OSSIAN BEZERRA PINHO FILHO

INVESTIGAÇÃO CRIMINAL TECNOLÓGICA –
A infiltração por *malware* nas investigações informáticas

Dissertação de mestrado com vistas à obtenção do grau de Mestre em Direito e Segurança, pela Faculdade de Direito da Universidade Nova de Lisboa.

Orientador:
Prof. Doutor José Fontes

OUTUBRO/2020

OSSIAN BEZERRA PINHO FILHO

INVESTIGAÇÃO CRIMINAL TECNOLÓGICA –
A infiltração por *malware* nas investigações informáticas

Dissertação de mestrado com vistas à obtenção do grau de Mestre em Direito e Segurança, pela Faculdade de Direito da Universidade Nova de Lisboa.

Orientador:
Prof. Doutor José Fontes

NOVA SCHOOL OF LAW

INVESTIGAÇÃO CRIMINAL TECNOLÓGICA – A infiltração por *malware* nas investigações informáticas

Ossian Bezerra Pinho Filho, estudante nº **6136**, declaro sob compromisso de honra que o conteúdo deste trabalho é original, de minha autoria, e todas as fontes consultadas estão mencionadas no texto, nas notas e nas referências.

OSSIAN BEZERRA PINHO FILHO:01070490

Assinado de forma digital por OSSIAN BEZERRA PINHO FILHO:01070490
Dados: 2020.11.16 11:18:22 -03'00'

Lisboa, 13 de outubro de 2020.

Dedico este trabalho ao meu amado e inesquecível pai Ossian Bezerra Pinho (*in memoriam*), que sempre me encorajou a buscar a realização dos meus objetivos pessoais e profissionais e, antes de partir, ainda no primeiro ano desse curso, incentivou-me a ter forças para prosseguir até o fim, mantendo firme a fé em Deus.

AGRADECIMENTOS

Agradeço a Deus, em primeiro lugar, por ter me permitido alcançar tão almejado propósito de qualificação pessoal, que certamente contribuirá não só para o meu crescimento acadêmico, mas sobretudo profissional.

Ao meu orientador, Professor Doutor José Fontes, pela oportunidade de aprender com os seus ensinamentos, por seu acolhimento e dedicação no direcionamento dessa pesquisa, desde a escolha do tema até a sua conclusão.

Expresso também o meu agradecimento ao Ministério Público do Estado do Maranhão, na pessoa do então Procurador-Geral de Justiça, Doutor Luiz Gonzaga Martins Coelho, instituição da qual me orgulho de fazer parte e que permitiu o meu afastamento para participar de tão qualificado curso de mestrado.

Agradeço aos meus amigos do grupo "*Friends*", pela demonstração de amizade, compreensão e incentivo, os quais, mesmo de longe, sempre estiveram presentes, encorajando a mim e a minha família a superar todos os desafios de permanecermos um ano distantes de nossos parentes e amigos.

Agradeço à minha mãe, aos meus irmãos e a toda a minha família que sempre manifestaram apoio irrestrito aos meus planos pessoais e profissionais.

Por fim, agradeço, em especial, à minha amada esposa, Lidiane Rosas Pinho, e aos meus filhos, Letícia Rosas Pinho e João Pedro Rosas Pinho, que superaram enormes desafios para estarem ao meu lado em outro país, durante um ano, sem a presença dos quais não teria conseguido superar a perda do meu pai e chegar até essa fase final do curso de mestrado. Minha eterna gratidão a vocês.

Resumo

O presente estudo objetiva analisar a possibilidade de o Estado brasileiro fazer uso da técnica de infiltração por *malware* na busca e recolha de dados informáticos para fins de investigação criminal, bem como os requisitos e os limites para a utilização desse método especial de investigação em ambiente digital. Para tanto, aborda a investigação criminal entre a eficiência e a proteção dos direitos fundamentais; discute a investigação criminal tecnológica e as limitações condicionadas pelo direito probatório; e discute a possibilidade de uso da infiltração por *malware* nas investigações informáticas levando-se em conta a experiência do direito comparado, a liberdade probatória e a legalidade dos métodos inovadores de investigação criminal em face do direito fundamental à reserva da intimidade da vida privada, o direito ao segredo das comunicações, o direito à autodeterminação informacional, o direito à integridade e o direito à confiabilidade dos sistemas informáticos. Foi visto que os métodos tradicionais de investigação criminal se mostram insuficientes para ultrapassar as dificuldades impostas à persecução criminal nesse complexo ambiente da atual sociedade em rede e em risco. É inevitável, portanto, que haja uma reação do sistema jurídico no sentido de permitir que o Estado-persecutor utilize-se dos avanços tecnológicos que impliquem investigações mais invasivas e insidiosas aos direitos fundamentais, para fazer frente à paralela evolução de práticas criminosas mais graves. Do exposto, concluiu-se pela possibilidade de uso do *malware* estatal como um dos meios de investigação ou de obtenção de prova por meio de intervenção legislativa com vistas à criação de um regime jurídico específico para o uso de *malware* estatal nas investigações criminais, definindo e delimitando o âmbito de utilização dessa ferramenta tecnológica a partir de critérios de justificação constitucional para a restrição dos direitos fundamentais envolvidos. Não obstante, na ausência de um regime legal específico, incumbe ao Poder Judiciário a avaliação casuística da possibilidade de autorizar o recurso ao *malware* estatal, enquanto medida investigativa inovadora, para compensar o déficit legislativo, em casos excepcionalmente desafiadores, decorrente da interpretação extensiva ou aplicação analógica de outros instrumentos já consolidados no ordenamento jurídico, obedecidos os mandamentos da excepcionalidade, provisoriedade, proporcionalidade e rígido controle judicial.

Palavras-chave: Investigação criminal. *Malware* estatal. Direitos fundamentais.

Abstract

The present study aims to analyze the possibility for the Brazilian State to use the technique of infiltration by malware in the search and collection of computer data for criminal investigation purposes, as well as the requirements and limits for the use of this special investigation method in a digital environment. To this end, it addresses the criminal investigation between efficiency and the protection of fundamental rights; discusses the technological criminal investigation and the limitations conditioned by the evidential law; and discusses the possibility of using malware infiltration in computer investigations taking into account the experience of comparative law, probative freedom and the legality of innovative methods of criminal investigation in view of the fundamental right to reserve the privacy of privacy, the right to confidentiality of communications, the right to informational self-determination, the right to integrity and the right to reliability of computer systems. It was seen that traditional methods of criminal investigation are insufficient to overcome the difficulties imposed on criminal prosecution in this complex environment of today's networked and at-risk society. It is inevitable, therefore, that there should be a reaction from the legal system in order to allow the persecuting State to use technological advances that imply more invasive and insidious investigations of fundamental rights, in order to face the parallel evolution of more serious criminal practices. From the above, it was concluded that it is possible to use state malware as one of the means of investigation or to obtain evidence through legislative intervention with a view to creating a specific legal regime for the use of state malware in criminal investigations, defining and delimiting the scope of use of this technological tool based on constitutional justification criteria for the restriction of the fundamental rights involved. However, in the absence of a specific legal regime, the Judiciary is responsible for the casuistic assessment of the possibility of authorizing the use of state malware, as an innovative investigative measure, to compensate for the legislative deficit, in exceptionally challenging cases, resulting from extensive interpretation or application analogous to other instruments already consolidated in the legal system, obeying the commandments of exceptionality, provisionality, proportionality and strict judicial control.

***Keywords*:** Criminal investigation. State malware. Fundamental rights.

Siglas e abreviaturas

AA.VV. – Vários autores

ADI – Ação Direta de Inconstitucionalidade

ADPF - Ação de Descumprimento de Preceito Fundamental

ARPA - *Advanced Research Projets Agency*

ARPANET - *Advanced Research Projects Agency Network*

CARICOM – Comunidade do Caribe

CEDH – Convenção Europeia dos Direitos do Homem

Cf. – Confrontar, ver também, referir-se a

CIPAV – *Computer and IP Address Verifier*

Cit., cits. – Citado, citada, cita-se; citação, citações

CP – Código Penal

CPP – Código de Processo Penal

CRFB – Constituição da República Federativa do Brasil

DDoS - *Distributed denial-of-service*

DEC - *Digital Equipment Corporation*

DF – Distrito Federal

DJ – Diário de Justiça

DJe – Diário de Justiça Eletrônico

DUDH – Declaração Universal dos Direitos Humanos

E. g. – (*Exempli grati*) por exemplo

ERBS – Estações rádio base

Et al. – (Et alii) e outros

EUA – Estados Unidos da América

FBI – Federal Bureau of Investigation

GCHQ - *Government Communications Headquarters*

GPS - *Global Position System*

HC – *Habeas Corpus*

HIPCAR - *Harmonization of ICT policies and legislation across*

Icann - Corporação da internet para Atribuição de Nomes e Números

IETF - *Internet Engineering Task Force*

IMEI - *International Mobile Equipment Identity*

IMSI - *International Mobile Subscriber Identity*

IP – *Internet Protocol*

JIC – Juízo Informal de Conciliação

MAC - *Media Access Control*

MIL-NET - *Military Network*

MP – Ministério Público

MS – Mato Grosso do Sul

NCF - *National Sciense Foundation*

NIST - *Nacional Institute for Standards and Technology*

ONU – Organização das Nações Unidas

PI - Piauí

PIC – Procedimento de Investigação Criminal

PNUD - Programa das Nações Unidas para o Desenvolvimento

RE – Recurso Extraordinário

RFC - Diretrizes para Coleta e Arquivamento de Evidências

RHC – Recurso em *Habeas Corpus*

RMS – Recurso em mandado de segurança

RS – Rio Grande do Sul

SMS - *Short Message Service*

STF – Supremo Tribunal Federal

STJ – Superior Tribunal de Justiça

SWGDE - *Scientific Working Groupon Digital Evidence*

TI – Tecnologia da Informação

TICs – Tecnologias da Informação e Comunicação

TJDF – Tribunal de Justiça do Distrito Federal

TJMT – Tribunal de Justiça do Mato Grosso

TJSP – Tribunal de Justiça de São Paulo

TRE – Tribunal Regional Eleitoral

UE – União Europeia

USB – *Universal Serial Bus*

USC - *United States Code*

VoIP - *Voice over Internet Protocol*

WWW - *World Wide Web*

ÍNDICE

INTRODUÇÃO

A sociedade contemporânea, em âmbito mundial, está inserida em um contexto de crescente complexidade das relações sociais, oriunda de importantes transformações provocadas pelo acelerado desenvolvimento dos recursos tecnológicos notadamente nas áreas da informação e da comunicação.

Vivenciamos a Era Digital1 baseada no novo paradigma tecnológico, que tem como uma de suas principais características a lógica de redes, por meio da qual se cria um espaço virtual mundialmente interligado onde é possível circular um número incalculável de informação, além de proporcionar a comunicação e a interação à distância.

O acelerado desenvolvimento tecnológico que se tem verificado nomeadamente nas últimas décadas, em constante evolução e sob ritmo alucinante, certamente contribuiu e continua a contribuir para o progresso da humanidade, nos mais diversos setores. Facilita-se o acesso à informação e ao conhecimento, rompem-se as barreiras geográficas e aproximam-se as pessoas por meio de canais de comunicação, de forma rápida, fácil e barata.

Por outro lado, em paralelo ao progresso, as novas ferramentas tecnológicas abrem espaço para a prática de atividades criminosas cada vez mais complexas e de difícil elucidação. As ameaças e os riscos se multiplicam na mesma velocidade da modernização tecnológica e da complexidade das relações sociais e assumem um caráter cada vez mais difuso e complexo.

Nessa perspectiva, o cenário político-social atual impõe desafios cada vez mais complexos aos Estados Democráticos de Direito no cumprimento de sua tarefa mais fundamental, associada ao compromisso da soberania, que é a de garantir segurança, ou seja, propiciar estabilidade individual e coletiva aos indivíduos, garantindo-lhes o direito fundamental à vida e à segurança como requisito indispensável para o exercício dos demais direitos relacionados à atividade humana.

No entanto, como bem adverte Bacelar Gouveia (2018, p.97), "o reforço da segurança como fim do Estado não pode fazer-se à custa da democracia e da liberdade dos cidadãos, criando-se um novo conjunto de opções dilemáticas em termos políticos e em termos jurídicos".

---

1 Era digital ou era da informação são expressões comumente utilizadas para designar o período histórico iniciado a partir dos avanços tecnológicos derivados da evolução informática, notadamente no âmbito da informação e da comunicação, tendo como uma de suas principais características a emergência e a difusão do ciberespaço. É nesse período, o qual se vivencia na atualidade, que surge a denominação de sociedade da informação ou da comunicação.

Ainda segundo a lição de Bacelar Gouveia (2018, p.658), "a investigação criminal coloca-se num ponto específico de relação entre a segurança e a justiça, fazendo a transição de uma dimensão policial para uma dimensão punitiva de natureza criminal perante um facto ocorrido". Nesta senda, exsurge o desafio de compatibilizar a necessidade de reforço de métodos de prevenção e repressão da criminalidade compatíveis com as demandas atuais da sociedade da informação, e os novos riscos decorrentes da utilização de recursos tecnológicos, com a preservação das garantias humanitárias fundamentais ao controle do exercício do poder punitivo estatal.

Embora não se possa atribuir à investigação criminal a função de garantia da segurança, com esta se relaciona à medida em que o dever estatal de garantir segurança não se circunscreve apenas a evitar condutas criminosas, mas também alcança a escorreita apuração das atividades ilícitas e, sendo o caso, a punição de seus reais responsáveis, com estrita obediência aos direitos e garantias fundamentais.

A pesquisa justifica-se, assim, em razão da atualidade das discussões acerca do reforço de métodos especiais de investigação criminal assentados na evolução tecnológica, ante a insuficiência dos métodos tradicionais nesse complexo ambiente da atual sociedade em rede e em risco.

Pretendeu-se, pois, explorar a temática sempre atual concernente aos métodos ocultos de investigação criminal no ambiente digital, com recorte específico à infiltração por *malware* nas investigações informáticas. Não se teve a presunção de esgotar o tema que, além de atual, caracteriza-se pela perene atualização correspondente ao paralelo desenvolvimento dos recursos tecnológicos.

A pesquisa foi realizada tomando-se como ponto de partida a premissa sociológica da sociedade de risco e o novo paradigma tecnológico que a norteia, de um lado, e a problematização da utilização pelo Estado de técnicas e tecnologias modernas e invasivas na investigação criminal, enquanto instrumentos de eficácia no ambiente digital, de outro, levando-se em conta os direitos e garantias fundamentais inalienáveis do Estado Democrático de Direito, em termos jurídicos.

O presente ensaio materializa uma pequena parcela dessa problematização, cujo desenvolvimento é inspirado em obter respostas ao problema traduzido nas perguntas: É possível o Estado brasileiro fazer uso da técnica de infiltração por *malware* na busca e recolha de dados informáticos para fins de investigação criminal? Em caso positivo, quais os requisitos e os limites para a utilização desse método especial de investigação em ambiente digital?

Na busca pelas respostas à questão problema, partiu-se inicialmente, em termos gerais, da hipótese de que os métodos tradicionais de investigação criminal já não se mostram suficientes nesse cenário de evolução tecnológica, exigindo-se do Estado, enquanto gestor da segurança e da justiça, o reforço de métodos especiais de investigação compatíveis com a complexidade presente no novo ambiente digital. Ainda em termos gerais, mas sob o enfoque jurídico, a proposição inicial volveu-se na perspectiva das finalidades essenciais da investigação criminal enquanto ferramenta imprescindível do sistema penal, e ainda que reflexamente instrumento de concretização de um Direito Fundamental à Segurança, mas sobretudo mecanismo de proteção dos direitos fundamentais do cidadão face ao poder punitivo estatal.

Nessa perspectiva, a mesma hipótese sinalizava que a investigação criminal tecnológica e o uso dos métodos ocultos de investigação, como é o caso da infiltração por *malware*, encontra limitações e requisitos condicionados pelo direito probatório orientado pelo respeito ao conjunto de garantias fundamentais de defesa inalienáveis.

De forma mais específica, a hipótese indicava a necessidade de perquirir os aspetos peculiares da infiltração por *malware*, enquanto método especial, a sua aptidão para a qualidade jurídica da investigação criminal no ambiente digital, a sua natureza jurídica, a integridade e confiabilidade de seus resultados, a utilidade desses resultados, e, enfim, a análise relacionada à utilização dessa técnica e a sua intromissão nos direitos fundamentais do investigado.

Não se pode olvidar o grande potencial de polêmica do tema proposto, não só por seu caráter inovador, mas por se inserir na antiga, mas sempre presente, discussão acerca da possível dicotomia entre liberdade e segurança. Agora acrescida de elementos muito mais desafiadores ante as peculiaridades da Sociedade da Informação, no seio da qual se maximiza a propalação dos riscos, das ameaças e do medo; amplifica-se a cultura emergencial, a cobrança por eficiência e por segurança; e, ao mesmo tempo, clama-se por mais liberdades.

Buscou-se, assim, evitar o raciocínio simplista que aponta a relação inversamente proporcional, e reciprocamente excludente, entre a liberdade individual e a segurança social, que certamente dificulta a compreensão e o desenvolvimento de um sistema penal2 menos sujeito a intervenções momentâneas e ideológicas.

---

2 Termo usado para descrever não somente o conjunto de normas penais que viabilizam o controle formal das condutas vistas como negativas à sociedade (Souza, 2015).

Essa polarização conduz ao inapropriado sentimento de mera disputa retórica e ideológica entre aqueles taxados de garantistas e *eficientistas*. Ao defenderem limites para a persecução penal nas garantias individuais, os primeiros são apontados como defensores de um sistema ineficiente e fomentador da impunidade. Por outro lado, os que defendem a necessidade de mudanças em prol da eficiência tendem a ser rotulados como fiadores do autoritarismo estatal em detrimento da liberdade individual.

De fato, não é tarefa fácil aproximar-se do equilíbrio entre a eficiência e a proteção dos direitos e garantias fundamentais. Não obstante, a presente produção acadêmica está comprometida com o rigor científico e a boa-fé, pelo que se procura afastar de eventuais interferências ideológicas, em que pese a incontestável impossibilidade de neutralidade ideológica.

O método de análise da investigação concentrou-se prioritariamente em uma abordagem qualitativa, combinada com o método hipotético-dedutivo de acordo com o qual a partir da formulação de hipóteses se operacionaliza o mapa de conceitos-chaves. Para tanto, as técnicas e instrumentos de investigação assentaram na coleta de documentação indireta, através da análise bibliográfica e documental.

Em razão disso, levantou-se material bibliográfico e documental não apenas da ciência jurídica, mas também de ciências afins ao objeto de estudo que se mostraram importantes para subsidiar a pesquisa notadamente no âmbito de enquadramentos conceituais, a exemplo das ciências políticas e sociais-filosóficas, utilizados sem a aspiração de aprofundamento em tais matérias.

Nesse ponto, adverte António Lara (2011, p.49) que "a abordagem ideal é, assim, de natureza interdisciplinar, recorrendo às metodologias específicas das várias ciências".

Nesta linha de análise, Nelson Lourenço ensina que a análise da segurança deve levar em consideração

> [...] os componentes principais do novo quadro de ameaças à Segurança Interna – a violência urbana, a criminalidade transnacional e as novas formas de terrorismo – que acompanham as mudanças da sociedade moderna e que se associam à densificação do conceito de Segurança. A sua leitura pressupõe que se retenha o percurso que se efectuou sobre os elementos constitutivos da modernidade, isto é, a globalização, a reflexividade e a descontextualização da sociedade moderna tardia (Lourenço, 2013, *online*).

Feitas as advertências supra, com o fim de facilitar a compreensão do assunto e alcançar as respostas às perguntas objetos do problema apresentado, o trabalho foi estruturado em três capítulos distintos e complementares.

No primeiro capítulo, buscou-se inicialmente identificar o(s) sentido(s) da palavra segurança, enquanto direito fundamental e associada à atividade e dever do Estado, contextualizando-a às principais características da atual Sociedade da Informação. A abordagem, embora sucinta, revelou-se necessária haja vista que a busca por segurança, ou pelo menos a declaração nesse sentido, muitas vezes orienta opções políticas e até jurídicas relacionadas à investigação criminal. Seguiu-se, no mesmo capítulo, na abordagem das características principais da Sociedade da Informação, baseada no paradigma tecnológico, a sua relação com a segurança e a privacidade, e os desafios que se impõem à investigação criminal e à segurança na Era Digital.

Buscou-se identificar e compreender o alcance das mudanças dos paradigmas sociais, provenientes do acelerado desenvolvimento tecnológico, e os reflexos dessa quebra de paradigmas sociais no objeto de estudo.

O segundo capítulo inicia-se com o objetivo de estabelecer as premissas conceituais sobre a investigação criminal e a prova penal, identificando-se conceitos da teoria da prova penal que se apresentem relevantes para a pesquisa, com o fim de esclarecer algumas das diversas denominações legais, doutrinárias e jurisprudenciais das principais categorias relacionadas à prova no processo penal, como, por exemplo, atos de prova, elementos de prova, fontes de prova, meios de investigação e meios de prova. Esse recorte epistemológico, embora conciso, revelou-se necessário para o debate acerca do valor probatório dos elementos colhidos na investigação criminal.

Prosseguindo-se na mesma linha, ainda no segundo capítulo, passou-se ao exame mais específico dos impactos das tecnologias de informação e de comunicação sobre o campo probatório penal. Pretendeu-se, assim, conceituar, identificar e caracterizar a prova digital, bem como analisar os meios de obtenção desta espécie de prova, os requisitos de aquisição e de preservação da fonte da prova digital para a sua admissibilidade no processo penal.

Esclarecidas as premissas conceituais retro referidas e analisados os impactos do desenvolvimento tecnológico no exame da prova penal, concluiu-se o segundo capítulo com a abordagem particular acerca dos métodos ocultos de investigação criminal, em sentido amplo, identificando o seu conceito, suas características, os princípios gerais aplicáveis e os limites impostos pelo direito probatório à sua aplicação.

O terceiro capítulo é dedicado ao estudo específico da infiltração por malware nas investigações informáticas. Buscou-se estabelecer a natureza jurídica do instituto, o seu conceito e características, enquanto método oculto de investigação criminal. Examinou-se a

experiência estrangeira quanto ao uso do *malware*, limitando-se a uma pequena amostra de países onde a discussão sobre o tema encontra-se em estágio mais avançado.

Destaca-se que a busca pelas experiências jurídicas de outros países quanto ao uso pelo Estado do *malware* à serviço das investigações criminais não se propõe a encontrar uma solução a ser copiada pelo Brasil. Na verdade, compreende-se a utilidade do exame de casos estrangeiros para o desenvolvimento crítico do estudo acerca da aplicação desse mecanismo no Brasil, tendo em mente as particularidades de seu sistema jurídico.

Por fim, prosseguindo-se no mesmo capítulo, passou-se à abordagem da intromissão do recurso da infiltração por *malware* nos direitos fundamentais do investigado, dentre os quais se destacam aqueles relacionados à proteção da intimidade e da vida privada, seja em ambiente material ou virtual, e a possibilidade de restrição dos direitos fundamentais. Pretendeu-se fazer uma ponderação entre as exigências impostas ao Estado quanto à necessidade de reforço da investigação criminal que acompanhe a evolução tecnológica e, por outro lado, a imprescindível proteção do núcleo essencial do quadro de direitos, liberdades e garantias do sujeito investigado.

1. Segurança, Sociedade da Informação e Investigação Criminal

Este capítulo aborda a segurança sob uma ótica multidisciplinar, relacionando-a à atual sociedade da informação e buscando identificar seus reflexos na investigação criminal.

A Segurança, ainda que tenha sido um tema tratado pelos estudos de relações internacionais desde o início do século XX, não foi um conceito que recebeu muita atenção dos estudiosos por não ser de fácil tratamento. Não é um conceito facilmente manejável. Tomando emprestado de W. B. Gallie, Buzan (2008, p.7) usa a noção de "conceitos essencialmente em disputa" para classificar o conceito de segurança. São conceitos que guardam um forte componente ideológico e que, por isso, tornam as manifestações concretas incapazes de resolver controvérsias sobre seu significado ou aplicação. Conceitos como "Estado" e "justiça", não podem admitir uma definição tão precisa que seja geralmente aceita, por se tratar de conceitos essencialmente em disputa, isto é, de natureza controversa. O mesmo ocorre com o conceito de segurança. Por não admitir uma única interpretação, generalizante, só pode ser definido levando-se em conta o caso concreto. Contudo, não é menos controverso do que outros conceitos das ciências humanas e sociais, como "liberdade", "amor" e "igualdade". O fato de ser um conceito controverso, ou essencialmente em disputa, não depõe contra ele. Inversamente, são as disputas em torno do conceito que fertilizam o campo científico.

Dito isto, inicia-se este capítulo demonstrando que a segurança é um poder-dever do Estado[3] e possui *status* de direito humano fundamental. Na sequência, tenta-se responder ao questionamento "O que é segurança?", sendo apresentados, pois, conceitos de segurança em múltiplas acepções embora com ênfase na segurança coletiva, de forma que seja possível compreender os impactos da sociedade da informação sobre a segurança bem como os meios que podem ser empregados para mitigar a violência e a criminalidade.

1.1. Afinal, o que é segurança?

Antes de conceituar segurança, é importante analisar o poder-dever histórico do Estado na preservação da segurança humana e coletiva. Historicamente, o Estado, enquanto

3 No Brasil, este poder-dever está consignado no art. 144 da CRFB/1988 que assim dispõe: "a segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio, através dos seguintes órgãos: I – polícia federal; II – polícia rodoviária federal; III – polícia ferroviária federal; IV – polícias civis; V –polícias militares e corpos de bombeiros militares.

organização administrativa surge como produto da sociedade a partir da evolução do convívio social, quando as formas primitivas de sociabilidade se tornaram incapazes de regular as ações humanas e garantir um equilíbrio à sociedade.

O conceito de Estado, as suas origens e os seus fins, os motivos de sua existência, a sua natureza, e principalmente a legitimidade do poder que lhe é inerente, foram objeto de aprofundado estudo de filósofos e juristas ao longo de vários séculos[4]. Ainda hoje não há consenso absoluto acerca do assunto, tratando-se de tema em constante evolução que acompanha a modernização e a complexidade das relações sociais.

É inegável que o Estado Moderno tem suas raízes históricas nos ideais absolutistas da Idade Média[5], tendo sido o Estado Absolutista a sua primeira expressão. No entanto, a sua atual compreensão passa por um natural, e permanente, processo de evolução, moldada a partir dos ideais iluministas da Idade Moderna.

Ancorado nos contributos dos pensadores do Iluminismo[6], surge o Estado Liberal, baseado na concepção do liberalismo econômico e na garantia das liberdades dos homens, visto como um mal necessário, sem o qual não se alcançaria a segurança indispensável à sadia manutenção das relações humanas, mas que deveria intervir o mínimo inevitável ao cumprimento de seus deveres.

Segundo a clássica posição de Adam Smith (1996), o poder do Estado Liberal limitava-se ao cumprimento de três deveres fundamentais, competindo-lhe, assim, atuar para garantir a segurança interna e externa da sociedade, bem como criar e manter instituições públicas e realizar obras de interesse coletivo que não forem realizadas por particulares.

Na sequência, a história demonstra que a mera preservação dos espaços de autonomia dos cidadãos, sob a ótica dos direitos fundamentais de defesa contra a intervenção estatal, não seria suficiente para atender às crescentes necessidades oriundas das, cada vez mais complexas, interações sociais.

Consolida-se, assim, especialmente após a II Guerra Mundial, a ideia de Estado Social ou Estado Providência, ou ainda Estado Democrático e Social de Direito, seguindo a paralela

---

4 Não abordaremos as mais diversas teorias acerca da formação do Estado e do poder político por não se tratar de objeto do estudo. Adotaremos a concepção de Estado Contemporâneo, notadamente, de Estado Democrático de Direito.

5 Dentre os teóricos que sustentaram o absolutismo podemos citar Nicolau Maquiavel, Thomas Hobbes, Jacques Bossuet e Jean Bodin. O Leviatã é a obra mais famosa de Thomas Hobbes publicada em Londres, em 1651, na qual defendia a origem contratualista do Estado e o governo de um soberano absoluto, com o fim de garantir segurança e paz à sociedade.

6 Dentre os principais pensadores do Iluminismo, destacam-se John Locke, Montesquieu, Voltaire, Jean-Jacques Rousseau e Adam Smith. Cita-se como a maior contribuição das ideias de Montesquieu a separação dos poderes em executivo, legislativo e judiciário.

evolução do Constitucionalismo. Nessa perspectiva, para além dos direitos de defesa impõe-se a atuação ativa do Estado na concretização de novos direitos fundamentais, sociais e políticos.

Hodiernamente, com o advento do século XXI e o consequente incremento da Globalização e as respectivas consequências nos planos econômico, social, cultural e político, fala-se em "Estado Pós-Social" ou "Estado Pós-Contemporâneo"[7], no contexto de uma Comunidade Internacional Global.

A partir dessa brevíssima excursão histórica, facilmente se percebe que a segurança sempre esteve presente na natureza íntima do Estado, qualquer que seja a teoria adotada, enquanto finalidade primária inarredável.

Denota-se essa assertiva da própria definição conceitual jurídica clássica do Estado[8], da qual se extraem três elementos constitutivos essenciais à sua existência – povo, território e soberania –, sem os quais não há que se falar em Estado.

Particularmente, o exercício da soberania – enquanto elemento funcional do Estado – exige a constituição de um aparelho que garanta a segurança da própria instituição política e de seu território – independente e detentora de poder soberano –, bem como que assegure a segurança de seu povo e a sua autoridade política sobre os membros da sua comunidade.

Mesmo quando ainda vigente a posição de Estado Liberal, tanto a segurança externa – nacional –, quanto a segurança interna – pública –, ou seja, a proteção dos cidadãos contra a injustiça e a opressão de qualquer outro membro da própria sociedade –, eram tratadas como tarefas primárias e fundamentais do Estado.

Importa destacar que, no curso desse processo evolutivo do Estado Moderno até chegar a fase atual, a partir dos ideais liberalistas, a designação de Estado de Direito sempre esteve presente. Conforme ensina Bobbio (1986, p.13), "direito e poder são as duas faces da mesma moeda: só o poder pode criar direito e só o direito pode limitar o poder".

Nesse panorama, a Constituição surge como norma jurídica fundamental à formação do Estado – como um Estatuto – com a finalidade primária de estabelecer a organização do Estado e os limites do Poder. A partir daí dá-se início ao processo de positivação dos direitos fundamentais, inaugurando-se com a provisão dos direitos fundamentais de defesa, que objetivavam impor limites à soberania em face das liberdades humanas.

---

7 Sobre a mutação do Estado Social para o Estado Pós-Contemporâneo ou Pós-Social, v. Jorge Bacelar Gouveia (2018), *Direito da Segurança: Cidadania, soberania e cosmopolitismo.* 1ª ed., Coimbra: Almedina. pp. 45 e ss.

8 Ver a definição em Jorge Bacelar Gouveia (2018), *Direito da Segurança: Cidadania, soberania e cosmopolitismo.* 1ª ed., Coimbra: Almedina. p.26.

Com a crescente e permanente evolução do Estado de Direito Constitucional gradativamente ampliou-se o catálogo de direitos fundamentais positivados no topo da pirâmide do Ordenamento Jurídico-Estadual – Constituição –, sem nunca olvidar do elemento subjetivo comum inarredável – a pessoa humana –, nem tampouco do objetivo precípuo de garantir a sua proteção.

A dignidade da pessoa humana é, portanto, objeto comum tanto dos direitos fundamentais quanto dos direitos humanos – estes consagrados no Direito Internacional Público em face da intensificação das relações internacionais. Ambos têm sua gênese na necessidade de proteção da pessoa humana.

O princípio da dignidade humana, alçado ao patamar de princípio universal, constitui hoje vetor de identificação material dos direitos fundamentais, e "significa que a pessoa é colocada como desígnio supremo do Estado e do Direito" (Gouveia, 2018, p.289).

Nesse contexto, a segurança transpõe o tradicional sentido de constituir apenas uma finalidade fundamental do Estado, desde as suas origens, e passa a ser reconhecida como direito fundamental nos Estados Democráticos de Direito e, igualmente, como direito humano internacional.

Atualmente, o direito à segurança está positivado na qualidade de direito fundamental nos mais diversos ordenamentos jurídico-estatais. É o que se observa, particularmente, nas Constituições de Portugal e do Brasil. A Constituição portuguesa dispõe em seu artigo 27º, nº 1, que "Todos têm direito à liberdade e à segurança". Por sua vez, a Constituição brasileira prescreve, no enunciado do seu artigo 5º, que "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".

Destaca-se que, em ambas as Constituições citadas, o direito fundamental à segurança encontra-se sedimentado no capítulo alusivo aos direitos, liberdades e garantias. Registra-se, ainda, pela pertinência, que ambos os ordenamentos jurídicos supremos estabelecem a dignidade da pessoa humana como princípio fundamental do Estado Democrático de Direito.

Igualmente, no âmbito internacional, também é possível perceber a positivação do direito fundamental à segurança em diversos diplomas legais que catalogam os direitos humanos fundamentais. A Declaração Universal dos Direitos Humanos (DUDH), oriunda da Organização das Nações Unidas – entidade máxima de discussão do Direito Internacional –, enuncia em seu artigo 3º que "Todo o indivíduo tem direito à vida, à liberdade e à segurança

pessoal". O mesmo enunciado é reproduzido no Pacto Internacional de Direitos Civis e Políticos.

A consagração do direito à segurança como direito humano universal é replicada nos demais sistemas regionais do Direito Internacional interligados ao eixo comum das Nações Unidas. No âmbito americano, destaca-se a Convenção Americana sobre Direitos Humanos – denominada de Pacto de San José da Costa Rica –, que reconhece em seu artigo 7, nº 1, primeira parte, que "Toda pessoa tem direito à liberdade e à segurança pessoais".

No continente europeu, a Convenção Europeia dos Direitos dos Homens consagra, no artigo 5º, nº 1, primeira parte, que "Toda à pessoa tem direito à liberdade e segurança". Do mesmo modo, a Carta dos Direitos Fundamentais da União Europeia também consolida o direito à segurança ao status de fundamental ao dispor, em seu artigo 6º, que "Todas as pessoas têm direito à liberdade e à segurança".

Não há dúvida, portanto, que a segurança constitui um fim indissociável do Estado – sentido teleológico – que implica a garantia da estabilidade, permanência do Poder Político e, por isso, associada à soberania. Nessa perspectiva, denota um dever do Estado de instituir instrumentos capazes de alcançar esse objetivo.

Por sua vez, ao mesmo tempo, a segurança avulta o sentido de direito fundamental humano assim consagrado nas Constituições dos Estados Democráticos de Direito e também no Direito Internacional jungido ao princípio universal da dignidade humana, denotando o sentido de direito subjetivo individual e coletivo.

Não obstante a identificação da segurança como fim e direito fundamental, respectivamente no âmbito político-estadual e jurídico-constitucional, convém questionar afinal o que é a segurança? A importância de uma definição do conceito de segurança é avultada por Luís Barroso que destaca quatro razões fundamentais:

> - é a busca da segurança que orienta os estados à utilização última da força militar;
> - são as preocupações com a segurança que determinam o que constitui as ameaças;
> - a definição do conceito ajuda a discriminar o que é verdadeiramente um assunto de segurança;
> - só com um conceito claro é que é possível alargar o âmbito de aplicação sem desvirtuar o seu objeto; (Barroso, 2014, p.158).

Nessa perspectiva, muito bem adverte Bacelar Gouveia (2918, p.97) que "o reforço da segurança como fim do Estado não pode fazer-se à custa da democracia e da liberdade dos cidadãos, criando-se um novo conjunto de opções dilemáticas em termos políticos e em termos jurídicos".

O sentido etimológico da palavra segurança, com origem do termo em latim *securos*, que significa "sem temor, garantido", derivando-se de *sine cure*, que quer dizer "sem cuidados", refere-se à qualidade daquilo que é seguro, estável, protegido, ou seja, que está a salvo de quaisquer perigos, danos ou riscos.

Por sua raiz etimológica, portanto, a segurança sugere o sentido de uma finalidade de proteção e, ao mesmo tempo, revela a ideia de atividade dirigida a atingir o desígnio desejado, de afastar os riscos que possam atingir aquilo que se deseja proteger.

Em uma abordagem mais ampla e permeada pela multidisciplinariedade, a segurança humana é a garantia da sobrevivência individual e do bem-estar com dignidade das pessoas no ritual preferido do convívio social. O fundamento desse conceito, que eu entendo ser apropriado, está no Artigo III da Declaração Universal dos Direitos Humanos (1948): "Toda pessoa tem direito à vida, à liberdade e à segurança pessoal" (ONU, 1948). Desse fundamento emerge a chave para o equilíbrio entre o pessoal e o social.

No âmbito da Organização das Nações Unidas (ONU), a segurança humana é descrita como um processo que engloba tanto a "libertação do medo" como a "libertação da necessidade". Desse modo, a ONU, ao tratar do conceito de segurança humana, busca a distinção entre os limites associados às ameaças à segurança do Estado e os limites pertinentes às ameaças que impactam o relacionamento dos seres humanos em três esferas: individual, familiar e comunitária. Nessa linha, no Relatório sobre Desenvolvimento Humano, elaborado pelo Programa das Nações Unidas para o Desenvolvimento (PNUD), publicado em Nova York, em 1994, a segurança humana, diferentemente da segurança tradicional, aparece descrita com um caráter essencialmente defensivo, envolvendo um conceito integrador de solidariedade, de modo a incluir todas as pessoas no processo de diálogo para o desenvolvimento humano, em condições de favorecer a preservação da vida digna.

No ano de 2000, Kofi Annan, então Secretário-Geral da ONU, referindo-se ao conceito de segurança humana, destacou elementos centrais inter-relacionados com a segurança do Estado, visando à manutenção da estabilidade em escala nacional, regional e global. Esses elementos dizem respeito à "libertação do medo e à libertação da necessidade, de modo a propiciar a interseção da liberdade de atitudes das gerações futuras com a herança estratégica de um ambiente natural saudável" (ONU, 2000).

O Relatório Especial, elaborado, em 2003, pela Comissão da ONU sobre Segurança Humana, denominado "Segurança Humana Agora", atrelou o conceito de segurança humana ao influxo da proteção contra ameaças sistêmicas que podem atingir o âmago de todas as vidas humanas. Daí por que, conforme enfatizou, em 1994, o Relatório do PNUD, a segurança

humana é parte fulcral no conjunto da infraestrutura política e administrativa do Estado, para assegurar os direitos, a cultura da paz e o desenvolvimento social, ampliando as escolhas pessoais. A segurança humana é, justamente, a fiança de que as pessoas possam exercer essas escolhas com firmeza, convicção e liberdade.

É oportuno observar que, na doutrina, são muitas as definições que buscam situar os vários componentes estáveis da segurança humana diante de situações de insegurança em distintos contextos de riscos, ameaças e vulnerabilidades[9].

Quando divulgou em Nova York, em 1994, o Relatório sobre Desenvolvimento Humano, o PNUD introduziu, no Capítulo Segundo do Relatório, a compreensão da ONU sobre a ideia, o conceito e a abordagem em torno da segurança humana, elegendo sete componentes centrais que estão interligados e se completam, em dinâmicos processos de alinhamento para viabilizar o potencial de cada indivíduo de modo a concretizar o seu enriquecimento como pessoa. As sete esferas componentes centrais de segurança humana que constam no referido Relatório do PNUD serão descritas a seguir.

A segurança econômica almeja uma renda básica segura para as pessoas, proveniente, geralmente, de trabalho remunerado e produtivo, ou, como último recurso, de uma rede de segurança com financiamento público. Embora a questão da segurança econômica seja mais séria em países em desenvolvimento, ele também suscita preocupações nos países desenvolvidos. O desemprego e a falta de renda constituem fatores importantes por trás das tensões que envolvem questões políticas, crises ou conflitos entre grupos étnicos (PNUD, 1994).

A segurança alimentar exige que todas as pessoas, em qualquer tempo, tenham acesso, tanto físico como econômico, aos alimentos básicos. Não há como ignorar que é enorme o desassossego com a carente disponibilidade global de alimentos para milhões de pobres que são vitimados não só pela deficiente distribuição de alimentos, como pela falta contínua de poder aquisitivo (PNUD, 1994).

A segurança na saúde visa garantir a proteção mínima com vistas ao combate a doenças e estilos de vidas insalubres. Seja nos países em desenvolvimento, seja nos países industrializados, os danos à segurança, no âmbito da saúde, são praxes no meio urbano e no meio rural, atingindo particularmente as crianças carentes e os idosos com dificuldades financeiras (PNUD, 1994).

---

9 Sobre as posições relacionadas ao conceito de segurança humana: Gasper, Des. (2008). The Idea of Human Security. In: *Garnet Working Paper*, University of Warwick, Coventry, United Kingdom, n. 28, p. 2-9. Cabe acrescentar a teoria de: Owen, Taylor. (2008). The Uncertain Future of Human Security in the UN. *International Social Science Journal of UNESCO Publication*, Paris, v. 59, p. 113-118.

A segurança ambiental visa proteger as pessoas das ameaças e estragos de origem antrópica à natureza, propiciando a deterioração do meio ambiente e trazendo prejuízos à governança ambiental. Nos países em desenvolvimento, a falta de acesso ao saneamento ambiental, tais como recursos hídricos limpos, redes de esgotos e tratamento de resíduos sólidos, constitui um dos maiores pesadelos da espécie humana no seu habitat. Nos países industrializados, um dos principais sobressaltos é a poluição atmosférica que atinge os ecossistemas. Por outro lado, o crescente impacto da mudança climática é outro fardo que traz instabilidade à segurança ambiental e, consequentemente, efeitos nocivos à segurança humana (PNUD, 1994).

A segurança cidadã se insere dentro do contexto da segurança humana, sendo o retrato do protocolo da política de segurança pública para a valorização dos direitos humanos. Ela mobiliza os instrumentos de transformação, sob a égide do aperfeiçoamento da educação, no cerne da luta contra a violência e a criminalidade. Tendo por prioridade a pacificação, a legitimidade da prevenção ao lado da prática policial eficiente, a segurança cidadã visa proteger as pessoas das aflições advindas da ameaça de violência física ou moral, seja por motivações internas, seja por motivações externas. Para muitas pessoas, a maior fonte de inquietude é a possibilidade de se tornarem vítimas de um crime violento em casa, na escola, no trabalho, na rua, no esporte, no lazer e, enfim, no cotidiano virtual da Internet. A sistematização da segurança cidadã é o caminho necessário para o desenvolvimento social com governança democrática (PNUD, 1994).

A segurança comunitária envolve os laços de solidariedade e de estima social com a filosofia e a estratégia organizacional das parcerias entre a população, governos e instituições públicas e privadas. Isso implica reformas e atualizações constantes nos mapas de planejamento, gestão e operacionalização, respeitando-se os valores, assim como as identidades étnicas e culturais (PNUD, 1994).

Por fim, a segurança política é inerente a uma sociedade que respeita a eficácia da segurança jurídica, como princípio da confiança legítima, ante ao exercício do poder, que precisa estar direcionado ao bem comum, cuidando da garantia da exigibilidade das regras do Direito que motivam as relações harmônicas entre o Estado e os cidadãos (PNUD, 1994).

Em complemento à abordagem multidisciplinar de segurança fornecida pelo PNUD, Arnold Wolfers, citado por Luís Barroso (2014) utiliza duas dimensões distintas – uma de natureza objetiva e a outra de natureza subjetiva. A partir desses vetores, a segurança é definida como a baixa probabilidade de ameaças aos valores adquiridos que simultaneamente corresponda à baixa probabilidade de medo que esses valores possam ser atacados.

Por certo que, no atual estágio de complexidade das relações sociais, de globalização política, econômica, social e cultural, em que cada vez mais diminuem as barreiras geográficas dos Estados gerando uma explosão migratória de tal modo que transforma a convivência social em um "quotidiano cosmopolita", os riscos e ameaças aos quais se expõe as pessoas e os próprios Estados multiplicam-se na mesma proporção. Trata-se do fenômeno que Ulrich Beck (2011) denominou de "sociedade de risco mundial".

Acerca da atual sociedade de risco, Felipe Pathé Duarte expõe que:

> A expectativa do devir, a percepção do risco e da imprevisibilidade tornaram-se então o eixo da contemporaneidade. A iminência e incerteza de um acontecimento são normalidade e elemento base do nosso quotidiano. Assim, o risco, associado à incerteza e probabilidade, influencia cada vez mais o processo de decisão. Condiciona-se a ação humana, sendo que hoje a decisão assenta mais na ideia de insegurança que na de progresso (Duarte, 2015, pp.452-453).

Com efeito, a diversidade dos riscos e ameaças aliada à incessante evolução dos valores humanos evidenciam o caráter multidimensional da segurança. Assim, a depender do critério utilizado, pode-se falar em variadas espécies de segurança como, por exemplo, segurança interna e externa – critério espacial –; segurança militar, segurança policial, segurança municipal – critério funcional –; segurança econômica, segurança financeira, segurança ambiental, segurança alimentar – critério objetivo.

Essa variedade de classificação da segurança decorrente da emergência de novos riscos e ameaças, bem como a busca pela aplicação de recursos cada vez mais modernos que se demonstrem aptos à proteção dos mutáveis valores erigidos ao caráter de fundamentais não implicam, todavia, a atribuição de novos conceitos de segurança. "Diferentes valores podem ser protegidos por diferentes meios sem minar o conceito" (Barroso, 2014, p.176).

A partir do exposto, a segurança pode ser sintetizada como o estado, condição ou circunstância na qual estejam reduzidas, ao menor grau possível, as probabilidades dos riscos e ameaças presentes virem a atingir os valores fundamentais assim entendidos num dado contexto histórico, de modo a permitir que os sujeitos individuais e coletivos convivam em um "quotidiano estável"[10], no qual sintam-se seguros a exercer livremente todos os direitos e deveres determinantes a uma vida com dignidade.

10 Expressão utilizada por Fontes, J. (2013). *O Direito ao Quotidiano Estável — Uma Questão de Direitos Humanos*. Coimbra: Coimbra Editora.

Consequentemente, o direito à segurança implica a prerrogativa de ser e se sentir seguro, livre de ameaças ou ofensas que possam tolher o exercício de qualquer valor fundamental à existência digna dos indivíduos e das comunidades nacionais e internacionais.

No entanto, com o advento da sociedade da informação, também denominada sociedade complexa ou de risco, surgem dúvidas sobre os limites que se pode ou deve impor aos órgãos de segurança pública para que seja possível conter a criminalidade. É o que será discutido a seguir.

1.2. Sociedade em rede e em risco: segurança, privacidade e vigilância na sociedade contemporânea

De acordo com a literatura especializada, a era da informação está relacionada aos avanços tecnológicos da comunicação e da informação no campo digital, a partir dos anos 70, com a invenção do computador, da internet e dos cabos de fibra óptica. Tem por base o processo e a dinâmica da comunicação *online*, por meio de redes, adquirindo um poder multidimensional, estabelecido de acordo com os interesses e os valores dos diferentes usuários (Castells, 1999).

Na década de 80, Alvin Toffler advertia que o desenvolvimento de todo este processo tecnológico acarretaria paralelamente, para a sociedade, sérios efeitos colaterais. Referindo-se à espionagem, no contexto da era da informação e das tecnologias, assim expressa:

> [...] o agente espião é uma das mais poderosas metáforas do nosso tempo pois vem equipado com a última e mais exótica tecnologia: microfones eletrônicos, bancos de computadores, câmeras infravermelhas, [...] pois o negócio básico da espionagem é a informação. E a informação, tornou-se talvez o negócio mais importante e o que mais cresce no mundo. O espião é um símbolo vivo da revolução que hoje invade a infosfera (Toffler, 1980, pp.161-162).

Tal perspectiva feita nos anos anteriores à privatização da internet, seria um prenúncio do momento em que se vive atualmente, caracterizado por uma revolução tecnológica pontuada por mudanças drásticas na maneira como as pessoas percebem e agem na sua intimidade e vida privada. O agente espião, a que Toffler fazia menção, é a tecnologia cibernética.

Costa Júnior (2007) vai além quando afirma que a revolução tecnológica digital promoveu um processo de corrosão das fronteiras da intimidade, na qual o devassamento da vida privada se tornou mais agudo e inquietante. Ele avalia que essa revolução, muitas vezes,

avança desprovida de diretrizes morais, o que acarreta uma deformação progressiva dos direitos fundamentais numa escala de assédio crescente.

