PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS
Programa de Pós-graduação em Direito

Marcus Vinícius Pimenta Lopes

A PARTICIPAÇÃO ATIVA DO ACUSADO NA PERSECUÇÃO QUE UTILIZA A BUSCA E A APREENSÃO DE ELEMENTOS DE PROVA DIGITAIS

Belo Horizonte
2023

Marcus Vinícius Pimenta Lopes

A PARTICIPAÇÃO ATIVA DO ACUSADO NA PERSECUÇÃO QUE UTILIZA A BUSCA E A APREENSÃO DE ELEMENTOS DE PROVA DIGITAIS

Tese apresentada ao Programa de Pós-graduação em Direito da Pontifícia Universidade Católica de Minas Gerais, como requisito parcial para obtenção do título de Doutor em Direito.

Orientadora: Professora Doutora Flaviane de Magalhães Barros Bolzan de Morais

Área de concentração: Democracia, Constituição e Internacionalização.

Belo Horizonte

2023

FICHA CATALOGRÁFICA
Elaborada pela Biblioteca da Pontifícia Universidade Católica de Minas Gerais

Lopes, Marcus Vinícius Pimenta
L864p A participação ativa do acusado na persecução que utiliza a busca e a apreensão de elementos de prova digitais / Marcus Vinícius Pimenta Lopes. Belo Horizonte, 2023.
235 f.: il.

Orientadora: Flaviane de Magalhães Barros Bolzan de Morais
Tese (Doutorado) - Pontifícia Universidade Católica de Minas Gerais. Programa de Pós-Graduação em Direito

1. Brasil. Código de processo penal (1941). 2. Persecução penal. 3. Investigação criminal. 4. Busca e apreensão (processo penal). 5. Medida cautelar. 6. Prova pericial. 7. Produção de prova - Inovações tecnológicas. I. Morais, Flaviane de Magalhães Barros Bolzan de. II. Pontifícia Universidade Católica de Minas Gerais. Programa de Pós-Graduação em Direito. III. Título.

CDU: 347.628
Ficha catalográfica elaborada por Fabiana Marques de Souza e Silva - CRB 6/2086

Marcus Vinícius Pimenta Lopes

A PARTICIPAÇÃO ATIVA DO ACUSADO NA PERSECUÇÃO QUE UTILIZA A BUSCA E A APREENSÃO DE ELEMENTOS DE PROVA DIGITAIS

Tese apresentada ao Programa de Pós-graduação em Direito da Pontifícia Universidade Católica de Minas Gerais, como requisito parcial para obtenção do título de Doutor em Direito.

Área de concentração: Democracia, Constituição e Internacionalização.

Professora Doutora Flaviane de Magalhães Barros Bolzan de Morais – PUC Minas

(Orientadora)

Professor Doutor Lucas de Alvarenga Gontijo – PUC Minas

Professora Doutora Marta Cristina Cury Saad Gimenes – USP

Professor Doutor Geraldo Luiz Mascarenhas Prado – UAL

Professor Doutor Leonardo Augusto Marinho Marques – UFMG

Professor Doutor José de Assis Santiago Neto – PUC Minas

Belo Horizonte, 12 de maio de 2023.

Para Rui Caldas Pimenta e Eládio Lopes.

AGRADECIMENTOS

Ao povo brasileiro, por financiar esta pesquisa.
À minha família, principalmente à Luana, Isabella, Clara e Alexandre.
Aos meus amigos, principalmente Flaviane Barros, minha orientadora.
Aos meus professores e aos funcionários da biblioteca da PUC Minas.
A todos os que de alguma maneira contribuíram para o trabalho.

"*Quem controla o passado controla o futuro;*
quem controla o presente controla o passado"
(ORWELL, 2009, p. 47)

RESUMO

O aumento da vigilância oficial da população é viabilizado por novas tecnologias. Essas novas tecnologias são utilizadas licitamente para obter elementos relevantes para a construção do juízo pela persecução penal; contudo, são operadas frequentemente sem o conhecimento do investigado, de maneira oculta. Isso altera a dinâmica da persecução; ao invés da cognição processual centralizada na audiência de instrução e julgamento em contraditório, cada vez mais, o inquérito e as cautelares realizadas na fase investigativa – por novos meios ocultos de investigação e com total surpresa para o investigado – ganham importância. Com o objetivo de que o acusado participe ativamente da persecução que utiliza novos meios ocultos de investigação e controle dos atos investigativos, este trabalho pesquisa o problema de como assegurar a participação ativa e estratégica do acusado na persecução penal que utiliza especificamente a busca de elementos de prova digitais e a apreensão desses elementos. A partir dos marcos teóricos do modelo constitucional do processo aplicado ao processo penal (principalmente da determinação de perfectibilidade do contraditório dinâmico) e da teoria do caso (que visa beneficiar a atuação estratégica em situações concretas da persecução), a hipótese da tese é que a perfectibilidade do contraditório é possibilitada por determinadas técnicas que asseguram a participação ativa do acusado na persecução que utiliza a busca e a apreensão de elementos de prova digitais. O desenvolvimento do trabalho começa explicitando quais são as principais características distintivas da persecução penal que utiliza novas tecnologias em relação à persecução tradicional; depois, são estudadas a tecnologia e a realização da busca e da apreensão de elementos de prova digitais em conformidade com o modelo constitucional do processo. Finalmente, a "tese" da tese é aprofundada no último capítulo, a partir das construções anteriores; é proposto que para assegurar a participação ativa do acusado na persecução penal que utiliza a busca e a apreensão de elementos de prova digitais devem ser executadas técnicas diretamente relacionadas às mudanças causadas na persecução pelos meios ocultos de investigação. Como resultados, o aumento da importância dos atos realizados fora do espaço do processo de conhecimento é denunciado; é explicitado que a sociedade de controle utiliza os meios ocultos de investigação como estratégia para a vigilância rapidíssima e em todos os lugares; e é demonstrado que os efeitos ilícitos da vigilância pela sociedade de controle podem ser mitigados por técnicas jurídicas específicas que aperfeiçoam o cumprimento do modelo constitucional do processo.

Palavras-chave: medida cautelar; modelo constitucional do processo; meios ocultos de investigação; sociedade de controle; busca e apreensão.

ABSTRACT

The increase in official surveillance of the population is made possible by new technologies. These new technologies are used licitly to obtain relevant elements for the construction of judgment by criminal prosecution; however, they are often operated without the knowledge of the investigated person, in a hidden way. This alters the dynamics of criminal prosecution; instead of procedural cognition centered on the instruction hearing and contradictory trial, increasingly, the inquiry and precautionary measures carried out in the investigative phase – by new hidden means of investigation and with total surprise for the investigated person – gain importance. With the goal of making the accused actively participate in the prosecution that uses new hidden means of investigation and control of investigative acts, this work investigates the problem of how to ensure the active and strategic participation of the accused in the criminal prosecution that specifically uses the search for elements of digital evidence and the seizure of these elements. Based on the theoretical framework of the constitutional model of the process applied to criminal prosecution (mainly the determination of the perfectibility of the dynamic contradictory) and the theory of the case (which aims to benefit the strategic performance in concrete situations of prosecution), the hypothesis of the thesis is that the perfectibility of the contradictory is made possible by certain techniques that ensure the active participation of the accused in the prosecution that uses the search and seizure of digital evidence. The work begins by explaining what are the main distinctive characteristics of criminal prosecution that uses new technologies in relation to traditional prosecution; then, the technology and the search and seizure of digital evidence are studied in accordance with the constitutional model of the process. Finally, the "thesis" of the thesis is deepened in the last chapter, from the previous constructions; it is proposed that to ensure the active participation of the accused in the criminal prosecution that uses the search and seizure of digital evidence techniques directly related to the changes caused in the prosecution by the occult means of investigation should be performed. As results, the increased importance of acts performed outside the space of the knowledge process is denounced; it is explained that the society of control uses the hidden means of investigation as a strategy for very fast surveillance everywhere; and it is demonstrated that the illicit effects of surveillance by the society of control can be mitigated by specific legal techniques that improve accomplishment with the constitutional model of the process.

Keywords: precautionary procedure; constitutional model of the process; hidden methods of investigation; control society; search and seizure.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

A.	Ano
ADI	Ação Direta de Inconstitucionalidade
Art.	Artigo
Arts.	Artigos
ABNT	Associação Brasileira de Normas Técnicas
CGU	Controladoria-Geral da União
CIPAV	*Computer and Internet Protocol Address Verifier*
CNJ	Conselho Nacional de Justiça
COAF	Conselho de Controle de Atividades Financeiras
Coord.	Coordenador
Coords.	Coordenadores
CFOAB	Conselho Federal da Ordem dos Advogados do Brasil
COMPAS	*Correctional Offender Management Profiling for Alternative Sanctions*
CPP	Código de Processo Penal
CP	Código Penal
DNA	*Deoxyribonucleic acid*
E.g.	*Exempli gratia*
Et al.	*Et alii*
Etc.	*Et cetera*
FBI	*Federal Bureau of Investigation*
FISA	*Foreign Intelligence Surveillance Act*
GAFI	Grupo de Ação Financeira Internacional
GPS	*Global Positioning System*
GSM	*Global System for Mobile Communications*
HTTP	*Hypertext Transfer Protocol*
IA	Inteligência Artificial
IMSI	*International Mobile Subscriber Identity*
IP	*Internet Protocol*
ISO/IEC	*International Organization of Standardization/International Electrotechnical Commission*
LGPD	Lei Geral de Proteção de Dados Pessoais
Mt.	Mateus
N.	Número

Ns.	Números
NBR	Norma Brasileira
NSA	*National Security Agency*
NSL	*National Security Letter*
ODR	*Online Dispute Resolution*
OECD	*Organization for Economic Co-operation and Development*
Orgs.	Organizadores
RAM	*Random Access Memory*
T.	Tomo
UIF	Unidade de Inteligência Financeira
Vs.	*Versus*
WWW	*World Wide Web*

SUMÁRIO

1 INTRODUÇÃO

Em "1984", o Grande Irmão observa pela teletela:

> A teletela recebia e transmitia simultaneamente. Todo som produzido por Winston que ultrapassasse o nível de um sussurro muito discreto seria captado por ela; mais: enquanto Winston permanecesse no campo de visão enquadrado pela placa de metal, além de ouvido também poderia ser visto. Claro que não havia como saber se você estava sendo observado num momento específico. Tentar adivinhar o sistema utilizado pela Polícia das Ideias para conectar-se a cada aparelho individual ou a frequência com que o fazia não passava de especulação. Era possível inclusive que ela controlasse todo mundo o tempo todo. Fosse como fosse, uma coisa era certa: tinha meios de conectar-se a seu aparelho sempre que quisesse. Você era obrigado a viver – e vivia, em decorrência do hábito transformado em instinto – acreditando que todo som que fizesse seria ouvido e, se a escuridão não fosse completa, todo movimento examinado meticulosamente. Wiston mantinha as costas voltadas para a teletela. Era mais seguro; contudo, como sabia muito bem, mesmo as costas de uma pessoa podem ser reveladoras. (ORWELL, 2009, p. 13).

A teletela é um objeto semelhante a uma televisão estática com câmera e microfone. George Orwell morreu antes das invenções do computador e do *smartphone*, ele não tinha como imaginar que o nível de captação de informação e de vigilância poderia ser muito maior do que o possibilitado pela teletela.[1]

Este aumento da vigilância é viabilizado especialmente pela persecução penal,[2] que possibilita o uso lícito de novas tecnologias para a investigação, principalmente em nome do combate à criminalidade organizada.

A propaganda[3] de combate à criminalidade organizada impulsiona a expansão da legislação processual penal com a promessa de mais vigilância e punição (HASSEMER, 1993b, p. 61-62). Com isso, ao invés de uma política criminal[4] orientada no sentido de contrair o sistema punitivo, há o caos legislativo com a edição de várias leis direcionadas ao

---

[1] O porquê da citação da obra literária de Orwell é explicado por Warat: "É através das ficções, brincando com as significações, que podemos trair os códigos das ciências. Esse é o sentido da literatura como prática sem sujeições que dava Barthes e que nós devemos recuperar para as aulas universitárias se desejamos que elas sirvam para esquivar a grande impostura autoritária da linguagem: o congelamento das significações. [...] Não se libertam os atores sociais (os desejos) apenas com os esquemas da lógica da ciência. A construção de discursos marginais (que não dependem de um cabedal de crenças autoritárias) – demanda uma hipersensibilidade muito diferente da contida sensibilidade dos sistemas científicos. Os paradigmas da ciência explicam, mas não mudam a cabeça da gente. Para isso precisamos desviar-nos das ficções científicas, carnavalizando-as com a utopia literária." (WARAT, 1985, p. 164-166). Sobre o direito e literatura no Brasil, vide: Trindade e Bernsts (2017).

[2] A persecução penal é composta pela fase investigativa e pela fase iniciada com a ação penal (FREDERICO MARQUES, 1998a, p. 128).

[3] Na lição de Edward Bernays, a propaganda é o esforço intenso e longo de moldar os eventos para influenciar as relações do público com uma empresa, um grupo ou uma ideia (BERNAYS, 2005, p. 52).

[4] "Do incessante processo de mudança social, dos resultados que apresentem novas ou antigas propostas do direito penal, das revelações empíricas propiciadas pelo desempenho das instituições que integram o sistema penal, dos avanços e descobertas da criminologia, surgem princípios e recomendações para a reforma ou transformação da legislação criminal e dos órgãos encarregados de sua aplicação. A esse conjunto de princípios e recomendações denomina-se *política criminal*." (BATISTA, 2011, p. 33).

controle da população. São exemplos: a Lei n. 9.296, de 1996 (interceptações telefônica, informática e telemática; captação ambiental de sinais eletromagnéticos, ópticos ou acústicos); Lei Complementar 105, de 2001 (quebra do sigilo fiscal e bancário); a Lei n. 12.850, de 2013 (organizações criminosas e investigação criminal; ação controlada; colaboração premiada; agente infiltrado; acesso a registros de dados); e a Lei 13.964, de 2019 (que alterou vários pontos da legislação, incluindo a expansão do uso de agente infiltrado virtual[5]).[6]

Assim, as reformas na legislação que ambicionam o combate à criminalidade organizada utilizam as novas tecnologias, principalmente as computadorizadas, para a ampliação das possibilidades de vigilância (FIGUEIREDO DIAS, 2008, p. 23). Há um progressivo aumento do uso de novas tecnologias na persecução penal.

Estes novos meios de investigação são inseridos num cenário distinto do direito penal repressivo, como pontua Hassemer (1993b, p. 69): "O 'combate preventivo ao crime' como objetivo da atividade policial acaba por aplainar os limites entre prevenção e repressão, entre prevenção de perigos e combate ao crime que, até então separaram nitidamente os domínios policial e processual penal."

Manuel da Costa Andrade (2011, p. 534-536) defende que, além da redução dos limites entre a repressão e a prevenção de crimes (com investigações prospectivas e que, frequentemente, apuram fatos e investigados diversos dos inicialmente suspeitos) e do aumento do espaço da polícia (responsável pela maior parte dos atos investigativos), a tendência para a privatização da recolha estatal de informação e o aumento do uso de novas tecnologias caracterizam a realização dos novos meios de investigação (principalmente pela autoincriminação dos sujeitos, que são os criadores dos próprios registros interceptados e apreendidos). Esses meios que visam a obtenção de elementos probatórios por investigações operadas sem o conhecimento do investigado são nomeados pelo professor português de "métodos ocultos de investigação" (COSTA ANDRADE, 2009, p. 104).

---

[5] O agente infiltrado virtual já era previsto nos artigos 190-A a 190-E da Lei 8.069, de 1990 (a partir da redação da Lei n. 13.441, de 2017) para a investigação de crimes contra a dignidade sexual de criança e de adolescente.

[6] O mesmo cenário ocorre em outras partes do mundo, como na Alemanha: "O atual debate público sobre Política criminal veicula a impressão de que a solução do problema consiste em conferir às autoridades da segurança pública, de uma vez por todas, todos os meios e instrumentos necessários que sempre reivindicaram, a fim de que possam assenhorear-se da C.O. [criminalidade organizada]. Nada mais falso e enganoso. Precisamente nos últimos anos as autoridades da segurança pública foram equipadas com uma gama de poderosos instrumentos legais coercitivos que vinham incessantemente reclamando. Na Alemanha eles foram acolhidos tanto nas legislações policiais e de ordem pública dos Estados quanto nos códigos penal e de processo da federação: agentes secretos, testemunhas da coroa (aquelas que, em troca da revelação do crime e seus autores, têm a sua própria participação perdoada ou tratada com benignidade), observação policial prolongada da vida das pessoas, escuta telefônica ampliada, proteção de testemunhas (que restringe a ação da defesa), captação e armazenamento de dados pessoais com larga escala, licitações para a prática da observação policial, escuta por meios eletrônicos, penas patrimoniais, punibilidade da lavagem de dinheiro." (HASSEMER, 1993b, p. 68-69).

1.1 Este trabalho

Partindo do exposto acima, este trabalho pesquisa especificamente o seguinte problema: como assegurar a participação do acusado na persecução penal que utiliza o meio oculto da busca de elementos de prova digitais e a apreensão desses elementos?

A escolha por este recorte ocorre em função da importância dos elementos de prova digitais para a cognição sobre os casos penais na sociedade atual, cada vez mais virtualizada. Somado a isso, o recorte possibilita a explicitação de diversos aspectos relacionados ao aumento da vigilância operado pelas novas tecnologias de investigação.

A pesquisa é regida por dois marcos teóricos: o modelo constitucional do processo e a teoria do caso.

Quanto ao primeiro marco teórico, desde o segundo pós-guerra existe a intensificação do movimento de aproximação entre a Constituição e o processo na busca pela racionalização do exercício do poder e cumprimento dos direitos fundamentais. Nesse movimento, o processo passa a ser entendido como direito fundamental que possibilita o controle do exercício das funções do Estado e assegura o respeito aos demais direitos fundamentais (BARACHO, 1984, p. 5) (CAPPELLETTI, 1976, p. 1-19). Na busca por racionalização do exercício do poder, Andolina e Vignera propõem que o processo é um modelo constitucional caracterizado pela: a) expansividade, decorrente da hierarquia constitucional dos institutos processuais, consistente na sua idoneidade em ser aplicado nos diversos ramos processuais; b) variabilidade, consistente na sua adaptação às especificidades desses ramos; e c) perfectibilidade, consistente na possibilidade da lei infraconstitucional aperfeiçoar o cumprimento dos institutos processuais constitucionalizados, assim como criar novos, desde que consonantes com o modelo geral (ANDOLINA; VIGNERA, 1997, p. 8-11). Sendo que a aplicação do modelo constitucional no processo penal exige consideração com as suas especificidades, vez que o provimento pretendido e as garantias processuais penais apresentam características próprias – a "base principiológica uníssona" que orienta o processo penal é composta também pelo estado de inocência, por exemplo, o que o distingue dos demais ramos (BARROS, 2008b, p. 14-17).[7]

[7] "Uma interpretação constitucionalmente adequada passa pela noção de que o modelo constitucional do processo é uma base principiológica uníssona, na qual os princípios que o integram são vistos de maneira co-dependente. Ou seja, ao desrespeitar um dos princípios se afeta também, de forma reflexa, os outros princípios fundantes." (BARROS, 2008b, p. 16-17). Sobre as diferentes proposições relacionadas ao processo constitucional, vide: Pimenta (2020).

A perfectibilidade do contraditório dinâmico – que não é simplesmente o *audiatur et altera pars*, é a participação ativa (ANDOLINA; VIGNERA, 1997, p. 172), configurada pela garantia de influência efetiva na construção do procedimento e pela garantia de não surpresa, que implica na exigência de provocação do juiz para que as partes se manifestem previamente sobre quaisquer questões, incluindo as de conhecimento *ex officio* (NUNES, 2008, p. 227-229) – na persecução que utiliza a busca e a apreensão de elementos de prova digitais é o foco deste trabalho.

Quanto à teoria do caso, ela é um método de análise com enfoque estratégico[8] na situação prática que visa beneficiar a atuação concreta dos sujeitos processuais. Os fatos, o Direito e as provas são simultaneamente considerados com o objetivo de possibilitar melhores inferências sobre os fatos e a postura ativa das partes em situações específicas (BENAVENTE CHORRES, 2011, p. 48).[9] Nesta pesquisa sobre a situação específica da participação ativa do acusado na persecução que utiliza a busca e a apreensão de elementos de prova digitais, isso significa que apesar da busca e da apreensão ser realizada na maioria das vezes na fase investigativa, seu impacto em toda a persecução penal será analisado com foco na resolução dos problemas concretos relacionados à participação do acusado na produção da prova.

A hipótese da pesquisa é de que a perfectibilidade do contraditório é possibilitada por determinadas técnicas[10] que asseguram a participação ativa do acusado na persecução que utiliza a busca e a apreensão de elementos de prova digitais. Em relação a cada uma das quatro principais características distintivas da persecução que utiliza meios ocultos frente à persecução do direito penal repressor tradicional (COSTA ANDRADE, 2011, p. 534-536)[11] é proposta a execução de técnicas específicas que efetivam[12] essa participação ativa.

Com base no modelo constitucional do processo (BARROS, 2008b, p. 14-17) e na teoria do caso (BENAVENTE CHORRES, 2011, p. 48), é proposta a hipótese de que para assegurar a participação ativa do acusado na persecução penal que utiliza a busca e a apreensão de elementos de prova digitais devem ser executadas técnicas diretamente relacionadas às mudanças causadas pelos meios ocultos de investigação: em relação à diminuição da fronteira entre repressão e prevenção de delitos, a cadeia de custódia de

[8] Com estratégia significando a melhor maneira de argumentar sobre determinado caso, para ser entendido e auxiliar ativamente a construção do juízo (HOLMAN, 2012, p. 28-29).

[9] "[…] a teoria do caso representa um aparato conceitual de caráter sistêmico que articula análises no plano fático, jurídico e probatório, beneficiando tanto as partes, que terão um maior amparo de seus interesses no processo, participando de forma ativa, quanto o juiz, que terá, à sua disposição, um conjunto de elementos informativos detalhado que lhe permitirá melhores inferências acerca dos fatos." (BARILLI, 2019, p. 116).

[10] "a técnica nada mais é que um agir humano voltado para um fim" (AGAMBEN, 2017, p. 91-92). Vide o capítulo 5, *infra.*

[11] Vide o último parágrafo do item 1, *supra.*

[12] Efetividade no sentido de cumprimento de finalidades, não de redução de custo dos meios (MIRANDA COUTINHO, 2002, p. 692).

elementos digitais, por possibilitar perceber se a investigação foi prospectiva ou baseada em elementos concretos preexistentes; em relação ao aumento do espaço da polícia e da importância da fase investigativa, o direito de confrontar os agentes públicos e privados envolvidos em audiência; em relação à tendência para a privatização da recolha estatal de informação, a proteção contra a autoincriminação por medidas antiforenses e pela atuação judicial na proteção preventiva das garantias processuais; e em relação ao progressivo aumento do uso de novas tecnologias na persecução penal, a paridade entre as partes no espaço virtual pela ampliação do uso dessas tecnologias pelo acusado.

Por revisão bibliográfica transdisciplinar – que abandona "o mito da divisão natural do saber" e, ao invés de estudar os ramos da ciência como ilhas autônomas, rompe suas fronteiras e considera os diversos saberes como influentes uns nos outros (MIAILLE, 2005, p. 60-62) – envolvendo Direito, cibernética[13] e história, o desenvolvimento da pesquisa ocorre em quatro capítulos.

Para a melhor compreensão da mutação causada pelas novas tecnologias de investigação, o capítulo 2 cuidará das diferenças da persecução penal que utiliza os meios ocultos de investigação em relação à do direito penal repressor tradicional. Como é uma comparação entre atos de diferentes momentos históricos e como há a necessidade de explicitar a dinâmica de poder envolvida, o capítulo 2 aplica a genealogia do poder como metodologia historiográfica (FOUCAULT, 2015b, p. 55-86, 262-295); o que é detalhado em item próprio.

O capítulo 2 demonstra, em primeiro lugar, que a diminuição da fronteira entre repressão e prevenção de delitos é consequência do aumento de vigilância na sociedade de controle (DELEUZE, 2008a; 2008b) e que os meios ocultos de investigação são frequentemente utilizados ilegalmente em investigações prospectivas. Em segundo lugar, pontua que o aumento do espaço da polícia na persecução penal ocorre em função dela centralizar a análise de riscos na rede de vigilância (ERICSON; HAGGERTY, 2007, p. 34-38). Em terceiro lugar, explicita que a tendência para a privatização da recolha estatal de informação ocorre pela autoincriminação dos indivíduos (em telefonemas e e-mails interceptados, revelações a agentes infiltrados *etc.*) e de empresas (em leniências, delações, comunicações rotineiras e colaboração das empresas de tecnologia com o Estado) na rede de vigilância composta por agências públicas e privadas. E, em quarto lugar, o capítulo pesquisa

[13] A cibernética é o estudo da comunicação por máquinas autômatas "ou seja, as que são capazes de realizar operações que, durante a execução, podem ser corrigidas, de tal modo que cumpram melhor seu objetivo. Essa correção chama-se *retroalimentação* (*feedback*). Como essa é a característica fundamental das operações realizadas pelo homem ou por qualquer ser inteligente, essas máquinas também são chamadas de *inteligentes* ou de *cérebros eletrônicos*, já que seu funcionamento se deve às propriedades físicas do elétron." (ABBAGNANO, 2007, p. 133).

o progressivo aumento do uso de novas tecnologias na persecução penal tendo como premissa que cada nova tecnologia é um novo potencial de otimização dos resultados na sociedade de controle (DELEUZE, 2008b, p. 221-226) e que o computador, especialmente, influencia várias outras tecnologias de vigilância da população (ERICSON; HAGGERTY, 1999, p. 237-244).

Explicitadas as diferenças da persecução penal que utiliza meios ocultos de investigação frente ao direito penal repressor tradicional, o trabalho passa a tratar especificamente da busca e da apreensão de elementos de prova digitais nos capítulos 3, 4 e 5.

O capítulo 3 apresenta noções sobre as tecnologias envolvidas na busca e na apreensão de elementos de prova digitais. É explicado o que é um computador e como funciona o espaço virtual, tendo como marco teórico as proposições de Penrose[14] (1993). Este ponto é fundamental vez que, sem o conhecimento básico da tecnologia envolvida, é impossível entender o funcionamento da busca e da apreensão de elementos digitais. Na sequência do capítulo, são pesquisadas tecnologias específicas de busca e de apreensão no espaço virtual.

O capítulo 4 demarca a conceituação, requisitos e procedimentos legais relacionados à busca e à apreensão de elementos de prova digitais em acordo com o modelo constitucional do processo aplicado ao processo penal (BARROS, 2008b, p. 14-22). Seu objeto é analisar as divergências jurídicas sobre o tema e diversos aspectos envolvidos, como a necessidade de cooperação internacional para a obtenção de elementos digitais e a ilicitude probatória.

Amparado no desenvolvimento dos demais capítulos, o capítulo 5 aprofundará na execução das técnicas relacionadas às situações concretas de participação ativa do acusado na persecução penal que utiliza a busca e a apreensão de elementos de prova digitais – considerando as mudanças dessa persecução em relação à do direito penal repressor tradicional, a partir da teoria do caso (BENAVENTE CHORRES, 2011, p. 48) e com a finalidade de perfectibilidade do contraditório dinâmico do modelo constitucional do processo (ANDOLINA; VIGNERA, 1997, p. 9, 172) (NUNES, 2008, p. 227-229) –, quais sejam: a cadeia de custódia virtual (em relação à diminuição da fronteira entre repressão e prevenção de delitos); o direito ao confronto contra os agentes investigadores (em relação ao aumento do espaço da polícia); a proteção contra a autoincriminação, utilizando-se medidas antiforenses ou não (em relação à tendência para a privatização da recolha estatal de informação); e a paridade entre as partes no espaço virtual (em relação ao progressivo aumento do uso de novas tecnologias na persecução penal).

[14] Prêmio Nobel de Física em 2020. Prêmio Wolf de Física em 1988 (com Stephen Hawking). Professor da *University of Oxford*.

"O Grande Irmão está de olho em você", escreveu George Orwell (2009, p. 12) em sua distopia, cada vez mais real, "1984". O objetivo da tese é que você, pelo processo, também possa "estar de olho" no Estado, para controlar o exercício do poder e fazer cumprir a lei democrática na realização dos meios ocultos de investigação, principalmente na busca e na apreensão de elementos de prova digitais.

2 MEIOS OCULTOS DE INVESTIGAÇÃO NA SOCIEDADE DE CONTROLE

As características que distinguem a persecução penal que utiliza meios ocultos de investigação da persecução do direito penal repressivo tradicional são a chave para a compreensão da mudança na dinâmica da atuação dos sujeitos processuais (consequentemente, da participação do acusado na persecução penal que utiliza o meio oculto da busca de elementos de prova digitais e a apreensão desses elementos, o problema da tese).

Estas características – que não são específicas da busca e da apreensão de elementos digitais, mas comuns a todos os meios ocultos de investigação –, como destacado na introdução, são: a diminuição da fronteira entre a repressão e a prevenção de delitos; o aumento do espaço da polícia; a tendência para a privatização da recolha estatal de informação (mormente pela autoincriminação); e a expansão do uso de novas tecnologias pela persecução penal (COSTA ANDRADE, 2011, p. 534-536).

Meios ocultos de investigação são métodos que visam a obtenção de elementos probatórios por investigações operadas sem o conhecimento do investigado (COSTA ANDRADE, 2009, p. 104). A pesquisa historiográfica das características da transformação da persecução penal pelos meios ocultos tornará mais explícita essa transformação e possibilitará o enfrentamento da questão de como assegurar a participação do acusado na construção do juízo.

Destaca-se que a pesquisa da história neste trabalho não é realizada para o melhor conhecimento dos fatos de alguma "história oficial", ela é feita para expor a dinâmica das relações de poder na execução das técnicas jurídicas e a transformação dessa dinâmica pelo uso de meios ocultos de investigação. Por isso é utilizada a metodologia historiográfica da genealogia do poder (FOUCAULT, 2015b, p. 55-86, 262-295), como detalhado em sequência.

2.1 Metodologia historiográfica: genealogia do poder

A genealogia pesquisa os efeitos do exercício do poder, não como pesquisa da origem de um fenômeno (como se fosse possível acessar uma "identidade ainda preservada"), mas como a pesquisa da proveniência das relações de poder e das condições de emergência dos saberes.[15]

[15] O saber é aquilo que possibilita a apropriação e utilização de um discurso; um discurso, por sua vez, é um conjunto de signos que demarca uma enunciação no espaço e tempo. O saber rege o discurso. O discurso só "faz sentido" se relacionado ao saber (FOUCAULT, 2014a, p. 105, 220).

Não há uma "meta-história" a ser revelada. A genealogia não visa descobrir a origem; não há investigação sobre a essência das coisas, sobre a causa primeira dos fenômenos ou sobre a narrativa mais idêntica ao que se passou.[16] A genealogia não é uma metafísica.[17] A genealogia é a pesquisa da proveniência das marcas singulares nos sujeitos, das relações de força, e da emergência das táticas e saberes que viabilizam o exercício do poder (FOUCAULT, 2015b, p. 55-86).[18]

Ela tem cinco precauções fundamentais: primeira, analisar o exercício do poder nas suas extremidades, principalmente nas suas consequências e técnicas; segunda, analisar as práticas, não as razões oficiais; terceira, enxergar o poder como uma relação exercida em rede, envolvendo tanto a dominação como a resistência; quarta, o silêncio dos excluídos deve ser considerado, as relações de poder devem ser pesquisadas partindo da capilaridade, a genealogia é uma "microfísica do poder"; quinta, devem ser pesquisadas as funções dos saberes e das técnicas nas relações de poder (FOUCAULT, 2015b, p. 282-289).

Nas palavras do professor francês:

> [...] meu discurso não procura obedecer às mesmas leis de verificação que regem a história propriamente dita, uma vez que esta tem como único fim dizer a verdade, dizer o que se passou, no nível do elemento, do processo, da estrutura das transformações. Eu diria, de maneira muito mais pragmática, que, no fundo, minha máquina é boa; não na medida em que ela transcreve ou fornece o modelo do que passou, e sim na medida em que ela consegue dar do que se passou um modelo tal que permita que nos libertemos do que se passou. (FOUCAULT, 2013, p. 150).

Portanto, a genealogia não é a pesquisa da história linear, como se existisse alguma evolução ou destino, e nem de alguma "identidade ainda preservada" a ser revelada por

[16] "A questão do poder ou mais especificamente a questão do poder disciplinar torna-se, para Foucault, um instrumento de análise capaz de explicitar a emergência dos saberes. É esta análise que Foucault, adotando explicitamente agora uma terminologia nietzscheana chama de Genealogia. [...] Nietzsche teria recusado, segundo ele, três postulados relativos à noção de origem a que se refere tradicionalmente a noção de genealogia: o da *origem-essência* que corresponderia à suposição de que a origem é o lugar da essência das coisas, isto é, a concepção da origem como revelação da plenitude; o da *origem-perfeição* que considera que depois da origem o que se segue é sempre degradação, decadência: captar a origem seria então encontrar o intemporal e o incorruptível; e o da *origem-verdade*: a origem concebida como o lugar da própria verdade." (CALVET DE MAGALHÃES, 1987, p. 70).

[17] A biblioteca de Aristóteles foi herdada por Teofrasto. Teofrasto deixou sua biblioteca para Neleu, que levou os livros para Escépcis (hoje pertencente à Turquia). Receoso de que os governantes se apoderassem dos livros, Neleu os escondeu em sua adega, onde permaneceram até o bibliotecário Apelicão comprá-los em 100 a.C. e levá-los para Atenas. Em 86 a.C., o romano Lúcio Cornélio Sula dominou Atenas, se apropriou dos livros e os enviou para Roma. Em Roma, a função de organizar os livros coube ao bibliotecário Andrônico de Rodes. Em sua organização dos escritos de Aristóteles, Andrônico de Rodes nomeou um conjunto de quatorze livros sem títulos que vinham após o livro "Física" como "os livros que vêm depois da Física" ou "*tá metá tá physicá*" (VALLE, Gabriel, 2007, p. 3) (VALLE, Gabriel; VALLE, Sofia, 2012, p. 7). Posteriormente, o conteúdo dos quatorze livros, o estudo do fundamento primeiro, foi associado ao vocábulo "metafísica". Sobre este tema, vide, também: Abbagnano (2007, p. 660-667).

[18] A genealogia de Foucault, segundo o próprio (FOUCAULT, 2015b, p. 55-61), é influenciada por Nietzsche. Vide: Nietzsche (2013, p. 25-28, 74-76), sobre a genealogia da moral.

alguém. É a pesquisa da proveniência das relações de poder e das condições de emergência dos saberes que possibilitam a dominação ou a resistência dos sujeitos.[19] As transformações das relações de poder e os efeitos concretos das técnicas nessas relações são seu objeto.[20]

Aplicada neste trabalho, a genealogia do poder explicitará as transformações operadas pelas novas tecnologias investigativas na persecução penal e a dinâmica de poder envolvida. A partir da pesquisa historiográfica realizada, o problema de como assegurar a participação do acusado na persecução que utiliza meios ocultos de investigação poderá ser melhor entendido e enfrentado.

2.2 Diminuição da fronteira entre repressão e prevenção de delitos

O centro da compreensão das modificações causadas na persecução penal pelo uso de novos meios ocultos está na intensificação da vigilância na "sociedade de controle" – que busca controlar no "céu aberto", sem término e com alta velocidade, utilizando a rede de informações alimentada tanto por agências públicas como por privadas e que é operada principalmente pelo computador (DELEUZE, 2008a, p. 216; 2008b, p. 220). A diminuição da fronteira entre repressão e prevenção de delitos tem relação direta com essa intensificação de vigilância; o que será demonstrado pela comparação da sociedade de controle com a sociedade disciplinar.

No século XVIII, como demonstrou Michel Foucault (2008b), ocorreu uma mudança significativa na dinâmica do poder de castigar. Cumprindo os anseios da ascendente burguesia que se beneficiava da Revolução Industrial e buscava regulamentação da conduta dos indivíduos para atender à nova economia, a punição, ao invés de se impor mais intensamente no corpo, passou a ser imposta mais intensamente na vontade, nas disposições. Da punição de alguns indivíduos em cerimônias longas por suplícios demorados e espetaculosos, resultado de procedimentos envolvidos de arbitrariedades pelos acusadores e juízes, foi operada uma passagem para a punição generalizada e controlada numa gestão de eficiência no castigo. Essa então nova punição, mais constante e distribuída, era vinculada a um sistema legal que diminuiu em alguma medida os excessos, tanto na punição como na indulgência e,

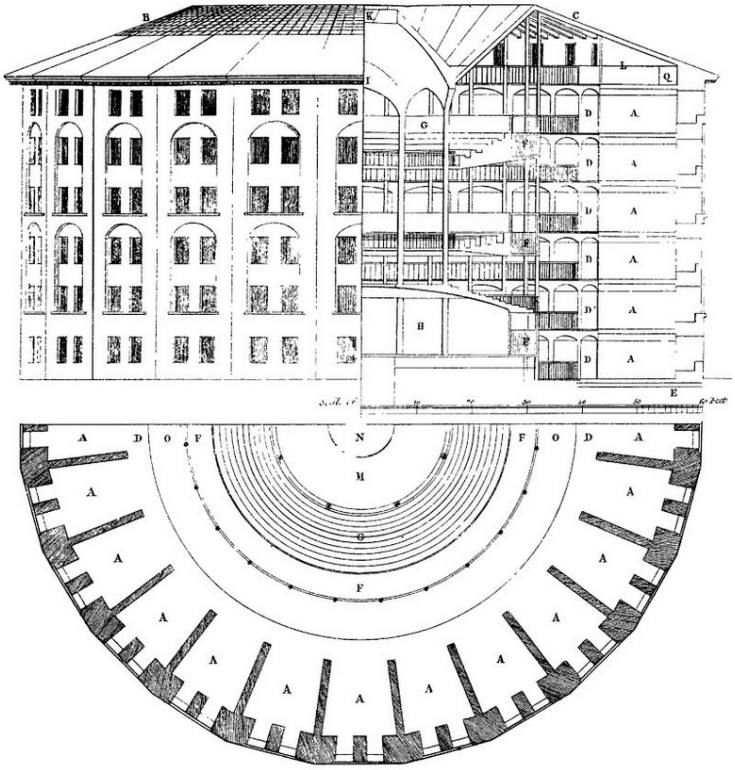
[19] O saber-poder inquisitório é um exemplo de saber que possibilita a dominação e o saber-poder acusatório é um exemplo de saber que possibilita a resistência. Sobre o tema, vide: Pimenta (2019).

