antecedentes de la legislación europea en materia de protección de datos: El derecho a la protección de los datos Tratado de Funcionamiento de la Unión Europea, artículo 16; Carta de los Derechos Fundamentales de la Unión Europea (la Carta), artículo 8 (derecho a la protección de los datos personales); Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Directiva sobre protección de datos), DO 1995 L 281 (en vigor hasta mayo de 2018); Decisión Marco 2008/977/JAI del Consejo relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, DO 2008 L 350 (en vigor hasta mayo de 2018); Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), DO 2016 L 119; Directiva (UE) 2016/680 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (protección de datos para las autoridades policiales y judiciales), DO 2016 L 119; Directiva 2002/58/CE relativa al tratamento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), DO 2002 L 201; Reglamento (CE) n.o 45/2001 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (Reglamento de protección de datos de las instituciones de la UE), DO 2001 L 8. (https://fra.europa.eu/sites/default/files/fra\_uploads/fra-coe-edps-2018-handbook-data-protection\_es.pdf) [↑](#footnote-ref-233)
234. VALENTE, Manuel Monteiro Guedes. O Reforço dos Princípios Constitucionais na Obtenção de Prova no Mundo Digital. **Corpus Delicti Revista de Direito de Policia Judiciária,** Brasília. ISSN 2526-4265 e-ISSN: 2526-9623, Ano 2, n° 3 (Janeiro-Junho 2018), p. 14. [↑](#footnote-ref-234)
235. RODRIGUES, Benjamim Silva. **Da prova penal: Tomo IV – Da prova-electrónico digital e da criminalidade informático-digital.** Lisboa: Rei dos Livros, 2011. ISBN: 9789898305183. p. 39. [↑](#footnote-ref-235)
236. VALENTE, Manuel Monteiro Guedes. Editorial dossiê “Investigação preliminar, meios ocultos e novas tecnologias”. **Revista Brasileira de Direito Processual Penal**, Porto Alegre, vol. 3, n. 2, p. 473-482, mai./ago. 2017. ISSN 2525-510x. [Consult. 10 Mar. 2022] Disponível em https://doi.org/10.22197/rbdpp.v3i2.82. p. 474. [↑](#footnote-ref-236)
237. *Ibid*., p. 475. [↑](#footnote-ref-237)
238. Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; LVI - são inadmissíveis, no processo, as provas obtidas por meios ilícitos; LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. [↑](#footnote-ref-238)
239. Artigo 26.º - Outros direitos pessoais: 1. A todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à proteção legal contra quaisquer formas de discriminação. 2. A lei estabelecerá garantias efetivas contra a obtenção e utilização abusivas, ou contrárias à dignidade humana, de informações relativas às pessoas e famílias. 3. A lei garantirá a dignidade pessoal e a identidade genética do ser humano, nomeadamente na criação, desenvolvimento e utilização das tecnologias e na experimentação científica. 4. A privação da cidadania e as restrições à capacidade civil só podem efetuar-se nos casos e termos previstos na lei, não podendo ter como fundamento motivos políticos. (<https://www.parlamento.pt/>Legislacao/Pag inas/ConstituicaoRepublicaPortuguesa.aspx) [↑](#footnote-ref-239)
240. GOUVEIA, Jorge Bacelar. **Manual de Direito Constitucional**. Coimbra: Almedina, 2016. ISBN 978-9724067964. p. 57 [↑](#footnote-ref-240)
241. DELGADO, Joaquín Martín. La prueba del whatsapp. **Diario La Ley**, núm. 8605, Sección Tribuna, 15 Sep.2015, Ref. D-331, Editorial LA LEY [Em linha] [Consult. 23 Mar. 2022] Diisponível em: https://docplayer.es/25786992-La-prueba-del-whatsapp-joaquin-delgado-martin-magistrado-de-la-audiencia-pr ovincial-de-madrid-doctor-en-derecho.html. [↑](#footnote-ref-241)
242. *Ibid*. [↑](#footnote-ref-242)
243. RODRIGUES, Benjamim Silva. **Da prova penal: Tomo IV – Da prova-electrónico digital e da criminalidade informático-digital.** Lisboa: Rei dos Livros, 2011. ISBN: 9789898305183. p. 31. [↑](#footnote-ref-243)