Castells (1999), criador do conceito de sociedade em rede, esclarece que estamos conectados a grupos de pessoas com interesses distintos e com acesso ilimitado, o que podemos compreender como redes. Basicamente, estas são estruturas abertas, integrativas e dinâmicas, com capacidade de expansão ilimitada, onde pessoas compartilham os mesmos códigos de comunicação para acessarem ou compartilharem suas informações.

O autor explica que tal fenômeno é resultado da interação de duas forças relativamente autônomas: o desenvolvimento de novas tecnologias e a tentativa da sociedade de se reaparelhar "com o uso do poder da tecnologia para servir à tecnologia do poder" (Castells, 1999, p.69).

Nesse contexto, é importante lembrar que, nessas redes, a hierarquia convencional e a identidade dos usuários se tornam insignificantes. Pela perspectiva de Souza e Quandt (2008), o aspecto mais marcante é a posição em que essas identidades se encontram dentro na própria rede, com os respectivos contatos e nós periféricos, muitas vezes mais importantes do que estar localizado em algum determinado nível hierárquico, mesmo que superior.

Utilizando o mesmo método de análise de contatos periféricos para identificar conexões e lideranças entre organizações criminosas, governos podem exercer vigilância por meio de constante monitoramento desses nós.

Fellman e Wrigth (2008), ocupando-se do tema ao esclarecer que a mensuração dessas redes está focada no seu grau de centralidade, revelam os indivíduos-chave no fluxo de informações e na troca de conhecimentos. Graus elevados de centralidade demonstram amplo acesso a recursos ocultos dentro da organização. Assim, depois de realizada a identificação, a vigilância opera no sentido de possibilitar o apontamento de outros contatos em torno deste e, paulatinamente, adicionar novas conexões até o mapeamento completo de quais pessoas são lideranças e com quem estão envolvidas. É nesse sentido que Castells (2013) afirma ser a interatividade um dos fatores que transformam essas redes em fontes decisivas de construção de parcela do poder, mas não de todo o poder.

É relevante dizer que a internet, concebida como produto da Guerra Fria no final da década de 50, se caracterizava, essencialmente, como um projeto de pesquisa militar elaborado pela Agência de Pesquisas em Projetos Avançados (*Advanced Research Projets Agency – ARPA*) a pedido do Departamento de Defesa dos Estados Unidos, destinado a conectar centros de pesquisa dos EUA com o Pentágono, oportunizando a troca de informações seguras entre esses centros.

Na lição de Castells (2003), a criação da internet foi também consequência da disputa por superioridade em tecnologia militar com os soviéticos, criando um canal de comunicação e armazenamento de dados científicos com segurança, em caso de guerra nuclear, o que à época, de fato, era uma real possibilidade.

Por outro lado, a história da internet é permeada de sucessos e retrocessos num processo longo. Resumidamente, no ano de 1971, uma equipe de cientistas, liderada por Vinton Cerf, considerado o pai da internet, realizara a façanha de conectar três redes diferentes num processo denominado *interneting*, termo que posteriormente passou a designar o sistema que hodiernamente é conhecido por internet. Com a criação de uma nova rede específica para comunicações militares, a *Military Network* (MIL-NET), no ano de 1983, a *Advanced Research Projects Agency Network* (ARPANET) perdeu sua exclusividade nessa área (Nether, 2018).

Na década de 90, sob o controle da *National Sciense Foundation* (NCF) e com a colaboração do Departamento de Defesa, a internet seria comercializada para outras instituições governamentais e da iniciativa privada. Com a inclusão dos protocolos TCP/IP e o sistema WWW (*World Wide Web*), desenvolvido por Tim Berners-Lee, ela seria privatizada a partir dos anos de 90, chegando desta forma, aos usuários (Nether, 2018).

O modelo estrutural de governança da internet é centralizado no Departamento de Comércio e de Defesa dos Estados Unidos, que detém o controle militar do ciberespaço, na Icann (Corporação da internet para Atribuição de Nomes e Números) e na empresa *Verising*, que detém, com exclusividade, o controle comercial. Vale ressaltar que, segundo a revista *Em Discussão* (2014), "as duas empresas são responsáveis por atribuir parâmetros de protocolo da internet, valendo-se da regulação do sistema de nome de domínio, pela alocação de blocos de números de endereços IP e pela gestão do servidor-raiz do sistema".

Simultaneamente, passou-se a referenciar a expressão ciberespaço. Trabalhar esse conceito é significativo para o presente estudo, pois é nesse ambiente metafísico que ocorrem as ameaças virtuais de diferentes tipos, incluindo a cibervigilância e a ciberespionagem. Palavras sinônimas são usualmente utilizadas para defini-lo, tais como, espaço virtual, mundo virtual e reino eletrônico. Contudo, sabe-se que a expressão teve origem na ficção científica, cunhada pelo escritor inglês na obra *Neuromancer*, de William Gibson[11], lançada no ano de 1984, sendo imediatamente incorporada à linguagem digital. A contribuição do autor torna-se de grande valia, pois, se referia ao ciberespaço como um campo de lutas e de conflitos no

11 Escritor que inaugurou a chamada "Era Cyberpunk", onde antecipou tecnologias, como a internet e criou o conceito "cyberspaço" ainda na década de 70 (Nether, 2018, p.69).

âmbito das redes digitais, na busca por informações secretas protegidas por programas, que acarretariam em novas fronteiras econômicas e culturais, conjuntura que se apresenta na atualidade.

O documento Estratégia Nacional para Assegurar o Ciberespaço (*Summary National Strategy to Secure Cyberspace of 2003-NSSC*), dos EUA, o define como centenas de milhares de computadores em rede, incluindo a internet, intranet e redes de telecomunicações, servidores, roteadores, tomadas e cabos de fibra ótica que possibilitam o funcionamento das estruturas críticas.

Pierre Levy (1999) contribui quando apresenta um conceito mais amplo de ciberespaço e inclui os seres humanos como parte ativa deste sistema. Ele assevera tratar-se de uma infraestrutura global de informações pela internet, integrada pelo universo de dados que circula por ela e pelos usuários, cientistas, técnicos e outros especialistas responsáveis por sua manutenção e desenvolvimento.

Libicki (2009) se aprofunda ainda mais, aduzindo que o ciberespaço se divide em três níveis: físico, sintático e semântico, sendo que é no âmbito de um desses níveis que se desenvolvem as ações de cibervigilância e ciberespionagem.

O nível físico é onde todos os sistemas de informação se situam numa camada física que os sustenta e são constituídos por caixas e fios. A seu turno, o nível sintático contém instruções que os criadores de programas e usuários dão à máquina, bem como os protocolos, por meio dos quais as máquinas interagem na elaboração de dados, reconhecimento de dispositivos e formatação de documentos. É neste nível que os *hackers* tendem a atuar. Por fim, o nível semântico consiste em informações que as máquinas contêm e nelas ocorrem os diferentes tipos de ataques, por meio de vírus e *sites* com códigos maliciosos embutidos (Libicki, 2009).

Tomando por base essa dimensão científica, pode-se identificar que é nos níveis sintático e semântico que as atividades de cibervigilância e ciberespionagem ocorrem, uma vez que são as que possibilitam o acesso a dados e informações. Contudo, segundo Nether (2018) a internet pode ser considerada apenas uma parcela pequena de comunicação na Web. Existe outro segmento ao qual não se tem acesso facilitado, conhecido como *Deep Web*, que é um ambiente virtual, não indexado, que organizações criminosas, piratas digitais e grupos terroristas gravitam com facilidade contando com as dificuldades técnicas e operacionais de um monitoramento efetivo.

Com efeito, é na *Deep Web* que se concentra significativa parcela do monitoramento de governos, praticado por meio de suas agências de inteligência e defesa, no sentido de se

antecipar a riscos e ameaças. Essa ação ocorre pela análise dos nós de conexões à rede e criação de perfis falsos. O maior problema é o de que suas páginas e *sites*, como das redes terroristas, de pedofilia e do narcotráfico, não permanecem por muito tempo acessíveis, sendo substituídas com sistematicidade.

Em um mundo globalizado, no qual procura-se acessar fartas quantidades de informações em tempo útil, o ciberespaço constitui-se em uma dimensão crítica do funcionamento normal da sociedade moderna, da sua segurança, sua economia, seus negócios (IDN, 2013).

Essa dimensão oportuniza novos e crescentes tipos de ameaças virtuais, fato que levou os países que detêm o domínio da tecnologia cibernética a utilizá-la com espectro mais amplo, inicialmente, como legítima defesa contra variadas suspeitas que atentem contra a segurança nacional. Mas também, para a coleta indiscriminada de informações e dados pessoais voltadas a diferentes interesses para as pessoas desconhecidos.

Diante da sinopse histórica apresentada, faz-se necessário mencionar dois pontos que ainda não tinham sido citados. O primeiro, diz respeito à descoberta realizada por Bob Thomas, o *worm* batizado de *The Creeper*. Na época, não foi considerado como tal, pois não existia ainda esse conceito, sendo tratado como um programa autorreplicante experimental. Thomas tinha por objetivo demonstrar que havia vulnerabilidades no sistema de segurança da máquina e, para tanto, enviou uma mensagem não autorizada contendo as seguintes expressões: "*Im the creeper, catch me if you can*" "Eu sou a trepadeira, prenda-me se for capaz" (Kleina, 2020).

O segundo foi a descoberta dos *spams* em 1979. Foi disseminado em forma de *e-mails* em massa, criados inadvertidamente pela *Digital Equipment Corporation* (DEC), que pretendia lançar um produto comercial no mercado norte-americano e, para tal, enviou uma série de mensagens de *marketing* que inundaram a rede.

Essas duas descobertas são bastante significativas, pois, tornaram possível constatar que o sistema recentemente criado possuía vulnerabilidades, caracterizadas pela possibilidade de acesso por usuários não autorizados e de forma imperceptível, a qualquer tipo de dados e informações, contexto que têm evoluído na mesma medida em que os novos programas e sistemas vão sendo desenvolvidos.

Segundo o Glossário de Segurança na Internet[12], vulnerabilidade é definida como qualquer fraqueza ou debilidade de um equipamento ou sistema, que podem ser explorados

12 Norton. *Glossário de segurança na internet*. Disponível em: http://br.norton. com/security-glossary/article.

por uma ou mais ameaças. Podem ser intencionais ou o resultado de erros de projeto que resultam em efeitos não desejados ou não esperados que comprometam a segurança do sistema. As que trazem maiores riscos são aquelas desconhecidas pelo fabricante ou gestor do sistema e, consequentemente, não há mecanismos de mitigação que tornem possível a proteção do perímetro de rede até a identificação e desenvolvimento de um novo *hardware* ou *software*.

Essa dinâmica, mais ampliada, aponta para plataformas tecnológicas, como serviços de nuvem, redes sociais e tecnologias móveis, como os *Tablets*, *Smarphones* e o *Black Berry*, os quais têm oferecido ao utilizador mal-intencionado uma nova porta para explorar seus ataques (IDN, 2013).

Wendt (2011), valendo-se dos estudos de *Caverty*, identifica cinco tipos de ameaças apresentadas em ordem ascendente, de acordo com a motivação e a potencialidade do risco. Etimologicamente os termos vêm precedidos da palavra ciber ou da expressão inglesa *cyber*, que internacionalmente expressa todo e qualquer tipo de comunicação que for realizada no espaço digital.

A primeira ameaça é nomeada pelo autor de Cibervandalismo, caracterizado pelas ações de *hackers*, motivados por desafios, brincadeiras ou desprezo. Um exemplo clássico é a substituição de parte do conteúdo de um site por outro conteúdo não autorizado, geralmente de natureza pornográfica ou com ofensas pessoais.

A segunda é o Cibercrime, cuja motivação supera o simples desafio e desencadeia algum tipo de dano tutelado na esfera penal. Entre uma variedade de casos, pode-se citar a captura de senhas de cartões de crédito destinada à realização de fraudes bancárias, distribuição de material pornográfico e violação de propriedade intelectual.

Na Ciberespionagem, as motivações específicas estão voltadas à obtenção de segredos comerciais, industriais e governamentais.

Já no Ciberterrorismo, os ataques que visam estruturas críticas de uma região ou país, capazes de ocasionar colapso nos serviços básicos ameaçando a integridade de um país. O primeiro caso de ciberterrorismo ocorreu no ano de 2007, na Estônia, onde foram paralisados, temporariamente, diversos serviços básicos à população, causando diversos transtornos ao país.

Por fim, tem-se a Ciberguerra quando afeta a soberania da nação por meio de ataques a computadores ligados às infraestruturas críticas do adversário, como redes de energia, água e transportes, serviços de saúde, causando a destruição dos sistemas e sua paralisação permanente.

Faz-se necessário destacar que, tanto na classificação citada acima como em estudos variados, a cibervigilância não está inserida como uma ameaça, sequer é citada.

Isso decorre, em parte, por dois aspectos. Primeiro: estudos mais aprofundados sobre as consequências da cibervigilância são recentes e ainda pouco compreendidos pelos usuários da rede mundial de computadores, de forma geral. Segundo: o desconhecimento em relação ao funcionamento e às capacidades tecnológicas da internet.

Conforme aduz Lemos (2016), compreender a tecnologia, suas forças e limitações deveria ser um componente fundamental de cidadania global. Isso equivale a dizer que, não compreendendo o seu funcionamento, os usuários, na maioria das vezes, não percebem que estão sendo alvo de vigilância e, quando percebem, não têm a noção exata de como tal ação não consentida impactará suas vidas.

Reforçando esta percepção, o laboratório *Kaspery* divulgou a existência de uma campanha de ciberespionagem internacional denominada *Outubro Vermelho*, direcionada a coletar dados e informações de organizações, de governos, órgãos diplomáticos e centros de pesquisa e tecnologia, todas consideradas sensíveis e protegidas por grau de sigilo no tocante ao acesso (Veloso, 2014).

Como fator decorrente, outros episódios correlatos chegaram ao conhecimento da mídia internacional, como o foi caso da agência de espionagem britânica, *Government Communications Headquarters* (GCHQ) que, juntamente com a NSA, passou a grampear as comunicações realizadas por meio de cabos de fibra ótica, incluindo ligações telefônicas e mensagens remetidas via *e-mails* no Reino Unido.

As provas, de caráter documental, também apontavam para a estreita colaboração de empresas privadas no fornecimento de dados pessoais a estes governos. Não obstante, pode-se afirmar, com base no conhecimento geral sobre essa tecnologia, que ambos os episódios trouxeram à tona novas e amplas reflexões, a saber: a derrubada definitiva do mito da utópica inviolabilidade do ciberespaço e de seu pretenso caráter de privacidade, o que permite aos usuários uma atenção redobrada em relação aos conteúdos que postam e acessam; um alerta internacional no sentido da necessidade de aperfeiçoamento constante dos meios tecnológicos, para garantir o sigilo dos seus documentos confidenciais e a proteção de informações e dados pessoais; e a demonstração da amplitude, abrangência e complexidade da rede de ciberespionagem governamental que conta com a colaboração direta de empresas privadas, além da exposição pública que acarreta nos países e cidadãos-alvo dessas atividades (Colli, 2010).

Nessa lógica, os argumentos expostos acima contribuem para elucidar, em parte, os motivos da reticência daqueles que desenvolvem e detêm a tecnologia cibernética no seu compartilhamento, ou mesmo as dificuldades em uma regulamentação, enquanto instrumento de controle e poder.

Oportuno arrolar a lição de Domingos e Couto (2011), para os quais não existe um conjunto de regras que regulamentem os servidores pelo mundo afora e como se deve agir quanto ao quesito liberdade e expressão, algo tão alardeado como sendo um direito humano. As empresas privadas que atuam na área, atuam em um mercado livre, agindo como bem entenderem. Igualmente, os criminosos, posto que no que diz respeito à ciranda agitada dos efeitos perniciosos da criminalidade se sobrelevam, atualmente, os embaraços dos crimes cibernéticos.

A diversidade da evolução da internet, por meio de computador, do telefone celular, da televisão interativa e do sistema de posicionamento global (GPS) é o mais candente dos assuntos no âmbito dos questionamentos inerentes ao direito de proteção da privacidade e da intimidade que se tornam dia a dia mais vulneráveis e mais fragilizados, em decorrência da implantação de *softwares* para informações, monitoramentos de investigação ilegal, espionagem, vigilância indevida ou ataque à segurança cibernética, situação essa muito bem retratada por Paulo Day (2014).

Com essa contextura a internet se transformou, segundo Oliveira (2019), em território de caça com recursos ao mercado clandestino virtual e no qual proliferam fantásticas arenas de informes, de comunicação e de relacionamento via *web*, seja nas conexões sociais, seja nas comunidades virtuais, com mais flexibilidade, mobilidade e massividade.

Em uma sociedade complexa, contingente, com inúmeras possibilidades de escolhas, pautada pela revolução dos meios de comunicação em massa e em tempo real com futuro incerto e inseguro, os indivíduos estão cada vez mais vulneráveis.

O conceito moderno de risco, segundo Fabretti (2014) representa uma nova maneira de enxergar o mundo e suas manifestações do caos, suas contingências e incertezas. Nesse contexto, o risco passa a se relacionar diretamente com a prevenção, ou seja, existe uma busca incessante pelo controle racional dos riscos, isto é, pelo cálculo de probabilidades estatísticas de ocorrência de determinado evento.

A sociedade de risco é – em contraste com todas as épocas anteriores – marcada fundamentalmente pela impossibilidade de imputar externamente as situações de perigo. Enquanto as culturas e fases anteriores se viam efetivamente e das mais variadas formas ameaçadas, "a sociedade pós-moderna se vê, ao lidar com riscos, confrontada consigo mesma"

(Beck, 2011, p.275). Assim, como pontua Ulrich Beck, na sociedade pós-moderna os riscos são simultaneamente produzidos para evitá-los, gerando novos riscos:

> A sociedade de risco, a autogeração das condições sociais de vida torna-se problema e tema (de início, negativamente, na demanda pelo afastamento dos perigos). Se os riscos chegam a inquietar as pessoas, a origem dos perigos já não se encontrará mais no exterior, no exótico, no inumano, e sim na historicamente adquirida capacidade das pessoas para a autotransformação, para a autoconfiguração e para a autodestruição das condições de reprodução de toda a vida neste planeta (Beck, 2011, p.275).

O risco mudou de natureza e de escala, como se, demasiadamente generalizado (risco social), se tornasse tão inseguro e incerto, ou que, demasiadamente elevado (risco tecnológico maior), se tornasse incalculável.

Ost (1999, p.343), nesse sentido, aponta um dilema: "como precaver-se do risco, na medida em que, infigurável, logra as nossas capacidades de avaliação, ou que, demasiado grande, desencoraja as nossas capacidades ético-políticas de responsabilização?".

O medo pela própria sobrevivência que leva os povos a lançarem-se nos braços do Leviatã de Hobbes[13] dá lugar na sociedade pós-moderna à "heurística do medo".

O princípio da precaução, que hoje obtém suas primeiras traduções jurídicas, surge assim como a forma contemporânea da prudência frente a um risco modificado – "a maneira contemporânea de assumir as promessas do futuro, de aceitar a aposta do futuro numa sociedade confrontada com riscos maiores e irreversíveis" (Ost, 1999, p.343).

Essa é, segundo Prittwitz (2004), a equação da formatação da sociedade de riscos: uma sociedade tecnológica, cada vez mais competitiva, que passou a deslocar rumo à marginalidade um grande contingente de pessoas, que imediatamente são percebidos pelos demais como fonte de riscos pessoais e patrimoniais. Em outras palavras, a sensação subjetiva de insegurança gera reação irracional e irrefletida por parte dos atingidos que buscam, na lei penal, a resposta imediata para toda e qualquer dor.

Uma sociedade que clama pelo controle de riscos é uma sociedade que almeja segurança, não sendo sem razão a tão usual referência a uma diversidade de circunstâncias sempre precedidas da expressão "segurança" para significar a minimização dos riscos em relação a uma determinada situação, tal como ocorre como "segurança econômica", "segurança alimentar", "segurança nuclear", "segurança social" e "segurança pública" (Fabretti, 2014, p.9). Parece, entretanto, que quanto mais se busca a segurança, paradoxalmente, mais cresce a insegurança.

---

13 Cf. Hobbes, Thomas (2006). *Leviatã*. São Paulo: Martin Claret.

A abertura da sociedade a partir da globalização acentuou esse processo: tragédias, desastres, crimes, ainda que possam ter efeito sob mais de um país, são experiências absorvidas em tempo real em todo o mundo e, naturalmente, vividas com a evidente perda de referência de tempo e espaço.

Ost (1999, p.348), aliás, bem ilustra que "a sucessão do dia e da noite (tempo cronológico) e a articulação vivida do passado, do presente e do futuro (tempo histórico) são como que absorvidas num "dia sem fim", um "presente eterno" que é o "instante dilatado" da comunicação interactiva".

Efeitos colaterais da globalização, vigilância, informação, coerção, criminalidade das mais variadas formas, inclusive, organizada e terrorista, todos afrontam a soberania dos Estados, afetando profundamente a sensação de insegurança em escala planetária e fazendo surgir o chamado Direito Penal do risco que vem, pois, acolhendo novas demandas e interesses penais[14] e antecipando a tutela penal (com tipificações abertas e amplas, frente ao uso de tipos de perigo abstrato, mera conduta, omissivos impróprios etc.). Tanto na legislação pátria quanto na estrangeira, o "direito penal do risco" vem autorizando a implementação de uma Política Criminal fundada na preocupação incessante de criminalizar e, ao mesmo tempo, de prevenir o crime organizado, a corrupção, o tráfico ilícito de entorpecentes, a criminalidade econômico-financeira, o terrorismo e os crimes contra a humanidade, primeiros indícios da tendência de tornar perene um Direito Penal de inimigos.

Assim, os riscos modernos, acentuados pelas inovações trazidas à humanidade (meio ambiente, drogas, o sistema monetário, globalização econômica e cultural, movimentos migratórios, celeridade do processamento de dados etc.), invariavelmente geram, nos dizeres de Moraes (2008), uma reação irracional e irrefletida por parte dos atingidos. Disso decorre a insegurança e o temor que têm motivado frequentes discursos postulantes de uma tutela da segurança pública, em detrimento de interesses puramente individuais.

Dito isto, o que se busca é uma tentativa de conciliar a eficiência com a proteção dos direitos fundamentais, pois, se de um lado, não se nega que os direitos fundamentais, a exemplo do direito à privacidade, devem ser preservados, por outro, não se pode perder de

14 V.g. meio ambiente, saúde pública, mercado de capital, processamento de dados, eutanásia, rechaço religioso à transfusão de sangue, greve de forme para o asseguramento do exercício de algum direito, reprodução genética, consumo de drogas, esterilização de pessoas, cirurgias transexuais, doação de órgãos, limites da liberdade sexual, limites da privacidade frente à informática e outras tecnologias modernas, do sistema econômico-financeiro, lavagem de capitais, uso de informação privilegiada nos mercados de valores, moralidade e probidade na Administração Pública, transplante de órgãos, tributos, controle cambial internacional etc.

vista, que a proteção do cidadão, para que seja eficiente, às vezes requer a violação desta privacidade.

Desta forma, as vulnerabilidades a que os indivíduos estão expostos no mundo digital reflete no papel do Estado tanto em relação à proteção da segurança quanto da privacidade, ou seja, ao mesmo tempo em que o Estado deve garantir segurança (e faz uso da vigilância para isso) também deve garantir o direito à privacidade. Assim, a vigilância estatal encontra limites posto não ser possível em uma investigação se ter acesso indiscriminado aos dados de todos os cidadãos sob a bandeira da segurança.

É esta a discussão que se avulta na próxima seção em que a investigação criminal será discutida procedendo-se a uma contraposição entre a eficiência e a proteção dos direitos fundamentais.

1.3. Investigação criminal entre a eficiência e a proteção dos direitos fundamentais

A busca da conciliação entre prevenção de criminalidade e repressão mais eficientes com respeito aos direitos humanos sempre foi, em teoria, o discurso almejado desde a consolidação do modelo de Política Criminal de inspiração clássico-iluminista.

Ainda que os movimentos pendulares e radicais tenham se sobreposto, de época em época, a essa busca do equilíbrio, nunca foi tão premente a efetivação de um projeto conciliatório.

Isso porque, conforme já assinalado, a pós-modernidade gera com todos seus hodiernos paradigmas (crise das formas mais recorrentes de controle social, formatação de uma sociedade de risco, Direito Penal de emergência, necessidade de criminalização de novas formas delituosas, dentre outros), uma crescente e inevitável hiperinflação legislativa, sem qualquer mediação ou busca de uma visão sistêmica e harmônica do ordenamento jurídico.

Em sede de investigação criminal, com vistas a contrapor a eficiência à proteção aos direitos fundamentais, é importante explorar os princípios da proibição do excesso (*Übermassverbot*) e da proibição da proteção deficiente (*Untermassverbot*), uma vez que a doutrina brasileira em especial foca somente no aspecto do processo penal como instrumento para conter o poder do Estado, sem, contudo, observá-lo também como instrumento de garantia dos direitos e valores erigidos pela sociedade.

O princípio da proibição de excesso enquadra-se no binômio indivíduo-Estado, dentro da concepção de um direito subjetivo de não intervenção estatal, decorrente do status negativo do cidadão. Referidos direitos eram definidos como direitos de defesa (*Abwehrrecte*) ou de

omissão (*Unterlassunggsrechete*). Essa concepção tradicional fez com que se defendesse a existência de um núcleo de salvaguarda essencial contra as investidas do Estado (Maciel Neto, 2020).

A definição de um direito subjetivo revela a existência de um núcleo subjetivo absoluto em favor da proibição do excesso. Nas palavras de Silva:

> Todas as versões das teorias que defendem a existência de um conteúdo essencial absoluto têm em comum a ideia de que, se fosse possível representar graficamente o âmbito de proteção dos direitos fundamentais, deveria existir um núcleo, cujos limites externos formariam uma barreira intransponível, independentemente da situação e dos interesses que eventualmente possam haver em sua restrição (Silva, 2017, p.187).

Não há como refutar, dentro da concepção de constituição de uma moldura alinhavada anteriormente, a existência de normas imutáveis e que servem de limitação material para a produção de normas infraconstitucionais. A moldura seria a forma federativa do Estado, a separação dos poderes, os direitos políticos e os direitos fundamentais individuais, restritos ao art. 5º da CRFB/1988.

O princípio da vedação deficiente também conhecido como princípio da vedação eficiente, pode ser encontrada, de forma inicial, pela teoria dos direitos fundamentais de Claus-Wilhelm Canaris (2016), que se expressa pelos denominados imperativos de tutela. De forma geral, a eficácia horizontal dos direitos fundamentais nas relações entre indivíduos se daria pelo binômio "proibição de intervenção" (decorrentes dos direitos de defesa) e "imperativos de tutela". Nas palavras de Canaris, os imperativos se justificariam porque:

> [...] o Estado é destinatário dos direitos fundamentais, já que é também sobre ele que recai a obrigação de os proteger. Por outro lado, resulta clara a razão pela qual outros cidadãos são também atingidos e os direitos fundamentais produzem também – de certa forma por uma via indirecta – efeitos em relação a eles: justamente porque também no campo jurídico-privado o Estado, ou a ordem jurídica, estão, em princípio, vinculados a proteger um cidadão contra o outro (Canaris, 2016, p.58).

A teoria de Canaris (2016), a respeito da tutela dos direitos fundamentais, rompe o subjetivismo de uma relação jurídica havida entre indivíduo-Estado, fruto daquela concepção mencionada a respeito dos status do cidadão defendida por Jellinek (1905). Os imperativos de tutela materializam a forma como a proteção objetiva dos direitos fundamentais se estabelece, com o reconhecimento necessário de que as colisões entre direitos fundamentais abarcam também reflexos a terceiros e incidem na relação cidadão-cidadão.

É, na mudança de paradigma protetivo, que o princípio da proteção eficiente encontra a sua *ratio essendi*: direitos fundamentais a prestações positivas do Estado no sentido de conferir a devida proteção aos que estiverem inseridos em uma relação jurídica.

É certo que Canaris (2016) justificou a sua teoria a fim de viabilizar a incidência da proteção dos direitos fundamentais nas relações decorrentes do direito civil. Todavia, o fato de ser construída para aplicação nas relações privadas, não impede a sua abrangência para toda e qualquer relação jurídica que envolva direitos fundamentais. Isso porque os direitos fundamentais não pertencem a uma esfera ou outra do direito; pelo contrário, são normas que pairam por todo e qualquer espaço do ordenamento jurídico. Vide, por exemplo, a disciplina dos atos e fatos ilícitos do direito civil.

Todo crime é um ato ou fato ilícito propriamente dito e que impõe a possibilidade de ressarcimento da parte prejudicada, pois, em uma relação entre iguais, a assertiva de que o direito de um termina quando começa o do outro se impõe em toda e qualquer conduta humana, independentemente da categoria normativa abstratamente alocada. Logo, a teoria de Canaris (2016) assenta-se na teoria geral do direito e possui incidência muito maior que eventualmente tenha pretendido o autor.

Os imperativos de tutela se materializam, conforme expressão de Canaris pelo dever constitucional de "proibição da insuficiência":

> [...] o Estado em princípio não regula a relação entre cidadãos através de imposições e proibições. Assim, entre eles é permitido aquilo que não for proibido. Quando, portanto, o Estado deixa um cidadão actuar sem regulamentação em face do outro, não pode ver-se-aí, em regra, a concessão de uma autorização para uma ofensa de bens do outro [...] (Canaris, 2016, pp. 60-61).

Os imperativos de tutela, por meio da proibição da insuficiência, seriam a outra corrente da balança, que contém, em oposição, as proibições de intervenção, determinadas pelas proibições de excesso. No entanto, Canaris assinala que a primeira vertente se colocaria em posição mais fraca em relação às proibições de intervenção:

> [...] a eficácia da função de imperativo de tutela, em combinação com a proibição de insuficiência, ser substancialmente mais fraca do que a da função dos direitos fundamentais como proibições de intervenção, conjugada com a proibição de excesso.
> [...] tanto no direito penal como no direito civil, é indispensável superar um primeiro específico limiar de argumentação, logo para fundamentar a existência de um dever jurídico de agir [...]. Em especial, não pode em princípio impor-se ao Estado, no âmbito das omissões, o mesmo ônus de fundamentação e de legitimação que no domínio das actuações interventivas. Pois enquanto nestas apenas tem tal ônus quanto a uma única medida – precisamente a tomada no caso – naquelas teria, eventualmente,

> de o satisfazer quanto a uma multiplicidade de medidas de protecção omitidas, ou até, mesmo, quanto à total ausência de actuação (Canaris, 2016, p.65).

Quanto à diferenciação de intensidade entre os imperativos de tutela e as proibições de intervenção, há que se ponderar duas questões. De fato, se a ideia é de construção de um Estado com fins relativistas (um meio-termo entre o liberal e o socialista), não há como negar que a liberdade individual deve ser a regra a priori e as intervenções, as exceções devidamente fundamentadas pelo Estado – seja por meio da atividade legislativa ou jurisdicional. Todavia, também não se pode olvidar que essas intensidades entre tutela e não intervenção são díspares entre as relações jurídicas de direitos civil e penal.

Como dito, Canaris (2016) estruturou sua teoria para a incidência nas relações de direito civil, nas quais prevalece o princípio da autonomia privada e se impõe uma intervenção mais restrita e justificada. Diferenciação que também acontece, mas em medida diferente, nas relações jurídicas de direito penal. Nessas, não se está diante de uma liberdade naturalmente irrestrita, manifestada em atos da vida civil, mas de comportamentos delituosos a violar direitos fundamentais de terceiros e da coletividade; portanto, ainda que haja obviamente a necessidade de ônus de fundamentação, esse juízo não se dá no terreno da autonomia da vontade civil e não se submete aos mesmos padrões restritivos que são impostos pelo direito civil.

Canotilho (2003) se refere à "proibição por defeito" (*Untermassverbot*) na equação havida com a proibição de excesso:

> Há, porém, um outro lado da proteção que, em vez de salientar o excesso, revela a proibição por defeito (*Untermassverbot*). Existe um defeito de protecção quando as entidades sobre quem recai um dever de proteção (*Schutzoflicht*) adoptam medidas insuficientes para garantir uma protecção constitucionalmente adequada dos direitos fundamentais. Podemos formular esta ideia usando uma formulação positiva: o estado deve adoptar medidas suficientes, de natureza normativa ou de natureza material, conducente a uma protecção adequada e eficaz dos direitos fundamentais. A verificação de uma insuficiência de juridicialidade estatal deverá atender à natureza das posições jurídicas ameaçadas e à intensidade do perigo de lesão dos direitos fundamentais (Canotilho, 2003, p.273).

A definição de Canotilho (2003) apresenta um aspecto interessante: a definição positiva do princípio, como sendo dever de proteção eficiente do Estado. Essa abordagem parece a mais adequada se analisada a teoria do status, pois, ainda que se esteja diante de uma proteção objetiva de direitos fundamentais, o dever de proteção eficiente se amolda ao direito

de prestações dos indivíduos em face do Estado, o que compreende o status positivo do cidadão.

O princípio da proteção eficiente tem a sua maior expressão na esfera penal. Diante da sociedade de risco e insegura, conforme já delineado por Beck (2011), os conflitos pós-modernos não mais se situaram na ausência de intervenção estatal, mas na necessidade de o Estado promover a defesa da sociedade. O avanço da criminalidade organizada, os atentados terroristas espalhados pelo mundo e o crescimento nos índices delitivos intensificaram o dever de proteção estatal, que não mais fixou seus olhos apenas para o infrator, mas também, e, principalmente, para a proteção da sociedade.

Sabe-se que há situações em que uma investigação criminal, para que seja eficiente e consiga assegurar a segurança da sociedade, precisa violar o direito à privacidade. No entanto, assim como ocorre em outras situações em que há conflitos entre direitos fundamentais, no caso em tela, em que o direito à segurança contrasta com o direito à privacidade, há que se valer da proporcionalidade para pacificar a questão.

A proporcionalidade passa, desta forma, a ser vista não somente como um limite material à investigação criminal, mas também como a proibição da proteção deficiente do bem jurídico.

Muitos países já empregam métodos massivos de vigilância e espionagem digital para fins de inteligência, prevenção criminal e investigação. No entanto, é grande ainda a resistência contra estes métodos sob a alegação de que nesta hipótese os usuários da internet estão a descoberto, tendo sua privacidade violada. Por outro lado, sabe-se que existem crimes cujos danos são de grande monta e as consequências desses delitos são mais gravosas e trazem mais danos à sociedade do que a violação da privacidade.

Dito isto tem-se que, nesse contexto, "a proibição de proteção deficiente encerra uma aptidão operacional que viabiliza ao intérprete determinar se um ato do Estado – eventualmente retratado em uma omissão, seja ela total ou parcial – mitiga um direito fundamental" (Feldens, 2007, p.222).

É exatamente nesse aspecto que a observação dos mandados de criminalização que constam em tratados internacionais de natureza rigorista implica, no caso brasileiro, a passagem do art. 5º para o art. 6º da CRFB/1988, isto é, na proteção dos direitos sociais, dentre os quais a segurança pública.

Esse garantismo denominado "garantismo positivo" já encontra, aliás, ilustração no próprio STF:

> Quanto à proibição de proteção insuficiente, a doutrina vem apontando para uma espécie de garantismo positivo, ao contrário do garantismo negativo (que se consubstancia na proteção contra os excessos do Estado) já consagrado pelo princípio da proporcionalidade. A proibição de proteção insuficiente adquire importância na aplicação dos direitos fundamentais de casos em que o Estado não pode abrir mão da proteção do direito penal para garantir a proteção de um direito fundamental[15].

Nesse diapasão, o respeito aos tratados internacionais (garantistas em sentido negativo e positivo[16]), a observância ao duplo significado da proporcionalidade e uma postura mais ativa do STF brasileiro implicam em nova leitura da relação entre a Constituição, Direito Penal e Direito Processual, qual seja: a Constituição como um limite material do Direito Penal, a Constituição como uma fonte valorativa do Direito Penal e a Constituição servindo como um fundamento normativo do Direito Penal incriminador (Feldens, 2007).

A cultura de estruturar o Direito Penal e Processual com princípios orientadores deu ensejo a um modelo de processo penal constitucional que transcende a mera hermenêutica para se transfigurar em efetivos limites da dogmática (Moraes, 2016). De um lado, os princípios estruturais da legalidade (art. 5º, II) e igualdade (art. 5º, caput) implicam a consagração do Direito Penal e Processual Penal iluministas. Além disso, a ênfase na proteção das garantias fundamentais e da dignidade da pessoa humana, consubstanciadas nos princípios do juiz e promotor naturais (art. 5°, XXXVII e LIII e art. 5º, LIII da CRFB), na inocência presumida (art. 5º, LVII, da CRFB), no princípio do devido processo legal (art. 5º, LV da CRFB)[17], nos princípios do contraditório (art. 5º, LV da CRFB) e da ampla defesa (art. 5º, LV da CRFB), na publicidade (art. 5º, LX, e art. 93, IX da CRFB) e motivação das decisões como regras (art. 93, IX da CRFB), na inadmissibilidade das provas ilícitas (art. 5º, LVI da CRFB) geraram alterações em todo o sistema Processual Penal brasileiro e, de outra parte,

---

15 O STF posicionou-se, pela primeira vez, acerca do tema, quando do julgamento do Recurso Extraordinário 418.376/MS16. Discutia-se, em síntese, se a negativa de equiparação do instituto da união estável ao casamento, para fins de incidência da hipótese especial de extinção de punibilidade nos tipos penais componentes dos "crimes contra os costumes", consubstanciada no art. 107, inc. VII do CP ocasionava uma violação ao art. 226, § 3º, da CRFB de 1988.

16 Neste sentido veja os mandados de criminalização do genocídio (Convenção para a Prevenção e a Repressão do Crime de Genocídio – Paris, 09.12.1948 – instituída pelo Decreto 30.822, de 06.05.1952); drogas (Convenção Única sobre Entorpecentes de 1961, emendada em 1972 e Convenção Contra o Tráfico Ilícito de Entorpecentes e Substâncias Psicotrópicas de 1988; organizações criminosas (convenção de Palermo – Decreto 5.015/04); corrupção (Convenção de Mérida – Decreto 5.687/06; ademais, veja-se os crimes contra a humanidade mencionados no art. 7º do Tratado de Roma, promulgado no Brasil pelo Decreto 4.388, de 25.09.2002).

17 Na acepção de cunho material, tem-se que "a essência do substantive *due process of law* reside na necessidade de proteger os direitos e as liberdades das pessoas contra qualquer modalidade de legislação que se revele opressiva ou destituída do necessário coeficiente de razoabilidade" (Min. Celso de Mello, STFADIMC-1755/DF)

representaram a adoção de uma postura do STF mais ativista e militante, contrariamente ao que advogam os defensores de um sistema puramente acusatório.

De outra parte, consoante expõe Moraes (2016), no denominado garantismo positivo, esse dever de proteção (hipótese na qual está incluída a segurança dos cidadãos), representa a obrigação de o Estado, nas situações em que for necessário, adequado e proporcional em sentido estrito, limitar os direitos fundamentais dos cidadãos.

Essa dualidade tem, inegavelmente, propagado discussões extremadas na jurisprudência nacional, a exemplo do que ocorreu com o debate sobre o poder investigatório do Ministério Público; a limitação de prazo para as interceptações telefônicas e telemáticas; a aplicação do princípio da insignificância no inquérito policial; dentre outros.

Estas são ilustrações que reforçam e repisam a tese ora exposta: os discursos ideológicos ucrônicos insistem em advogar teses puras e radicais sem atentar ao presente tempo social e, dessa forma, ignoram que a moral média, o equilíbrio e a razoabilidade exigem algo diverso e conciliador para a construção de um Direito Penal de temperança.

No magistério de Moraes (2008), tanto o discurso considerado politicamente correto (que afirma que a prisão não recupera), quanto o discurso que defende a tolerância zero (ignorando que parcela do aumento da criminalidade encontra-se na omissão do Poder Político e de outras esferas de controle social), impedem o bom senso, a racionalidade e uma Política conciliatória que deveriam nortear o tema.

A busca de uma Política Criminal de temperança, esculpida pelo bom senso e racionalmente hábil a atender as diferentes formas de criminalidade, apenas começa com o conhecimento sobre esse contexto contemporâneo: o do mundo pós-moderno, pós-industrial e globalizado.

O grande desafio atual é, portanto, constituir a legitimidade de uma investigação criminal que pretende tutelar bens transindividuais e, simultaneamente, combater a criminalidade de massa, o terrorismo, as organizações criminosas e o crime de colarinho branco, isto é, conciliar modelos eficientes e eficazes para enfrentar a criminalidade com os princípios constitucionais do Estado democrático de Direito.

Jakobs e Meliá (2005), aliás, há algum tempo sustentou a tese de que um "Direito Penal do inimigo" claramente delimitado ofereceria menos risco, na perspectiva do Estado de Direito, que emaranhar todo o Direito Penal com fragmentos de regulações inerentes a um Direito Penal de terceira velocidade.

Constata-se de um lado uma sociedade insegura, enervada por uma mídia sensacionalista e por um discurso criminológico de baixo custo (transformando Política

Criminal em exclusiva política policial); de outro, o sonho romântico e ucrônico de manutenção pura do modelo de inspiração clássica que defende, de forma paradoxal, políticas de despenalização sem metodologia científica e sem suporte empírico, visando simplesmente a diminuição da população carcerária.

O que se percebe é que a defesa das garantias individuais tende a conduzir seus defensores à categoria de construtores de um sistema frágil, inoperante frente ao caos e rotulados política e ideologicamente à esquerda. A seu turno, aqueles que defendem a primazia da segurança pública tendem a ser vistos como conservadores e perpetuadores do autoritarismo estatal em detrimento das garantidas individuais e da proteção dos direitos humanos.

Os argumentos nascidos da falsa cisão entre laxismo e rigorismo, entre busca da liberdade e da segurança coletiva conduzem a extremos indesejados e que não representam a moral média coletiva. Esta oposição não pode continuar sendo vista como excludente, mas, sim, complementar, para fazer uso da concepção de Bobbio (1996) uma vez que ambos os modelos implicam no desejo de estabilidade e respeito à ordem legal estabelecida no Estado Democrático de Direito.

2. Investigação Criminal Tecnológica e as limitações condicionadas pelo Direito Probatório

Os humanos e as máquinas vivem uma relação cada vez mais próxima. Uma relação que oferece grandes oportunidades, mas também ameaças. Na verdade, a tecnologia nunca é neutra. É muito pessoal porque tem implicações éticas, políticas e jurídicas.

Sem dúvida, os sistemas de justiça criminal podem se beneficiar muito com o uso das tecnologias digitais. Muitos países já estão usando essas tecnologias para aumentar a eficiência de seu sistema de justiça, aumentar a transparência, fortalecer as investigações criminais, melhorar a gestão de casos e combater o crime.

Assim, em um esforço para combater a criminalidade e coletar evidências digitais relevantes para todos os tipos de delitos, as agências de aplicação da lei estão incorporando a coleta e análise de evidências digitais em sua infraestrutura (Bueno de Mata, 2014).

No entanto, é preciso cautela, pois se é verdade que a tecnologia facilita a investigação criminal, é também verdade que esta facilidade pode vir acompanhada de violações aos direitos fundamentais, a exemplo da privacidade, que é um direito humano fundamental, essencial para se viver com dignidade e segurança.

Este capítulo analisa a investigação criminal tecnológica e as limitações condicionadas pelo direito probatório. Assim, em sua primeira seção apresenta as premissas conceituais sobre a investigação criminal e a prova penal e, na sequência, se debruça sobre os sentidos da prova no processo penal e sobre a distinção entre as intituladas provas cautelares, não repetíveis e antecipadas.

A segunda seção se dedica à análise da prova penal digital. Para tanto, apresenta o seu conceito, suas características, formas de aquisição e de preservação.

Por fim, na terceira e última seção foram abordados os métodos ocultos de investigação criminal e os limites impostos pelo direito probatório. Assim, inicia trazendo os conceitos e as características dos referidos métodos, passando-se na sequência a discutir os princípios gerais aplicáveis às provas e finaliza apresentando as proibições de prova enquanto limites aos métodos ocultos de investigação criminal.

2.1 Premissas conceituais sobre investigação criminal e prova penal

Do ponto de vista sociológico, é possível afirmar que o crime é um fenômeno presente em todas as sociedades de todos os tipos. "Não há nenhuma onde não haja criminalidade.

Muda de forma, os atos assim qualificados não são os mesmos em todo o lado; mas sempre e em toda a parte existiram homens que se conduziram de modo a incorrer na repressão penal". (Durkhéim, 2005, p. 82)

Por sua vez, o Direito Penal, material e processual, vem sendo aplicado como mecanismo de controle desse fenômeno social em todas as sociedades politicamente organizadas, desde as mais primitivas até as complexas sociedades modernas, não obstante as variadas e seguidas crises de legitimidade que se impõem ao sistema penal.

Na verdade, a busca dessa legitimação nunca encontrou consenso, variando entre os extremos da defesa do abolicionismo à maximização do Direito Penal. O que de fato se observa nas sociedades contemporâneas, mesmo as com maior desenvolvimento democrático, é um aumento de normas incriminadoras e, consequentemente, de instrumentos a serviço da prevenção e do esclarecimento de infrações penais, muito em razão da difusão dos riscos e do medo crescentes na atualidade (Silva Sánches, 2001).

Nesse quadro, a notícia da ocorrência de um crime faz surgir a obrigação dos órgãos estatais integrantes do sistema penal de dar início à busca pelo esclarecimento do fato noticiado[18], com o fim de restabelecer a verdade e possibilitar a responsabilização do possível transgressor.

A verdade, especialmente a sua busca, é tradicionalmente apontada como o principal objetivo do processo penal, cujo conteúdo é objeto de complexo debate, tanto no campo filosófico quanto jurídico. O debate sobre o sentido da verdade no processo penal não é objeto desta pesquisa. Cabe, no entanto, aqui pontuar a visão da doutrina contemporânea que afasta a ideia de um realismo ingênuo, de uma verdade real absoluta, devendo ser concebida no âmbito processual penal sob a forma de reconstrução aproximativa dos fatos a partir das evidências obtidas no processo (Taruffo, 2009).

Nessa perspectiva, reconhecendo-se a impossibilidade de se alcançar um grau absoluto de conformidade com os fatos ocorridos no mundo real, a atividade investigativa, assim como a instrução probatória, deve se orientar no sentido de buscar os mais qualificados elementos capazes de melhor se aproximar da reconstrução fática, com a devida obediência aos limites impostos pelo Estado Democrático de Direito.

A busca da verdade, no sentido da reconstrução fática aproximativa, é, pois, tarefa comum da investigação criminal e da prova penal em juízo. É por meio da investigação criminal que se inicia esse importante encargo estatal. Essa atividade traduz-se, portanto, no

18 Considera-se aqui a obrigatoriedade da ação penal nos crimes de ação penal pública, que constituem a maioria dos crimes previstos na legislação brasileira.

ponto de partida da persecução penal, instrumento essencial do sistema penal sem o qual o Estado não pode exercer o seu poder-dever de punir. Trata-se, assim, do alicerce da ação penal, onde se delimita o objeto do processo penal.

Nesse sentido, ao abordar o tema no âmbito do processo penal português, Costa Pinto (2018, p.9) sublinha que "é no inquérito que se desenvolve a investigação criminal, se delimita sucessivamente o objecto do processo, se identificam ou se eliminam suspeitos, se recolhe o essencial das provas e se decide levar ou não o caso a julgamento".

Do ponto de vista normativo, não há na legislação brasileira conceito taxativo de investigação criminal, em que pese esta atividade estatal esteja prevista na CRFB, no CPP, e em outras legislações dispersas[19].

Em regra[20], a investigação criminal no Brasil é conduzida pela polícia judiciária, por meio do inquérito policial, qualificado como procedimento administrativo informativo, composto por um conjunto de diligências preliminares devidamente formalizadas destinadas a apurar a existência de um crime, identificar os seus autores e recolher provas e elementos informativos de tudo que possa servir ao esclarecimento do fato para instruir e subsidiar futura ação penal (Nucci, 2002).

Ao contrário do Brasil, o ordenamento jurídico português apresenta um conceito legal de investigação criminal definindo-a como um "conjunto de diligências que, nos termos da lei processual penal, se destinam a averiguar a existência de um crime, determinar os seus agentes e a sua responsabilidade e descobrir e recolher as provas, no âmbito do processo"[21].

No âmbito doutrinário, numa perspectiva mais clássica, a investigação criminal é definida como o conjunto de atividades do Estado, desenvolvidas em um procedimento administrativo preparatório da ação penal, voltadas a reunir elementos suficientes à apuração da autoria e da materialidade de uma infração penal, destinados à formação do convencimento do responsável pela acusação[22].