[20] "Temos antes que admitir que o poder produz saber (e não simplesmente favorecendo-o porque o serve ou aplicando-o porque é útil); que poder e saber estão diretamente implicados; que não há relação de poder sem constituição correlata de um campo de saber, nem saber que não suponha e não constitua ao mesmo tempo relações de poder. [...] não é a atividade do sujeito de conhecimento que produziria um saber, útil ou arredio ao poder, mas o poder-saber, os processos e as lutas que o atravessam e que o constituem, que determinam as formas e os campos possíveis do conhecimento." (FOUCAULT, 2008b, p. 27).

simultaneamente, estabeleceu a expansão da quantidade de punições com meios mais eficientes para o aumento de controle. Era uma nova economia da pena, mais calculada, dirigida à disposição do sujeito, operada sobre o tempo da existência do indivíduo, que era colocado como exemplo para que os outros não desviassem do padrão estabelecido. A pena deixava de ser apenas a afirmação do poder soberano e tornava-se, principalmente, a reativação de um código de conduta estabelecido pelo conjunto de proprietários autores da nova legislação. Essa dinâmica da punição era um retrato da sociedade nomeada por Foucault (2008b, p. 173) de "sociedade disciplinar", que visava a obediência de todo o corpo social ao padrão de conduta estabelecido pelos que controlavam a circulação das riquezas.

A arquitetura de efetivação da sociedade disciplinar é a do panóptico de Bentham.

Figura 1 – Planta da estrutura do Panóptico idealizado por Bentham
(desenho do arquiteto inglês Willey Reveley, 1791)



Fonte: Wikipedia (2020)

No panóptico existe uma torre central de vigilância onde o inspetor observa; em volta estão as celas onde o observado não sabe se é vigiado. Essa arquitetura possibilita centralidade da vigilância e sua invisibilidade. As vantagens são relacionadas à facilitação da inspeção: aparente onipresença do inspetor; necessidade de menos funcionários para a vigilância; melhor controle hierárquico (pelos relatórios e pela simplificação da vigilância); e

inspeção mais rápida nas celas (BENTHAM, 2008, p. 20-23; 30-33). O panóptico proporciona uma vigilância constante, permanentemente registrada, e que, em função de ser invisível ao observado, o estimula a agir como se sempre estivesse sendo analisado, o que tendencia o indivíduo a uma autorrestrição. O poder, assim, opera de forma automática: mesmo sem a observação concreta do indivíduo num determinado momento, por não ver o vigia, o indivíduo é estimulado a alterar o seu comportamento em todo o tempo pelo receio de estar sendo observado (FOUCAULT, 2008b, p. 153, 162-172). O resultado é a facilitação da inspeção e da consequente sanção àquele que desvia do padrão de conduta estabelecido como normal pelos proprietários do século XVIII, produzindo "máquinas sob a aparência de homens" (BENTHAM, 2008, p. 78).

O projeto de Bentham (de 1791) foi que a mesma arquitetura de panóptico fosse aplicada tanto nos presídios como nas fábricas, nos hospícios, nos hospitais e nas escolas: em todos esses lugares a vigilância aparentemente onipresente por uma autoridade central invisível possibilitaria a melhor economia na efetivação da disciplina[21] (BENTHAM, 2008, p. 57-84).

Na sociedade disciplinar, num primeiro momento a ofensa ao código é percebida pelo vigia; na sequência, é realizado um exame sobre o indivíduo, que o qualifica, classifica e determina a medida de sua punição conforme uma metodologia regida por um determinado saber. Esse exame objetifica o indivíduo, transformando sua singularidade em um caso a ser enquadrado no padrão "normal" de conduta. No momento da sanção, a repressão ao indivíduo é uma reativação do código e um estímulo para que o desvio não ocorra novamente (FOUCAULT, 2008b, p. 154-161; 2001, p. 108-111). Como observa Lucas Gontijo, Bentham "foi tanto o primeiro a preocupar-se com a *intencionalidade do infrator* quanto o mentor do *Estado que tudo observa mas não é observado.*" (GONTIJO, 2019, p. 129, grifos do autor).

A sociedade disciplinar inaugura uma biopolítica. A biopolítica é "o que faz com que a vida e seus mecanismos entrem no domínio dos cálculos explícitos, e faz do poder-saber um agente de transformação da vida humana" (FOUCAULT, 2015a, p. 154). Nela, a população (que não é a soma dos indivíduos, mas a espécie humana governada)[22] de um território é dirigida por uma política de segurança; numa acepção biológica, a vida da população num meio é governada pela política (FOUCAULT, 2008a, p. 3, 14-15, 29-30).

[21] "De uma maneira global, pode-se dizer que as disciplinas são técnicas para assegurar a ordenação das multiplicidades humanas." (FOUCAULT, 2008b, p. 179).
[22] A população "[…] é aquilo sobre o que se age por meio de educação, das campanhas, dos convencimentos. A população é portanto tudo o que vai se estender do arraigamento biológico pela espécie à superfície de contato oferecida pelo público" (FOUCAULT, 2008a, p. 98-99).

2.2.1 A sociedade de controle

Foucault escreveu sobre a sociedade disciplinar do século XVIII ao início do século XX. De lá para cá muito aconteceu. A velocidade, as tecnologias e os controladores do exercício do poder se aprimoraram. Sobre isso, é fundamental a contribuição intelectual de Gilles Deleuze (2008b), que explica o aumento da intensidade da vigilância na "sociedade de controle".

Deleuze (2008b) defende que, desde a Segunda Guerra, o controle constante e ultrarrápido sobre todos vem sendo paulatinamente expandido numa escala que não era anteriormente possível e que foi viabilizada pelas novas tecnologias cibernéticas.[23]

Na proposição do autor, na sociedade de controle o foco não é a punição de um indivíduo. A singularidade do sujeito é dividida em cifras incognoscíveis aos que não têm acesso aos códigos e todos são classificados em bancos de dados. Mais que a punição por confinamento de um indivíduo, controla-se preventivamente – e em escala gigantesca – blocos inteiros de perfis de pessoas armazenadas nos bancos de dados. Assim, não importa tanto a punição repressiva de alguns sujeitos (apesar de ela não ter sido abandonada), importa mais a constante prevenção de danos pelo máximo de controle ultrarrápido sobre todos (DELEUZE, 2008b, p. 220-224).

Na sociedade de controle, movida pelas sensações de crise constante e de permanente e urgente necessidade de reforma,[24] não importa muito a conduta do indivíduo no longo prazo, importa mais o resultado provável (num sentido de probabilidade) no curto prazo. O controle

[23] Vide a nota n. 13, *supra*.

[24] Exemplificadamente, percebe-se facilmente a sensação de crise constante na criminologia midiática. Nela, há a manipulação do medo estrategicamente utilizada para obterem-se determinados efeitos. O medo é um sentimento instintivo de autopreservação contra um perigo. Na criminologia midiática há a manipulação desse instinto. Num primeiro ato, a mídia separa a sociedade entre homens de bem e de mal. Num segundo ato, um determinado sujeito de um grupo que tenha cometido alguma ação é colocado como exemplo de causa dos problemas sociais; como um jovem negro que tenha sido flagrado com substância entorpecente colocado como a imagem do traficante. No terceiro ato, é feita uma identificação por semelhança: se um jovem negro foi encontrado com droga, outros jovens negros parecidos são potenciais suspeitos de tráfico. No quarto ato, a sociedade manipulada pede o controle de todo o grupo suspeito, mesmo que isso implique na redução de garantias jurídicas e éticas. Como resultado, tanto o grupo alvo da criminologia midiática como todos os afetados pela redução de garantias passam a estar mais sujeitos ao controle (ZAFFARONI, 2012, p. 303-324). O grupo eleito pela mídia como bode expiatório pode ser qualquer um (como já foram os estudantes, os advogados, os juízes, os políticos *etc*.). O ponto é que a manipulação é constante; a todo o tempo a mídia bombardeia os jornais com novos relatos de novos casos, envolvendo novos grupos de inimigos e é estimulado que a sociedade está em permanente crise, necessitando sempre de novas reformas que aumentem o controle. Essa impressão de crise permanente é chamada por Deleuze de "*moratória ilimitada das sociedades de controle*" e, também existe, com magnitude de efeitos diversa, na rivalidade infinita nas empresas, na formação acadêmica interminável e no acúmulo de capital como fim em si. Destaca-se que a sensação de crise constante e o consequente permanente clamor por reformas se faz presente em múltiplas esferas da vida na sociedade de controle – e, como nota Deleuze, enquanto os sujeitos estão ocupados em projetos infinitos, os controladores exercem o domínio social (DELEUZE, 2008a, p. 216; 2008b, p. 221-222).

necessita de tempo para ser exercido. Com a possibilidade de operação ultrarrápida proporcionada pelos computadores, o controle também passou a ser ultrarrápido. Do confinamento pontual vigiado num lugar fechado da sociedade disciplinar, passa-se para o controle constante, ultrarrápido (preferencialmente preventivo) e em todos os lugares da sociedade de controle. Não como a substituição de um modelo de sociedade por outro, mas como a convivência de ambos e um aumento gradativo da intensidade de vigilância (DELEUZE, 2008a, p. 217-218; 2008b, p. 224-226).[25]

O esfacelamento da singularidade do sujeito dividida em cifras de bancos de dados, a codificação da vida, o controle ininterrupto e ultrarrápido, os efeitos drásticos nos processos de subjetivação, tudo isso operado por computadores em escala gigantesca e causando mudanças significativas nas relações de poder; essa é a configuração da sociedade de controle. De acordo com Deleuze (2008b, p. 220-221, 224-225): "O controle é de curto prazo e de rotação rápida, mas também contínuo e ilimitado"; as prisões caminham para penas "'substitutivas', ao menos para a pequena delinquência, e a utilização de coleiras eletrônicas que obrigam o condenado a ficar em casa em certas horas"; as escolas gradativamente abandonam a pesquisa e, com formação permanente para atender ao mercado, criam técnicos avaliados continuamente; os hospitais resgatam "doentes potenciais e sujeitos à risco"; tudo vira empresa, "uma alma, um gás" permanentemente em transformação para prever e otimizar os resultados – "Não cabe temer ou esperar, mas buscar novas armas".

Indissociável do exercício do poder, o Direito é profundamente alterado na sociedade de controle. Na busca por resultados práticos, o perigo, o risco e a segurança substituem o dano, a ofensa a bem jurídico e a distribuição de justiça do sistema penal liberal (HASSEMER, 1993a, p. 279).

A política criminal deixa de visar a repressão do delinquente individual e passa a promover análises de riscos. Ao invés da reeducação de alguém, é preferido o controle de

[25] "Os confinamentos são *moldes*, distintas moldagens, mas os controles são uma *modulação*, como uma moldagem auto-deformante que mudasse continuamente, a cada instante, ou como uma peneira cujas malhas mudassem de um ponto a outro. Isto se vê claramente na questão dos salários: a fábrica era um corpo que levava suas forças internas a um ponto de equilíbrio, o mais alto possível para a produção, o mais baixo possível para os salários; mas numa sociedade de controle a empresa substituiu a fábrica, e a empresa é uma alma, um gás. Sem dúvida a fábrica já conhecia o sistema de prêmios, mas a empresa se esforça mais profundamente em impor uma modulação para cada salário, num estado de perpétua metaestabilidade, que passa por desafios, concursos e colóquios extremamente cômicos. Se os jogos de televisão mais idiotas têm tanto sucesso é porque exprimem adequadamente a situação da empresa. A fábrica constituía os indivíduos em um só corpo, para a dupla vantagem do patronato que vigiava cada elemento na massa, e dos sindicatos que mobilizavam uma massa de resistência; mas a empresa introduz o tempo todo uma rivalidade inexplicável como sã emulação, excelente motivação que contrapõe os indivíduos entre si e atravessa cada um, dividindo-o em si mesmo. O princípio modulador do "salário por mérito" tenta a própria Educação nacional: com efeito, assim como a empresa substitui a fábrica, a *formação permanente* tende a substituir a escola e o controle contínuo substitui o exame." (DELEUZE, 2008b, p. 221).

grupos suspeitos e a incapacitação seletiva de perfis. São feitos cálculos dos níveis de delinquência num âmbito macro. A pluralidade da população é enquadrada em classificações que tentam criar subgrupos homogêneos, visando a predição de quais perfis ameaçam mais a segurança (PRATT, 1995, p. 21-24).[26] Guiada pela "periculosidade", a política criminal adere ao direito penal do autor, o caso penal[27] sai do foco e entra a história pregressa analisada segundo algum saber científico preditivo (CANÊDO; LEMOS, 2021, p. 16-21).[28]

A permanente sensação de crise[29] sacrifica as garantias processuais (como o contraditório, a ampla defesa, a paridade entre as partes e o estado de inocência) pelo combate ao inimigo[30] e o processo de conhecimento é visto como um entrave para a confirmação do que já foi apurado cautelarmente e pelo inquérito[31]; por isso, o processo de cognição – que exige tempo para o exercício das garantias processuais – tende a ser ilicitamente acelerado e o espaço cautelar aumenta em importância e em quantidade de atos (BARROS, 2018, p. 21-23)

[26] O *Correctional Offender Management Profiling for Alternative Sanctions* (COMPAS) é um exemplo escandaloso disso. O COMPAS é um *software* de inteligência artificial projetado para auxiliar órgãos judiciais a identificarem o risco de reincidência criminal de um indivíduo. Skeem e Louden (2021) explicam que ele funciona atribuindo o risco baixo, médio ou alto aos indivíduos conforme sua classificação em "fatores criminógenos" supostamente aceitos pela criminologia – certamente não a crítica – como "atitudes antissociais", "sentimentos antissociais", "dependência química", "pouca afetividade parental" e "autoestima". Esta predição determinista se provou falsa. Apesar de seu criador Tim Brennan dizer que o COMPAS era "racialmente neutro" (BRENNAN; DIETERICH, 2018, p. 49, tradução nossa: "race-neutral"), o *software* classificou negros que nunca reincidiram nos dois anos seguintes como de alto risco de reincidência em 44,9% dos casos; com os brancos, a classificação errada ocorreu em 23,5% das vezes. Já as pessoas negras classificadas como de baixo risco de reincidência que cometeram novos crimes nos anos seguintes foi de 28,0%; e as de brancos classificados como de baixo risco de cometerem novos crimes, mas que cometeram, foi de 47,7%. Ou seja, os (muitos) erros da predição do sistema foram quase duas vezes maiores quando o classificado era negro (ANGWIN; LARSON; KIRCHNER, 2021).

[27] "Para expressar essa reconstituição que se efetiva no processo penal – geralmente de forma conflitual, mas não sempre –, e tem importância prática já na primeira fase de persecução penal, o ideal seria uma expressão ainda não comprometida com outros significados relevantes: caso penal, por exemplo. Trata-se, entenda-se bem, de encontrar uma palavra, uma expressão, adequada ao fenômeno que se dá no processo e, dessa maneira, o melhor é deixar, na medida do possível, um menor espaço à indeterminação, por sua natureza sempre presente. Caso penal cumpre o requisito a contento." (MIRANDA COUTINHO, 1989, p. 134-135).

[28] O que frequentemente é ignorado pelos analistas de risco é a advertência de Raffaele De Giorgi (2008, p. 38): "risco e perigo são produzidos conforme o observador e o destinatário; constrói-se uma gritaria ecológica do saber; fica-se imune à realidade do risco (que é a realidade do não-saber); formam-se os *experts* em risco e se oculta o risco dos *experts*".

[29] Vide a nota n. 24, *supra*.

[30] "No que respeita à *razão* (motivação) de ser da concepção de inimigo, podemos aferir que os inimigos para o Direito penal são aqueles que representam uma ameaça à segurança cognitiva ou do seu comportamento se extrai um estádio de perigosidade ao sistema ou ordem jurídico social. Razões de segurança do coletivo implicam que, como no *Anónimo de Jâmblico*, o ser humano se encontre em estado de ilegalidade e, por isso, gere desconfiança e risco permanente para a comunidade, devendo essa ameaça ser extirpada." (VALENTE, 2016, p. 50). Vide também: Barros (2011).

[31] Como anotado em outro trabalho, com base em Foucault, no inquérito: "Ao invés da dependência da 'sorte' em ordálias e duelos e a manifestação viva e presente da verdade, pelo inquérito há uma produção racional da verdade sobre o passado segundo um conjunto de regras estabelecidas pelo poder" (PIMENTA, 2019, p. 80). Nas palavras do professor francês: "O inquérito era o poder soberano que se arrogava o direito de estabelecer a verdade através de um certo número de técnicas regulamentadas." (FOUCAULT, 2008b, p. 185). Destaca-se que o inquérito policial brasileiro tem como finalidades: a formação da opinião da acusação sobre o delito; e a demonstração de existência ou inexistência de justa causa para a ação penal ou de necessidade cautelar (GOMES FILHO; BADARÓ, 2007, p. 193).

(afinal, a resposta rápida cautelar – tanto a pessoal como a probatória e a patrimonial – atende mais à pressão por controle ultrarrápido do que o processo de conhecimento).

Há "Um movimento de mistura e confusão de águas que se acentua à medida que tanto a prevenção como a repressão se deslocam cada vez mais para o campo avançado (*Vorfeld*) da ocorrência dos fatos criminosos" (COSTA ANDRADE, 2011, p. 535) e o processo penal passa a ocupar um lugar central na vigilância constante ultrarrápida e preferencialmente preventiva de grupos de suspeitos na sociedade de controle.

De um sistema focado na repressão, caminha-se para um focado na prevenção; em que se prende preventivamente e a cautelaridade probatória e patrimonial também ganham importância, numa antecipação de efeitos que só deveriam ocorrer eventualmente pelo processo de conhecimento ou de execução (BARROS, 2018, p. 21-23).

Os grandes viabilizadores deste controle constante ultrarrápido são os meios ocultos de investigação, realizados principalmente antes do início da ação penal, autorizados rapidamente e que imediatamente possibilitam a obtenção unilateral de informações sensíveis antes inacessíveis – sendo que a difícil fiscalização quanto à regularidade de sua realização é estratégica para a expansão do controle por permitir aos controladores operar sem resistência. Com isso – e mascarando sua flagrante ilegalidade sob a descoberta inevitável e o encontro fortuito[32]–, interceptações telefônicas de suspeitos viram grandes operações sobre fatos antes desconhecidos, gravações ambientais sobre um sujeito investigam pessoas diversas, agentes infiltrados investigam fatos novos não previamente demarcados na autorização judicial e delações premiadas sem comprovações "fundamentam" prisões cautelares que estimularão novos delatores a revelar novos fatos.

O resultado é a redução da fronteira entre a repressão e a prevenção dos delitos elementar a esses meios, numa tentativa de atuação antes do fato criminoso, e não após (frequentemente, e ilicitamente, não por investigação de fatos específicos, mas de grupos suspeitos em potencial – lembrando que não é incomum a investigação de "traficantes conhecidos" sem qualquer situação concreta no Brasil, por exemplo). Com isso, o sistema penal gradativamente aumenta seu potencial de vigilância e viabiliza o controle preventivo de suspeitos que caracteriza a sociedade de controle.

O que se destaca é que a diminuição da fronteira entre a repressão e a prevenção dos delitos é consequência desta intensificação de vigilância na sociedade de controle (DELEUZE, 2008b, p. 224) e que, no processo penal, utiliza os meios ocultos de investigação como técnicas preferidas pela sua velocidade e potencial de controlar.

[32] Vide os itens 4.16.1 e 4.16.2, *infra.*

2.3 Aumento do espaço da polícia

Compreender a magnitude do potencial de vigilância possibilitado pelos meios ocultos de investigação na sociedade de controle é fundamental para entender o porquê do aumento do espaço da polícia, a executora dos meios ocultos na persecução penal; o que é a segunda característica da persecução que utiliza meios ocultos de investigação.

Ressalta-se que a genealogia da polícia brasileira é imensamente importante não só porque a polícia é a principal executora dos meios ocultos de investigação. Ela é a porta de entrada da persecução e grande parte das testemunhas ouvidas em audiências são os próprios policiais.

Na sequência, primeiro será feita a genealogia da polícia – o que explicitará sua proveniência e sua complexa institucionalização. Depois disso, a função da polícia na persecução que utiliza novos meios de investigação será tratada.

2.3.1 Genealogia da polícia

A polícia moderna emerge da nova distribuição do patrimônio no século XVIII. Na Inglaterra, com a Revolução Industrial e aumento da produção armazenado em estoques, surgiu a demanda dos donos da produção de proteção desse patrimônio contra os famintos e pobres que passaram a ter contato direto com a riqueza nos centros urbanos em expansão. Para atender aos donos da produção na proteção de armazéns, estoques e docas é instituída a polícia como aparelho do Estado. Na França, contra a pilhagem camponesa em propriedades cada vez menores e mais disputadas, a polícia é instituída para exercer a segurança dos proprietários agrícolas[33] (FOUCAULT, 2013, p. 100-101) (ZAFFARONI, 2012, p. 92) (MAIER, 2003, p. 390-391).

Como demonstra Foucault, a polícia primeiro foi uma utopia, depois uma prática e depois uma disciplina acadêmica. Como utopia, ela foi pensada como mantenedora da ordem pública; cuidaria da educação, dos necessitados, da circulação de mercadorias e do território.

[33] "[na França] haverá essa perpétua ideia fixa da pilhagem camponesa, da pilhagem da terra, desses vagabundos e trabalhadores agrícolas frequentemente desempregados, na miséria, vivendo como podem, roubando cavalos, frutas, legumes etc. Um dos grandes problemas da Revolução Francesa foi o de fazer desaparecer esse tipo de rapina camponesa. As grandes recoltas políticas da 2ª parte da Revolução Francesa na Vendeia e na Provença foram de certa forma o resultado político de um mal-estar dos pequenos camponeses, dos trabalhadores agrícolas que não encontravam mais, nesse novo sistema de divisão de propriedade, os meios de existência que tinham no regime de grandes propriedades agrícolas." (FOUCAULT, 2013, p. 101).

Envolvendo diversas funções administrativas (como as ligadas ao exército e ao controle da propriedade e das estradas), a polícia foi primeiro pensada como algo que englobava a relação do homem com um território, incluindo desde suas relações de propriedade ao controle de doenças. Neste primeiro momento utópico, a polícia teve como objeto o cuidado do homem. Como prática, o aparelho estatal organizou a polícia como controladora especializada de diversos âmbitos da vida – como a religião, a moralidade, a saúde, o abastecimento, as vias públicas, a segurança pública, as artes, o comércio, as fábricas, o trabalho e os pobres. A missão da polícia seria conduzir a sociedade ao padrão de felicidade estabelecido pelos governantes. Seu objeto passou a ser a vida, o controle da produção do indivíduo. Como disciplina acadêmica, a polícia manteve a missão de condução a determinado padrão de felicidade; contudo, passou a ter como estratégia, principalmente, a intervenção na conduta dos indivíduos; formou-se um saber sobre como deveria operar a ação policial, incluindo a consideração sobre como é povoado um território, informações demográficas, como é a circulação de mercadorias e maior consideração com as leis. O objeto da polícia torna-se a segurança na relação da população com o território, a gestão da vida num meio. Para tanto, ela intervém ativamente na conduta dos indivíduos amparada num saber acadêmico. A polícia passa a ser um agente da biopolítica e "Sendo a população apenas aquilo de que o Estado cuida, visando, é claro, ao seu próprio benefício, o Estado pode, ao seu bel-prazer, massacrá-la" (FOUCAULT, 2004, p. 309-316). Como anotam Lucas Gontijo e Douglas Price (2020, p. 251), no exercício da biopolítica a população é objeto de "cuidado" policial, num sentido semelhante ao cuidado dos humanos com os animais, de controle da sua vida.

Da utopia para a prática, e daí para a disciplina acadêmica (séculos XVI a XVIII), o que ocorreu foi a consolidação do aumento da interferência do Estado na gestão da vida dos indivíduos (biopolítica)[34] pela polícia, que assume a função de braço operacional do poder disciplinar, de agente do biopoder. No século XVIII, com base na disciplina acadêmica que organiza a regulação da população, o objeto da polícia não é matar (como o soberano podia fazer na sociedade da soberania que antecedeu à disciplinar), mas exercer o poder sobre a vida "de cima a baixo" (FOUCAULT, 2015a, p. 150):

> Em suma, a polícia do século XVIII, a seu papel de auxiliar da justiça na busca dos criminosos e de instrumento para o controle político dos complôs, dos movimentos de oposição ou das revoltas, acrescenta uma função disciplinar. Função complexa, pois une o poder absoluto do monarca às mínimas instâncias de poder disseminadas na sociedade; pois, entre essas diversas instituições fechadas de disciplina (oficinas, exércitos, escolas), estende uma rede intermediária, agindo onde aquelas não podem intervir, disciplinando os espaços não disciplinares; mas que ela recobre, liga entre

[34] Vide o item 2.2, *supra.*

> si, garante com sua força armada: disciplina intersticial e metadisciplina. (FOUCAULT, 2008b, p. 177).

No século XVIII, a polícia exerce a função de estimular o povo a obedecer a uma disciplina. O sentido do vocábulo "polícia", etimologicamente derivado do grego Πολιτεία (*politeía*), que significa governo da cidade (CÂMARA LEAL, 1942, p. 80), fica mais claro com este esclarecimento; a polícia moderna é um instrumento da biopolítica.

As configurações de polícia composta por agentes profissionais que mais se difundiram nos séculos XVIII e XIX no ocidente foram a francesa e a inglesa. Na França, a *gendarmerie*, de proveniência militar, foi instituída durante a Revolução, em 1791, e substituiu a *maréchaussée* (que desde 1526 tinha a atribuição de conhecer de crimes de "vagabundos" e de "ladrões de estradas" e desde 1564 passou a ter a atribuição de também combater os delinquentes do campo [ESMEIN, 1882, p. 41-42]). Centralizada, de hierarquia militar, regida pela disciplina, a *gendarmerie* francesa tinha como função assegurar a ordem e chegou a servir ao exército de Napoleão (MAIER, 2003, p. 393-394). Em Paris, desde 1667, existia, também, a tenência de polícia criada por Luís XIV para impedir panfletos de adversários do monarca e da Igreja (como judeus, protestantes e outros vários), espionar e combater inimigos; subordinados à tenência, na linha de frente, atuavam comissários e inspetores que cumpriam as funções de juízes de instrução, de mediadores e de controlar os espiões (como os observadores pagos periodicamente e as prostitutas) (FOUCAULT, 2008b, p. 176). No *Code des Délits et des Peines* de 1795 (arts. 19 e 20), a França separou a polícia administrativa para manter a ordem pública e prevenir delitos e criou a polícia judiciária para apurar crimes que não se conseguiu impedir e auxiliar juízes na investigação, numa especialização da atuação policial e com maior observância da legalidade (FRANÇA, 2020).[35]

A Inglaterra repulsou a configuração francesa e no início do século XIX criou uma polícia descentralizada, com uniformes que a tornavam visíveis e controláveis por todos; composta por civis, a polícia inglesa tinha formação profissional e a persuasão dos agentes locais era mais importante que a obediência à ordem hierárquica (MAIER, 2003, p. 393). Os *constables* de Londres tinham como função assegurar a ordem, mas, para isso, não deviam

[35] Próximo à Revolução de Julho de 1830, em março de 1829, também foram criados guardas civis uniformizados em Paris (MONET, 2001, p. 49-52). Entre a *gendarmerie* de 1791 e os guardas civis de Paris de 1829, Napoleão uniu o exercício espetacular de demonstração de poder da sociedade da soberania com a hierarquia e disciplina da sociedade disciplinar e influenciou significativamente na passagem de uma sociedade à outra: "A sociedade disciplinar, no momento de sua plena eclosão, assume ainda com o Imperador o velho aspecto do poder de espetáculo. Como monarca ao mesmo tempo usurpador do antigo trono e organizador do novo Estado, ele recolheu numa figura simbólica e derradeira todo o longo processo pelo qual os faustos da soberania, mas manifestações necessariamente espetaculares do poder apagaram-se um por um no exercício cotidiano da vigilância, num panoptismo em que a penetração dos olhares entrecruzados há de em breve tornar inúteis a águia e o sol." (FOUCAULT, 2008b, p. 179).

intervir mais que o necessário. Como lembra Monet, no século XIX a legitimidade da atuação da polícia já é questionada e a configuração da polícia da Inglaterra se popularizou mais que a da França na Europa (até Napoleão III chegou a enviar delegação para a Inglaterra para aprender sobre a polícia inglesa) (MONET, 2001, p. 51-53).

Contudo, seja a polícia francesa ou a inglesa, todas elas foram criadas como aparelho de Estado para proteger o patrimônio dos proprietários dos séculos XVIII e XIX e efetivaram o biopoder necessário à sociedade disciplinar emergente; intervindo, cada vez mais, nos múltiplos aspectos da vida do indivíduo.

O Brasil preferiu a configuração francesa (CÂMARA LEAL, 1942, p. 82). Após a fuga de Dom João VI para o Brasil (1807-1808), foi criada a Divisão Militar da Guarda Real da Policia no Rio de Janeiro pelo Decreto de 13 de maio de 1809 para disciplinar a população ao estilo europeu; nas palavras do príncipe regente fugitivo: "com a possível semelhança daquella que com tão reconhecidas vantagens estabeleci em Lisboa" (BRASIL, 2020b); que, por sua vez, foi inspirada na *gendarmerie* e na tenência de polícia francesa (COTTA, 2020, p. 1) (ZULLI, 2018, p. 43-58).

O Código de Processo Criminal de Primeira Instância, de 1832, também foi influenciado pela França[36] e atribuiu a investigação criminal a juízes de paz, sob inspiração do juízo de instrução francês (PIERANGELLI, 1983, p. 99-106) (ZACCARIOTTO, 2005, p. 66-67).[37] E, após movimentos como a Cabanagem (1832-1835), a Revolução Farroupilha (1835-1845), a Sabinada (1837-1838) e a Balaiada (1838-1841), na ambição de domínio interno, o Império do Brasil editou a Lei n. 261, de 1841, que reformou o Código de Processo Criminal fazendo com que, ao invés de juízes de paz, que eram eleitos[38], a investigação criminal fosse conduzida por chefes de polícia, delegados e subdelegados escolhidos pelo imperador ou pelos presidentes das províncias, num regime centralizado (e com maior protagonismo da polícia do que na própria França, que manteve o juízo de instrução). Posteriormente, após pressão dos oligarcas liberais, as funções de polícia administrativa, polícia judiciária e de juiz

[36] A revolucionária, não a napoleônica, em função da atuação dos oligarcas liberais na redação do Código de 1832: "Quando da abdicação, o Partido Liberal dividiu-se em dois grupos. Um deles formava a facção denominada de *jurujubas* ou *farroupilhos liberais exaltados*, que, embora entendesse ter se constituído na força que determinou a queda do Imperador, encontrava-se fora das decisões governamentais. O outro, chamava-se *chimangos*, a ala liberal moderada e que se encontrava no poder. Uma terceira força política era formada pelos *caramurus*, restauradores, que postulavam o retorno de D. Pedro I e que apresentava uma linha conservadora. Com os liberais, ainda que os moderados, formando o Gabinete, o Código do Processo Criminal só poderia ser orientado num sentido liberal." (PIERANGELLI, 1983, p. 100).

[37] Sobre o juízo de instrução, vide: Pradel (1996).

[38] Pelos homens, proprietários e brancos – a exclusão de mulheres, analfabetos e negros do processo eleitoral permaneceu por décadas no Brasil. Vide: Ramayana (2005, p. 7-12).

foram separadas e foi criado o inquérito policial pela Lei n. 2.033, de 1871, regulamentada pelo Decreto n. 4.824, para apurar repressivamente a autoria e materialidade dos casos penais.

Na Primeira República, os militares foram protagonistas: promoveram o golpe de Estado que a proclamou e governaram de 1889 a 1894, primeiro liderados pelo Marechal Deodoro da Fonseca e depois por Floriano Peixoto, que havia sido ministro da guerra do Exército (os oligarcas civis assumiram o governo apenas posteriormente). Especificamente quanto ao processo penal, a polícia continuou conduzindo a primeira fase da persecução (sendo que o inquérito policial foi abolido brevemente em alguns estados e no Distrito Federal)[39] (ZACCARIOTTO, 2005, p. 47-50).[40]

No Estado Getulista, o aumento do espaço da polícia se intensificou, principalmente durante o Estado Novo, momento em que foi decretado o Código de Processo Penal brasileiro, de 1941. Segundo a Exposição de Motivos do Código, redigida por Francisco Campos:

> As nossas vigentes leis de processo penal asseguram aos réus, ainda que colhidos em flagrante ou confundidos pela evidencia das provas, um tão extenso catálogo de garantias e favores, que a repressão se torna, necessariamente, defeituosa e retardatária, decorrendo daí um indireto estímulo à expansão da criminalidade. Urge que seja abolida a injustificável primazia do interesse do indivíduo sobre o da tutela social. Não se pode continuar a contemporizar com pseudodireitos individuais em prejuízo do bem comum. O indivíduo, principalmente quando vem de se mostrar rebelde à disciplina jurídico-penal da vida em sociedade, não pode invocar, em face do Estado, outras franquias ou imunidades além daquelas que o assegurem contra o exercício do poder público fora da medida reclamada pelo interesse social. Este o critério que presidiu à elaboração do presente projeto de Código. No seu texto, não são reproduzidas as fórmulas tradicionais de um mal-avisado favorecimento legal aos criminosos. O processo penal é aliviado dos excessos de formalismo e joeirado de certos critérios normativos com que, sob o influxo de um mal-compreendido individualismo ou de um sentimentalismo mais ou menos equívoco, se transige com a necessidade de uma rigorosa e expedita aplicação da justiça penal. (BRASIL, 2020g).

[39] "Com a Constituição Republicana de 1891, o Distrito Federal e os Estados-Membros passaram a ter competência para legislar em matéria processual – desse período, destaca-se que no 'Codigo do Processo Penal para o Distrito Federal', de 1924, a investigação era realizada majoritariamente pela polícia, mas seu registro era feito em dois autos distintos. No primeiro, os autos de investigação, eram juntados, *e.g.*, os registros do exame de corpo de delito, do flagrante, das buscas e apreensões e os documentos relacionados ao suposto delito. No segundo, nos autos de inquirição, feitos em apartado, eram registradas as declarações de pessoas que tinham conhecimento sobre os fatos. […] Em 1928, período de greves trabalhistas, que tinha presidente Washington Luís e em que 'A questão social se converte – quer tenha pronunciado ou não a frase o último presidente da República Velha – numa questão de polícia.' (FAORO, 2008, p. 756), o inquérito policial foi reestabelecido pelo Decreto 5.515, tendo sido determinado em seu art. 33 que 'O inquerito policial, quando concluido ou no caso do art. 19, paragrapho unico. acompanhará sempre a denuncia ou queixa, iniciadora da acção penal, e, merecendo valor até prova em contrario, será incorporado aos autos do processo.'" (PIMENTA, 2019, p. 102-103).

[40] Na Primeira República, em 1918, também foi dissolvida a organização civil paramilitar da Guarda Nacional pelo Decreto n. 13.040 (art. 22). Criada no início da Regência (1831), em substituição às milícias, para que os aristocratas rurais escravocratas exercessem o controle local (FARIA, 1977, p. 9-13), a Guarda Nacional foi instrumento dos "coronéis". Sobre o "coronelismo", vide obra clássica de Victor Nunes Leal (2012).

Neste Código contra o "rebelde à disciplina jurídico-penal da vida em sociedade", o inquérito continua conduzido pela polícia judiciária, é registrado em autos que são transpostos para a fase iniciada com a ação penal[41] e a audiência tem como testemunhas frequentes os próprios policiais. No que importa a esta pesquisa, destaca-se que durante a sua vigência, o CPP de 1941 permaneceu como lei regente do processo penal no pós-guerra e, também na ditadura militar.

Somado a isso, tanto a Constituição de 1934 (art. 167) como a Constituição de 1946 (art. 183) colocaram a Polícia Militar como reserva do Exército; de acordo com Pontes de Miranda:

> Escrevíamos nos Comentários à Constituição de 1934 (II, 438): "As polícias militares entraram na Constituição. Entidades intraestatais possuem Exércitos. Não sejamos ingênuos. Foi isso que a Constituição de 1934 permitiu […] É um mal, consagremos o mal. Enegre-se o futuro? Desafiemo-lo." […] Sociologicamente, as polícias militares são consequências do ditarorialismo estadual, que o presidencialismo de 1891 a 1946 vem organizando, na razão direta da decadência intelectual e moral do país: presidencialismo múltiplo, esteado em fôrças armadas também múltiplas, e organizado em simetrias tribais (federal e local) de centro, para que se retarde a democratização do país. A luta passa a ser só entre centro federal e centros estaduais, Rei e senhores feudais. Como antes do século XVIII. (1947, p. 133).[42]

Por óbvio, a expansão do espaço da polícia aumentou na ditadura militar. Pelo Decreto-lei n. 317, de 1967 (BRASIL, 2020h), a Polícia Militar foi novamente configurada como força auxiliar e reserva do Exército. Tendo como missão a manutenção da ordem pública nos estados, nos territórios e no Distrito Federal, à ela foram atribuídas as funções de: policiamento ostensivo; atuação preventiva "como fôrça de dissuasão, em locais ou áreas específicas, onde se presuma ser possível a perturbação da ordem"; atuação regressiva "em caso de perturbação da ordem, precedendo o eventual emprêgo das Fôrças Armadas"; e atender ao executivo federal na situação de guerra "ou para prevenir ou reprimir grave subversão da ordem ou ameaça de sua irrupção". Em 1969, pelo Decreto-lei n. 667, foi-lhe atribuída, também, a função "de assegurar à Corporação o nível necessário de adestramento e disciplina ou ainda para garantir o cumprimento das disposições deste Decreto-lei […]" por

[41] Sobre a necessidade de exclusão dos autos do inquérito da fase iniciada com a ação penal para a efetivação da imparcialidade, vide: Pimenta (2019).

[42] A Polícia Militar não teve sua configuração demarcada de forma detalhada na Constituição de 1937 e obedeceu ao arbítrio do ditador Getúlio Vargas, vez que: "A Carta de 1937 não teve, porém, aplicação regular. Muitos de seus dispositivos permaneceram letra morta. Houve ditadura pura e simples, com todo o Poder Executivo e Legislativo concentrado nas mão do Presidente da República, que legislava por via de decretos-leis que ele próprio depois aplicava, como órgão do Executivo." (AFONSO DA SILVA, 1999, p. 85). Durante o Estado Novo, permaneceu vigente a Lei n. 192, de 1936, que organizava a Polícia Militar como reserva do Exército, cumprindo o artigo 167 da Constituição de 1934.

meio da sua convocação em conjunto pelo executivo federal (BRASIL, 2020e). No fim dos anos 1960, a Polícia Militar foi organizada como órgão de exército; centralizada, obediente à hierarquia e à disciplina (SULOCKI, 2007, p. 108).

Num momento singular de massacre da população pelo autoritarismo, à Polícia Militar coube agir como órgão de segurança no exercício da biopolítica, tanto preventiva quanto repressivamente. Em 1973, pelo Decreto n. 73.332, a ditadura militar também reorganizou[43] a Polícia Federal para: agir como polícia marítima, aérea e de fronteiras; exercer a censura; assegurar a incolumidade física do Presidente da República e de outros agentes públicos; e reprimir e prevenir crimes de interesse da União (BRASIL, 2020c).[44]

A Constituição de 1988 manteve a Polícia Militar como força auxiliar e reserva do Exército (com a atribuição de policiamento ostensivo e a preservação da ordem pública); a Polícia Civil como polícia judiciária para apurar casos penais (exceto os militares); e a Polícia Federal para atuar preventiva e repressivamente nos casos penais de interesse da União (com atribuições expressas de atuar contra o tráfico ilícito de entorpecentes e drogas afins, o contrabando e o descaminho; atuar em casos de repercussão interestadual ou internacional; ser a polícia judiciária da União; e também ser polícia marítima, aeroportuária e de fronteiras) (BRASIL, 2020a).[45] O que se destaca é que a Polícia Militar continuou como órgão de exército, a Polícia Civil continuou como polícia judiciária responsável pelo inquérito e a Polícia Federal continuou como polícia preventiva e repressiva nos casos de interesse da União – as configurações das polícias do período da ditadura militar foram mantidas pela Constituição de 1988.

[43] A Polícia Federal foi criada pelo Estado Novo em 1944. Pelo Decreto-lei n. 6.378, a Polícia Civil do Distrito Federal foi transformada no Departamento Federal de Segurança Pública para, no Distrito Federal, ser polícia judiciária e administrativa e, no território nacional, ser polícia marítima, aérea e de fronteiras (BRASIL, 2020f).

[44] Segundo a Comissão Nacional da Verdade (2014, p. 963) sobre a atuação estatal durante a ditadura militar: "Conforme se encontra amplamente demonstrado pela apuração dos fatos apresentados ao longo deste Relatório, as graves violações de direitos humanos perpetradas durante o período investigado pela CNV, especialmente nos 21 anos do regime ditatorial instaurado em 1964, foram o resultado de uma ação generalizada e sistemática do Estado brasileiro. Na ditadura militar, a repressão e a eliminação de opositores políticos se converteram em política de Estado, concebida e implementada a partir de decisões emanadas da presidência da República e dos ministérios militares. Operacionalizada através de cadeias de comando que, partindo dessas instâncias dirigentes, alcançaram os órgãos responsáveis pelas instalações e pelos procedimentos diretamente implicados na atividade repressiva, essa política de Estado mobilizou agentes públicos para a prática sistemática de detenções ilegais e arbitrárias e tortura, que se abateu sobre milhares de brasileiros, e para o cometimento de desaparecimentos forçados, execuções e ocultação de cadáveres. Ao examinar as graves violações de direitos humanos da ditadura militar, a CNV refuta integralmente, portanto, a explicação que até hoje tem sido adotada pelas Forças Armadas, de que as graves violações de direitos humanos se constituíram em alguns poucos atos isolados ou excessos, gerados pelo voluntarismo de alguns poucos militares."

[45] De menor relevância para esta pesquisa, a Constituição (art. 144) também coloca como órgãos de segurança pública a polícia rodoviária federal (para o patrulhamento ostensivo das rodovias federais); a polícia ferroviária federal (para o patrulhamento ostensivo das ferrovias federais); os corpos de bombeiros militares (para atuar na defesa civil); e as polícias penais federal, estaduais e distrital, criadas pela Emenda Constitucional n. 104, de 2019 (para atuar no sistema prisional) (BRASIL, 2020a).

Claro que o conteúdo das atuações policiais foi modificado pela Constituição democrática. A Polícia Militar não pode mais torturar e a Polícia Federal não pode mais exercer a censura, por exemplo.[46] O ponto é que a Constituição não promoveu reformas que extirpassem do sistema jurídico brasileiro o desenho institucional das polícias feito pela ditadura militar. E, com a Lei da Anistia (n. 6.683, de 1979), a própria permanência da tradição autoritária desses órgãos foi facilitada.[47]

Toda esta genealogia da polícia foi feita para explicitar a configuração desta instituição que é central no processo penal: a polícia é a porta de entrada da persecução e a função judicial atua apenas num segundo momento, na legitimação ou contenção dos atos policiais (ZAFFARONI, 2012, p. 433) e grande parte das testemunhas ouvidas em audiências são os próprios policiais. Somado a isso:

> Há modelos deteriorados em que os juízes são muito débeis e não tem possibilidade alguma de controlar, limitando-se praticamente a se submeter à legitimação formal do poder policial. No geral, respondem a sistemas com Executivos muito fortes, bastante onipresentes, a cujo serviço acreditam que as agências executivas estão (até que se descontrolam, entram em conflito com elas e lhes dão golpes de Estado, desestabilizando-os). (ZAFFARONI, 2012, p. 433).

Contudo, o Brasil não é totalitário e nem autoritário, é um Estado Democrático de Direito.[48] A polícia não pode agir sem limites e nem em primazia da ordem hierárquica sobre o sistema jurídico democrático. A legitimidade da atuação da polícia emana da mesma fonte que legitima a atuação de todas as funções públicas: da participação democrática do povo nas funções legislativa, administrativa e judicial pelo exercício do processo.[49] Num primeiro momento, o povo estabelece, pelo processo legislativo, a legalidade democrática regente da

[46] Sobre a atuação destes órgãos na ditadura militar, vide o Relatório da Comissão Nacional da Verdade (2014).

[47] Somente em 2018 o Brasil foi condenado pela Corte Interamericana de Direitos Humanos por não ter investigado e punido os responsáveis por crimes cometidos contra os cidadãos durante a ditadura militar no Caso Herzog e outros *vs*. Brasil. De acordo com Orlando Zaccone (2021, p. 248): "Foi num contexto de uma anistia negociada, através das relações civil-militares voltadas para a manutenção da hegemonia política dos grupos dominantes, que o legado autoritário da ditadura foi incorporado na Constituição Brasileira em vigor, na forma da exceção permanente na segurança pública."

[48] Sobre a diferença entre os regimes totalitário e autoritário: "O princípio do Líder não estabelece nenhuma hierarquia no Estado totalitário, como não o faz no movimento totalitário; a autoridade não se filtra de cima para baixo através de todas as camadas intermediárias até a base da estrutura política, como no caso dos regimes autoritários. A razão concreta é que não há hierarquia sem autoridade: e, a despeito dos muitos erros de interpretação cometidos em relação à 'personalidade autoritária', o princípio da autoridade é, para todos os efeitos, diametralmente oposto ao princípio do domínio totalitário. O seu caráter primígeno já aparece na história romana: ali a autoridade, sob qualquer forma, visa a restringir ou limitar a liberdade, mas nunca a aboli-la. O domínio totalitário, porém, visa à abolição da liberdade e até mesmo à eliminação de toda espontaneidade humana e não a simples restrição, por mais tirânica que seja, da liberdade." (ARENDT, 2012, p. 543).

[49] Todos os atos policiais devem respeito à legalidade democrática: a precedência da lei democrática é requisito da atuação policial. Sem o respeito à legalidade democrática, todos os atos policiais são viciados e devem ser sancionados com a nulidade (VALENTE, 2009, p. 137-142).

atuação policial. Num segundo momento, pelo direito de petição, pela publicidade, pela ampla defesa e pelos demais princípios componentes do modelo constitucional do processo, o povo participa da concretização dos atos policiais e os fiscaliza. Nas palavras de Manuel Monteiro Guedes Valente: "A Polícia é ou deve ser, hoje, um garante da liberdade do cidadão face às ofensas ilícitas concretizadas e produzidas quem por outrem quer pelo próprio Estado."; e deve tratar o povo, que é quem promove a atuação democrática que legitima o exercício policial, como sujeito de direitos, não como objeto (VALENTE, 2009, p. 39, 51, 128).

Assim, existe uma herança histórica da polícia relevante de ser explicitada, um desenho institucional da polícia criado pela ditadura militar e mantido pela Constituição de 1988 – facilitado pela Lei da Anistia – e, simultaneamente, um sistema jurídico que tem a democracia e o limite ao exercício do poder como fundamentos. A contradição é evidente, sendo por isso que a Comissão Nacional da Verdade (2014, p. 971) recomendou, por exemplo, quanto à Polícia Militar que:

> A atribuição de caráter militar às polícias militares estaduais, bem como sua vinculação às Forças Armadas, emanou de legislação da ditadura militar, que restou inalterada na estruturação da atividade de segurança pública fixada na Constituição brasileira de 1988. Essa anomalia vem perdurando, fazendo com que não só não haja a unificação das forças de segurança estaduais, mas que parte delas ainda funcione a partir desses atributos militares, incompatíveis com o exercício da segurança pública no Estado democrático de direito, cujo foco deve ser o atendimento ao cidadão. Torna-se necessário, portanto, promover as mudanças constitucionais e legais que assegurem a desvinculação das polícias militares estaduais das Forças Armadas e que acarretem a plena desmilitarização desses corpos policiais […].

Enquanto as mudanças jurídicas não ocorrem, esta configuração complexa das polícias permanece sociedade de controle. Na sociedade disciplinar, a polícia realiza a gestão da vida para adestrar o indivíduo ao padrão "normal" estabelecido pelos que controlam o Estado e é a agente principal da vigilância no aparelho estatal (FOUCAULT, 2015a, p. 150). Na sociedade de controle, a vigilância não é pelo panóptico dirigido por um vigia: ela não necessita do confinamento e é realizada a céu aberto por várias agências diferentes (DELEUZE, 2008b, p. 224-226). Isso é facilmente percebível pela quantidade de agências que vigiam o cidadão, como as próprias agências públicas Polícia Militar, Polícia Civil e Polícia Federal, e também a Polícia Rodoviária Federal, a Polícia Ferroviária Federal, as Polícias Penais federal, estaduais e distrital, o Ministério Público, as Guardas Municipais, as Comissões Parlamentares de Inquérito, a Agência Brasileira de Inteligência, o Conselho de Controle de Atividades Financeiras e o Banco Central do Brasil; e pelas agências privadas, de número incalculável, como o Google, a Amazon, o Facebook, a Apple e a Microsoft.

Como funciona a polícia, então, na sociedade de controle? Se ela não é apenas a vigia do panóptico (apesar de não ter abandonado completamente esta função) ou o braço operacional do poder disciplinar, qual sua função na sociedade de controle?

2.3.2 A polícia na sociedade de controle

Ericson e Haggerty (2007, p. 34-38) respondem que, além da intervenção na vida dos indivíduos, a polícia centraliza as informações produzidas por várias agências diferentes, num sistema de troca de informações em rede. É a polícia quem ocupa a centralidade da análise de risco em nome do Estado baseada na imensidão de informações fornecidas pelas agências públicas e privadas ao ser ela quem cruza essas informações e inicia a investigação – destacando-se que, apesar de receber muitas informações, a polícia não transfere as informações com a mesma facilidade (sendo diferente a transparência da propaganda institucional; a clareza na metodologia policial não é o mesmo que relatórios de número de prisões, *e.g.*).

Na análise de riscos, a cada nova tecnologia é expandido o arsenal de vigilância policial (ERICSON; HAGGERTY, 2007, p. 37). São exemplos o telefone, o microfone, a câmera, o computador, o *Global Positioning System*, o *smartphone etc.* O controle constante ultrarrápido utiliza os meios ocultos de investigação como técnicas preferidas pela sua velocidade e potencial de controlar. Por isso, sem qualquer coincidência, foi editada a Lei n. 9.296, de 1996 (interceptações telefônica, informática e telemática), e os arts. 7º (captação ambiental de sinais eletromagnéticos, ópticos ou acústicos) e 14 (agente infiltrado virtual) da Lei 13.964, de 2019.

Somado a isso, na sociedade atual super virtualizada as empresas de tecnologia colaboram com o Estado e são agentes privados relevantes na alimentação da rede de informações monitorada pela polícia.

O Facebook[50], por exemplo, (dono também do Instagram e do WhatsApp) – que, segundo o segundo o The New York Times (2020), já forneceu informações de mais de 2,2 bilhões de usuários para vários clientes (entre eles: Microsoft, Amazon, Apple, Yahoo, Sony, Rotten Tomatoes, Spotify, Huawei, Yandex, Netflix, Royal Bank of Canada e dezenas de fabricantes de tecnologia), incluindo informações de geolocalização, preferência religiosa e política dos usuários, e também possibilitou ler, escrever e deletar mensagens privadas, assim

[50] Que recentemente passou a chamar-se Meta Platforms.

como obter informações dos contatos dos usuários – admite expressamente que colabora com os Estados em sua "Política de dados" (FACEBOOK, 2020).

O Google também afirma em seus "Termos de Serviço" que colabora com Estados, principalmente com os Estados Unidos (GOOGLE, 2020).[51]

Além disso, em situações de alegada ameaça à segurança nacional, o *Federal Bureau of Investigation* (FBI) pode determinar às empresas, sem prévia autorização judicial, que forneçam informações privadas de usuários por meio da *National Security Letter* (NSL) viabilizada pela seção 505 do *USA Patriot Act* que, assinado em 26 de outubro de 2001 por George W. Bush, após os eventos de 11 de setembro, modificou a legislação dos Estados Unidos em diversos pontos e possibilitou o aumento da vigilância mundial estadunidense (previsto para ser temporário, o *USA Patriot Act* foi renovado sucessivas vezes nas administrações W. Bush, Obama e Trump).[52]

No que importa a esta pesquisa, o *USA Patriot Act* prevê ampla extraterritorialidade dos Estados Unidos por tratar não apenas daqueles que exerceram atividade no país, mas da persecução contra qualquer pessoa física ou jurídica do mundo suspeita de contrariar a lei estadunidense – entre outras condutas, pelo uso abusivo ou fraude por computador que comprometa o comércio ou a comunicação dos Estados Unidos (seção 814) (GEIST, 2003, p. 344-345) (BURKE, 2020).

A vigilância estadunidense também é operada por meio de vários órgãos públicos; como a *National Security Agency* (NSA) que, autorizada pelo *Foreign Intelligence Surveillance Act* (FISA), vigia eletronicamente pessoas de todos os lugares – inclusive nos Estados Unidos, como demonstrou Edward Snowden – para a obtenção de informações de inteligência. Sendo que as informações são estrategicamente compartilhadas com outros Estados, como Glenn Greenwald provou que ocorreu com Israel (JAEGER; BERTOT; MCCLURE, 2003) (THE GUARDIAN, 2020a; 2020b; 2020c). E, assim como cooperou com Israel, os Estados Unidos podem compartilhar essas informações com outros Estados, como o Brasil.

Portanto, voluntariamente ou não, as empresas de tecnologia colaboram com o Estado – e é condição de uso de seus serviços que os usuários concordem com essa colaboração.

[51] O Google, entre outros buscadores (como o Yahoo, o Bing e o DuckDuckGo), também acumulam a função estratégica de serem os veículos pelos quais a maior parte das pessoas encontra informações na internet (BOLZAN DE MORAIS; FESTUGATTO, 2021, p. 55).

[52] Hannah Bloch-Wehba (2016) afirma que, em função da falta de clareza nos requerimentos do FBI, da falta de regulamentação sobre os requerimentos e da falta de transparência e controle judicial, a *National Security Letter* é conflitante com a Primeira Emenda à Constituição dos Estados Unidos por possibilitar ofensas à liberdade religiosa, à liberdade de expressão e ao direito de petição.

Na sociedade de controle que tem o computador como máquina principal (DELEUZE, 2008a, p. 216), as empresas privadas de tecnologia são agentes relevantes na alimentação da rede de informações utilizadas pela vigilância estatal. O monitoramento na internet não é feito apenas pelo Google – e o que ele monitora pode ser também compartilhado com as polícias (sendo que o Google não é responsável pela maior parte dos usuários não lerem seus "Termos de Serviço", onde consta: "A NSL não precisa de autorização judicial"; "Mandados e autorizações da FISA podem ser usados para impor vigilância eletrônica e divulgação de dados armazenados, incluindo conteúdo de serviços como o Gmail, Drive e Fotos"; "podemos fornecer informações de usuários" de acordo com a legislação [GOOGLE, 2020]).

Retomando o que foi dito: como as empresas de tecnologia compartilham informações com a polícia; como os meios ocultos de investigação são realizados predominantemente no inquérito pela polícia; como eles detectam informações sensíveis (várias vezes indispensáveis) para a construção do juízo sobre o caso penal[53]; como a polícia ocupa posição central na reunião e cruzamento de informações da rede de vigilância; como a polícia é a porta de entrada da persecução e o judiciário só atua num segundo momento (na legitimação ou contenção dos atos policiais [ZAFFARONI, 2012, p. 433]); e como as testemunhas das audiências são frequentemente os próprios policiais; o aumento do espaço da polícia na persecução penal é a segunda característica da persecução que utiliza os meios ocultos de investigação.

Com influência relevantíssima no resultado do procedimento[54], centralidade na análise do risco, pouco controle efetivo da realização de seus atos (CHOUKR; BACILA, 2003, p. 147) e cada vez mais especialização no uso de novas tecnologias, a polícia – de complexa configuração institucional – é protagonista no processo penal da sociedade de controle.

2.4 Tendência para a privatização da recolha estatal de informação

A tendência para a privatização da recolha estatal de informação é uma das principais características da persecução que utiliza meios ocultos de investigação, principalmente pela autoincriminação em elementos digitais registrados pelos próprios indivíduos. A dinâmica relacionada a essa característica – que difere radicalmente da persecução penal regida pelo direito ao silêncio – é o objeto deste item.

[53] Vide a nota n. 27, *supra.*
[54] Eliomar da Silva Pereira (2019, p. 13-15) destaca a importância do respeito aos institutos processuais no inquérito em função da relevância do acervo investigativo nas decisões jurídicas.

A autoincriminação na sociedade de controle tem aspectos distintos da confissão na inquisição,[55] como mostra Byung-Chul Han. A confissão não necessita mais da tortura em grande parte dos casos;[56] indivíduos se confessam voluntariamente por *smartphones* em redes sociais como o Facebook, o Instagram e o WhatsApp. Na "ditadura da transparência", cada um vira um vigia de si e fornece espontaneamente quantidades imensas de informações para a rede de vigilância:

> O *curtir* é o amém digital. Quando clicamos nele, subordinamo-nos ao contexto de dominação. O *smartphone* não é apenas um aparelho de monitoramento eficaz, mas também um confessionário móvel. O Facebook é a igreja ou a sinagoga (que literalmente significa «assembleia») do digital. (HAN, 2018, p. 18-24, 57).

Esta rede de vigilância é monitorada pela polícia, que reúne informações vindas tanto das agências públicas como das privadas (tema tratado no item anterior).

A autoincriminação ocorre também na fala em telefone e no e-mail interceptados, nas revelações ao agente infiltrado, assim como nos demais meios ocultos de investigação em que o sujeito produz o registro da informação sem esperar que ela vai ser utilizada para lhe incriminar. Portanto, conscientemente ou não, o indivíduo colabora com a criação de registros que podem relacioná-lo à autoria de um delito.

A participação de indivíduos e empresas privadas na recolha de informações para a rede de vigilância estatal é o terceiro elemento caracterizador dos meios ocultos de investigação (COSTA ANDRADE, 2011, p. 534-537).

A autoincriminação de indivíduos foi abordada acima, falta tratar da participação das empresas na alimentação da rede de vigilância estatal.

[55] A confissão foi técnica central na autoincriminação da inquisição do século XIII. O protagonista da instituição disso no direito canônico foi Lotario dei Segni (futuro papa Inocêncio III). Quando cardeal, ele escreveu que ao nascer o homem é consumido em sua própria maldade. Segundo o principal autor do saber inquisitório, ninguém deve escapar da punição porque não existe alguém imune à culpa (DEI SEGNI, 1978, p. 141-143, 207). O pecado original de Adão seria transmitido de geração em geração, fazendo com que todos os humanos já nascessem culpados e tivessem que buscar a salvação (BOFF, 1993, p. 9-10). Na inquisitoriedade, conforme o papa regente do IV Concílio de Latrão, se o humano tentar se justificar quanto à sua culpa, a sua boca deve condená-lo; cada fala sua deve prestar contas e ele pagar até o último centavo. Sendo que, podendo o juiz (que também é acusador e advogado) revelar tudo o que estava oculto, nem testemunhas são necessárias para o julgamento. Buscando o desocultamento total, Inocêncio III alegrava-se com a vergonha que os pecadores sentiam quando expostos para todos (DEI SEGNI, 1978, p. 229-233). A principal técnica de desocultamento do saber inquisitório é a confissão. Pela confissão, o indivíduo revelaria a si mesmo para um outro, enviado de Deus, que, detentor de conhecimento privilegiado (acesso às premissas divinas), o conduziria à salvação (FOUCAULT, 2011, p. 134-140; 2018, p. 8, 160-164). Como observou Cordero (1986, p. 47-48), o procedimento inquisitório desvela a verdade até então escondida no interior do réu, inclusive valendo-se da tortura: *reus tenetur se detegere* para atender à veridição inquisitória. Sobre a legislação inquisitória no Brasil, vide: Santiago Neto (2019, p. 267-399).

[56] Em outros ainda se prende para obter delação premiada; o que, além de ser ilícito, é uma secularização da tortura inquisitória para se obter a confissão.

Desde 1970, com a "guerra às drogas" (liderada pelos Estados Unidos) e o combate às organizações criminosas transnacionais que utilizam complexos sistemas para encobrimento de suas ações – como na circulação de dinheiro pelo sistema financeiro e no financiamento da corrupção –, vem aumentando a pressão internacional para a maior vigilância do funcionamento de empresas cujas atividades têm grande potencial criminoso, principalmente as que podem facilitar a ocorrência de lavagem de dinheiro. São exemplos desse aumento de pressão internacional a Convenção de Palermo (combate às organizações criminosas), a Convenção de Mérida (combate à corrupção) e as recomendações do Grupo de Ação Financeira Internacional (GAFI) (BLANCO CORDERO, 2015, p. 65-68; 206-207) (BADARÓ; BOTTINI, 2012, p. 28-32).

Conforme a recomendação n. 29 do GAFI:

> Os países deveriam estabelecer uma unidade de inteligência financeira (UIF) que sirva como um centro nacional de recebimento e análise de: (a) comunicações de operações suspeitas; e (b) outras informações relevantes sobre lavagem de dinheiro, crimes antecedentes e financiamento do terrorismo, e de disseminação dos resultados dessa análise. A UIF deveria ser capaz de obter informações adicionais das entidades comunicantes e ter acesso rápido a informações financeiras, administrativas e de investigação que necessite para desempenhar suas funções adequadamente. (FINANCIAL ACTION TASK FORCE, 2020, tradução nossa[57]).

A Convenção de Palermo (art. 7) e a Convenção de Mérida (arts. 12 e 14) determinam que os Estados adotem medidas legislativas que assegurem a prevenção à lavagem de dinheiro e à corrupção por meio de programas de integridade e da colaboração das empresas privadas.

O Brasil atendeu às recomendações internacionais e editou a Lei de Lavagem (n. 9.613, de 1998) e a Lei Anticorrupção (n. 12.846, de 2013, regulamentada pelo Decreto n. 8.420, de 2015). Pela primeira, foi estabelecido o Conselho de Controle de Atividades Financeiras (COAF) como unidade de inteligência financeira (UIF) estatal que disciplina, aplica sanções administrativas, recebe, examina e identifica ocorrências suspeitas de lavagem de dinheiro; e as empresas e pessoas físicas de atividades que podem facilitar a ocorrência de lavagem de dinheiro (como bolsas de valores, seguradoras, administradoras de cartões de crédito, empresas de fomento comercial, agentes imobiliários, joalheiros, juntas comerciais, registros públicos, empresas de transporte e guarda de valores *etc.*) foram obrigadas a identificar seus clientes, manter registro das transações financeiras, adotar controles internos

[57] Countries should establish a financial intelligence unit (FIU) that serves as a national centre for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and terrorist financing, and for the dissemination of the results of that analysis. The FIU should be able to obtain additional information from reporting entities, and should have access on a timely basis to the financial, administrative and law enforcement information that itrequires to undertake its functions properly.

para cumprir a lei, cadastrarem-se no órgão regulador competente, comunicar todas as atividades suspeitas de lavagem para o COAF e atender às suas requisições. Pela Lei Anticorrupção, atos contrários à administração pública – que já tinham previsão legal de responsabilização criminal das pessoas físicas (Código Penal, arts. 317 e 333; Lei 8.666, de 1993) – passaram a ter extenso rol de punições civis e administrativas para empresas[58] (até a dissolução compulsória da pessoa jurídica, art. 19, III). Esta lei determinou (art. 7º, VIII) que, na aplicação de sanção, deve ser observada a existência de programa de integridade e (art. 16) condicionou a celebração de acordo de leniência pela empresa: à confissão da infração; à identificação de demais envolvidos; à produção de elementos de informação sobre a infração; à empresa ser a primeira a manifestar interesse em cooperar; ao encerramento das atividades infracionais; à colaboração com a investigação; e à reparação do dano causado. O decreto regulamentador n. 8.420, de 2015, acrescentou que, entre outras, o acordo de leniência deve conter cláusula sobre à implantação de programa de integridade pela empresa (art. 37, IV)[59] – o que foi mantido pelo decreto n. 11.129, de 2022 (art. 45, IV).

As razões oficiais das mudanças legislativas são o combate ao crime organizado, principalmente pelo combate à lavagem de dinheiro e à corrupção, e mudança da ética empresarial; o que, inegavelmente, foi obtido em alguma medida.[60] Todavia, e atendendo à

[58] Sobre as empresas públicas, vide, também, a Lei n. 13.303, de 2016.

[59] De acordo com o decreto n. 8.420, de 2015, o programa de integridade deve ser orientado pelos seguintes parâmetros: "Art. 42. Para fins do disposto no § 4º do art. 5º, o programa de integridade será avaliado, quanto a sua existência e aplicação, de acordo com os seguintes parâmetros: I – comprometimento da alta direção da pessoa jurídica, incluídos os conselhos, evidenciado pelo apoio visível e inequívoco ao programa; II – padrões de conduta, código de ética, políticas e procedimentos de integridade, aplicáveis a todos os empregados e administradores, independentemente de cargo ou função exercidos; III – padrões de conduta, código de ética e políticas de integridade estendidas, quando necessário, a terceiros, tais como, fornecedores, prestadores de serviço, agentes intermediários e associados; IV – treinamentos periódicos sobre o programa de integridade; V – análise periódica de riscos para realizar adaptações necessárias ao programa de integridade; VI – registros contábeis que reflitam de forma completa e precisa as transações da pessoa jurídica; VII – controles internos que assegurem a pronta elaboração e confiabilidade de relatórios e demonstrações financeiros da pessoa jurídica; VIII – procedimentos específicos para prevenir fraudes e ilícitos no âmbito de processos licitatórios, na execução de contratos administrativos ou em qualquer interação com o setor público, ainda que intermediada por terceiros, tal como pagamento de tributos, sujeição a fiscalizações, ou obtenção de autorizações, licenças, permissões e certidões; IX – independência, estrutura e autoridade da instância interna responsável pela aplicação do programa de integridade e fiscalização de seu cumprimento; X – canais de denúncia de irregularidades, abertos e amplamente divulgados a funcionários e terceiros, e de mecanismos destinados à proteção de denunciantes de boa-fé; XI – medidas disciplinares em caso de violação do programa de integridade; XII – procedimentos que assegurem a pronta interrupção de irregularidades ou infrações detectadas e a tempestiva remediação dos danos gerados; XIII – diligências apropriadas para contratação e, conforme o caso, supervisão, de terceiros, tais como, fornecedores, prestadores de serviço, agentes intermediários e associados; XIV – verificação, durante os processos de fusões, aquisições e reestruturações societárias, do cometimento de irregularidades ou ilícitos ou da existência de vulnerabilidades nas pessoas jurídicas envolvidas; XV – monitoramento contínuo do programa de integridade visando seu aperfeiçoamento na prevenção, detecção e combate à ocorrência dos atos lesivos previstos no art. 5º da Lei nº 12.846, de 2013; e XVI – transparência da pessoa jurídica quanto a doações para candidatos e partidos políticos." (BRASIL, 2020d). Posteriormente, o Decreto n. 8.420, de 2015, foi revogado pelo decreto n. 11.129, de 2022, que estabeleceu disposições semelhantes no artigo 57.

[60] Sendo bastante questionável a ética que se baseia a delação (MIRANDA COUTINHO; CARVALHO, 2006).

metodologia historiográfica desta pesquisa, que se foca muito mais nos efeitos concretos que nas razões oficiais (FOUCAULT, 2015b, p. 262-272), mudanças nas práticas empresariais não foram os únicos efeitos obtidos. Na sociedade de controle em que tanto agentes públicos como privados alimentam a rede de vigilância monitorada pela polícia, as Leis de Lavagem e Anticorrupção (com as autoincriminações empresariais, identificação dos clientes, denúncias dos clientes, auditorias internas, análises de riscos, canais de denúncia, disciplina interna, monitoramento contínuo, *know your client*, *know your partner*, *know your employee*, transparência e registro de tudo) promoveram um aumento inédito na privatização da recolha estatal de informação.

As empresas alimentam a rede de informações – pelo COAF, por outros órgãos reguladores, pela Controladoria-Geral da União (CGU), pela polícia, pelo Ministério Público *etc.* – tanto em comunicações rotineiras como em anexos de acordos de leniência e de delações premiadas contendo relatórios de auditoria, gravações, documentos internos, e-mails dos funcionários e registros diversos. Estruturas criadas pelas próprias empresas resultam no aumento do controle, na autoincriminação e na delação de terceiros em níveis exponenciais. Toda esta operação configura participação das empresas privadas na vigilância da sociedade de controle.

Portanto, seja nos registros criados pelos próprios investigados, seja na autoincriminação do indivíduo que realiza uma ligação ou envia um e-mail sem saber que está sendo interceptado; seja na revelação ao agente infiltrado; seja na leniência com a CGU ou nas delações ao Ministério Público e à polícia; e seja, também, na colaboração das empresas com o Estado – inclusive as de tecnologia (como demonstrado no item anterior) –, a tendência para a colaboração privada na recolha estatal de informação está presente na realização dos meios ocultos de investigação.

2.5 Progressivo aumento do uso de novas tecnologias

Cada nova tecnologia é, na sociedade de controle, uma nova técnica potencial de otimização dos resultados (DELEUZE, 2008b, p. 221-226). O progressivo aumento do uso de novas tecnologias pela investigação – com impactos em toda a persecução penal – é característica indispensável para a compreensão da atividade investigativa que visa a prevenção de danos pelo máximo de controle ultrarrápido sobre grupos de suspeitos.

A virada tecnológica no Direito tem causado mudanças imensas no sistema jurídico, não apenas como uma mudança de meio (do físico para o virtual), mas como transformação do Direito pela tecnologia (NUNES, 2021, p. 19, 30) – isso inclui a persecução penal.

Na expansão do controle, cada nova invenção tecnológica é uma nova oportunidade de vigilância (ERICSON; HAGGERTY, 2007, p. 37). O rol de suas modalidades não é fechado, mas mutável e aumentado com o surgimento de novas tecnologias eficientes em controlar.

Telefone, câmera, microfone, *Global Positioning System,* computador, *smartphone* e internet já são utilizados amparados na Lei n. 9.296, de 1996 (interceptações telefônica, informática e telemática; captação ambiental de sinais eletromagnéticos, ópticos ou acústicos) e na Lei n. 12.850, de 2013 (agente infiltrado virtual) – principalmente após a Lei 13.964, de 2019 –; e a inteligência artificial já é utilizada, *e.g.*, pelo Laboratório de Tecnologia contra Lavagem de Dinheiro do Ministério da Justiça e Segurança Pública (STOPANOVSKI, 2020).

Como destacam Ericson e Haggerty (1999, p. 237-244), o computador, especialmente, influenciou várias outras tecnologias de vigilância da população, como imagens de satélite, sensores, controle remoto de veículos (como o *drone*), reconhecimento facial e a inteligência artificial.

É a persecução penal que viabiliza o uso lícito de novas tecnologias para a vigilância estatal. E frente ao volume e importância das informações obtidas pelos novos meios ocultos, as investigações são bastante estimuladas a usá-los. Principalmente por isso, cada vez mais são utilizadas novas tecnologias na persecução penal.

Não adianta negar a existência do fenômeno, cabe compreendê-lo. No que se refere a este trabalho, o capítulo 3 será integralmente dedicado à tecnologia envolvida na busca e na apreensão de elementos de prova digitais.

2.6 Limiar

Apesar da crença do legislador de que a instrução ocorre principalmente na audiência,[61] a prática demonstra que a audiência é frequentemente a rediscussão do inquérito[62], que atrai o foco dos sujeitos processuais, pois: em primeiro lugar, a polícia é a porta de entrada da persecução e a função judicial atua apenas num segundo momento, na legitimação ou contenção dos atos policiais (ZAFFARONI, 2012, p. 433); em segundo lugar, grande parte das testemunhas ouvidas em audiências são os próprios policiais; e, em terceiro

[61] A Lei n. 11.719, de 2008, que pretendeu a centralidade da cognição na audiência de instrução e julgamento, é exemplo disso (BARROS, 2008b, p. 127-131). Vide: Barros e Pimenta (2020).
[62] Vide a nota n. 31, *supra.*

lugar, muitas informações sensíveis e importantes sobre o caso penal[63] são obtidas por escutas telefônicas e outras cautelares realizadas principalmente no inquérito.

Permanece – e é acentuada – a "fraude neoinquisitória" nas persecuções que utilizam meios ocultos de investigação.

> A fraude reside no fato de que a prova é colhida na inquisição do inquérito, sendo trazida integralmente para dentro do processo e, ao final, basta o belo discurso do julgador para imunizar a decisão. Esse discurso vem mascarado com as mais variadas fórmulas, do estilo: a prova do inquérito é corroborada pela prova judicializada; cotejando a prova policial com a judicializada; e assim todo um exercício imunizatório (ou, melhor, uma fraude de etiquetas) para justificar uma condenação, que, na verdade, está calcada nos elementos colhidos no segredo da inquisição. O processo acaba por converter-se em uma mera repetição ou encenação da primeira fase. (LOPES JR., 2015, p. 154).

Na persecução que utiliza meios ocultos, com maior intensidade, ao investigado ou acusado é negada a participação consciente nos atos que atraem o foco do juízo. Os elementos relevantes para a cognição sobre o caso penal são obtidos pela polícia no inquérito e a audiência é convertida na rediscussão dos atos policiais. A neoinquisitoriedade – que constrói a culpa na fase preliminar, privilegia o segredo e a escritura, desvaloriza a audiência e menospreza o acusado (MARINHO MARQUES, 2014, p. 26) – é agravada na persecução que utiliza os novos meios ocultos, executados principalmente na fase investigativa e sem o conhecimento do investigado.

Sem crítica ou prévio contraditório, a realização dos meios ocultos de investigação aumenta a importância dos atos realizados fora do processo de conhecimento e a resposta rápida cautelar ganha protagonismo (BARROS, 2018, p. 21-23).

Em nome do combate à criminalidade organizada, as novas leis ampliam as possibilidades de vigilância e reduzem os direitos de defesa (COSTA ANDRADE, 2011, p. 533). Ao invés da cognição construída em audiência, com direito ao silêncio e assistência por advogado, ela é formada principalmente pelos meios ocultos de investigação e cautelares realizadas no inquérito, sem a participação prévia e consciente do investigado e visando a sua autoincriminação. Antes da instrução processual na audiência já há uma "verdade" construída pelos meios ocultos de investigação registrados por escrito no inquérito.[64]

Apesar da propaganda ser de que o uso de novas tecnologias de investigação só ocorrerá em casos graves envolvendo organizações criminosas, a prática tem mostrado a sua

[63] Vide a nota n. 27, *supra.*

[64] Afinal: "A informação penal escrita, secreta, submetida, para construir suas provas, a regras rigorosas, é uma máquina que pode produzir a verdade na ausência do acusado." (FOUCAULT, 2008b, p. 34).

vulgarização[65] e uso exponencialmente mais frequente. O fenômeno não é apenas brasileiro, Lawrence Lessig (2006, p. 207-208) dá o exemplo da tecnologia de coleta e análise de *Deoxyribonucleic acid* (DNA): em 1995, a Inglaterra criou um banco de amostras de DNA para combater o terrorismo; em 2005, o banco de amostras de DNA passou a ser utilizado para identificar quem cuspir em transporte público, como no metrô. No Brasil, a *overcharging* – imputação propositadamente desproporcional ou sem elementos concretos (GRAHAM, 2020, p. 13-16)[66] – é empregada frequentemente para aparentar falsamente que um caso penal tem gravidade ou trata de tipo específico exigido pela lei para a autorização da realização do meio oculto de investigação (por exemplo, a investigação de uso de drogas que afirma que é de tráfico para realizar interceptação telefônica).[67]

Com isso, há o uso de meios ocultos de investigação extremamente invasivos em casos que não envolvem a criminalidade organizada[68], mas a criminalidade de massa (como furtos, roubos e uso de drogas – que não são cometidos por grandes, hierarquizadas e sofisticadas associações criminosas), numa vulgarização desses meios[69] que excluem a participação ativa do acusado.