Ao abordar o inquérito policial enquanto principal instrumento de investigação criminal no Brasil, Nucci (2015) aponta que:

---

19 Dentre as legislações dispersas, pode-se citar a Lei 12.830/2013, que dispõe sobre a investigação criminal conduzida pelo delegado de polícia; e a Lei nº 12.850/2013, que define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal a ser aplicado.

20 Diz-se, em regra, pois a investigação criminal no Brasil pode ser conduzida diretamente pelo Ministério Público, conforme entendimento pacificado no STF (RE 593727, Rel. Min. Cezar Peluso, DJ 14/05/2015).

21 Lei nº 49, de 27 de Agosto de 2008.

22 Nesse sentido: André Nicolitt (2010, p. 71); Nucci (2011, p. 148); e Pacelli (2012, p. 4).

> O inquérito policial é um procedimento preparatório da ação penal, de caráter administrativo, conduzido pela polícia judiciária e voltado à colheita preliminar de provas para apurar a prática de uma infração penal e sua autoria. [...]
> Seu objetivo precípuo é servir de lastro à formação da convicção do representante do Ministério Público (*opinio delicti*), mas também para colher provas urgentes, que podem desaparecer, após o cometimento do crime. Não se pode olvidar, ainda, servir o inquérito à composição das indispensáveis provas pré-constituídas que servem de base à vítima, em determinados casos, para a propositura da ação penal privada (p.98).

Sob a mesma conotação pragmática, Valente (2009) também destaca a função preparatória da investigação criminal ao destacar que:

> A investigação criminal, levada a cabo pela polícia, procura descobrir, recolher, conservar, examinar, e interpretar provas reais e também procura localizar, contactar e apresentar as provas pessoais que conduzam ao esclarecimento da verdade material judicialmente admissível dos factos que consubstanciam a prática de um crime, ou seja, a investigação criminal pode ser um motor de arranque e o alicerce do processo crime que irá decidir pela condenação ou pela absolvição (p. 102).

Pelos conceitos apresentados, percebe-se que a investigação criminal tem por finalidade básica amealhar um conjunto de elementos informativos e probatórios, de cognição sumária, capazes de subsidiar um juízo de probabilidade acerca da ocorrência de um crime e de sua autoria destinados a quem tem competência para oferecer a acusação (ou seu arquivamento). Esse conjunto de elementos probatórios razoáveis reveladores da materialidade e autoria do delito é o que se denomina de justa causa para a ação penal (Greco Filho, 1999).

A justa causa, entendida no sentido da existência de um suporte probatório mínimo, repita-se de cognição sumária, da existência de um crime e da presença de indícios de sua autoria (*fumus comissi delicti*), constitui requisito específico para o recebimento da denúncia no ordenamento jurídico brasileiro, sem a qual a denúncia deverá ser rejeitada[23].

No entanto, em que pese a busca pelo esclarecimento do fato apontado como criminoso constitua objetivo imediato da investigação, esta não é a única razão de sua existência. Tampouco se presta à mera satisfação jurídica de uma pretensão acusatória, que só pode se iniciar sob a presença de justa causa, mas sim constitui instrumento para o eficaz funcionamento da justiça penal.

Denota-se, então, o caráter instrumental da investigação criminal a serviço de outro instrumento (o processo penal). Nesse sentido, Lopes Jr. (2003) dispõe que:

---

23 É o que dispõe o artigo 395, inciso III, do Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal brasileiro).

> O processo penal, em teoria, pode prescindir da investigação preliminar. Mas a investigação preliminar existe para o processo. É importante frisar que "em teoria" o processo pode não necessitar da investigação preliminar, inclusive porque pode ter o caráter facultativo. Sem embargo, na prática, quanto maior for a gravidade do delito, maior será a importância da instrução, ao ponto de poder-se afirmar que, excetuando-se os delitos de menor potencial lesivo, nenhum promotor ou juiz prescinde dessa investigação prévia (pp. 40-41).

Discorda-se, todavia, do sobredito autor quanto à prescindibilidade, ainda que teórica, da investigação criminal. Na verdade, a lei processual penal brasileira autoriza o Ministério Público a dispensar o inquérito policial para o oferecimento da denúncia[24], desde que disponha de elementos que o habilitem a promover a ação penal. Assim, mesmo em casos mais simples que possam prescindir da formalização de um inquérito policial, a investigação preliminar ainda que sumária é indispensável.

Na verdade, compreende-se a investigação criminal como instrumento imprescindível para a efetiva garantia processual constitucional e para a busca da concretização da justiça. Nesse sentido, Rangel (2013) destaca que:

> [...] a verdade é que o inquérito policial tem uma função garantidora. A investigação tem nítido caráter de evitar a instauração de uma persecução penal infundada, por parte do Ministério Público, diante do fundamento do processo penal, que é a instrumentalidade e o garantismo penal (p.71).

Nessa perspectiva, a investigação criminal não pode ser compreendida somente como uma ferramenta a serviço do Estado para reunir informações e evidências capazes de fundamentar uma acusação contra um suspeito da prática de um crime. Mais do que isso, a investigação preliminar traduz-se em importante instrumento de proteção dos direitos e garantias individuais à medida em quem exerce a função de filtro processual para evitar acusações infundadas, desprovidas de lastro probatório suficiente, assegurando-se ao cidadão investigado que ele não será processado e muito menos punido de forma arbitrária (Lopes Jr., 2016).

Sobre essa função garantidora da investigação criminal, Mendes de Almeida (1973) destacava que:

> A instrução preliminar é uma "instituição indispensável à justiça penal". Seu primeiro benefício é "proteger o inculpado". Dá à defesa a faculdade de dissipar as suspeitas, de combater os indícios, de explicar os fatos e de destruir a prevenção no nascedouro;

24 Cf. artigo 39, parágrafo 5º, e artigo 28, do Código de Processo Penal brasileiro.

> propicia-lhe meios de desvendar prontamente a mentira e de evitar a escandalosa publicidade do julgamento (p. 11).

Na mesma linha, ao tratar sobre o papel do inquérito policial, Bonfim (2008) leciona que:

> O inquérito policial tem caráter essencialmente instrumental. Sua finalidade é possibilitar a reunião de elementos de prova que reforcem e fundamentem as suspeitas acerca da prática de delito de natureza penal. Nesse sentido o inquérito policial é um procedimento preparatório para eventual ajuizamento de ação penal.
> Além disso, o inquérito policial serve também como elemento de "filtragem" do sistema penal, ao prevenir a movimentação do Poder Judiciário para o processamento de fatos não esclarecidos ou de autoria desconhecida (pp. 104-105).

Além das funções essenciais de descoberta da "verdade" (busca do fato oculto) e de filtro processual contra acusações infundadas (função garantidora), a doutrina moderna destaca, ainda, que a investigação criminal desempenha importante função simbólica, a partir da visibilidade da atividade investigativa, contribuindo-se para dissuadir a prática de crimes e afastar o sentimento de impunidade (Lopes Jr., 2016).

Assim, em que pese o caráter instrumental da investigação criminal, pelo que não se lhe impõe a missão de conter a violência, a sua função simbólica exerce valiosa influência na confiança social no sistema de justiça penal e consequentemente na redução do índice de criminalidade oculta. Assim, quanto mais eficaz for a investigação criminal na busca do fato oculto, menor será o índice de criminalidade desconhecida.

Nesse sentido, ensina Lopes Jr. (2003) que:

> Existe uma clara relação entre a eficácia da instrução preliminar e a diminuição dos índices de *criminal case mortality*, de modo que, quanto mais eficaz é a atividade destinada a descobrir o fato oculto, menor é a criminalidade oculta ou latente, ou ainda, as *cifras de la ineficiencia de la justicia*, como prefere Ferrajoli. Em síntese, quando menor é a diferença entre a *criminalidade real* e a *criminalidade conhecida* pelos órgãos estatais de investigação, mais eficaz será o processo penal como instrumento de reação e controle formal da criminalidade (pp. 40-41).

Essa tríplice funcionalidade da investigação criminal destacada pela doutrina moderna traduz o paradigma constitucional garantista, alicerçado no respeito aos direitos humanos fundamentais inalienáveis, que deve orientar o sistema penal no Estado Democrático de Direito. Nesse quadro, o investigado passa a ser visto como sujeito de direitos e não como mero objeto de investigação.

Para o cumprimento das destacadas funcionalidades, a investigação criminal busca afastar as dúvidas e presunções, e reunir um "conjunto probatório" capaz de conferir um juízo de probabilidade suficiente à abertura de uma ação penal. Também de caráter instrumental, busca-se no processo penal a descoberta da verdade por meio da produção de provas.

É exatamente no contexto da descoberta da verdade que avulta a importância de buscar esclarecer algumas das diversas acepções da palavra prova no processo penal e a sua relação com os atos desenvolvidos na investigação criminal.

Não obstante a polissemia da palavra prova, cujo conteúdo será objeto de discussão no item a seguir, em sentido amplo, provar significa demonstrar a veracidade de um enunciado acerca de um fato acontecido na realidade.

No campo penal, Florian (1983) expõe que "provar é fornecer, no processo, o conhecimento de qualquer fato, adquirindo, para si, e gerando noutrem, a convicção da substância ou verdade do mesmo fato" (p. 87).

Por sua vez, Ferrua (2018) destaca três componentes essenciais da prova penal: - os *meios* potencialmente adequados para provar, ou seja, as provas no sentido de instrumentos que serão utilizados para corroborar as proposições probatórias (*elementos* de prova); - o *objeto* ou *tema* da prova, no sentido de proposição a ser provada, que deve ser constituída por uma frase apofântica, isto é, verdadeiro ou falso; e a prova no sentido de *critério* ou *regra de julgamento*, representado pelo cânone "além de qualquer dúvida razoável" (pp. 83-84).

Em termos gerais, portanto, a prova é uma operação que visa verificar qualquer proposição ou hipótese, para determinar se tal é verdadeira ou falsa, a partir da coleta de elementos que confirmem ou neguem aquela asserção a respeito de um fato que interessa ao julgamento. Estabelecidas as premissas ora apresentadas, cumpre discorrer na próxima seção da pesquisa sobre os variados sentidos da prova no processo penal.

2.1.1. Os variados sentidos da prova no processo penal: em busca por definições

A prova é um dos temas mais importantes e complexos da ciência processual, cujas funções e natureza relacionam-se diretamente com a compreensão acerca dos fundamentos existenciais do processo, do alcance da verdade e da justiça da decisão.

Consoante apontado em linhas anteriores, a definição da verdade que se busca no processo é ponto cercado de controvérsias, longe de consenso científico. No entanto, seja qual for o sentido empregado ao termo, a prova é o meio através do qual se propõe alcançar a verdade no processo.

O processo é o lugar onde se busca estabelecer qual a narrativa é a "mais verdadeira", através das evidências disponíveis, cuja confirmação probatória da "verdade dos fatos" constitui condição fundamental da justiça da decisão (Taruffo, 2009, p. 30). Conforme já advertia Benthman, "a arte do processo não é essencialmente senão a arte de administrar as provas" (Bentham *apud* Ferreira, 1988, p. 221).

No âmbito do processo criminal, a prova assume ainda mais importância, "pois só a prova cabal do fato criminoso é capaz de superar a presunção de inocência do acusado, que representa a maior garantia do cidadão contra o uso arbitrário do poder punitivo" (Gomes Filho, 2005, p. 303).

Como se vê, as funções atribuídas à prova no processo, por si sós, já denota a complexidade da sua compreensão, cuja dificuldade é acrescida pela natureza polissêmica do emprego da palavra prova no âmbito do processo penal. Isto porque o conceito de prova no aspecto processual não é unívoco, mas sim polissêmico, porque ora designa o resultado buscado para a comprovação do fato investigado, ora se refere à atividade desenvolvida no processo, para a demonstração daquele fato, como as perícias, os documentos, a confissão etc., também chamados meios probatórios (Silva, 2019).

Ademais, adverte Gomes Filho (2005) que:

> [...] grande parte das dificuldades encontradas pelo jurista no tratamento da matéria está no emprego, nem sempre adequado, de certas expressões próprias da linguagem comum, da terminologia filosófica e científica ou mesmo elaborada em outras culturas jurídicas, que nem sempre servem para esclarecer a natureza dos fenômenos ligados à prova judiciária, mas, ao contrário, muito contribuem para incertezas, equívocos e contradições (p. 303).

Daí a importância de se mergulhar, ainda que de maneira rasa, no léxico probatório, limitando-se à busca dos significados que interessam diretamente a esta pesquisa, naquilo que se relaciona com o tema. Notadamente, no intuito de permitir examinar os reflexos das limitações do direito probatório na investigação criminal tecnológica.

A palavra prova, no âmbito do processo penal, assume diferentes conotações. Basta uma sucinta incursão no CPP brasileiro, por exemplo, para se constatar essa polissemia do termo. Ora a prova é utilizada no sentido de elemento de prova ou *factum probans*[25], ora denota a ideia de meios de prova[26], ora se refere às fontes de prova[27], só para citar alguns exemplos.

25 Nesse sentido é o artigo 155, *caput*, do CPP.

26 Nesse sentido o parágrafo único do artigo 155 do CPP.

27 Nesse sentido artigo 157 do CPP.

Inicialmente, mencionam-se pelo menos três acepções do vocábulo prova, empregadas igualmente tanto na linguagem comum quanto no discurso jurídico, quais sejam: como demonstração; como atividade ou procedimento de experimentação; e como desafio ou competição (Gomes Filho, 2005).

Como *demonstração*, a prova é entendida como o elemento capaz de confirmar a "verdade" das asserções sobre os fatos apresentados. Na linguagem comum, provar seria atestar a verdade de algo. Na mesma linha, no campo jurídico, utilizando expressão análoga, Taruffo (2009) aponta a função epistémica da prova, com a conotação de instrumento de descoberta sobre os fatos do processo, ou mais corretamente, sobre as declarações dos fatos. As provas, nesse sentido, correspondem aos elementos capazes de atribuir credibilidade às assertivas relevantes para a decisão, com base cognitiva suficiente e adequada a ser considerada como "verdadeiras" (p. 33).

Como *atividade ou procedimento de experimentação*, na linguagem comum a prova tem a conotação de teste, experiência, conjunto de exames para verificar a validade de uma hipótese ou declaração. No âmbito processual, a prova enquanto atividade denota o sentido de *instrução probatória*, ou seja, a tarefa de recolher os elementos ou evidências que permitam confirmar ou refutar as alegações sobre os fatos, para permitir o estabelecimento da verdade aproximativa do fato histórico.

Por sua vez, como *desafio ou competição*, a prova indica comumente um obstáculo a ser ultrapassado para se alcançar o reconhecimento de determinada habilidade ou competência. Nessa conotação, o termo prova é empregado na linguagem processual para se referir ao *ônus da prova*, ou seja, o encargo imposto à parte processual para demonstrar a credibilidade de alegações de seu interesse.

Consoante adverte Gomes Filho (2005), a tríplice acepção sublinhada acima não é suficiente, todavia, para esclarecer e delimitar o emprego do vocábulo prova no âmbito processual, em especial no processo penal. Justifica-se, assim, perquirir os principais sentidos atrelados à prova na doutrina processual penal, nomeadamente o que se denomina de *objeto* de prova, *fontes* de prova, *elementos* de prova, *resultado* de prova, *meios* de prova e *meios de investigação* da prova

Tradicionalmente, a doutrina costuma tratar o *objeto* de prova como os fatos ou circunstâncias que devam ser demonstrados, isto é, aquilo sobre o qual a prova deve recair para a correta aplicação do direito ao caso em julgamento. Nesse sentido, pontua Marques (1997) que o "objeto da prova, ou *thema probandum* é a coisa, fato, acontecimento ou circunstância que deva ser demonstrado no processo" (p. 254).

Já Coimbra (2018) afirma que objeto de prova ou *thema probandum* consiste em circunstâncias e fatos juridicamente relevantes[28], principais ou secundários, que precisam ser demonstrados perante o órgão julgador (autoria, materialidade, causas de aumento, qualificadoras, causas excludentes de ilicitude etc.). Assim, o *thema probandum* corresponde aos fatos e circunstâncias a serem provados, por terem relevância ou potencial para influir na decisão acerca das circunstâncias de fato e de direito vinculadas ao processo, alcançando não só a própria procedência ou improcedência da acusação, mas também os limites da responsabilização criminal e da fixação da pena ou medida de segurança.

No entanto, a epistemologia moderna, ao reconhecer a total impossibilidade de se reconstituir fidedignamente um fato passado, sustenta que não se busca no processo provar fatos pretéritos, mas a demonstração de sua ocorrência por meio de provas das *proposições sobre os fatos*. O objeto da prova não são fatos, mas *hipóteses* sobre fatos (Dallagnol, 2016).

Nesse sentido, Gascón Abellán (1999) pontua que "um fato não pode ser provado *a posteriori*, apenas se lhe pode constatar a ocorrência. O que se provam são enunciados assertivos, ou seja, proposições" (p. 83). Na mesma linha de pensamento, Gomes Filho (2005) adverte que:

> [...] o que se procura no processo é a verdade ou falsidade de uma *afirmação sobre um fato.* É que o fato, como fenômeno do mundo real, somente poderia ser constatado no próprio momento em que se verifica; não é possível, portanto, *provar* um acontecimento passado, mas somente demonstrar se uma afirmação sobre este é ou não verdadeira (p. 317).

A partir dessa atual visão sobre o *thema probandum*, a doutrina moderna conclui que a atividade probatória não pode estar dissociada do contraditório processual, uma vez que o seu objeto não são simples *fatos externos*, mas a interpretação acerca das *afirmações sobre os fatos* (Gomes Filho, 2005). Os *raciocínios probatórios* são, assim, sempre probabilísticos construídos a partir dos argumentos apresentados pelas partes, em contraditório, com o fim de construir a *melhor resposta* capaz de conferir a "certeza" necessária para o julgamento (Dallagnol, 2016, p. 113).

Ancorado no *standart* probatório americano cuja premissa pressupõe a impossibilidade de se alcançar mais do que probabilidades na atividade probatória, Dallagnol (2016) pontua que a "certeza" necessária para se condenar alguém no processo penal não pode ser a "certeza

28 Extrai-se do art. 124º do CP de Portugal: "[...] constituem objeto da prova todos os factos juridicamente relevantes para a existência ou inexistência do crime, a punibilidade ou não punibilidade do arguido e a determinação da pena ou medida de segurança aplicáveis e os factos relevantes para a determinação da responsabilidade civil".

filosófica", definida como a completa ausência da capacidade subjetiva para duvidar, mas a certeza ancorada em provas que vão além da "dúvida razoável", ou seja, que afastem qualquer possibilidade de inocência do acusado (p. 113).

Sobre o assunto, Ferrua (2018) destaca que o elemento de prova no processo penal pertence ao modelo de prova argumentativa em que as premissas "subdeterminam" a proposição de provar, isto é, tornam o argumento mais ou menos provável, mais ou menos fundamentado, visto que não existe garantia de que "ser provado como verdadeiro" corresponde necessariamente "ser verdadeiro". Assim, seja qual for o grau da prova presente no processo, sempre é possível questionar a culpa afirmada pelo juiz. Daí a necessidade de moderar as reivindicações da verdade, substituindo à fórmula categórica de além de qualquer "dúvida lógica", a fórmula mais modesta e flexível de além de qualquer "dúvida razoável" (pp. 111-112).

Acrescenta o mesmo autor que, do ponto de vista operacional, a regra tem uma função dupla: - a de afastar o risco de uma condenação injusta, na medida em que o juiz só pode condenar com base em provas robustas e que não haja nenhuma "negação significativa" a implicar dúvida razoável; e - simetricamente, a mesma regra implica que, se a culpa é apoiada por um quadro de provas sólido e coerente, o reconhecimento honesto da falibilidade das investigações não deve evitar uma condenação. Assim, se a dúvida não parece razoável, o resultado das provas deve ser assumido como certo, dada a impossibilidade de justificá-lo em termos absolutos e definitivos (Ferrua, 2018).

Prosseguindo-se na busca das acepções terminológicas da prova no processo penal, as *fontes* de prova são os elementos externos ao processo dos quais se podem obter os dados relevantes à comprovação da afirmação sobre o fato alegado (*elementos* de prova). Na linguagem comum, fonte é a pessoa ou situação da qual provém as informações sobre um determinado fato.

No âmbito da ciência processual, "fala-se em *fonte* de prova para designar as *pessoas* ou *coisas* das quais pode-se conseguir a prova (*rectius*, o elemento de prova), resultando disso a sua usual classificação em *fontes pessoais* (testemunhas, vítima, acusado, peritos) e *fontes reais* (documentos, em sentido amplo)" (Gomes Filho, 2005, p. 308).

Constituem *elementos* de prova os dados objetivos que confirmam ou negam a proposição a respeito de fato que interessa à decisão da causa, ou seja, são aquilo que se extrai das fontes de prova, como, por exemplo, a declaração de uma testemunha, o conteúdo de um documento, a informação prestada pela vítima, dentre outros (Tonini, 2002).

Os *elementos* de prova devem ser, em regra, produzidos na fase judicial com a participação dialética das partes, ou seja, obtidos necessariamente sob contraditório judicial, salvo nos casos das provas irrepetíveis, cautelares ou antecipadas, produzidas antes da instrução judicial, as quais serão analisadas no tópico a seguir.

Nesse ponto, importa destacar outra expressão congênere utilizada na linguagem processual penal brasileira que se trata do elemento de informação[29]. A doutrina tradicional costuma distinguir o elemento penal informativo (ou de informação) a partir de três critérios: - quanto ao momento do procedimento; quanto ao método de produção; e quanto ao valor probatório atribuído.

Sob esse prisma, tradicionalmente, o elemento penal informativo é apontado como o dado objetivo colhido na fase de investigação (pré-processual), sem contraditório judicial, isto é, resultado material dos atos de investigação, com limitado valor probatório, destinado a essencialmente a embasar a ação penal a ser promovida pelo seu titular (*opinio delicti*) ou como fundamento para a decretação de medidas cautelares (Bechara, 2014).

Em abordagem aprofundada sobre o tema, Soares (2014) apresenta definições de elemento penal de informação, em sentido amplo e em sentido estrito, correlacionando-o com o que entende por *elemento* de prova. Em sentido amplo, elemento penal de informação se trata do gênero que contempla os *elementos informativos em sentido estrito* e os *elementos de prova* pré ou pós-constituídos.

Por sua vez, segundo Soares (2014), *elemento penal informativo* ou, simplesmente, *elemento de informação* ou *elemento investigativo*, em sentido estrito, "é o dado objetivo colhido sem regular contraditório judicial, geralmente (mas nem sempre) em fase pré-processual penal, referente ao suposto fato penalmente relevante sob reconstrução e passível de ser posteriormente reproduzido na fase e modo processualmente próprios" (p. 38). Neste trilhar, conclui Soares (2014) que:

> Por tudo isso, dito de outro modo, no Direito Processual Penal brasileiro *elemento de prova* pode ser entendido como elemento informativo *geralmente* qualificado (jurídica e epistemologicamente) por ter sido colhido sob regular contraditório judicial ou, quando *excepcionalmente* ausente este, justificado por situações de irrepetibilidade, cautelaridade ou legítima antecipação, conforme a ressalva feita no *caput* do art. 155 do nosso CPP (p. 38).

29 Art. 155. O juiz formará sua convicção pela livre apreciação da prova produzida em contraditório judicial, não podendo fundamentar sua decisão exclusivamente nos elementos informativos colhidos na investigação, ressalvadas as provas cautelares, não repetíveis e antecipadas.

A conclusão que se extrai dos *elementos* de prova pré ou pós-constituídos, legitimamente integrados ao processo penal, por meio da atividade de interpretação fundamentada do julgador, é o que se denomina de *resultado* da prova (Gomes Filho, 2005). Como *resultado,* a prova é entendida no sentido de *critério* ou *regra de julgamento*, representado pelo cânone "além de qualquer dúvida razoável" (Ferrua, 2018, pp. 83-84).

Por sua vez, os *meios* de prova são "os instrumentos ou atividades por intermédio dos quais os dados probatórios (elementos de prova) são introduzidos e fixados no processo (produção da prova). São, em síntese, os *canais de informação* de que se serve o juiz" (Gomes Filho, 2005, pp. 308-309).

No mesmo sentido, Badaró (2003) afirma que *meios* de prova são os instrumentos por meio dos quais as *fontes* de prova são levadas para o processo. "Assim, a testemunha de um fato é a fonte de prova, enquanto suas declarações em juízo são o meio de prova. O documento é uma fonte de prova, a sua incorporação ao processo é o meio de prova" (p. 2003). Os *meios* de prova se referem, portanto, às diferentes maneiras segundo as quais as partes processuais podem introduzir, ao processo, os conhecimentos determinados e necessários, certos ou prováveis, sobre as proposições sustentadas (Maier, 2011).

Ao distinguir *meios* de prova de *elementos* de prova, Marques, citando Pontes de Miranda, aponta que "meios de prova são as fontes probantes, os meios pelos quais o juiz recebe os elementos ou motivos de prova: os documentos, as testemunhas, os depoimentos das partes. Elementos ou motivos de prova são os informes sobre fatos ou julgamentos sobre eles, que derivam do emprego daqueles meios" (Miranda, 1947 *apud* Marques, 2000, p. 336).

Distinguem-se, ainda, os *meios* de prova dos *meios de investigação*, *meios de pesquisa* ou *meios de obtenção* de prova. Estes são os procedimentos ou atividades, empregados geralmente em fase pré e extraprocessual[30], destinados à busca de elementos de informação em sentido amplo e *fontes* de prova, das quais se poderá extrair *elementos* de prova, quando introduzidas no processo (Soares, 2014).

De acordo com a lição de Gomes Filho (2005), pode-se concluir que os *meios de pesquisa ou investigação* não são por si fontes de conhecimento, ou seja, não oferecem resultados probatórios diretamente utilizáveis na decisão. Servem para adquirir coisas materiais, traços ou declarações dotadas de força probatória, mediante a busca de elementos de informação em

30 Os meios de investigação não são realizados necessariamente antes e fora do processo. É possível que, no curso do processo, as partes solicitem determinada diligência investigativa como, por exemplo, a oitiva de possíveis testemunhas até então não identificadas ou, ainda, o afastamento de sigilo bancário e fiscal de alguém.

sentido amplo e fontes de prova, cujo procedimento é caracterizado comumente pela surpresa e, portanto, com nenhuma ou pouca participação do investigado.

Lopes Jr. (2016) aponta como exemplos de *meios de investigação* ou *de obtenção de prova* a delação premiada, as buscas e apreensões, as interceptações telefônicas, dentre outros, e conclui que não se tratam propriamente de provas, mas caminhos para se chegar à prova, ou seja, enquanto o *meio de prova* se presta ao convencimento direto do julgador, os *meios de obtenção de provas* somente indiretamente, e dependendo do resultado de sua realização, poderão servir à reconstrução da história dos fatos.

Adverte-se, todavia, que embora os *meios de investigação* se destinem originalmente à busca de elementos de informação e fontes de prova, podem, excepcionalmente, se dirigir diretamente à busca de elementos de prova pré-constituídos, nos casos mencionados das provas irrepetíveis, cautelares ou antecipadas, produzidas antes da instrução judicial (Soares, 2014).

Como bem pontua Gomes Filho (2005), essa diversidade terminológica da prova tem importante repercussão prática quanto às consequências das irregularidades verificadas em relação aos *meios de prova* e aos *meios de investigação*. "No primeiro caso, a consequência do vício será a *nulidade* da prova produzida (*rectius*: dos elementos de prova), enquanto no segundo tratar-se-á de prova *inadmissível* no processo, diante da violação das regras relacionadas à sua *obtenção* (art. 5º, LVI, da CRFB)" (Gomes Filho, 2005, p. 310).

2.1.2. Provas cautelares, não repetíveis e antecipadas: uma distinção necessária

Realizada a breve análise das premissas epistemológicas da palavra prova no processo penal, cumpre examinar as categorias das intituladas de *provas cautelares, não repetíveis e antecipadas*, vez que se relacionam estreitamente com o resultado de grande parte das medidas investigativas decorrentes de inovação técnica e tecnológica.

Importa ressaltar, todavia, que não temos a pretensão de realizar um estudo exaustivo do tema, mas um exame suficiente a colaborar com a compreensão da atividade probatória relacionada à fase de investigação criminal.

Essas categorias de prova estão previstas no artigo 155 do CPP brasileiro, positivadas após as alterações promovidas pela Lei 11.690 de 2008 que, dentre outros escopos, buscou melhorar a compreensão do princípio do livre convencimento motivado na avaliação

probatória judicial, em concordância com os princípios do contraditório e do devido processo legal[31].

A redação atual do referido dispositivo legal dispõe expressamente que "o juiz formará sua convicção pela livre apreciação da prova produzida em contraditório judicial, não podendo fundamentar sua decisão exclusivamente nos elementos informativos colhidos na investigação, ressalvadas as provas cautelares, não repetíveis e antecipadas" (Brasil, 1941).

Em que pese o seu intuito original de aclarar a compreensão dos temas relacionados com a prova, a sua valoração e os princípios correlatos, essa inovação legislativa acabou por suscitar importantes dúvidas, notadamente no âmbito doutrinário, quanto ao conteúdo das espécies excepcionais de provas cautelares, não repetíveis e antecipadas.

Não houve uma atribuição legal dos significados dessas categorias inovadoras, deixando-se esse papel à doutrina que, por sua vez, demonstra-se bastante hesitante na constituição desses novos conceitos.

Denota-se essa hesitação doutrinária nas palavras de Gomes Filho (2008), então integrante da reportada comissão de reforma processual, que, em obra publicada logo após a positivação da inovação legislativa, chegou a afirmar que "a distinção [entre provas *cautelares* e *antecipadas*] não tem importância prática, pois o que o procedimento cautelar propicia é justamente a antecipação da formação da prova" e conclui que "a medida acautelatória é o instrumento para a antecipação da produção da prova" (Gomes Filho, 2008, p. 253).

Antes de prosseguirmos na busca da definição dos conteúdos dessas categorias de prova aqui em discussão e as suas distinções, revela-se necessário um breve parêntese sobre a vinculação do conteúdo da prova à observância do contraditório.

Se há uma certa hesitação na doutrina quanto ao conteúdo e distinção das provas cautelares, não repetíveis e antecipadas, o mesmo não pode ser dito quanto à exigibilidade da presença do contraditório na formação da prova penal. Ainda que, para alguns se admita determinada flexibilização do seu exercício, o contraditório não é visto apenas como uma característica essencial do processo, mas verdadeira *condição de existência* da prova penal (Gomes Filho, 2008).

Nesse sentido, prova (no sentido de *elemento de prova*) só pode ser assim considerada se produzida em contraditório judicial, distinguindo-se dos *elementos informativos em sentido estrito* provenientes dos atos de investigação, colhidos sem contraditório judicial. Estes, para serem

31 Nesse sentido importa citar a redação anterior do art. 157, o qual continha a positivação original do princípio do livre convencimento motivado: "Art. 157 do CPP – "O juiz formará sua convicção pela livre apreciação da prova".

utilizados no resultado da prova, devem ser corroborados com os elementos de prova produzidos em contraditório, não podendo o livre convencimento motivado basear-se exclusivamente em tais elementos de informação[32].

Feita essa breve observação, voltemos à busca do conteúdo e distinção das categorias especiais de provas às quais se refere a parte final do artigo 155 do Código de Processo Penal brasileiro. Para Soares (2014), trata-se de "três espécies de excepcionais de elemento probatório, cuja produção é cautelar, irrepetível ou legitimamente antecipada", as quais constituem o que se denomina de prova pré-constituída, ou seja, "elementos de prova colhidos antes da instauração de processo penal e trazidos aos autos sem o adequado contraditório em sua produção, cuja valoração judicial a lei excepcionalmente admite" (Soares, 2014, p.45).

Sustenta Soares (2014) que a parte final do *caput* do artigo 155 do CPP prevê uma "diminuição da abrangência do princípio do contraditório" exclusivamente quanto à produção dessas provas pré-constituídas, tratando-se de limitações ao direito constitucional ao contraditório judicial, cuja admissibilidade deve ser aferida em cada caso concreto à luz da proporcionalidade (Soares, 2014, p. 48).

Nesse sentido, Gomes Filho (2008), ao discorrer sobre as provas cautelares e antecipadas, afirma que "o perigo de desaparecimento ou de comprometimento da fonte de prova, pelo decurso do tempo, autoriza, excepcionalmente, uma restrição inicial ao pleno exercício do contraditório". Não significa, todavia, a aniquilação do princípio (que seria inconstitucional), mas a postergação do momento de seu exercício, o que se denomina de *contraditório diferido* (p. 253).

Por sua vez, Mendes (2020) defende que "o fator que diferencia estas categorias não é a relativização do exercício do contraditório, mas tão somente o momento no qual deverá ser exercido, cujo critério é a possibilidade de preservação da (fonte de) prova ou a produção imediata ou antecipada de *elementos de prova*" (p. 129).

As chamadas provas antecipadas, como se denota do próprio nome, são aquelas produzidas antes do momento destinado à instrução processual (Capez, 2012, p. 467). A formação do elemento de prova (que pode ser utilizado no resultado da prova) se dá de forma antecipada, ainda na fase investigativa, ou seja, o elemento que normalmente seria produzido

32 Neste sentido, veja-se o caput do art. 155 do CPP: "O juiz formará sua convicção pela livre apreciação da prova produzida em contraditório judicial, não podendo fundamentar sua decisão exclusivamente nos elementos informativos colhidos na investigação, ressalvadas as provas cautelares, não repetíveis e antecipadas".

como mero ato de investigação passa a ter *status* de ato de prova (valorável na sentença), por ter sido legitimamente antecipado (Lopes Jr., 2016).

A prova antecipada é, portanto, o produto da antecipação da produção probatória que deve ser justificada pela "relevância e imprescindibilidade do seu conteúdo para a sentença" e pela "impossibilidade de sua repetição na fase processual, amparado por indícios razoáveis do provável perecimento da prova" (Lopes Jr., 2016. p. 228).

Esses requisitos traduzem a urgência e o risco de perda irreparável de alguns dos elementos recolhidos na investigação preliminar que legitimam a formação das provas antecipadas. Nesse caso, não se afasta o contraditório. Ao contrário, o contraditório se efetiva de forma plena e antecipada, com a garantia de participação das partes interessadas e do magistrado.

Distintamente da categoria acima referida, a prova penal *irrepetível* ou *não repetível* (ou o elemento probatório penal de produção *irrepetível*)[33] "é aquela que, uma vez produzida, não tem como ser novamente coletada ou produzida, em virtude do desaparecimento, destruição ou perecimento da fonte probatória" (Lima, 2015, p. 573). A sua principal característica é a emergência temporal de sua obtenção em razão da irrecuperabilidade da fonte de prova, o que exige a sua realização no momento do seu descobrimento.

Um dos exemplos mais citados na doutrina de prova *irrepetível* é o exame de corpo de delito nos crimes de lesão corporal e/ou contra a liberdade sexual, dentre outros, cuja produção deve ser realizada imediatamente após a prática do delito, sob pena de desaparecimento dos vestígios deixados pela infração penal, não podendo ser "repetidos" na instrução processual.

Diferente do que ocorre com a prova antecipada, em cuja formação há a antecipação do contraditório real e pleno, na constituição da prova irrepetível o contraditório é diferido ao momento processual adequado à formação dos elementos de prova.

No que tange à categoria das provas cautelares, para a busca de sua definição faz-se necessário perceber do que se tratam as medidas cautelares penais. Sobre o assunto, Pitombo (1997) adverte que a comparação e aplicabilidade do conceito de cautelares do processo civil no processo penal "mostra-se limitada, em razão da dificuldade e quase impossibilidade de transposição dos conceitos civilistas para o processo penal" (p. 198).

Razão assiste à autora retro citada. Não se busca, com as medidas cautelares no processo penal, assegurar o provimento final, visto que a culpa não se presume, admitindo-se

33 Designação empregada por Soares (2014).

a absolvição como provimento final. Daí que se deve buscar uma sistematização própria das medidas cautelares no processo penal, adequada aos seus particulares fundamentos existenciais.

Nesse sentido, Mendes (2020), citando Pujadas Tortosa, considera mais acertada a definição segundo a qual as "medidas cautelares penais servem para a proteção do processo sobre vários perigos de frustração, ou seja, protege-se o processo do risco da frustração processual". Assim, no âmbito da atividade probatória, "uma tutela cautelar probatória presta-se a evitar a ocultação, destruição ou manipulação de *fontes* e *meios* de prova" (Mendes, 2020, p. 133).

A partir dessa definição, Mendes (2020) defende que a prova cautelar na verdade não se trata de um elemento de prova, mas de *fonte* de prova recolhida a partir da execução de uma medida cautelar probatória. Essa *fonte* de prova permanece conservada até a sua inclusão no processo penal por um *meio* de prova, para só então constituir-se a prova penal, sob o contraditório das partes.

Em sentido diverso, Soares (2014) afirma que:

> [...] a chamada prova penal *cautelarmente* produzida (ou simplesmente prova penal cautelar) deve ser entendida como o elemento de prova pré-constituído cuja produção seria, em princípio, repetível no futuro, mas, diante do *perigo na demora* e da *aparente pertinência e relevância de tal produção*, o ordenamento jurídico-penal autoriza a imediata exploração da respectiva fonte (p. 55).

De fato, seja na qualidade de fonte de prova ou de elemento de prova, as provas cautelares, assim como as provas irrepetíveis, são submetidas ao contraditório diferido. Ao contrário, nas provas antecipadas o contraditório é realizado de forma antecipada no momento de sua produção. Todas essas categorias, pela dicção do artigo 155 do CPP brasileiro, podem ser valoradas para a definição da culpa penal.

2.2. Prova penal digital: uma análise do conceito, das características, da aquisição e da preservação

Com o advento da Era da Tecnologia ou Era da Internet, as relações sociais rompem as barreiras físicas e geográficas tal como conhecemos, fazendo emergir um ambiente virtual complexo de interação e difusão, armazenamento, processamento e transmissão de dados que exigem a adaptação das ciências jurídicas a essa nova conjuntura social.

Essa nova realidade, ao tempo em que proporciona a difusão do saber e do conhecimento humano, também propicia a proliferação da prática de crimes de difícil elucidação. Esse cenário atual impõe reflexos significativos nos métodos de investigação criminal atrelados às novas tecnologias e consequentemente à aquisição e preservação das provas penais.

Surge, então, nesse contexto de complexidade oriunda dos avanços tecnológicos em constante evolução, a noção de prova penal digital, cuja compreensão e distinção se revela imprescindível para o estudo do uso de novas tecnologias nos métodos de investigação criminal, enquanto meios técnicos de recolha desse tipo de prova.

Não há um conceito legal de prova digital no âmbito do Direito Processual Penal brasileiro, o que se demonstra compreensível e coerente, uma vez que a elaboração de uma definição legal tenderia a oscilar entre a excessiva abstração e a curta duração conceitual, ante o acelerado progresso da tecnologia. Não obstante, "a tentativa de formulação de uma definição que seja suficientemente precisa e, simultaneamente, flexível para ser duradoura", revela-se de extrema importância "porque é cada vez mais um elemento incontornável de qualquer processo criminal" (Ramalho, 2017, pp. 98-99).

Na doutrina, costuma-se encontrar a utilização dos termos prova digital e prova eletrônica como sinônimos. No entanto, como adverte Ramalho (2017), é preciso fazer a devida distinção porque pode implicar diferentes procedimentos probatórios e processuais a cada forma de prova.

O termo "prova eletrônica" deve ser entendido como generativo que compreende tanto as provas em formato digital como as provas em formato analógico, a exemplo das gravações em áudio e vídeo ou fotografias em rolo fotográfico que, apesar de digitalizáveis, não têm origem em arquitetura digital, mas que podem ser manipuladas, armazenadas ou transmitidas através de qualquer dispositivo informático (Ramalho, 2017).

Segundo Ramalho (2017), o termo digital pode abranger as tecnologias e os sistemas de comunicação não eletrônicos, mas está associado de maneira inseparável à lógica binária e, mais amplamente, à informática. Daí considera acertada a qualificação de prova digital como uma prova *eletrônico-digital* por se tratar de uma subespécie da prova eletrônica em formato digital.

De acordo com Pinheiro (2013, p. 216), "[...] a evidência digital é toda informação ou assunto de criação, intervenção humana ou não, que pode ser extraído de um compilado ou depositário eletrônico".

Por sua vez, Vaz (2012, p. 64) define prova digital como "os dados em forma digital (no sistema binário) constantes de um suporte eletrônico ou transmitidos em rede de comunicação, os quais contêm a representação de fatos ou ideias". Conclui a autora que a menção à prova digital designa, na verdade, *fonte de prova*, ou seja, o objeto a partir do qual se podem extrair informações relevantes à comprovação da afirmação sobre os fatos de interesse à persecução penal.

Para Ortuño Navalón (2014), a prova digital é a informação armazenada ou transmitida na forma binária que pode ser considerada em tribunal. Ela pode ser encontrada no disco rígido de um computador, no celular, no CD e no cartão *flash* de uma câmera digital, entre outros locais. A prova digital é comumente associada ao crime eletrônico, como pornografia infantil ou fraude de cartão de crédito. No entanto, as provas digitais agora são utilizadas para processar todos os tipos de crimes e não somente os crimes eletrônicos. A título de exemplificação, os arquivos de *e-mail* ou celular de suspeitos podem conter evidências críticas sobre sua intenção, seu paradeiro no momento do crime e seu relacionamento com outros suspeitos.

A prova digital é definida por Rodrigues (2009, p. 536) como:

> Qualquer fluxo informacional ou comunicacional digital, que, estaticamente, se encontre armazenado, tratado ou processado, ou, pelo contrário, dinamicamente, seja transmitido, veiculado ou não por meio das redes informáticas ou de serviços e comunicações electrónicas, quer ao nível de um ciclo informacional e comunicacional fechado ou aberto, privado ou público.

De forma mais simplificada, o *Scientific Working Groupon Digital Evidence* - SWGDE define prova digital (*digital evidence*) como qualquer informação com valor probatório que se encontre armazenada ou é transmitida sob a forma binária[34].

Assim, prova digital pode ser obtida quando ainda se encontra armazenada em um dispositivo eletrônico, em poder do investigado ou de terceiros, ou quando esteja sendo transmitido por meio telemático. No primeiro caso, os meios de investigação ou de obtenção de prova se dirigem aos suportes físicos (computador, *tablet*, etc.) e aos dados estáticos e, no segundo, há a captação das informações em movimento (Vaz, 2012).

Vale destacar que a prova digital não se confunde com a mera prestação de informações em formato digital, a exemplo dos dados obtidos de entidades públicas ou privadas, por meio de requisição, apenas por serem registradas em meios digitais. Por outro

34 *Scientific Working Group on Digital Evidence* (SWGDE). Disponível em: https://www.swgde.org/.

lado, no caso de captação de arquivos que se encontrem armazenados em servidores das mesmas instituições, por meio de busca e apreensão, as informações obtidas estarão na categoria de provas digitais (Vaz, 2012).

Variadas são as possibilidades de fontes de provas digitais nos dias de hoje em razão do uso cada vez mais crescente de dispositivos tecnológicos e tecnologia de comunicação eletrônica, a exemplo de *smartphones, tablets*, computadores, aplicativos de redes sociais, dentre outros, o que torna cada vez mais comum e importante a utilização das provas digitais na investigação criminal e consequentemente no processo penal.

Os diferentes meios utilizados para a recolha das provas digitais distinguem-se dos métodos tradicionais de obtenção de prova em razão da própria natureza e particularidade de suas fontes. As provas digitais apresentam, assim, características próprias que reivindicam conhecimentos técnicos para a sua recolha e cuidados específicos para o seu registro, preservação e apresentação em juízo, demonstrando-se muitas vezes inadequadas as normas processuais penais tradicionais a essa realidade digital (Ramalho, 2017).

Muitas são as características apontadas na doutrina da prova digital[35]. Umas das principais características distintivas da prova digital é a sua *imaterialidade* ou *invisibilidade*, isto é, os dados digitais existem independentemente do suporte físico no qual é incorporado, tratando-se de impulsos elétricos que podem ser transferidos a outros dispositivos eletrônicos sem perder a sua essência. Assim, embora precise de um suporte transportador, a prova digital a este não se resume (Ramalho, 2017).

A característica *imaterial* da prova digital, ao tempo em que permite grande acumulação de dados sem ocupação de espaço físico considerável, ao contrário dos documentos tradicionais, a torna *frágil* e *volátil*. Frágil porque facilmente suscetível à contaminação, podendo sofrer alterações de suas propriedades ou mesmo ser eliminada intencionalmente ou por mero descuido, exigindo-se, assim, o uso de determinadas técnicas e conhecimentos científicos para sua recolha, sob pena de comprometimento de sua força probatória em juízo (Rodrigues, 2009).

Por sua vez, indissociável da *fragilidade* aponta-se a *volatilidade* também como característica da prova digital. Isso porque pode desaparecer ou dissipar-se facilmente em razão de eventos simples como a falta de carga da bateria do equipamento eletrônico ou a gravação de informações novas no lugar dos arquivos antigos ou, até mesmo, simplesmente por se tratar de arquivo temporário (Ramalho, 2017).

35 Para aprofundamento do tema, conferir: Ziccardi (2007), Rodrigues (2011) e Ramalho (2017).

Ao lado das características acima descritas, Vaz (2012, pp. 66-70) acrescenta a *suscetibilidade de clonagem*, isto é, admite a efetivação de infinitas cópias idênticas e sua transferência a outros dispositivos, sem que se possa falar em um exemplar original, e a *necessidade de intermediação*, ou seja, precisa de um equipamento para ser acessado de modo que a informação seja compreensível pelo ser humano.

Complementarmente, Bueno de Mata (2014) cita que ao contrário dos meios tradicionais de prova, a prova digital tem as seguintes características: é intangível, o que significa que não pode ser apreciada diretamente pelos sentidos, mas por complexos processos computacionais; é replicável, ou seja, encontra-se em formato digital, podendo ser copiada ou replicada quantas vezes for necessário. Isso levanta o problema da distinção da originalidade, que é declarada trivial para sua aquisição de força probatória se puder ser indubitavelmente provado que o original e a cópia são exatos, *bit* a *bit*. É também uma prova passível de ser facilmente destruída, não sendo necessária a destruição do suporte digital que a contém. E, por fim, trata-se de uma prova parcial. Isto porque a prova digital às vezes é formada por múltiplos arquivos de computador, espalhados por diferentes mídias e locais digitais, como um sistema de informações na nuvem, o que adiciona ainda mais complexidade na sua apreensão e preservação.

Adverte-se, todavia, que, embora *volátil*, não se pode assentar que toda prova digital tenha escassa durabilidade, uma vez que os dados informáticos são armazenados em dispositivos eletrônicos muitas vezes submetidos a técnicas especiais de preservação ou, quando transmitidos são fixados em suportes eletrônicos capazes de torná-los fontes permanentes (Vaz, 2012).

Sabe-se que cada vez mais a evolução tecnológica faz emergir a necessidade de utilização de provas digitais no processo penal. No entanto, essa mudança de paradigma não tem sido bem acompanhada pela necessária adequação legislativa e enquadramento doutrinário. Há dúvidas sobre sua aquisição, características e armazenamento.

Referente à aquisição, sabe-se para que as provas digitais sejam obtidas, duas operações devem ser realizadas. A primeira consiste no despejo ou clonagem de dados, que consiste em fazer uma cópia espelhada, bit a bit, da informação digital original. Tão logo os dados forem despejados, é obtida a assinatura *hash* dos arquivos eletrônicos apreendidos. A referida assinatura *hash* é uma função baseada num algoritmo de resumo dos *bits* que constituem o ficheiro, cuja aplicação prática é afirmar que o referido ficheiro não foi posteriormente alterado. Ao alterar um único *bit* do arquivo digital, a assinatura *hash* muda. Assim, a integridade do conteúdo é obtida comparando as assinaturas *hash* obtidas da informação

capturada e da formação original, ocasião em que ambas devem ser as mesmas (Rodríguez Acosta, 2018).

As características específicas da prova digital e do próprio ambiente virtual, cercado de sofisticados recursos tecnológicos e de riscos de interferências externas, impõem a necessidade de estabelecimento e aplicação de procedimentos próprios de aquisição e preservação que possam garantir a sua integridade e autenticidade, a fim de possibilitar a sua correta valoração judicial. Nesse sentido, aponta Vaz (2012, p. 80) que:

> [...] a obtenção e a produção da prova digital devem ser orientadas pelas finalidades de preservação, autenticidade ou genuinidade, durabilidade e acessibilidade dos dados digitais, assim como pela possibilidade de análise conjunta das informações coletadas. Esses procedimentos devem também ser pautados pelas garantias do devido processo legal, respeitando-se os direitos fundamentais, de modo a se obter prova válida e legítima.
> Para isso, são imprescindíveis normas que prescrevam os procedimentos adequados para a aquisição, conservação, análise e produção dos dados digitais, complementando as regras existentes no ordenamento atual.