[65] "O recurso, quer no plano legiferante quer no plano operacionalizante da norma legitimadora, imbuído do espírito securitário *ab initio*, a meios de obtenção de prova ou instrumentos de combate (repressão) ao crime de natureza excepcional induz à vulgarização dos meios que só excepcionalmente deviam ser utilizados, quando os menos onerosos e agressivos para o cidadão – arguido ou não – se mostrassem inidóneos e inadequados e incapazes de obter a prova ou a descoberta da verdade." (VALENTE, 2008, p. 181).

[66] O problema da imputação abusiva é antigo e foi atacado por Heleno Fragoso (2022, p. 11): "O M.P. não é uma espécie de inquisidor-mor que possa a seu bel-prazer, denunciar quem bem entenda ou quem apraz ao executivo (em cujo nome atua) perseguir. Não se cogita aqui de *ilegalidade*: a denúncia pode ser formalmente incensurável. Cogita-se, isso sim, de *abuso de poder*, ou seja, de desvio dos deveres do próprio ofício, na prática arbitrária de um ato legal. Há abuso de poder quando o funcionário se serve ilegitimamente de faculdades ou de meios de que legalmente pode dispor. O abuso de poder é, em suma, o mau uso de poder na denunciação, quando o M.P., inteiramente fora da realidade e sem qualquer elemento de convicção, inicia o procedimento criminal."

[67] A Lei 9.296, de 1996, só permite a interceptação telefônica em crimes punidos com reclusão (artigo 2º, III); o que não é o caso do crime do uso de drogas do artigo 28 da Lei 11.343, de 2006, mas é o do crime de tráfico dos artigos 33, *caput* e § 1º, e 34. Vide, *e.g.*, o julgamento do *Habeas Corpus* 186.118/RS, de relatoria do ministro Sebastião Reis Júnior, pelo Superior Tribunal de Justiça.

[68] O conceito de criminalidade organizada, apesar de ser tipificada no artigo 2º, da Lei 12.850, de 2013, não é unânime na literatura jurídica. Hassemer (1993b, p. 67) defende que a "'Criminalidade organizada' - é um fenômeno cambiante; ela segue mais ou menos as tendências dos mercados nacionais e internacionais e torna-se portanto difícil de ser isolada (exemplo, o tráfico clandestino de lixo nos países industrializados); - compreende uma gama de infrações penais sem vítimas imediatas ou com vítimas difusas (ex. tráfico de drogas, corrupção) e portanto não é levada ao conhecimento da autoridade pelo particular; - intimida as vítimas, quando elas existem, a não levarem o fato ao conhecimento da autoridade e a não fazerem declarações (ex. extorsão de 'pedágios' ou 'seguros' por organizações criminosas); - possui tradicionais solos férteis em bases nacionais e, em outras latitudes, não viceja ou produz resultados diversos (ex. Máfia em outros países que não o seu berço); - dispõe de múltiplos meios de disfarce e simulação.". Para Figueiredo Dias (2008, p. 26-27): "o conceito jurídico-penal de *criminalidade organizada* deve supor, por um lado, a prática do crime de associação criminosa e, por outro, a prática – no estádio da consumação, da tentativa ou mesmo da preparação – de particular natureza e gravidade (os chamados *crimes do catálogo*)."

[69] Vide a nota n. 65, *supra*, e o item 4.7, *infra.*

Não há como negar a existência do fenômeno, cabe buscar mitigar seus efeitos para que mesmo neste novo cenário seja assegurada a participação ativa do acusado na construção do juízo.

Este capítulo 2 teve como objeto explicitar as características da transformação da persecução penal pelos meios ocultos. Endossando a proposta de Costa Andrade (2011, p. 534-536), o capítulo tratou da diminuição da fronteira entre a repressão e a prevenção de delitos, do aumento do espaço da polícia, da tendência para a privatização da recolha estatal da informação e do progressivo aumento do uso de novas tecnologias na persecução penal. Com a explicitação dessas características, o problema de como assegurar a participação do acusado na persecução penal que utiliza o meio oculto da busca de elementos de prova digitais e a apreensão desses elementos pode ser melhor entendido e enfrentado.

É daí que emerge a "tese" desta tese: de que determinadas técnicas relacionadas às mudanças causadas pelos novos meios ocultos de investigação na persecução devem ser executadas para assegurar a participação ativa do acusado na persecução que utiliza a busca e a apreensão de elementos de prova digitais: em relação à diminuição da fronteira entre repressão e prevenção de delitos, a cadeia de custódia de elementos digitais, por possibilitar perceber se a investigação foi prospectiva ou baseada em elementos concretos preexistentes; em relação ao aumento do espaço da polícia e da importância da fase investigativa, o direito de confrontar os agentes públicos e privados envolvidos em audiência; em relação à tendência para a privatização da recolha estatal de informação, a proteção contra a autoincriminação por medidas antiforenses e pela atuação judicial na proteção preventiva das garantias processuais; e em relação ao progressivo aumento do uso de novas tecnologias na persecução penal, a paridade entre as partes no espaço virtual pela ampliação do uso dessas tecnologias pelo acusado.

Doravante, a pesquisa aprofundará no estudo da tecnologia envolvida (capítulo 3); da conceituação e procedimentos legais relacionados (capítulo 4) e dessa tese (capítulo 5).

3 TECNOLOGIA UTILIZADA NA BUSCA E NA APREENSÃO DE ELEMENTOS DIGITAIS

Como indicado na introdução, esta pesquisa é transdisciplinar (MIAILLE, 2005, p. 60-62). Neste trabalho que trata da busca e da apreensão de elementos digitais – criados, acessados, alterados e extinguidos pelo uso de computador –, é fundamental explicitar noções sobre o funcionamento do computador e das demais tecnologias envolvidas.

Sem o conhecimento básico sobre o que é um computador e como ele funciona é impossível aferir se a Lei[70] foi observada na realização da busca e apreensão de elementos digitais – por exemplo: como saber se a integridade de um arquivo de computador foi preservada numa apreensão, respeitando-se a cadeia de custódia, sem se conhecer o que é um arquivo de computador?

Portanto, cumpre expor noções sobre a tecnologia envolvida na busca e na apreensão de elementos digitais; apenas após será possível compreender tanto a relevância do código informático na realização desses meios quanto como fazer com que a Constituição jurídica democrática tenha primazia sobre a constituição da arquitetura virtual.

3.1 O que é um computador e como ele funciona?

Em 1900, no Congresso Internacional de Matemáticos de Paris, David Hilbert desafiou a todos a resolver o seguinte problema matemático: criar um algoritmo geral que respondesse se qualquer equação tem solução (ou seja, "uma resposta para a pergunta se tal procedimento pode ou não existir em princípio" [PENROSE, 1993, p. 35]) (HILBERT, 1902, p. 458).

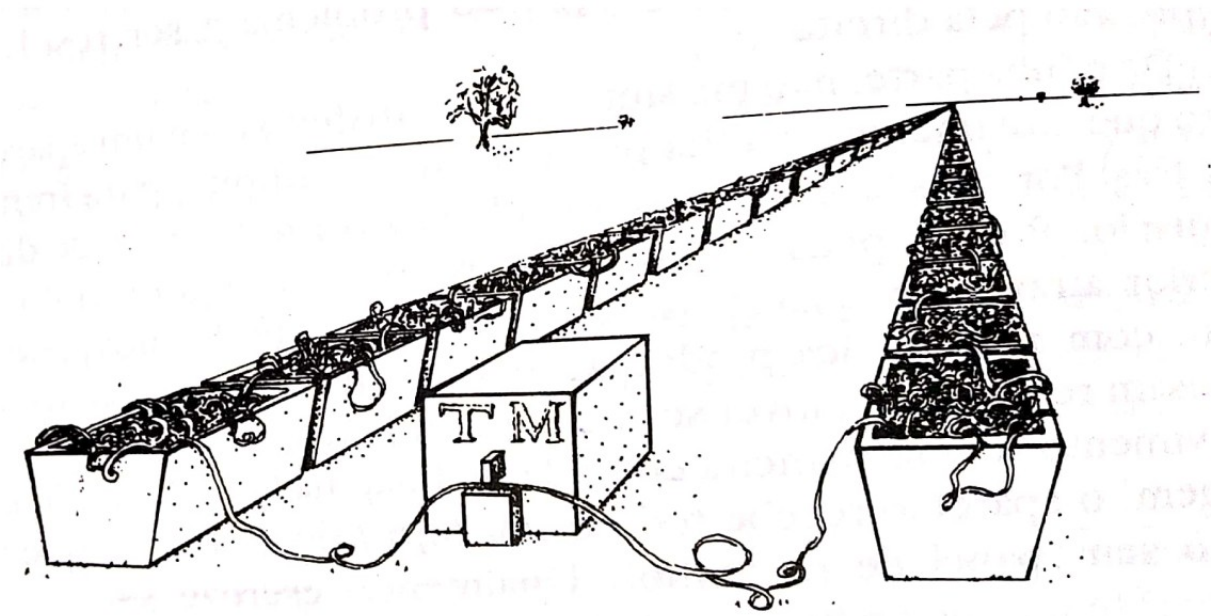
Um algoritmo é um procedimento composto por uma sequência finita de operações matemáticas. O nome advém do sobrenome de um matemático persa que viveu no século IX, Abu Ja'far Mohammed ibn Mûsâ *al-Khowârizm*. Penrose (1993, p. 32) afirma que anteriormente a al-Khowârizm já existiam algoritmos (os gregos antigos já o utilizavam), mas foi com o trabalho do matemático persa que o vocábulo "algoritmo" foi associado com o procedimento sistemático finito de operações matemáticas.

Na ambição de resolver o problema de Hilbert e criar um algoritmo geral de cálculo, o matemático inglês Alan Turing criou uma máquina de cálculo que ficou conhecida como "máquina de Turing universal". Essa máquina tem como finalidade receber informações de

[70] Lei, com maiúscula, refere-se à totalidade do sistema jurídico.

entrada (*input*), calcular essas informações e fornecer informações de saída (*output*). A figura seguinte ilustra a proposta do matemático:

Figura 2 – Uma máquina de Turing rigorosa exige uma fita infinita!



Fonte: Penrose (1993, p. 37)

A máquina é composta por três partes: um estoque (uma "fita", que também contém o "livro de regras" de funcionamento), uma unidade de execução (que realiza operações individuais) e um controle (que acessa o "livro de regras" e faz elas serem cumpridas) (TURING, 1950, p. 437) – no computador atual, o estoque é o *hard drive*, a unidade de execução é a memória de leitura e escrita (*Random Access Memory*, a memória RAM) e o controle é o processador.

Turing (1937; 1950, p. 441-442) propôs que a máquina funcionasse utilizando uma "fita" potencialmente infinita com determinadas marcações. A máquina pode movimentar a "fita" para frente e para trás, lê-la e marcá-la. Essa "fita" é uma sequência linear de quadrados marcados ou não. Apesar da "fita" ser potencialmente infinita, o número de marcações é finito. A marcação em um quadrado na "fita" é indicada pelo símbolo "1", o quadrado em branco é indicado pelo símbolo "0". A sequência de "1s" e "0s" expressa um código binário de instruções; por exemplo: 110 para mover a "fita" para a direita, 1110 para mover a "fita" para a esquerda e 11110 para parar a "fita". Pela possibilidade de a máquina aceitar diversos códigos de instruções (e não ser necessário construir uma máquina para cada código) ela é uma máquina universal (PENROSE, 1993, p. 36-62).

Assim, utilizando números binários indicados por "1s" e "0s" a máquina de Turing universal foi pensada para conseguir fazer com que o código de instruções (por exemplo, um algoritmo) seja operado sobre qualquer *input*, resolvendo o problema de Hilbert. Contudo, como confessou o próprio Turing (1937, p. 259), o problema de Hilbert não tem solução.

Existem conjuntos de números que não são computáveis[71] (que não podem ser calculados por operações finitas):

> Podemos ter […] uma classe de problemas para os quais a solução, em cada caso, é "sim" ou "não", mas para os quais não há nenhum algoritmo geral para se decidir qual é realmente a resposta. Algumas dessas classes de problema são de uma aparência notavelmente simples. Vejamos [...] o problema de encontrar soluções inteiras de sistemas de equações algébricas com coeficientes inteiros. Tais equações são conhecidas como *diofantinas* (assim chamadas em homenagem ao matemático grego Diofanto, que viveu no século III a.C. e que estudou equações desse tipo). Um conjunto dessas equações poderia ser $z^3-y-1=0$, $yz^2-2x-2=0$, $y^2-2xz+z+1=0$ e o problema é decidir se podem ou não ser resolvidas por valores inteiros de x, y e z. De fato, neste caso específico, podem, sendo a solução dada por x=13, y=7, z=2. Não há, porém, algoritmo que decida essa questão para um conjunto arbitrário de equações diofantinas: a aritmética diofantina, apesar da natureza elementar de seus ingredientes, é parte da matemática não-algorítmica! (PENROSE, 1993, p. 142-143).

Existindo conjuntos de números reais que não são computáveis surge o seguinte problema: para a máquina de Turing fornecer uma resposta (*output*) às informações de entrada (*input*), utilizando um código prévio (algoritmo) e uma "fita" para o cálculo, como ela poderia gravar na "fita" uma solução final que não pode ser prevista por uma sequência de operações finitas? Sem existir um algoritmo finito para calcular esses números, como programar a máquina? E, como a máquina decidiria quando parar (e oferecer uma resposta) se ela não tem como calcular a solução final? A resposta para estas questões é: não tem como. Por isso, segundo o próprio Turing (1937, p. 230-231, 254-259), não é matematicamente possível à máquina que leva o seu nome responder a qualquer equação imaginável; o problema de Hilbert não tem solução. A matemática composta por números reais – e por subconjuntos de números computáveis e não computáveis – que busca expressar a realidade física não pode ser calculada completamente na máquina de Turing universal (PENROSE, 1993, p. 54, 64).

Somado a isso, Gödel já havia demonstrado que um sistema matemático não possibilita a prova ou refutação da totalidade da sua composição. A explicação aritmética disso foge ao escopo desta pesquisa.[72] O ponto é que a visão de completude da demonstração

[71] "Acontece, porém, que alguns irracionais não podem (notavelmente) ser produzidos por nenhuma máquina de Turing […] Os números que podem ser gerados dessa maneira são os *computáveis*. Os que não podem (na realidade, a grande maioria!), *não-computáveis*." (PENROSE, 1993, p. 54).

[72] Penrose demonstra a argumentação do teorema da incompletude de Gödel com um exemplo: num determinado sistema, é formulado o axioma (enunciado básico do sistema aceito por convenção [ABBAGNANO, 2007, p. 101-102]) "não há prova de X" (em que X é uma proposição específica); se existisse a "prova de X" então o axioma seria falso, mas a matemática não admite axiomas falsos; assim, "não há prova de X" é uma proposição

matemática é incorreta (os axiomas mais básicos do sistema são aceitos por convenção, não por demonstração); e não existe computador que não seja um calculador matemático, logo, que não parta de axiomas indemonstráveis e arbitrários.

A matemática tem, também, outras limitações, por ser uma linguagem. A matemática que utiliza números reais busca uma relação entre o discurso matemático e a correspondência com a realidade física (o que não ocorre com os números imaginários e complexos). A linguagem relaciona conceitos e imagens das coisas[73]. A conversão dum estímulo nervoso provocado por uma coisa em imagem e dessa imagem num som obviamente não é a coisa em si, é uma metáfora[74] das coisas. A matemática é uma linguagem artificial que facilita o domínio do homem sobre a natureza; e sua contribuição para o conhecimento da natureza somente é relevante se expressar relações que têm correspondência com a realidade física. Contudo, como demonstra Nietzsche (2008, p. 29-42), um conceito é utilizado não apenas sobre a coisa única, individual, mas em múltiplos casos; exemplo: o conceito de "folha de árvore" não é utilizado para expressar a imagem de somente uma folha individual, ele é utilizado para expressar as imagens de várias folhas que são diferentes em tamanho, forma, cor *etc.* – nenhuma "folha de árvore", portanto, corresponde exatamente a alguma folha de árvore primeira. Na fala do filólogo alemão: "Todo conceito surge pela igualação do não-igual" e

> […] entre duas esferas absolutamente diferentes tais como entre sujeito e objeto não vigora nenhuma causalidade, nenhuma exatidão, nenhuma expressão, mas, acima de tudo, uma relação *estética*, digo, uma transposição sugestiva, uma tradução balbuciante para uma língua totalmente estranha. (NIETZSCHE, 2008, p. 35, 41).

Assim, além dos conceitos no máximo conseguirem aproximar imagens diferentes e não corresponderem exatamente às coisas, a linguagem exige o humano para lhe conferir significado, sendo por isso que Penrose (1993, p. 463) afirma que:

> A verdade matemática *não* é alguma coisa que comprovamos simplesmente pelo uso de um algoritmo. Creio também que a consciência é um elemento crucial em nossa compreensão da verdade de um raciocínio matemático para nos convencer de sua

"verdadeira" e que não tem como ser comprovada no sistema (por não existir "prova de X"). Portanto, a proposição básica do sistema é indemonstrável e arbitrária – "Não importa o quanto acreditamos ter sido abrangente, haverá sempre proposições que escapam da rede" (PENROSE, 1993, p. 117-119). Para a explicação aritmética, vide: Gödel (1992).

[73] A explicação, aqui, é feita em Nietzsche. Posteriormente a esse autor, o estudo da relação sígnica entre os conceitos (significados) e as imagens acústicas (significantes) foi desenvolvido por diversos autores, especialmente após as obras de Saussure (2012) e Peirce (2015). Sobre o tema, vide: Blikstein (1990) e Yaguello (1991).

[74] No sentido de imagem substitutiva: "A metáfora é para o autêntico poeta não uma figura de retórica, porém uma imagem substitutiva, que paira à sua frente em lugar realmente de um conceito." (NIETZSCHE, 1992, p. 59).

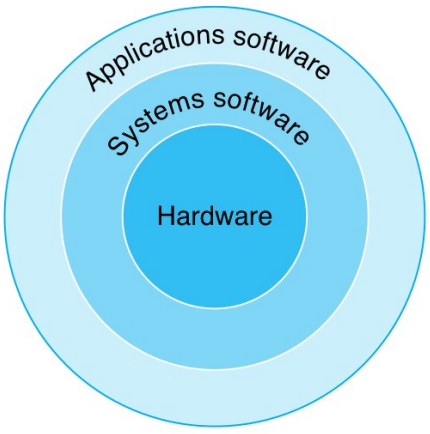
> validade. Esse "ver" é a própria essência da consciência. Deve estar presente sempre que percebemos diretamente a verdade matemática. Quando nos convencemos da validade do teorema de Gödel, não apenas o "vemos", mas ao fazê-lo revelamos a própria natureza não-algorítmica desse "ver" o próprio processo.

Isso quer dizer que a máquina de Turing universal é inútil? Claro que não. Apenas se destaca que ela apresenta limitações matemáticas e linguísticas, não sendo capaz de resolver todos os problemas matemáticos (consequentemente, também os físicos que a matemática busca expressar) e necessitando do humano para lhe conferir significado. E, sendo o computador uma máquina de Turing universal (PENROSE, 1993, p. 61, 448), a ele cabem os mesmos problemas.

3.1.1 O computador atual

Até o trabalho de von Neumann [1945]/(1993) a máquina de Turing universal era mais próxima da abstração matemática do que do computador utilizado hoje. Foi o húngaro John von Neumann quem criou a engenharia que transformou as operações algorítmicas com números binários num circuito eletrônico em que o "1" é expresso como o estado energizado e o "0" como o estado desenergizado. Desde seu início até hoje, a máquina computadora foi bastante aperfeiçoada – sendo que princípios estabelecidos por Turing permaneceram (como o uso da notação binária *etc*.). Resumidamente, o funcionamento do computador atual ocorre principalmente em três camadas:

Figura 3 – A simplified view of hardware and software as hierarchical layers, shown as concentric circles with hardware in the center and applications software outermost



Fonte: Patterson e Hennessy (2012, p. 10)

A camada de *hardware* recebe o fluxo de elétrons (corrente) que é convertida em "1s" (estado energizado, o que fornece tensão) e "0s" (estado desenergizado, que não fornece

tensão). Neste nível está o *hard drive* (estoque), a memória RAM (unidade de execução) e o processador (controle) – componentes básicos da máquina de Turing universal (TURING, 1950, p. 437). Acima, estão os *softwares* do sistema operacional, incluindo o *kernel* (Linux, Windows, macOS *etc.*), o núcleo do sistema operacional, responsável pela comunicação entre o *hardware* e a aplicação – o *kernel* executa a gestão dos recursos do *hardware* conforme a demanda da aplicação. Acima, está a camada da aplicação, o *software* que, com base em códigos de programação, recebe informações (*input*), requisita ao *kernel* o uso de recursos do *hardware*, recebe as informações do *hardware* pelo *kernel* e as transforma em uma resposta (*output*) – o *software* da aplicação transforma a resposta da máquina, por exemplo, no conteúdo gráfico que é visto na tela do computador (utilizando um comando para o *kernel* que determina a projeção de uma determinada cor [vermelho, verde, azul] em cada *pixel* [menor ponto da imagem digital] do *hardware* monitor). O usuário é externo ao sistema, mas o alimenta com informações (*input*) e interpreta o resultado (*output*) (PATTERSON; HENNESSY, 2012, p. 13-26).

O *hardware* também tem *software* próprio, chamado *firmware*, que se comunica com o *kernel* no nível dos *softwares* do sistema (Figura 3). E a comunicação entre o *kernel* e a aplicação é frequentemente realizada pelo *shell*, que é um *software* que transmite comandos inseridos em aplicações gráficas para o *kernel* (como o GNU Bash, o GNOME Shell e o KDE Plasma).

Assim, existe um ciclo para um *input* inserido pelo usuário retornar com um *output* para ele: usuário, *software* da aplicação, *softwares* do sistema, *hardware*; *hardware*, *softwares* do sistema, *software* da aplicação, usuário.

3.1.1.1 O elemento digital

Como demonstrado no item acima, as operações algorítmicas do computador são efetuadas com elementos digitais.

Em noção clássica, “Elemento de cada coisa é o constitutivo primeiro” “e que é indivisível em outras espécies” (ARISTÓTELES, 2002, p. 197). O constitutivo primeiro digital, indivisível em outras espécies, é o *bit*, o dígito binário (*binary digit* em inglês, de cuja contração resulta o nome [MACKENZIE, 1980, p. 12]) que pode ser um estado energizado, expresso em notação binária por “1”, ou um estado desenergizado, expresso por “0” (vide os itens 3.1 e 3.1.1, *supra*). O *bit*, armazenado ou transmitido, é o elemento digital. Se um humano utilizar o elemento digital numa significação, o elemento é uma informação; se uma

máquina operar o elemento, o elemento é um dado (VIANNA; MACHADO, 2013, p. 16-20); e os dados sobre outros dados são os metadados[75]; conceitos endossados pela Associação Brasileira de Normas Técnicas (ABNT, 2013b, p. 2).

Por convenção (hoje, é utilizado o ISO/IEC 2382), chamou-se o conjunto de oito *bits* de *byte*. Um *byte*, por ser uma sequência de oito *bits*, possibilita que um código mínimo (um *byte*) tenha 256 valores matemáticos possíveis (MACKENZIE, 1980, p. 12, 26) – precisamente, o *bit* é um elemento eletrônico-digital, já que existem outras notações digitais além da eletrônica, como o código Morse, contudo, pela ampla associação do vocábulo *bit* à notação utilizada em computadores, neste trabalho é utilizada a expressão "elemento digital", não "elemento eletrônico-digital".

Os arquivos de computador, como uma foto, uma gravação de som, um vídeo ou um documento escrito, são sequências de *bits* (MARSHALL, 2008, p. 69-70) (que sempre têm um armazenamento físico – mesmo os arquivos armazenados em nuvem estão num *hardware* de terceiro [LIN, 2018, p. 8]).[76]

Para esta tese sobre busca e apreensão de elementos digitais, é fundamental compreender o que é o elemento digital que constitui o arquivo de computador – o que é indissociável da compreensão do que é o computador, a máquina pela qual os elementos digitais são operados.[77] Feito isso, o capítulo explicitará noções específicas das tecnologias relacionadas à busca e apreensão de elementos digitais para, depois, aplicar transdisciplinarmente toda a construção anterior à situação legislativa vigente.

3.2 Técnicas de busca e de apreensão de elementos digitais

A Convenção sobre o Crime Cibernético, celebrada em Budapeste[78], recomenda que a busca e a apreensão ocorram fisicamente ou por ingresso remoto no sistema informático (artigo 19). Em ambos, a coleta dos arquivos – e o próprio acesso a eles, como será demonstrado – é feito por cópia.

A importância da noção de cópia no sistema informático é fundamental para compreender a busca e apreensão de elementos digitais e até o funcionamento do computador. Por isso, a noção de cópia será a próxima explicitada.

[75] Os metadados possibilitam a identificação de certos elementos do recurso informático, a sua proveniência e o monitoramento de seu funcionamento. Existem padrões de metadados. O padrão mais utilizado para a catalogação de recursos eletrônicos na Web, por exemplo, é o International Organization of Standardization/International Electrotechnical Commission (ISO/IEC) 11179, desenvolvido pela Dublin Core Metadata Initiative para facilitar a circulação de dados pela internet (PON; BUTTLER, 2021).

[76] Vide o item 4.10, *infra.*

[77] Para o aprofundamento na dinâmica de funcionamento do computador, vide: Patterson e Hennessy (2012).

[78] Os aspectos jurídicos da Convenção de Budapeste serão tema do próximo Capítulo.

3.2.1 Cópia

A máquina de Turing universal transformada por von Neumann no computador é composta por ao menos três partes: um estoque de armazenamento (que contém as regras de funcionamento), o *hard drive*; uma unidade de execução responsável por operações individuais de leitura e escrita, a memória RAM; e um controle que acessa o *hard drive* e a memória RAM e opera o cumprimento das regras de funcionamento, o processador (item 3.1, *supra*).

A cópia é fundamental no funcionamento do computador. Quando o processador acessa o *hard drive* para o cumprimento dos códigos lá escritos em *bits* ele cria uma cópia desta sequência de *bits* (o arquivo) na memória RAM, onde o arquivo será lido e pode ser alterado. O computador não funciona sem cópias; o acesso a um arquivo digital é o acesso a uma cópia do arquivo original (gravado no *hard drive*), momentaneamente existente na memória RAM. O que o monitor projeta para a interpretação humana, portanto, é a projeção da cópia do arquivo original na memória RAM, não o arquivo original. Assim, toda atividade por computador envolve cópias (pelo menos a cópia do arquivo do *hard drive* para a memória RAM) (LESSIG, 2006, p. 192-193).

Por estas razões, tecnicamente, todo acesso a elemento digital envolve cópias (internas no sistema ou por máquina externa ao *hard drive* original apreendido).

A cópia integral é a cópia completa do dispositivo de armazenamento, incluindo o espaço livre, arquivos deletados, mas não apagados definitivamente do *hard drive* e áreas que tenham sofrido algum dano. A cópia integral cria uma imagem idêntica do sistema informático para ser acessada *offline*. A cópia parcial é a cópia de certos arquivos (mas não do sistema inteiro) relacionados ao caso investigado, tal como demarcado na decisão judicial que autoriza a busca e apreensão. O espelhamento de arquivos é a sincronização dos arquivos dum primeiro dispositivo num segundo, operado pelo envio de cópia dos arquivos da primeira máquina, assim como das alterações neles feitas, para a segunda (MARSHALL, 2008, p. 47-48).

3.2.2 Apreensão material do dispositivo eletrônico

A busca e apreensão de dispositivos não é novidade e consiste em dois atos distintos, a procura do dispositivo e a sua obtenção material (PITOMBO, Cleunice, 2005, p. 109, 230).

Existem particularidades tanto na busca como na apreensão de dispositivo eletrônico.

A principal particularidade na busca é a possibilidade de procurar o dispositivo eletrônico pela localização do cartão SIM[79] ou do GPS[80] fornecida pelo próprio dispositivo, o que facilita a busca. De outro lado, o avanço de tecnologia faz com que o tamanho do dispositivo eletrônico que armazena os dados possa ser bastante reduzido (um *pen drive* do tamanho de 2 centímetros pode conter, *e.g.*, 64 *gigabytes*, o suficiente para armazenar cerca de treze mil livros em formato PDF), o que pode facilitar seu ocultamento e dificultar a busca.

Uma vez localizado o dispositivo eletrônico, sua apreensão material deve ser realizada com cautela. Computadores encontrados ligados, por exemplo, devem ser examinados antes de seu transporte, sob o risco de perda de dados sensíveis com o seu desligamento (como o que está na memória RAM ou no *cache* do navegador) (RAMALHO, 2019, p. 118-120).[81]

3.2.2.1 Criptografia

O dispositivo eletrônico encontrado e apreendido não é, necessariamente, passível de acesso. Uma das principais causas é a existência de criptografia.

Técnicas de criptografia existem há milhares de anos. Julius Caesar, *e.g.*, a utilizou para encobrir o conteúdo de suas mensagens (com técnica em que cada letra correspondia à terceira posterior no alfabeto; a letra "a" criptografada, descriptografada era "d", por exemplo) (SMART, 2016, p. 119-121). Etimologicamente, criptografia deriva das palavras gregas κρυπτός (*kryptos*), que significa escondido, e γράφειν (*grafein*), que significa escrever (EDGE; O'DONNELL, 2016, p. 497). Pela criptografia, uma mensagem simples é transformada numa mensagem cifrada, decifrada apenas por uma ou mais chaves.

Foge ao escopo da pesquisa explicar as muitas técnicas de criptografia existentes. Apenas é destacada a situação da criptografia por algoritmos complexos poder impossibilitar

[79] O cartão SIM contém pouco espaço de armazenamento, mas associa uma identificação física, a International Mobile Subscriber Identity (IMSI) – número único do cartão SIM registrado na sua fabricação física – a um endereço lógico (semelhante ao IP), que é o número do telefone (MARSHALL, 2008, p. 113-116, 150-156). No cartão SIM estão armazenados dados, *e.g.*, sobre: provedor de telefonia e internet; números gravados na agenda do celular; registro de chamadas telefônicas e de texto; configurações do telefone; e localização (pelo Global System for Mobile Communications [GSM], que é o sistema utilizado pelas provedoras de telefonia para a comunicação entre os telefones e a rede, e que registra a localidade das antenas que um aparelho esteve conectado num determinado momento) (MARSHALL; MILLER, 2019) (LIN, 2018, p. 399-405).

[80] O Global Positioning System (GPS) é tecnologia que utiliza rede de satélites ao redor do planeta para identificar a localização de um aparelho em qualquer lugar da Terra (MARSHALL, 2008, p. 116-117). Desenvolvido pelo Departamento de Defesa dos Estados Unidos nos anos 1960 e 1970, o GPS calcula a localização pelo tempo de resposta na comunicação de ao menos três satélites com o dispositivo receptor. Além do uso militar para estabelecer precisamente qualquer localização (independente do clima, hora ou luminosidade), o GPS, hoje, é utilizado em telecomunicações, transmissão de energia elétrica, transporte e várias outras aplicações (MCNEFF, 2002).

[81] Vide o item 5.1.2, *infra.*

o acesso aos dados armazenados num dispositivo eletrônico, mesmo com a sua apreensão física. Exemplificadamente, o Superior Tribunal de Justiça (Recurso em Mandado de Segurança nº 49.349 [BRASIL, 2021b]), já autorizou cooperação internacional do Brasil com os Estados Unidos para o uso de tecnologia avançada para desencriptar um *hard drive* objeto de investigação criminal, em função da inexistência de tecnologia suficiente para acessar os dados no Brasil – o que não assegura a desencriptação (o que ocorreu, *e.g.*, na operação Satiagraha, em que, após mais de um ano, o FBI estadunidense não conseguiu desencriptar um *hard drive* apreendido pela Polícia Federal [FOLHA DE S. PAULO, 2021]).

Um computador, assim, pode, apesar de ter seu armazenamento físico apreendido, ter seus dados completamente inacessíveis por estarem criptografados.

3.2.3 Ingresso remoto

A Convenção de Budapeste (artigo 19.1.a) recomenda a edição de medidas legislativas que regulamentem a busca e apreensão por ingresso remoto – novamente, lembra-se a opção metodológica de tratar dos aspectos jurídicos relacionados no capítulo seguinte e, neste, tratar das noções tecnológicas envolvidas.

A ligação de dois ou mais computadores (ou outros dispositivos eletrônicos, como roteadores, modens *etc.*) que podem transmitir dados entre si é uma rede (*network*). Nessa transmissão, são necessários, ao menos, dois dispositivos, um meio transmissor e um protocolo de comunicação (KIZZA, 2017, p. 3). O ingresso remoto de um computador em outro é um ingresso remoto em rede.

Qualquer *hardware*, *software* ou equipamento que limite a comunicação em rede é um *firewall* (CHESWICK *et al.*, 2003, p. 175). Além do *firewall* protegendo a transmissão de dados em rede, o sistema informático pode (ou não) ter outras barreiras de proteção variadas, como antivírus e senhas fortes. Por isso, como explicam Hutchins, Cloppert e Amin (2011), não existe um procedimento único para o ingresso remoto num sistema informático. Cada invasão adota estratégia diferente, conforme as especificidades do sistema que será invadido.

Contudo, os mesmos autores elencam uma sequência de atos frequente na invasão remota, composta por: reconhecimento, armamento, entrega, execução, instalação, comandar e controlar, cumprir os objetivos. O reconhecimento é a identificação e pesquisa sobre o alvo. O armamento é a preparação dos recursos que serão utilizados, como a criação de um *software* malicioso para atacar uma vulnerabilidade do sistema (*exploit*)[82]. A entrega é o envio

[82] O *exploit* é a exploração de uma vulnerabilidade no código do *software* instalado no sistema (FRAGA, 2019, p. 141). Uma lista gratuita de vulnerabilidades pode ser acessada em: https://www.exploit-db.com/.

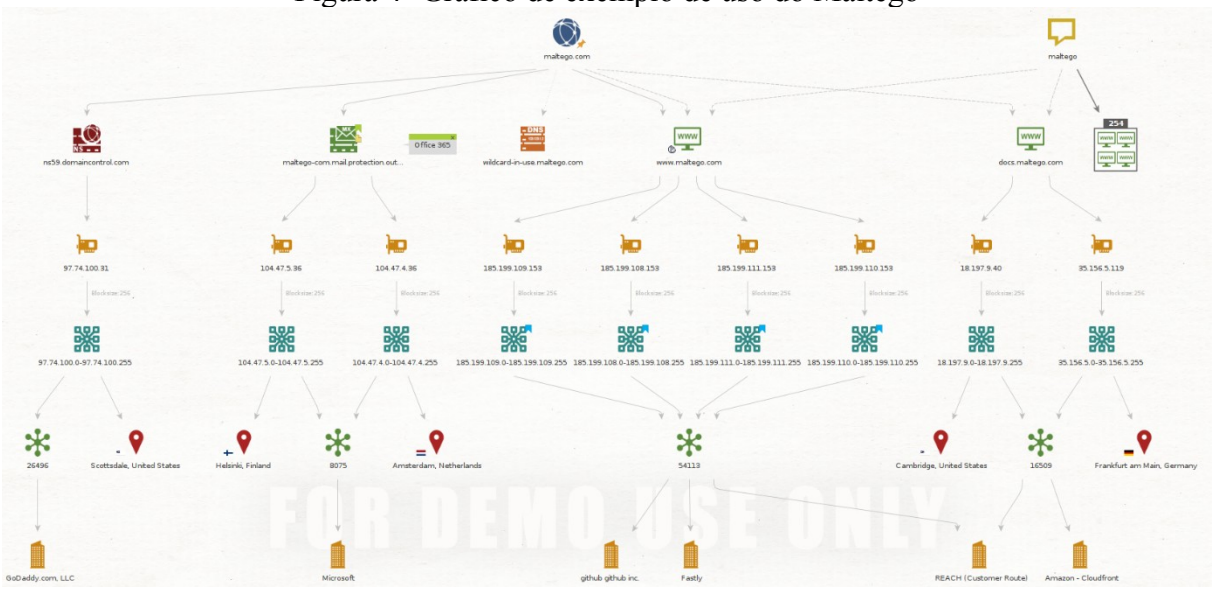
do *software* para o alvo. A execução é a ativação do *software*, de maneira remota ou autoexecutável. A instalação é a inserção do *software* no sistema do alvo para ser armazenado de maneira persistente. Comandar e controlar é assumir as operações do sistema do alvo destruindo barreiras contra o *software* malicioso (tal como desativar o *firewall*). Cumprir os objetivos é usar o sistema do alvo para atingir as finalidades da invasão, como coletar arquivos específicos, a integralidade do sistema ou criar espelhamento (HUTCHINS; CLOPPERT; AMIN, p. 87-96, 2011).

Exemplificadamente, Hutchins, Cloppert e Amin (2011, p. 96-99) citam caso concreto envolvendo um *e-mail* para o alvo. Primeiro, o alvo foi identificado e foi descoberto seu endereço de *e-mail* (reconhecimento). Depois, foi criado um arquivo em PDF com um *backdoor*[83] escondido, explorando uma vulnerabilidade conhecida em arquivos em PDF descoberta em 19 de fevereiro de 2009, mas só corrigida em 10 de março de 2009 (armamento). Após, o *e-mail* com o anexo em PDF foi enviado para o alvo (entrega). Ao abrir o arquivo PDF contendo o *backdoor*, o alvo, sem saber, possibilitou a autoexecução do *software* (execução). Na sequência, o *backdoor* foi instalado no diretório "C:\" (instalação). Após isso, o invasor passou a controlar o sistema do alvo, por comando enviado pela internet (comandar e controlar). Finalmente, as finalidades da invasão foram alcançadas (cumprir os objetivos).

A etapa de reconhecimento é especialmente importante para traçar a estratégia de ingresso remoto. Neste capítulo sobre noções de tecnologia, para exemplificar como pode ser feito o uso de *software* para descobrir informações sobre quem sofrerá a busca, cita-se brevemente as funcionalidades do *Maltego*.[84]

[83] Vide o item 3.2.3.1, *infra*.
[84] Disponível em: https://www.maltego.com/downloads/.

Figura 4- Gráfico de exemplo de uso do Maltego



Fonte: Maltego Technologies (2021)

O *Maltego* é um *software* que possibilita o cruzamento entre bancos de dados disponíveis na internet e a projeção gráfica de pesquisas que relacionam nome de pessoas, *e-mail*, número de IP, *skype*, endereços físicos, filiações institucionais, *site*, dados disponibilizados em redes sociais como o *Facebook* e o *LinkedIn*, *etc.* Somado a isso, o *Maltego* pode ser integrado com outros bancos de dados (como os das polícias – em sistema interno disponível apenas para as próprias polícias – e os de empresas privadas – inclusive com acesso à *deep web*[85]) (FRAGA, 2019, p. 79-83).

Na etapa de reconhecimento, pode ser encontrado um número de IP ou um endereço de *e-mail*, por exemplo. Com essas informações é possível desenhar a melhor estratégia de ingresso remoto para a busca – como o envio de *malware* ou outra técnica, como será demonstrado nos subitens seguintes.

3.2.3.1 Malware

O *malware* é *software* com propósito malicioso que executa código sem a permissão do usuário (LIN, 2018, p. 426). Vírus, *worm*, *spyware*, *Trojan Horse* e *rootkit* são espécies de *malware.*

O vírus é *software* que replica a si mesmo de um sistema para outro, por meio de entrega que pode utilizar arquivo ou outro *software*. Sem depender da atuação humana para se multiplicar, o vírus sempre atua sobre outra aplicação (como o vírus biológico) (MARSHALL, 2008, p. 66-67). Já o *worm* não necessita de hospedeiro e opera por redes,

[85] A parte da internet não acessível aos buscadores (GREENBERG, 2021).

como a internet, replicando-se de máquina para máquina por vulnerabilidades de segurança (*exploit*) (LESSIG, 2006, p. 20). Por exemplo, em julho de 2001, o "Code Red worm" infectou computadores da Universidade de Foshan, na China, e espalhou-se para mais de 350.000 máquinas em um dia, explorando vulnerabilidade do Microsoft Windows NT4 e Microsoft Windows 2000: o alvo era escolhido aleatoriamente para infecção por tentativa e erro; encontrando uma máquina suscetível à vulnerabilidade, o *worm* explorava uma falha de programação e acessava a máquina pela porta TCP 80 (utilizada para a conexão com a internet); inserido na máquina, ele executava comandos automáticos; entre esses comandos, estava um para que o *worm* fosse copiado e enviado, a partir da máquina infectada, para outra escolhida aleatoriamente. Esse *worm*, especificamente, não causou grandes danos – apesar de fazer com que aparecesse no navegador a frase "HELLO! Welcome to http://www.worm.com! Hacked By Chinese!" –, mas o mesmo tipo de ataque pode ser utilizado para comandar remotamente várias máquinas para, exemplificadamente, sobrecarregar um servidor e "derrubar um site" (KIZZA, 2017, p. 76-77).

O *spyware* é *malware* autoexecutável ou executado remotamente que periodicamente obtém dados sobre determinada aplicação, evento ou usuário e envia esses dados para máquina externa (KIZZA, 2017, p. 509). O FBI, por exemplo, desenvolveu o *Computer and Internet Protocol Address Verifier* (CIPAV), que é um *spyware* que monitora: endereços de IP; portas abertas em *firewall*; os programas em execução na máquina; o sistema operacional; a versão do sistema operacional; o navegador; a versão do navegador; o nome do usuário; e o endereço do último site visitado. Primeiro, o FBI insere o CIPAV em determinados sites; depois, o alvo é rastreado e estimulado a acessar um *link*; com o acesso ao *link*, é instalado o *spyware* que envia os dados automaticamente da máquina do alvo para o investigador (POULSEN, 2021).

O *Trojan Horse* (Cavalo de Troia)[86] é *malware* que possibilita o acesso remoto à máquina pelo invasor (MARSHALL, 2008, p. 67). O nome do *malware* traduz sua operação: assim como os gregos liderados por Odisseu esconderam-se num cavalo de madeira para invadir Troia,[87] o *Trojan Horse malware* esconde-se em outro *software* para ser infiltrado no

[86] Também chamado de *backdoor* (LIU; MA; BAILEY; LU, 2021, p. 2).

[87] "Ora começa de novo, e o cavalo de pau nos invoca, que por Epeio foi feito com a ajuda de Palas Atena, esse, que o divo Odisseu com astúcia pôs dentro de Troia, cheio de heróis destemidos, que os muros sagrados saquearam. […] no tempo em que muitos se achavam na praça de Troia junto do muito famoso Odisseu, e escondidos no bojo desse cavalo, que os próprios Troianos à acrópole tiram. Ei-lo na praça; a redor se cruzavam diversas propostas, desencontradas. Mas três agradaram, por fim, no conselho: ou desfazer do cavalo madeiro com bronze impiedoso, ou conduzi-lo para o alto da rocha e no abismo atirá-lo, ou, qual imagem propícia, esperar que os divinos placasse, tal como logo depois decidiram que assim fosse feito, pois o Destino assentara que fosse assolada a cidade, quando abrigasse o possante cavalo, que tinha no bojo fortes Argivos, que a morte e o extermínio dos Troianos levaram." (HOMERO, 2011, p. 146).

sistema e possibilitar ao invasor o acesso remoto e a execução de seus comandos na máquina invadida (KIZZA, 2017, p. 340).

O *rootkit* é composto por um conjunto de códigos projetados para possibilitar ao invasor o nível máximo de acesso ao sistema (*root* em sistemas GNU/Linux). Pela exploração de vulnerabilidade do sistema (*exploit*) ele é instalado na máquina, eleva os privilégios de usuário para o nível de administrador, elimina os rastros de sua instalação e torna-se praticamente indetectável, podendo alterar os registros do sistema, o *kernel* e até *firmware*, escapando das detecções por antivírus operadas no nível das aplicações (EVANCICH; LI, 2016, p. 100, 104).

Sobre o uso de técnicas tão invasivas que podem assumir total controle das funções do sistema e, inclusive, eliminar o rastro das operações, observa Angus Marshall (2008, p. 46, tradução nossa[88]) que "qualquer programa que faz uso de funções do sistema deve ser considerado impreciso, a menos que possa ser provado o contrário". O ato do investigador no sistema, por óbvio, já não é o ato investigado, e os elementos produzidos serão da atividade do investigador, que não são exatamente os da atividade do investigado e que podem ser resultado de implantação, pelo investigador, de elementos não existentes anteriormente (o que, com o dolo específico de produzir efeitos no processo penal, é crime de fraude processual, conforme o Código Penal, artigo 347, parágrafo único[89]).

Nesta situação, até a prova de se os atos são do investigador ou do investigado pode ser impossível se os registros do sistema forem eliminados pelo investigador, o que é explícita ofensa à cadeia de custódia de elementos digitais em função da eliminação dos vestígios da história cronológica do elemento de prova (tema específico dos itens 5.1.1 a 5.1.2.2, *infra*).

Na Europa e nos Estados Unidos há regulamentação do uso de *malware* pela investigação criminal[90]; o que ainda não ocorreu no Brasil[91].

3.2.3.2 Wireless

[88] "any program which makes use of system functions must be considered inaccurate unless it can be proven otherwise".
[89] "Art. 347 – Inovar artificiosamente, na pendência de processo civil ou administrativo, o estado de lugar, de coisa ou de pessoa, com o fim de induzir a erro o juiz ou o perito: Pena - detenção, de três meses a dois anos, e multa. Parágrafo único – Se a inovação se destina a produzir efeito em processo penal, ainda que não iniciado, as penas aplicam-se em dobro." (BRASIL, 2022g).
[90] Vide: David Ramalho (2019, p. 335-352) e Carlos Mendes (2018).
[91] "Não há, atualmente, lei processual que contemple o direito fundamental restringido pelo referido método de obtenção de prova. Dizer isso, por evidente, é dizer que não se trata simplesmente de interceptação da comunicação de dados, logo, incompatível com a Lei 9.296/96; ademais não se trata — tão somente — da restrição ao direito à livre comunicação. Muito menos haveria que se falar em uso análogo dos dispositivos processuais referentes à busca e apreensão (e custódia) de provas físicas. O uso de procedimentos análogos de busca e apreensão para provas físicas não contempla as peculiaridades de preservação da prova (custódia), o que poderá invalidar o material probatório." (LOPES JR.; MENDES, Carlos, 2022).

O ingresso remoto também pode utilizar ataque por *wireless*, que é a conexão de rede sem fio. A tecnologia mais famosa de *wireless* é o *WiFi*, que é um conjunto de protocolos que possibilita a comunicação de dispositivos por ondas de rádio. Outra tecnologia muito conhecida é o *bluetooth*, que também utiliza ondas de rádio para a transmissão de dados, mas segue protocolos diferentes (LESSIG, 2006, p. 272-273) (MARSHALL, 2008, p. 38-41). Essas tecnologias são utilizadas em grande escala e estão nas casas, cafés, *shopping*, universidades, escolas, hotéis, aeroportos, *smartphone*, computadores, *notebook*, fones de ouvido e em vários outros lugares e dispositivos.

Diferente da rede conectada por fio, que exige o conhecimento da localidade exata dos dispositivos e das conexões à rede para ser investigada, a conexão por *WiFi* ou *bluetooth* pode ser investigada sem o conhecimento da localidade exata dos dispositivos e à distância, por outro dispositivo que possa receber e transmitir dados na mesma frequência utilizada na rede (MARSHALL, 2008, p. 40).

Descoberta, a rede pode ser investigada, os dispositivos conectados podem ser localizados por *GPS* e (como para acessar a rede basta relacionar seu nome a uma senha) é possível ataque de força bruta (tentativa e erro) para o acesso à rede e posterior ingresso remoto num dispositivo específico (HERTZOG *et al*., 2021, p. 300) (FRAGA, 2019).[92]

A facilidade de detecção da existência da rede e o uso em grande escala de *wireless* tornam os ataques a redes sem fio atrativos como escolha de estratégia de ingresso remoto.

3.3 Uso de sistemas privados

A investigação criminal deve ser impulsionada por órgãos públicos "em completa independência da vontade e da actuação de quaisquer particulares" (FIGUEIREDO DIAS, 1974, p. 116). A Constituição de 1988 determina que a segurança pública deve ser exercida por órgãos oficiais em seu artigo 144, e o Código de Processo Penal (artigo 4º) que a função de polícia judiciária deve ser realizada por órgãos da administração pública (BRASIL, 2020a; 2021).[93]

Contudo, o uso de sistemas privados de tecnologia pelas polícias não é novidade no Brasil. A operação Lava Jato, a investigação do homicídio de Marielle Franco e Anderson

[92] Exemplificadamente, a rede pode ser descoberta pelo *Nmap*, investigada pelo *Fern Wifi*, a localização em *GPS* dos dispositivos pode ser obtida pelo *Kismet* e é possível ataque de força bruta com o *John the Ripper* – sendo que todas as aplicações indicadas são pré-instaladas no *Kali Linux* (HERTZOG *et al*., 2021).

[93] Todavia, o próprio CPP dá espaço para a intervenção privada na promoção da persecução penal ao condicioná-la à vontade do ofendido nas situações de ação penal de iniciativa privada e de iniciativa condicionada à representação (art. 5º, §§ 4º e 5º, e arts. 24 e 30) (TOURINHO FILHO, 1992, p. 43-44).

Gomes e a investigação da morte de Henry Borel, por exemplo, utilizaram o sistema *Cellebrite* (BBC NEWS, 2021) que, conforme a própria empresa, possibilita o desbloqueio de aparelhos *Apple* e *Android* e a extração completa de dados com o uso de inteligência artificial (CELLEBRITE, 2021).

Segundo o Instituto de Pesquisa em Direito e Tecnologia do Recife, o gasto público do governo de Jair Bolsonaro em 2020 com a contratação de sistemas privados como o *Cellebrite* foi de R$ 54,5 milhões e o gasto público dos estados foi de R$ 45 milhões em 2021 (RAMIRO, 2022, p. 47).

Em outros países, há confirmação do uso do *Pegasus*, um *spyware* que consegue o ingresso remoto em *smartphone* (basta proximidade com o *WiFi* do aparelho, sem ser necessário qualquer comportamento do alvo), a abertura e gravação do microfone e da câmera, a cópia de mensagens, a obtenção de localização, a extração de dados e o espelhamento (THE GUARDIAN, 2021). Existe a comprovação do uso do *Pegasus* em *smartphones* de mais de quarenta e cinco países. Apenas no México, quinze mil aparelhos foram objeto do *spyware*. Cento e oitenta jornalistas do *Financial Times*, *CNN*, *The New York Times*, *France 24*, *The Economist*, *Associated Press*, *Reuters,* entre outros, estão no grupo de pessoas que tiveram seus aparelhos invadidos.[94]

3.4 Engenharia social

Todo sistema tem usuário com poderes especiais (para acessar e editar determinados diretórios, alterar o sistema operacional, *software etc.*). Ainda que protegidos de várias maneiras diferentes, os elementos digitais sempre estarão sujeitos ao fator humano na segurança da informação e "não existe uma tecnologia no mundo que evite o ataque de um engenheiro social" (MITNICK, 2003, p. 195).

A engenharia social é estratégia de ataque de sistema informático consistente na manipulação do usuário para que comprometa a segurança do sistema, por exemplo, fornecendo informações confidenciais ou facilitando a instalação de *malware*. Ela pode ocorrer pela exploração de informações pessoais do usuário, por conversas telefônicas, pela sabotagem do sistema e simulação de que é a empresa que resolve o problema, pela combinação de técnicas; enfim, o limite é a imaginação do atacante (KROMBHOLZ *et al*., 2015, p. 114-115). O *hacker* Mitnick dá um exemplo:

A ligação para Sarah

[94] Sobre a sociedade de controle, vide o Capítulo 2, *supra*.

> "Recursos Humanos, aqui é Sarah."
> "Oi Sarah, Aqui é George do estacionamento. Você sabe o cartão de acesso usado para entrar no estacionamento e nos elevadores? Bem, tivemos um problema e precisamos reprogramar os cartões de todos os funcionários novos que foram contratados nos últimos 15 dias."
> "Você precisa dos nomes?"
> "E dos números de telefone."
> "Posso verificar a nossa lista de novos contratados e ligar de volta. Qual é o número do seu telefone"
> "É 73… Ah, estou saindo para o café, que tal se eu ligar de volta em meia hora?"
> "Tudo bem"
> Quando ele ligou de volta, ela explicou: "Ah, sim. Bem, há apenas dois. Anna Myrtle do Financeiro, ela é secretária. E aquele vice-presidente novo, o Sr. Underwood."
> "E os números dos telefones?"
> "Certo… O número do Sr. Underwood é 6973. O de Anna Myrtle é 2127."
> "Olhe, você me ajudou muito. Obrigado." (MITNICK, 2003, p. 160, grifo do autor).

Assim como os nomes de novos funcionários de uma empresa e seus telefones, a engenharia social pode obter várias outras informações e conduzir o alvo a determinados comportamentos.

A busca e apreensão de elementos digitais pode ser muito difícil em sistemas com proteção avançada – configurados para não serem encontrados, que utilizem o Tor para a navegação pela internet, com *firewall*, criptografia *etc.* Nessas situações, pode ser necessário o cúmulo da busca e apreensão com o agente infiltrado que atue como engenheiro social para a obtenção dos elementos digitais.

O cúmulo de meios ocultos será tratado no item 4.17, *infra*. Sobre a parte tecnológica do assunto, apenas é destacado que a obtenção de informações por agente infiltrado que utilize engenharia social (desde senha de *WiFi* à implantação de *malware*) pode ser útil para a busca e apreensão dos elementos digitais.

3.5 Computação forense

O progressivo aumento do uso do computador pela sociedade de controle (item 2.5, *supra*), simultâneo à regulamentação jurídica desse uso, provoca o aumento da importância da computação forense, ou seja, da aplicação de técnicas da ciência da computação no trato com os elementos digitais – incluindo a extração, registro, preservação e interpretação científica dos elementos (KIZZA, 2017, p. 304) – quanto a aspectos relevantes no foro judicial.[95]

[95] A ciência forense é muito antiga. Na China, já era utilizada há milhares de anos atrás, para a conferência de impressões digitais em documentos (LIN, 2018, p. 3).

Na computação forense, o saber organizado (ciência) da computação orienta o agir humano que visa às finalidades (técnicas)[96] de extrair, registrar, preservar e interpretar os elementos digitais (*bits*) para contribuir na construção do juízo.

Xiaodong Lin (2018, p. 22-27) sintetiza os atos mais comuns da computação forense em procedimento sequencial de três etapas. A primeira é a etapa de preparação; nela, as ferramentas necessárias são reunidas e as autorizações legais para atuar são conferidas. A segunda etapa ocorre no lugar da busca e apreensão; essa etapa é composta pela coleta dos elementos e pela atuação para a sua preservação. A terceira etapa ocorre no laboratório; a compõem: o exame do material apreendido para extrair os elementos digitais (incluindo a recuperação dos elementos digitais apagados), a análise dos elementos descobertos, a reconstrução da sequência de atos a que o elemento digital foi submetido (identificando quem fez o quê, quando, como, onde) e a apresentação, que é a criação do laudo dos atos realizados para uso processual.

Ressalta-se que deve existir primazia da Constituição jurídica democrática sobre a constituição da arquitetura do espaço virtual (LESSIG, 2006, p. 275); a questão é de legitimidade.[97] Códigos de programadores não são construídos pelos destinatários normativos (seus autores, em grande maioria, inclusive, trabalham para empresas privadas), não são submetidos à fiscalização democrática e nem são elaborados por pessoas que foram eleitas ou que, ao menos, têm formação jurídica para compreender o que significa criar um código informático que respeite o modelo constitucional do processo – se tivessem, todos os sistemas informáticos utilizados na investigação já produziriam automaticamente a cadeia de custódia da obtenção de determinados elementos de prova, com o registro de quem fez o que, quando, como, onde e porquê, por exemplo; algo que não apresenta qualquer dificuldade de programação e é sistematicamente ignorado no Brasil (o Sistema Guardião – *software* utilizado em interceptações telefônicas para recepção e armazenamento dos elementos de prova –, a título de exemplo, só registra os eventos ocorridos em parte dos atos e os *logs* [registros informáticos] do sistema são praticamente inacessíveis à defesa [SANTORO; TAVARES; GOMES, 2017, p. 629] que, com isso, não tem como conhecer, *e.g.*, como

[96] Vide o capítulo 5, *infra.*

[97] "A legitimidade democrática das decisões jurisdicionais, comprometidas com o princípio do Estado Democrático de Direito, está assentada na exclusiva sujeição dos órgãos jurisdicionais às normas que integram o ordenamento jurídico, sobretudo as normas constitucionais, emanadas da vontade do povo, porque discutidas, votadas e aprovadas pelos seus representantes, no Congresso Nacional. Por conseguinte, se todo o poder emana do povo, em nome de quem os órgãos do Estado o exercem, inclusive os órgãos jurisdicionais, o que é fundamento básico do Estado Democrático de Direito, assim declarado no parágrafo único, do artigo 1º, do texto constitucional, está a exigir a Constituição Federal de 1988 dos juízes e tribunais brasileiros decisões conforme as normas constitucionais e infraconstitucionais que integram o ordenamento jurídico." (BRÊTAS, 2018b, p. 166).

ocorreu a recepção dos elementos e quem acessou o sistema, o que é fundamental para aferir se o momento do ato foi posterior à decisão judicial, se existiu alteração no armazenamento do elemento de prova e para responsabilizar quem tenha acessado o sistema indevidamente).

Não importa somente a contribuição da ciência da computação para a cognição sobre o caso penal,[98] os limites jurídicos devem ser necessariamente observados para que o discurso do cientista computacional possa validamente integrar procedimento jurídico. O legislador previamente avaliou que os direitos fundamentais e as demais normas jurídicas regulamentadoras das diligências investigativas e das provas são superiores a qualquer outro critério (seja ele científico, moral, religioso *etc*.). São inadmissíveis o elemento de informação e a prova construídos ilicitamente, que sequer podem integrar o procedimento[99] (tema aprofundado no item 4.15, *infra*). A escolha política pela dignidade humana, pelo modelo constitucional do processo e por não realizar a cognição sobre o caso penal a qualquer preço já foi feita pelo constituinte.[100]

Por isso, na computação forense, a ciência da computação deve servir ao Direito, não o contrário. Esta noção implica na regência de todos os atos do cientista computacional pelo Direito democrático.

3.6 Limiar

Elementos digitais são *bits* operados pelo computador. Conhecer o que é o computador possibilita fiscalizar seu funcionamento e, consequentemente, as operações com elementos digitais.

A Convenção sobre o Crime Cibernético, celebrada em Budapeste, recomenda que a busca e a apreensão de elementos digitais ocorram fisicamente ou por ingresso remoto no sistema informático (artigo 19). Neste capítulo, a tecnologia envolvida foi o objeto. O próximo tratará dos aspectos jurídicos relacionados.

[98] Vide a nota n. 27, *supra.*

[99] "A *admissibilidade* da prova constitui, portanto, um conceito de direito processual e consiste numa valoração prévia feita pelo legislador, destinada a evitar que elementos provenientes de fontes espúrias, ou meios de provas reputados inidôneos, tenham ingresso no processo e sejam considerados pelo juiz na reconstrução dos fatos; daí sua habitual formulação em termos negativos: *inadmissibilidade, proibição de prova, 'exclusionary rules'*." (GOMES FILHO, 1997, p. 95). Código de Processo Penal, artigo 157 (BRASIL, 2021a).

[100] Constituição de 1988, artigos 1º, III, e 5º, II, LIV e LVI (BRASIL, 2020a).

4 BUSCA E APREENSÃO DE ELEMENTOS DE PROVA DIGITAIS

Após explicadas noções sobre a tecnologia envolvida na realização da busca e da apreensão de elementos de prova digitais torna-se possível a pesquisa de como é a realização concreta destes meios em consonância ao modelo constitucional do processo (BARROS, 2008b, p. 10-22) (ANDOLINA; VIGNERA, 1997); o objeto deste capítulo.

4.1 Conceituação

Busca e apreensão são atos distintos, apesar do legislador tê-los reunido no mesmo capítulo (XI), do título VII ("Da prova"), do livro I ("Do processo em geral"), do Código de Processo Penal (BRASIL, 2021a). A busca configura-se na procura de pessoas, elementos de prova ou bens relacionados ao caso penal[101] (como de foragidos, pessoas a serem notificadas; livros contábeis, computadores; e bens auferidos com a prática delituosa) (PITOMBO, Cleunice, 2005, p. 102-109). Apreender, conforme Sérgio de Moraes Pitombo, "em latim, *apprehendo*, *is endi*, *ensum*, *ere*, é verbo que significa tomar, agarrar, segurar, prender. *Apprehensio*, *onis*, é a ação de tomar algo, de segurar.". A apreensão processual é o ato de apossamento de pessoas, elementos de prova ou bens para finalidades processuais ou penais (como para proteger sequestrados, conservar elementos de prova ou assegurar a indenização da vítima) (PITOMBO, Sérgio, 1973, p. 72). De especial importância para esta pesquisa sobre a busca e apreensão de elementos de prova digitais, lembra-se a lição clássica de Eugenio Florian (1961, p. 187) de que, somado à conservação, sempre deve ser assegurada a identidade e a integridade elemento de prova (tema diretamente ligado à cadeia de custódia, tratada nos itens 5.1.1 a 5.1.2.2, *infra*).

Há divergência na literatura jurídica sobre se a busca e a apreensão são coerções lícitas, cautelares, meios de prova, meios de obtenção de prova ou medidas instrumentais.

Espínola Filho (1980, p. 195-196) entende a busca e apreensão como coerção lícita e meio de obtenção de prova, por configurar possibilidade do Estado de utilizar a força para obter o elemento de prova. No mesmo sentido: Bento de Faria (1960, p. 354-355).

Para Sérgio Pitombo (1973, p. 81), apesar da "atividade de coação processual real física, porque restritivas de direitos, possuem finalidade cautelar, quando impostas para garantia da instrução criminal". Contra a "natural demora do processo", a busca e a apreensão evitariam o "*periculum in mora*, nascedouro de dano à causa". Também entendendo que são

[101] Vide a nota n. 27, *supra.*

cautelares: Noronha (1979, p. 92); Pacelli de Oliveira (2010, p. 450); Nicolitt (2014, p. 807); e Rosa (2020, p. 425).

Nucci (2011, p. 207) entende a busca como "meio de prova, quando se vincule à autorização conferida pelo juiz para a realização de uma diligência ou uma perícia em determinado domicílio" e "meio assecuratório, quando se ligar ao ato preliminar de apreensão de produto de crime, razão pela qual se destina à devolução à vítima". E classifica a apreensão como "medida assecuratória, que toma algo de alguém ou de algum lugar, com a finalidade de produzir prova ou preservar direitos", sendo que a apreensão, segundo o autor, "Eventualmente, tem a finalidade de atuar como meio de prova".

Badaró (2015, p. 491) entende que a busca e a apreensão são meios de obtenção de prova: "não se trata, propriamente, de meio de prova, mas […] de meio de obtenção de prova. A busca e a eventual apreensão da coisa ou da pessoa, em si, nada provam. Entretanto, por meio da busca e da apreensão se conservam os elementos de prova apreendidos [...]". O autor se vale da distinção defendida por Antonio Magalhães Gomes Filho, a partir da literatura jurídica italiana:

> Os *meios de prova* referem-se a uma atividade *endoprocessual* que se desenvolve perante o juiz, com o conhecimento e participação das partes, visando a introdução e a fixação de dados probatórios *no processo*. Os *meios de pesquisa* ou *investigação* dizem respeito a certos procedimentos (em geral, *extraprocessuais*) regulados pela lei, com o objetivo de conseguir provas materiais, e que podem ser realizados por outros funcionários (policiais, por exemplo). Com base nisso, o Código de Processo Penal italiano de 1988 disciplinou, em títulos diferentes os *mezzi di prova* (testemunhos, perícias, documentos), que se caracterizam por oferecer ao juiz resultados probatórios diretamente utilizáveis na decisão, e os *mezzi di ricerca della prova* (inspeções, buscas e apreensões, interceptações de conversas telefônicas etc.) que não são por si fontes de conhecimento, mas servem para adquirir coisas materiais, traços ou declarações dotadas de força probatória, e que também podem ter como destinatários a polícia judiciária ou o Ministério Público. Outra importante distinção, ressaltada por Paolo Tonini, reside na *surpresa* que quase sempre acompanha a realização dos procedimentos de investigação, sem a qual seria inviável a obtenção das fontes de prova, ao passo que nos meios de prova é rigorosa a obediência ao contraditório, o que supõe tanto o conhecimento como a efetiva participação das partes na sua realização. (GOMES FILHO, 2005, p. 309).

Num exemplo concreto: "[…] se tratava de vítima de crime de extorsão mediante sequestro ou de redução à condição análoga à de escravo, poderá comparecer a juízo e prestar declarações. O meio de prova, contudo, não será a busca e a apreensão da pessoa, mas as 'declarações do ofendido'." (BADARÓ, 2015, p. 491). No mesmo sentido: Campanholo Marques (2019, p. 122).

Cleunice Pitombo (2005, p. 116-117) advoga que a busca é medida instrumental "no escopo de achar, encontrar pessoas, semoventes, coisas ou vestígios, que, de modo direito ou

indireto, se relacionem com o fato, pretensamente, ilícito e típico, investigado, ou perquirido" e a apreensão é "meio cautelar de obtenção de provas, quando visa a assegurar elementos indispensáveis à verdade criminal perquirida" – no que é acompanhada por Lopes Jr. (2012, p. 701). E entendem que é a combinação das anteriores: Tucci (2012, p. 1231) – meios de obtenção de prova, cautelares e coerções lícitas –; Frederico Marques (1998b, p. 287) – cautelares e coerções lícitas –; Tornaghi (1978, p. 53) e Grinover (2000, p. 479) – cautelares, não necessariamente probatórias, já que podem recair sobre pessoas, e coerções lícitas.

Como demonstrado na sequência, as diferenças conceituais na literatura são provenientes de três principais causas: parte dos autores não diferencia a busca da apreensão; parte não distingue o meio de prova do meio de obtenção de prova; e o tradicional predomínio do estudo do processo de conhecimento, com o estudo do cautelar em segundo plano (o que também ocorre com o executivo).

Sobre isto, em primeiro lugar, o Código de Processo Penal (BRASIL, 2021a) trata da busca e da apreensão conjuntamente, o que influenciou muitos autores a não as diferenciar.[102] Ocorre que a busca não resulta necessariamente em apreensão; o elemento de prova pode não ser encontrado, por exemplo. E a apreensão também não é necessariamente precedida da busca, pois pode ocorrer a entrega espontânea da pessoa, elemento de prova ou bem. Os atos de buscar e apreender são distintos; na lição de Sérgio de Moraes Pitombo (1973, p. 60):

> A apreensão, no mais das vêzes, segue a busca. Emerge, daí, o costume de vê-las unidas. Conceitos que se teriam fundido, como se fossem uma e mesma coisa, ou objetivamente inseparáveis. As buscas, contudo, se distinguem das apreensões, como os meios diferem dos fins.

Por isso, a organização do tema no Código de Processo Penal Militar é correta ao, no Livro I, Título XIII ("Das medidas preventivas e assecuratórias"), Capítulo I ("Das providências que recaem sobre coisas ou pessoas"), separar a Seção I para o tratamento "Da busca" e a Seção II para o tratamento "Da apreensão" (BRASIL, 2022a).[103]

Em segundo lugar, o mesmo Código reúne os atos em um único título, "Da prova". Contudo, cabe razão a Badaró (2015, p. 491) por sustentar que "A busca e a eventual apreensão da coisa ou da pessoa, em si nada provam". O resultado da busca e da apreensão não é "a prova", mas apenas a obtenção de elementos de prova que, submetidos aos meios de prova, resultam na prova. De acordo com Rosemiro Leal (2021, p. 197):

[102] *E.g.*, Frederico Marques (1998b, p. 287) e Tucci (2012, p. 1231).
[103] Com o mesmo entendimento: Cleunice Pitombo (2005, p. 102-104).

> A existência do *elemento* de prova, ainda que de certeza inegável, não autoriza, por si mesma a coleta de prova *contra legem*. A liberdade de apreensão do *elemento* de prova no *espaço* real há de sofrer o controle dos *meios* legais indicados na lei para se lavrar o *instrumento* de prova. Provar em direito é representar e demonstrar, instrumentando, os *elementos* de prova pelos *meios* de prova. A exemplificar, a *perícia* é um *meio* de prova para o exame de *elementos* de prova com a elaboração final do laudo que é *instrumento* de prova.

Assim, existe um procedimento de produção da prova – composto pelas fases de proposição, admissão, produção e valoração da prova; todas regidas pelas garantias processuais, principalmente o contraditório (BRÊTAS, 2016a, p. 106-107). Exemplificadamente, no processo penal: um *hard drive* apreendido é elemento de prova que, após a proposição pela acusação (*e.g.*, na denúncia) de que seja feito o meio de prova perícia sobre ele, pode ter sua relevância questionada pela defesa (*e.g.*, em resposta à acusação) e o meio de prova perícia pode ser ou não admitido pelo juízo; se admitido, é iniciada a produção do meio de prova com a apresentação de quesitos pelas partes e indicação de assistente técnico, seguido pelo exame pericial e elaboração do laudo, colocação da coisa à disposição do assistente técnico e elaboração de laudo próprio (CPP, arts. 158 e seguintes). O elemento de prova *hard drive* submetido ao meio de prova perícia resulta no registro da realização do meio de prova, o laudo, que será objeto de argumentação das partes em alegações finais, inclusive quanto à sua valoração.[104] Na sentença, o juízo decidirá sobre a regularidade de todos os atos probatórios e se o resultado da produção probatória (o laudo) confirma, nega ou é irrelevante à argumentação das partes sobre suas pretensões. Assim, a prova só existe no processo após a produção do meio de prova em contraditório; antes, o que a busca e apreensão pode possibilitar é a obtenção do elemento de prova, que não tem força probante. Afinal, somente com a participação em contraditório – como influência e não surpresa (NUNES, 2008) – dos destinatários do provimento a decisão jurídica pode ser qualificada como legítima (GONÇALVES, 1992, p. 146, 173-178), o que não ocorre na busca e apreensão, que é feita frequentemente *inaudita altera pars*.[105]

Em terceiro lugar, existem razões históricas para o foco da maior parte da academia ser tradicionalmente a pesquisa do processo de conhecimento (e, consequentemente, considerar a busca e a apreensão como meio de prova[106]). Chiovenda[107] afirmou serem as

[104] Por valoração compreende-se tanto a consideração da existência da prova nos autos, como a atribuição de importância da prova frente aos demais atos do procedimento (BRÊTAS, 2016a, p. 106-107).
[105] Vide os itens 4.13, 4.14 e 4.14.1, *infra.*
[106] *E.g.*: Nucci (2011, p. 207).
[107] Que teve (e tem) influência imensa no Brasil: "Após Bülow, a teoria da relação jurídica foi desenvolvida na Alemanha especialmente por Wach, Hellwig e Köhler – para quem, respectivamente, a relação jurídica seria triangular, angular, linear. Na Itália, Chiovenda foi o pioneiro que, nas palavras de Carnelutti, determinou 'uma mudança de rota, orientando para Alemanha o pensamento italiano'. Dentre os discípulos de Chiovenda estava

cautelares "*meras* ações" fundadas no direito do Estado (e não da parte) de tutela jurídica para assegurar sua futura atuação do conteúdo da lei no caso concreto (CHIOVENDA, 1923, p. 184, tradução nossa[108]; 1969, p. 34). Para Chiovenda, "a verdadeira jurisdição é apenas a *declaratória* do direito posto em causa" e que forma a coisa julgada (BAPTISTA DA SILVA, 2001, p. 35-36). Calamandrei, também endossando o caráter publicista das cautelares, as colocou como "instrumentos do instrumento", "subsidiárias", sustentou que elas visam assegurar o "*imperium judicis*" e que estão no limite entre a função judicial e a de polícia, mas como um acessório ao procedimento definitivo, nunca como um fim em si (CALAMANDREI, 2019, p. 163-166, 175-176, 252, tradução nossa[109]).

Como destaca Flaviane Barros (2019, p. 209-210), o processo penal se apropriou dos conceitos do processo civil (fundado na relação jurídica, em obrigações e que prioriza a teorização do processo de conhecimento à do cautelar) não considerando suas especificidades próprias[110] e, mormente em função da pressão pelo aumento do controle social:

> A cognição ordinária é interpretada como demora. Justificar-se-iam, assim, julgamentos antecipados que busquem tanto a prevenção de delitos quanto o controle social mediante respostas imediatas que privem de liberdade o inimigo interno. Assim, o dito processo penal cautelar se inicia muito antes e sobrepõe ao processo de conhecimento; sendo certo, porém, que apenas o processo de conhecimento se presta(ria) à imputação de uma conduta criminosa e à formação da culpa. O resultado disso é o menoscabo pelo processo de conhecimento e a quase impossibilidade de desconstituição do denominado juízo cautelar, que não deve(ria) estar atrelado à culpa. (BARROS; DALLE, 2021, p. 97-98)

As cautelares não estão em segundo plano no processo penal – principalmente na sociedade de controle que busca medidas ultrarrápidas, não quer esperar o tempo necessário para o processo de conhecimento e tende a diminuir a fronteira entre repressão e prevenção de delitos (item 2.2, *supra*). No cenário atual:

Liebman, que chegou ao Brasil no final da década de 1930 e iniciou seu trabalho como professor na Faculdade de Direito de São Paulo em 1941 – o que continuaria até 1946. Na docência em São Paulo, Liebman acumulou seguidores que continuariam o estudo da teoria da relação jurídica; entre eles estavam José Frederico Marques, Alfredo Buzaid e Moacyr Amaral Santos, que além de compor um grupo de discípulos que foi orientado diretamente por Liebman, moldaram toda uma geração do direito processual brasileiro." (PIMENTA, 2019, p. 28).

[108] "*mera* azione".

[109] "strumenti dello strumento"; "sussidiarietà".

[110] Carnelutti, ao discorrer sobre a relação entre o processo penal, o direito penal e o processo civil, utilizou a metáfora da Cinderela: descendentes do mesmo tronco comum, as "irmãs" processo penal e direito penal dividiram a mesma habitação por muito tempo, sendo que esta tomou para si o "bom e o melhor", atraindo a atenção dos estudantes, e àquela coube lidar com o resto de sua irmã mais chamativa; em relação à "irmã" processo civil, que conquistou autonomia científica própria frente ao direito civil (desde Bülow), o papel do processo penal foi de coadjuvante ao, também por muito tempo, apenas adaptar as noções elaboradas pelo processo civil. O processo penal, na metáfora de Carnelutti, era a Cinderela, a "irmã" que se contentava com as roupas usadas deixadas por suas "irmãs" direito penal e processo civil (CARNELUTTI, 1946, p. 73-78).

> […] o processo penal brasileiro vivencia uma situação paradoxal: nele vigora de fato uma 'cautelaridade permanente' e uma 'executoriedade provisória' […] Verifica-se assim uma concreta transmutação das características distintivas da suposta cautelaridade e da executoriedade: (I) a cautelaridade que deveria ser provisória e excepcional se torna permanente; e (II) a execução penal que deveria ser definitiva será provisoriamente iniciada com a condenação em primeira instância pelo conselho de sentença, desde que o juiz-presidente estipule uma pena alta. (BARROS; DALLE, 2021, p. 99).