Assim, cumulativamente aos princípios gerais referentes à prova no processo penal, a obtenção da prova digital implica o reconhecimento e aplicação de princípios específicos respeitantes às características especiais desse tipo de prova. Adotando-se a lição de Rodrigues (2009, p. 726 e segs.), destacam-se os princípios *da não alteração da prova eletrônico-digital*; *da especialização ou qualificação do pessoal adstrito à investigação forense digital*; e *da obrigatoriedade de documentação de todas as fases de acesso, recolha, armazenamento, transferência, preservação ou apresentação da prova eletrônico-digital*.

Pelo *princípio da não alteração da prova eletrônico-digital*, durante o decurso da investigação, deverá ser exigido do investigador forense digital todo o esforço no sentido de zelar para que a sua atuação não contamine os dados obtidos, desde o momento de recolha até a sua ulterior apresentação, adotando-se medidas que garantam a integralidade e autenticidade da prova digital livre de elementos estranhos ao sistema ou rede informáticos sob investigação.

Não menos importante é o *princípio especialização ou qualificação do pessoal adstrito à investigação forense digital*, segundo o qual o acesso, recolha, conservação e análise da prova digital devem estar confiados à esfera de competência de pessoal especializado, dotado de conhecimentos técnico-científicos, para garantia do correto e eficiente manuseio da prova de modo a impedir o seu comprometimento e consequente inadmissibilidade de avaliação judicial.

Especialmente relevante, tem-se, ainda, o *princípio da documentação de todas as fases de acesso, recolha, armazenamento, transferência, preservação ou apresentação da prova eletrônico-digital*, cujo escopo é preservar uma cadeia de custódia da prova digital, através da descrição detalhada e cronológica de todas as fases de identificação e obtenção das fontes de prova, de modo a demonstrar a confiabilidade da prova e possibilitar o exercício do contraditório.

Ainda quanto à temática da aquisição da prova digital, a pluralidade das mais variadas ferramentas tecnológicas que se encontram no quotidiano da atividade humana da atual sociedade da informação, através dos quais circulam uma imensidão de dados, denota a abundante potencialidade de se identificar fontes de provas digitais passíveis de utilização na investigação e no processo criminal. Consequentemente, a obtenção de potenciais provas imersas nesse mundo digital sujeita-se a diferentes formas de aquisição.

Nesse sentido, Mendes (2020), citando Delgado Martin destaca que a multiplicidade de instrumentos e elementos tecnológicos determinam uma certa heterogeneidade nas formas de aquisição da fonte de prova. Uma dessas possibilidades é o alcance do conteúdo contido no sistema a partir da apreensão do equipamento ou dispositivo eletrônico. Outra forma de obtenção de provas digitais se dá através da busca remota (*remote search*), sem a necessidade de apreensão do suporte físico no qual a informação encontra-se armazenada ou foi transmitida (Delgado Martin, 2013 *apud* Mendes, 2020).

A informação digital é armazenada em formato binário, por meio de um sistema que transforma impulsos elétricos ou fotossensíveis e, por meio de cuja decomposição e recomposição computacional registrada em formato eletrônico, gera e armazena as informações. Da mesma forma, é necessário diferenciar entre o que é armazenado e o que é externalizado, que é o resultado da transformação da informação digital armazenada, por meio de processos informatizados, em um formato inteligível pelo homem (Carmelo LLopis, 2016). Um exemplo do que é afirmado é a representação escrita de um *e-mail*, em comparação com o arquivo de computador criptografado que constitui o próprio *e-mail*. É essencial ter clareza sobre esse conceito.

Essas informações em formato digital são produzidas, armazenadas ou transmitidas por meio de dispositivos ou instrumentos digitais. Dessa forma, pode-se definir o dispositivo digital como qualquer sistema ou dispositivo de computador, incluindo sistemas de armazenamento e transmissão de informações por meio digital (Nether, 2018).

A investigação informática pode ser dividida, assim, em duas grandes categorias: a investigação *off-line* ou estática, dependente da apreensão do suporte eletrônico; e a investigação *online* ou remota, cuja principal característica é a possibilidade de obtenção dos

dados sem a necessidade de apreensão de seu respectivo suporte físico (Delgado Martin, 2013 *apud* Mendes, 2020, p. 141).

Não obstante à distinção referida, é possível ainda distinguir duas grandes maneiras de se alcançar as provas digitais. A primeira seria a não intrusiva, quando obtida por permissão voluntária do detentor do dado digital ou por ser publicamente acessível. A segunda é a obtenção intrusiva, ou seja, operada coercitivamente sem a permissão de quem tem a disponibilidade ou controle, seja mediante a apreensão física do equipamento eletrônico ou por meios ocultos de acesso remoto aos dados digitais (Silva, 2019).

Com efeito, é possível que o acesso aos dados digitais se dê por mera liberalidade de quem pode deles dispor ou porque encontram-se acessíveis publicamente, havendo, nesse caso, renúncia à eventual natureza íntima da informação ou comunicação. Assim, considera-se legítima a obtenção de fotografias, mensagens, vídeos e informações pessoais publicados nas redes sociais, sem prévia autorização judicial (Silva, 2019).

Por outro lado, a pesquisa informática coercitivamente encetada, isto é, a obtenção da prova digital de maneira intrusiva, seja pela apreensão do suporte eletrônico (investigação *off-line*), seja por meio de métodos ocultos de busca remota (investigação *online*), depende de prévia autorização e posterior validação da autoridade judiciária competente para sua apreensão.

Independentemente da diversidade das formas de se alcançar os dados digitais, hoje em abundância nas mais variadas plataformas eletrônicas, esses só poderão ser valorados em processo criminal se for possível comprovar a sua integridade, autenticidade e confiabilidade, devendo, por isso, atender fielmente os princípios destacados e, em especial, a cadeia de custódia da prova digital.

O tema "cadeia de custódia", apesar da sua importância fundamental em relação à teoria da prova penal, tem sido pouco explorado na doutrina brasileira e só recentemente se encontra a sua abordagem no âmbito jurisprudencial, o que se justifica pela histórica ausência de sua previsão expressa no âmbito legal (Souza, 2020).

A cadeia de custódia consiste em um conjunto de procedimentos e protocolos utilizados com o objetivo de preservar e documentar cronologicamente a história da descoberta e conservação das provas e dos elementos informativos, ou, na dicção do novo art.158-A do CPP, vem ele a ser "[...]o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte" (Souza, 2020, p. 194).

Assim, a admissão da prova digital não constitui algo arbitrário, mas responde a um regime jurídico que exige, na ausência de regulamentação legal adequada, um esforço para aproximar os conceitos processuais à realidade tecnológica usual na sociedade de informações, em muitos aspectos, ainda em construção.

Quando é realizada a análise forense, após a apreensão da prova, é necessário preservá-la. É extremamente importante que seja mantida sua integridade, com documentos e evidências para apoiar sua confiabilidade.

Assim, a preservação da cadeia de custódia da prova tem por objetivo garantir que o juízo, bem como as partes, possam verificar a licitude e suficiência de determinada prova vinculada em especial à demonstração da materialidade, bem como sua adequação para atender a sua finalidade probatória, decorrendo essa necessidade de preservação da prova, da garantia da presunção de inocência e do objetivo de reconstrução da verdade possível através do devido processo penal, que inclui a coleta e preservação dos vestígios, para que não sejam adulterados.

O acusado é presumidamente inocente até sua condenação definitiva, a qual está vinculada, diretamente, à comprovação, acima de qualquer dúvida razoável, de que foi ele o autor da infração e de que esta está demonstrada em todos os seus aspectos e em especial em relação à autoria e à materialidade.

Impõe-se, então, por força da garantia da presunção de inocência e da exigência do devido processo legal, que sejam assegurados os meios necessários à conservação da prova produzida pela acusação, pela defesa e, em caráter excepcional e complementar, pelo juízo. E para que tal verificação seja fidedigna, é indispensável a preservação ou conservação (custódia) de todos os elos da cadeia probatória, de forma que seja possível percorrer todo caminho dos vestígios, desde a sua coleta até a análise pelos peritos, e confirmar a origem lícita, bem como que não houve substituição, contaminação ou adulteração daqueles elementos de convicção colhidos no decorrer da investigação e do processo penal (Souza, 2020).

Segundo Rodríguez Acosta (2018), para proteger a prova digital e ser possível atestar que ela não foi modificada é empregado o algoritmo *hash*, que é um algoritmo de verificação de integridade e que gera um valor/chave para alguns dados/arquivo. Desta forma, se as provas tiverem sofrido qualquer alteração no decorrer da investigação, este valor deixará de ser o mesmo.

Acerca dessa temática, a Força Tarefa de Engenharia da Internet (*Internet Engineering Task Force* — IETF) elaborou o memorando "RFC 3227 - Diretrizes para Coleta e

Arquivamento de Evidências"[36], no qual elenca uma diversidade de princípios e condutas que precisam ser adotadas na apuração das evidências digitais, com o objetivo de fornecer à comunidade internacional diretrizes para a correta recolha e preservação das provas digitais.

O documento (RFC 3227) preceitua que a evidência digital deve ser *admissível* (em conformidade com as regras legais), *autêntica* (passível de ser demonstrada por todas as etapas de aquisição e guarda), *completa* (deve contar toda a história e não apenas um ponto de vista particular), *confiável* (deve haver a correta identificação, descrição e individualização dos equipamentos técnicos utilizados na recolha e armazenamento) e *crível* ou *acreditável* (compreensível tanto pelas partes quanto pelos julgadores).

Exige-se, portanto, o atendimento de rigorosos critérios para a validade da prova digital em juízo, o que torna a cadeia de custódia componente de fundamental importância nesse procedimento de recolha e armazenamento até a sua inserção no processo judicial (Casey, 2011).

A evidência digital desempenha um papel importante na investigação do crime cibernético, pois é usada para vincular indivíduos a atividades criminosas. Portanto, é de extrema importância para garantir a integridade, autenticidade e capacidade de auditoria das evidências digitais à medida que se movem ao longo de diferentes níveis de hierarquia na cadeia de custódia durante a investigação do crime cibernético (Borri & Ávila, 2019).

A tecnologia moderna é mais avançada em termos de portabilidade e potência. Uma grande quantidade de informações é gerada por bilhões de dispositivos conectados à internet que precisam ser armazenados e acessados, o que representa grandes desafios na manutenção da integridade e autenticidade das provas digitais para sua admissibilidade no tribunal. O manuseio de evidências digitais apresenta desafios únicos porque são latentes, voláteis, frágeis, podem cruzar as fronteiras jurisdicionais de forma rápida e fácil e, em muitos casos, também dependem do tempo/máquina (Prado, 2019). Garantir, assim, a autenticidade e legalidade dos processos e procedimentos de recolha e transferência de provas numa sociedade digital é um verdadeiro desafio.

A cadeia de custódia na perícia digital também pode ser chamada de elo forense, trilha de papel ou documentação cronológica de evidências eletrônicas. Indica a coleta, sequência de controle, transferência e análise. Ele também documenta cada pessoa que manipulou as evidências, a data/hora em que foram coletadas ou transferidas e a finalidade da transferência. É importante manter a cadeia de custódia para preservar a integridade das provas e evitar sua

36 RFC 3227 - Diretrizes para Coleta e Arquivamento de Evidências. (2018). Trad. Tiago Souza. Disponível em: https://www.academiadeforensedigital.com.br/rfc-3227-melhores-praticas-referen cias/.

contaminação, o que pode alterar o estado das provas. Se não forem preservadas, as provas apresentadas em tribunal podem ser contestadas e julgadas inadmissíveis. Nesse sentido, Casey (2011, p. 60) destaca que:

> A cadeia de custódia e a documentação de integridade são importantes para demonstrar a autenticidade das evidências digitais. A cadeia de custódia adequada demonstra que as evidências digitais foram adquiridas de um sistema e / ou local específico e que foram continuamente controladas desde que foram coletadas. Portanto, a documentação adequada da cadeia de custódia permite que o tribunal vincule as evidências digitais ao crime. A documentação incompleta pode resultar em confusão sobre onde a evidência digital foi obtida e pode levantar dúvidas sobre a confiabilidade da evidência digital (Livre tradução).

Utilizando-se mais uma vez das Diretrizes para Coleta e Arquivamento de Evidências - RFC 3227, a cadeia de custódia deverá ser claramente documentada e, assim, ser capaz de descrever onde, quando e por quem a prova foi descoberta e coletada, bem como onde, quando e por quem a prova foi tratada e examinada[37].

Além de constituir elemento essencial à garantia da autenticidade e confiabilidade da prova digital, a cadeia de custódia adequada permite ao investigado/acusado o conhecimento de todo o procedimento de constituição dessa prova e o acesso a suas fontes, garantindo-se, assim, o pleno exercício do contraditório.

Segundo a lição de Prado (2019, p. 72):

> O conhecimento das fontes de prova pela defesa é fundamental, porque a experiência histórica que precede a expansão da estrutura trifásica de procedimento penal, adequada ao modelo acusatório, contabiliza a supressão de elementos informativos como estratégia das agências de repressão que fundam as suas investigações em práticas ilícitas.

Ademais, cumpre sublinhar a tendência generalista de se atribuir exagerada presunção de fidedignidade aos sistemas informáticos e, consequentemente, à prova digital, o que ressalta ainda mais a importância da preservação da cadeia de custódia, transformando-a em um verdadeiro requisito de admissibilidade desse tipo de prova no processo penal.

Nesse sentido, destaca Ramalho (2017, p. 261) que:

> [...] é comum atribuir-se aos sistemas informáticos e à prova digital uma tácita presunção de fidedignidade, por vezes em prejuízo da presunção de inocência. Tal

37 RFC 3227 - Diretrizes para Coleta e Arquivamento de Evidências. (2018). Trad. Tiago Souza. Disponível em: https://www.academiadeforensedigital.com.br/rfc-3227-melhores-praticas-referencias/.

> facto deve-se, em parte a uma certa confiança injustificada em sistemas informáticos, à qual subjaz a ideia de que as máquinas tendem a não cometer erros.

Ainda segundo a lição de Ramalho (2017), embora esteja naturalmente excluído o contraditório na obtenção da prova digital pelos métodos ocultos na fase de investigação, deverá haver a adequada preservação da cadeia de custódia de modo a garantir o seu pleno exercício, não bastando a mera possibilidade formal do exercício do contraditório. É necessário que as partes possam controlar a prova introduzida ao processo penal, aferindo a sua pertinência, fidedignidade e aptidão para demonstração das assertivas fáticas apresentadas em juízo.

Não obstante à imprescindibilidade da cadeia de custódia da prova digital, não há consenso doutrinário acerca da metodologia e das etapas a serem seguidas no processo de recolha, preservação e apresentação dessa prova em juízo. Todavia, impõe-se a adoção de um modelo de procedimento minimamente adequado que contemple as etapas de recolha, autenticação, exame, análise e relatório da prova digital (Mendes, 2020).

Esse modelo quadripartido das etapas a serem seguidas numa investigação em ambiente digital é proposto pelo *Nacional Institute for Standards and Technology* - NIST (Kent, 2006). Embora reconheça a possibilidade de serem concebidas outras etapas, o modelo proposto contempla o essencial a ser seguido para a correta preservação da cadeia de custódia da prova digital (Ramalho, 2017).

Seguindo o modelo sugerido, a primeira fase do processo forense de produção da prova digital é a da recolha, durante a qual são identificadas as fontes potenciais de dados relevantes ao que se pretende investigar. Exige-se, para tanto, conhecimento técnico-científico para garantia da correta identificação e manuseio dessas fontes. Também, deve haver pleno conhecimento das regras legais para o acesso às fontes, notadamente quando se exigir a obtenção intrusiva, de maneira a não invalidar a prova digital. Após a identificação das fontes, ainda na etapa de recolha, o investigador deverá rotular e registrar os dados obtidos em cumprimento às diretrizes e procedimentos que possibilitem garantir a integridade da prova.

Na cadeia de custódia, os nomes, títulos e informações de contato dos indivíduos que identificaram, coletaram e adquiriram as evidências devem ser documentados, bem como de quaisquer outros indivíduos para os quais as evidências foram transferidas, detalhes sobre as evidências que foram transferidas, a hora e a data da transferência e a finalidade da transferência (Prado, 2019).

Logo após a recolha e registro das fontes e dados identificados, passa-se à segunda etapa, denominada de exame. Esta fase corresponde ao processamento forense dos dados

recolhidos, na qual o examinador recorrerá a ferramentas e técnicas de pesquisa adequadas aos tipos de dados que foram coletados, para identificar e extrair as informações relevantes, protegendo sempre a sua integridade. Essa fase também pode envolver ignorar ou atenuar recursos do sistema operacional ou do aplicativo que obscurecem dados e código, como compressão de dados, criptografia e mecanismos de controle de acesso.

Recolhidos, registrados e examinados os dados obtidos, destacando os de maior relevância probatória, passa-se à fase de análise crítica de todo o material colhido para obter informações úteis que abordem as questões que foram o ímpeto para a realização da coleta e do exame. O processo de análise implica a interpretação dos elementos objetivos colhidos e o seu cotejo com a as hipóteses levantadas na investigação e, quando aplicável, com a proposição do próprio investigado. É nesta fase que os dados informáticos são convertidos em prova (Ramalho, 2017).

Várias formas de análises são realizadas dependendo do tipo de evidência digital buscada, como rede, sistema de arquivos, aplicativo, vídeo, imagem e análise de mídia (ou seja, análise de dados no dispositivo de armazenamento) (European Network of Forensic Science Institute, 2015).

Os arquivos são analisados para determinar sua origem e quando e onde os dados foram criados, modificados, acessados, baixados ou carregados, e a possível conexão desses arquivos em dispositivos de armazenamento para, por exemplo, armazenamento remoto, como armazenamento baseado em nuvem (Carrier, 2005). O tipo de evidência digital (por exemplo, *e-mails*, mensagens de texto, geolocalização, documentos de processamento de texto, imagens, vídeos e registros de bate-papo) procurado depende do caso do crime cibernético.

Geralmente, existem quatro tipos de análises que podem ser realizadas em computadores. São elas: análise de período de tempo; análise de propriedade e posse; aplicação e análise de arquivos; e análise de ocultação de dados. A *análise do período de tempo* busca criar uma linha do tempo ou sequência de tempo das ações usando carimbos (data e hora) que levaram a um evento ou para determinar o horário e a data em que um usuário executou alguma ação. Essa análise é realizada com vistas a atribuir um crime a um suspeito ou, pelo menos, atribuir um ato que levou a um crime a um indivíduo específico (US National Institute of Justice, 2004).

A *análise de propriedade e posse* é usada para determinar a pessoa que criou, acessou e/ou modificou arquivos em um sistema de computador (US National Institute of Justice, 2004). Por exemplo, esta análise pode revelar uma imagem de material de abuso sexual infantil (ou seja, a representação, por qualquer meio, de uma criança envolvida em atividades sexuais

explícitas reais ou simuladas ou representação das partes sexuais de uma criança para fins principalmente sexuais no dispositivo de um suspeito). Esta informação por si só não é suficiente para provar a propriedade de material de abuso sexual infantil. Mais evidências são necessárias, como o uso exclusivo do computador onde o material foi encontrado.

A *análise do aplicativo e do arquivo* é realizada para examinar os aplicativos e arquivos em um sistema de computador para determinar o conhecimento do perpetrador, a intenção e as capacidades de cometer o crime cibernético (por exemplo, o rótulo ou nome do arquivo pode indicar o conteúdo do arquivo; por exemplo, o nome do arquivo pode ser o nome da vítima do crime cibernético) (US National Institute of Justice, 2004).

A *análise de ocultação de dados* também pode ser realizada. Como o nome indica, a análise de ocultação de dados procura dados ocultos em um sistema. Os criminosos usam várias técnicas de ocultação de dados para ocultar suas atividades ilícitas e informações de identificação, como o uso de criptografia, dispositivos de proteção de senha e conteúdo específico, alteração de extensões de arquivo e ocultação de partições (Maras, 2014). Durante a fase de análise, o investigador precisa abordar as técnicas de ocultação de dados que os perpetradores poderiam ter usado para ocultar suas identidades e atividades. Os dados ocultos podem revelar conhecimento [de um crime], propriedade [do conteúdo] ou intenção [de cometer um crime] (US National Institute of Justice, 2004).

Como o US National Institute of Justice (2004) concluiu, os resultados obtidos de qualquer uma dessas análises podem não ser suficientes para tirar uma conclusão. Quando vistas como um todo, no entanto, podem fornecer uma imagem mais completa.

O objetivo dessas análises é a *reconstrução do crime* (ou reconstrução de eventos). A *reconstrução do evento* busca determinar *quem* foi o responsável pelo evento, o *que* aconteceu, *onde* o evento ocorreu, *quando* o evento ocorreu e *como* o evento se desdobrou, por meio da identificação, comparação e vinculação de dados (revelando o quadro geral ou a essência de um evento). A reconstrução de eventos pode envolver uma *análise temporal* (ou seja, a determinação dos eventos de tempo ocorridos e a sequência desses eventos), *análise relacional* (ou seja, a determinação dos indivíduos envolvidos e o que eles fizeram, e a associação e relações entre esses indivíduos) e *análise funcional* (ou seja, avaliação do desempenho e das capacidades dos sistemas e dispositivos envolvidos em eventos) (Casey, 2011). Em geral, a reconstrução do evento é realizada para provar ou refutar uma hipótese de trabalho sobre o caso (ou seja, suposição fundamentada sobre a sequência de atos que levaram a um evento) (ENFSI, 2015).

Por fim, o relatório é a etapa que fecha o ciclo da cadeia de custódia, no qual inclui-se a descrição de todas as ações executadas nas demais etapas. O relatório final deverá relatar cada passo relevante da investigação, com informações dos processos técnicos utilizados, mas redigido com linguagem compreensível aos sujeitos processuais, de modo a tornar possível o pleno contraditório no processo judicial.

Os resultados da análise são documentados em um relatório. Estes, a seu turno, devem ser tão claros e precisos quanto possível. Material demonstrativo (por exemplo, figuras, gráficos, resultados de ferramentas) e documentos de apoio, como a documentação da cadeia de custódia, devem ser incluídos, juntamente com uma explicação detalhada dos métodos usados e as etapas tomadas para examinar e extrair dados (US National Institute of Justice, 2004).

As conclusões devem ser explicadas à luz dos objetivos da análise (ou seja, o objetivo da investigação e o caso sob investigação). As informações sobre as limitações dos achados também devem ser incluídas no relatório. O conteúdo do relatório varia de acordo com a jurisdição, dependendo das políticas nacionais (onde houver) em relação a investigações e perícia digital (US National Institute of Justice, 2004).

Prova penal digital: analisados o conceito, as características e a aquisição e preservação da prova digital, na próxima seção serão abordados os métodos ocultos de investigação criminal.

2.3. Métodos ocultos de investigação criminal e os limites impostos pelo direito probatório

Com o surgimento de novos delitos e, também, de novas formas de praticar os delitos já tipificados nos diplomas penais existentes, é necessário que o Estado tenha condições de investigar, processar, prevenir e reprimir estas infrações.

Excepcionalmente, a exemplo de situações que envolvem organizações criminosas, levando-se em conta que, muitas vezes, são constituídas por pessoas que gozam de prestígio e influência social, a investigação se torna difícil caso sejam empregados somente os meios convencionais de investigação.

Para esses casos, é possível que sejam empregados os meios investigativos ocultos, a exemplo das interceptações telefônicas, infiltração de agentes, informantes, acordos de colaborações premiadas, gravações ambientais, rastreamento de celulares, dentre outros, nos termos autorizados pela legislação vigente.

Ocorre que esses meios ocultos, que deveriam ser utilizados somente em casos excepcionais, às vezes são empregados de maneira desregrada, em claro desrespeito aos princípios e garantias vigentes na lei brasileira e nos tratados internacionais dos quais o Brasil é signatário.

Não raro se tem notícias via mídia de interceptações telefônicas e acordos de colaboração premiada teriam sido empregados como único meio de prova para fundamentar sentenças penais condenatórias, o que não é admitido em um Estado democrático de direito. Esses meios ocultos deveriam ser empregados somente em caráter excepcional, como formas para obter outras provas e, assim, em conformidade com o contexto probatório, poderiam ajudar a fundamentar uma condenação. Porém, o emprego de meios investigativos ocultos como única "prova" somente poderia ser utilizado para embasar sentenças absolutórias, mas não as condenatórias (Valente, 2017).

O Brasil, com o objetivo de prevenir e reprimir os delitos mais complexos de serem apurados, a exemplo da corrupção, tráfico de drogas e outros praticados por organizações criminosas, tem buscado exemplos em outros países, especialmente os países que adotam a *common law*, meios investigativos que, da maneira como vêm sendo utilizados, sem as necessárias adaptações ao ordenamento jurídico brasileiro, mostram-se claramente inconstitucionais, além de violarem tratados internacionais de direitos humanos (Valente, 2017).

O uso desses meios é de fundamental importância para a investigação e o processamento de casos complexos, mas é necessário que seja regulamentada pelo ordenamento pátrio, de maneira a evitar sua vulgarização, devendo ser empregados apenas excepcionalmente (em situações em que outros meios investigativos não puderem atingir as mesmas provas que se fazem necessárias) e sempre em consonância com os princípios e garantias, especialmente a ampla defesa, o contraditório, o devido processo legal e a presunção de inocência.

Nesta seção serão abordados os métodos ocultos de investigação criminal e os limites impostos pelo direito probatório. Inicia-se trazendo conceitos e as características dos referidos métodos.

2.3.1. Conceitos e características

O desejo por uma justiça mais célere e veloz, que atenda ao clamor dos cidadãos, que se sentem amedrontados perante os fenômenos da criminalidade econômico-financeira, do

crime organizado transnacional e do terrorismo, motivou os decisores políticos a implementarem meios especiais e excepcionais para a obtenção de prova, a saber:

> ampliação do âmbito das interceptações telefônicas, registro 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 (Valente, 2017, p.474).

Estes meios são denominados métodos ocultos de investigação criminal, que são definidos como "aqueles métodos que representam uma intromissão nos processos de acção, interacção, informação e comunicação das pessoas concretamente visadas, sem que as mesmas disso tenham consciência, conhecimento ou disso sequer se apercebam" (Rodrigues, 2010, p. 37).

Embora já existissem, estes novos métodos de obtenção de provas, experimentaram um maior desenvolvimento nos últimos anos, motivado pelo progresso tecnológico, possibilitando a expansão daqueles métodos já existentes e tornando possível o surgimento de novos métodos (Andrade, 2009).

Aliado a este desenvolvimento, foi observada a existência de uma nova concepção "securitária" do direito penal, que segundo Andrade (2009b) tem levado à redução das garantias dos cidadãos e, consequentemente, à violação de seus direitos fundamentais. No entanto, a cada dia, a prospecção para o emprego dos mesmos tem sido majorada, motivado pelo crescente desenvolvimento da criminalidade, de maneira a alcançar-se maior eficácia na investigação criminal.

A título de exemplificação, a interceptação das comunicações, de um modo geral, e, em particular, a interceptação telefônica, situa-se no campo dos meios probatórios que têm elevado potencial de produzir danos individuais e coletivos ou sociais e, por isso, mereceu restrição em nível constitucional no art. 5º, inc. XII, que, protegendo a intimidade das pessoas, prevê: "[...] é inviolável o sigilo das correspondências 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".

Visando a regulamentar a exceção constitucional, no que diz respeito à possibilidade de autorização para a escuta telefônica, com vistas à persecução penal, foi editada a Lei

9.296/1996, que, ao contrário de legislações como a de Portugal e Alemanha, não trouxe um catálogo fechado de infrações penais que sujeitam os suspeitos a esse especial meio de captação de provas, preferindo-se estabelecer, de forma negativa, as hipóteses de não cabimento da medida:

> Art. 2º. Não será admitida a interceptação de comunicações telefônicas quando ocorrer qualquer das seguintes hipóteses: I – não houver indícios razoáveis de autoria ou participação em infração penal: II – a prova puder ser feita por outros meios disponíveis; o fato investigado constituir infração penal punida, no máximo, com pena de detenção.

Diante da opção do legislador, as infrações penais punidas com pena de detenção, prisão simples ou exclusiva pena de natureza pecuniária, ou educativa, não autorizam a utilização da interceptação de comunicações telefônicas do investigado ou do réu respectivo e dentre essas infrações acham-se a ameaça (art. 147 do CP), os crimes contra a honra (arts. 138-140 do CP), a aquisição de drogas para consumo próprio (art. 28 da Lei nº 11.343/2016) e outros crimes, cujos meios de execução, não raro, envolvem esse tipo de comunicação. Como existe expressa previsão de que esse tipo de infração penal não autoriza o deferimento da medida probatória sob análise, não existe dúvida de que, se houver uma interceptação telefônica com fundamento em alguma dessas infrações penais, constituirá meio ilícito de captação de prova e inviabilizará a sua introdução e avaliação no processo, por força do disposto no art. 5º, inc. LVI da CRFB/1988 ("são inadmissíveis, no processo, as provas obtidas por meios ilícitos").

Há também que se pontuar sobre o acesso aos dados armazenados em aparelhos de comunicação eletrônica. Vários aparelhos eletrônicos permitem o acesso à internet e a outros sistemas de informação e comunicação, gerando uma verdadeira revolução nos meios de comunicação, seja através de conversas eletrônicas ou de trocas de mensagens escritas, gravadas, filmadas (vídeos), por meio de símbolos etc., ou mesmo das diversas formas de armazenagem dessas mensagens. Dentre esses aparelhos, merecem especial destaque os computadores tradicionais, *nootbooks*, *tablets* e, particularmente, os celulares e *smartphones* (estes capazes de gerar a conversação entre os interlocutores, além de oferecer quase todas as funcionalidades de um computador).

Tais aparelhos, cada vez mais dotados de alta carga tecnológica que torna possível a sua múltipla aplicação como meio de comunicação falada e escrita; arquivo eletrônico de dados dos mais variados, inclusive relacionados com a intimidade do usuário e de terceiros; agenda de contatos; hospedeiro de aplicativos bancários, de registro viagens, de controle de

finanças, de geolocalização etc., encontram-se disseminados dentre a população em geral, tornando-se comum a sua apreensão nas mais diversas situações de intervenção policial, bem como a utilização de sistema de geolocalização empregado para encontrar pessoas foragidas, vincular suspeitos ao local do crime, rastrear o próprio aparelho quanto subtraído etc. (Coimbra, 2018).

A partir dessas apreensões, emergem algumas discussões dignas de análise: i) a apreensão desses aparelhos está condicionada à prévia ordem judicial de apreensão? ii) os dados armazenados nesses aparelhos são protegidos pelo sigilo das comunicações? iii) os policiais estão autorizados a atender as chamadas efetuadas para o suspeito ou custodiado? iv) a utilização de sistemas de geolocalização para localizar foragidos ou como instrumento de investigação necessita de prévia autorização judicial? Estes questionamentos serão respondidos na seção dedicada à análise das proibições de provas enquanto limites aos métodos ocultos de investigação criminal.

Em continuidade, tem-se que os países europeus também tardaram a regulamentar o uso dessas tecnologias de geolocalização, que integram o rol dos denominados métodos ocultos de investigação criminal (Andrade, 2009b), figurando dentre os pioneiros a Alemanha[38] e a França[39], sendo que este último, somente em 2014, criou a expressa previsão de que a

38 "A Alemanha é, a par da França, o único país que detém regulação sobre a geolocalização ainda que não o faça tão detalhadamente como o ordenamento francês. De destacar com gáudio a forma mais ou menos hierarquizada com que o legislador alemão sistematizou todas as constelações ocultas de obtenção de prova § 100 –§)100j do CPPa [...]". Pereira, Bruno Carvalho. (2016). *O Sistema de Geolocalização GPS no Processo Penal Português*: Visão integradora ou atípica no quadro dos meios de obtenção de prova. Tese apresentada na Universidade de Lisboa, p. 98-101. Disponível em: https://repositorio.ul.pt/bitstream/10451/26178/1/ulfd132671_tese.pdf.

39 "Até muito recentemente o ordenamento jurídico francês passava pela mesma tormenta que o português e espanhol, ausência de reserva positivadora da figura da geolocalização e que levou, pontualmente, a *Cour de Cassation – Chambre Criminelle* a deliberar e rejeitar o recurso a este tipo de instrumentos por inexistência de regime habilitador, declarando nula toda a prova recolhida através da sua utilização. Em três situações o dito Tribunal considerou essencial a existência de uma reserva de lei que determinasse com exatidão as condições de utilizabilidade à luz dos preceitos de previsibilidade e determinabilidade consagrados no art. 8.º n.º 2 da CEDH para restrições de direitos. O Ac. de 15-10-2014 é claro quanto a esta questão arrazoando conclusivamente que '*en vertu de l'article 8, § 2, de la Convention européenne, toute ingérence dans le droit au respect de la vie privée doit reposer sur une base légale suffisamment claire et précise ; que «dans le contexte de mesures de surveillance secrète la loi doit user de termes assez clairs pour indiquer à tous de manière suffisante en quelles circonstances et sous quelles conditions elle habilité la puissance publique à recourir à de telles mesures*'. Neste sentido vai também o Ac. 22-10-2013 que, à semelhança do anterior, considera ilegítima a autorização do MP para o recurso a forma de investigação que contende com a privacidade das pessoas, devendo essa incumbência recair sobre um juiz. Refere o mencionado aresto que a '*technique dite de géolocalisation constitue une ingérence dans la vie privée dont la gravité nécessite qu'elle soit exécutée sous le contrôle d'un juge'*, único capaz de acautelar procedimentos arbitrários cabendo-lhes assegurar '*que cette ingérence dans la vie privée de la personne concernée était proportionnée au but poursuivi*'. Neste sentido menção ainda a fazer ao Ac. de 22-11-2011 que anulou a decisão do JIC que permitiu a instalação de um dispositivo GPS numa viatura de um suspeito do crime de tráfico de estupefacientes pelo fato de a polícia judiciária ter tido a necessidade de se introduzir na garagem daquele tendo-o feito com a autorização do JIC que, à luz do CPPf – art. 706-96, não detém competências para o determinar, antes o Juiz das Liberdades e da Detenção. Se não fosse essa incompetência decisória a argumentação da *Cour de Cassation* iria no sentido de homologar a decisão por ter sido tomada por um juiz, fazendo jus às exigências de cautela e controlo prévio

geolocalização pode, por questões de necessidade, durante o inquérito, ser realizada por qualquer meio técnico que possibilite, em tempo real, obter a localização de uma pessoa, veículo ou objeto, sem o conhecimento do seu proprietário ou possuidor (Lei 372/2014, art. 230-32).

Na jurisprudência dos tribunais portugueses, observa-se uma tendência de adotar em relação ao uso dessas tecnologias de geolocalização, que se valem dos sinais emitidos através do GPS ou similares, integrados a aplicativos de aparelhos celulares[40], *smartphones*, *tablets*, veículos e outros, critérios similares àquelas aplicáveis às interceptações telefônicas[41], com a sujeição a prévia autorização judicial. Na Legislação brasileira, naquilo que já foi objeto de regulação, a exigência de prévia autorização judicial é regra, por força do disposto no art. 13-B do CPP, com a redação dada pela recente Lei 13.344/2016, mas sujeita à exceção, prevista no § 4º do mesmo artigo, que autoriza a autoridade policial a requisitar os meios tecnológicos adequados – como sinais, informações e outros, que permitam a localização da vítima ou dos suspeitos, diretamente, com imediata comunicação ao juiz competente.

Dentre os métodos ocultos de investigação criminal cita-se também a captação ambiental, que é um meio de obter prova, destinado a combater organizações criminosas, com previsão legal no art. 3º, II, da Lei 12.850/2013.

Trata-se de uma forma de registrar, dentro de um ambiente específico (em um determinado local), sinais eletromagnéticos, ópticos ou acústicos trocados entre pessoas presentes, a partir do uso de gravadores ou da colocação de microfones com amplificadores em pontos estratégicos. Noutras palavras, alguém, mediante utilização de aparelhagem específica, gravará áudios, imagens e sons compartilhados num certo espaço físico (Zanella, 2016).

---

que os dois anteriores acórdãos pontificaram de forma lapidar". Pereira, Bruno Carvalho. *O Sistema de Geolocalização GPS no Processo Penal Português*: Visão integradora ou atípica no quadro dos meios de obtenção de prova". Tese apresentada na Universidade de Lisboa, 2016, p. 102-104. Disponível em: https://repositorio.ul.pt/bitstream/10451/26178/1/ulfd 132671_tese.pdf.

40 TRE Processo nº 648/14.6GCFAR-A.E1 [..] 3) Os dados de tráfego e de localização celular só podem ter como visados as pessoas enumeradas no n.º 4 do artigo 187.º do Código de Processo Penal ex vi do n.º 2 do artigo 189.º do mesmo diploma legal: suspeito ou arguido; pessoa que sirva de intermediário, relativamente à qual haja fundadas razões para crer que recebe ou transmite mensagens destinadas ou provenientes de suspeito ou arguido; ou vítima de crime, mediante o respectivo consentimento efectivo ou presumido (Tribunal da Relação de Évora –Rel. João Gomes de Sousa – Publicação 20.01.2015).

41 Ac. TRE de 18-10-2011 – Processo 19/11.6 GGEVR-A. E1: I. A utilização de meios electrónicos para identificação do IMEI de um posto telefónico móvel, cujo número é desconhecido, cabe na alçada do n.º 2 do artigo 189.º do Código de Processo Penal, uma vez que a utilização de tais meios electrónicos é um meio prévio e instrumental de acesso a dados a cuja protecção a norma se destina (Tribunal da Relação de Évora – Rel.: Fernando Ribeiro Cardoso, Publicação: 18.10.2011).

Entende-se que, assim como ocorre com as conversas telefônicas, a captação dos sinais dentro de um ambiente pode assumir três formas diversas: gravação unilateral (feita por um dos interlocutores), escuta (feita por terceiro com consentimento de um dos interlocutores) e interceptação ambiental (realizada por terceiro sem consentimento de ninguém).

Aqui, sob o prisma da validade da prova decorrente de uma captação ambiental, devemos considerar que a Lei 12.850/2013 não exigiu autorização judicial[42],[43]. Porém, Zanella (2016) entende que a autorização será necessária em alguns casos, em razão de se preservar direitos fundamentais dos envolvidos. A análise do fato dependerá de dois fatores: I) da natureza da medida: se é uma gravação unilateral, uma escuta ou uma interceptação; II) da natureza do local: se público (local público, aberto ou exposto ao público) ou privado (recinto particular). Se for uma captação ambiental gravada unilateralmente, isto é, feita por um dos interlocutores, a intimidade revela-se compartilhada, não sendo necessária autorização judicial, seja o local público ou privado (mesmo raciocínio da gravação telefônica).

Se for interceptação ambiental, isto é, realizada por terceiro sem ciência nem consentimento de nenhum dos interlocutores, ela será lícita, independentemente de autorização judicial, se o local for público, já que nestes casos abre-se mão da intimidade. Isto ocorre porque num ambiente público as pessoas naturalmente têm sua imagem exposta e sabem que, ao falar poderão ser ouvidas por terceiros. A captação teria o mesmo efeito de uma testemunha que pudesse ter visto o investigado no local, ou que o tivesse ouvido falar algo. Não há diferença substancial (a distinção dá-se apenas quanto ao grau de precisão sobre a reprodução do fato em juízo, não havendo maior ou menor violação de intimidade). Porém, para se realizar a interceptação ambiental em local privado, a autorização judicial será necessária, por haver ofensa à intimidade (art. 5º, X, da CRFB/1988). Com efeito, o local é de acesso restrito e nele o investigado somente receberá quem autorizar. Desta forma, para inserir aparelhagem de gravação numa casa ou num escritório, os órgãos de investigação necessitarão de autorização judicial.

Quando se trata de escuta ambiental, ou seja, realizada por terceiro, com autorização de um dos interlocutores, esta será indiscutivelmente válida, desde que colhida em ambiente público (assim como a interceptação). Se em ambiente privado, a questão deve ser resolvida da

---

42 Diferentemente da norma anterior de combate ao crime organizado (Lei 9.034/1995, hoje revogada) que exigia expressamente prévia autorização judicial para captação ou interceptação ambiental.

43 Não nos parece que foi um mero esquecimento do legislador, pois este, quando entendeu pertinente, condicionou expressamente o emprego de certos meios de obtenção de prova à prévia autorização judicial: art. 8º, § 1º (ação controlada) e art. 10 (infiltração de agentes).

mesma forma proposta para as escutas telefônicas (até porque as conversas telefônicas ocorrem privativamente entre interlocutores), a partir de uma análise de proporcionalidade: ponderação entre os bens jurídicos envolvidos (Brentel, 2011).

Por fim, a legislação pátria admite a captação ambiental somente após a prática do delito (em qualquer fase da persecução penal), assim como ocorre com a interceptação telefônica. Diferentemente, a lei estadunidense conhece da captação ambiental, por meio de microfones, interceptores a laser, recepção por satélite e fibras óticas, se houver suspeita de que o local está sendo ou será utilizado para a prática dos crimes previstos no § 2516 do título 18 do United States Code[44] (18 U.S.C. § 2516), dentre os quais os cometidos por organizações criminosas.

Também importa citar a infiltração de agentes que, tal como definida na Convenção das Nações Unidas contra o Crime Organizado Transnacional (Convenção de Palermo), é uma técnica especial de investigação criminal que tem por fim específico a obtenção da prova, "a fim de combater eficazmente a criminalidade organizada"[45].

Por meio desta técnica, um agente policial (chamado de agente infiltrado, ou, em outros países, de agente encoberto) infiltra-se na organização criminosa, como se dela fosse membro, para buscar informações e colher elementos relevantes para apurar os fatos, como, por exemplo, saber quem são seus líderes, quais as tarefas executadas por cada um dos membros e as sedes utilizadas para os negócios escusos, entre outros.

É um mecanismo muito útil – e bastante usado no direito estrangeiro, sobretudo nos Estados Unidos da América – para conhecer a engrenagem de uma organização criminosa, seus dados mais relevantes e seus pontos fracos. Por isso, como veremos nos itens seguintes, a infiltração, se usada da maneira adequada, pode ser assaz efetiva para a desestruturação do grupo criminoso.

Na doutrina pátria, muito oportuna é a definição de Mendonça e Carvalho (2012, p.277), para quem a infiltração de agentes consiste em

> [...] técnica especial de investigação que se caracteriza pela introdução, devidamente autorizada a tal fim, de um ou vários agentes de polícia como se fossem membros da organização criminosa, com o objetivo de descobrir crimes passados, prevenir os futuros e desbaratar toda a organização criminosa.

44 EUA – *US Code*. Disponível em: https://www.law.cornell.edu/uscode/text/18/2516.

45 Art. 20 da Convenção de Palermo, que se refere à vigilância eletrônica e às "operações de infiltração".

A doutrina aponta três importantes características do instituto da infiltração: a dissimulação do agente infiltrado, já que este oculta sua condição de policial; o engano dos membros da organização criminosa, os quais pensam que o agente infiltrado é um deles e assim acabam por lhe confiar informações e tarefas; e a interação, ou seja, o contato direto e pessoal do agente com os investigados (Massom & Marçal, 2015).

Em Portugal, a infiltração de agentes é disciplinada pela Lei nº 101/2001, que trata exclusivamente das "ações encobertas para fins de prevenção e investigação criminal". Esta lei passou por duas atualizações recentes, promovidas pelas Leis nº 60/2013 e nº 61/2015.

O art. 1º, item 2, da Lei define ação encoberta (ou infiltração) como aquela desenvolvida por agentes públicos ou por terceiro atuando sob o controle da Polícia Judiciária, para prevenir ou reprimir os crimes indicados no art. 2º da lei[46], com ocultação da sua qualidade e identidade, tipificados na Lei 109/2009, cujo art. 19 permite para sua investigação o recurso às ações encobertas.

Além de prever a possibilidade da infiltração (ações encobertas) para um grande número de crimes, mesmo não praticados por associações ou organizações criminosas, a legislação portuguesa traz como novidade – em relação às outras legislações – a possibilidade de um particular ser o agente infiltrado, desde que esteja sob o controle e comando da Polícia. Em relação aos agentes públicos, estes não são obrigados a se infiltrar[47].

O art. 3º, item 1, da lei portuguesa traz como requisitos: a adequação da ação encoberta "aos fins de prevenção e repressão criminais identificados em concreto", em especial a colheita de material probatório; e a proporção da medida em relação "à gravidade do crime em investigação". Vê-se, portanto, a previsão expressa para observância ao princípio da proporcionalidade, tal como ocorre no art. 10, § 2º, e 11, ambos do ordenamento brasileiro (Lei 12.850/2013).

Por fim, tem-se a investigação criminal valendo-se de *malwares*, que será detalhada no terceiro capítulo desta dissertação.

46 Assim, a infiltração pode ter por meta recolher provas de crimes já praticados, mas também de evitar crimes futuros. Neste sentido: Gonçalves, F.; Alves, Manuel J.; Valente, Manuel M.G. *Lei e crime*: o agente infiltrado versus o agente provocador. Os princípios do processo penal. Coimbra: Almedina, 2001. p. 28.

47 Há a mesma voluntariedade das legislações espanhola, francesa e brasileira.

2.3.2. Princípios Gerais

Referente aos princípios aplicáveis às provas, podem ser elencados os seguintes: princípio da legalidade; princípio da subsidiariedade; princípio da proporcionalidade; princípio da reserva do juiz; e o princípio da inviolabilidade da área nuclear da intimidade.

Com fundamento no art. 5º, inc. XXXIX da CRFB/1988, c.c. o art. 1º do Código Penal, "Não há crime sem lei anterior que o defina"; significa que para a tipificação penal e para a aplicação da pena faz-se necessária a existência prévia de lei em sentido estrito, tendo em vista que não é permitida a analogia para prejudicar o réu.

Na definição de legalidade há três significados: o significado político (garantia constitucional dos direitos humanos fundamentais; o significado jurídico em sentido lato (que dispõe que ninguém pode ser obrigado a fazer ou deixar de fazer algo senão em virtude de lei, consoante art. 5º, inc. II da CRFB/1988); e o significado jurídico em sentido estrito ou penal (o qual fixa o conteúdo das normas penais incriminadoras). Neste último prisma, também conhecido como princípio da reserva legal, os tipos penais incriminadores só podem ser criados por legislação em sentido estrito, emanada do Legislativo, segundo o procedimento previsto na Constituição Federal.

Existe, também, o que se denomina de reserva legal qualificada, que é a reserva de lei, dependendo das especificações realizadas pela Constituição. Desta feita, não basta que uma lei seja editada para disciplinar determinada questão de interesse social, sendo indispensável que o âmbito estabelecido pelo constituinte seja respeitado. A título de exemplificação, a violação do sigilo das comunicações telefônicas está vinculada aos ditames legais, que, a seu turno, está limitada às finalidades da investigação criminal ou instrução processual penal (art. 5º, XII, CRFB).

Ao contrário do Direito Penal Material, no âmbito do qual se aplica a obrigatoriedade da restrita legalidade prévia (não há crime sem lei anterior que o defina), no Direito Processual Penal, no qual se inclui a investigação criminal, embora esteja adstrito ao princípio da legalidade, admite-se o uso das técnicas da *analogia* e da *interpretação extensiva* para suprir eventuais lacunas legais[48], o que se justifica pelo próprio dinamismo investigativo e da relação processual que deve acompanhar a evolução das relações sociais.

Desse modo, a atividade probatória *lato sensu*, na qual se inclui a investigação criminal e por consequência o uso de métodos ocultos de investigação, está submetida ao princípio da

48 Cf. Art. 3º do Código de Processo Penal brasileiro.

legalidade, do que decorre que a prova penal deve ser produzida nos termos da lei, admitindo-se, contudo, o recurso a meios de prova e meios de obtenção de prova atípicos ou inominados, nos casos em que a lei se revele insuficiente e não haja obstáculo constitucional e/ou legal para a utilização desse meio.

Sob a ótica do princípio da legalidade, e em razão da natureza invasiva e do elevado grau de ingerência nos direitos fundamentais dos métodos ocultos de investigação criminal, o *ideal* é a exigência de regulação legal expressa e satisfatória de todas as técnicas ocultas e inovadoras no âmbito da atividade investigativa estatal. No entanto, ante a impossibilidade prática e racional de se regular o porvir, na ausência da legalidade restrita, não se pode afastar aprioristicamente o recurso a métodos ocultos de investigação criminal, por analogia, enquanto meios atípicos de obtenção de prova, de forma excepcional e subsidiária, no contexto de evolução legislativa progressiva.