Isso importa para a classificação da busca e da apreensão porque grande parte dos autores classifica a busca e a apreensão como cautelares (como demonstrado acima).

O que significa ser cautelar também merece esclarecimentos.

Veja-se, na socialização processual iniciada no final do século XIX e impulsionada pelo Estado de Bem-Estar Social (*Welfare State*),[111] o protagonismo do juiz deveria promover a mudança da sociedade para cumprir finalidades metajurídicas, como promover a paz social. Na defesa do hipossuficiente (Menger) ou para promover o bem-estar social (Klein), o juiz seria o protagonista sensível aos anseios sociais que promoveria a justiça pela relação jurídica pública do processo (Bülow). Num contexto de simplificação procedimental e ativismo judicial, o processo era instrumento do juiz para a tutela da sociedade (NUNES; BAHIA; PEDRON, 2020, p. 86-104). Calamandrei escreveu que as cautelares são "instrumentos do instrumento" neste cenário de socialização processual, em que os limites liberais à atuação dos juízes cederam espaço para o protagonismo judicial. Esse protagonismo precisava de meios de ser assegurado e Calamandrei – inspirado no *contempt of court* inglês[112] – conceituou as cautelares como "instrumentos do instrumento" exatamente para assegurar o "*imperium judicis*" (CALAMANDREI, 2019, p. 176, 252, tradução nossa[113]) (BAPTISTA DA SILVA, 2001, p. 35, 37).

Ocorre que o processo não é instrumento do juiz para realizar escopos metajurídicos e nem as cautelares são "instrumentos do instrumento" no Estado Democrático de Direito. Em primeiro lugar, o processo não é um meio que visa concretizar escopos metajurídicos: isso

[111] "É a fase processual típica do século XX, que se inicia no final do século XIX e que ganha força a partir do delineamento do paradigma do Estado do Bem-Estar Social (*Welfare State*), com a ruptura com a perspectiva liberal. Nesse período ocorre o agigantamento da atuação estatal; enorme preocupação com questões sociais; fortalecimento do Executivo no quadro da tripartição de funções; defesa de um perfil clientelista do cidadão (cidadão hipossuficiente); e a ingerência do Estado nas relações jurídicas." (NUNES; BAHIA; PEDRON, 2020, p. 86).

[112] Joseph Beale Jr. explica que, no direito inglês, qualquer ato que prejudique o funcionamento ou a dignidade do tribunal é um *contempt of court*, um desacato ao tribunal (de maneira parecida ao *contempt* contra o rei por ofensas contra ele ou o *contempt* contra o parlamento por perturbação em suas atividades); e que, para combater o desacato, o julgador usa de medidas coercitivas, como a prisão preventiva (BEALE JR., 1908, p. 162, 170).

[113] "strumenti dello strumento".

levaria à existência de um nível normativo superior ao democraticamente legislado,[114] que o regeria e que só seria acessível ao intérprete privilegiado juiz (GONÇALVES, 1992, p. 182). Essa noção de acesso restrito aos escopos metajurídicos pelos juízes possibilita a manipulação do sentido normativo e a impossibilidade de sua fiscalização (já que o Direito deveria respeitar a uma ordem invisível sentida apenas pelos privilegiados e que, por não poder ser conhecida pelo restante, não poderia sequer ser confrontada pelos demais) (CORDEIRO LEAL, 2008, p. 59-68). No Estado Democrático de Direito, o sistema jurídico deve atender apenas a critérios lógicos estabelecidos em lei, e não a ideologias de alguns; ao invés de escopos metajurídicos, quem rege o sistema jurídico é a Constituição (GONÇALVES, 1992, p. 183). Na democratização processual não existe protagonismo das partes ou do juiz. A decisão jurídica é resultado da atividade policêntrica e comparticipativa dos sujeitos do processo que atuam conjuntamente e sem hierarquia na construção do provimento final. Nela, não se busca a tutela do juiz na realização de escopos metajurídicos; é buscada, de maneira compartilhada, a efetividade[115] dos princípios constitucionais democráticos que estabelecem os critérios lógicos que possibilitam o controle da construção do procedimento e a participação ativa das partes, que são as destinatárias do provimento e se reconhecem como seu coautor (NUNES; BAHIA; PEDRON, 2020, p. 122-126). Na lição de Aroldo Plínio Gonçalves (1992, p. 195):

> Com as novas conquistas do Direito, o problema da justiça no processo foi deslocado do "papel-missão" do juiz para a garantia das partes. O grande problema da época contemporânea já não é o da convicção ideológica, das preferências pessoais, das convicções íntimas do juiz. É o de que os destinatários do provimento, do ato imperativo do Estado que, no processo jurisdicional, é manifestado pela sentença, possam participar de sua formação, com as mesmas garantias, em simétrica igualdade, podendo compreender por que, como, por que forma, em que limites o Estado atua para resguardar e tutelar direitos, para negar pretensos direitos e para impor condenações.

Com o processo não sendo instrumento do juiz, o fundamento da cautelar não tem como ser a segurança, numa acepção de vigilância do judiciário para evitar perigos à sua futura manifestação, como defenderam Chiovenda (1923, p. 184) e Calamandrei (2019, p. 252). O fundamento da cautelar é, no processo penal, o risco iminente, concreto e substancial

[114] "A admissão de escopos metajurídicos da jurisdição e do processo pressupõem, necessariamente, a existência de três ordens normativas distintas: a jurídica, a social e a política. Os escopos metajurídicos só poderiam ser entendidos, portanto, como escopos pré-jurídicos." e "A ordem jurídica e a ordem social têm seu fundamento na ordem jurídica, existem dentro do ordenamento jurídico e sofrem a sua regulamentação. Supor o contrário seria o mesmo que se admitir a possibilidade de se afirmar que, na sociedade organizada, o poder se exerce dentro da ei e pela lei, e que o poder não se exerce dentro da lei e pela lei." (GONÇALVES, 1992, p. 182-183).

[115] Vide a nota n. 12, *supra.*

à futura atuação das partes – as destinatárias do provimento (BARROS, 2008a, p. 179) –; e o que rege a cautelaridade não é a segurança, mas a "base principiológica uníssona" (BARROS, 2008b, p. 17) que constitui o modelo constitucional do processo, principalmente o princípio da inocência, que distingue o ramo processual penal dos demais e que implica no tratamento digno, no ônus probatório ser da acusação e na excepcionalidade das medidas que ofendam os direitos do investigado ou acusado (BARROS; DALLE, 2021, p. 91, 106-111).[116] Logo, no Estado Democrático de Direito as cautelares não são medidas instrumentais do instrumento do juiz ("instrumentos do instrumento", na expressão de Calamandrei), mas um conjunto de institutos processuais e procedimentos que asseguram a futura atuação das partes segundo o modelo constitucional do processo.

Feito este esclarecimento, classificar todas as buscas e apreensões como coerções lícitas é equivocado; vez ser possível, *exempli gratia*, a busca em local público sem coerção e a entrega espontânea da coisa a ser apreendida. Meios de prova também não são, por não serem produzidas em contraditório (frequentemente, com total surpresa) e só possibilitarem a obtenção do elemento de prova, não a produção do meio de prova (que tem procedimento específico, com normas, posições subjetivas e atos próprios). Não são, necessariamente, cautelares probatórias, já que existe a busca para citação ou intimação e a apreensão de pessoas (como as sequestradas, por exemplo). E, no Estado Democrático de Direito, também não são medidas instrumentais do instrumento do juiz. Com isso, percebe-se que não é possível classificar todas as buscas e todas as apreensões de maneira idêntica – mas é possível classificar a situação concreta de busca e apreensão de elementos de prova digitais (o que será muito importante para compreender seus requisitos).[117]

Lembra-se a premissa explicitada acima de que a busca e a apreensão são atos distintos.

A busca é a procura de pessoas, elementos de prova ou bens relacionados ao caso penal[118]. A busca de elementos de prova digitais tem a finalidade específica de descobrir os elementos necessários para a demonstração do delito ou para a defesa do acusado (CPP, artigo 240, § 1º, alínea *e*).[119] Se existir possibilidade de ofensa a direitos na realização da busca – como à privacidade e à inviolabilidade de domicílio (Constituição, art. 5º, X e XI) –, é

[116] Sobre o princípio da inocência, vide o item 4.3.1, *infra.*
[117] Tema do item 4.3, *infra.*
[118] Conceito exposto no início deste item. Sobre a noção de "caso penal", vide a nota n. 27, *supra.*
[119] A busca de elementos digitais também pode ter finalidade distinta, como encontrar vítimas, foragidos, instrumentos e produto de crimes (demarcadas nas demais alíneas do § 1º, do art. 240, do CPP); contudo, o objeto desta tese são, exclusivamente, os elementos de prova digitais, por isso, somente a busca deles é classificada.

necessária prévia autorização judicial em função da reserva de jurisdição (Constituição, art. 5º, XXXV), que deve ser precedida de contraditório; exceto se existir risco iminente, concreto e substancial à futura atuação das partes (CPP, art. 282, § 3º).[120] E a busca que não ofenda direitos não necessita de prévia autorização judicial.[121] Contudo, a prática demonstra a vulgarização (VALENTE, 2008, p. 181) na autorização judicial de buscas e apreensões, que não são autorizadas apenas excepcionalmente, mas que podem investigar qualquer delito e que quase nunca são precedidas de contraditório.[122] Esta situação de ausência de conhecimento e participação prévia do investigado na decisão pela busca é relevantíssima e é exatamente o que pode caracterizar a busca de elementos de prova digitais como meio oculto de investigação, ou seja, como método que visa a obtenção de elemento probatório por investigação operada sem o conhecimento do investigado (COSTA ANDRADE, 2009, p. 104) – o que implica em todos os problemas destacados no capítulo 2.

A situação concreta pode fazer com que a busca seja meio oculto de investigação e, simultaneamente, coerção lícita (como no ingresso forçado em domicílio, mediante autorização judicial, para procurar um dispositivo de armazenamento de elementos digitais); mas nem sempre o será (como a busca com o consentimento do investigado, que não é meio oculto e nem coerção). A busca de elementos de prova digitais também pode ser cautelar se existir risco iminente, concreto e substancial à futura atuação das partes (como na situação de risco concreto de destruição de um *hard drive* descoberto por agente infiltrado); todavia, também nem sempre o será, como a busca de registros de conexão armazenados por administrador de sistema autônomo, que deve ser guardado pelo administrador por ao menos um ano (Lei n. 12.965, de 2014, art. 13) e que não apresenta risco de destruição neste período.[123]

Portanto, somente a situação concreta permite classificar a busca de elementos de prova digitais – e, consequentemente, seus requisitos. Como a situação de consentimento do investigado (livre, expresso e informado, como defendido no item 4.4, *infra*) é praticamente inexistente e o contraditório prévio à decisão judicial que autoriza a busca quase nunca ocorre,

[120] A privacidade, a inviolabilidade de domicílio, a necessidade de autorização judicial, de mandado e os requisitos da busca serão tratados na sequência do capítulo.
[121] Vide o item 4.4, *infra.*
[122] Vide o item 2.6*, supra*, especialmente a nota n. 65.
[123] Conceitos demarcados no artigo 5º, incisos IV e VI, do Marco Civil da Internet: são registros de conexão "o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados"; é administrador de sistema autônomo "a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País" (BRASIL, 2022b).

a imensa maioria das buscas de elementos de prova digitais configura meio oculto de investigação.

Já a apreensão de elementos de prova digitais é medida[124] cautelar de obtenção de elemento de prova (CPP, artigo 240, § 1º, alínea *h*). Frente ao risco iminente, concreto e substancial de destruição do elemento de prova digital (de grande volatilidade e facilidade de adulteração) relacionado a um caso penal,[125] a apreensão retira os elementos digitais de quem os detém, assegura a confiabilidade, integridade e disponibilidade dos elementos digitais (pelo cumprimento dos atos da cadeia de custódia) e protege a futura atuação das partes.[126] Medida cautelar realizada frequentemente na fase investigativa, para que as partes – principalmente a acusação, que tem o ônus da prova (GIACOMOLLI, 2014, p. 95) –, obtenha elementos de prova que servirão à sequência da persecução penal, a apreensão é mais um ato que aumenta a importância do espaço cautelar e do inquérito.[127]

4.2 Regulamentação legislativa

A busca e apreensão de elementos de prova digitais é disciplinada principalmente no Código de Processo Penal, nos artigos 240 a 250 (quanto à busca e a apreensão) e artigos 158 a 184 (quanto à cadeia de custódia e às perícias). Somado a isso, institutos processuais relacionados são também previstos na Constituição de 1988, na Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica) e no Pacto Internacional dos Direitos Civis e Políticos (como será demonstrado na sequência do trabalho).

São também normas importantes na regulamentação da busca e da apreensão de elementos digitais: a Lei de Organizações Criminosas (Lei 12.850, de 2013), que disciplina o acesso a registros, dados cadastrais, documentos e informações sobre qualificação pessoal, filiação e endereço mantidos por empresas telefônicas e provedores de internet (artigos 15 e 17); o Marco Civil da Internet (Lei 12.965, de 2014); e a Convenção de Budapeste (Convenção sobre o Cibercrime), aprovada no Brasil pelo Decreto Legislativo n. 37, de 17 de dezembro de 2021.

[124] Endossa-se a teoria da cautelaridade de Flaviane Barros e Ulisses Dalle (2021, p. 96) que "[…] considera como incidente tudo aquilo que altere o curso normal, esperado e regirar do processo, abarcando (I) os incidentes propriamente ditos (incidente de falsidade e de insanidade mental); (II) as exceções processuais; (III) as cautelares reais; (IV) as provas cautelares, (V) as cautelares pessoais; (VI) e as prisões processuais, compreendidas como categoria distinta das cautelares - sejam elas probatórias ou reais - dadas as características que são próprias no curso do processo."
[125] Vide a nota n. 27, *supra.*
[126] A cadeia de custódia é aprofundada no item 5.1.1, *infra.*
[127] Vide o capítulo 2, *supra*.

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei 13.709, de 2018, não se aplica para fins de segurança pública ou atividades de investigação e repressão de infrações penais, por disposição expressa do artigo 4º, inciso III, alíneas *a* e *d*.[128]

4.2.1 Convenção de Budapeste

A internet é a reunião de camadas de protocolos que possibilita a transmissão de pacotes entre dispositivos de qualquer lugar do mundo.[129] Neste ambiente internacionalizado, a padronização do tratamento à busca e à apreensão de elementos de prova digitais promovida pela Convenção de Budapeste é muito importante e merece destaque.

Celebrada pelo Conselho da Europa em Budapeste, na Hungria, em 23 de novembro de 2001, a Convenção sobre o Cibercrime tem como partes dezenas de países do mundo, entre eles: Alemanha, Argentina, Austrália, Áustria, Bélgica, Canada, Chile, Colômbia, Croácia, Costa Rica, Dinamarca, Espanha, Estados Unidos, Estônia, Finlândia, França, Grécia, Holanda, Hungria, Inglaterra, Israel, Itália, Japão, Mônaco, Noruega, Panamá, Paraguai, Peru, Polônia, Portugal, República Checa, Romênia, Senegal, Suécia, Suíça, Turquia e Ucrânia. O Brasil foi convidado pelo Conselho da Europa a aderir à Convenção em dezembro de 2019 e aprovou sua adesão sem reservas pelo Decreto Legislativo n. 37, publicado no Diário Oficial da União em 17 de dezembro de 2021 (BRASIL, 2021c, p. 6).

A Convenção é organizada em quatro capítulos. O capítulo I trata da "Terminologia". O capítulo II das "Medidas a serem adotadas nas jurisdições nacionais"; ele é dividido em: seção 1 "Direito penal", seção 2 "Direito processual" e seção 3 "Jurisdição". O capítulo III trata da "Cooperação internacional" e é subdividido em: seção 1 "Princípios gerais" e seção 2

[128] Em *lege ferenda*, o Projeto de Lei da Câmara dos Deputados n. 8045/10 (que institui um Novo Código de Processo Penal), o Projeto de Lei da Câmara dos Deputados n. 4921/19 (proposto por Margarete Coelho) e o Projeto de Lei da Câmara dos Deputados n. 4939/20 (proposto por Hugo Leal) propõem alterações na regulamentação da busca e da apreensão de elementos digitais. Contudo, em função da possibilidade de emendas no processo legislativo, da diversidade das propostas e de como as reformas são tratadas no processo penal brasileiro – em que, por exemplo, a reforma aprovada pela Lei nº 13.964/2019 (que alterou diversos artigos do CPP, criou o juiz das garantias e excluiu o acervo investigativo das fases de instrução e julgamento) está suspensa "cautelarmente" há anos na ADI nº 6.298 –, este trabalho optou, metodologicamente, por pesquisar exclusivamente a *lege lata*.

[129] A arquitetura da internet, em resumo, tem quatro camadas. Uma física, composta pelos protocolos que interligam materialmente os dispositivos. Uma segunda, em que o protocolo IP estabelece as bases do tráfego na rede. Uma terceira, em que o protocolo TCP determina o fluxo dos pacotes. E uma quarta, a camada da aplicação que usa a internet – *e.g.*, nesta quarta em que é aplicado o protocolo *Hypertext Transfer Protocol* (HTTP), que possibilita publicar e ler documentos na *World Wide Web* (WWW) pela interação entre navegadores e servidores. A reunião das quatro camadas de protocolos é a internet (LESSIG, 2006, p. 144-145) (BEMERS-LEE; CAILLIAU, 2021).

"Disposições específicas". O capítulo IV trata das "Disposições finais" (BRASIL, 2021c, p. 7-37).[130]

David Silva Ramalho (2019, p. 69-70) defende que a Convenção contra o Cibercrime teve três objetivos principais: conceituar infrações comuns entre os Estados; construir procedimentos que possibilitem aos Estados a obtenção de elementos de prova digitais em seu território; e otimizar medidas de cooperação internacional para a facilitação da obtenção, conservação e comunicação rápida entre os Estados signatários, quanto aos elementos de prova digitais.

Pelo recorte temático desta pesquisa, a busca e a apreensão de elementos de prova digitais, foge à sua finalidade a crítica quanto à criminalização material proposta pela Convenção (capítulo II, seção 1); por isso, a tese terá como foco, em relação à Convenção de Budapeste, a busca e apreensão de elementos de prova digitais e a cooperação internacional necessária para essa obtenção. Por opção metodológica, em função da Convenção contra o Cibercrime não ser isolada do restante do sistema jurídico brasileiro, a pesquisa de suas disposições pertinentes à tese será feita na sequência, de maneira sistemática, em conjunto com as demais normas nacionais e internacionais vigentes.

4.3 Fundamento e requisitos

Para a realização válida da busca e da apreensão de elementos de prova digitais na atual situação legislativa do Brasil deve ser criticado seu fundamento e devem ser observados certos requisitos. Eles serão tema dos itens seguintes.

4.3.1 Fundamento cautelar

Como visto, a apreensão é medida cautelar, enquanto a busca não necessariamente. Contudo, para a melhor organização da tese, as modalidades de buscas não cautelares serão objeto dos itens 4.4, 4.5 e 4.11; neste ponto serão tratados os fundamentos das apreensões e das buscas que sejam cautelares.

Para tanto, cumpre revisitar e criticar os fundamentos clássicos das cautelares.

[130] A Convenção de Budapeste foi escrita originalmente em inglês e em francês (COUNCIL OF EUROPE, 2022a). Nesta tese optou-se por ter como referência a tradução oficial para o português utilizada pelo Senado Federal no Projeto de Decreto Legislativo n. 255, de 2021 (BRASIL, 2021c), por ter sido aquela que foi objeto da aprovação legislativa.

Primeiro, o *periculum in mora.* Ovídio Baptista da Silva explica que no direito germânico medieval a proteção contra um "estado perigoso" era feita pelo uso dos conceitos de *damnum irreparabile* e *periculum in mora*. Aquele, o dano irreparável, implicava numa situação específica, externa à demanda, concreta e ocasional de um risco de dano insanável de cuja proteção emergencial se fazia necessária para assegurar o direito, sem, ao mesmo tempo, satisfazer a pretensão. Já o perigo na demora não era específico a um caso individualizado, toda uma tipologia de casos, como os que exigiam alimentos, era protegida; a necessidade de proteção era interna à tipologia da demanda. Nesta última situação, o próprio tipo de causa exigia uma decisão rápida que não poderia esperar a ordinariedade do procedimento e implicava um procedimento mais simples e veloz. Como destaca Baptista da Silva, na situação de *periculum in mora* existia a antecipação da satisfação da pretensão (BAPTISTA DA SILVA, 2001, p. 13-15).

Os conceitos de *damnum irreparabile* e *periculum in mora* foram misturados no direito moderno. Calamandrei (2019, p. 180) classificou as cautelares em quatro grupos: procedimentos instrutórios antecipados; procedimentos dirigidos a assegurar a execução forçada; antecipação dos procedimentos decisórios; e execução provisória. Enquanto os dois primeiros não anteciparam os efeitos do procedimento principal, seja para conservar "a prova" ou para assegurar futura execução (semelhante ao *damnum irreparabile* do direito medieval), os dois últimos anteciparam a satisfação da pretensão (semelhante ao *periculum in mora* medieval). Sobre os dois últimos grupos, segundo o autor italiano, para afastar o perigo e assegurar a execução forçada: "o procedimento cautelar consiste mesmo em uma decisão antecipada e provisória do mérito, destinada a durar até que a esse regulamento provisório da relação controversa não se sobreponha o regulamento estável obtido através do mais lento processo ordinário" (CALAMANDREI, 2019, p. 185, tradução nossa[131]). Quanto à execução provisória, Calamandrei afirmou que na situação da execução provisória ter sido determinada pelo juiz com base no caso concreto, por entender que "segundo um cálculo de probabilidade, que as ulteriores fases do processo não modificarão as conclusões a que chegou o juiz de primeiro grau", a execução é cautelar; e a execução provisória estabelecida pela lei para toda uma tipologia de casos não seria cautelar, mas procedimento executivo (CALAMANDREI, 2019, p. 188-189, tradução nossa[132]).

[131] "il provvedimento cautelare consiste proprio in una decisiona anticipara e provvisoria del merito, destinata a durare fino a che a questo regolamento provvisorio del rapporto controverso non si sovrapporrà il regolamento stabilmente conseguibile attraverso il più lento processo ordinario."
[132] "secondo un calcolo di probabilità, che le ulteriori fase del processo non modigicheranno le concluisoni a cui è giunto il giudice di primo grado".

Ovídio Baptista da Silva (2001, p. 42-48, 55, 63) defende que essa associação entre as noções de *damnun irreparabile* e *periculum in mora*, misturando a satisfação da pretensão com a cautelaridade, sempre provisória, é a causa da linha turva entre o processo cautelar e o de execução; e da causa das divergências quanto à fundamentação da cautelar, que no direito medieval era configurada pela demora que a ordinariedade do procedimento causava nas situações de *periculum in mora* ou pelo risco concreto e insanável num caso específico nas situações de *damnum irreparabile*.

Calamandrei uniu noções muito distintas. Contudo, frente à ampla utilização da expressão *periculum in mora* no direito processual, seja para os casos que o direito medieval nomeava de *damnum irreparabile* ou para os que eram propriamente *periculum in mora*, não há sentido – *data venia* a Ovídio Baptista, que pensa diferente (BAPTISTA DA SILVA, 2001, p. 81) – em querer uma espécie de retorno à noção de *damnum irreparabile*. A literatura jurídica e a jurisprudência já consagraram de forma tal a expressão *periculum in mora* para tratar de medidas não satisfativas e relacionadas a uma situação concreta que o esforço para mudar toda tradição jurídica sobre o assunto seria infrutífero.

Nesta tese, cabe especificar a cautelaridade penal em acordo com o modelo constitucional do processo; ou seja, a partir da premissa de que as medidas cautelares visam assegurar a futura atuação das partes segundo as garantias processuais, principalmente o princípio do estado de inocência[133] (BARROS; DALLE, 2021).

O estado de inocência estabelece a liberdade como regra. Em primeiro lugar, ele implica o ônus probatório ser da acusação, é ela quem deve buscar demonstrar a autoria e materialidade do delito apto a alterar o *status quo* de liberdade do acusado; até eventual inexistência de uma tese arguida pela defesa deve ser demonstrada pela acusação; para a acusação, o ônus da prova é um dever, para o acusado uma faculdade; e, na dúvida, o julgamento deve ser favorável ao acusado (*in dubio pro reo*). Em segundo lugar, o estado de inocência implica no tratamento do investigado ou acusado de maneira digna e considerando-

[133] Sobre a nomenclatura do estado de inocência: em primeiro lugar, a expressão "presunção de não culpabilidade", segundo Gomes e Mazzuoli (2010, p. 105) "tem origem no fascismo italiano, que não se conformava com a ideia de que o acusado fosse, em princípio, inocente", e pode levar a equívocos interpretativos: *e.g.*, no conceito analítico de crime, em que ele é uma ação típica, ilícita e culpável (TOLEDO, 1982, p. 148-150), somente a não culpabilidade seria presumida? Existiria, então, presunção de tipicidade e ilicitude? Em segundo lugar, como observa Vinícius Thibau (2011, p. 99-100): "[…] a Presunção não se compatibiliza com as bases normativas do paradigma jurídico-constitucional do Estado Democrático de Direito, porque 'o convencimento antecipado da verdade provável a respeito de um fato desconhecido, obtida mediante fato conhecido e conexo' é adquirido sem que, para esse, concorram os destinatários, e, também, coautores da decisão expendida, mediante o exercício dos direitos de participação e de fiscalização incessantes, intersubjetivas e livres de coerção, que lhes são assegurados na Constitucionalidade Democrática". Por isso – e, também, pela situação de inocente do acusado poder ser alterada por sentença condenatória transitada em julgado – é preferida a expressão "estado de inocência" em lugar de "presunção de inocência"; como o faz Pacelli de Oliveira (2010, p. 49-50).

o inocente até eventual sentença penal condenatória transitada em julgado. Isso implica, *e.g.*, na vedação da exposição midiática do caso penal e do investigado ou acusado, na vedação do uso desnecessário de algemas, na irrelevância de registros policiais anteriores que não resultaram em condenação, na inadmissibilidade da identificação criminal ao civilmente identificado, no direito de recorrer em liberdade, na excepcionalidade da prisão preventiva; enfim, na concepção de que é o processo acusatório que cria o juízo, não elucubrações mentais inquisitórias (GIACOMOLLI, 2014, p. 94-100) (MORAES, 2010, p. 424-502).[134] Logo, é inadmissível a antecipação dos efeitos do processo de conhecimento ou de execução; a cautelaridade penal não tem, em qualquer situação, caráter satisfativo, ela somente visa assegurar a futura atuação das partes em acordo com o modelo constitucional do processo. Com isso, os terceiro e quarto grupos de cautelares classificados por Calamandrei (2019, p. 185-191) – a antecipação dos procedimentos decisórios e a execução provisória – não existem no sistema jurídico processual penal brasileiro pela sua manifesta inconstitucionalidade por ofensa ao princípio do estado de inocência (Constituição Federal, artigo 5º, inciso LVII).

Em relação ao tempo necessário para a construção ordinária do processo de conhecimento e de execução, cabem as observações de Ronaldo Brêtas (2018b, p. 212-213): para que o procedimento seja realizado com duração razoável, basta que os sujeitos processuais cumpram a Lei e os prazos legais. O juiz, especialmente, tem o dever de promover o impulso oficial e não pode deixar que existam "etapas mortas" de duradoura inatividade procedimental. A acusação, por sua vez, não deve fazer denúncias ineptas e sem justa causa (como de condutas insignificantes[135], que aumentam desnecessariamente o número de casos a serem julgados). E todos, inclusive os advogados de defesa, devem agir

[134] Segundo Cordero (1966, p. 168, tradução nossa: "Il modo più serio d'affrontare l'argomento consiste nel cominciare dalla nomenclarura. Gli aggettivi «inquisitorio» e «accusatorio» sono usati in almeno due significati: nel primo, sottolineano la differenza tra i procedimenti instaurati *ex officio* e quelli nei quali la decisione presuppone una domanda (donde il binomio «potere d'agire e potere di decidere»). Nel secondo, configurano due modi, che stanno agli antipodi, d'intendere ciò che avviene nel processo: l'inquisitore è un giudice al quale la legge accorda un credito illimitado, e ciò spiega perchè all'inquisito non sia permesso d'interloquire. Nei sistemi accusatori, al contrario, vale la regola del dialogo: ciò che si fa *in judicio*, si fa pubblicamente. Si potrebbero enumerare altri caratterri diferenziali ma questi sono i più interessanti."): "O modo mais sério de encarar o tema consiste em iniciar pela nomenclatura. Os adjetivos «inquisitório» e «acusatório» são usados em ao menos dois significados: no primeiro, sublinham a diferença entre os procedimentos instaurados *ex offcio* e aqueles nos quais a decisão pressupõe uma demanda (donde o binômio «poder de agir e poder de decidir»). No segundo, configuram dois modos, que são aí antípodas, de entender o que acontece no processo: o inquisidor é um juiz a quem a lei concede um crédito ilimitado, e isso explica porque ao inquirido não seja permitido discutir. Nos sistemas acusatórios, ao contrário, vale a regra do diálogo: o que se faz *in judicio*, se faz publicamente. Se podem enumerar outras características diferenciais mas essas são as mais interessantes."

[135] Como consta em pesquisa da Fundação Getúlio Vargas (2022, p. 109): "Não é compatível com as responsabilidades do STF nem do STJ ter de julgar casos que envolvam supostos furtos de tabletes de manteiga ou pacotes de biscoito." Acrescenta-se: não é responsabilidade de qualquer órgão do judiciário ter de julgar condutas insignificantes.

diligentemente, com lealdade e probidade. Assim, contra a demora da cognição ou execução, basta que os sujeitos processuais cumpram as determinações do sistema jurídico, principalmente os prazos legais; não é necessário subverter a teoria cautelar e o estado de inocência.

Finalmente, parte da literatura jurídica afirma que o *periculum in mora* deve ser substituído pelo *periculum libertatis*, com este último conceito significando o perigo concreto ao conhecimento ou à execução causado pela liberdade do investigado ou acusado "ao desenvolvimento do processo, à futura aplicação da lei penal ou se coloca em risco a ordem pública ou econômica, e não o risco de perecimento do direito em tese existente, diante da demora em se obter a prestação jurisdicional (*periculum in mora*)" (BANDEIRA, 2003, p. 53); nesta substituição, "O perigo não brota do lapso temporal entre o provimento cautelar e o definitivo. Não é o tempo que leva ao perecimento do objeto. O risco no processo penal decorre da situação de liberdade do sujeito passivo." (LOPES JR., 2012, p. 780). Contudo, – e apesar do esforço dos autores que defendem essa substituição, no sentido de criar conceitos próprios do processo penal – como pontuam Flaviane Barros e Ulisses Dalle (2021, p. 100-101), a substituição não rompe drasticamente com a cautelaridade pensada para o processo civil.

A noção de *periculum libertatis* como perigo concreto à cognição (pela destruição de provas) ou à execução (pela fuga do acusado) apenas ressalta a necessidade de risco concreto – que já existia na noção de Calamandrei de *periculum in mora* que misturou medidas não satisfativas e relacionadas a uma situação concreta (o *damnum irreparabile* medieval, existente nos grupos de "procedimentos instrutórios antecipados" e de "procedimentos dirigidos a assegurar a execução forçada" propostos por Calamandrei) com a decisão rápida que não poderia esperar a ordinariedade do procedimento e antecipa a satisfação da pretensão (o *periculum in mora* medieval, existente nos grupos "antecipação dos procedimentos decisórios" e "execução provisória" propostos por Calamandrei). Sendo que o perigo que a liberdade do acusado pode causar não tem como ser fundamento geral das medidas cautelares, pois não explica as situações em que a medida cautelar é requerida pelo próprio investigado ou acusado, como nas medidas cautelares probatórias, ou as cautelares reais.[136]

[136] Até Aury Lopes Jr. (2012, p. 907) afirma que: "Contudo, nas medidas cautelares reais, por sua estreita vinculação com o interesse patrimonial a ser satisfeito na esfera cível, em sede de ação de indenização, por exemplo, a adoção dos conceitos *fumus boni iuris* e *periculum in mora* não constitui a mesma inadequação. Inclusive, em relação ao *periculum in mora*, é ele ainda mais evidente, na medida em que o perigo não decorre do 'estar em liberdade o agente', senão das possibilidades de deterioração dos bens móveis ou imóveis, alienações fraudulentas etc."

Sobre o *fumus boni iuris*: para Calamandrei (2019, p. 201-202), o *fumus boni iuris* é um juízo de probabilidade e de verossimilhança, mais precisamente, a probabilidade hipotética de julgamento favorável. Essa noção também é absolutamente incompatível com o processo penal. Não existe juízo antecipatório de julgamento favorável no sistema processual penal regido pelo estado de inocência (como explicado acima). No processo penal, não existe antecipação do juízo de culpa; e não é plausível qualquer direito que ofenda a garantia constitucional do estado de inocência.

Portanto, a sumariedade da cognição cautelar não se traduz na probabilidade hipotética de julgamento favorável (noção elaborada para o processo civil por Calamandrei). A mesma corrente da literatura jurídica citada acima defende a substituição do *fumus boni iuris* pelo *fumus commissi delicti*, com este consistindo "na constatação da materialidade delitiva e na verificação de indícios de autoria" (BANDEIRA, 2003, p. 44); "enquanto probabilidade da ocorrência de um delito" (LOPES JR., 2012, p. 779).

Ocorre que, como argumentam Flaviane Barros e Ulisses Dalle (2021, p. 101), ainda que as medidas cautelares sejam provisórias, o *fumus commissi delicti* "assume ares de antecipação do mérito e a decisão de mérito apenas dá continuidade ao que já fora decidido cautelarmente". Assim, apesar do foco em temas próprios do processo penal, como a autoria e a materialidade, a substituição continua antecipando um juízo que só poderia existir no provimento final do processo de cognição. O entendimento de que os indícios de autoria e materialidade indicam a probabilidade da ocorrência de um delito também antecipa o mérito – repete-se, ainda que provisoriamente.

Barros e Dalle (2021) abandonam as expressões latinas *periculum in mora*, *fumus boni iuris*, *periculum libertatis* e *fumus commissi delicti* – que são instrumentais à "eficaz aplicação do poder de penar" (LOPES JR., 2012, p. 778-779) – para conceituar que as medidas cautelares protegem a futura atuação das partes, segundo o modelo constitucional do processo, contra o risco concreto, iminente e substancial à participação na instrução criminal (pela destruição de elementos de prova) ou na execução penal (pelo risco de fuga).[137] Vez que no caso penal "[…] estamos diante de uma situação de incerteza, de dúvida, quanto à aplicação da sanção penal a agente que, com sua conduta, incidiu no tipo penal" e que "Em não sendo auto-executável a sanção, não há outro caminho que o processo para fazer o acertamento do caso penal" (MIRANDA COUTINHO, 1989, p. 135); e considerando a fragilidade epistêmica dos elementos informativos obtidos unilateralmente pela acusação na

[137] "Afastam-se, assim, hipóteses de justificação da prisão preventiva mediante termos abertos e repletos de sentidos morais, como 'ordem pública'." (BARROS; DALLE, 2021, p. 104).

fase investigativa sem contraditório prévio (em regra) – e sem fiscalização efetiva, portanto –, os indícios concretos de autoria e materialidade sobre o caso penal exigidos pela lei para as medidas cautelares (CPP, art. 312) não podem resultar em qualquer antecipação do julgamento de mérito; no que é indispensável a separação do juiz que atuou na fase investigativa e decidiu sobre as medidas cautelares do das fases de instrução e de julgamento do processo de cognição, o que prejudicaria a imparcialidade (BARROS; DALLE, 2021, p. 104).[138]

Portanto, a sumariedade da cognição cautelar não é a probabilidade da ocorrência do delito segundo indícios de autoria e materialidade obtidos num espaço reduzido de argumentação; mas a cognição sobre a situação excepcional de risco concreto, iminente e substancial à futura atuação das partes na persecução penal demonstrada por elementos de informação que, por serem obtidos sem contraditório prévio, implicam em baixa "credibilidade epistêmica" e em juízo provisório (BARROS; DALLE, 2021, p. 103). A cognição cautelar é sumária não pelo espaço reduzido de argumentação, mas pela restrição da cognição à situação fática excepcional. Ou seja, em função do modelo constitucional do processo regente da cautelaridade – principalmente do contraditório, da ampla defesa e do estado de inocência – a cognição cautelar "há de ser ampla, profunda, exaustiva e cuidadosa, mas limitada à situação fática excepcional" (BARROS; DALLE, 2021, p. 103).

Feita esta releitura crítica da cautelaridade em acordo com o modelo constitucional do processo, o trabalho aprofundará nos requisitos específicos da busca e da apreensão.

4.3.2 Requisitos específicos

O primeiro requisito é a fundamentação[139] qualificada concreta (Constituição, artigo 93, inciso IX). Como ato de explicitação da racionalidade da decisão que demonstra se a lei estabelecida pelo legislativo democrático foi premissa da decisão e se a decisão é resultado da

[138] Pois: "Após ter gasto tempo e recursos na análise do caso em sede liminar, de modo a avaliar a existência de requisitos autorizadores da concessão de medidas de urgência ou tutelas de evidência, o juiz deverá revisitar, quando da prolação da sentença, a decisão proferida anteriormente. E o viés de trancamento, associado ao viés de confirmação, exercerá coerção cognitiva de modo a favorecer uma confirmação da decisão liminar concedida." (NUNES; LUD; PEDRON, 2018, p. 97). Sendo que o viés de trancamento "[…] faz com que o julgador, ao revisitar uma decisão anterior (uma decisão liminar, por exemplo), a ela se vincule pelo fato de nela ter investido anteriormente tempo e pesquisa." (NUNES; LUD; PEDRON, 2018, p. 91) e o viés de confirmação "[…] pode ser caracterizado como sendo a tendência do observador de procurar ou interpretar informações de forma que estas confirmem preconcepções próprias." (NUNES; LUD; PEDRON, 2018, p. 80).

[139] "Evidente que motivação não é o mesmo que fundamentação. Admitir que motivação seja igual ou possa substituir o conceito de fundamentação possibilita que o juiz primeiro decida e, depois, apenas motive aquilo que já escolheu. Isto seria a morte da Teoria do Direito e do Direito Processual, porque a decisão ficaria refém da (boa ou má) vontade (de poder) do julgador." (STRECK, 2018, p. 13).

argumentação das partes em contraditório (BARROS, 2009, p. 19), a decisão que autoriza a busca e a apreensão de elementos de prova digitais deve ser qualificada por razões expressadas por atores que dominam o conteúdo conceitual jurídico e o tecnológico (sem o domínio das noções de tecnologia envolvidas, o julgador não conseguirá, por exemplo, analisar se a medida é adequada, necessária ou a menos gravosa possível no caso concreto, e as partes não conseguirão fiscalizar a regularidade da decisão). Além da fundamentação dever ser qualificada pelo domínio de noções da tecnologia, ela deve basear-se na situação fática. O Código de Processo Penal (artigo 240, § 1º) e a Convenção de Budapeste (artigo 19.2) exigem fundadas razões para a admissibilidade da busca e da apreensão; que são razões baseadas em elementos concretos sobre a necessidade e a adequação da busca e da apreensão para descobrir e obter o elemento de prova relacionado ao caso penal – e não abstrações violadoras do estado de inocência do investigado. Portanto, e em aplicação subsidiária no processo penal do artigo 489, do Código de Processo Civil:

> "[…] § 1º Não se considera fundamentada qualquer decisão judicial, seja ela interlocutória, sentença ou acórdão, que: I – se limitar à indicação, à reprodução ou à paráfrase de ato normativo, sem explicar sua relação com a causa ou a questão decidida; II – empregar conceitos jurídicos indeterminados, sem explicar o motivo concreto de sua incidência no caso; III – invocar motivos que se prestariam a justificar qualquer outra decisão; IV – não enfrentar todos os argumentos deduzidos no processo capazes de, em tese, infirmar a conclusão adotada pelo julgador; V – se limitar a invocar precedente ou enunciado de súmula, sem identificar seus fundamentos determinantes nem demonstrar que o caso sob julgamento se ajusta àqueles fundamentos; VI – deixar de seguir enunciado de súmula, jurisprudência ou precedente invocado pela parte, sem demonstrar a existência de distinção no caso em julgamento ou a superação do entendimento." (BRASIL, 2022c).

Pelo potencial de lesão ou ameaça aos direitos fundamentais na realização da busca e da apreensão de elementos de prova digitais, a atuação prévia da jurisdição é inafastável (Constituição, artigo 5º, inciso XXXV[140]). Como visto (item 2.3, *supra*), na sociedade de controle há um aumento do espaço da polícia, quem predominantemente realiza as medidas ocultas, primeiro detecta informações sensíveis e ocupa posição central na reunião de informações da rede de vigilância. Isso não pode levar à "subalternização da autoridade judiciária na investigação", como anota Anabela Miranda Rodrigues (2012, p. 1010). Como também destaca Manuel da Costa Andrade, com base em Brüning, a reserva da jurisdição não pode ser transformada num "tigre sem dentes", e, contra isso, o julgador deve criticar de maneira autônoma a narrativa da acusação quanto à sua plausibilidade e pertinência, sem cópia acrítica das razões do requerimento do Ministério Público e indeferindo medidas que

[140] "a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito" (BRASIL, 2020a).

não atendam a todos os requisitos legais e atuando preventivamente na proteção dos direitos fundamentais (COSTA ANDRADE, 2009, p. 118-119; 2011, p. 547).[141] Somado a isso, a fundamentação também deve ser bastante, ou seja, suficiente quanto ao preenchimento dos requisitos legais e explícita quanto ao porquê da proporcionalidade e relevância da busca e da apreensão na situação fática, com base nos elementos concretos existentes antes do ato decisório (o aparecimento futuro de elemento concreto não tem o potencial de sanar o vício de decisão anterior desprovida de fundamento) (COSTA ANDRADE, 2009, p. 114, 118).[142]

Em função do estado de inocência como princípio orientador da cautelaridade (BARROS; MACHADO, 2011, p. 28-34) e da ilegalidade da pescaria probatória (*fishing expedition*), a fundamentação da busca e da apreensão de elementos de prova digitais deve ser relacionada a fatos pretéritos, não pode ser prospectiva (apesar da pressão da sociedade de controle pela vigilância preventiva generalizada e ininterrupta).[143]

A fundamentação deve explicitar a relevância da busca e da apreensão para a futura atuação da parte; o segundo requisito. Na lição de Cordero (1963, p. 19), a distinção entre a relevância e a irrelevância é resultado do confronto de dois juízos hipotéticos: um em que a medida é produzida e outro em que não; se os juízos são coincidentes há irrelevância, se são divergentes, há relevância.

A fundamentação também deve demarcar a finalidade, as modalidades e o alcance da tarefa dos agentes; o terceiro requisito. A decisão que autorize a busca e a apreensão deve especificar a relevância, a adequação, a necessidade e a imprescindibilidade da procura e obtenção dos elementos de prova digitais no caso concreto.

As modalidades de busca e de apreensão também devem ser especificadas. As modalidades de busca permitidas pela legislação serão objeto do item 4.11 (*infra*), desde já, o que deve ser esclarecido é que a busca e a apreensão de elementos de prova digitais no

[141] "A defesa da desjudicialização do inquérito – onde a investigação criminal detém seu maior fulgor – não se afigura quer constitucionalmente quer em termos de política criminal o caminho possível. Só um Estado de direito erigido, na prevenção da liberdade e da segurança, segundo políticas securitárias […] pode admitir a desjudicialização da obtenção da prova, policializando de todo em todo um processo e inutilizando o juiz das liberdades e nihilificando o MP." (VALENTE, 2008, p. 173). Pelas mesmas razões, o Superior Tribunal de Justiça decidiu, no julgamento do Recurso em Habeas Corpus n. 51.531/RO: "Ilícita é a devassa de dados, bem como das conversas de *whatsapp*, obtidas diretamente pela polícia em celular apreendido no flagrante, sem prévia autorização judicial." (BRASIL, 2022c).

[142] Pedro Marques (2019, p. 239-240) sustenta que "[…] o juízo de admissibilidade de uma busca requerida exige do magistrado um raciocínio que vai muito além de uma operação de subsunção, impondo igualmente a valoração de elementos de informação até então colhidos que revelem conteúdo robusto o suficiente para que se mostrem configurados os *standards* probatórios das 'fundadas razões' ou 'fundadas suspeitas' exigidas pela legislação processual penal, a depender da modalidade de busca."

[143] Vide o item 2.2, *supra.*

sistema jurídico atual são dirigidas para a apreensão material do dispositivo que armazena os elementos digitais.[144]

Pelo seu potencial de ofender direitos fundamentais e pela reserva da jurisdição, a decisão que autoriza a busca e a apreensão de elementos digitais é limite rígido sobre o alcance da tarefa dos agentes. Se a decisão não autorizar o ingresso em domicílio, não é lícita a coerção relacionada a esse ingresso. Igualmente, o objeto da busca e da apreensão é o especificado na decisão, e nenhum outro; o morador, inclusive, deve ser intimado a entregar o dispositivo de armazenamento de dados (CPP, art. 245, § 5º) – sendo que tem direito contra a autoincriminação, mas pode optar por voluntariamente entregá-lo para mitigar os efeitos da busca e da apreensão. O local especificado e o nome do proprietário ou morador do local também são limites: a decisão não é "carta em branco" e nem autoriza burla aos requisitos legais.[145] Os limites estabelecidos na decisão, inclusive quanto à finalidade, além de orientar os atos da busca e da apreensão, desestimulam a vulgarização em sua utilização e a pescaria probatória (*fishing expedition*).[146]

A fundamentação exige indicação do local onde será realizada a busca e a apreensão dos elementos de prova digitais; o quarto requisito. Esse lugar é o endereço físico do lugar em que se suspeita, por elementos concretos, que está o dispositivo material de armazenamento dos elementos de prova digitais.[147]

Também decorrente da fundamentação, o proprietário ou morador do local onde será realizada a busca e a eventual apreensão domiciliar deve ser identificado (CPP, artigos 243, inciso I, e 245, *caput* e § 4º); o quinto requisito. O proprietário ou morador do local tem o direito de acesso ao mandado judicial, que deve indicar seu nome, e de assistir aos atos da busca e da apreensão. Esse requisito é importantíssimo para viabilizar a fiscalização da regularidade dos atos de busca e de apreensão e exercício da ampla defesa.

[144] A interceptação do fluxo de comunicações em sistemas de informática e telemática é possível, nos termos da Lei n. 9.296, de 1996; todavia, ela tem requisitos próprios e não faz parte do recorte da tese. Sobre o assunto, vide: Sidi (2016).

[145] No mesmo raciocínio, sobre o agente "encoberto", diz Manuel da Costa Andrade: "Por exemplo, autorizando a lei portuguesa nos termos em que o faz, as *ações encobertas*, quem a levar a cabo não pode, só por isso, e no contexto da acção, proceder a escutas, *gravações fonográficas ou fotográficas não consentidas*, formas de devassa que a lei não inscreveu no pertinente âmbito de legitimação. Como não pode entras arbitrariamente no *domicílio* de um suspeito ou perseguido, já que a figura não está contida no regime da figura. Isso diferentemente do que ocorre na Alemanha em que o § 110 c) StPO autoriza o 'agente encoberto' a entrar no domicílio da pessoa suspeita, utilizando sua identidade falsa (*Legende*). De igual modo, se um qualquer dispositivo legal legitimar a recolha de dados associados à comunicação (efectivamente) realizada por telemóvel, tal não legitima, só por si, a recolha de dados na posição de *stand-by*. Como não autoriza o recurso às técnicas de *IMSI-catcher* ou de *SMS-Blaster*." (COSTA ANDRADE, 2011, p. 543).

[146] Tratada especificamente no item 4.7, *infra.*

[147] Este ponto será aprofundado nos itens 4.10 e em seus subitens, *infra*.

A fundamentação garante que a legalidade orientou a decisão (ANDOLINA; VIGNERA, 1997, p. 200). Sexto requisito, a legalidade é a precedência da lei ao fato. Nos termos da Constituição de 1988, artigo 5º, inciso II: "ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei" (BRASIL, 2020a); com a lei, aqui, significando a integralidade do sistema jurídico (BRÊTAS, 2018b, 165-171).[148] Toda questão jurídica tem, por óbvio, a lei como requisito – sem ela não seria jurídica! seria ética, religiosa *etc*. Assim, toda questão jurídica tem como pressuposto o Direito, que demarca o limite jurídico entre o devido e o indevido (CORDERO, 1985, p. 484; 1967, p. 33).

Como a Constituição assegura a todos legalidade, privacidade, inviolabilidade do domicílio, devido processo legal, contraditório, ampla defesa, proibição de provas ilícitas e estado de inocência (Constituição, art. 5º, II, X, XI, LIV, LV, LVI e LVII), somente com expressa disposição constitucional ou lei ordinária fundamentada na Constituição, essas garantias podem ser limitadas.[149]

O fundamento constitucional que ampara a limitação a essas garantias na realização dos meios ocultos e das cautelares probatórias é a segurança (Constituição, art. 5º, *caput*) nas acepções de estabilidade, previsibilidade e ausência de perigos.[150]

A busca e a apreensão de elementos digitais podem ofender às garantias acima descritas. Portanto, somente com lei expressa anterior à busca e à apreensão de elementos digitais, esses atos podem ser realizados validamente.[151] E, como pontua Manuel da Costa Andrade (2009, p. 112-113): "a lei deve permitir identificar com rigor e segurança tanto o bem jurídico ou o direito fundamental lesado ou atingido como o teor do respectivo sacrifício", com precisão, clareza, fundamentação, demarcação da finalidade e limites.

Frente à inexistência de lei que autorize a busca por ingresso remoto, essa espécie de busca é inadmissível no direito brasileiro; no sistema jurídico atual, somente são válidas a busca e a apreensão física do dispositivo que armazena os elementos digitais – e nos limites da Lei. A Convenção de Budapeste (artigo 19) recomenda que os Estados signatários editem

[148] Sobre outras conjecturas relacionadas à legalidade, vide: Rosa Maria Cardoso da Cunha (1979).

[149] Na lição de Gilmar Ferreira Mendes e Paulo Gustavo Gonet Branco (2015, p. 200), amparados na literatura jurídica alemã: "Os direitos fundamentais enquanto direitos de hierarquia constitucional somente podem ser limitados por expressa disposição constitucional (*restrição imediata*) ou mediante lei ordinária promulgada com fundamento na própria Constituição (*restrição mediata*)."

[150] Cláudio de Souza Neto (2013, p. 231-232) conceitua que a segurança tem três acepções distintas: a) estabilidade, ligada ao direito adquirido, ao ato jurídico perfeito e à coisa julgada; b) previsibilidade, vinculada à legalidade, expressa na possibilidade de expectativa quanto às consequências jurídicas dos atos; e c) ausência de perigos, que é traduzida na incolumidade das pessoas e do patrimônio pela vigilância e repressão aos delitos. Esta terceira acepção é a que autoriza a restrição de direitos fundamentais na realização dos meios ocultos de investigação; mas a segurança, simultaneamente, assegura a estabilidade e a previsibilidade (primeira e segunda acepções), portanto, a legalidade é regente da realização da vigilância e repressão aos delitos.

[151] "As intervenções não previstas em lei são intervenções em que nós, cidadãos, não consentimos, de forma que o Estado carece de uma autorização para as impor." (GRECO, Luís, 2018, p. 38).

leis que possibilitem a busca por ingresso remoto. Contudo, a disposição da Convenção de Budapeste é apenas uma recomendação e a edição de novas medidas legislativas e a validade da busca por ingresso remoto no Brasil depende de lei futura. Isso é percebido, inclusive, pelo tempo verbal da redação da Convenção de Budapeste, "Cada parte adotará medidas legislativas e outras providências necessárias", repetida nos artigos 16, 17, 18 e 19 (BRASIL, 2021c, p. 17-19).[152] O artigo 22, inciso I, da Constituição de 1988, determina a competência privativa da União para legislar sobre direito penal e processual do Brasil. Portanto, apenas após nova lei de iniciativa da União poderá ser válida a busca por ingresso remoto. Qualquer outra interpretação é inconstitucional, por ofensa à legalidade e ao devido processo legislativo.[153]

O sétimo requisito é a proporcionalidade (princípio constitucional[154]; Código de Processo Penal, artigo 282; Convenção de Budapeste, artigo 15.1). A proporcionalidade proíbe o excesso (BARROS; MACHADO, 2011, p. 38) na realização da busca e da apreensão de elementos de prova digitais. Esse requisito implica a adequação da busca e da apreensão para alcançar as finalidades de procurar e obter os elementos de prova digitais. E na necessidade, ou seja, na situação concreta da busca e da apreensão de elementos de prova digitais ser medida necessária e exigível por ser a mais eficiente e menos gravosa aos direitos fundamentais para o cumprimento das finalidades descritas; o que tem como consequências: a preferência por qualquer outro meio menos gravoso aos direitos fundamentais; e no dever de demonstração concreta pelo requerente de que a obtenção dos elementos digitais é imprescindível e que não é possível por outro meio o conhecimento que a busca e a apreensão dos elementos de prova digitais viabilizaria. A proporcionalidade também tem uma conotação *stricto sensu*, que é a relação entre a gravidade da medida com as suas finalidades, para que o

[152] Este tema foi objeto de debate em situação semelhante envolvendo a Convenção de Palermo (Convenção das Nações Unidas contra o Crime Organizado Transnacional). Essa Convenção recomendou a criminalização de condutas cometidas por organizações criminosas. Todavia, não apresentou redação que cumprisse a taxatividade da legalidade penal, não demarcou as penas e utilizou a mesma expressão da Convenção de Budapeste, "Cada Estado Parte adotará" (artigo 6.1) (BRASIL, 2022e). O Supremo Tribunal Federal foi provocado a se manifestar sobre se a Convenção de Palermo tinha criado novos tipos penais – especificamente se tinha criminalizado a lavagem de dinheiro cometida por organização criminosa – ou não. No julgamento do Habeas Corpus 96.007/SP, de relatoria do ministro Marco Aurélio, o tribunal declarou, em decisão unânime, que a Convenção de Palermo não criou o tipo penal das organizações criminosas e que era necessária nova lei, de acordo com o processo legislativo nacional, para a criminalização recomendada pela Convenção.

[153] Sobre o devido processo legislativo, vide: Cattoni de Oliveira (2016, p. 189-217) e Del Negri (2008).

[154] Gilmar Mendes e Paulo Gonet Branco (2015, p. 218-225) explicam que parte da literatura jurídica alemã fundamenta a proporcionalidade nos direitos fundamentais, o que tem efeitos na relação do cidadão com o Estado. Parte a fundamenta no Estado Direito, sendo regente da relação do cidadão com o Estado e das funções do Estado entre si. E outra parte a fundamenta na própria noção geral de Direito. Os autores também explicam que, no Brasil, o fundamento da proporcionalidade é a proibição do excesso, os direitos fundamentais e o devido processo legal, que impedem a irrazoabilidade e a arbitrariedade ao limitar a atuação pública pela adequação, necessidade e proporcionalidade *stricto sensu*.

remédio não seja pior que a doença e nem se "mate moscas com disparos de canhão" (NÚÑEZ, 2016, p. 70, tradução nossa[155]). Somado a isso, a proporcionalidade limita a atuação do legislador para somente autorizar medida tão invasiva para os casos penais graves (VALENTE, 2009, p. 144-145; 2008, p. 61-65).[156]

O oitavo requisito, a subsidiariedade, deriva da proporcionalidade. Ele tem como conteúdo a relação das medidas entre si. Num contexto de registros imensos sobre a vida das pessoas em elementos digitais, a busca e a apreensão desses elementos divulgam aspectos da vida íntima que frequentemente em nada dizem respeito à persecução penal. A ofensa à privacidade e à própria dignidade das pessoas é muito intensa nas buscas e apreensões de elementos de prova digitais, por isso, é intolerável a sua vulgarização. Portanto, em primeiro lugar, novamente com Costa Andrade (2009, p. 115), não deve ser utilizado qualquer meio oculto (como a busca) se é possível utilizar o "descoberto"; entre dois meios que proporcionem o mesmo conhecimento sobre o caso penal, é preferível o menos gravoso aos direitos fundamentais; e deve ser evitada ao máximo a cumulação entre dois ou mais meios ocultos, como agente infiltrado e busca de elementos de prova digitais.

O nono requisito é a legitimidade da requisição. Na lição de Aroldo Plínio Gonçalves (1992, p. 146-152), as partes são as destinatárias do provimento e não há um legitimado ativo que ajuíza a ação contra um legitimado passivo que a responde, ambas as partes são ativas na construção do procedimento; sendo que a individualização das partes é hipotética, pela expectativa de que o provimento final provoque algum efeito nelas, ou seja "com base na hipótese de que, ao final, aquele ato seja emanado e os envolva" (FAZZALARI, 1996, p. 85, tradução nossa[157]). O uso do vocábulo "réu" também é inadequado: sua proveniência é de *reus*, em latim, que deriva de *res*, que significa coisa (MOMMSEN, 1905, p. 200). Quem responde à ação penal não é coisa, mas sujeito de direitos.

O artigo 242 do Código de Processo Penal determina que as partes podem requerer a busca. As partes são o Ministério Público (ou o querelante, se a ação for de iniciativa privada),

[155] "matar moscas a cañonazos".
[156] Por exemplo, a Convenção de Budapeste determina (artigo 21º) que apenas num catálogo restrito de infrações graves deve ser admitida a "interceptação de dados de conteúdo", que é a obtenção ou gravação, em tempo real, do conteúdo de comunicações transmitidas por "sistema de computador".
[157] "in base alla ipotesi che, alla fine, quell'atto venga emanato e li coinvolga".

a vítima[158] e o investigado ou acusado, que são os que podem ser envolvidos pelos efeitos do provimento final.[159]

No processo penal acusatório brasileiro, o Ministério Público é o titular do exercício da ação penal pública, com independência funcional (Constituição, arts. 127, § 1º e 129, I). Esse é o sujeito processual responsável pelo ato de arquivamento ou ajuizamento da ação penal. Na separação das funções entre os sujeitos do processo, é o Ministério Público quem tem o dever de iniciar a ação penal, se presentes os requisitos, e demarcar seu objeto. Na fase de investigação, a acusatoriedade também é a regente[160] e as críticas feitas por Geraldo Prado à possibilidade da polícia judiciária poder requerer cautelar pessoal mesmo sem ser parte no processo penal também cabem às cautelares probatórias:

> Com efeito, a autoridade policial não é parte no processo penal, não tem interesse que possa deduzir em juízo e a investigação criminal não guarda autonomia, ela existe orientada ao exercício futuro da ação penal. A constatação de comportamentos do indiciado prejudiciais à investigação deve ser compartilhada entre a autoridade policial e o Ministério Público (ou o querelante, conforme o caso), para que o autor da ação penal ajuíze seu real interesse em ver a prisão decretada. Vale dizer que em um País de tradição autoritária, no qual durante décadas a polícia foi concebida como braço armado do arbítrio, a gestão de uma polícia democrática requisita a articulação da Polícia com o Ministério Público, dividindo as preocupações quanto ao sucesso da própria investigação. A autonomia da polícia, preservado no artigo 311 do Código de Processo Penal pela via da "representação" pela prisão preventiva, contradiz a própria noção de devido processo legal, pois que a elege, indevidamente, órgão acusador, ainda que sem o poder de iniciativa para o processo. Também neste ponto a norma é inconstitucional. (PRADO, Geraldo, 2011, p. 131).

Ora, a polícia não tem legitimidade para a ação penal, seja ela de conhecimento, execução ou cautelar, por não ser a titular do interesse; por determinação constitucional (Constituição, artigo 129, inciso I) e por respeito à acusatoriedade. A função da polícia judiciária é apurar a autoria e materialidade dos supostos delitos de que tenha tido notícia (Constituição, artigo 144, §§ 1º e 4º). Portanto, cabe a cada função seu espaço

[158] "[…] a vítima possui direitos fundamentais no processo penal, definidos a partir do texto constitucional, quais sejam: direito à reparação do dano e direitos de participação contraditória no processo penal de iniciativa pública, decorrente de sua posição como participante do fato delituoso, que será reconstruído para garantia do devido processo penal, em virtude de sua posição de sujeito de direitos, que será afetado pelo provimento emanado no processo penal de conhecimento. Portanto, a ela devem ser garantidas, em virtude das características do modelo constitucional do processo, direitos, faculdades, deveres e ônus adequados à sua posição de parte contraditora, já que o contraditório, elementos definidor do processo, deve ser compreendido como a posição de simétrica paridade daqueles que são afetados pelo provimento jurisdicional." (BARROS, 2008a, p. 201).

[159] "O Código de Processo Penal, em seu artigo 242 nos traz a possibilidade de requerer, por intermédio do advogado do ofendido, a expedição de mandado de busca e apreensão. Trata-se de possibilidade pouco explorada pela advocacia, com larga aplicação e potencial inestimável para a investigação defensiva." (DIAS, 2019, p. 125-126).

[160] "ainda na fase pré-processual é possível vislumbrar o princípio da acusatoriedade, o qual aparecerá sempre que, de algum modo, o titular da ação penal atuar com vista à aquisição de elementos de formação da convicção judicial, mesmo que superficial, voltada ao recebimento da denúncia ou queixa." (PRADO, Geraldo, 1999, p. 124).

constitucionalmente demarcado. Com isso, sempre que a busca ou a apreensão possa ofender direito fundamental (como a inviolabilidade de domicílio) e necessitar de autorização judicial, somente o Ministério Público terá legitimidade para, pelo Estado, requerer medida cautelar; a polícia judiciária pode representar pela busca e pela apreensão, mas, sem a expressa concordância do Ministério Público – o titular do interesse (inclusive do cautelar) –, a medida é carente de legitimidade e ofende à acusatoriedade constitucional. Neste caso, a busca e a apreensão devem ser indeferidas pelo juízo.

Finalmente em relação a este requisito, cabe ressaltar que inexiste poder geral de cautela no processo penal. Como demonstrado acima (item 4.3.1), o fundamento da cautelar não é a segurança vigilante do judiciário (concepção publicista, socializadora), mas a proteção da futura atuação das partes. Somado a isso: em primeiro lugar, o judiciário não pode invadir o espaço da acusação, deixar de ser imparcial e atuar como inquisidor; em segundo lugar, não há "poder geral" e irrestrito no processo penal, todas as atuações de todos os sujeitos do processo encontram limites na legalidade (inclusive os limites de legitimidade) (ROSA, 2020, p. 422-423) (LOPES JR., 2012, p. 781-783). Assim, o judiciário não é vigilante no processo penal cautelar (e nem no de conhecimento e no de execução) e somente pode sair da inércia se provocado pelo titular do interesse. Por isso, a iniciativa das cautelares cabe somente às partes. Assim, obviamente, o juiz não pode determinar, de ofício, a busca e a apreensão de elementos de prova digitais.

Décimo requisito: juízo natural.[161] O juízo natural é garantia que determina que o órgão julgador deve ter sua competência determinada por lei, em momento anterior ao fato e que são proibidos tribunais de exceção (os tribunais de exceção são os criados arbitrariamente, sem lei ou após o fato, para perseguir grupos ou pessoas determinadas, de maneira contrária ao modelo constitucional do processo) (Constituição, artigo 5º, incisos XXXVII e LIII) (FIGUEIREDO DIAS, 1974, p. 321-325) (BRÊTAS, 2018b, p. 158-160) (BARROSO, 2001, p. 47). Como ressaltam Andolina e Vignera (1997, p. 22, 40-47), o juízo natural é indissociável da imparcialidade; a determinação do juízo competente em momento anterior ao fato evita manipulações que comprometam a equidistância do juiz em relação às partes.[162]

[161] Aroldo Plínio Gonçalves (1992, p. 180) explica que (ao menos desde o Congresso Internacional de Direito Processual de Gand, na Bélgica, em 1977) a decisão jurídica não é mais entendida como reservada ao juiz, mas à jurisdição. Por isso, a expressão mais técnica é "juízo natural" e não "juiz natural", como está, inclusive, na Constituição (artigo 5º, XXXVII): "não haverá juízo ou tribunal de exceção" (BRASIL, 2020a).

[162] No modelo constitucional do processo, a imparcialidade implica na ausência de interesses pessoais do juiz na causa (vínculo subjetivo); na situação do juiz ser um terceiro estranho ao objeto do processo (vínculo objetivo); e na inexistência de decisão anterior do juiz quanto à mesma causa, seja em outro grau ou fase do procedimento (vínculo psicológico) (ANDOLINA; VIGNERA, 1997, p. 40-47). Sobre o tema, vide pesquisa anterior: Pimenta

A competência para a decisão sobre a busca e a apreensão de elementos de prova digitais realizada na fase investigativa é do juiz das garantias (CPP, artigo 3º-C),[163] em acordo com a organização judiciária do tribunal competente para o julgamento de eventual ação de conhecimento (ou execução, se for o caso).

Sem qualquer dos requisitos explicitados, a busca e a apreensão são inadmissíveis.

4.4 Consentimento do investigado

No processo acusatório, o investigado tem o direito de não se autoincriminar, o que implica na vedação de qualquer estímulo ou engano aptos a alterar a sua vontade e incliná-lo à autoincriminação.

Todavia, a lei admite que se existir consentimento do investigado, a busca e a apreensão podem ocorrer sem prévia autorização judicial (CPP, art. 245). O Código de 1941 não especifica como deve ser o consentimento. O Marco Civil da Internet (Lei n. 12.965, de 2014), em seu artigo 7º, inciso VII, exige, para o fornecimento das informações do usuário para terceiro, o consentimento livre, expresso e informado. Se para algo importante, mas menor, como as informações do usuário de internet, o sistema jurídico exige o consentimento livre, expresso e informado; para algo maior, como a liberdade, a privacidade e a inviolabilidade do domicílio, o consentimento do investigado para a busca e a apreensão sem prévia autorização judicial deve ser, no mínimo, também livre, expresso e informado (mormente porque o sistema jurídico processual penal expressamente admite a analogia: Código de Processo Penal, artigo 3º).

Ser livre implica que o consentimento do investigado deve ser resultado da sua autodeterminação na escolha de autorizar ou não a busca e a apreensão; sem violência, coerção ou qualquer espécie de engano (PITOMBO, Cleunice, 2005, p. 133).

Ser expresso significa que o consentimento deve ser explícito e inequívoco. É vedado o consentimento tácito. Num país de histórico de ditaduras, autoritarismo[164] e torturas policiais (COMISSÃO NACIONAL DA VERDADE, 2014) é ingênuo acreditar que alguém consentiu com a invasão de seu domicílio por policial. E, afinal, cabe à acusação demonstrar o consentimento (em função do estado de inocência como norma probatória);[165] com isso, o

(2019, p. 33-37).

[163] Vide observações na nota n. 128, *supra.*

[164] "Este autoritarismo se caracteriza pela produção de uma cidadania de baixa intensidade. Em uma cidadania de baixo escalão, uma cidadania desfigurada, a ordem sempre estará acima das regras, da lei, enfim. A ordem determina tanto a aplicação rigorosa da lei, quanto a sua própria subversão." (GLOECKNER, 2018, p. 153).

[165] Vide o item 4.3.1, *supra.*

consentimento deve ser expresso, tanto para demonstrar a sua inequivocidade quanto para a acusação poder cumprir seu ônus e demonstrá-lo.

A informação clara e suficiente ao investigado da finalidade, dos meios, do objeto e das possíveis implicações da busca e da apreensão é dever do agente público para eventual consentimento do investigado. A informação aperfeiçoa o exercício da ampla defesa enquanto autodefesa.[166] Informado, o investigado não será um estranho[167] ao evento e poderá agir racionalmente para consentir ou não com a busca e a apreensão.[168]

Nestes termos, o consentimento deve ser livre, expresso e informado.

Quanto ao registro do consentimento, o Superior Tribunal de Justiça, no julgamento do Habeas Corpus n. 598.051/SP, de relatoria do ministro Rogerio Schietti Cruz, publicado em 15 de março de 2021, decidiu:

> São frequentes e notórias as notícias de abusos cometidos em operações e diligências policiais, quer em abordagens individuais, quer em intervenções realizadas em comunidades dos grandes centros urbanos. É, portanto, ingenuidade, academicismo e desconexão com a realidade conferir, em tais situações, valor absoluto ao depoimento daqueles que são, precisamente, os apontados responsáveis pelos atos abusivos. E, em um país conhecido por suas práticas autoritárias – não apenas históricas, mas atuais –, a aceitação desse comportamento compromete a necessária aquisição de uma cultura democrática de respeito aos direitos fundamentais de todos, independentemente de posição social, condição financeira, profissão, local da moradia, cor da pele ou raça. […] Por isso, avulta de importância que, além da documentação escrita da diligência policial (relatório circunstanciado), seja ela totalmente registrada em vídeo e áudio, de maneira a não deixar dúvidas quanto à legalidade da ação estatal como um todo e, particularmente, quanto ao livre consentimento do morador para o ingresso domiciliar. Semelhante providência resultará na diminuição da criminalidade em geral – pela maior eficácia probatória, bem como pela intimidação a abusos, de um lado, e falsas acusações contra policiais, por outro – e permitirá avaliar se houve, efetivamente, justa causa para o ingresso e, quando indicado ter havido consentimento do morador, se foi ele livremente prestado. […] 12. Habeas Corpus concedido, com a anulação da prova decorrente do ingresso desautorizado no domicílio e consequente absolvição do paciente, dando-se ciência do inteiro teor do acórdão aos Presidentes dos Tribunais de Justiça dos Estados e aos Presidentes dos Tribunais Regionais Federais, bem como às Defensorias Públicas dos Estados e da União, ao Procurador-Geral da República e aos Procuradores-Gerais dos Estados, aos Conselhos Nacionais da Justiça e do Ministério Público, à Ordem dos Advogados do Brasil, ao Conselho Nacional de Direitos Humanos, ao Ministro da Justiça e Segurança Pública e aos Governadores dos Estados e do Distrito Federal, encarecendo a estes últimos que deem conhecimento do teor do julgado a todos os órgãos e agentes da segurança pública federal, estadual e distrital. 13. Estabelece-se o prazo de um ano para permitir o aparelhamento das polícias, treinamento e demais providências necessárias para a adaptação às diretrizes da presente decisão, de modo a, sem

[166] Aperfeiçoando o modelo constitucional do processo (ANDOLINA; VIGNERA, 1997, p. 8-11).
[167] Ennio Amodio (2016, p. 5) destaca que o investigado, leigo, é quem tem mais intensidade na percepção durante a persecução penal e, simultaneamente, quem tem mais estranhamento, por não compreender o que orienta a construção do procedimento.
[168] A informação "possibilita ao leigo uma autoproteção. Assim, sob o ponto de vista substancial (qualitativo), a informação deve somar, deve acrescer, deve preencher o vazio da assimetria informacional, equalizando-a." (BIONI, 2019, p. 245).

> prejuízo do exame singular de casos futuros, evitar situações de ilicitude que possam, entre outros efeitos, implicar responsabilidade administrativa, civil e/ou penal do agente estatal. (BRASIL, 2022d).[169]

Ainda cabem duas observações. A primeira é que não basta que seja livre, expresso e informado para que o consentimento seja válido. Existem situações em que o consentimento é irrelevante, inadmissível e o resultado do meio jamais poderá integrar validamente o procedimento. Essas situações que nem mesmo o consentimento do investigado autoriza que sejam feitas são as que ofendem a dignidade humana, como a tortura[170] (COSTA ANDRADE, 2013, p. 214-215).

A segunda observação tem relação com a soberania dos Estados.[171] A Convenção de Budapeste pautou-se pela limitação da atuação dos Estados ao seu território (artigos 18 a 21).[172] Contudo, no artigo 32.b, ela autoriza que um Estado acesse ou receba, a partir de um computador em seu território, elementos digitais armazenados no território de outro Estado, desde que tenha o consentimento da pessoa autorizada legalmente a revelar os elementos digitais – sem necessidade de cooperação internacional ou até de notificação ao outro Estado, conforme a nota de orientação n. 3, item 3.3 (COUNCIL OF EUROPE, 2022b).

Quem é o autorizado pela Lei a revelar os elementos digitais varia em cada sistema jurídico nacional. A pergunta a ser feita é se esta modalidade de acesso ou recebimento de elementos digitais armazenados em outro Estado, a partir da vontade de um único indivíduo, ofende a soberania nacional (RAMALHO, 2019, p. 73-75).

A modalidade do artigo 32.b é claramente situação de extraterritorialidade, afinal, os elementos digitais estão armazenados no território de outro Estado.

O processo penal brasileiro é regido pela territorialidade, mas o artigo 1º, inciso I, do Código de Processo Penal, admite ressalvas determinadas em tratados, convenções e regras de direito internacional. Tourinho Filho (1992, p. 124) elenca três situações possíveis de extraterritorialidade: no território onde nenhum Estado exerce soberania; se o Estado estrangeiro onde ocorrerá o ato autorizar; em guerra, no território ocupado. A Convenção de Budapeste foi assinada pelo Brasil e por outras dezenas de Estados Partes; logo, há concordância entre os signatários para a prática da modalidade de acesso e recebimento

[169] Após a interposição do Recurso Extraordinário n. 1.342.077, o feito está pendente de julgamento no Supremo Tribunal Federal.
[170] Proibida: na Constituição, artigo 5º, inciso III; na Convenção Americana sobre Direitos Humanos, artigo 5.2; e no Pacto Internacional sobre Direitos Civis e Políticos, artigo 7.
[171] Na lição de Baracho, a soberania é o "poder último de ação e decisão sobre a ordem jurídica" (BARACHO, 1987, p. 71).
[172] Tema aprofundado no item 4.10, *infra.*

transfronteiriço de elementos digitais sem a necessidade de cooperação internacional, se existir o consentimento da pessoa autorizada legalmente a revelar os elementos digitais.

Como pontua Anna-Maria Osula (2015, p. 727-728), se não existisse a concordância dos Estados Partes, haveria ofensa à soberania pela intervenção arbitrária de um Estado no território de outro. Como na Convenção de Budapeste há a concordância, não há ofensa à soberania na modalidade de acesso e recebimento de elementos digitais do artigo 32.b.

4.5 Elementos digitais disponíveis ao público

A busca em local de uso comum do povo[173] (como praças, ruas, estradas, mares e rios), em que o seu uso por qualquer pessoa carece de prévia autorização específica da administração, não tem regramento específico no Código de Processo Penal, mas a literatura jurídica entende não ser necessária autorização judicial (PITOMBO, Cleunice, 2005, p. 165).

A busca específica de elementos digitais disponíveis ao público tem regramento na Convenção de Budapeste, artigo 32.a, que permite o acesso a esses elementos independentemente da localização geográfica de seu armazenamento. Como argumenta Nicolai Seitz (2004, p. 38), a Convenção de Budapeste neste ponto apenas regulamentou a prática anterior e costumeira de acesso, a partir de qualquer localidade, a elementos digitais armazenados em servidores espalhados em todo o mundo. Assim, numa primeira leitura, os elementos digitais disponíveis ao público poderiam ser procurados e obtidos para fins de segurança pública ou persecução penal, sem prévia autorização judicial ou notificação ao Estado estrangeiro.

Contudo, há de se diferenciar a exposição voluntária de uma informação pela sua disponibilização ao público da autorização do uso dessa informação na persecução criminal:

> É um tema que tem de ser discutido, porque o argumento de que se as próprias pessoas de livre e espontânea vontade expõe a sua vida particular nas redes sociais e nas comunicações digitais, elas autodiminuem a força jurídica tutelante dos seus direitos fundamentais pessoais, não colhe e é contrária ao próprio artigo 18º, nºs 2 e 3 da CRP. São dimensões distintas e díspares que não podem ser confundidas: uma é a autodeterminação expositiva; a outra é essa informação própria da sua autodeterminação expositiva ser fundamento de prova criminal. A pessoa expõe, não autoriza a utilização dessa informação ou desses dados para fins criminais, ou seja, não presta prévio consentimento, não produz uma declaração de ciência e de vontade. A postagem ou a colocação do vídeo não é uma declaração de vontade, mas tão-só uma declaração de ciência. (VALENTE, 2019, p. 19).