Avulta-se, portanto, não apenas o caráter excepcional dos métodos ocultos de investigação criminal, mas, sobretudo, o aspecto da sua aplicação subsidiária em relação aos meios típicos de obtenção de prova penal, devendo-se àqueles recorrer tão somente quando os demais meios se revelem, em abstrato, funcionalmente inaptos a alcançar os dados pretendidos ou, em concreto, inúteis ou impraticáveis (Ramalho, 2017).

O princípio da subsidiariedade se traduz no fato de que a norma penal exerce uma função meramente suplementar da proteção jurídica em geral, só valida a imposição de suas sanções quando os demais ramos do Direito não mais se mostram eficazes na defesa dos bens jurídicos (Tavares, 2002).

Assim, em se tratando de métodos ocultos de investigação criminal, pelo princípio da subsidiariedade, depreende-se que só se deve recorrer aos referidos métodos quando já se tiver recorrido aos demais métodos (métodos abertos), menos invasivos e lesivos. Assim, em um Estado Democrático de Direito, o uso de métodos ocultos de investigação empregados pelo Estado deve ser a exceção e demanda especial justificativa (Andrade, 2009).

No que tange à possibilidade de utilização excepcional da prova ilícita, tem-se que é possível, de forma excepcional, o uso, no processo penal, da prova obtida ilicitamente, quando isto for necessário para salvaguardar um bem jurídico ou valor que, no caso concreto, mostre-se mais relevante do que o direito violado quando da obtenção indevida da prova (Avolio, 2015).

Trata-se da adoção, em matéria probatória, do princípio da proporcionalidade, o qual, para Robert Alexy, é o "princípio dos princípios", já que se trata de um método interpretativo para solucionar um choque de valores fundamentais num caso concreto:

> O caráter principiológico das normas de direito fundamental implica a necessidade de um sopesamento quando elas colidem com princípios antagônicos, o qual será feito com a "máxima da proporcionalidade", "com suas três máximas parciais da adequação, da necessidade e da proporcionalidade em sentido estrito (Alexy, 2014, p.160).

O caso Weber and Saravia *vs* Germany (n.º 54934/00[49]) é um precedente vinculativo que ilustra bem o princípio da proporcionalidade, podendo-se da análise do caso abstrair-se os princípios da *reserva da lei*; da *subsidiariedade*; e da *reserva de juiz*. Neste caso, os requerentes alegaram que a lei alemã sobre a limitação da privacidade das comunicações postais e telecomunicações foi violada, especialmente, os artigos 8º, 10º e 13º da Convenção Europeia dos Direitos do Homem, em razão de uma mudança na citada norma, que ocorreu em 1994 e ampliou os poderes de interceptação de comunicações do sistema de inteligência alemão, criando a possibilidade de "monitoramento estratégico de telecomunicações". Referido monitoramento consiste na coleta de informação valendo-se da interceptação de comunicações com vistas a identificar e evitar graves ameaças à República Federal da Alemanha. Os requerentes, uma jornalista alemã (Weber) e um cidadão uruguaio (Saravia), argumentaram que a técnica investigativa de monitoramento estratégico de telecomunicações violava seus direitos, a exemplo do direito à vida privada e ao sigilo de correspondência. O Tribunal Europeu dos Direitos do Homem não reconheceu nenhuma das violações alegadas pelos postulantes e entendeu que a legislação alemã era devidamente densificada e continha salvaguardas suficientes que poderiam ser empregadas para proteger os direitos fundamentais dos investigados.

A aplicação do princípio da proporcionalidade em se tratando de métodos ocultos de investigação é uma posição intermediária entre as teorias da admissibilidade e da inadmissibilidade. A característica basal da teoria da proporcionalidade é o respeito à vedação constitucional dos métodos ocultos, como regra, e sua utilização, como exceção, em casos graves e extremos. Há, pois, um juízo de ponderação, buscando-se um ideal de justiça na análise do caso concreto.

Tal juízo é estruturado em três elementos: adequação (ou idoneidade da medida); necessidade; e proporcionalidade em sentido estrito (ou justa medida). Sobre o assunto Zanella assim dispõe:

> O juízo de proporcionalidade é desenvolvido a partir de um critério trifásico de seus subelementos estruturantes: adequação (idoneidade), necessidade (exigibilidade) e

49 European Court of Human Rights. (2006). Weber and Saravia *vs* Germany (n.º 54934/00). Disponível em: https://opil.ouplaw.com/view/10.1093/law-oxio/e199.013.1/law-oxio-e199.

> proporcionalidade em sentido estrito. Um meio é adequado quando o seu uso é apto a alcançar o resultado almejado; é necessário quando não existe outro meio distinto que seja igualmente eficaz; é proporcional (em sentido estrito) quando as vantagens do fim alcançado superam as desvantagens da limitação ou restrição ao direito fundamental atingido (Zanella, 2016, p. 101).

Assim, o uso dos métodos ocultos de investigação seria permitido – repita-se excepcionalmente – se ele for adequado e necessário e, mormente, se o valor a ser tutelado pelo uso destas provas que poderão ser obtidas for tão significante a ponto de justificar a violação. Nas palavras de Alexandre de Moraes:

> Essa atenuação prevê, com base no princípio da proporcionalidade, hipóteses de admissibilidade das provas ilícitas, que, sempre em caráter excepcional e em casos extremamente graves, poderão ser utilizadas, pois nenhuma liberdade pública é absoluta, havendo possibilidade, em casos delicados, em que se perceba que o direito tutelado é mais importante que o direito à intimidade, segredo, liberdade de comunicação, por exemplo, de permitir-se sua utilização (Moraes, 2016, p.263).

A doutrina processual penal aceita, em sua ampla maioria, a aplicação da teoria da proporcionalidade quando os métodos ocultos de investigação forem empregados em favor do réu, uma vez que o bem jurídico a se tutelar, qual seja, a liberdade e privacidade de um indivíduo, é assaz relevante, preponderante no que se refere à inadmissibilidade do uso do método – e, por consequência, do próprio direito violado, como, por exemplo, a intimidade de outrem.

Cita-se o clássico exemplo do indivíduo que, vendo-se injustamente processado criminalmente, grava, sem autorização judicial, a interceptação telefônica de diálogo mantido entre o verdadeiro autor da infração e terceiro, e depois pretende fazer uso no processo-crime em que é acusado para demonstrar não ser o verdadeiro autor dos fatos apurados. Neste sentido os ensinamentos de Grinover, Gomes Filho e Fernandes (2001), para quem a ilicitude da prova em favor do réu é eliminada, seja por causas de justificação legal (estado de necessidade ou legítima defesa), seja pelo critério de proporcionalidade, diante da prevalência da ampla defesa, direito consagrado pela Constituição Federal.

Num balanço feito por Tourinho Filho (2012), o fundamento para permitir, em favor do acusado, a utilização de métodos investigativos ocultos é a consideração de que a garantia de ampla defesa (princípio constitucional) e, principalmente, o direito de liberdade (também consagrado constitucionalmente) superam, numa análise de proporcionalidade – adequação, necessidade e justa medida – a vedação (também constitucional) da inadmissibilidade da prova

obtida por métodos ocultos e, por consequência, o direito transgredido (intimidade, vida privada, entre outros).

Apesar de a teoria da proporcionalidade ser bem aceita pela doutrina e jurisprudência em favor do réu, minoritário é o entendimento no sentido de que ela também pode ser utilizada *pro societate*, ainda que a prova ilícita seja a única nos autos em desfavor do acusado (Zanella, 2016).

A razão para isso é que seu uso em benefício do acusado poderia preservar o direito à ampla defesa no processo, em busca de sua (adequada) proteção ou absolvição e, por consequência, preservaria também sua liberdade. Já o seu uso em favor da acusação e, portanto, como preceito, pelo Estado (a regra é que as ações penais são públicas), seria inconcebível, tendo em vista que este tem por obrigação pautar-se pela legalidade em todos os segmentos, inclusive na busca da prova. Este uso geraria descontrole e incentivaria atos funcionais abusivos.

Aury Lopes Junior (2016) sintetiza que o uso da teoria da proporcionalidade em favor da sociedade traria um perigo imenso, devido à amplitude do conceito (indeterminado e, portanto, "manipulável") e o incorreto reducionismo binário do interesse público versus interesse privado, para justificar uma escolha do primeiro e assim legitimar restrições indevidas dos direitos fundamentais.

Por fim, cita-se Bonfim (2012) que, em detida análise do princípio da proporcionalidade, menciona que o juiz, frente a determinado caso no qual há colisão de direitos protegidos pela Constituição, deverá, após as análises de adequação e necessidade, estabelecer o peso de cada um deles (proporcionalidade em sentido estrito), optando por aquele que entende predominar na situação *sub judice*. Em decorrência disso, conclui ser inviável a inadmissibilidade absoluta da utilização de métodos ocultos de investigação, porquanto esta afrontaria "o princípio do livre convencimento do juiz, na medida em que obriga o magistrado a desconsiderar a realidade, ou seja, a busca da verdade real" (Bonfim, 2012, p. 369).

No caso em particular dos métodos ocultos de investigação criminal, o princípio da proporcionalidade funciona de baliza ao Poder Judiciário, no exercício do controle preventivo e também repressivo dos atos de investigação criminal, para, no caso concreto, avaliar a pertinência do uso de tais técnicas, a sua justificação constitucional frente às factíveis restrições aos direitos fundamentais, a sua aplicação excepcional e subsidiária, bem como a sua adequação e imprescindível necessidade, ponderando-se a gravidade e complexidade do fato investigado e o grau de ingerência aos direitos fundamentais envolvidos.

Referente ao princípio da reserva do juiz, este significa que cabe ao juiz e não a outra entidade competente, autorizar o uso de métodos investigativos ocultos, exceto quando existir "perigo de demora". Fundamentalmente, este princípio tem o condão de assegurar preventivamente a tutela dos direitos de um indivíduo (na maioria das vezes o arguido) exposta à devassa sem a possibilidade de preservar sua própria defesa. Ademais, os métodos ocultos referem-se a medidas cujo dano é certo, inobstante as vantagens sejam incertas. Esta é, pois, a justificativa para que uma autoridade neutra e imparcial seja autorizada a intervir (Almeida, 2009).

Portanto, cabe ao magistrado, enquanto entidade imparcial no processo, analisar de forma objetiva os bens jurídicos em conflito nos termos da lei penal e da CRFB/1988 e, perante a proposta do Ministério Público para o uso de algum método investigativo, decidir pela justificação ou não da restrição de direitos fundamentais.

O último princípio é o da inviolabilidade da área nuclear da intimidade, os conhecimentos fortuitos oriundos de investigações criminais em ambiente digital e demais requisitos dos métodos ocultos. Este princípio significa que o direito dos meios ocultos de investigação criminal precisa integrar soluções normativas indispensáveis para assegurar a inviolabilidade da área nuclear da intimidade, além de determinar medidas que sirvam para tutelar o direito à recusa de prestar depoimento, direito este que em se tratando de direito processual "aberto" é assegurado às testemunhas em nome das relações de solidariedade familiar, ou, melhor dizendo em nome da importância pessoal e institucional dos distintos deveres de sigilo (Martinez, 2019).

Porém, pela natureza das coisas, e em razão de os meios investigativos ocultos serem, em sua maioria, constituídos por procedimentos automatizados, em um primeiro momento parece ser difícil salvaguardar a tutela nuclear da intimidade logo no momento em que os dados forem recolhidos ou que as provas forem produzidas. No entanto, isto poderá ocorrer em momento ulterior, no momento em que as provas recolhidas forem apreciadas. Assim, caso se verifique que foram recolhidos dados afetos à área nuclear da reserva da intimidade, é preciso que estes dados sejam destruídos, posto que sua valoração não será admitida (Andrade, 2009).

Cabe também aos investigadores um cuidado especial para com os conhecimentos fortuitos oriundos das investigações criminais em ambiente digital. Isto porque na grande maioria dos computadores de uso pessoal, há armazenadas em disco rígido, diversas informações pessoais não apenas do visado como também de terceiros, a exemplo de vídeos, fotografias, diários íntimos, registros dos *websites* acessados, de conversas privadas, *e-mails*,

contatos e outros elementos armazenados muitas vezes ao longo de anos no sistema informático, tornando possível conhecer em profundidade a vida e a personalidade do investigado.

Por esta razão é possível afirmar que a apreensão ou o acesso remoto (valendo-se, por exemplo de um *malware*) representa o acesso a uma fonte de informação significativamente superior a qualquer outra prova acessível em processo penal (Martinez, 2019). Não se nega, também, que esta intromissão pode produzir consequências irreparáveis e, por esta razão, existem proibições de prova que servem como limites aos métodos ocultos de investigação criminal, conforme se verá na próxima seção.

2.3.3. As proibições de prova enquanto limites aos métodos ocultos de investigação criminal

Em um Estado Democrático de Direito, em que a matriz fundamental é a dignidade da pessoa humana, o Estado não pode se valer de qualquer método de obtenção de prova nem tampouco de determinadas provas que possam ferir de morte as garantias fundamentais do cidadão.

Assim, a busca da verdade não se dá a qualquer custo, mas tão somente por meios justos e leais conforme o Estado democrático de direito, ainda que eventualmente tenha que renunciar à descoberta da verdade para salvaguardar direitos intransponíveis. Nesse sentido, as proibições de prova funcionam como verdadeiros limites à descoberta da verdade e, como tal, limitam a atividade de investigação criminal e os métodos utilizados.

A CRFB/1988 impõe em seu art. 5º, inc. LVI - são inadmissíveis, no processo, as provas obtidas por meios ilícitos.

As limitações impostas pelo Direito Probatório refletem diretamente na atividade de investigação criminal (e, mais especificamente, nos meios de obtenção de prova), não se admitindo ato investigativo criminal que não conduza a fonte de prova ou elemento que possa ser utilizado em juízo.

Conforme destacado em linhas pretéritas, a tecnologia está cada vez mais presente no cotidiano das pessoas, das empresas e das instituições públicas. Essa nova realidade impõe novos desafios sobretudo à segurança dos dados que circulam no ambiente digital, deixando mais vulneráveis a privacidade e a intimidade dos cidadãos. Por outro lado, também traz novos obstáculos à elucidação de condutas criminosas e de seus autores.

Nesse contexto de evolução tecnológica e de vulnerabilidade do ambiente digital, têm sido desenvolvidos "métodos de remoção, ocultação e subversão de evidências com o objetivo de mitigar os resultados de análises forenses computacionais" (Henrique, 2006), nos quais se incluem técnicas, *hardware* e programas informáticos. São o que se denomina de medidas antiforenses.

Essas medidas antiforenses podem se revestir de natureza legítima, quando utilizadas para proteção dos dados informáticos ou como meio de preservação da intimidade e da liberdade de expressão. Mas, por outro lado, também são muitas vezes utilizadas como meios de esconder e camuflar a prática de crimes e frustrar potenciais atividades de recolha de provas nos sistemas informáticos (Ramalho, 2017).

Nas palavras de Harris (2006, p. 45), as medidas antiforenses são:

> [...] quaisquer tentativas de comprometer a disponibilidade ou utilidade da prova no processo forense. Comprometer a disponibilidade da prova inclui quaisquer tentativas de evitar que a prova venha a existir, de esconder prova existente ou de manipular a prova no sentido de assegurar que a mesma deixe de estar ao alcance do utilizador. A utilidade pode ser comprometida através da obliteração da própria prova ou da destruição da sua integridade.

Muitas são as medidas antiforenses por meio das quais objetivam-se evitar que as entidades de investigação alcancem dados digitais com potencial valor probatório (Ramalho, 2017, p. 150-175), o que não só tornam mais fácil a prática de crimes em ambiente digital e o seu anonimato, como, inversamente, tornam mais difícil a sua descoberta e a obtenção de provas. Em razão disso, algumas vezes demonstra-se imperiosa a utilização de métodos ocultos de investigação criminal para que o Estado possa ter acesso às fontes de provas digitais e, consequentemente, alcance a verdade no processo penal.

Na busca desse equilíbrio, o Estado não deve ser, por um lado, um Estado-polícia com poderes ilimitados, sob pena de o combate à criminalidade gerar uma verdadeira "criminalidade de Estado"; e, por outro lado, não deve constituir-se também em um mero Estado-observador, omisso (que em nada intervém), o que pode gerar a primazia da "lei do mais forte". Assim, o sistema de justiça penal, no qual se inclui a investigação, deve encontrar uma solução intermediária entre o Estado débil e o Estado forte, fruto de uma adequada ponderação entre a necessidade da busca da verdade e realização da justiça, de um lado, e o respeito à inviolabilidade do núcleo essencial dos fundamentais do cidadão (Ramalho citou Gossel, 2007, pp.146-147 *apud* Ramalho, 2017, p. 183).

Nesse sentido, Correia (1999, p.191 *apud* Ramalho, 2017, pp. 183-184), conclui que:

> O direito processual é assim um instrumento privilegiado de agressão aos direitos, liberdades e garantias individuais e, ao mesmo tempo, um meio indispensável para a sua proteção. A sua observância é, por isso mesmo, uma garantia fundamental, que confere segurança, previsibilidade e certeza aos cidadãos.

Deve-se buscar, portanto, a concordância prática entre os propósitos paradoxais do processo penal da correta investigação dos ilícitos penais, da descoberta da verdade e subsequente realização da justiça, com o respectivo restabelecimento da paz jurídica, e, ao mesmo tempo, da proteção dos direitos individuais contra a atuação arbitrária do Estado.

Assim, a busca da verdade no processo penal em um Estado Democrático de Direito não pode ser realizada a qualquer preço, mas somente a partir de meios legítimos. Conforme a lição de Dias (2004), a verdade processual não é absoluta ou ontológica, mas antes de tudo, é uma verdade judicial, prática e, principalmente, uma verdade que não é obtida a qualquer custo, mas processualmente válida, ou seja, obtida em observância de todas as formalidades judiciais.

Como ensina Silva (2010, pp. 82-83):

> A justiça criminal é chamada a investigar actividades suspeitas, tanto de pessoas honestas como de malfeitores, mas todos são, pessoas. Por outra parte, não se compreende que aqueles que se dedicam a servir a justiça possam usar na luta contra os malfeitores meios análogos aqueles que lhes reprovam. A eficácia da justiça é também um valor que deve ser perseguido, mas, porque numa sociedade livre e democrática os fins nunca justificam os meios, só será louvável quando alcançada pelo engenho e arte, nunca pela força bruta, pelo artifício ou pela mentira, que degradam quem as sofre, mas não menos quem as usa.

Por mais grave que seja o ilícito criminal cometido e quão difícil seja se alcançar a verdade, o Estado jamais poderá se utilizar de meios que imponham a aniquilação do núcleo essencial dos direitos fundamentais. Por isso, a Constituição Federal brasileira estabelece expressamente que "são inadmissíveis, no processo, as provas obtidas por meios ilícitos"[5] (como referir). A atuação do Estado na descoberta da verdade deve sempre estar adstrita ao princípio da lealdade. Esta postura do Estado é um dever essencialmente moral traduzindo "uma maneira de ser da investigação e obtenção de provas em conformidade com os direitos da pessoa e a dignidade da justiça" (Silva, 2010, p. 80).

Assim, a salvaguarda do núcleo essencial dos direitos fundamentais e a obediência à postura leal impõem restrições aos meios de obtenção de prova no processo penal democrático, ainda que isso implique eventualmente renunciar à descoberta da verdade e

consequentemente abdicar de condenar um criminoso quando a única prova da sua culpa apenas possa ser obtida a partir de meios, em abstrato, inadmissíveis num Estado de Direito ou, em concreto, desproporcionais (Ramalho, 2017, p. 185).

Nesse sentido, segundo Leite (2014, p. 257 *apud* Ramalho, 2017, p. 185):

> [...] o Estado de Direito Democrático, assente na autonomia e dignidade da pessoa humana e no pluralismo, tem, forçosamente, de conviver com o fracasso e de reconhecer que, no caminho da prosecução da justiça, há, por vezes, um dever de recuar face à prevalência de direitos fundamentais.

Por outro lado, se é certo que essa orientação implica severas restrições ou limites à descoberta da verdade e à investigação criminal, "também é verdade que existem casos em que se justifica que o Estado vá mais longe do que noutros na procura da verdade, avançando paulatinamente em direcção ao limite – a todos os títulos intransponíveis – da dignidade e integridade pessoal do visado" (Ramalho, 2017, p. 185).

Na busca desse equilíbrio, o Estado deve decidir qual é o preço que está disposto a pagar para a prossecução penal de quem pratica um crime. Em outras palavras, o sacrifício que o Estado está disposto a fazer no que tange aos direitos fundamentais para o alcance da verdade. Esse sacrifício é materialmente executado, na etapa de investigação, a partir da utilização "um *arsenal* de meios de investigação criminal progressivamente mais agressivos dos direitos dos cidadãos em função da gravidade e danosidade social do crime em causa ou da absoluta indispensabilidade do meio de prova em face das circunstâncias" (Ramalho, 2017, pp. 185-186).

Mesmo reconhecendo-se os enormes desafios para a descoberta da verdade oriundos da complexidade do ambiente digital e dos métodos desenvolvidos pelos recursos tecnológicos para esconder e camuflar a prática de crimes e obstaculizar o acesso às provas, o preço que o Estado se disponha a pagar não pode chegar ao ponto de corroer a liberdade de atuação do cidadão comum, por receio de uma ingerência estatal remota e secreta, preventiva ou repressiva, nas atividades de sua vida (Ramalho, 2017, p. 186).

É nesse âmbito que as proibições de prova funcionam como verdadeiros limites autoimpostos pelo Estado à descoberta da verdade, ancoradas no princípio da dignidade da pessoa humana, matriz fundamental do Estado Democrático de Direito, cuja violação atinge a própria legitimidade do exercício do poder punitivo do Estado (Mata-Mouros, 2011, pp. 330-331).

A partir desse panorama inicial e resguardando-se principalmente a dignidade da pessoa humana, é que importa realizar os apontamentos necessários que permitam

compreender as investigações tecnológicas e seus reflexos sobre os direitos da personalidade e, consequentemente, sobre a dignidade da pessoa humana.

Pereira (2016) entende que a apreensão de computadores, *smartphones, tablets* e celulares está sujeita às mesmas regras que regem a apreensão de bens em geral, particularmente aquelas inseridas no capítulo da "busca e apreensão", exceto quando se tratar de objetos que tenham relação com o fato criminoso[50] ou mesmo de objetos sujeitos a medidas assecuratórias[51] ou cautelares patrimoniais, que possuem regramento específico. Assim, em se tratando de apreensão vinculada à produção de provas em geral, a regra é a de que deva ser precedida de ordem ou autorização judicial, pois se trata atividade constritiva com incursão sobre o patrimônio e a intimidade da pessoa afetada pela diligência e com reflexos na prova a ser produzida nas investigações extrajudiciais ou judiciais.

Importa destacar que eventuais excessos por parte dos agentes encarregados da investigação podem configurar, inclusive, desde que presente o elemento especial subjetivo do dolo (dolo específico) previsto no art. 1º, § 2º da Lei 13.869/2019[52], o tipo penal previsto no art. 25 da referida Lei de Abuso de Autoridade[53], desde que a prática ocorra no curso de procedimento de investigação (inquérito, sindicância, PIC, entre outros) ou fiscalização, havendo ainda a possibilidade da extensão do crime em questão àquela autoridade que: "[...] faz uso de prova, em desfavor do investigado ou fiscalizado, com prévio conhecimento de sua ilicitude"[54].

Nesse sentido, importa colacionar a jurisprudência do STJ sobre o tema:

> [...] a jurisprudência deste Tribunal Superior firmou-se no sentido de ser ilícita a prova oriunda do acesso aos dados armazenados no aparelho celular, relativos a mensagens de texto, SMS, conversas por meio de aplicativos (*WhatsApp*), obtidos diretamente pela polícia no momento da prisão em flagrante, sem prévia autorização judicial. II – *In casu*, os policiais civis obtiveram acesso aos dados (mensagens do aplicativo *WhatsApp*)

50 Art. 6º do CPP brasileiro.

51 Art. 125 do CPP brasileiro e seguintes.

52 Art. 1º - Esta Lei define os crimes de abuso de autoridade, cometidos por agente público, servidor ou não, que, no exercício de suas funções ou a pretexto de exercê-las, abuse do poder que lhe tenha sido atribuído. § 1º As condutas descritas nesta Lei constituem crime de abuso de autoridade quando praticadas pelo agente com a finalidade específica de prejudicar outrem ou beneficiar a si mesmo ou a terceiro, ou, ainda, por mero capricho ou satisfação pessoal. § 2º A divergência na interpretação de lei ou na avaliação de fatos e provas não configura abuso de autoridade.

53 Art. 25. Proceder à obtenção de prova, em procedimento de investigação ou fiscalização, por meio manifestamente ilícito: Pena – detenção, de 1 (um) a 4 (quatro) anos, e multa. Parágrafo único. Incorre na mesma pena quem faz uso de prova, em desfavor do investigado ou fiscalizado, com prévio conhecimento de sua ilicitude.

54 Parágrafo único do art. 25 da referida Lei de Abuso de Autoridade.

> armazenados no aparelho celular do corréu, no momento da prisão em flagrante, sem autorização judicial, o que torna a prova obtida ilícita, e impõe o seu desentranhamento dos autos, bem como dos demais elementos probatórios dela diretamente derivados. III– As instâncias ordinárias fundamentaram a prisão preventiva do recorrente nos indícios de materialidade e autoria extraídos a partir das conversas encontradas no referido celular, indevidamente acessadas pelos policiais, prova evidentemente ilícita, o que impõe a concessão da liberdade provisória[55].
>
> No que concerne à ilegalidade das provas colhidas no aparelho telefônico do recorrente, tem-se que, a despeito de a situação retratada não se configurar como interceptação telefônica de comunicações, demanda igualmente autorização judicial devidamente motivada – haja vista a garantia constitucional à intimidade e à vida privada -, o que efetivamente foi observado no caso dos autos. De fato, o celular do recorrente foi apreendido em razão de mandado de busca e apreensão, devidamente fundamentado, que autorizou a apreensão de aparelhos eletrônicos, bem como o acesso às informações armazenadas, desde que guardem relação com o crime sob investigação. 5. Recurso em habeas corpus improvido[56].

Os dados armazenados em quaisquer desses aparelhos (computador, *smartphone*, celular etc.) não se confundem com as comunicações das quais derivaram e, uma vez concluídas estas comunicações, desde que armazenadas, passam elas a ter a natureza de documentos guardados ou arquivados, podendo ser acessados e utilizados como prova, desde que observadas as mesmas restrições aplicáveis à apreensão de documentos em geral. Assim como um policial não está autorizado a acessar um escritório ou uma residência, quando ausentes as hipóteses previstas em lei ou da presença de concordância do responsável, e apreender documentos arquivados ou guardados, assim também não está autorizado a acessar o banco de dados desses equipamentos eletrônicos, exceto se tiver autorização judicial para esta diligência[57].

Prática comum, mas nem por isso lícita, vem a ser aquela em que o policial realiza uma diligência ou mesmo uma prisão em flagrante e, sem autorização judicial ou do custodiado, atende as ligações destinadas a ele, acessa a sua agenda de contatos, o seu arquivo de fotos ou mesmo lê as mensagens ou *emails* do custodiado, sem o consentimento dele. Esta prática, apesar de contar com o apoio de alguma corrente jurisprudencial, é ilegal e fere o direito de privacidade das comunicações do indivíduo investigado (art. 5º, XII da CRFB [58]) quando se

---

55 STJ–RHC: 92009 RS 2017/0302378-7–Rel.: Min.Felix Fischer–DJe 16.04.2018.

56 RHC 64.713/SP – Rel. Min. Reynaldo Soares Da Fonseca – DJe 02.12.2016.

57 RHC 64.713/SP – Rel. Min. Reynaldo Soares Da Fonseca – DJe 02.12.2016.

58 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.

trata de ligações ou mensagens em curso; ou a sua privacidade (art. 5º, X da CRFB [59]), quando se refere a mensagens ou ligações armazenadas, movimentação bancária, etc., neste caso concebidas como dados armazenados e não como dados interceptados, gerando uma prova ilícita.

Não obstante a posição aqui externada, há considerável corrente jurisprudencial, principalmente nos tribunais de 2ª instância, sustentando a tese da licitude da diligência policial consistente em acessar e ler ou decifrar os arquivos dos aparelhos celulares ou *smartphones*, sem consentimento de quem de direito, ao argumento de tal prática decorreria da autorização de apreensão prevista no art. 6º do CPP, o que parece decorrer de equívoco interpretativo, uma vez que as regras que dizem respeito a limitação de direitos fundamentais precisam ser interpretadas restritivamente. No entanto, o acesso indevido aos dados armazenados não os invalida, tornando ilícitas apenas o uso do conteúdo acessado ilegalmente, mas permitindo que, após invalidado aquele conteúdo, outras investigações possam partir da mesma fonte, de forma ampla.

Essa exceção se explica, pois uma vez concebida a ilicitude da prova (v.g. conteúdo de mensagens armazenadas em aplicativo de *WhatsApp*; registro de conversas por meio de *e-mail* etc.), por ter sido obtida com afronta a regra de direito material (inseridas na Constituição Federal, em Normas Internacionais internalizadas pelo Brasil e Leis), não pode aquela própria prova ser aproveitada ou refeita, mas tendo o equipamento tecnológico (celular, *smartfhone* etc.) sido apreendido regularmente, como na situação aqui analisada ele se constitui em fonte de provas e não em elemento de prova, desde que tenham sido obedecidas as regras de integridade da cadeia de custódia na preservação do aparelho e de seus dados armazenados e aplicativos periciados, conforme recentes alterações introduzidas no CPP[60] pela Lei 13.964/2019, encontra-se autorizado o novo acesso ao conteúdo daquelas fontes, para a produção de provas judicialmente autorizadas[61].

---

59 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.

60 CPP, arts. 158-A/158-F, no que for aplicável ao tema.

61 STJ: por ocasião da própria prisão em flagrante – sem, portanto, a prévia e necessária autorização judicial -, o policial atendeu o telefone do réu e afirmou que a ligação tratava de um pedido de venda de substância entorpecente. Na delegacia o celular do réu foi apreendido, desbloqueado e nele verificada a existência de mensagens de texto que indicavam prévia negociação da venda de entorpecentes, sem, portanto, anterior autorização judicial. 3. A denúncia se apoiou em elementos obtidos a partir da apreensão do celular pela autoridade policial, os quais estão reconhecidamente contaminados pela forma ilícita de sua colheita. [...](STJ–HC: 542293 SP 2019/0322281-7–Rel.: Min.Rogerio Schietti Cruz–DJe 19.12.2019).

Já a geolocalização é a localização que alguns equipamentos fornecem, seja de um objeto ou de um indivíduo. Existem várias tecnologias que fornecem a geolocalização exata do dispositivo móvel, pessoas ou veículos. Atualmente, é mais comum encontrar a citada tecnologia em aparelhos celulares, *tablets* e até *smartwatches*, o que vem popularizando a utilização dessas tecnologias não só para fins militares e profissionais, mas também para finalidades probatórias e de monitoramento nos mais diversos ramos, desde os vinculados às relações de trabalho, àqueles com viés de investigação criminal.

A utilização da tecnologia para indicar a localização ou propiciar o rastreamento do investigado/usuário, desenvolveu-se especialmente através da monitoração dos sinais emitidos pelas estações rádio base (ERBS). A ERBS é constituída de um ou mais emissores, de rádio receptor de antenas. Quando uma chamada é efetuada, ondas de rádio são emitidas pelo telefone celular. As ondas de rádio (radiofrequência) são recebidas por antenas das estações de rádio mais próximas e a operadora de telefonia móvel registra em quais antenas as ondas de um determinado celular são recebidas. Por meio da triangulação do posicionamento do aparelho fazendo uso de *softwares*, a operadora identifica a área aproximada em que se encontra o usuário do telefone celular.

Com os avanços na área da tecnologia das comunicações, há hoje diversas tecnologias aptas a possibilitar a localização de aparelhos e usuários, embora a suas finalidades sejam diversas daquelas vinculadas às investigações criminais, destinando-se no uso cotidiano a fins de segurança e conforto dos usuários, informando com exatidão o local onde se encontra uma pessoa, veículo ou objeto, inclusive para que pais monitorem os seus filhos ou as pessoas em geral tenham a comodidade de seguir um trajeto para um determinado lugar, em especial através do uso de GPS (*Global Position System*).

Para desencadear uma operação de geolocalização através do *smartphone* ou aparelho similar, normalmente é necessário que se saiba o número ou código utilizado pelo procurado ou investigado em seu aparelho ou equipamento, em especial o IMEI – *International Mobile Equipment Identity*. Na esfera criminal, essa diligência pode funcionar como ferramenta de rastreamento e localização, mas também é apta a atender outras finalidades, como o cumprimento de mandados de prisão e o monitoramento dos hábitos do indivíduo investigado através dos locais por ele frequentados, que pode ser útil em relação a vários aspectos analisados em um processo criminal, como a presença, ou não, no local do crime; a trajetória feita em determinada ocasião (Andrade, 2009b); demonstração de indícios de riqueza; ausência do local de trabalho, afastando possível álibi; frequência a "bocas de fumo";

descumprimento de medidas cautelares restritivas (CPP, art. 319) ou de medidas protetivas de urgência (Lei 11.340/2006), além de tantos outros.

Essas tecnologias de geolocalização, máxime o geoposicionamento por GPS, são importantes ferramentas tecnológicas de investigação com vistas à produção de provas e também para a localização de pessoas monitoradas, foragidas ou vítimas de sequestro para os mais diversos fins, o que é possível valendo-se da captação de sinais emitidos por telemóveis, *smartphones*, "tornozeleiras eletrônicas" e similares, possuindo, de outra parte, inquestionável potencial invasivo, levando à necessidade do controle jurisdicional, com vistas a possibilitar a sua adequada utilização, sem excessos que comprometam desnecessariamente a intimidade das pessoas.

A Lei 13.344/2016, que dispõe sobre prevenção e repressão ao tráfico interno e internacional de pessoas e sobre medidas de atenção às vítimas, regulamentou de forma ainda restritiva e insuficiente a utilização da tecnologia de geolocalização, para fins de investigação criminal vinculada àquelas modalidades criminosas, reconhecendo a importância desse moderno instrumento de investigação e da necessidade de controle sobre a sua utilização[62]. Na ausência de uma legislação mais abrangente sobre o tema, o judiciário vem concedendo tais autorizações através da aplicação da Lei 9.296/1996, o que não parece ser adequado a todas as situações que possibilitam o geolocalização para fins processuais, através do acesso a equipamentos que sejam propriedade do investigado ou estejam legitimamente na sua posse, não havendo necessidade de autorização quando o sinal for captado de equipamentos que estejam ilicitamente com o investigado (v.g. em especial no caso de furto ou roubo de veículos, celulares, *smartphones, tablets* etc.).

A edição da Lei 13.344/2016 regulamentando a utilização desse meio tecnológico de prova, com aplicação limitada a crimes de alto potencial lesivo, e reconhecimento, como regra,

---

62 Art. 13-B do CPP (introduzido pena Lei 13.344/2016). Se necessário à prevenção e à repressão dos crimes relacionados ao tráfico de pessoas, o membro do Ministério Público ou o delegado de polícia poderão requisitar, mediante autorização judicial, às empresas prestadoras de serviço de telecomunicações e/ou telemática que disponibilizem imediatamente os meios técnicos adequados – como sinais, informações e outros – que permitam a localização da vítima ou dos suspeitos do delito em curso. § 1º - Para os efeitos deste artigo, sinal significa posicionamento da estação de cobertura, setorização e intensidade de radiofrequência. § 2º - Na hipótese de que trata o caput, o sinal: I – não permitirá acesso ao conteúdo da comunicação de qualquer natureza, que dependerá de autorização judicial, conforme disposto em lei; II – deverá ser fornecido pela prestadora de telefonia móvel celular por período não superior a 30 (trinta) dias, renovável por uma única vez, por igual período; III – para períodos superiores àquele de que trata o inciso II, será necessária a apresentação de ordem judicial. § 3º - Na hipótese prevista neste artigo, o inquérito policial deverá ser instaurado no prazo máximo de 72 (setenta e duas) horas, contado do registro da respectiva ocorrência policial. § 4º Não havendo manifestação judicial no prazo de 12 (doze) horas, a autoridade competente requisitará às empresas prestadoras de serviço de telecomunicações e/ou telemática que disponibilizem imediatamente os meios técnicos adequados – como sinais, informações e outros – que permitam a localização da vítima ou dos suspeitos do delito em curso, com imediata comunicação ao juiz.

de que se trata de matéria sujeita à reserva constitucional de jurisdição, a um só tempo confirma a necessidade de prévia autorização jurisdicional para aquelas diligências que afetem a esfera de proteção da intimidade do investigado, quando ele fizer uso lícito do aparelho ou equipamento e não houver consentido voluntariamente com a medida, assim como também confirma a necessidade de prévia previsão legal para a utilização dessas tecnologias como meios de obtenção de prova, sob pena de a prova obtida ser considerada ilícita, especialmente quando for em desfavor do investigado.

3. A infiltração por *malware* nas investigações informáticas

"Norma social que é, o direito não surge à toa na sociedade, mas para satisfazer as imprescindíveis urgências da vida. Ele é fruto das necessidades sociais e existe para satisfazê-las, evitando, assim a desorganização" (Neto, 2008, p. 412).

Como é sabido, a sociedade está sempre em constante evolução e o direito não pode ficar alheio a essas transformações sociais, mas acompanhá-las, ainda que não consiga alcançar a mesma velocidade.

A complexidade da atual sociedade, na qual a conectividade e a informatização potencializam oportunidades e capacidades de desenvolvimento humano, também carrega consigo incertezas, riscos e inseguranças que impactam o âmbito jurídico e, em especial, o processo penal.

Não há dúvida que, no cenário atual, para além dos meios tradicionais de investigação criminal, a investigação informática, assentada no uso de recursos tecnológicos, se faz necessária e, muitas vezes, imprescindível para que o Estado consiga cumprir o seu compromisso de único detentor do direito de punir.

Essa necessidade é facilmente compreensível em razão da utilização crescente das modernas ferramentas tecnológicas e, também, de meios técnicos criados originalmente para fins de proteção de dados e segurança cibernética, de maneira subversiva, por organizações criminosas ou mesmo individualmente por quem tenha o único propósito de praticar crimes.

Nesse sentido, os sistemas operacionais de última geração utilizados nos *smartphones*, *tablets* e demais equipamentos informáticos, de uso cada vez mais comum no cotidiano da sociedade atual, utilizam técnicas de criptografia de ponta a ponta que garantem a confidencialidade dos dados ou comunicações, através da codificação da informação de modo que só o emissor e o receptor consigam decifrá-la, tornando-a ininteligível para quem não detenha o código de acesso.

A criptografia de ponta a ponta está presente em praticamente todas as plataformas modernas de mensagens e comunicações eletrônicas (*Whatsaap, Facebook Messenger, Instagram, Google Allo, Skype*, dentre outros) e visa originalmente garantir a segurança dos dados e das comunicações, isto é, a sua confidencialidade e privacidade (Indovina, 2018).

No entanto, essas técnicas de encriptação de dados e comunicações, indubitavelmente necessárias à garantia da privacidade, constituem obstáculos ao acesso a uma enorme quantidade de dados que circulam no ambiente digital, com grande potencial de se identificarem fontes de provas passíveis de utilização na investigação e no processo penal, os

quais somente são acessíveis por ato voluntário do usuário/detentor ou por meios intrusivos, como a apreensão de dispositivos ou a interceptação dos fluxos de comunicação.

Vale ressaltar que, em alguns casos, até mesmo a apreensão do dispositivo físico (*smartphones*, *tablets* e outros equipamentos informáticos) não será suficiente à obtenção dos dados nele contidos. Basta, para tanto, que o usuário se negue a fornecer a senha de acesso, uma vez que o investigado não é obrigado a produzir prova contra si mesmo (princípio *nemo tenetur se detegere*) e não se disponha de programa capaz de quebrar a senha criptografada.

Ademais, há de se considerar o uso massivo da computação em nuvem que garante o armazenamento de dados, a utilização *online* de tecnologias e recursos disponibilizados por grandes provedores, sem a necessidade de alocação de dados e arquivos em dispositivo do usuário (Indovina, 2018), o que torna inútil a apreensão do equipamento pertencente ao investigado, exigindo-se, assim, o uso de meios de infiltração nesse ambiente digital.

Não se pode olvidar, ainda, da utilização da *deep web* (rede profunda), considerada a parte "escondida" da internet por permitir o acesso à rede mediante o uso de navegador não indexado, impedindo-se a identificação do endereço de IP do usuário. Essa rede vem sendo utilizada por organizações criminosas para a prática de vários crimes, a exemplo de tráfico de drogas, tráfico de armas, pornografia infantil, etc. (Palmieri, 2018), cujas infrações e seus autores não são alcançáveis sem o uso pelo Estado de meios investigativos tecnológicos.

Todavia, a aplicação de recursos tecnológicos nas investigações criminais, ao tempo em que se demonstra inevitável, não pode ser realizada desacompanhada das correspondentes balizas legais que possam estabelecer o devido equilíbrio entre a necessidade de eficiência da atividade investigativa e a tutela individual dos direitos fundamentais do investigado.

Dito isto, não obstante as mudanças sociais tragam a necessidade de segurança, estas impõem também a utilização de novas tecnologias de informática, especialmente por métodos ocultos, no entanto, seu emprego deve ser realizado atendendo a limites que garantam a preservação do núcleo essencial dos direitos individuais, sob pena de transformarem-se em meios de controle absoluto das pessoas.

Daí a importância de discutir a infiltração por *malware* nas investigações informáticas, o que foi feito neste terceiro capítulo apresentando-se conceitos, modalidades e distinções entre os *malwares*; o *malware* do Estado e o conflito entre a liberdade probatória e a legalidade dos métodos inovadores de investigação criminal; expondo a experiência do direito comparado; discutindo o recurso ao *malware* e a intromissão nos direitos fundamentais, a exemplo do direito fundamental à reserva da intimidade da vida privada, direito ao segredo das

comunicações, direito à autodeterminação informacional, direito à integridade e direito à confiabilidade dos sistemas informáticos.

3.1. *Malware*: conceitos, modalidades e distinções

O termo *malware* é oriundo da combinação das palavras em inglês *malicious software* que, traduzido para o português, quer dizer programa malicioso. No âmbito da informática, utiliza-se o termo para se referir a qualquer tipo de programa que pode provocar danos aos dados armazenados, aos sistemas e aos próprios dispositivos informáticos (Alves, 2017).

Há, na realidade, uma variedade de *softwares* maliciosos, cada um com características e limites próprios, tratando-se o *malware* de um termo geral que compreende todas essas categorias, as quais estão constantemente sujeitas a mutações provenientes da evolução tecnológica, mas que têm em comum a finalidade intrusiva, de modo clandestino, com o objetivo de alguma maneira comprometer as funções do dispositivo ou sistema infectado (Ramalho, 2013).

Não obstante a sua amplitude significativa, o *malware* pode ser definido, em síntese, como todo o tipo de programa instalado clandestinamente por terceiros em um sistema de processamento de dados, com vista a comprometer as suas funções, de modo a transpor os seus controles de acesso e, assim, permitir que o invasor tenha amplo acesso ao sistema corrompido e, com isso, consiga remotamente acessar as informações, arquivos ou comunicações nele contidas, monitorizar a sua atividade em tempo real, desativar ou ativar as suas funcionalidades (áudio, vídeo, teclado, *mouse*, microfone, câmera, *email*, *web*, etc) e apropriar-se, eliminar e/ou alterar dados informáticos (Ramalho, 2013).

No mesmo sentido, de acordo com a lição de Torre (2015), o *malware* consiste em um software espião que, uma vez instalado clandestinamente em um sistema informático específico, permite que o invasor assuma o controle, tanto em termos de downloads quanto em termos de envio de dados e informações de caráter digital. Esse tipo de programa é constituído de dois módulos principais, um servidor e um cliente, sendo o servidor um programa que infecta o dispositivo alvo e o cliente o aplicativo que o infiltrado usa para controlar o dispositivo infectado.

Antes de procedermos à análise da utilização do *malware* como método oculto de investigação criminal em ambientes digitais, passaremos a uma breve exposição acerca das principais categorias de *malware* atualmente existentes, com o fim de facilitar a compreensão acerca das especificidades e da capacidade de alcance dessa ferramenta no âmbito investigativo

estatal. Recorda-se, mais uma vez, que as funcionalidades desses *softwares* estão sujeitas a constantes mutações decorrentes da incessante evolução tecnológica, notadamente no campo das comunicações eletrônicas.

Dentre os tipos de *malware* mais comumente conhecidos, têm-se os vírus que recebe essa denominação porque age à semelhança de um vírus biológico comum, pois além de infectar o dispositivo para o qual foi programado, espalha-se facilmente para outras máquinas que estejam em rede. Um vírus é um software malicioso anexado a um documento ou arquivo que oferece suporte a macros para executar seu código e se espalhar de um *host* para outro. Depois de baixado, o vírus ficará inativo até que o arquivo seja aberto e em uso. Os vírus são projetados para interromper a capacidade de operação de um sistema. Como resultado, os vírus podem causar problemas operacionais significativos e perda de dados (Cupa, 2013).

Por sua vez, os *worms* são *softwares* maliciosos que se replicam e se espalham rapidamente para qualquer dispositivo da rede. Ao contrário dos vírus, os *worms* não precisam de programas hospedeiros para se disseminar. Um *worm* infecta um dispositivo por meio de um arquivo baixado ou de uma conexão de rede antes de se multiplicar e se dispersar a uma taxa exponencial. Como os vírus, os *worms* podem interromper gravemente as operações de um dispositivo e causar perda de dados (Ramalho, 2017).

Os vírus *trojans*, também conhecidos como cavalos de tróia, são disfarçados como programas de *softwares* úteis. Mas, depois que o usuário faz o *download*, o vírus *trojan* pode obter acesso a dados confidenciais e depois modificar, bloquear ou excluir estes mesmos dados. Isso pode ser extremamente prejudicial ao desempenho do dispositivo. Ao contrário dos vírus e *worms* normais, os vírus de *trojan* não são projetados para se auto-replicar (Wild, 2016).

A seu turno, o *spyware* é um *software* malicioso executado secretamente em um computador e reporta a um usuário remoto. Em vez de simplesmente interromper as operações de um dispositivo, o *spyware* visa informações confidenciais e pode conceder acesso remoto a predadores. O *spyware* é frequentemente usado para roubar informações financeiras ou pessoais. Um tipo específico de *spyware* é um *keylogger*, que registra as teclas digitadas para revelar senhas e informações pessoais (Araújo, 2018).

Já o *adware* é um *software* malicioso usado para coletar dados sobre o uso do seu computador e fornecer anúncios apropriados para suas potenciais vítimas. Embora o *adware* nem sempre seja perigoso, em alguns casos o *adware* pode causar problemas ao seu sistema. O *adware* pode redirecionar seu navegador para sites inseguros e pode até conter *trojans* e *spyware*s. Além disso, níveis significativos de *adwares* podem tornar o sistema invadido

visivelmente lento. Como nem todo *adware* é malicioso, é importante ter uma proteção que verifique esses programas de maneira constante e inteligente (Wild, 2016).

Um *botnet* - abreviação de rede de robô - envolve cibercriminosos usando *malwares* para sequestrar secretamente uma rede de máquinas. Embora não seja um *malware* em si, essas redes geralmente são construídas infectando dispositivos vulneráveis (Araújo, 2018).

Cada uma das máquinas fica sob o controle de uma única operação de ataque, que pode emitir comandos remotamente para todas as máquinas infectadas a partir de um único ponto. Ao emitir comandos para todos os computadores infectados na rede zumbi, os invasores podem realizar campanhas coordenadas em grande escala, incluindo ataques DDoS, que aproveitam o poder do exército de dispositivos para inundar uma vítima com tráfego, sobrecarregando seu *site* ou serviço (Cupa, 2013).

Outros ataques comuns realizados por *botnets* incluem campanhas de anexo de *e-mail*, os spams, que também podem ser usadas para recrutar mais máquinas para a rede - e tentativas de roubar dados financeiros, enquanto *botnets* menores também têm sido usados em tentativas de comprometer alvos específicos (Ramalho, 2017).

Os *botnets* são projetados para permanecerem silenciosos para garantir que o usuário não perceba que sua máquina está sob o controle de um invasor. À medida que mais dispositivos se conectam à Internet, mais dispositivos se tornam alvos de *botnets* (Alves, 2017).

O *ransomware* é um software malicioso que obtém acesso a informações confidenciais dentro de um sistema, criptografa essas informações para que o usuário não possa acessá-las e, em seguida, exige um pagamento financeiro para que os dados sejam liberados. O *ransomware* geralmente faz parte de um esquema de *phishing*. Ao clicar em um *link* disfarçado, o usuário baixa o *ransomware*. O invasor continua criptografando informações específicas que só podem ser abertas por uma chave matemática que apenas ele conhece. Quando o invasor recebe o pagamento, os dados são desbloqueados (Araújo, 2018).

Existe, ainda, o *malware* sem arquivo é um tipo de programa residente na memória. Como o termo sugere, é um *malware* que opera a partir da memória do computador da vítima, não de arquivos no disco rígido. Como não há arquivos para verificar, é mais difícil de detectar do que o *malware* tradicional. Isso também torna a perícia mais difícil porque o *software* malicioso desaparece quando o computador da vítima é reiniciado (Alves, 2017).

No passado, antes da disseminação da *World Wide Web*, o *malware* e os vírus precisavam ser manualmente entregues por meio de disquete ou CD Rom. Em muitos casos, o *malware* ainda é entregue por meio de um dispositivo externo (*pen drive*), embora hoje em dia seja mais provável que seja entregue por uma unidade *flash* ou *stick* USB. Existem casos de *pen drives*

deixados em estacionamentos fora das organizações visadas, na esperança de que alguém pegue um por curiosidade e o conecte a um computador conectado à rede. No entanto, mais comum agora é o *malware* entregue em um *email* de *phishing* com cargas distribuídas como um anexo de *email* (Wild, 2016).

A qualidade das tentativas de *email* de *spam* varia amplamente - alguns esforços para entregar *malware* envolverão os invasores com esforço mínimo, talvez até mesmo enviando um *email* contendo nada além de um anexo nomeado aleatoriamente. Nesse caso, os invasores esperam arriscar em alguém ingênuo o suficiente para simplesmente seguir em frente e clicar em anexos de *email* ou *links* sem pensar nisso - e que eles não tenham nenhum tipo de proteção contra *malware* instalada (Cupa, 2013).

Com a evolução tecnológica e, em consequência, a evolução e especialização da criminalidade, o *malwares*, até então usados pelos criminosos, passaram também a ser usados pelo Estado com objetivo diverso, qual seja, o de desvendar crimes cometidos na internet e fora dela (Alves, 2017).

Segundo Mendes, citando Ortiz Pradillo, o *malware* "quando utilizado pelo Estado se trata de instrumento sofisticado, um programa informático utilizado por agentes estatais que possui capacidade de interceptação e gravação em tempo real de dados transmitidos, recebidos ou armazenados em equipamentos eletrônicos" (Ortiz Pradillo, 2012 *apud* Marques, 2020, p. 163).

Ao contrário de seu uso criminoso, e embora a denominação possa soar pejorativa, o *software* malicioso, ou simplesmente o *malware*, utilizado para a investigação criminal não se propõe a destruir ou danificar dados, mas interceptar e capturar informações importantes à obtenção de provas digitais essenciais ao esclarecimento de crimes graves.

O *malware* estatal é uma ferramenta multifacetada capaz de controlar plenamente o instrumento alvo. Uma vez inoculado no sistema, permite que o agente invasor assuma o controle do dispositivo infectado e atue remotamente, sem o conhecimento do investigado, permitindo realizar captura de tela, acessar dados armazenados no disco rígido e extrair cópias, ativar e desativar microfone e câmera de vídeo, localizar geograficamente o dispositivo, bem como interceptar mensagens e comunicações criptografadas (Calavita, 2020).

Conforme a lição de Griffo (2020) o investigador, no uso dessa ferramenta investigativa tecnológica, consegue decifrar tudo o que se digita no teclado; acompanhar o que aparece na tela; monitorar a navegação na internet; acessar os dados e arquivos contidos no disco rígido ou guardados na nuvem e deles extrair cópias; acessar aplicativos de mensagens e e-mails; captar os SMS já recebidos e enviados e interceptá-los em tempo real; interceptar

conversas telefônicas e/ou fluxos de comunicações em aplicativos de chamadas de voz e vídeo; ativar o microfone e a câmera do dispositivo e, com isso, realizar interceptações ambientais e captar imagens.

Trata-se, assim, de um método oculto de investigação criminal, que se utiliza de técnicas de inoculação ou mascaramento capazes de evitar que sejam detectados pelos sistemas antivírus do dispositivo onde é alocado, criando-se um portal de acesso (backdoor) que possibilita uma comunicação oculta e remota entre o centro de comando da investigação e o dispositivo monitorado (Indovina, 2018).

Esses programas podem ser introduzidos no dispositivo alvo de diferentes maneiras. Podem ser inseridos manualmente ao equipamento por meio de qualquer suporte físico removível (CD, unidade *flash* ou *stick* USB, pen-drive, HD externo) ou de maneira remota, por *email* ou via *web* (internet). O mais comum, no entanto, é a instalação remota (*on line*) muitas vezes com a utilização de técnicas de engenharia social para facilitar a contaminação (Indovina, 2018).

Considerando a variedade de categorias de *malware* e o potencial técnico multifacetado desse instrumento, a doutrina costuma distinguir o uso de *malware* estatal para fins de investigação criminal em dois grandes modos de operação: a pesquisa *online* e a vigilância *online*.

A pesquisa *online* inclui os programas que permitem fazer cópias, integral ou parcial, das unidades de memória do sistema informático alv. Nessa modalidade, os dados e arquivos podem ser capturados e transmitidos em tempo real ou em intervalos pré-estabelecidos aos órgãos de investigação, de forma remota (Griffo, 2020).

Por sua vez, os programas que se enquadram na modalidade de vigilância *online* permitem interceptar o fluxo de informações e comunicações entre os periféricos (microfone, *screen*, teclado, *webcam*) e o processador do dispositivo infectado. Por esse meio, possibilita-se que a central de controle da investigação, remotamente, monitore e capture tudo o que é exibido na tela do dispositivo (*varenyky torjan*), bem como o que é digitado no teclado (*keylagger*) ou falado no microfone ou, ainda, as imagens da câmera. São *softwares* que conseguem interceptar o fluxo da informação tecnológica, captando todos as informações e comunicações trocadas ou mensagens digitadas (Griffo, 2020).

No campo da aplicação prática dessa inovadora ferramenta de investigação criminal, têm havido inúmeras intervenções jurisprudenciais de diferentes Estados – como se verá adiante – com o objetivo de esclarecer vários problemas relativos à natureza jurídica ou qualificação das diferentes potencialidades investigativa-tecnológicas desse instrumento de obtenção de prova no âmbito digital.

Busca-se, dentre outros aspectos, definir o que é uma atividade de interceptação, que tipos de dados podem ser encontrados em um único dispositivo e se a captura e/ou interceptação desse fluxo de informações e comunicações tecnológicas podem ser comparadas ou não com meios de investigação ou de obtenção de prova análogos já presentes no ordenamento jurídico dos Estados, bem como a utilidade probatória do material recolhido por meio da utilização do *malware*.

Não custa relembrar que, por meio do uso de *software* espião estatal, pode-se realizar interceptações telemáticas (fluxo de comunicações em sistemas de informática e telemática); interceptações ambientais (captação de áudio em tempo real); monitoramento e gravação de vídeo; acompanhamento e localização geográfica do dispositivo via GPS; além de pesquisa e recolha de dados e arquivos armazenados nas unidades de memória ou salvos em nuvem (busca *online*).

É extensa a amplitude investigativa a partir da utilização do *malware* em dispositivos informáticos e o alcance desse recurso, não se limitando apenas às buscas *online*. Com o *malware* é possível a realização de monitoramento *online*, captação ambiental com gravação de áudio e vídeo do investigado, interceptação de dados telemáticos, além da obtenção de geolocalização dos dispositivos informáticos (Mendes, 2013).

No caso da gravação de vídeo (videovigilância), segundo Mendes (2013) esta pode ocorrer de duas formas: registro do comportamento comunicativo, que se constitui em uma nova forma de interceptar a comunicação entre pessoas presentes. Nessa modalidade de registro, a captação se dá a partir do registro do áudio e vídeo, demonstrando-se lesivo à direitos da personalidade a exemplo da privacidade. A segunda, a seu turno, refere-se ao vídeo registro de comportamento não comunicativo. Esta definição requer que os espaços onde o registro é efetivado sejam diferenciados. É importante distinguir entre a investigação por vídeo em domicílio, em local reservado ou em espaço público. A importância destas distinções é, indubitavelmente, as consequências que podem ser relacionadas ao material coletado.

A investigação via acesso à geolocalização dos dispositivos informáticos também se mostra extremamente invasiva, especialmente quando o dispositivo de geolocalização é móvel, pois a localização do usuário é demonstrada a todo momento, impactando também no direito à privacidade (Bene, 2014).

É esta invasão à privacidade que faz com que a legalidade do uso do *malware* por parte do Estado seja constantemente questionada conforme será visto a seguir.

3.2. O *malware* do Estado, entre a liberdade probatória e a legalidade dos métodos inovadores de investigação criminal

Consoante destacado no capítulo anterior, em termos gerais, a prova é uma operação que visa verificar qualquer proposição ou hipótese, para determinar se tal é verdadeira ou falsa, a partir da coleta de elementos que confirmem ou neguem aquela asserção a respeito de um fato que interessa ao julgamento.

No âmbito do processo criminal, a prova assume ainda mais importância, "pois só a prova cabal do fato criminoso é capaz de superar a presunção de inocência do acusado, que representa a maior garantia do cidadão contra o uso arbitrário do poder punitivo" (Gomes Filho, 2005, p. 303).

Dentre os variados sentidos atribuídos à prova no processo penal, convém rememorar a distinção que se faz entre os *meios de prova* e os *meios de investigação de prova*. Os primeiros se referem aos instrumentos utilizados pelas partes para introduzir no processo as fontes de provas das quais se obtêm os elementos destinados à formação do convencimento judicial. Já os *meios de investigação*, *meios de pesquisa* ou *meios de obtenção* de prova se referem aos procedimentos ou atividades empregados na busca por elementos de informação e fontes de provas, estando originalmente relacionados à atividade de investigação criminal.

Da leitura do CPP brasileiro, percebe-se que, no título referente à prova, consta um rol de meios de prova que podem ser utilizados no processo penal, pouco ou quase nada apresentando acerca dos meios de investigação ou de obtenção de prova[63]. Por sua vez, no título que trata do inquérito mais uma vez o CPP brasileiro é lacunoso quanto aos meios de investigação, trazendo um comando genérico no sentido de determinar à autoridade policial, logo que tiver conhecimento da prática de crime, "colher todas as provas que servirem para o esclarecimento do fato e suas circunstâncias"[64].

Diante desse cenário legislativo, debate-se doutrinária e jurisprudencialmente se a legislação brasileira impõe obediência à estrita legalidade da prova, somente admitindo as denominadas *provas típicas* ou *nominadas*, assim entendidas como aquelas cujos meios estejam previamente catalogados e regulados por lei ou acolhe a liberdade da atividade probatória,

63 Os meios de prova são previstos nos artigos 158 a 250 do CPP. No rol, consta a busca e apreensão, considerada pela doutrina não um meio de prova, mas um meio de investigação (Lopes Júnior, 2016). Os meios especiais de investigação de prova, como p. ex., interceptação telefônica, infiltração de agentes, delação premiada, entre outros, são previstos em legislações apartadas.

64 Cf. artigo 6º, inciso III, do CPP.

admitindo-se as intituladas *provas atípicas* ou *inominadas,* isto é, aquelas provenientes de meios não contemplados na lei.

Ao tratar dessa distinção entre provas típicas ou atípicas, a doutrina se refere especificamente a regulamentação em lei ou sua ausência de determinados *meios de prova* que não se assemelham aos *meios de investigação ou de obtenção de prova*, como acima destacado.

Há quem entenda que o rol de meios de prova apresentado no CPP deve ser considerado taxativo, constituindo as regras probatórias normas de garantia, o que impõe que a atividade probatória seja informada pela obediência à estrita legalidade (Gomes Filho, 2009). Nesse sentido, Gomes Filho (2005) imputa que as fontes de provas são limitadas, sendo difícil imaginar meios de prova diversos daqueles já relacionados pelo legislador. Para o autor, mesmo os meios resultantes do desenvolvimento tecnológico se reduziriam sempre às noções de documento ou perícia, devendo, assim, submeter-se às regras legais atinentes a tais modalidades.

A aduzida legalidade probatória deveria, então, conduzir à *inadmissibilidade* dos elementos resultantes de meio de prova não previstos no ordenamento jurídico e, ainda com mais rigor, levar à *nulidade* dos elementos quando introduzidos por procedimento diverso daquele previsto em lei para o meio de prova constante no rol legal e efetivamente utilizado pela parte (Gomes Filho, 2005). No último caso, não se poderia admitir a utilização do chamado *reconhecimento fotográfico*, vez que a lei processual só admite o reconhecimento pessoal (art. 226 do CPP), mediante o atendimento de regras procedimentais previamente estabelecidas[65].

Ousamos, contudo, discordar dessa visão que impõe a estrita tipicidade legal dos meios de prova. Não seria razoável exigir que o legislador definisse taxativamente todos os meios de prova possíveis de serem utilizados no processo, sob pena de impedir que a prova processual acompanhasse a evolução social, tornando-se rapidamente obsoleta.

Assim, embora não haja uma previsão legal específica da liberdade probatória, como ocorre no Direito Processual Civil (art. 332 do CPC), a interpretação do princípio do livre convencimento motivado (art. 155 do CPP) conjugado com as limitações das proibições probatórias, deve conduzir à autorização da "liberdade probatória" no processo penal condicionada à estrita observância dos limites constitucionais e processuais da prova. Dito de

65 Não é esse o entendimento consolidado na jurisprudência brasileira, que admite a utilização do reconhecimento fotográfico a título de prova inominada, isto é, por meio anômalo, desde que ratificado em juízo. Nesse sentido, STJ, Habeas Corpus 216.902 SP (2011/0202104-0). Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/24348806/habeas-corpus-hc-216902-sp-2011-0202104-0-stj/inteiro-teor-24348807/amp.

outra forma, a atividade probatória está submetida ao princípio da legalidade, do que decorre que a prova penal deve ser produzida nos termos da lei, admitindo-se, todavia, o recurso a meios de prova atípicos, quando a lei se revele insuficiente e não haja obstáculo constitucional e/ou legal para a utilização desse meio.

Por conseguinte, em regra, devem ser utilizados os meios de prova tipificados na legislação processual penal. Contudo, excepcionalmente, é possível admitir-se a produção das intituladas provas atípicas ou inominadas constituídas por meios não previstos em lei, desde que não subvertam a forma estabelecida para uma prova típica e, ainda, conservem estrita conformidade com as regras constitucionais e processuais atinentes à prova penal, isto é, não sejam proibidas[66] (Lopes Junior, 2016).

Na mesma linha, na visão de Ramalho (2017), o recurso a novos meios de prova não catalogados na legislação (prova atípicas) deve implicar na utilização de instrumentos probatórios efetivamente não previstos na lei e não no uso de procedimentos diversos dos já legalmente disciplinados. Ademais, além de excepcional, a prova atípica deve ser encarada como subsidiária da prova típica, o que implica que o recurso à prova inominada somente será válido quando os meios previstos em lei se revelem, abstratamente, inaptos à comprovação dos fatos ou, concretamente, inúteis ou impraticáveis.

Desse modo, a "liberdade probatória" aqui sustentada não é absoluta, mas moderada pelos limites constitucionais e legais que proíbem a produção de prova que viole os direitos fundamentais do investigado/acusado. Daí que a Constituição Federal preconiza expressamente que são inadmissíveis, no processo, as provas obtidas por meios ilícitos (art. 5º, LVI), comando corroborado pela legislação processual penal, segundo a qual são inadmissíveis, devendo ser desentranhadas do processo, as provas ilícitas, assim entendidas as obtidas em violação a normas constitucionais ou legais (art. 157 do CPP).

Admitida essa "liberdade probatória moderada" (ou legalidade mitigada) quanto aos meios de prova, que se destinam à formação dos elementos destinados à avaliação judicial da culpa criminal, o que dizer quanto aos meios de investigação ou de obtenção de prova, constituídos de variados mecanismos para se chegar às fontes de prova? Estariam estes incluídos na liberdade probatória, admitindo-se a utilização de métodos não previstos em lei, ou ao princípio da legalidade estrita, somente se permitindo o uso de meios investigativos previamente enumerados em lei?

66 Na legislação portuguesa, o artigo 125º do CPP português dispõe expressamente que "são admissíveis as provas que não forem proibidas por lei", admitindo, portanto, o uso de meios não tipificados expressamente na legislação processual penal.

Antes de tentarmos buscar uma resposta a esse questionamento, é preciso relembrar que, entre os inúmeros meios de investigação criminal, há aqueles menos invasivos – a exemplo da colheita de depoimentos de testemunhas e da apreensão de objetos no local do crime –, que pouco interferem na esfera dos direitos fundamentais da pessoa investigada, e outros, por sua vez, que são especialmente invasivos, isto é, interferem de maneira expressiva no conjunto de direitos fundamentais do investigado, especialmente quanto à intimidade.

É certo que os direitos fundamentais não se revestem de caráter absoluto, mas são dotados de aplicação imediata (art.5º, parágrafo 1º, CRFB/88) e, como tal, toda e qualquer intromissão do Estado em tais direitos carece de um fundamento legal (reserva de lei autorizadora) e atendimento à proporcionalidade, devendo-se preservar o núcleo essencial do direito atingido[67].

Aliás, toda e qualquer restrição aos direitos fundamentais deve ter fundamento na própria Constituição, seja diretamente no próprio texto constitucional, seja por cláusulas de reserva explícitas (quando atribui ao legislador infraconstitucional uma competência de restrição), seja restrição tacitamente constitucional, ou seja, não expressamente autorizada na Constituição, mas que decorre da própria necessidade de convivência prática das diversas posições constitucionais (Canotilho, 2003).

Acrescenta-se, ainda, que a própria restrição aos direitos fundamentais encontra limites. São, por assim dizer, os limites dos limites, cuja análise, segundo Canotilho (2003, p. 451), é a "3ª instância do procedimento da restrição de direitos". Assim, a lei restritiva deverá estar não só em conformidade formal, mas também material com o texto constitucional, o que impõe a observância do núcleo essencial do direito fundamental e do postulado da proporcionalidade.

Daí porque, no âmbito do Direito Penal Material, somente a lei pode criar tipos penais incriminadores e definir suas penas, segundo norma expressa da Constituição Federal, que dispõe em seu art. 5º, inciso XXXIX: "não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal" (Brasil, 1988). Mais do que o mero sentido formal, impõe-se ao

67 Nesse sentido é a jurisprudência do STF, Pleno, RMS 23.452/RJ, Relator Ministro Celso de Mello, DJ de 12.05.2000, p. 20: "OS DIREITOS E GARANTIAS INDIVIDUAIS NÃO TÊM CARÁTER ABSOLUTO. Não há, no sistema constitucional brasileiro, direitos ou garantias que se revistam de caráter absoluto, mesmo porque razões de relevante interesse público ou exigências derivadas do princípio de convivência das liberdades legitimam, ainda que excepcionalmente, a adoção, por parte dos órgãos estatais, de medidas restritivas das prerrogativas individuais ou coletivas, desde que respeitados os termos estabelecidos pela própria Constituição. O estatuto constitucional das liberdades públicas, ao delinear o regime jurídico a que estas estão sujeitas - e considerado o substrato ético que as informa - permite que sobre elas incidam limitações de ordem jurídica, destinadas, de um lado, a proteger a integridade do interesse social e, de outro, a assegurar a coexistência harmoniosa das liberdades, pois nenhum direito ou garantia pode ser exercido em detrimento da ordem pública ou com desrespeito aos direitos e garantias de terceiros.".

legislador que a lei incriminadora atenda ao conteúdo material da Constituição, não podendo criar tipos penais que impliquem restrição desproporcionada a direitos fundamentais. Rejeita-se, portanto, qualquer tentativa judicial de criação ou ampliação penal incriminadora incompatível com o âmago interpretativo de legislação prévia e expressa (Ferrajoli, 2010).

Por sua vez, no âmbito do Direito Processual Penal, sobretudo no domínio da investigação criminal, a compreensão da restrita legalidade prévia é muito mais complexa (Soares, 2014), em razão da característica dinâmica da relação processual continuada e do próprio dinamismo investigativo que deve acompanhar a evolução social. Em razão disso, o CPP brasileiro adota o princípio da aplicação imediata das normas processuais (*tempus regit actum*) e admite a *interpretação extensiva*, enquanto método para estabelecer o sentido e a vontade da lei, bem como o uso da *analogia*, compreendida como processo de integração do direito, pelo qual se aplica uma norma existente para determinada situação a um caso semelhante, para o qual não há qualquer previsão legal[68].

A partir da permissão legal do uso das técnicas da *interpretação extensiva* e da *analogia* às normas processuais penais pode parecer que a resposta ao questionamento feito em linhas anteriores seja simples, no sentido de admitir-se plenamente a utilização de métodos inovadores de investigação criminal, oriundos da evolução tecnológica, como seria o caso do recurso ao *malware* pelo Estado. No entanto, a solução não é tão simples quanto parece.

A regras da *interpretação extensiva* e da *analogia* na seara dos métodos de investigação ou de obtenção de prova no processo penal não podem ser empregadas de maneira incondicional ou arbitrária, notadamente quanto se está a falar de métodos atípicos que interferem nos direitos fundamentais, sob pena de propiciar a criação extralegal de graves restrições à liberdade pessoal do investigado ou a seus direitos individuais de defesa (Soares, 2014).

Assim, nas palavras de Soares (2014, p. 254):

> Há que se encontrar ponto de equilíbrio para o emprego da interpretação extensiva e da aplicação analógica no âmbito dos meios de investigação criminal, qua não lhes tire a necessária dinamicidade, mas que tampouco abra espaço para o descontrole do Estado-Persecutor.

Descarta-se, portanto, *ab initio*, qualquer hipótese de se admitir a utilização de meios investigativos inovadores (atípicos) restritivos de direitos fundamentais fora de qualquer embasamento legal (*extra legem*), isto é, completamente afastados da lei, nem tampouco *contra legem,* ou seja, que derroguem ou modifique o efeito de uma lei (Soares, 2014).

68 É o que dispõe o art. 3º do CPP: "A lei processual penal admitirá interpretação extensiva e aplicação analógica, bem como o suplemento dos princípios gerais de direito".

Propõe, então, Soares (2014) uma teoria jurídica da inovação investigativa criminal embasada nos pilares da excepcionalidade, da provisoriedade da omissão legislativa, da proporcionalidade e do controle judicial dos métodos investigativos inovadores oriundos da evolução tecnológica, para que a atividade investigativa possa acompanhar a evolução social e, assim, cumprir a eficiência reconstrutiva desejada, sem constituir intolerável desrespeito aos direitos fundamentais do investigado. Nesse sentido, adverte o autor que:

> A inovação investigativa criminal deve ser entendida como *praeter legem*, excepcional, provisória, decorrente de interpretação extensiva ou aplicação analógica e inserida em contexto de evolução legislativa progressiva. Mas, além desses requisitos, apenas pode ser tolerada à medida em que puder ser juridicamente controlada (Soares, 2014, p. 266).

Desse modo, a possibilidade prática do uso de *malware* pelo Estado, ou o recurso de qualquer outro meio investigativo que imponha ingerência aos direitos fundamentais do investigado, deve ser aferido à luz dos requisitos referidos em total harmonia com o do ordenamento jurídico constitucional e legal correspondente à espécie.

3.3. O uso de *malware* na experiência estrangeira

Nesta seção será analisada a experiência de uso de *malwares* em investigações criminais no direito comparado, a começar pela experiência norte-americana, tendo em vista que foi nos Estados Unidos que o *malware* foi utilizado pela primeira vez como ferramenta de apoio à investigação criminal.

3.3.1. A experiência norte-americana

A experiência americana tem sido interessante no que diz respeito ao uso de *malware* como meio de obtenção de provas digitais em processos criminais. O uso secreto de diferentes tipos de *malwares* pela polícia tem sido o tema de interpretação da Constituição dos EUA (Ramalho, 2014).

O primeiro caso a ser objeto de ampla atenção da mídia sobre o uso de *keyloggers* pela polícia data de janeiro de 1999 (embora, neste caso, tenha sido *malware* e *hardware* malicioso), quando, como parte de uma investigação criminal conduzida pelo FBI sobre Nicodemo S. Scarfo, um suposto membro de uma organização mafiosa suspeito de crimes relacionados

com a gestão de um negócio de jogo ilegal. O FBI descobriu que uma parte substancial dos arquivos com valor potencial de evidência foi criptografada (Mason, 2014).

Dada a necessidade de obter tais dados, e uma vez que os dados criptografados pelo *software* usado pelo suspeito só poderiam ser descriptografados com a senha (talvez conhecida apenas pelo próprio suspeito), o FBI buscou um novo mandado, desta vez para introduzir um *keylogger* diretamente no computador do suspeito, para capturar a senha e enviá-la por ondas de rádio para o FBI. O mandado foi obtido e o *keylogger*, neste caso na forma de *hardware* e *software* foi fisicamente instalado entre o teclado do suspeito e seu computador. Depois de dois meses, a senha foi finalmente obtida, permitindo assim que o FBI prendesse o suspeito e descriptografasse o conteúdo dos arquivos (Pradillo, 2013).

As compreensíveis dificuldades práticas levantadas pela instalação física de *keyloggers* em computadores suspeitos de serem usados para fins de atividade criminosa, juntamente com a crescente gravidade e âmbito internacional do crime, aumentaram o sentimento de necessidade de instalar tais mecanismos remotamente e sem *hardware* (Ramalho, 2014).

Assim, em 2001, surgiu o *Magic Lantern* (Lanterna Mágico), que era um *keylogger* que podia ser instalado clandestinamente e remotamente pela internet em um sistema de computador específico - mesmo que não estivesse fisicamente localizado nos EUA - quando pertencia a indivíduos suspeitos de serem praticantes de naturezas criminosas, nomeadamente de natureza terrorista (Pradillo, 2013).

O *Magic Lantern* pode ser instalado abrindo anexos em mensagens de *email* enviadas para o sistema do computador do suspeito ou por meio da exploração de vulnerabilidades nos sistemas operacionais. No entanto, como certos programas antivírus podem detectar o *Magic Lantern*, é relatado que o governo dos EUA solicitou algumas empresas dedicadas à comercialização desses produtos para evitar interferir fazendo uso do *Magic Lantern* (Pradillo, 2013).

O *Magic Lantern* seria substituído pelo *Computer and Internet Protocol Address Verifier* (CIPAV), um tipo de *malware* que adicionava à lista de informações coletadas, entre outros, o endereço IP e o endereço MAC ou ambos do sistema de computador do suspeito, como sua localização, a lista de programas em execução a qualquer momento, o sistema operacional usado (tipo, versão e número de série), a conta do usuário registrada no computador de destino e o último site visitado (Pradillo, 2013).

Embora existam relatos de seu uso desde 2001, o CIPAV só viria à tona em 2007, quando a mídia publicou um pedido de mandado apresentado pelo Agente Especial do FBI

Norman Sanders, solicitando o uso deste *software* para detectar o autor de várias ameaças de bomba (Mason, 2014).

No entanto, foi apenas em abril de 2011, na sequência de um pedido da *Electronic Frontier Foundation* submetido ao abrigo do *Freedom of Information Act*, que o FBI divulgou vários documentos com informações detalhadas sobre a utilização e operação do enquadramento legal e funcionamento do CIPAV. A análise de tais documentos permite que se chegue a duas conclusões preliminares: primeiro, que esse programa foi usado abundantemente, mesmo por agências governamentais que não o FBI; e, em segundo lugar, que inicialmente existiam diversos entendimentos quanto aos requisitos legais para sua admissibilidade, que atendiam, por um lado, os proponentes da inexistência de quaisquer requisitos legais para sua utilização, e, por outro lado, os defensores da necessidade de autorização judicial antes de seu uso (Ramalho, 2014).

Apesar dos efeitos que teve a divulgação desta informação, continuou o recurso ao *malware* no âmbito das investigações criminais. Uma demonstração disso pode ser encontrada na publicação, em abril de 2013, de uma ordem judicial assinada pelo juiz Stephen Smith, da Divisão de Houston do Tribunal Distrital do Sul do Texas, negando autorização judicial para o uso de um tipo não identificado de *malware* em uma investigação criminal com base no fato de que sua instalação não foi especificada corretamente e, consequentemente, haveria incerteza quanto à possibilidade de o *malware* em questão ser instalado em sistemas de computador diferentes do destinatário pretendido (Mason, 2012).

Mesmo que a decisão não mencione o nome do *malware* em questão, se fosse uma versão mais recente do CIPAV, deveria ser uma versão mais avançada do que a referida nos documentos fornecidos pelo FBI, pois inclui o seguinte às funções descritas acima: registros de atividade na Internet, incluindo *logs* de *firewall*, *caches*, histórico do navegador, *cookies*, páginas da *web* "marcadas" ou "favoritas", termos de pesquisa que o usuário inseriu em qualquer mecanismo de pesquisa da Internet, registros da *web* digitada pelo usuário endereços, nomes de usuário e senhas registradas, contatos de *email*, conteúdo de *email*, *chat* e outros *logs* de programa de mensagens, fotografias no sistema de computador de destino, entre outros (Ramalho, 2014).

Além disso, o *malware* em questão também permite o controle remoto do sistema do computador alvo, incluindo a capacidade de usar a *webcam* para tirar fotos, a fim de permitir a identificação do usuário e sua localização.

Outro país que merece ser citado, tendo em vista sua importante experiência com o uso do *malware* é a Alemanha. A experiência alemã será melhor descrita a seguir.

3.3.2. A experiência alemã

Em 2006, como parte de uma investigação criminal sobre fatos supostamente relacionados ao terrorismo, um promotor público solicitou a concessão de um mandado judicial, autorizando uma busca remota no computador de um suspeito por meio da instalação de um cavalo de Tróia. O pedido foi rejeitado em 25 de novembro de 2006, e o promotor recorreu para o Tribunal Federal de Justiça da Alemanha (*Bundesgerichtshof*), argumentando que as disposições legais incluídas no *Strafprozeßordnung* (CPP alemão), relativas à busca (física) serviria como analogia para permitir o uso de tais meios de obtenção de provas. O Tribunal Federal concluiu que essa analogia não poderia ser feita e que a utilização dessa medida carecia de fundamento legal, tornando-a inadmissível no processo penal (Rosenbach, Stark & Winter, 2011).

Menos de um mês após esta decisão, em 20 de dezembro de 2006, o Gesetz über den Verfassungsschutz em Nordrhein-Westfalen (Lei de Proteção da Constituição da Renânia do Norte-Vestfália) foi alterado e uma disposição foi introduzida no artigo § 5.2 (11), prevendo uma cláusula que concede à Autoridade de Proteção da Constituição (*Bundesamt für Verfassungsschutz*) os poderes de usar medidas para adquirir informações por meio de monitoramento secreto e outro reconhecimento da Internet, incluindo a participação secreta em bate-papos e mesmo - embora esta solução seja menos clara - acesso a *webmail* ou para *sites* com acesso restrito usando as credenciais coletadas de várias fontes, como informantes (Ramalho, 2014).

Por fim, a lei em questão também permitia o acesso secreto aos sistemas informáticos através da utilização de técnicas que possibilitassem a descoberta e exploração de vulnerabilidades técnicas para a instalação de *software* malicioso. O *malware* em questão permitiria então a essa autoridade espionar, monitorar e analisar conteúdos, bem como controlar os sistemas informáticos afetados - embora a aplicabilidade desta medida se limitasse às funções da Autoridade de Proteção da Constituição, conforme previsto no § 3º da Lei de Proteção da Constituição da Renânia do Norte-Vestfália (Rosenbach, Stark & Winter, 2011).

Um recurso foi apresentado perante o Tribunal Constitucional Federal Alemão. Em 27 de fevereiro de 2008, o tribunal chegou a uma decisão. Em primeiro lugar, considerou a questão à luz de três direitos fundamentais: (i) o direito ao sigilo da correspondência, correio e telecomunicações, (ii) o direito à inviolabilidade do domicílio e (iii) o direito à autodeterminação informativa. No entanto, considerando-se o método pelo qual as provas foram obtidas estava em questão, argumentou-se que a proteção constitucional não se limitava

ao objeto de cada um desses direitos fundamentais. Assim, tendo em vista a necessidade de oferecer, de forma mais abrangente, a proteção constitucional em relação à integridade dos sistemas informáticos, bem como aos dados por eles armazenados e transmitidos, o tribunal consagrou o direito fundamental à garantia da confidencialidade e integridade dos sistemas de tecnologia da informação (*Grundrecht aug Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*). O direito fundamental baseia-se na dignidade humana e, sobretudo, no direito geral da personalidade (Mendes, 2013).

Depois de submeter o dispositivo em análise ao escrutínio constitucional, em particular ao recém-denominado direito fundamental, o tribunal concluiu que violava os princípios da transparência, segurança jurídica e proporcionalidade, sendo, portanto, inconstitucional. No entanto, o tribunal sugeriu uma futura formulação jurídica da utilização de tais meios de obtenção de provas de acordo com os requisitos constitucionais (Mendes, 2013).

A admissibilidade do uso de *malware* em casos de terrorismo internacional foi introduzida na lei alemã por meio do *Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt* (Lei de Defesa contra os Perigos do Terrorismo Internacional através da Polícia Criminal Federal) de 25 de dezembro 2008. Foram considerados os comentários do Tribunal Constitucional Federal, embora não para fins de ação penal, mas apenas para fins de prevenção (Rosenbach, Stark & Winter, 2011).

Em 8 de outubro de 2011, um grupo de *hackers* chamado *Chaos Computer Club* divulgou informações sobre o uso de um tipo de *malware* pela polícia alemã - comumente classificado como Trojan, mas aparentemente uma ameaça combinada - que viria a ser conhecido como *Bundestrojaner* ou *Staatstrojaner*. Esse tipo de *malware* é enviado ao sistema do computador do suspeito na forma de uma atualização de *software* aparentemente inofensiva. Após a instalação do usuário, a autoridade por trás dele é capaz de gravar chamadas VoIP (incluindo *Skype*), monitorar toda a atividade do suspeito *online*, gravar senhas, inserir dados no sistema do computador de destino e até mesmo ativar o *hardware*, permitindo o uso remoto do microfone e da *webcam* para tirar fotos e gravar sons que são posteriormente enviados às autoridades investigadoras (Ramalho, 2014).

Portanto, apesar das observações estabelecidas pelo Tribunal Constitucional Federal para o uso de *malware*, e independentemente da natureza excepcional em que se baseia legalmente, houve em relatórios de 2011 do *Bundestrojaner* sendo usado mais de cinquenta vezes, não se limitando aos casos em que é legalmente destinado (Rosenbach, Stark & Winter, 2011).

3.3.3. A experiência italiana

Na Itália, o legislador esperou mais de dez anos para regulamentar o uso de *malware* como novo instrumento investigativo por meio do Decreto Legislativo nº 216, de 29 de dezembro de 2017, que produziu alterações no Código de Processo Penal italiano que ficaram conhecidas como a "reforma de Orlando". Ainda assim, explorou apenas parte do multiforme potencial técnico que a ferramenta tecnológica oferece, regulando apenas a interceptação de comunicações entre presentes (interceptação ambiental) (Palmiere, 2018; Calavita, 2020).

Durante o longo período de silêncio legislativo e tendo em vista as necessidades pragmáticas que foram surgindo e as potencialidades técnicas demonstradas pelo *software* espião, o Judiciário italiano foi chamado a intervir em vários casos práticos ao longo de todos esses anos para resolver os problemas exegéticos do novo instrumento em relação ao ordenamento jurídico então em vigor.

Em resumo, firmou-se o entendimento jurisprudencial nas Seções Unidas do Tribunal de Cassação, no sentido de que o uso de *malware* para captura ambiental audiofônica (interceptação de conversas ou comunicações entre presentes) deveria ser incluída nos regulamentos referidos no artigo 266 do CPP italiano, limitado a processos por crime organizado e inserido em dispositivos eletrônicos portáteis (*smartphones*, *tablets*, etc.), mesmo em locais de residência privada, ainda que não sejam identificados individualmente e mesmo que não haja fundada suspeita de atividade criminosa nesses locais[69].

A jurisprudência do Supremo Tribunal italiano limitou, assim, o recurso ao *malware* estatal para os casos relacionados a crimes organizados, quando o local de interceptação for legalmente indiferente ou permitido em qualquer domicílio imprevisível, exigindo para tanto uma obrigação de motivação reforçado na decisão autorizativa, com observância também para a correta qualificação jurídica do fato.

Na esteira da jurisprudência construída no Tribunal de Cassação, o legislador italiano de 2017 – na chamada reforma de Orlando – regulamentou o uso de *software* espião somente quanto à função de interceptação de comunicações entre presentes. No entanto, a lei ampliou o âmbito da aplicação do recurso ao *malware* estatal para incluir a permissão de sua utilização nos casos de crimes comuns previstos no artigo 266, nº 1, do CPP italiano, em relação aos quais permitiu a infiltração viral em dispositivos instalados em residência privada, desde que

69 Cf. Cass., Sez. Un., 01 luglio 2016, n. 26889, Scurato, in CED n. 266905. Disponível em: http://www.archiviopenale.it/intercettazioni—cass-sez-un-1-luglio-2016-(cc-28-aprile-2016)-scurato/contenuti/6142.

haja fundada razão para crer que ali se desenvolva atividade criminosa. No caso dos crimes organizados, a norma legal manteve a autorização de uso do *malware* em qualquer caso, ou seja, independentemente da indicação do *fumus perdurantis criminis* (art. 266, nº 2-bis)[70].

A lei italiana exige que a autorização do uso de *malware* estatal seja outorgada pelo juiz das apurações preliminares, por meio de decreto fundamentado atestando a indispensabilidade da medida para as investigações de crimes graves. Em se tratando de crimes comuns, exige-se, ainda, a indicação dos locais e do tempo, ainda que indiretamente determinados, em relação aos quais é permitida a ativação do microfone (art. 267, nº 1).

Em 2019, a intitulada "lei da varredura corrupta" alargou o âmbito de atuação do *malware* estatal para permitir o seu uso nos casos de crimes praticados por funcionários públicos contra a administração pública, equiparando-os, apenas para esse fim, aos crimes de máfia, terrorismo e associações subversivas (Calavita, 2020).

Mais recentemente, houve mais uma alteração legal promovida pelo decreto legislativo nº 161, de 30 de dezembro de 2019, convertido com modificações na lei nº 7, de 28 de fevereiro de 2020, que, dentre outras mudanças, alterou o artigo 267, nº 2-bis, do CPP italiano, permitindo ao Ministério Público emitir decreto de emergência de interceptação entre presentes, mediante uso de *software* espião em dispositivo eletrônico portátil, submetido à avaliação judicial a *posteriori*, para os casos de crimes de máfia, terrorismo e de associação subversiva, bem como nos crimes praticados por funcionários públicos contra a administração pública (Calavita, 2020).

Mesmo após as alterações referidas desde a sua disciplina original em 2017, o ordenamento jurídico italiano não tratou das funções adicionais do *malware* estatal, não aderindo ao projeto de lei Quinrarelli (projeto de Lei da Câmara 4260), apresentado ao legislativo em 31 de janeiro de 2017. O projeto dividia o uso de *software* espião em três categorias de meios de investigação ou de obtenção de prova: buscas *online*, ou seja, pesquisa de arquivos armazenados no dispositivo ou guardados em nuvem; interceptações de tráfego de voz em sistemas de informática e telemática, equiparadas às interceptações telefônicas; e interceptações entre presentes, por meio da gravação de áudio e vídeo, que teriam sido submetidas à regulamentação das interceptações ambientais (Calavita, 2020).

Como se percebe, a normatização legal italiana não regulou a controversa possibilidade de utilização do *malware* para a realização de buscas *online* (pesquisa remota) que, por suas características e alcance, constitui meio investigação ou de obtenção de prova de natureza

70 Cf. Codice di Procedura Penale. Disponível em: https://lexscripta.it/codici/codice-procedura-penale.

distinta da interceptação ambiental. Nesta, o programa é utilizado para capturar o fluxo de comunicações em sistemas de informática e telemática. Já no caso da pesquisa remota em ambiente digital, o *software* se destina a permitir que o investigador acesse dados armazenados em suportes físicos e, também, aqueles que estejam guardados em nuvem (Ramalho, 2014).

Nesse ponto, a matéria continua sendo tratada pelos Tribunais italianos, cuja jurisprudência firmou-se no sentido de considerar válidos os resultados obtidos através da pesquisa remota por *malware* (busca *online*), qualificando o ato investigativo como um meio de investigação ou de obtenção de prova atípico, nos termos do art. 189 do CPP italiano, subtraindo-o da disciplina prevista para a busca tradicional (art. 365 do CPP italiano) – que garante o direito do investigado de ser notificado e acompanhado por advogado de sua confiança –, bem como da regulamentação legal da interceptação das comunicações informáticas ou telemáticas (art. 266-bis do CPP italiano).

Ainda em 2009, a Corte Suprema italiana decidiu que é legítima a busca *online* por meio de programa espião (*malware*), para recolher documentação informática armazenada em dispositivo eletrônico pessoal utilizado pelo investigado, ao reputar que a atividade realizada por meio de um vírus de computador, destinada a capturar "um fluxo unidirecional de dados", isto é, uma "relação operacional entre microprocessador e vídeo do sistema eletrônico" não constituiria interceptação de comunicações, mas meio de prova atípica, afastado da disciplina prescrita no art. 266-bis do CPP italiano. Esse entendimento vem sendo reiterado por decisões posteriores da Corte Superior. Nesse sentido, Cass., sez. VI, 27 novembre 2012, Bisignani, ivi, n. 254865; Cass., sez. IV, 17 aprile 2012, Ryanair, in Cass. pen., 4 (2013), pp. 1523 ss. (Curtotti, 2017).

3.3.4. Outras experiências

Outra experiência que merece ser destacada é a da Espanha. Existe atualmente neste país legislação específica sobre a utilização de *malware* como meio de obtenção de provas em processos penais, no entanto, sobre a matéria ainda pairam controvérsias. Ilustrando este ponto com um exemplo, Ortiz Pradillo (2012) demonstra o estabelecimento, por meio de três sentenças do Supremo Tribunal da Espanha, do uso de dispositivos eletrônicos denominados IMSI *catchers* ou *Cell Site Simulators*. Estes são projetados para determinar, a partir da localização física de certos telefones móveis e sua proximidade com as antenas que fornecem uma conexão à rede telefônica, sua localização física aproximada, seu número IMSI (*International Mobile Subscriber Identity*) e o telefone móvel número associado a ele.

O Supremo Tribunal espanhol considerou que as provas obtidas a partir de tais dispositivos eram admissíveis em relação ao quadro jurídico que rege a recolha e tratamento de dados pessoais pelas forças e corpos de segurança para efeitos de aplicação da lei. No entanto, como observou Ortiz Pradillo (2012), a lei não prevê um mandado para a coleta e processamento desses dados.

Tendo em conta o disposto no artigo 22.º da Lei Orgânica 15/1999, judicialmente aplicável à recolha destes dados - qualificados pelo tribunal como dados pessoais -, e o enquadramento jurídico que rege a transmissão dos mesmos dados aos operadores telefônicos, que prevê a necessidade da precedência do mandado, pode-se tirar a conclusão bastante ilógica de que não será necessária autorização judicial quando a polícia puder, por impulso próprio, obtê-la, mas será legalmente obrigatória quando a mesma entidade exigir a cooperação de operadoras de telefonia (Mendes, 2013).

Destacando a disparidade injustificada de critérios nesta matéria, Ortiz Pradillo (2012) alerta que o entendimento jurisprudencial, segundo o qual a coleta de dados no contexto de uma investigação criminal - nunca de caráter exclusivamente exploratório - para a descoberta de um crime particularmente grave pode ser considerada proporcionada, necessária e, como tal, livre de qualquer violação dos direitos e liberdades fundamentais, podendo igualmente abrir caminho a tentativas de obtenção de dados pessoais em redes *Wi-Fi* abertas, recorrendo a *spyware* (Gercke, 2012).

Opondo-se a esta tendência da jurisprudência de se colocar no lugar do legislador e expressando sua oposição a uma interpretação que visa legitimar o uso de *malware* como meio de obtenção de provas sem qualquer disposição expressa nesse sentido, Ortiz Pradillo reconhece que é possível que a jurisprudência espanhola possa interpretar certas regras de forma a fundamentar a admissibilidade da utilização de *malware* em violação dos requisitos mínimos de legalidade e clareza estabelecidos pela CEDH (Ramalho, 2014).

Se tal acontecer na ausência da reforma do Código de Processo Penal espanhol, certos requisitos para a utilização de *malware* devem ser definidos judicialmente, os quais incluem (i) o requisito de precedência de autorização judicial; (ii) a imposição do caráter secreto do uso da medida; (iii) o estabelecimento da cooperação obrigatória de terceiros, incluindo operadoras de telecomunicações quando necessário; (iv) dever de fundamentar a decisão do tribunal; (v) o caráter excepcional da medida e respectiva aplicação apenas a crimes particularmente graves; e (vi) a recolha de forma a garantir a autenticidade e integridade das informações obtidas (Gercke, 2012).

O caminho percorrido no ordenamento jurídico espanhol parece ter sido diferente. Atualmente se discute uma reforma no nível processual espanhol, que previsivelmente levará à adoção de um novo Código de Processo Penal espanhol, efetuado por meio do que alguns chamam de Projeto de Lei Gallardón (Gercke, 2012).

O regime jurídico previsto no novo Título XI, apresentado sob o título "Registros remotos sobre equipes informáticas", parece cumprir, em geral, os requisitos propostos por Ortiz Pradillo, prevendo dever de fundamentar a legalidade da idoneidade, necessidade e proporcionalidade da medida (Ramalho, 2014).

O artigo 351.º prevê, ainda, o dever de cooperação, incluindo os fornecedores de serviços de Internet e os responsáveis pelo sistema informático ou base de dados objeto da medida[71].

Não obstante o fato de a técnica legislativa poder implicar excessiva margem de latitude para o juiz de instrução e de o conceito de "infracção de natureza particularmente grave" não ser devidamente especificado, caso a proposta em causa seja aprovada, o sistema jurídico espanhol ganhará em termos de clareza e certeza na aplicação de tais medidas (Gercke, 2012).

Na União Europeia (UE), com o aprimoramento das técnicas utilizadas para a prática do crime cibernético em escala global, vem crescendo o interesse em estabelecer instrumentos uniformes em nível internacional para lidar com essa nova forma de criminalidade. Com efeito, considerando que o estado em que opera o sujeito-alvo não pode ser aquele em que se produz o resultado típico, e visto que a aplicação desses instrumentos ainda é (ou pelo menos deveria ser) limitada pelo princípio da territorialidade da aplicação do Direito processual penal, é do maior interesse que os instrumentos considerados mais eficazes sejam estabelecidos no maior número possível de estados (Rosenbach, Stark & Winter, 2011).

Assim, em particular a partir da Convenção sobre o Cibercrime, várias iniciativas supranacionais têm se desenvolvido, com o objetivo de promover a adoção do uso de *malware* como meio de obtenção de evidências em ambiente digital. Assim, em dezembro de 2008, a Comissão Europeia e a União Internacional de Telecomunicações iniciaram a Harmonização de Políticas de TIC, Legislação e Procedimentos Regulatórios no Caribe (HIPCAR) com o objetivo de promover a uniformidade da legislação nos países da Comunidade do Caribe (CARICOM) em nove áreas em relação à tecnologia da informação. O resultado foi, possivelmente, o modelo legislativo de crimes cibernéticos e evidências digitais mais

71 Espanha. *Real Decreto de 14 de septiembre de 1882, aprobatorio de la Ley de Enjuiciamiento Criminal*. Disponível em: https://www.boe.es/biblioteca_juridica/codigos/codigo.php?id=334&modo=2&nota=0&tab=2.

detalhados que existe, que pode servir de guia para os vários estados que desejam implementá-lo (Rosenbach, Stark & Winter, 2011).

Assim, no artigo 27 que dispõe sobre o *Cybercrime* foi criada uma regra que prevê o uso de *malware* para fins de investigação criminal (software forense remoto). Consciente do caráter altamente intrusivo deste meio, a proposta introduz algumas restrições à sua aplicação, como a exigência de que as provas não possam ser obtidas de outra forma, a necessidade de autorização de um juiz ou magistrado, o dever de fundamentação a autorização e a limitação do seu âmbito de aplicação.

Esta disposição é um bom exemplo de técnica legislativa que pode ser utilizada por Estados que pretendam agregar este meio de obtenção de provas aos seus procedimentos.

Por outro lado, a UE também tem procurado - embora com pouca ênfase - fomentar o estabelecimento deste meio de obtenção de provas. Já em 2008, por ocasião da adoção da estratégia de reforço das disposições que tratam da cibercriminalidade, o Conselho de Ministros da UE anunciou que a sua estratégia para os próximos cinco anos incluiria, entre outras, ciber-patrulhas para a finalidade de rastreamento de criminosos *online* e pesquisas remotas. No entanto, com maior expressividade, foi referido no considerando 27 da Diretiva 2011/92/UE do Parlamento Europeu e do Conselho, relativa ao combate ao abuso sexual e à exploração sexual de crianças e à pornografia infantil, e que substitui o Quadro do Conselho (Ramalho, 2014).

Tendo em conta a popularidade que este meio de obtenção de provas tem vindo a acumular cada vez mais e dadas as suas vantagens óbvias, é possível que, no futuro, os Estados-Membros o estabeleçam por lei, não apenas no que diz respeito ao tratamento do abuso sexual e da exploração sexual de crianças e pornografia infantil, mas também em relação a outros tipos de crimes graves, a exemplo do terrorismo.

3.4. O caso envolvendo o aplicativo *WhatsApp* no Brasil

O *WhatsApp* é um aplicativo multiplataforma de comunicação instantânea, por meio do qual os seus usuários podem trocar mensagens instantâneas e fazer chamadas de voz e vídeo pela internet, disponível para dispositivos informáticos, como *smartphones* e computadores. O programa é um dos tantos instrumentos oriundos da transformação digital que permeia a atual sociedade da informação, responsável por proporcionar uma verdadeira revolução na dinâmica das comunicações entre as pessoas.

O alcance dessa ferramenta de comunicação digital no mundo, e em particular no Brasil, chega a números cada vez mais impressionantes. Recentemente, a empresa proprietária do aplicativo (*Facebook*) anunciou que ultrapassou a marca de 2 bilhões de usuários em todo o mundo (Loubak, 2020). No Brasil, segundo pesquisa recente, o *WhatsApp* está instalado no *smartphone* de 99% dos brasileiros, e 93% usam o aplicativo todo dia. A pesquisa também revelou que 90% dos brasileiros usam o aplicativo para enviar mensagens de texto, 81% se comunicam por áudio, e 67% utilizam a chamada de voz (Ventura, 2020).

A partir dessa amostra, não há dúvida que a quantidade de dados de informação e comunicação (mensagens de texto, documentos em arquivo digital, fotografias, vídeos, chamadas de voz e vídeo) que circula no ambiente digital por meio desse aplicativo alcança números incomensuráveis. Também não se duvida que, ao lado do uso responsável desse inovador instrumento tecnológico, seja este utilizado para facilitar, difundir ou mesmo executar condutas criminosas[72].

Em razão dessa funcionalidade multiforme do *WhatsApp* e do seu crescente alcance social, cada vez mais substituindo as tradicionais formas de comunicação (a exemplo das chamadas telefônicas), tem-se nessa plataforma uma enorme potencialidade de circular informações e dados capazes de interessar à investigação criminal e ao processo penal, para a aquisição de provas digitais essenciais à obtenção do esclarecimento de crimes.

Nessa perspectiva, juízes brasileiros, em atendimento a requerimentos do Ministério Público ou representação de autoridades policiais, passaram a determinar à empresa *Facebook* – proprietária do aplicativo – o compartilhamento de informações sobre os usuários e, mais ainda, a interceptação do fluxo de comunicações, para fins de subsidiar investigações criminais ou ações penais em curso. As decisões judiciais, quanto à finalidade de interceptação, fundamentaram-se na Lei nº 9.296/1996[73] que, no parágrafo único do art. 1º, dispõe expressamente que se aplica o mesmo tratamento legal da interceptação das comunicações telefônicas à interceptação do fluxo de comunicações em sistemas de informática e telemática,

72 Cf. Portal UOL. Bandidos criam "telemarketing do golpe"; entenda de vez invasão ao WhatsApp. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2020/02/06/bandidos-criam-telemarketing-do-golpe-para-invadir-whatsapp-saiba-evitar.htm.

73 Art. 1º A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça.

Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9296.htm.

bem como na Lei nº 12.965/2014 – Marco Civil da Internet, art. 10, § 2º[74], e art. 12[75], incs. III e IV.

No entanto, a detentora do aplicativo negou-se a atender todas as decisões judiciais proferidas em diversos Estados do País, sob a alegação de impossibilidade técnica, pois, segundo o representante do *WhatsApp*, o sistema de criptografia ponto a ponto impede que qualquer dado entre interlocutores ou grupos possa ser acessado por quem quer que seja, afirmando que nem os *hackers*[76] e nem mesmo a empresa que gerencia o aplicativo consegue interceptar esses dados[77].

Essa recusa reiterada da empresa *Facebook* levou alguns juízes brasileiros a proferirem decisões que determinavam o bloqueio do aplicativo *Whatsapp* em todo o território nacional, até que a empresa fornecesse o acesso ao conteúdo das conversas de investigados em crimes, nos anos de 2015 e 2016. O aplicativo chegou a ficar desabilitado (*off line*) no Brasil por até 24 horas, mas todas as decisões de bloqueio foram derrogadas pelas respectivos Tribunais, os quais consideraram que a determinação de bloqueio se tratava de medida desproporcional e violava as liberdades de comunicação, atingindo milhões de usuários do aplicativo alheios às investigações e processos criminais (Gomes, 2020).

Em entrevista, o magistrado autor da primeira decisão judicial que determinou o bloqueio do *Whatsapp* no Brasil – o juiz então titular da Central de Inquéritos da Comarca de Teresina/PI – justificou a aplicação da medida ao dizer que se tratava de uma forma de forçar o aplicativo a criar canais para que os policiais pudessem proceder as investigações de crimes graves que estavam sob apuração. Acrescentou, ainda, que "até pouco tempo atrás nós fazíamos interceptações telefônicas, mas hoje ninguém usa telefone [para falar], usa o

---

74 Art. 10. 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. [...]

§ 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º .

75 Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa: [...] III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.

76 Olhar Digital. (2020). *Novo malware ataca usuários de whatsapp e facebook*. Disponível em: https://olhardigital.com.br/fique_seguro/video/novo-malware-ataca-usuarios-de-whatsapp-e-facebook/101037.

77 Nesse sentido, ver Brasil. Supremo Tribunal Federal. 21ª Audiência Pública do STF. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf.

WhatsApp. Para que se possa saber o que criminosos comunicaram, onde estão, é através dos apps" (sic) (Maia, 2015).

Por sua vez, a então juíza da 2ª Vara Criminal de Duque de Caxias/RJ, que também determinou o bloqueio do *Whatsapp* no ano de 2016, ponderou que:

> Se as decisões judiciais não podem efetivamente ser cumpridas e esta informação é sempre rechaçada por peritos da polícia federal e da polícia civil que afirmam ser possível o cumprimento, como foi possível ao *Google* do Brasil, em determinada ocasião, cumprir decisões judiciais que até então alegava ser impossível, devemos então concluir que o serviço não poderá mais ser prestado, sob pena de privilegiar inúmeros indivíduos que se utilizam impunemente do aplicativo *Whatsapp* para a prática de crimes diversos (Migalhas, 2016).

O tema acabou gerando grande repercussão no País e a discussão jurídica chegou ao Supremo Tribunal Federal, por meio de ações constitucionais (ADPF 403 e ADI 5527) que questionam a constitucionalidade dos artigos 10, § 2º (1), e 12, III e IV (2), da Lei 12.965/2014 (Marco Civil da Internet), cujos dispositivos foram utilizados pelos magistrados que decretaram a suspensão temporária do aplicativo *Whatsapp* no Brasil.

Em razão da grande repercussão social do assunto e tendo em vista a complexidade da matéria, que envolve discussão extremamente técnica e de caráter multidisciplinar para além de jurídica, o STF convocou uma audiência pública que contou com a participação de representante do aplicativo *Whatsapp*, de várias instituições públicas relacionadas à investigação e perícia, bem como de associações de classe e de ciência e tecnologia habilitadas no debate. Em suma, o conteúdo do debate envolveu a discussão sobre a (im) possibilidade técnica da interceptação do conteúdo das conversas criptografadas e a (im) possibilidade do aplicativo de se adaptar à realidade jurídica brasileira (Brasil, 2017).

Em manifestação por ocasião da audiência pública, o senhor Brian Acton – co-fundador do *Whatsapp* – voltou a afirmar que a tecnologia de criptografia utilizada no aplicativo visa proteger a privacidade das comunicações entre seus usuários, permitindo que as pessoas se sintam seguras para se expressarem sem medo. Declarou que as mensagens enviadas por *Whatsapp* usam um cadeado e uma chave que só o emissor e o receptor possuem, não sendo possível interceptar o fluxo de comunicação nem mesmo pela empresa. Acrescentou, ainda, que qualquer ferramenta que permitisse o acesso da empresa à comunicação de seus usuários representaria um risco de ser utilizada por criminosos ou *hackers*. Por fim, disse que a única maneira de desativar a criptografia para apenas um usuário seria desativando a proteção para todos (Brasil, 2017).

Por outro lado, na mesma audiência, os representantes da perícia criminal da Polícia Federal e do Ministério Público Federal discordaram das justificativas apresentadas pelo mandatário do *Whatsapp*, e defenderam a possibilidade de adoção de medidas técnicas capazes de permitir a interceptação do fluxo de informações e comunicações no referido sistema tecnológico.

Nesse sentido, o perito criminal Ivo de Carvalho Peixinho defendeu que, embora a criptografia ponta a ponta impeça o servidor do *Whatsapp* de ver as mensagens de seus usuários, a interceptação telemática seria possível através da troca de chaves diferentes pelo servidor ou duplicando-se uma sessão para um terceiro. Afirmou, ainda, que a empresa pode fornecer metadados que seriam de grande valia para a resolução de investigações criminais (Brasil, 2017).

Por sua vez, o então Secretário de Cooperação Internacional da Procuradoria Geral da República também se manifestou a favor da possibilidade de interceptação do fluxo de informações e comunicações no *Whatsapp*. Destacou que, embora deva se reconhecer a importância da proteção dos dados pessoais que circulam no aplicativo – tratando-se de inquestionável direito fundamental –, deve-se ter em mente que, infelizmente esses serviços também são utilizados por criminosos e terroristas no mundo inteiro (Brasil, 2017).

Lembrou, ainda, o representante do Ministério Público Federal que a Corte Interamericana de Direitos Humanos tem reafirmado que o Direito Penal também serve como mecanismo para a proteção dos direitos humanos e, com base nisso, condenou o Brasil, em alguns dos seus últimos julgados, por não cumprir com a obrigação de investigar delitos graves cometidos em território nacional. Finalizou o seu discurso alertando que o Brasil não pode se tornar um "paraíso digital" no qual criminosos possam cometer infrações penais livremente, violando direitos fundamentais tão importantes quanto o direito à privacidade (Brasil, 2017).

Recentemente, em maio de 2020[78], o Plenário do STF iniciou julgamento conjunto das duas ações constitucionais que tramitam naquela Corte sobre o tema. Ambos os ministros relatores já proferiram seus votos no sentido de atribuir interpretação conforme à Constituição e, assim, afastar a hipótese de permitir que o Judiciário possa aplicar as penalidades de suspensão temporária e de proibição das atividades por descumprimento de ordem judicial de disponibilização de conteúdo de comunicações para fins de investigação criminal. De acordo com os votos, tais penalidades somente podem ser impostas aos provedores de conexão e de aplicativos de internet nos casos de descumprimento da legislação

78 Brasil. (2020). Supremo Tribunal Federal. *Informativo 979*. Brasília, 25 a 29 de maio de 2020. Disponível em: http://www.stf.jus.br//arquivo/informativo/documento/informativo979.htm.

brasileira quanto à coleta, guarda, armazenamento ou tratamento dos dados, bem como nos casos de violação dos direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros (Brasil, 2020).

No que se refere ao aspecto da possibilidade técnica de interceptação do fluxo das comunicações criptografadas, para fins de investigação criminal, o ministro Edson Fachin, inicialmente, destacou as premissas de que a criptografia protege os direitos dos usuários da internet, garantindo-lhes privacidade de suas comunicações, mas, paralelamente, também impõe dificuldades técnicas na apuração de crimes que gravemente violam direitos fundamentais tão importantes quanto a privacidade. Assim, ressaltou que a questão principal a se enfrentar circunscreve-se em buscar responder se o risco público representado pelo uso da criptografia justifica a restrição do direito à privacidade e segurança na internet, por meio da imposição de soluções de *software*, como, por exemplo, a proibição da criptografia ou a criação de canais excepcionais de acesso ou pela diminuição do nível de proteção (Brasil, 2020).

Em seu voto, o referido ministro relator aduziu que a resposta a esse problema depende de um rigoroso exame de proporcionalidade entre a garantia de proteção à privacidade e à liberdade de expressão por meio da criptografia e, por outro lado, a necessidade de eficiência das investigações criminais, porquanto a capacidade de monitoramento e de interceptação de mensagens é tida como uma das principais formas — e para alguns crimes até a única — de se apurar ilícitos. Nesse ponto, concluiu o ministro que o risco causado pelo uso da criptografia ainda não justifica a imposição de soluções que envolvam acesso excepcional e, portanto, assentou ser inconstitucional proibir as pessoas de utilizarem a "criptografia ponta-a-ponta". Após os votos proferidos pelos relatores, o ministro Alexandre de Moraes pediu vista das duas ações, não tendo sido ainda retomado o julgamento até o presente momento (Brasil, 2020).

Consoante os votos até então proferidos, independentemente da possibilidade técnica de criação de mecanismos tecnológicos capazes de permitir a interceptação do fluxo de informações e comunicações nos atuais aplicativos de comunicação instantânea, caso prevaleça esse entendimento pelos demais integrantes da Corte Suprema, caminha-se no sentido de proibir-se a quebra da criptografia, ainda que autorizada judicialmente e ainda que seja possível o afastamento dessa técnica de encriptação para determinado alvo de instigação criminal ou de processo penal, sem comprometer a segurança dos demais usuários.

Não podemos, porém, concordar com a solução até então adotada pelo Supremo Tribunal Federal. Com efeito, não se pode deixar de reconhecer a importância da criptografia para a navegação segura da comunicação digital, para a proteção dos dados sensíveis relativos à

intimidade das pessoas, enfim, para a proteção dos direitos fundamentais à privacidade e à liberdade de expressão, pelo que qualquer mecanismo que tenda a afastar por completo ou vulnerar coletivamente a criptografia deve ser rechaçado. No entanto, sendo possível a quebra individualizada e temporária dessa encriptação para fins de investigação criminal, nos moldes do que ocorre com a interceptação telefônica, não parece macular de maneira letal tais direitos individuais.

Caso prepondere a interpretação até então adotada pelos ministros relatores da Corte Suprema, implica concluir que as autoridades brasileiras jamais poderão ter acesso simultâneo ao conteúdo das comunicações informáticas e telemáticas criptografadas. Seria, portanto, admitir a existência de um espaço digital completamente imune à vigilância estatal, em qualquer hipótese, isto é, um ambiente de privacidade absoluta onde se possa expressar ou transmitir qualquer informação com qualquer propósito, seja lícito ou ilícito. Restaria, assim, unicamente a hipótese de infiltração digital por meio de *malware* (*software* espião), caso admitido o uso desse meio oculto de obtenção de prova, como forma de se efetuar a interceptação desse tipo de fluxo de comunicação.

3.5. O recurso ao *malware* e a intromissão nos direitos fundamentais

A instalação de *malware* é talvez o meio mais controverso de obtenção de evidências suscetíveis de serem submetidas a controle legal em um estado democrático. O alto potencial de prejuízo social que o monitoramento remoto da conduta privada de um indivíduo ao usar seu sistema de computador representa - talvez até mesmo acompanhado pela gravação de imagens e sons - é uma intrusão potencialmente violadora no núcleo intangível da intimidade pessoal. Quando combinado com a invasão de direitos fundamentais como a preservação da intimidade da vida privada, a inviolabilidade do domicílio, a confidencialidade, a imagem, a palavra e, além disso, a integridade dos sistemas de informação, é imperativo que o estabelecimento legal de uma disposição seja devidamente controlada e que as características dos meios técnicos a utilizar sejam delimitadas de forma clara e precisa, respeitando o princípio da proporcionalidade (Rodrigues, 2010).

Por isso, Palmieri (2018) chega a dizer que o *malware* estatal constitui mais do que uma "violação", sendo mais correto falar em um "ataque" ao direito fundamental à privacidade. Declara o autor que "não é por acaso que a doutrina foi tão longe a ponto de afirmar que ouvir e ler um *smartphone* beira do controle psíquico de "opiniões e pensamentos" antes de "ações e condutas" concretas (Palmieri, 2018, pp. 60-61).

Para além do direito fundamental à privacidade, o recurso ao *malware*, por suas características peculiares, complexidade e ampla capacidade de alcance enquanto ferramenta tecnológica inovadora no âmbito investigativo criminal, produz ingerência em outros direitos fundamentais, alguns dos quais reconhecidos como tais em razão do impacto da revolução tecnológica na dimensão humana da sociedade da informação, a exemplo do direito à autodeterminação informacional e o direito à integridade e à confiabilidade dos sistemas informáticos.

Ademais, não custa lembrar que os direitos fundamentais não podem constituir um catálogo fechado, mas, ao contrário, submetem-se a uma evolução contínua que acompanha o desenvolvimento crescente dos valores humanitários de cada época. Daí que não se pode descartar o surgimento de outros direitos fundamentais ao longo do tempo, além dos aqui tratados, que também possam estar relacionados com o uso do *malware* estatal. Nessa perspectiva, Barrocu (2017) menciona a elaboração de um novo direito fundamental ao respeito pelo "corpo digital". Segundo o autor, o *malware* seria comparado a um chip inserido sob a pele que permite controlar todas as ações, comunicações e até mesmo os pensamentos de um indivíduo, pelo que não seria possível separar o que pode ser utilizável no processo penal dos aspectos que são e devem necessariamente permanecer privados.

Não obstante, importa relembrar que os direitos fundamentais não se revestem de caráter absoluto, pelo que razões de interesse público ou exigências da própria necessidade de convivência das liberdades individuais autorizam, excepcionalmente, a adoção de medidas restritivas de prerrogativas individuais ou coletivas, desde que respeitados os termos constitucionais, o atendimento à proporcionalidade e a preservação do núcleo essencial do direito atingido.

Aliás, conforme já destacado em linhas pretéritas, não há como se conceber um sistema processual penal minimamente eficaz sem qualquer ingerência nos direitos fundamentais dos cidadãos. A persecução penal, na qual se inclui a investigação criminal, por si só, já representa evidente constrangimento, abalo moral e ingerência estatal na vida privada da pessoa investigada/acusada. Deve-se buscar, portanto, o justo equilíbrio baseado no rigoroso exame de proporcionalidade entre a necessidade de eficiência das investigações criminais e a garantia de proteção aos direitos fundamentais atingidos pelo recurso de *malware* estatal na atividade investigativa.

Dito isto, busca-se nesta seção relacionar o recurso ao *malware* estatal com a intromissão nos direitos fundamentais que, de maneira particular, são afetados pela utilização desse inovador meio de investigação criminal tecnológica. Nesse sentido, serão analisados: o

direito fundamental à reserva da intimidade da vida privada; o direito ao segredo das comunicações; o direito à autodeterminação informacional; e o direito à integridade e à confiabilidade dos sistemas informáticos. Inicia-se com a reserva da intimidade da vida privada.

3.5.1. O direito fundamental à reserva da intimidade da vida privada

A privacidade e a intimidade são termos com significados distintos, porém, que se inter-relacionam. Privacidade derivada do termo "privado", originária do latim *privatus*, que significa "pertencente a si mesmo, colocado à parte, fora do coletivo ou grupo", e particípio passado de *privare*, que significa "retirar de; separar". Intimidade derivada do latim *intimus*, que é um superlativo de in, "em; dentro". Assim, intimidade se refere a questões relativas ao interior da pessoa, questões essas que a pessoa não compartilha com as outras, exceto as questões relacionadas com a vida íntima. Assim, a intimidade pessoal faz parte da privacidade pessoal, sem com ela se confundir. Entretanto, "as noções de intimidade e vida privada trazem consigo uma carga emotiva que as faz equívocas, ambíguas e dificulta a precisão de seu significado" (Doneda, 2006, p. 110).

A noção de privacidade teve origem na filosofia antiga, em decorrência da distinção entre o que fazia parte do domínio público ou privado. Essa distinção é fruto da contribuição aristotélica dicotômica acerca da participação na vida política (*polis*),ou na doméstica (*oikos*). Em Política I, a *oikos* (família, casa) é definida como a forma específica de *koinwnia* (comunidade, sociedade), integrada por indivíduos de vida em comum. Porém, tal integração permite que os membros de uma *oikos* tornem-se também membros de uma *polis* (comunidade política, cidade-estado). Nessa época, os interesses do Estado sobrepujavam os interesses particulares, porém, como observa Cotrin (2006) com o declínio da participação do cidadão nos destinos da cidade e, consequentemente, na vida política grega, em virtude da invasão macedônica e o início do chamado período helenístico, a reflexão política também se enfraqueceu. As preocupações coletivas cedem lugar às preocupações individuais. Com efeito, o centro das reflexões filosóficas deixa de ser a vida pública e passa à vida privada. Assim, as principais correntes filosóficas desse período vão tratar da vida interior do homem, portanto da intimidade.

Acerca da intimidade, Arendt (2001) menciona que Rousseau foi o autor que primeiro teorizou sobre o tema, aduzindo tratar-se de uma rebelião contra a intrusão da sociedade nos mais recônditos ambientes interiores do homem, os quais até então não precisara de qualquer

tipo de proteção especial. Essa reação de rebeldia foi dirigida primeira-mente contra as exigências sociais de nivelamento de comportamento, que consistiria na uniformidade de condutas de todos os membros de uma sociedade, como se fosse uma só família em que haveria única opinião e único interesse. Essa circunstância seria também chamada de conformismo social.

Diante desse quadro, Robl Filho (2010) assevera que a intimidade proporciona na vida privada o desenvolvimento da subjetividade, visando o rechace da padronização social e fazendo com que a vida privada deixe de ter um sem número de privações e passe a ser um ambiente de libertação das estandardizações.

Segundo Rodotà (2008), o surgimento do conceito próprio de privacidade, pode ser historicamente associado ao declínio da sociedade feudal, na qual o isolamento era privilégio de poucos que, por necessidade ou opção, viviam distantes da vida em comunidade, e com o crescimento da classe burguesa. Ressalta ainda que a privacidade se estabelece como uma possibilidade da classe burguesa, a qual consegue desfrutá-la, sobretudo, graças às transformações socioeconômicas relacionadas à Revolução Industrial. Observa também o referido autor que em nível social e institucional, o nascimento da privacidade se apresentou como a aquisição de um privilégio por parte de um grupo, e não como a realização de uma exigência natural de cada indivíduo. Por isso que seus instrumentos jurídicos de tutela foram predominantemente estabelecidos com base na propriedade, o direito burguês por excelência.

Entretanto, a privacidade vai se transformando, gradativamente, em um instrumento de promoção da igualdade de tratamento entre os cidadãos, e da paridade social, e perdendo o seu caráter aristocrático e elitista, abandonando o nexo que a identificava com os privilégios da classe burguesa. Fazendo uma síntese retrospectiva dessa transformação, Ascenção (2003) afirma que até a primeira metade do século XIX, a tutela da privacidade confundia-se com a da propriedade privada e da honra, porém, a partir da segunda metade do século XIX a tutela da privacidade passa a ter novos parâmetros na Europa e na América.

Nessa perspectiva de transformação, cabe destacar a lição de Ferraz Junior (1993) no sentido de que a generalização do termo "sociabilidade" fez surgir outra distinção entre o social público (área da política) e o social privado (área do econômico, do mercado), o que fez surgir também duas novas e importantes dicotomias que estão na raiz dos direitos humanos modernos: Estado e sociedade, sociedade e indivíduo.

Além dessa generalização que fez surgir essa distinção, o avanço tecnológico do século XX provocou mudanças de paradigmas e da concepção do que seja a privacidade, ao aumentar o risco de violação desse direito a patamares constantemente mais altos, diante do crescente

interesse de grupos econômicos e políticos de obter informações pessoais, sob a justificativa de que quem detém a informação detém o poder nos dias atuais e, consequentemente, o lucro. Diante desse quadro, importante destacar que "a privacidade é uma noção cultural induzida no curso do tempo por condicionantes sociais, políticas e econômicas, pelo que justi-fica proceder no plano histórico para a sua contextualização jurídica" (Doneda, 2006, p. 114).

Assim, constata-se que apesar de a privacidade ser entendida por todas as nações como um direito a ser protegido, sua dimensão varia conforme as diferenças culturais de cada povo. Com efeito, o seu conceito varia no tempo e no espaço segundo as circunstâncias que proporcionam uma mudança de percepção de uma sociedade acerca do que faça parte da intimidade ou da vida privada. Tais circunstâncias podem ser sociais, ambientais, econômicas, políticas, religiosas, ou até as relacionadas com as facilidades proporcionadas pelas tecnologias de informação, o que proporciona a dificuldade de "uma definição âncora"[79].

Preliminarmente, uma questão que dificulta o entendimento da privacidade consiste no fato de que o instituto envolve diversos aspectos, ou dispõe de vários âmbitos de proteção: "honra", "imagem", "intimidade", "vida privada" (Gamiz, 2012). Tal consideração demonstra que o consenso conceitual pelos doutrinadores também em relação à privacidade é extremamente difícil. Devido a essa complexidade, quando ocorre violação de um direito, nem sempre ocorre, necessariamente, a violação dos demais.

Com isso, a dificuldade em conceituar "privacidade" e "intimidade" advém da própria extensão e do próprio conteúdo desses direitos. Normalmente, é apresentada por meio de interesses caracterizados por objetivos diversos. Nesse aspecto, a privacidade tem por objetivo proteger o homem contra: 1. Uma diversidade de invasões que possam influenciar em sua vida particular, familiar e doméstica; 2. A comunicação de acontecimentos importantes e embaraçosos afetos à sua intimidade; e 3. A transmissão de informações enviadas ou recebidas decorrente de segredo profissional. Entretanto, existem inúmeros obstáculos para a referida conceituação, conforme retrata Silva:

> São inúmeras as dificuldades que o tema suscita. A primeira delas é precisar a extensão e o conteúdo desse direito, cujo interesse subjacente é de caráter eminentemente subjetivo, por isso mesmo variável de pessoa para pessoa; os valores sociais são diferentes e mutáveis no tempo e no espaço; o sentimento que constitui o seu núcleo oscila no âmbito de cada pessoa. Essa dificuldade ainda mais se evidencia nas tentativas dos autores em formular uma definição do direito à intimidade. Torna-se mais difícil ainda quando se tem que estabelecer em que medida ou em que situações o interesse de preservação da intimidade deve ser sacrificado em prol de um outro

79 Termo utilizado por Danilo Doneda (2006)

> interesse juridicamente protegido, quando os dois se colocam em posição de absoluto antagonismo (Silva, 2003, pp.4-5).

Fora esses aspectos, um ponto que contribui para dificultar o consenso no entendimento da questão provém do fato de que diplomas legais ou convenções internacionais tendem a não cuidar de precisar seu conceito. Exemplo disso é visto na CRFB/1988 brasileira, que identifica as situações pelas quais o referido direito não pode ser violado, todavia, em nenhum momento, estabelece qualquer noção conceitual sobre o tema. Diante disso, os doutrinadores não possuem uma base inicial que possa servir de referência.

Além desses fatores, outra questão que torna essa tarefa árdua advém do pluralismo social: os valores entre as diferentes comunidades não são homogêneos ou iguais. Em adição às condições sociais, os aspectos materiais afetam significativamente o entendimento do direito à intimidade.

Para Sarlet, Marinoni e Mitidiero (2014), por exemplo, a densidade da população, o grau de interação, as condições de residência, a divisão do trabalho, a natureza da família e outras relações sociais devem ser considerados como fatores determinantes na definição do referido direito.

Nessa mesma linha de pensamento, Doneda (2006) destaca que a definição de privacidade não é um problema puramente dogmático, visto que se encontra estreitamente relacionada aos valores e projeções humanas em cada sociedade e, no âmbito de cada um dos muitos grupos, esta tarefa possui forte conteúdo social e também ideológico. Desta forma, há uma multiplicidade de opiniões arroladas acerca do tema.

Há, ainda, necessidade de buscar um mínimo de conteúdo – apto a satisfazer as garantias pessoais dos cidadãos das sociedades – que seja comum para o entendimento do direito à privacidade. Todavia, Leal (2015) pontua que não se pode, a princípio, definir, em toda a sua plenitude, a intimidade e a vida privada posto que seus contornos inequívocos só podem ser mensurados, considerando suas especificidades e o contexto em que ocorreu o caso concreto.

A situação em pauta conduz à noção de que a privacidade é um problema que o meio jurídico necessita solucionar, principalmente agora, com o avanço tecnológico e, em especial, com a proliferação do acesso à internet.

É importante também distinguir privacidade de direito à privacidade. Sobre essa dicotomia, nas várias consultas bibliográficas realizadas na doutrina brasileira, não se vislumbrou – de forma clara e objetiva – a preocupação dos estudiosos pátrios com o tema. Entretanto, na doutrina norte-americana, Solove, Rotenberg e Schwartz (2006), por meio de

sua obra *Privacy Information and Technology*, tratam do assunto como preliminar para a defesa do entendimento do referido direito numa visão pragmática. Nesse sentido, o direito da privacidade diz respeito às medidas pelas quais ela deve ser legalmente protegida. Então, por essa linha de raciocínio, entende-se como tal, no Direito brasileiro, o constante dos incs. X, XI e XII do art. 5º da CRFB/1988. Em contrapartida, "privacidade" abarca todo o conceito que não esteja inserido em documento legal, vislumbrado, por conseguinte, como um valor a ser compreendido.

Contribui, outrossim, para a complexidade do entendimento da privacidade – dificultando a elaboração de um conceito fechado sobre o tema – a possibilidade de renúncia, ainda que temporária, do direito à privacidade, o que decorre do fato de ele mesmo integrar o direito da personalidade e apresentar a característica, entre outras, de não ser absoluto.

Canotilho e Machado (2013), em estudo sobre a privacidade contemporânea, destacam que as expressões "intimidade" e "vida privada" carecem de interpretações consoante o contexto variável e possível de mudanças no tempo e no espaço. Assim sendo, o conceito de privacidade poderá adquirir maior ou menor elasticidade, dependendo da evolução da mentalidade da época, da identidade dos indivíduos envolvidos, de sua função social e estilo de vida dos interessados. Assim, quando uma pessoa decide tornar público seu comportamento (geralmente protegido pelo direito à privacidade), ela não renuncia totalmente ao referido direito, apenas passa a exercê-lo conforme suas preferências. Assim, a privacidade não pode ser analisada de forma generalizada e única para todos: necessita avaliação conforme o caso concreto.

Na atualidade, a importância (ou até mesmo indispensabilidade) da Internet requer a adequação de inúmeros conceitos ao seu ambiente, entre os quais a privacidade.

Fortes (2016, p.183) estabelece quatro direitos-base a título de direitos de privacidade na Internet (originalmente, *Internet Privacy Rights*): "o direito de navegar pela Internet [sic] com privacidade; o direito de monitorar quem monitora; o direito de deletar os dados pessoais; o direito a uma identidade online".

Os conceitos de privacidade e de proteção de dados pessoais na Internet possuem muitos aspectos, resultado das várias possibilidades de uso desse instrumento, o que cria um desafio legal para a correta tutela dos interesses dos indivíduos.

Sendo o direito à privacidade corolário da dignidade humana e um direito fundamental de primeira dimensão, sua tutela de modo adequado é elemento indispensável em um Estado democrático de direito. Nesse sentido, o ciberespaço tem enorme potencial para a participação

política e atividades comunitárias. Longhi (2017) salienta que a privacidade na Internet é um pressuposto de um sistema democrático deliberativo por dois grandes motivos.

O primeiro diz respeito à guarida dos dados pessoais como forma de evitar hierarquizações e discriminações com base em informações pessoais. O segundo, a restrição da autonomia privada do indivíduo frente ao abuso de poderes públicos e privados quando detentores de informações pessoais.

Mas estes não são os únicos problemas jurídicos em torno da proteção da privacidade dos cidadãos em um sistema democrático. O primeiro deles é o da definição de sua abrangência. Isto porque, há, no ocidente, dois grandes sistemas que se dedicam à guarnecer a privacidade: liberdade e dignidade. O da liberdade, oriundo dos países da *common law*, tutela a privacidade como uma espécie de liberdade pública abrangente, que justifica a não intervenção de terceiros na esfera de decisão do indivíduo. Já a privacidade como dignidade é uma característica dos países da tradição jurídica continental, restringindo-se à proteção da intimidade e vida privada dos indivíduos (Doneda, 2006).

Restringindo-se às Tecnologias da Informação e Comunicação (TICs), leciona Rodotà (2008) que o direito à privacidade hoje ganha novos contornos, dando margem à existência de um direito autônomo dele decorrente, a proteção dos dados pessoais. Embora ambas façam alusão à proteção da dignidade humana, os dados pessoais tutelam um bem jurídico diverso da intimidade. Enquanto um cuida do "corpo físico" o outro cuida do "corpo eletrônico". Ou seja, os dados, quando analisados e disponibilizados em conjunto, permitem que se formem perfis a serviço tanto do mercado como do Estado. Algo que põe em risco todos os outros direitos e garantias fundamentais.

E o tema da proteção dos dados pessoais se depara com novos desafios diuturnamente. Exemplificativamente, a questão do *big data*, o problema do direito ao esquecimento, o "consentimento" do cidadão em disponibilizar informações relevantes em sites de redes sociais, cujos provedores "praticamente sabem o que pensamos" e o uso de *malware* nas investigações criminais (Ferguson, 2015).

Assim, o avanço tecnológico, além de trazer vários benefícios para a sociedade, também trouxe algumas preocupações. A inserção de dados pessoais na rede, o posterior desejo de torná-los indisponíveis, bem como as novas formas como tais informações são utilizadas, acenderam a discussão sobre o direito de os usuários terem protegida a sua privacidade, além dos seus dados pessoais.

Nether (2018) expõe que os defensores da divulgação de determinados fatos, especialmente crimes, ainda que envolvam a privacidade do indivíduo sustentam suas razões

no exercício do direito à liberdade de expressão e comunicação, as quais promoverão a informação e a salvaguarda da paz social. Por outro lado, os defensores da manutenção de sigilo de determinados fatos sustentam suas razões na proteção dos direitos da personalidade, especialmente nos elementos que compõem a privacidade.

As possibilidades de obtenção dos mais diversos tipos de informações passaram a ser incomensuráveis. Assim, associando a grande quantidade de informações que podem ser obtidas, mediante os recursos tecnológicos contemporâneos, e a facilidade com que as informações pessoais possam se tornar conhecidas, seja pelo exercício do direito à liberdade de expressão e comunicação, ou manifestação do pensamento, seja pela vulnerabilidade de determinados bancos de dados em que há informações pessoais, surge o inevitável conflito do direito fundamental à informação com o direito fundamental à privacidade (Nether, 2018).

Diante desse panorama e tendo em vista o propósito do estudo, as possibilidades de violação da privacidade aumentaram substancialmente com o avanço tecnológico, ainda que a pessoa não se exponha deliberadamente. Determinados atos da intimidade e da vida privada, discretamente ou cuidadosamente, realizados no espaço público e privados, atualmente podem ser capturados pelos mais diversos recursos tecnológicos informacionais. A imagem da pessoa, da casa, as comunicações de todos os tipos, mediante correspondência tradicional (carta) ou eletrônica (*e-mail*), telefônica (voz ou mensagens eletrônicas), de dados, e telegráfica passaram a ser registrados, arquivados, tratados e com possibilidade de serem manipulados em locais desconhecidos, tendo em vista a estrutura mundial de rede que a Internet inaugurou.

Com o uso de *malwares*, informações sobre a vida privada ou da intimidade da pessoa, portanto, dados da privacidade podem ser acessados sem a autorização, ou sequer, o conhecimento pelo titular. Essa circunstância ocorre, tendo em vista a maneira como informações relacionadas à pessoa podem ser capturadas, classificadas, arquivadas e tratadas, pelas tecnologias informacionais.

Segundo Robl Filho (2010), para a concretização desses direitos exigidos pela ética pós-moralista, gerou a necessidade de a doutrina e jurisprudência brasileiras desenvolverem instrumentos jurídicos compatíveis com as necessidades cotidianas e contemporâneas desses direitos, onde há colisões, negociações e até renúncia[80] de alguns desses direitos fundamentais. Sobre a questão da renúncia tácita, Stefano Rodotà faz a seguinte observação:

80 Exemplo básico dessa renúncia ocorre quando a condição para se usufruir de determinadas utilidades oferecidas pela internet é o cadastramento pessoal com fornecimento de dados pessoais, até então considerados cadastrais e juridicamente possível de conhecimento público na era imediatamente anterior à atual sociedade da informação.

> Raramente o cidadão é capaz de perceber o sentido que a coleta de determinadas informações pode assumir em organizações complexas e dotadas de meios sofisticados para o tratamento de dados, podendo escapar a ele próprio o grau de periculosidade do uso destes dados por parte de tais organizações (Rodotá, 2008, p. 37).

Tem-se, assim, a circunstância em que direitos fundamentais passam a ser renunciados de maneira tácita, o que desafia uma análise de aspectos sobre a interpretação, associados à questão do conflito entre princípios.

No caso do Direito Penal, entende-se que em cada caso particular deve-se dar atenção à melhor adequação proposicional. A esta questão segundo Cupello (2005) deve-se ponderar alguns aspectos. Se tivermos em perspectiva que o que predomina é o interesse social, independentemente do direito individual sob exame, a violação trazida pelo uso de *malware* em investigações criminais aniquilaria inelutavelmente a zona que circunda o direito primário de intimidade do investigado. Ademais, se a solução dessa questão fosse adotada como sendo uma regra geral, de substrato de direito absoluto, o direito à reserva da vida privada se tornaria inexistente, violando, enfim, os direitos humanos que todo Estado tem o dever de proteger.

Assim, pugna-se pelo sopesamento dentre as várias faces do domínio da pessoa com vistas a decidir acerca de qual será a melhor resolução para a questão configurada e a correspondente determinação do conteúdo e extensão juridicamente relevante.

Pelo exposto conclui-se que a ingerência estatal na intimidade dos cidadãos, no âmbito da investigação criminal, deve ser encarada como excepcional, devendo-se recorrer aos métodos investigativos mais gravosos, quando outras medidas menos gravosas demonstrarem ser insuficientes ou inúteis para a obtenção dos fins da investigação criminal. Assim, não se pode banalizar o recurso aos métodos ocultos de investigação, como é o caso do uso de *malware* para infiltração digital, de tal sorte que avulta a importância de estabelecimento de critérios legais que estabeleçam limites concretos para a restrição desse direito fundamental.

Dito isto, na sequência, será analisado outro direito que também parece ser violado com o uso de *malwares* em investigações criminais: o direito ao segredo das comunicações.

3.5.2. O direito ao segredo das comunicações

Preocupado com a violação do direito à intimidade, notadamente a cometida contra a liberdade de comunicação e de manifestação do pensamento, o Constituinte estabeleceu no art. 5º, inc. XII, da Magna Carta: "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" (Brasil, 1988).

O sigilo das comunicações foi erigido a direito fundamental do indivíduo, ou seja, considerado bem jurídico essencial para a vida em sociedade. Trata-se de uma variante do direito à intimidade, já consagrado no art. 5º, inc. X, da CRFB/1988.

Todavia, como qualquer outro direito individual, não é absoluto e poderá ceder nos casos especificados na própria CRFB/1988 e regulados pela Lei 9.296/96, que cuida da interceptação telefônica e de telemática. Isso porque não só negócios lícitos são entabulados pelo telefone, e-mail e redes sociais. Muitos criminosos se valem desses meios de comunicação para combinar, acertar ou mesmo praticar delitos. Por isso, a válvula de escape esculpida na Carta Magna permitindo o acesso às conversações telefônicas e telemáticas visando apurar a prática de delitos.

No Brasil, a Constituição Federal e a legislação ordinária proíbem e punem a interceptação telefônica (ou *stricto sensu*) ilícita, não se posicionando expressamente sobre a gravação ou escuta clandestina e nem quanto à interceptação ambiental e sobre a interceptação de *malwares* para obter provas criminais. Compreensível essa omissão legislativa ante a constante inovação tecnológica que rapidamente modifica as formas de comunicação.

As mudanças no processo de comunicação oriundas dos avanços tecnológicos trazem mais desafios à interpretação sobre o sigilo das comunicações. Ademais, a ingerência estatal consoante ao direito ao sigilo das comunicações pressupõe a autorização judicial para fins de investigação criminal e/ou instrução processual, não se confundindo com intervenções prospectivas do Estado para a prevenção de crimes.

A Lei 9.296/96, em seu art. 1º, § único, permitiu a interceptação do fluxo de comunicações em sistemas de informática e telemática. Diz a norma: "O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática" (Brasil, 1996).

Logo após a publicação da lei, esse assunto causou grande controvérsia no mundo jurídico. Isso porque, analisando-se gramaticalmente o inc. XII, do art. 5º, da CRFB/1988, alguns doutrinadores passaram a entender que a Carta Magna apenas excepcionou a violação das comunicações telefônicas, deixando inabalados o sigilo da correspondência, da comunicação de dados e telegráficas, uma vez que o texto diz "salvo, no último caso", e esse seria apenas as comunicações telefônicas.

A seu turno, depois de vários anos em tramitação no Congresso Nacional, foi publicada a Lei 12.737/2012, que inseriu no Código Penal o art. 154-A, punindo com pena de

detenção de três meses a um ano, e multa, aquele que invadir dispositivo informático alheio, conectado, ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidade para a obtenção de vantagem ilícita[81].

Também é punido com a mesma pena quem produzir, oferecer, distribuir, vender ou difundir dispositivo ou programa de computador com o intuito de permitir a invasão do dispositivo informático.

A norma tutela a vida privada e a intimidade das pessoas físicas e jurídicas, visando coibir e punir o acesso indevido a dispositivo informático com a finalidade de obter, adulterar ou destruir dados ou informações, ou com o propósito de instalar vulnerabilidades para a obtenção de vantagem ilícita.

Trata-se de uma discussão importante, pois, o sigilo das comunicações é um direito constitucional que não tem caráter absoluto e, como tal, pode sofrer ingerências estatais, desde que na forma prevista em lei e prévia autorização judicial.

No caso específico do uso de *malware*, as especificidades desse recurso tecnológico impõem o estabelecimento de ditames regulatórios específicos, tendo em vista que esse meio peculiar de investigação criminal afeta outros direitos fundamentais além do sigilo das comunicações.

Greco Filho (2015) se manifestou pela inconstitucionalidade do art. 1º da Lei 9.296/96, na medida em que a CRFB/1988 somente permitiu a interceptação telefônica, partindo-se de uma interpretação gramatical, com elementos de natureza lógica, teleológica, sociológica e técnica. Assim, a expressão "no último caso" diria respeito somente à interceptação telefônica, sendo que, se a intenção do Constituinte fosse a de permitir a interceptação do fluxo de comunicações em sistema de telemática, teria redigido o artigo de outra forma. Além do que, como a garantia do sigilo é a regra e a interceptação a exceção, a interpretação deve ser restritiva (*exceptiora non sunt amplianda*).

---

81 A lei em questão foi alcunhada de "Lei Carolina Dieckmann" e teve impulso em razão de acesso a fotografias da atriz e sua difusão na rede mundial de computadores, causando comoção na mídia televisiva. A atriz deixou o computador pessoal para conserto em loja especializada e seus arquivos foram indevidamente violados. A partir de então, passou a ser extorquida por indivíduo que teve acesso a suas imagens em situação de intimidade. O fato apenas veio a confirmar o que já era sabido, ou seja, que não havia norma adequada para a punição daquele que invadisse dispositivo informático em que, não raras vezes, há imagens ou informações comprometedoras, que podem causar grave lesão à intimidade, se conhecidos ou divulgados. Com o novo tipo penal, aquele que invadiu indevidamente o dispositivo informático da atriz e obteve acesso a seus dados eletrônicos (fotografias), receberia adequada sanção penal.

Grinover também entendeu pela inconstitucionalidade do dispositivo, pugnando que:

> A informática tem por objeto o tratamento da informação através do uso de equipamentos e procedimentos na área de processamento de dados. Nesse sentido técnico, o dispositivo vulnera a Constituição, que não permite a quebra do sigilo dos bancos de dados. Já a telemática versa sobre a manipulação e utilização da informação através do uso combinado do computador e meios de telecomunicação, de modo que aqui se tem uma comunicação de dados via telefone. Cabe, então, verificar se a expressão constitucional "comunicações telefônicas" seria, ou não, abrangente das comunicações "via telefone". Mesmo assim, a resposta seria negativa, dado que as regras limitadoras de direitos, sobretudo quando excepcionais, devem ser interpretadas restritivamente. Desse modo, a "comunicação telefônica" parece adstrita à transmissão da voz (Grinover, s/d, p. 115).

Um dos primeiros juristas a se manifestar pela constitucionalidade do dispositivo foi o professor Alexandre de Moraes (2019), que concluiu ser perfeitamente possível a interceptação em outras espécies de inviolabilidade, dada a relatividade da norma constitucional, haja vista que nenhuma liberdade é absoluta, sendo possível, respeitados certos parâmetros, a interceptação das correspondências, das comunicações e de dados, sempre que essas liberdades públicas estiverem sendo utilizadas como instrumento de salvaguarda de práticas ilícitas.

Há crimes extremamente graves praticados com o emprego do computador, que se tornou instrumento de pessoas ligadas a organizações criminosas. Sem a possibilidade de interceptação dessa modalidade de correspondência eletrônica não será possível o efetivo combate ao crime organizado, que tenta se instalar de forma definitiva no país.

Para que um direito individual extremamente importante não seja violado, mas também não seja a sociedade colocada em perigo, caberá ao Poder Judiciário analisar concretamente os casos que forem surgindo, a fim de decidir se a intimidade de alguém poderá ser violada quando estiver presente interesse público relevante, haja vista que o direito à intimidade não pode ser empregado como instrumento de impunidade e acobertamento de práticas ilícitas.

3.5.3. O direito à autodeterminação informacional

A primeira lei sobre a proteção de dados pessoais foi na Alemanha, a lei do Land de Hesse, de 1970. Segundo Doneda (2006, p. 192) a República Federal da Alemanha possuía, desde 1977, uma lei federal de proteção de dados pessoais, a *Bundesdatenchutzgesetz*. Os trabalhos do censo alemão, os quais foram regulamentados por uma lei aprovada em 1982,

deveriam ser finalizados em 1983. Entretanto, provocaram desconfiança em vários setores da sociedade, quanto ao método de coleta de informações utilizado e pela destinação destas. Esta foi a causa de uma célebre sentença da Corte Constitucional Alemã (*Bundesverfassungsricht*), a qual até hoje é referência no tema da proteção de dados pessoais.

Tal lei que organizava o censo foi a causa da sentença. Previa, segundo Rodotá (2008) que cada cidadão deveria responder a 160 perguntas, as quais seriam posteriormente submetidas a tratamento informatizado. Permitia-se também que os dados recolhidos no censo fossem rastreados até os cidadãos recenseados e fossem utilizados para outras finalidades diversas do recenseamento, como, e.g., pelas autoridades locais para corrigir os cadastros de moradores dos municípios.

A decisão proferida pelo Tribunal Constitucional Federal Alemão em 25.12.1983 concordou com os propósitos estatísticos da lei, porém declarou que os direitos fundamentais dos cidadãos deveriam ser protegidos contra certos abusos. Entendeu que a transferência de dados obtidos no recenseamento do governo federal para autoridades locais seria inconstitucional.

Apesar de tal situação na decisão dizer respeito ao princípio da finalidade, a doutrina é uníssona em afirmar que nessa decisão foi reconhecido o direito à autodeterminação informativa.

Segundo Ruaro (2015), a autodeterminação informativa é a possibilidade de um indivíduo, titular de determinado dado, exigir que seus dados não sejam tratados. Dito de outra forma é a capacidade, possibilidade e liberdade que as pessoas têm para decidir sobre o tratamento de seus dados, e se desejarem, interromper este tratamento.

Conforme acentua Rodotà (2008) esse direito considera ilegítima toda coleta de informações pessoais que for realizada sem um prévio conhecimento e explícito consentimento do interessado. Esse direito consiste em que determinadas informações coletadas sobre uma determinada pessoa não devem circular fora da instituição pública ou privada que tenha coletado essas informações originalmente para certa finalidade.

Segundo a previsão da Lei brasileira 12.965/2014[82], tal direito encontra plasmado nos dispositivos que: 1) veda o fornecimento a terceiros de registros de conexão e de acesso à aplicações de Internet, exceto mediante consentimento livre, expresso e informado; 2) exige clareza e completude das informações sobre a coleta, uso, tratamento e proteção de seus dados pessoais; e 3) que somente poderão ser utilizados para as finalidades que fundamentaram sua coleta.

82 Incisos VI e VII do art. 7º da Lei 12.965/2014.

Por sua vez, a Lei 13.709/2018 (Lei geral de proteção de dados pessoais) prevê expressamente que a autodeterminação informativa é um dos fundamentos da disciplina da proteção de dados pessoais[83]. A resultante dessa previsão está no elenco de direitos previstos, os quais são: a) à confirmação da existência de tratamento; b) ao acesso aos dados; c) à correção de dados incompletos, inexatos ou desatualizados; d) à anonimização[84], bloqueio ou eliminação de dados desnecessários, excessivos ou tratados desconformes com as disposições legais; e) à portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e desde que observados os segredos comercial e industrial, conforme a regulamentação do órgão controlador; f) à eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses de conservação dos dados previstas na Lei[85]; g) à informação das entidades públicas e privadas com as quais o controlador compartilhou dados; h) à informação acerca da possibilidade de não conceder consentimento e sobre as consequências da negativa; e i) à revogação do consentimento.

Vê-se que a finalidade legal é atribuir à pessoa, o direito de saber o que é feito com as informações pessoais e decidir se autoriza ou não a utilização para fim diverso da que foi obtida. Nesse sentido, resta claro que o uso de *malwares* em investigações criminais afeta também o direito à autodeterminação informativa.

3.5.4. O direito à integridade e à confiabilidade dos sistemas informáticos

Consoante já delineado em linhas pretéritas, o potencial técnico multifacetado do uso de *malware* para fins de investigação criminal permite uma extensa amplitude investigativa com potencialidade de atingir diferentes direitos fundamentais da pessoa investigada. Isso porque não se trata da pura e simples interceptação da comunicação de dados, nem se limita à realização de buscas *online*. Por meio desse instrumento tecnológico pode-se realizar interceptações telemáticas (fluxo de comunicações em sistemas de informática e telemática); interceptações ambientais (captação de áudio em tempo real); monitoramento e gravação de vídeo; acompanhamento e localização geográfica do dispositivo via GPS; além de pesquisa e

83 Art. 2º da Lei geral de proteção de dados pessoais.

84 Termo novo na legislação pátria cujo conceito previsto na Lei é a utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

85 Art. 16. [...] autorizada a conservação para as seguintes finalidades: I – cumprimento de obrigação legal ou regulatória pelo controlador; II – estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; III – transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei.

recolha de dados e arquivos armazenados nas unidades de memória ou salvos em nuvem (busca *online*).

Nessa perspectiva, desponta um novo direito fundamental que segundo Lopes Jr. e Mendes (2019) surge em razão da "dataficação" da vida decorrente da dinamicidade relacionada à sociedade de informação. A intrusão de *malware* em dispositivos informáticos, assim, além de incidir sobre o direito à livre comunicação, intimidade, privacidade, autodeterminação informativa, entre outros, limita significativamente o direito fundamental à integridade e confiabilidade dos sistemas informáticos[86].

Proteger os sistemas informáticos e, mais especificamente, os dados que neles encontram-se inseridos é proteger também os sujeitos aos quais os dados se referem. Referida proteção permeia o critério para a legitimação política daquilo que Perez Luño (1989, p.139) denomina de "sistemas democráticos tecnologicamente desenvolvidos", em razão do fato de que a proteção de dados e a liberdade informática integram o *status* que constitui o cidadão.

A CRFB/1988, em seu art. 5º, § 2º não obsta a possibilidade de incorporar outros direitos que em razão de seu conteúdo possuam *status* de fundamentais. Trata-se, assim, do que se denomina cláusula de abertura. Assim, para além dos direitos fundamentais que estão dispostos de forma expressa na Constituição (fundamentalidade formal), é preciso, segundo Sarlet (2015) ser observada a fundamentalidade material do direito relacionado à estrutura fundamental do Estado e da sociedade.

Dito isto, referente à integridade e confiabilidade do sistema informático como direito fundamental, resta claro que seu conteúdo o apensa à definição material de direitos fundamentais. Neste trilhar, pela análise realizada, o direito à integridade e à confiabilidade do sistema informático, tendo em vista seu conteúdo, integram a estrutura básica do Estado Democrático brasileiro.

Para que os *malwares* possam ser utilizados em investigações criminais pelo Estado denota-se essencial e urgente a disciplina legal específica sobre esse método inovador. No entanto, adotando-se a teoria jurídica da inovação investigativa criminal de Soares (2014), não se pode descartar a possibilidade de autorização judicial do uso dessa ferramenta, aplicando-se por analogia às normas legais já existentes, desde que se limite os fins específicos e o alcance do uso do *malware* ao encontro do método disciplinado em lei (como, por exemplo, a interceptação telemática e a infiltração virtual), atendidos os pilares da excepcionalidade,

86 O Tribunal Constitucional alemão definiu a confiabilidade e integridade dos sistemas de TI como um novo direito fundamental, de forma a protege-lo das ingerências estatais no que tange às investigações que buscassem atingir o fluxo de informações de forma oculta fazendo uso da internet (Abel & Schafer, 2009).

proporcionalidade e controle judicial da medida inovadora e da provisoriedade, isto é, enquanto houver omissão legislativa. Justifica-se essa interpretação sob pena de inviabilizar-se por completo investigações criminais de crimes graves cujas provas não possam ser alcançadas de outra forma.

Nesse sentido, tem-se o exemplo da experiência italiana, país em que o Estado foi autorizado por decisões judiciais a fazer uso do *malware* durante vários anos até que houvesse a primeira disciplina legal sobre o assunto.

Também Soares (2014) defende que as inovações investigativas criminais são possíveis de aplicação atendendo-se ao controle de legalidade (*prater legem*), proporcionalidade, tipificação processual progressiva (não estabilização de insuficiências legislativas) e modulação temporal (pelo poder judiciário).

Cita o autor legislação estrangeira que admite inovações investigativas, a exemplo de Portugal que, no art. 125 do CPP, prevê a liberdade probatória como regra e institui os métodos proibidos de prova (art. 126), ou seja, permite-se a inovação que não seja legalmente proibida.

Aponta o mesmo autor que a jurisprudência brasileira é excessivamente tolerante com a inovação investigativa ao ponto de permitir a estabilização de omissões legislativas. Cita, como exemplo, a infiltração de agentes, método judicialmente autorizado e implementado por anos, sem que houvesse regulamentação procedimental. Propõe, então, o estabelecimento de critérios para a limitação *temporal* e *material* das inovações investigativas (Soares, 2020). Assim, embora não defenda expressamente a possibilidade de uso de *malware* como inovação investigativa no Brasil, abre espaço para se admitir sob os critérios já expostos.

CONCLUSÃO

O caminho percorrido ao longo dessa pesquisa confirmou a advertência feita ao leitor já na introdução do trabalho quanto ao grande potencial de polêmica do tema proposto. Isso porque não se trata de tarefa fácil, longe disso, encontrar o justo equilíbrio entre a necessidade de eficiência das investigações criminais e a garantia de proteção dos direitos fundamentais dos cidadãos, notadamente no atual contexto de complexidade das relações sociais da Era Digital, baseada no paradigma tecnológico.

De fato, os modernos dispositivos tecnológicos, a exemplo dos *smartphones*, *tablets*, *smartwatches*, *notebooks*, etc., e os crescentes aplicativos de redes sociais, fazem parte do cotidiano da atual socidade da informação. Essa nova realidade, ao passo que contribui para o inegável progresso da humanidade ao facilitar o acesso à informação e ao conhecimento, também impõe novos desafios sobretudo à segurança dos dados que circulam no ambiente digital, deixando mais vulneráveis a privacidade e a intimidade dos cidadãos. Por outro lado, também apresenta novos obstáculos à eficiência das investigações criminais e consequentemente à obtenção da prova penal, somente transponíveis mediante o recurso de métodos especiais de investigação criminal assentados na evolução tecnológica

Não por acaso, em recente julgamento de ação constitucional em tramitação no Supremo Tribunal Federal[87], o ministro relator da demanda reconheceu, em seu voto, que o recurso do Estado a métodos ocultos de investigação criminal, como é o caso da interceptação de comunicações telefônicas ou telemáticas, revela-se muitas vezes como uma das principais formas – e para alguns crimes até a única – de se apurar ilícitos penais. Ainda, assim, a utilização desses meios investigativos deve submeter-se a um rigoroso exame de proporcionalidade entre a necessidade de eficiência das investigações criminais e a preservação da garantia de proteção dos direitos fundamentais restringidos.

Confirma-se, assim, a hipótese inicial segundo a qual os métodos tradicionais de investigação criminal se mostram insuficientes para ultrapassar as dificuldades impostas à persecução criminal nesse complexo ambiente da atual sociedade em rede e em risco. É inevitável, portanto, que haja uma reação do sistema jurídico no sentido de permitir que o Estado-persecutor utilize-se dos avanços tecnológicos que impliquem investigações mais invasivas e insidiosas aos direitos fundamentais, para fazer frente à paralela evolução de práticas criminosas mais graves.

87 Brasil. (2020). Supremo Tribunal Federal. *Informativo 979*. Brasília, 25 a 29 de maio de 2020. Disponível em: http://www.stf.jus.br//arquivo/informativo/documento/informativo979.htm.

Nesse contexto, o uso de *malware* estatal (*software* espião) apresenta-se como um dos meios de investigação ou de obtenção de prova dos mais insidiosos, não só por sua natureza oculta, mas principalmente pelo seu multiforme potencial técnico que o habilita a uma ampla capacidade investigativa, com repercussão limitativa de diferentes direitos fundamentais. O recurso de *malware* na atividade investigativa já não é novidade na experiência estrangeira. No entanto, no Brasil, o assunto ainda é pouco explorado, o que, de certa forma, fomentou a presente pesquisa, pela qual também se confirma a advertência introdutória da necessidade de que o tema continue sob constante debate e reflexão não apenas por sua exploração científica, no âmbito acadêmico, mas também nos domínios político e jurídico.

A análise amostral da experiência estrangeira demonstrou que a discussão sobre a admissão do uso dessa ferramenta tecnológica de investigação criminal chegou primeiro aos Tribunais, antes mesmo de sua regulamentação legal. No caso da Itália, em particular, o legislador demorou mais de dez anos para regulamentar o uso de *malware* como novo instrumento investigativo. Durante todo esse tempo de omissão legislativa, o Judiciário italiano acolheu o novo meio investigativo, limitando o seu uso para processos por crime organizado, admitindo-o por analogia à interceptação de conversas ou comunicações entre presentes e, em outros casos, enquanto meio atípico de investigação criminal (busca *online*).

O exemplo italiano é uma clara demonstração do quão vagarosa pode ser a produção legislativa contrastante com a velocidade e dinamismo das constantes alterações sociais, notadamente a partir da evolução tecnológica. Aqui reside uma das questões mais problemáticas e de difícil solução, qual seja, como assegurar que o Estado não perca a sua capacidade de investigar e punir condutas criminosas em um cenário de inadequação legislativa decorrente de transformação social, obviamente não prevista pelo legislador, sem, no entanto, deixar de preservar a proteção necessária dos direitos e liberdades fundamentais, impedindo que as investigações se transformem em atividades exploratórias sem qualquer parâmetro legal e desprovidas de proporcionalidade?

A resposta a esse questionamento passa necessariamente pela avaliação da possibilidade ou não de se admitir o emprego de métodos investigativos atípicos mediante a aplicação analógica da regulação estabelecida a outros meios de investigação que possam conter semelhanças. Nesse ponto, deve-se descartar, *ab initio*, qualquer hipótese de se admitir a utilização de meios investigativos inovadores (não previstos em lei) restritivos de direitos fundamentais fora de qualquer embasamento legal (*extra legem*), isto é, completamente afastados da lei, nem tampouco *contra legem,* ou seja, que derroguem ou modifique o efeito de uma lei.

Por outro lado, a recusa absoluta da possibilidade do emprego de técnicas investigativas inominadas ou insatisfatoriamente regulamentadas poderá resultar na total incapacitação do Estado de cumprir a sua importante missão de apurar condutas criminosas de alta complexidade. Desse modo, a exclusão apriorística da possibilidade do emprego de todo e qualquer método investigativo inovador oriundo da evolução tecnológica não parece se coadunar com o desejável equilíbrio entre a necessidade de eficiência das investigações criminais e a garantia de proteção dos direitos fundamentais. A tolerância ao recurso de meios atípicos de investigação tecnológica deve ser, portanto, embasada nos pilares da excepcionalidade, da provisoriedade da omissão legislativa, da proporcionalidade e do rigoroso controle judicial.

Ademais, a ordem constitucional e legal brasileira não impõe um sistema rígido de taxatividade dos meios de obtenção de prova, admitindo-se o recurso a meios de investigação ou de obtenção de prova não disciplinados expressamente em lei, desde que respeitada a estrita observância dos limites constitucionais e processuais da prova, atendidas, ainda, a excepcionalidade e a proporcionalidade da medida[88], para garantia do núcleo essencial dos direitos fundamentais atingidos.

No caso, em especial, das investigações digitais a tensão entre as necessidades de eficiência da persecução penal e de garantia dos direitos e liberdades fundamentais da pessoa investigada mostra-se em toda a sua intensidade. Isso porque a realidade virtual deixou de ter uma conotação metafísica, sendo hoje o lugar onde se manifestam todos os aspectos da vida humana; uma verdadeira extensão da pessoa. Ao mesmo tempo, é no terreno sombrio desse ambiente onde se desenvolvem ou se escondem práticas criminosas de extrema gravidade capazes de lesar direitos fundamentais tão inportantes quanto o direito à privacidade.

Nesse contexto, a permissão do uso do *malware* pelo Estado como instrumento de investigação criminal tecnológica no ambiente digital, objeto da pesquisa, para além de superar o já mencionado problema do elevado grau de invasividade na vida privada deve também

88 Em Voto-vista, o Min. Rogério Schietti Cruz, no julgamento do Habeas Corpus nº 315.220/RS do Superior Tribunal de Justiça (HC 315.220/RS, Rel. Ministra MARIA THEREZA DE ASSIS MOURA, SEXTA TURMA, julgado em 15/09/2015, DJe 09/10/2015), entendeu que o acesso à conta de correio eletrônico não se trata de interceptação, porque a sua captação não era atual, mas se cuida de quebra de sigilo de comunicações telemáticas (sem previsão legal). Desse modo, sustentou que a medida implementada judicialmente aproxima-se, em sua essência, da busca e apreensão de documentos virtualmente armazenados em provedor de internet, devendo, pois, regular-se pelo disposto no art. 240 [, §1º, f] do Código de Processo Penal, que regulamenta a busca domiciliar ou pessoal. Acesso em 01.10.2020. Disponível em: https://ww2.stj.jus.br/processo/revista/inteiroteor/?num_registro=201500197570&dt_publicacao=09/10/2015.

buscar solução para a garantia da autenticidade, integridade e confiabilidade dos dados digitais colhidos. Somente pode-se cogitar admitir a utilização do *malware* ou de qualquer outro recurso tecnológico em investigação criminal a partir da demonstração inequívoca de procedimentos que garantam a confiabilidade do material recolhido, desde a sua aquisição e a preservação da cadeia de custódia da prova digital, de modo a possibilitar o exercício do contraditório.

Não há dúvida de que o ideal é a intervenção legislativa para a criação de um regime jurídico específico para o uso de *malware* estatal nas investigações criminais, definindo e delimitando o âmbito de utilização dessa ferramenta tecnológica a partir de critérios de justificação constitucional para a restrição dos direitos fundamentais envolvidos. Todavia, a mera previsão legal não se mostra suficiente, sem que nela conste mecanismos de garantia da autenticidade, integridade e confiabilidade dos dados recolhidos, em razão das características peculiares da prova digital.

Não obstante, na ausência de um regime legal específico, incumbe ao Poder Judiciário a avaliação casuística da possibilidade de autorizar o recurso ao *malware* estatal, enquanto medida investigativa inovadora, para compensar o déficit legislativo, em casos excepcionalmente desafiadores, decorrente da interpretação extensiva ou aplicação analógica de outros instrumentos já consolidados no ordenamento jurídico, obedecidos os mandamentos da excepcionalidade, provisoriedade, proporcionalidade e rígido controle judicial.

Em que pese as relevantes vozes contrárias[89], entendemos que o atual arcabouço normativo brasileiro abre espaço para a permissão excepcional do recurso ao *malware* estatal em investigações criminais, em casos excepcionalmente desafiadores, isto é, para a apuração de crimes de elevada gravidade e quando todas as demais medidas se demonstrarem inaptas, inúteis ou impraticáveis, abalizado em rigoroso controle judicial preventivo e repressivo, sob cobertura regulatória de instrumentos de investigação já previstos em lei.

Nessa perspectiva, embora não tenha havido a nominação legal específica do *malware* enquanto técnica de investigação, a Lei 12.850/2013 - que define organização criminosa e dispõe sobre a investigação criminal e os meios de obtenção da prova dos crimes correlatos –

89 Nesse sentido conferir: Mendes, C.H.C.F. (2020). *Tecnoinvestigação criminal: entre a proteção de dados e a infiltração por software*. Salvador: Editora Juspodium; e Lopes Jr., A.; Mendes, C.H.C.F. (2019). *Vírus espião como meio de investigação: a infiltração por softwares.* Disponível em: https://www.conjur.com.br/2019-jun-07/limite-penal-virus-espiao-meio-investigacao-infiltracao-softwares.

permite e regula métodos especiais de investigação criminal, dentre os quais se destacam: - a captação ambiental de sinais eletromagnéticos, ópticos ou acústicos; - ação controlada; - acesso a registros de ligações telefônicas e telemáticas, a dados cadastrais constantes de bancos de dados públicos ou privados e a informações eleitorais ou comerciais; - a interceptação de comunicações telefônicas e telemáticas; e - a infiltração, por policiais, em atividade de investigação. Neste último caso, a lei expressamente admite a *infiltração virtual* de agentes policiais.

Menciona-se, ainda, a Lei 13.441/2017 que alterou o Estatuto da Criança e do Adolescente para autorizar expressamente a *infiltração de agentes de polícia na internet*, com o fim de investigar crimes contra a dignidade sexual de criança e de adolescente.

Todavia, a tolerância da aplicação analógica desse importante método oculto de investigação criminal, antes da constituição legal específica que estabeleça um regime jurídico próprio para o *malware* na atividade investigativa estatal, não pode ser vista como uma solução ideal e permanente, mas temporária e excepcional, sob rigorosa submissão aos parâmetros da proporcionalidade (adequação, necessidade e proporcionalidade em sentido estrito) e estabelecimento de requisitos judicialmente definidos que traduzam o necessário equilíbrio entre a eficiência e a proteção dos direitos e garantias fundamentais, devendo-se compelir a inevitável, imprescindível e progressiva regulamentação legal.

REFERÊNCIAS BIBLIOGRÁFICAS

Livros

Abel, W.; Schafer, B. (2009, April). *The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems* – a case report on BVerfG, NJW 2008, 822. In Madhuri, V. (Ed.), Hacking. (pp. 167-91). Icfai University Press. Volume 6, Issue 1.

Alves, D.B. (2017). Uso de Malware em investigação criminal. *Actualidad Jurídica Uría Menéndez*, v.47, n.1, p.19-30.

Araújo, J.S. (2018). *Malware: cyber ameaça*. São Paulo: Perícia Digital.

Badaró, G. (2003). *Ônus da prova no processo penal.* São Paulo: Editora Revista dos Tribunais.

Barroso, L. (2014, Jan-Jun). A Segurança: uma aproximação conceptual. *Revista de Direito de Direito e Segurança*, ano II, nº 3, Lisboa.

Bechara, F.R. (2014, Jan-Jun). Natureza jurídica do Relatório de Inteligência Financeira do COAF (Conselho de Controle das Atividades Financeiras). *Revista Fórum de Ciências Criminais – RFCC* (p. 69-84), Belo Horizonte, ano 1, n. 1.

Beck, U. (2011). *Sociedade de risco: rumo a uma outra modernidade*. (2ª ed.). Tradução de Sebastião Nascimento. São Paulo: Editora 34.

Bene, T. (2014). Il pedinamento elettronico: truismi e problemi spinosi. In: (a cura di) Scalfati, A. *Le indagini atipiche*. (p.348). G. Giappichelli Editore. Torino.

Bobbio, N. (1986). *O Futuro da Democracia. Uma defesa das regras do jogo.* Tradução Marco Aurélio Nogueira. (6ª ed.). Rio de janeiro: Paz e Terra.

Bobbio, N. (1996). *Os Intelectuais e o Poder*. São Paulo: Unesp.

Bonfim, E.M. (2008). *Curso de processo penal*. (3ª ed.). São Paulo: Saraiva.

Buzan, B. (2008). People, States, and Fear: an agenda for international security studies in the post-cold war era. *Revista Académica de Relaciones Internacionales*, n.9.

Canaris, C.W. (2016). *Direitos fundamentais e direito privado*. Tradução de Ingo Wolfgang Sarlet e Paulo Mota Pinto. Coimbra: Almedina.

Canotilho, J.J.G. (2003). *Direito constitucional e teoria da constituição*. (7ª ed.). Coimbra: Almedina.

Casey, E. (2011). *Digital evidence and computer crime: forensic science, computers and the internet*. (3rd ed.). Elsevier.

Castells, M. (1999). *A era da informação*. São Paulo: Paz e Terra.

Castells, M. (1999). *A sociedade em rede*: *a era da informação, economia, sociedade e cultura*. Tradução de Roneide Venâncio Majer. São Paulo: Paz e Terra. v. 1.

Castells, M. (2003). *A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade*. Tradução de Maria Luiza X. de A. Borges. Revisão Paulo Vaz. Rio de Janeiro: Zahar.

Castells, M. (2013). *Redes de indignação e esperança: movimentos sociais na era da internet*. Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Zahar.

Colli, M. (2010). *Cibercrimes - Limites e Perspectivas à Investigação Policial de Crimes Cibernéticos*. Curitiba: Juruá Editora.

Correia, J.C. (1999). *Contributo para a análise da inexistência e das nulidades processuais*, Coimbra: Coimbra Editora.

Costa Júnior, P.J. (2007). *O direito de estar só: tutela penal da intimidade*. (4ª ed.). São Paulo: Revista dos Tribunais.

Costa Pinto, F.L. (2018, jan-abr). A Fase de Inquérito e a Evolução do Processo Penal. *Revista Portuguesa de Ciência Criminal,* ano 20, nº 1.

Cupa, B. (2013). *Trojan Horse Resurrected: On the Legality of the Use of Government Spyware (Govware)*, Living in Surveillance Societies: The State of Surveillance, LISS.

Cupello, L.P.F. (2005). *Tutela Penal & Processual Penal da Privacidade*. Curitiba: Juruá Editora.

Dallagnol, D.M. (2016). A Visão Moderna da Prova Indício, In: Salgado, D.R.; Queiroz, R.P. (orgs.). *A prova no enfrentamento à macrocriminalidade*. (2ª ed.) (pp. 105 – 128). Salvador: Juspodivm.

Day, P. (2014). *Cyber Attack. The Truth About Digital Crime, Cyber Warfare and Government Snooping*. (pp. 59-64). London: Carlton Books.

Dias, J.F. (2004). *Direito Processual Penal*. Coimbra: Coimbra Editora.

Domingos, J.A.; Couto, S.P. (2011). *Wikileaks: segredos, informações e poder*. Bauru (SP): Idea Editora.

Duarte, F.P. (2015) Sociedade de risco. In: Jorge Bacelar Gouveia & Sofia Santos. AAVV, *Enciclopédia de Direito e Segurança* (pp. 452-453). Coimbra: Almedina.

Durkheim, É. (2005). *As Regras do Método Sociológico*. São Paulo: Martin Claret.

Fabretti, H.B. (2014). *Segurança Pública: Fundamentos Jurídicos para uma Abordagem Constitucional*. São Paulo: Atlas.

Feldens, L. (2007). Deveres de Proteção Penal na Perspectiva dos Tribunais Internacionais de Direitos Humanos. *Revista Brasileira de Direitos Fundamentais e Justiça*, v.1.

Fellman, P.V.; Wright, R. (2008). Modelando redes terroristas. In: Duarte, F.; Quandt, C.; Souza, Q. (Org.). *O tempo de redes*. São Paulo: Perspectiva.

Ferrajoli, L. (2010). *Direito e razão: teoria do garantismo penal*. (3ª ed.). São Paulo: Revista dos Tribunais.

Ferreira, M.M. (1988). Meios de Prova. *Jornadas de Direito Processual Penal* (p. 221-260), Lisboa.

Fontes, J. (2013). *O Direito ao Quotidiano Estável — Uma Questão de Direitos Humanos*. Coimbra: Coimbra Editora.

Gascón Abellán, M. (1999). *Los Hechos em el derecho – bases argumentales de la prueba*. Madrid, Marcial, Pons, Ediciones Jurídicas y Sociales S.A.

Gasper, Des. (2008). The Idea of Human Security. In: *Garnet Working Paper* (p. 2-9), University of Warwick, Coventry, United Kingdom, n. 28.

Gercke, M. (2012). *Understanding Cybercrime: Phenomena, Challenges and Legal Response*. Geneva: ITU.

Gomes Filho, A.M. (2005). Notas sobre a terminologia da prova (reflexos no processo penal brasileiro), In: Yarshell, F.L.; Moraes, M.Z. (orgs.). *Estudos em homenagem à Professora Ada Pelegrini Grinover* (pp. 303–318). São Paulo: DPJ Editora.

Gonçalves, F; Alves, M.J; Valente, M.M.G. (2001). *Lei e crime*: *o agente infiltrado versus o agente provocador. Os princípios do processo penal*. Coimbra: Almedina.

Gossel, K.H. (2007). *El Derecho Processal Penal en el estado de Derecho* (pp. 146-147). Buenos Aires: Rubinzal – Culzoni Editores.

Gouveia, J.B. (2018). *Direito da Segurança: Cidadania, soberania e cosmopolitismo*, Coimbra: Almedina.

Greco Filho, V. (1999). *Manual de Processo Penal*. (6ª ed.). São Paulo: Saraiva.

Greco Filho, Vicente. Interceptação Telefônica. (3ª ed.). São Paulo: Saraiva, 2015.

Grinover, A.P.; Fernandes, A.S.; Gomes Filho, A.M. (2011). As nulidades no processo penal. (12ª ed.). São Paulo: Revista dos Tribunais.

Grinover, A.P. (1997). O regime brasileiro das interceptações telefônicas. In: *RBDCRIM*, 17/115.

Harris, R. (2006). Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensic sproblem, *Digital Investigation - The international Journal of Digital Forensics & Incident Response*, Vol. 03 – Suplemento.

Hobbes, T. (2006). *Leviatã*. São Paulo: Martin Claret.

Jakobs, G.; Meliá, M.C. (2005). *Direito Penal do Inimigo – Noções e Críticas*. Organização e Tradução de André Luís Callegari e Mereu José Giacomolli. Porto Alegre: Livraria do Advogado.

Jellinek, G. (1905). *Teoria general del estado*. Tradução de Fernando de Los Rios. Buenos Aires: Albatroz.

Jesus, D.E. (2016). *Código Penal anotado*. (23ª ed.). São Paulo: Saraiva.

Lara, A.A.S. (2011). *Ciência Política, Estudo da Ordem e da Subversão* (p.49). Lisboa: ISCSP.

Leite, I.F. (2014). *O novo regime das escutas telefónicas. Uma visão panorâmica da reforma de 2007*. Direito da Investigação Criminal e da Prova (coord. Maria Fernanda Palma et al.), Coimbra: Almedina.

Lemos, A. (2016). *Cibercultura: tecnologia e vida social na cultura contemporânea*. (8ª ed.). Porto Alegre: Sulina.

Levy, P. (1999). *Cybercultura*. Tradução de Carlos Irineu da Costa. São Paulo: Editora 34.

Lopes Jr., A. (2003). Sistemas de investigação preliminar no processo penal. (2ª ed.). Rio de Janeiro: Lumen Juris.

Lopes Jr., A. (2016). *Direito Processual Penal*. (13ª ed.). São Paulo: Saraiva.

Machado Neto, A.L. (2008). *Sociologia Jurídica*. São Paulo: Saraiva.

Maciel Neto, A.A. (2020). *Liberdades, Garantias e Direitos Sociais*. Curitiba: Juruá Editora.

Magalhães Noronha, E. (1983). *Curso de Direito Processual Penal*. (15ª ed.). São Paulo: Ed. Saraiva.

Maier, J.B. (2011). *Derecho processual penal. Tomo III: parte general: actos procesale.* Ciudad Autónoma de Buenos Aires: Del puerto.

Marques, J.F. (1997). *Elementos de Direito Processual Penal*. Campinas: Bookseller, v. II.

Marques, J.F. (2000). *Instituições de Direito Processual Civil*. Campinas: Millennium Editora, v. III.

Mason, S. (2012). *Electronic Evidence* (3rd edn) (p.109-147), LexisNexis Butterworths.

Mason, S. (February 2014). *Electronic Evidence*, chapter 5 and Stephen Mason, 'Electronic evidence: A proposal to reform the presumption of reliability and hearsay', *Computer Law and Security Review* (pp. 80–84), v.30, Issue 1.

Mata-Mouros, M.F. (2011). *Juiz das Liberdades – Desconstrução de um Mito do Processo Penal*. Coimbra: Almedina.

Mendes, C.H.C.F. (2020). *Tecnoinvestigação criminal: entre a proteção de dados e a infiltração por software*. Salvador: Editora Juspodium.

Mendes, P.S. (2013). *Lições de Direito Processual Penal*. Coimbra: Almedina.

Mendes de Almeida, J.C. (1973). *Princípios fundamentais do processo penal*. São Paulo: Revista dos Tribunais.

Moraes, A. (2019). *Direito constitucional*. (35ª ed.). São Paulo: Atlas.

Moraes, A.R.A. (2008). *Direito Penal do Inimigo: a Terceira Velocidade do Direito Penal*. Curitiba: Juruá.

Moraes, A.R.A. (2016). *Direito Penal Racional*. Curitiba: Juruá Editora.

Nether, N.A.B. (2018). *Proteção de Dados dos Usuários de Aplicativos*. Curitiba: Juruá Editora.

Nucci, G.S. (2002). *Código de Processo Penal comentado*. São Paulo: Revista dos Tribunais.

Nucci, G.S. (2015). Manual de processo penal e execução penal. (12ª ed.). Rio de Janeiro: Forense.

Oliveira, E. (2019). *O Universo da Segurança Humana*. Curitiba: Juruá Editora.

Ost, F. (1999). *O Tempo do Direito*. Tradução de Maria Fernanda de Oliveira. Lisboa: Instituto Piaget.

Owen, T. (2008). The Uncertain Future of Human Security in the UN. *International Social Science Journal of UNESCO Publication* (p. 113-118), Paris, v. 59.

Perez Luño, A.E. (1989). Los derechos humanos en la sociedad tecnológica. In: Losano, M.G.; Perez Luño, A.E.; Guerrero Mateus, M.F. Liberdad informática y leyes de proteccion de datos personales. *Cuadernos y Debates* (p. 139). Centro de estúdios constitucionales. Madrid.

Pinheiro, P.P. (2013). *Direito digital*. (5ª ed.). São Paulo: Saraiva.

Pradillo, J.C.O. (2012). "Hacking" legal al servicio de la investigación criminal: nuevos instrumentos para la investigación y prueba de la delinquencia informática', in Redacción Editorial Aranzadi, *Delincuencia Informática. Tiempos de Cautela y Amparo* (p.187–191). Navarra: Thomson Reuters Aranzadi.

Pradillo, J.C.O. (2013). *Problemas Procesales de la Ciberdelincuencia.* Madrid: Editorial Colex.

Prado, G. (2019). *A cadeia de custódia de prova no processo penal*. São Paulo: Marcial Pons.

Prittwitz, C. (2004, mar-abr). O Direito Penal entre Direito Penal do Risco e Direito Penal do Inimigo: tendências atuais em direito penal e política criminal. *Revista Brasileira de Ciências Criminais* (p.44), São Paulo, v. 47.

Programa das Nações Unidas para o Desenvolvimento - PNUD. (1994). *Relatório de desenvolvimento humano 1994: segurança humana*. Lisboa: Tricontinental.

Ramalho, D.S. (2013, out-dez). O uso de *malware* como meio de obtenção de prova em processo penal, *Revista de Concorrência e Regulação*, n. 16, ano IV, pp. 195-244.

Ramalho, D.S. (2014). A recolha de prova penal em sistemas de computação em nuvem. *Revista de Direito Intelectual* (pp. 123-162), nº 2.

Ramalho, D.S. (2014). The use of malware as a means of obtaining evidence in Portuguese criminal proceedings. *Digital Evidence and Electronic Signature Law Review* (p.55-75), 11.

Ramalho, D.S. (2017). Métodos Ocultos de Investigação Criminal em Ambiente Digital, Coimbra, Almedina.

Rangel, P. (2013). *Direito Processual Penal*. São Paulo: Atlas.

Rodrigues, B.S. (2009). *Direito Penal Parte Especial, Tomo I*. Direito Penal Informático-Digital, 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, Coimbra Editora, Limitada.

Rodrigues, B.S. (2009). *Das escutas telefónicas à obtenção da prova em ambiente digital*. (2ª ed.). Coimbra: Editora Coimbra.

Rodrigues, B.S. (2010). *Refers to the idea of digital domicile for the purpose of online searches – Da Prova Penal – Bruscamente… A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal* (pp.472–473). Lisboa: Rei dos Livros, v. 2.

Silva, C.D.M. (2015). *Tutela Penal da Intimidade*. Curitiba: Juruá Editora.

Silva, G.M. (2010). *Curso de Processo Penal*, Tomo I, Verbo.

Silva, VA. (2017). *Direitos fundamentais: conteúdo essencial, restrições e eficácia*. (2ª ed.). São Paulo: Malheiros.

Silva Sánches, J-M. (2001). *La Expansión del Derecho Penal. Aspectos de la política criminal en las sociedades postindustriales*. (2ª ed.). Madrid: Civitas.

Smith, A. (1996). *A Riqueza das Nações. Investigação sobre sua natureza e suas causas.* Vol. II. Tradução de Luiz João Baraúna. São Paulo: Nova Cultural.

Soares, G.T. (2014). *Investigação criminal e inovações técnicas e tecnológicas: perspectivas e limites*. Tese (Doutorado em Direito) – São Paulo, Faculdade de Direito da Universidade de São Paulo.

Souza, K.R.F. (2015, jul-dez). O sistema penal como instrumento de controle social: o papel da pena privativa de liberdade. *Revista de Criminologias e Políticas Criminais* (p.164-180), Minas Gerais, v.1, n.2.

Souza, Q.; Quandt, C. (2008). Metodologia de análise de redes sociais. In: Duarte, F.; Quandt, C.; Souza, Q. (Org.). *O tempo de redes*. São Paulo: Perspectiva.

Taruffo, M. (2009). *Consideraciones sobre la prueba judicial*. Madrid: Fundación Coloquio Jurídico Europeo.

Toffler, A. (1980). *A terceira onda*. Tradução de João Távora. (11ª ed.). Rio de Janeiro: Record.

Tonini, P. (2002). *A prova no processo penal italiano* (tradução de Alexandra Martins e Daniele Mróz). São Paulo: Revista dos Tribunais.

Valente, M.M.G. (2009). *Teoria Geral do Direito Policial*. (2ª ed.). Coimbra: Almedina.

Vaz, D.P. (2012). *Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório.* Tese de doutorado. São Paulo, Faculdade de Direito da Universidade de São Paulo.

Wendt, E. (2011). Ciberguerra, inteligência cibernética e segurança virtual. *Revista Brasileira de Inteligência*. Agência Brasileira de Inteligência, Brasília/DF, n. 6.

Wild, M. (2016). *Código Malicioso*. Rio de Janeiro: Harper Collins Brasil.

Documentos Eletrônicos:

Barrocu, G. (2017). Il captatore informatico: un virus per tutte le stagioni. *Rivista Diritto penale e processo* (pp. 379-390), Milano. Disponível em: https://www.unikore.it/index.php/biennio-2016-2018/i-anno/materiali-didattici/item/download/13240_801d4147469dbfd1e4692f023 979646f.

Brasil. (2017). Supremo Tribunal Federal. *21ª Audiência Pública do STF*. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf.

Brasil. (2020). Supremo Tribunal Federal. *Informativo 979*. Brasília, 25 a 29 de maio de 2020. Disponível em: http://www.stf.jus.br//arquivo/informativo/documento/informativo979.htm.

Bronzo, P. (2017). L'impiego del trojan horse informatico nelle indagini penali. *Rivista italiana per le scienze giuridiche* (pp. 329-356), Roma: Jovene Editore, n.8. Disponível em: https://www.rivistaitalianaperlescienzegiuridiche.it/sites/default/files/8.%20Bronzo%20Pasquale%20%E2%80%93%20L%E2%80%99impiego%20del%20trojan%20horse%20informatico%20nelle%20indagini%20penali.pdf.

Calavita, O. (2020). La contro-riforma bonafede delle intercettazioni: sul captatore informatico rimangono alcune perplessità. *Rivista Istituzioni Diritto Economia* (pp. 152-169), anno II, n.1. Disponível em: https://istituzionidirittoeconomia.eu/wp-content/uploads/Gen-Apr_2020/calavita_IDE_2_1_2020.pdf.

Cass., Sez. Un., 01 luglio 2016, n. 26889, Scurato, in CED n. 266905. Disponível em: http://www.archiviopenale.it/intercettazioni—cass-sez-un-1-luglio-2016-(cc-28-aprile-2016)-scurato/contenuti/6142.

Commission on Human Security (2003). *Human Security Now: Protecting and empowering people*. Report of the Commission on Human Security. New York: United Nations. Disponível em: https://reliefweb.int/report/world/human-security-now-protecting-and-empowering-people.

Curtotti, D. (2017). Il captatore informatico nella legislazione italiana. *Rivista di Scienze Giuridiche*, JusOnline n. 3. Disponível em: https://jus.vitaepensiero.it/news-papers-il-captatore-informatico-nella-legislazione-italiana-4843.html.

EUA – *US Code*. Disponível em: https://www.law.cornell.edu/uscode/text/18/2516.

European Court of Human Rights. (2006). *Weber and Saravia vs Germany (n.º 54934/00)*. Disponível em: https://opil.ouplaw.com/view/10.1093/law-oxio/e199.013.1/law-oxio-e199.

Galantini, M.N. (2011, set.). Giusto processo e garanzia costituzionale del contraddittorio nella formazione della prova. Testo della relazione al Convegno "Il diritto delle prove dall'Unità d'Italia alla Costituzione repubblicana", *Rivista Diritto Penale Contemporaneo*, Milano. Disponível em: https://archiviodpc.dirittopenaleuomo.org/d/842-giusto-processo-e-garanzia-costituzionale-del-contraddittorio-nella-formazione-della-prova.

Gomes, H.S. (2020, mai.). Whatsapp vai ser bloqueado? Entenda o processo que corre no STF. Tilt Uol, São Paulo, Seção Redes Sociais. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2020/05/20/whatsapp-vai-ser-bloqueado-entenda-o-processo-que-corre-no-stf.htm.

Gomes Filho, A.M. (2009, jul-set.). Princípios gerais da prova no Projeto de Código de Processo Penal Projeto no 156/2009 do Senado Federal. *Revista de Informação Legislativa*. Brasília a. 46 n. 183. Disponível em https://www2.senado.leg.br/bdsf/bitstream/handle/id/194929/000871238.pdf?sequence=3&isAllowed=y.

Griffo, M. (2020, set.). Il captatore informatico ed i suoi multiformi impieghi: le intrusioni non finiscono mai. *Rivista Diritto di Difesa* – 9. Disponível em: http://dirittodidifesa.eu/il-captatore-informatico-ed-i-suoi-multiformi-impieghi-le-intrusioni-non-finiscono-mai-di-mario-griffo/.

Henrique, W.G. (2006). *Anti Forensics: dificultando análises forenses computacionais*. Disponível em: http://ws.hackaholic.org/artigos/AntiForensics.ppt.

Indovina, B. (2018). I captatori informatici: una riforma troppo contenuta per uno strumento investigativo così pervasivo. *Rivista di diritto dei media*, n.2. Disponível em: http://www.astrid-online.it/static/upload/pape/paper6_indovinab.pdf.

Instituto da Defesa Nacional - IDN. (2013). *Estratégia da informação e segurança no ciberespaço. Investigação conjunta*. IDN-CESEDEN, n. 12, Lisboa. Disponível em: http://www.idn.gov.pt/publicacoes/cadernos/idncaderno_12.pdf.

Kleina, N. (2011). *A história da internet: pré-década de 60 até anos 80*. Disponível em: http://www.tecmundo.com.br/infografico/9847-a-historia-da-internet-pre-decada -de-60-ate-anos-80-infografico-.htm.

Libicki, M.C. (2009). *Cyberdeterrence and cyberwar*. RAN Corporation. Disponível em: http://www.rand.org/pubs/monographs/2009/RND_MG877.pdf.

Lopes Jr., A.; Mendes, C.H.C.F. (2019). *Vírus espião como meio de investigação: a infiltração por softwares*. Disponível em: https://www.conjur.com.br/2019-jun-07/limite-penal-virus-espiao-meio-investigacao-infiltracao-softwares.

Loubak, A.L. (2020, Fev). *WhatsApp ultrapassa 2 bilhões de usuários em todo o mundo*. Techtudo, São Paulo, Seção Redes Sociais. Disponível em: https://www.techtudo.com.br/noticias/2020/02/whatsapp-ultrapassa-2-bilhoes-de-usuarios-em-todo-o-mundo.ghtml.

Lourenço, N. (2013). S*ociedade Global, Segurança e Criminalidade*. Disponível em: http://www..fd.unl.pt/docentes_docs/ma/aens_MA_20207.pdf.

Maia, F. (2015, abr.). Juiz que proibiu WhatsApp quer forçar o app a colaborar com polícia. *Diário do Sudoeste*, São Paulo. Disponível em: https://diariodosudoeste.com.br/brasil-2/juiz-que-proibiu-whatsapp-quer-forcar-app-a-colaborar-com-policia/.

Migalhas, Redação do. (2016, Jul.) Juíza do RJ bloqueia WhatsApp em todo o país. *Migalhas*, São Paulo. Disponível em: https://migalhas.uol.com.br/quentes/242570/juiza-do-rj-bloqueia-whatsapp-em-todo-o-pais.

Norton. *Glossário de segurança na internet*. Disponível em: http://br.norton. com/security-glossary/article.

Olhar Digital. (2020). *Novo malware ataca usuários de whatsapp e facebook*. Disponível em: https://olhardigital.com.br/fique_seguro/video/novo-malware-ataca-usuarios-de-whatsapp-e-facebook/101037.

Palmieri, L. (2018). La nuova disciplina del captatore informatico tra esigenze investigative e salvaguardia dei diritti fondamentali Dalla sentenza "Scurato" alla riforma sulle intercettazioni. *Diritto Penale Contemporaneo Rivista trimestrale*, n.1. Disponível em: http://www.astrid-online.it/static/upload/pape/paper6_indovinab.pdf.

Pereira, B.C. (2016). *O Sistema de Geolocalização GPS no Processo Penal Português*: *Visão integradora ou atípica no quadro dos meios de obtenção de prova*. (pp.98-101). Tese apresentada na Universidade de Lisboa. Disponível em: https://repositorio.ul.pt/bitstream/10451/26178/1/ulfd132671_tese.pdf.

Portal UOL. (2020*). Bandidos criam "telemarketing do golpe"; entenda de vez invasão ao WhatsApp*. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2020/02/06/bandidos-criam-telemarketing-do-golpe-para-invadir-whatsapp-saiba-evitar.htm.

Revista Em Discussão. (2014) *O mundo perplexo diante do Big Brother*. Disponível em: https://ptdocz.com/doc/343198/espionagem-cibern%C3%A9tica.

RFC 3227 (2018). Diretrizes para Coleta e Arquivamento de Evidências. Trad. Tiago Souza. Disponível em: https://www.academiadeforensedigital.com.br/rfc-3227-melhores-praticas-referencias/.

Rosenbach, M.; Stark, H.; Winter, S. (2011, Oct.). Trojan Trouble: The shady past of Germany's Spyware, *Spiegel Online International*. Disponível em: http://www.spiegel.de/international/germany/trojan-trouble-theshady-past-of-germany-s-spyware-a-792276.html.

Scientific Working Group on Digital Evidence (SWGDE). Disponível em: https://www.swgde.org/.

Summary National Strategy to Secure Cyberspace of 2003. (2003). Disponível em: http://energy.gov/sites/prod/files/National%20Strategy%20to%20Secure%20Cyber space.pdf.

Supremo Tribunal Federal - STF (2017). *STF inicia audiência pública que discute bloqueio judicial do WhatsApp e Marco Civil da Internet*. Disponível em: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=345369#:~:text=A%20presidente%20do%20Supremo%20Tribunal,o%20funcionamento%20do%20aplicativo%20WhatsApp.

Supremo Tribunal Federal - STF (2020). *Informativo 979*. Disponível em: http://www.stf.jus.br/arquivo/informativo/documento/informativo979.htm.

Torre, M. (2015). *Indagini Informatiche e Processo Penale*. Tese de Doutorado em Ciências Legais. Universidade de Florença. Disponível em: https://flore.unifi.it/retrieve/handle/2158/1028650/114466/Tesi%20completa.pdf;jsessionid=B4621CB3473F3870800F93FF047A6591.suir-unifi-prod-02.

United Nations. (2000). *Secretary General salutes internacional work shop on human security in Mongólia*. Disponível em: https://www.un.org/press/en/2000/20000508.sgsm7382.doc.html.

Veloso, M.A. (2014, mar.). Ciberespionagem Global e o Decreto 8.135: Uma Avaliação da Segurança das Informações do Governo Brasileiro. CONSAD 2014, Brasília. *Anais Eletrônico*. Centro de Convenções Ulysses Guimarães Brasília/DF: CONSAD. Disponível em: http://pt.slideshare.net/mvsecuri ty/artigo-consad-2014-ciberespionagem-global-e-o-decreto-8135-uma-avaliao-da-segurana-das-informaes-do-governo-brasileiro.

Ventura, F. (2020, Fev.). WhatsApp chega a 99% dos celulares no Brasil; Telegram cresce. *Tecnoblog*, São Paulo. Seção Aplicativos e Sotware. Disponível em: https://tecnoblog.net/326932/whatsapp-chega-a-99-por-cento-celulares-brasil-telegram-cresce/.

Xavier, A.I.M. (2010). *A União Europeia e a Segurança Humana: um actor de gestão de crises em busca de uma cultura estratégica? Análise e considerações prospectivas*. Coimbra, Universidade de Coimbra. Disponível em: https://estudogeral.uc.pt/bitstream/10316/14516/3/A%20Uni%C3%A3o%20Europeia%20e%20a%20Seguran%C3%A7a%20Humana.pdf.

Legislação:

Brasil. (1988). *Constituição da República Federativa do Brasil de 1988*. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

Brasil. (1940). *Decreto-Lei nº 2.848, de 7 de dezembro de 1940*. Código Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm.

Brasil. (1941). *Decreto-Lei nº 3.689, de 3 de outubro de 1941*. Código de Processo Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm.

Brasil. (1996). *Lei nº 9.296, de 24 de julho de 1996*. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9296.htm.

Brasil. (2012). *Lei nº 12.737, de 30 de novembro de 2012*. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm.

Brasil. (2014). *Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

Espanha. (1882). *Real Decreto de 14 de septiembre de 1882, aprobatorio de la Ley de Enjuiciamiento Criminal*. Disponível em: https://www.boe.es/biblioteca_juridica/codigos/codigo.php?id=334&modo=2&nota=0&tab=2.

Espanha. (2020). *Codice di Procedura Penale*. Disponível em: https://lexscripta.it/codici/codice-procedura-penale.

Portugal. (1976). *Constituição da República Portuguesa*. Disponível em: https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx.

Portugal. (1982). *Código Penal Português*. Disponível em: https://www.codigopenal.pt/.

Portugal. (1987). *Código de Processo Penal Português*. Disponível em: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=199&tabela=leis&so_miolo=.

Portugal. (2001). *Lei 101/2001, de 25 de Agosto – Acções Encobertas*. Disponível em: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=89&tabela=leis.

Portugal. (2009). *Lei 109/2009, de 15 de Setembro – Lei do Cibercrime*. Disponível em: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis.

Nações Unidas do Brasil. (1948). *A Declaração Universal dos Direitos Humanos*. 1948. Disponível em: https://nacoesunidas.org/direitoshumanos/declaracao/.