[173] Código Civil, artigo 99, inciso I.

Contra a supervigilância ininterrupta que pode criar perfis com base nos elementos digitais disponibilizados pelos próprios usuários,[174] a limitação do uso da informação ou dado digital ao fim consentido é medida que mitiga a ingerência do Estado na esfera privada e que dificulta as buscas desproporcionais e automatizadas (NÚÑEZ, 2016, p. 43-44). Esta noção é traduzida na autodeterminação informativa, que se concretiza na faculdade do titular controlar o uso das suas informações e dados pessoais por terceiros e no dever de abstenção de terceiros em usar as informações e dados pessoais sem prévio consentimento do titular.[175]

A autodeterminação informativa é um dos fundamentos da Lei Geral de Proteção de Dados Pessoais (LGPD) (art. 2º, II, da Lei 13.709, de 2018). A LGPD não é aplicada para fins de segurança pública e atividades de investigação e repressão de infrações penais (art. 4º, III, *a* e *d*, da mesma lei). Todavia, a autodeterminação informativa é também prevista como fundamento do Anteprojeto de Lei de Proteção de Dados para segurança pública e investigação criminal, no artigo 2º, inciso II (BRASIL, 2021d), e deriva da privacidade e da proteção dos dados pessoais, assegurados constitucionalmente (Constituição de 1988, artigo 5º, incisos X e LXXIX – Incluído pela Emenda Constitucional n. 115, de 2022 –; Constituição Portuguesa, artigos 26º e 35º) (VALENTE, 2019, p. 19) (NÚÑEZ, 2016, p. 43).[176]

A disponibilização de elementos digitais ao público pode ser motivada pelas mais diversas razões. O ponto é que é absurdo e ficcional presumir, contrariamente ao investigado, que este ato é de consentimento do uso do elemento digital em persecução penal. Portanto, pelo uso do elemento digital poder ofender a privacidade, a autodeterminação informativa e a proteção contra a autoincriminação, a busca e a apreensão de elementos digitais disponibilizados ao público para finalidade diversa das consentidas pelo usuário devem ser

[174] Vide o capítulo 2, *supra.*

[175] "Se o indivíduo tem um direito à autodeterminação informacional, isso significa que a atividade informacional do Estado referida a um indivíduo configura uma *intervenção informacional* (Informationseingriff), que necessita de um fundamento legal […] Se o indivíduo tem de ser protegido de condutas estatais como a *obtenção*, o *armazenamento*, a *utilização* e a *transferência* de dados, as quais têm de encontrar limites, isso significa que essas quatro fases do processamento de informações são intervenções e, principalmente, que elas são intervenções de natureza autônoma: uma norma que autoriza a obtenção de um dado não autoriza já automaticamente a utilização ou o armazenamento, muito menos a transferência. Necessita-se de uma norma para cada uma das quatro fases. Como o indivíduo tem de poder saber que uso se que fazer de seus dados, os dados obtidos estão submetidos ao *princípio da vinculação a um fim* ou da *vinculação finalística* (Zweckbindung) [...]" (GRECO, Luís, 2018, p. 44).

[176] Para Laura Schertel Ferreira Mendes (2018, p. 198), o fundamento constitucional da autodeterminação informativa é o *habeas data*: "as informações pessoais, armazenadas e processadas por outras entidades, – pelo simples fato de possibilitarem a identificação de determinado indivíduo –, podem afetar a sua esfera de direitos e, por isso, merecem a tutela constitucional a partir da garantia do *habeas data*. […] o *habeas data* e autodeterminação informativa podem ser considerados dois lados da mesma moeda, sendo o primeiro uma garantia processual de proteção das liberdades e da personalidade frente ao tratamento de dados e o segundo o direito material propriamente dito, que protege o indivíduo dos riscos decorrentes desse processamento."

precedidas de autorização judicial (reserva da jurisdição, Constituição, artigo 5º, XXXV), que fiscalizará a proporcionalidade, a impessoalidade e a fundamentação.

4.6 Inteligência artificial na busca, acesso e análise dos elementos digitais

Na sociedade de controle (item 2.2, *supra*), que visa o controle constante, ultrarrápido (preferencialmente preventivo) e em grande escala de grupos de suspeitos pela classificação dos indivíduos em cifras registradas em imensos bancos de dados (DELEUZE, 2008b), nada é mais estratégico para a vigilância que a inteligência artificial.[177]

Luciano Frontino de Medeiros (2018, p. 21-23), que entende a "inteligência artificial" (IA) como o ramo de pesquisa da automação do comportamento inteligente (inteligência como sequência de cálculos[178]), explica que as pesquisas de IA concentram-se, principalmente, em três grandes linhas: a conexionista, que busca imitar as sinapses entre os neurônios do cérebro humano e criar um cérebro artificial; a simbólica, que busca imitar a significação humana dos fenômenos; e a evolucionária, que baseia-se na imitação da seleção natural.

Integram a linha conexionista as pesquisas de redes neurais (que reconhecem padrões, a partir de algoritmos alimentados por bancos de dados ou por informações de usuários reais, e que otimizam as classificações) e de sistemas imunológicos artificiais (que identificam fatores estranhos no funcionamento normal do sistema e opera comandos para excluí-los – essa tecnologia é utilizada, por exemplo, para sistemas de segurança da informação e antivírus). Integram a linha simbólica as pesquisas de sistemas de especialistas (que buscam transformar o conteúdo aprendido por um especialista humano numa determinada ciência em uma linguagem informática programável) e de ontologias (que buscam imitar a mente humana a partir de semelhanças em análises, classificando e relacionando proposições humanas em que há maior consenso). E integram a linha evolucionária as pesquisas dos algoritmos

[177] Destaca-se que a utilização da expressão "inteligência artificial" nesta tese é feita exclusivamente pela sua recorrência em trabalhos científicos. Na década de 1950, Turing (1950, p. 433-434) questionou se as máquinas poderiam ser consideradas inteligentes caso conseguissem imitar o comportamento humano inteligente (que, para o autor, é um procedimento mecânico, uma sequência de cálculos); todavia, o próprio Turing (1937, p. 259) já havia demonstrado que não (na década de 1930), em função das máquinas não conseguirem resolver equações com números não computáveis – o que é possível de ser feito por humanos. Portanto, como anota Penrose (1993, p. 36): "Talvez haja alguma ironia no fato de que esse aspecto do trabalho do próprio Turing [de 1937] possa agora proporcionar-nos, indiretamente, um provável furo no seu ponto de vista relativo à natureza dos fenômenos mentais [expresso no artigo de 1950]". Assim (e também pelas razões expressadas no item 3.1, *supra*), as máquinas não conseguem imitar o comportamento humano inteligente, não sendo, propriamente, "inteligência" artificial – no sentido de inteligência como o potencial de seres sencientes e sapientes de articular inferências, que os possibilita agir por razões (BRANDOM, 2001a, p. 157).

[178] Vide a nota anterior.

genéticos (que apresentam uma solução inicial para o problema e que é programado por algoritmo que possibilita a sua própria alteração durante a execução) e da programação genética (em que o próprio algoritmo cria a solução inicial para o problema e os blocos de programas alteram a programação inicial até alcançar o objetivo) (MEDEIROS, Luciano, 2018, p. 22-26).

Dessas três linhas de pesquisa resultam novas tecnologias, cogitações sobre a vida real, questionamentos filosóficos sobre a inteligência, alterações de comportamento e, potencialmente, modificações infinitas (MUNÁRRIZ, 1994, p. 42).

A inteligência artificial já é utilizada para diversas funções na persecução penal. Por exemplo, a Áustria utiliza o *AI for analysis of investigative data* para analisar grandes quantidades de dados obtidos em buscas domiciliares, relacionando as pessoas referidas em documentos ou gravações. E utiliza o *Facial recognition for inmates* para criar alertas, baseados em vigilância do espaço público por vídeo, na situação do sistema reconhecer comportamentos anormais que possam resultar em eventos criminais – são identificadas o número de pessoas numa imagem e atos de agressão, por exemplo; o sistema, no futuro, utilizará, também, microfones e outros sensores. A Dinamarca utiliza o *Exploring the use of face AI recognition technology for victim identification across pictorial material of child abuse* para o reconhecimento facial de vítimas de abuso infantil. A Alemanha utiliza o *Cognitive systems at the prosecutor's office* para auxiliar investigadores a analisar dados, criando visualizações gráficas do cruzamento dos dados, por exemplo. Utiliza o *Research project to fight child pornography with methods of AI* para identificar atos de pedofilia em banco de dados com imagens de pornografia. E utiliza o *Identification of hate crime on social media* para ranquear postagens na internet e identificar postagens de ódio ou ilegais. A Itália utiliza o *Aut Dedere Aut Judicare* para análise de dados e estatística sobre matérias relacionadas à cooperação internacional, como termos semelhantes em documentos diferentes, tais quais mandados de prisão ou decisões de extradição. E utiliza o *Giustizia penale e intelligenza artificiale* para identificar padrões entre dados referentes a procedimentos diferentes. A Lituânia utiliza o *Real-time network, text, and speaker analytics for combating organised* (ROXANNE) para rastrear e revelar a atuação de organizações criminosas pela identificação e monitoramento de pessoas suspeitas através de reconhecimento de voz, reconhecimento facial e criação de gráficos. Portugal utiliza o *AI technology for evidence analysis* para classificar, indexar e pesquisar no banco de dados, criando visualizações compreensivas dos dados. E utiliza o BALCAT para criar banco de dados sobre armas e munições, e identificar o tipo, a marca, o modelo e o proprietário, para que a balística forense

consiga otimizar sua análise. A Suécia utiliza o PROFILE para identificar fraudes fiscais no transporte internacional de bens. E o *Enhancing the Efficiency of Investigative Work by the Swedish Competition Authority's Enforcement Units* para classificar e separar elementos de prova, como e-mails, que contenham informações relevantes para investigações antitruste (EUROPEAN COMMISSION, 2022, p. 111-115, 120-125, 127, 131-132, 140).

No Brasil, a inteligência artificial já é utilizada no Direito, por exemplo, para classificação de dados, *Online Dispute Resolution* (ODR), predição estatística, cruzamento entre bases de dados e, em 2020, metade dos tribunais brasileiros já utilizava tecnologias de IA (como o Victor do Supremo Tribunal Federal – que, entre outras funções, identifica peças dos autos, classifica recursos extraordinários quanto a temas de repercussão geral e opera parte da comunicação com os tribunais de origem –, o Athos, o Sócrates, E-juris e o Tua do Superior Tribunal de Justiça – que, respectivamente, entre outras operações, são utilizados para auxiliar os gabinetes na análise do juízo de conformidade com a jurisprudência, agrupamento de casos semelhantes, auxílio à secretaria de jurisprudência e distribuição dos feitos de competência originária e recursal) (NUNES, 2021, p. 26-29) (SALOMÃO, 2021). Na persecução penal, a inteligência artificial já é utilizada por agências públicas como o Laboratório de Tecnologia contra Lavagem de Dinheiro do Ministério da Justiça e Segurança Pública e o COAF (BARROS; BOLZAN DE MORAIS, 2021, p. 349-352).

Nesta tese, tem importância a utilização da inteligência artificial especificamente para a busca, acesso e análise dos elementos digitais. Na sequência serão expostos alguns exemplos brasileiros, para contextualização.

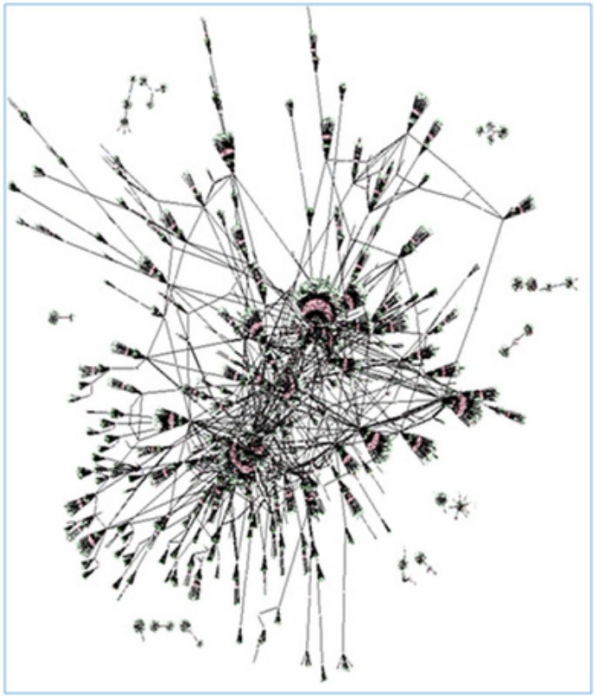
Na operacionalização da busca o Tribunal de Contas da União utiliza o *software* de inteligência artificial ALICE. Esse *software* coleta informações do Diário Oficial da União e de bancos de dados governamentais diariamente. Coletados, o robô analisa editais de licitação, estima o valor do contrato, cruza os dados (como os de fornecedores) e identifica situações tais quais a restrição de competitividade na habilitação (como exigir documentos indevidos), o impedimento de empresas contratarem com a União (como as envolvidas em corrupção) e fraudes (como empresas concorrentes com os mesmos sócios) (BARROS; BOLZAN DE MORAIS, 2021, p. 350).

No acesso aos elementos digitais, a inteligência artificial é utilizada principalmente em função da existência de criptografia (item 3.2.2.1, *supra*). Como dito no item 3.3, *supra*, pelo uso do *Cellebrite* é possível superar a criptografia de aparelhos Apple e Android e extrair a integralidade dos dados. No caso da investigação da morte de Henry Borel, por exemplo, o

Cellebrite foi utilizado para desbloquear *smartphone* de investigado e acessar suas mensagens de texto e arquivos de imagens deletados (BBC NEWS, 2021).

Na análise dos elementos digitais, o Laboratório de Tecnologia contra Lavagem de Dinheiro do Ministério da Justiça e Segurança Pública – também exemplificativamente – se vale de várias ferramentas para combater o crime de lavagem de dinheiro (o que é especialmente estratégico para a repressão das organizações criminosas). Uma das ferramentas, o *IBM i2 Analyst's Notebook*, baseado no grande volume de dados obtidos pela quebra dos sigilos bancário, fiscal e de comunicação, cruza os dados, identifica a circulação de dinheiro e cria um gráfico sobre essa circulação (STOPANOVSKI, 2020):

Figura 5 – Gráfico do Laboratório de Tecnologia contra Lavagem de Dinheiro



Fonte: Stopanovski (2020)

No gráfico acima, produzido pelo *software* de inteligência artificial, as linhas conectam dois pontos. Os pontos são contas bancárias e as linhas simbolizam a circulação financeira entre as contas. Pelo gráfico, que pode ser baseado em milhares de transações, percebe-se que determinadas transações ocorreram em contas separadas das demais. No centro estão as contas que mais participaram da circulação de dinheiro. Isso indica, por exemplo, que certas pessoas têm relações financeiras constantes com algumas, e nenhuma com outras, o que ajuda a investigar possíveis atos de lavagem de dinheiro (STOPANOVSKI,

2020). Sem a inteligência artificial e a projeção por gráfico, seria perto do impossível um humano analisar o banco de dados.

Esses são apenas alguns exemplos citados para contextualizar o uso da inteligência artificial na busca, acesso e análise dos elementos digitais no Brasil. As implicações jurídicas são várias.

Uma das principais decorre do problema causado pela opacidade no funcionamento da inteligência artificial, que deve ser controlável pelos agentes jurídicos (NUNES; VIANA, 2021) (VACIAGO, 2019, p. 282). Como o Parlamento Europeu realçou na Resolução de 16 de fevereiro de 2017:

> 12. Realça o princípio da transparência, nomeadamente o facto de que deve ser sempre possível fundamentar qualquer decisão tomada com recurso a inteligência artificial que possa ter um impacto substancial sobre a vida de uma ou mais pessoas; considera que deve ser sempre possível reduzir a computação realizada por sistemas de IA a uma forma compreensível para os seres humanos; considera que os robôs avançados deveriam ser dotados de uma «caixa negra» com dados sobre todas as operações realizadas pela máquina, incluindo os passos da lógica que conduziu à formulação das suas decisões; (PARLAMENTO EUROPEU, 2021b).

A falta de transparência deriva do sigilo intencional das empresas privadas ou do Estado, do "analfabetismo técnico" das pessoas quanto à tecnologia e da própria operação do robô, que relaciona os dados de maneira diferente dos humanos, fazendo com que seu funcionamento sobre imensas bases de dados seja incompreensível (basta pensar no tempo que seria necessário para conferir cada uma das trilhões de operações matemáticas da máquina manualmente[179]) (BARROS; BOLZAN DE MORAIS, 2021, p. 359) (BOLZAN DE MORAIS; MENEZES NETO, 2018, p. 1144).

Sem transparência, como exercer o contraditório e a ampla defesa quanto ao funcionamento da inteligência artificial? O prejuízo à efetividade desses institutos processuais é explícito.

Contra isto, em relação ao sigilo intencional das empresas e do Estado, Flaviane Barros e José Luiz Bolzan de Morais defendem a atuação confidencial de consultor independente e a abertura dos códigos. Em relação ao "analfabetismo técnico", os autores recomendam o ensino dos indivíduos. E em relação à opacidade no funcionamento do robô, sustentam que deve seguir um código de boas práticas, devem ser reduzidos os conjuntos de dados de análise – "já que o excesso de dados gera muitas sub-ramificações em modelos operacionais de classificação e ao invés de aprimorar análises deixam elas mais passíveis de

[179] Já existem computadores que conseguem atingir dez trilhões de operações por segundo (XU et al., 2021, p. 44).

erro" –, os critérios do robô devem ser mais claros e os dados inaugurais que influenciaram as operações da máquina devem ser acessíveis às partes (BARROS; BOLZAN DE MORAIS, 2021, p. 361-365).

Outro ponto é o funcionamento das tecnologias de inteligência artificial, como observa Paolo Comoglio (2018, p. 344-345), aumentar ainda mais a importância de atos escritos realizados fora do espaço processual de conhecimento. Ao invés da prova produzida em contraditório, com oralidade e publicidade,[180] os elementos informativos escritos produzidos por inteligência artificial antes do ajuizamento da ação revelam fatos importantes e atraem o foco da decisão judicial; o que, como demonstrado no item 2.6, *supra*, diminui a participação ativa do acusado na construção da decisão jurídica.

A inteligência artificial também apresenta vulnerabilidades pelos erros humanos na criação do algoritmo e na inserção dos dados (como dados com erros materiais ou duplicados), pelos dados fragmentados (que não têm como traduzir a totalidade do contexto) e pelo enviesamento resultante da transmissão para a máquina das predisposições mentais dos humanos (na programação e na alimentação da máquina) (FERGUSON, 2017, p. 1145-1150).[181] Por isso, como sugerem Simon Egbert e Matthias Leese (2021, p. 222-223), são devidas as seguintes cautelas: compreender que os dados não são uma tradução fiel do mundo, são sempre apenas parte de um contexto; a programação de *softwares* utilizados pelos órgãos públicos deve ser sempre transparente e compreensível, ainda que tenha sido produzida por empresas privadas; deve existir, necessariamente, crítica humana à operação do algoritmo; as instituições devem estimular a crítica aos algoritmos e que as decisões sejam feitas por

[180] A oralidade não é leitura da escritura, é opção política e técnica de construção oral dos atos do procedimento. Como opção política, a oralidade possibilita a participação ativa do acusado e o respeito aos seus direitos na construção da decisão jurídica. Como técnica de construção oral dos atos do procedimento, ela assegura a imediação, a publicidade e a identidade física do juiz; na síntese de Binder (1999, p. 100-101, tradução nossa: "si se utiliza la palabra hablada, las personas deben estar presentes (inmediación) y, además, se comunican de un modo que es fácilmente controlable por otras personas (publicidad)"): "se se utiliza a palavra falada, as pessoas devem estar presentes (imediação) e, ademais, se comunicam de um modo que é facilmente controlável por outras pessoas (publicidade)".

[181] Dierle Nunes e Ana Luiza Pinto Coelho Marques (2018) nomeiam de vieses algorítmicos à transmissão para a máquina das predisposições mentais dos humanos que a programaram e a alimentaram com informações. De maneira não intencional, o enviesamento da pessoa envolvida na programação ou na alimentação do sistema informático contamina tanto o algoritmo que constitui o espaço virtual quanto as informações de entrada (*input*), que são as referências da resposta da máquina (*output*). Consciente da ausência de neutralidade e do potencial do erro das máquinas, o Parlamento Europeu expressamente considerou, na Resolução de 14 de março de 2017: "que os dados e /ou os procedimentos de baixa qualidade em que se baseiam os processos de tomada de decisão e os instrumentos analíticos podem traduzir-se em algoritmos parciais, correlações ilegítimas, erros, numa subestimação das implicações jurídicas, sociais e éticas, no risco de utilização de dados para fins discriminatórios ou fraudulentos e na marginalização do papel dos seres humanos nestes processos, podendo resultar em processos imperfeitos de tomada de decisão, com um impacto nocivo nas vidas e nas oportunidades dos cidadãos, mormente nos grupos marginalizados, bem como em consequências negativas para as sociedades e as empresas;" (PARLAMENTO EUROPEU, 2021a). Sobre o tema, vide: Nathália Medeiros (2019).

humanos; análises de risco devem ser consideradas como mera estimativa, não como prova de um evento futuro; os agentes públicos devem estar atentos para não se enviesarem pelas previsões dos algoritmos; devem ser conhecidas as limitações tecnológicas existentes hoje, e não se deve confundir as possibilidades futuras da tecnologia com o que já existe.

Para regulamentar o uso da inteligência artificial pelo judiciário, o Conselho Nacional de Justiça (CNJ) editou a Resolução n. 332, de 21 de agosto de 2020[182]. Nela, foi determinado, principalmente: que a implantação e o uso da Inteligência Artificial devem ser compatíveis com os direitos fundamentais (art. 4º); deve existir igualdade de tratamento (art. 5º); os dados pessoais e o segredo de justiça devem ser protegidos no desenvolvimento e treinamento do sistema (art. 6º); não deve existir discriminação por viés algorítmico ou qualquer outra causa (art. 7º); o uso da inteligência artificial deve ser transparente (art. 8º[183]), com "explicação dos passos que conduziram ao resultado" (art. 19) e preferência de programação do *software* em código aberto (art. 24);[184] devem ser cumpridos padrões de qualidade, como os relacionados à interface de programação de aplicativos (arts. 9º a 12); a proveniência de dados deve ocorrer por fontes seguras, o sistema deve impedir a alteração dos dados antes do treinamento, deve ser feita cópia de cada versão de modelo desenvolvida, o acesso aos dados deve ser restrito e o ambiente de armazenamento e execução da inteligência artificial deve atender a padrões de segurança da informação[185] (arts. 13 a 16); e o usuário deve estar no controle da inteligência artificial, que terá seu uso sempre fiscalizado (arts. 17 a 19) (BRASIL, 2022n).

As agências públicas já utilizam a inteligência artificial diuturnamente. A regulamentação pela Resolução do CNJ n. 332, de 21 de agosto de 2020, é o começo da normatização específica relacionada a esse uso pelo judiciário e influencia o uso dessa tecnologia no geral, o que inclui a busca, o acesso e a análise dos elementos digitais.

[182] A Resolução n. 332 do CNJ foi baseada na Carta Europeia de Ética sobre o Uso da Inteligência Artificial em Sistemas Judiciais e seus ambientes, como consta em suas considerações iniciais (BRASIL, 2022n, p. 2).

[183] "Art. 8º Para os efeitos da presente Resolução, transparência consiste em: I – divulgação responsável, considerando a sensibilidade própria dos dados judiciais; II – indicação dos objetivos e resultados pretendidos pelo uso do modelo de Inteligência Artificial; III – documentação dos riscos identificados e indicação dos instrumentos de segurança da informação e controle para seu enfrentamento; IV – possibilidade de identificação do motivo em caso de dano causado pela ferramenta de Inteligência Artificial; V – apresentação dos mecanismos de auditoria e certificação de boas práticas; VI – fornecimento de explicação satisfatória e passível de auditoria por autoridade humana quanto a qualquer proposta de decisão apresentada pelo modelo de Inteligência Artificial, especialmente quando essa for de natureza judicial." (BRASIL, 2022n).

[184] A noção de código aberto (*open source*) é distinta da de *software* livre (*free software*). Ser *free software* implica no endosso de quatro noções de liberdade: a liberdade de usar o *software* como quiser; a liberdade de entender como o *software* funciona e de alterá-lo (o *free software* tem código aberto [*open source*] – seu código de programação é disponível a qualquer um –, apesar de nem todo software de código aberto ser um *free software* – por não respeitar as demais liberdades –); a liberdade de copiar o *software*; e a liberdade de distribuir cópias de suas versões modificadas para outros (STALLMAN, 2015, p. 3-7, 64-67). Vide, também: Stallman (2021).

[185] Como as da NBR ISO/IEC 27002 (ABNT, 2013a).

4.7 Ilegalidade da pescaria probatória (fishing expedition)

Como os elementos de prova digitais são apreendidos principalmente pela obtenção do dispositivo que os armazena, que contém imensa quantidade de informações, frequentemente em nada relacionadas à decisão que autorizou a medida, a busca e a apreensão dos elementos de prova digitais têm grande potencial de serem utilizadas para a pescaria probatória: autoriza-se a busca sob alegação genérica e, pela apreensão de vários elementos digitais, encontram-se informações sem qualquer vínculo com o caso originário (RAMALHO, 2019, p. 253). Essa prática é evidentemente ilegal.

A pescaria probatória é a prática de devassa indiscriminada à procura de elementos de prova por meios previstos na legislação, como a busca e a apreensão, mas sem prévios indícios concretos ou fundamentação específica relacionada a um caso penal determinado. Pela pescaria probatória há tentativa de burla aos requisitos legais para, ao invés de investigar fatos revelados por elementos de informação já conhecidos, se promover investigação prospectiva genérica e ampla (ROSA, 2020, p. 675-678).

Os requisitos legais (tratados no item 4.3.2, *supra*), são limites contra a arbitrariedade nas autorizações judiciais de realização da busca e da apreensão de elementos de prova digitais. A indicação do local da busca, da finalidade da apreensão e dos indícios concretos de materialidade, por exemplo, diminui os abusos, como os que ocorrem na pescaria probatória (*fishing expedition*) (LESSIG, 2006, p. 159).

No sistema jurídico brasileiro, há vinculação dos atos da busca e da apreensão de elementos de prova digitais à decisão jurídica que os autorizou. Os elementos digitais obtidos somente podem ser utilizados para o caso penal tratado na fundamentação da decisão. Apenas para esse caso existiu prévia autorização judicial (indispensável para medida tão invasiva e de grande potencial de ofensa aos direitos fundamentais, como à privacidade e à proteção contra a autoincriminação) (LOPES JR., 2012, p. 585).[186]

Como decidiu o Superior Tribunal de Justiça no Agravo Regimental em Recurso em Mandado de Segurança n. 62.562/MT, de relatoria do ministro Jesuíno Rissato:

> Os indícios de autoria antecedem as medidas invasivas, não se admitindo em um Estado Democrático de Direito que primeiro sejam violadas as garantias constitucionais para só então, em um segundo momento, e eventualmente, se justificar a medida anterior, sob pena de se legitimar verdadeira *fishing expedition*, conhecida como pescaria probatória, ou seja, "a procura especulativa, no ambiente

[186] Vide os itens 4.16.1 e 4.16.2, *infra.*

> físico ou digital, sem 'causa provável', alvo definido, finalidade tangível ou para além dos limites autorizados (desvio de finalidade), de elementos capazes de atribuir responsabilidade penal a alguém". (BRASIL, 2022f)

Portanto, é ilegal a prática de pescaria probatória em qualquer situação,[187] o que inclui a busca e a apreensão de elementos de prova digitais.

4.8 Mandado

Em função dos direitos fundamentais que podem ser ofendidos, a busca e a apreensão de elementos de prova digitais exigem prévia autorização judicial e expedição de mandado (Constituição, artigo 5º, inciso XXXV);[188] sem ambos, a busca e a apreensão são ilegais – como já decidiu o Superior Tribunal de Justiça quanto a elementos digitais armazenados em aparelhos celulares[189].

O código decretado pelo ditador Getúlio Vargas prevê a hipótese de busca sem mandado se o julgador pessoalmente executá-la (artigo 241, do CPP). Essa hipótese é inconstitucional, por ofensa ao processo acusatório.

A eleição constitucional foi pelo processo acusatório (PRADO, Geraldo, 1999, p. 149-172). Quem investiga cria a expectativa de confirmação de sua hipótese e, com isso, não age imparcialmente na sequência dos atos do procedimento:

> A solidão na qual os inquisidores trabalham, jamais expostos ao contraditório, fora dos grilhões da dialética, pode ser que ajude no trabalho policial, mas desenvolve quadros mentais paranoicos. Chamemo-los "primado das hipóteses sobre os fatos": quem investiga segue uma delas, às vezes com os olhos fechados; nada a garante mais fundada em relação às alternativas possíveis, nem este trabalho estimula cautela autocrítica; como todas as cartas do jogo estão na sua mão e é ele quem as coloca na mesa, aponta para a "sua" hipótese. Sabemos com quais meios persuasivos conta (alguns irresistíveis: por exemplo, a tortura do sono, calorosamente recomendada pelo piedoso penalista Ippolito Marsili); usando-a orienta o êxito para onde quer. Nas causas milanesas da peste manufaturada, junho-julho de 1630, vemos como juízes por nada desonestos, antes inclinados a um incomum garantismo, fabriquem delito e delinquentes: o inquirido responde docilmente; o inquisidor lhe retira da cabeça os fantasmas que tenha ali projetado. (CORDERO, 1986, p. 51-52, tradução nossa).[190]

[187] Como em interceptações telefônicas de grande período, sem indícios concretos prévios ou de números de telefone indeterminados; ou na cooperação internacional sem demarcação específica da finalidade (ROSA, 2020, p. 677).
[188] Vide o item 4.3.2, *supra*.
[189] *E.g.*: Recurso Especial n. 1.630.097/RJ, relator ministro Joel Ilan Paciornik, publicado em 28 de abril de 2017; Agravo Regimental no *Habeas Corpus* n. 542.940/SP, relator ministro Nefi Cordeiro, publicado em 10 de março de 2020. No mesmo sentido: Leonardo Marcondes Machado (2020, p. 208-209).
[190] "Logica deforme. La solitudine in cui gli inquisitori lavorano, mai esposti al contraddittorio, fuori da griglie dialettiche, può darsi che giovi al lavorìo poliziesco ma sviluppa quadri mentali paranoidi. Chiamiamoli 'primato dell'ipotesi sui fatti': chi indaga ne segue una, talvolta a occhi chiusi; niente la garantisce più fondata rispetto

Aquele que executa a busca tem a expectativa de encontrar o elemento de prova digital relevante para o conhecimento da autoria ou materialidade de um delito. Se o juiz assumir esta função ele criará a mesma expectativa e, inconscientemente, não conseguirá ser imparcial.

Ora, é inadmissível que o juiz crie hipóteses antes dos fatos, antes da construção em contraditório do procedimento, atue proativamente na gestão da prova e deixe de ser imparcial, como ocorrerá com o juiz executor da busca. Por estas razões, a busca executada pessoalmente por juiz é inconstitucional; o que pode ser declarado, inclusive, por qualquer órgão do judiciário, em controle difuso de constitucionalidade (LOPES JR., 2012, p. 716).

Como requisitos do mandado, o Código de Processo Penal (artigo 243) exige: indicação do local onde ocorrerá a busca; o nome do proprietário ou morador; o porquê da sua realização; e as assinaturas do escrivão e do juiz.[191] Além de ser garantia para quem pode ser afetado pela busca, o atendimento aos requisitos legais também protege o mandante e o executor: pela demarcação específica da finalidade, dos meios e do alcance da tarefa dos agentes, o mandante é protegido contra eventuais abusos do executor, que podem configurar crime,[192] e o executor tem assegurado que age em estrito cumprimento do dever legal (TORNAGHI, 1978, p. 62).

Finalmente, a redação do mandado incumbe ao escrivão (Código de Processo Civil, artigo 152, inciso I, aplicado subsidiariamente ao processo penal).

4.9 Horário

O Código de Processo Penal determina que as buscas sejam realizadas durante o dia (artigo 245, *caput*), mas não estabelece qual período é o dia – que pode variar em função da latitude do local e da fase de translação da Terra em torno do Sol (o que faz com que o verão tenha dias mais longos que o inverno, por exemplo). Tourinho Filho (2012, p. 742-745) defende que o período do dia é o compreendido entre as seis e as dezoito horas e que a

alle alternative possibili, né questo mestiere stimola cautela autocritica; siccome tutte le carte del gioco sono in mano sua ed è luiche l'ha intavolato, punta sulla 'sua' ipotesi. Sappiamo su quali mezzi persuasivi conti (alcuni irresistibili: ad esempio, la tortura del sonno, caldamente raccomandata dal pio penalista Ippolito Marsili); usandoli orienta l'esito dove vuole. Nelle cause milanese di peste manufacta, giugno-luglio 1630, vediamo come giudici nient'affatto disonesti, anzi inclini a inconsueto garantismo, fabbrichino delitto e delinquenti: l'inquisito risponde docilmente; l'inquisitore gliscova in teste i fantasmi che vi ha proiettato."

[191] Todos os atos e termos do processo devem ser assinados pelos que neles intervierem (CPC, art. 209).

[192] Como o de abuso de autoridade (Lei 13.869, de 2019).

determinação do processo civil de se realizar os atos processuais entre seis e vinte horas[193] é inaplicável ao processo penal: "Ninguém ousará dizer que às 20 horas ainda seja dia…". Iniciadas antes das dezoito horas, a busca e a apreensão podem adentrar à noite (PITOMBO, Cleunice, 2005, p. 213).

A Lei 13.869, de 2019 (que dispõe sobre os crimes de abuso de autoridade) (BRASIL, 2022l), tipificou como crime a execução de mandado de busca e apreensão domiciliar após as vinte e uma horas e antes das cinco horas (artigo 22, § 1º, inciso III). Rogério Greco e Rogério Sanches Cunha (2020, p. 202) comentam que a partir dessa tipificação surgiram duas correntes na literatura jurídica: a primeira entende ser ilícita a busca iniciada entre às dezoito e às seis horas e que é também criminosa a busca iniciada entre vinte e uma e cinco horas (a busca iniciada entre às dezoito e vinte e uma horas e entre às cinco e seis horas é ilícita mas não criminosa); a segunda entende que "enquanto houver iluminação solar" pode ocorrer a busca entre as cinco e vinte uma horas, e que há crime na busca executada entre vinte e uma e cinco horas, existindo luz solar ou não (corrente a que se filiam).

A razão está com a primeira corrente; em primeiro lugar, não se pode confundir a tipificação de crime com a normatização processual penal. Um crime exige especial intensidade de ofensa ao bem jurídico[194]; entender que isso é o mesmo que norma processual é um erro, são conceitos diferentes; nada vai contra o entendimento de que o legislador estabeleceu que é ilegal a busca executada à noite e que é especialmente grave, devendo ser tipificado como crime, a execução da busca no período dedicado ao repouso noturno, das vinte e uma às cinco horas; as diferenças da norma penal para a processual penal, aqui, são de grau de intensidade de ofensa à inviolabilidade do domicílio à noite e de sanção (pena privativa de liberdade na norma penal e nulidade[195] na norma processual penal). Em segundo lugar, o artigo 3º do Código de Processo Penal admite a analogia naquilo que for compatível

[193] O autor faz referência à disposição do artigo 172 do Código de Processo Civil de 1973, alterada pela Lei n. 8.952, de 1994, que teve a redação mantida no artigo 212 do Código de Processo Civil de 2015.

[194] "[…] a proteção dos bens jurídicos não se realiza somente mediante o Direito penal, senão que a ele há de cooperar o instrumental de todo o ordenamento jurídico. O direito penal só é inclusive a última entre todas as medidas protetoras que devem ser consideradas, é dizer que só se pode fazer-lhe intervir quando falhem outros meios de solução social do problema – como a ação civil, as regulações de polícia ou jurídico-técnicas, as sanções não penais, etc. –. Por ele se denomina a pena como a '*ultima ratio* da política social' e se define sua missão como proteção subsidiária de bens jurídicos." (ROXIN, 1997, p. 65, tradução nossa: "[…] la protección de bienes jurídicos no se realiza sólo mediante el Derecho penal, sino que a ello ha de cooperar el instrumental de todo el ordenamiento jurídico. El Derecho penal sólo es incluso la última de entre todas las medidas protectoras que hay que considerar, es decir que sólo se le puede hacer intervenir cuando fallen otros medios de solución social del problema – como la acción civil, las regulaciones de policía o jurídico-técnicas, las sanciones no penales, etc. –. Por ello se denomina a la pena como la '*ultima ratio* de la política social' y se define su misión como protección subsidiaria de bienes jurídicos.").

[195] "Nulidade é consequência jurídica prevista para o ato praticado em desconformidade com a lei que o rege, que consiste na supressão dos efeitos jurídicos que ele se destinava a produzir. Como consequência jurídica, a nulidade se integra na categoria das sanções." (GONÇALVES, 1993, p. 12).

com suas disposições expressas e com os princípios que orientam o processo penal. Há disposição expressa no artigo 245 do Código de Processo Penal de que as buscas devem ser executadas "de dia" (BRASIL, 2021a) e, repetindo Tourinho Filho (2012, p. 742), "Ninguém ousará dizer que às 20 horas ainda seja dia…". Portanto, a analogia é indevida por existir disposição expressa e específica em sentido contrário à interpretação de Greco e Cunha. Em terceiro lugar, manter que "enquanto houver iluminação solar" (GRECO, Rogério; CUNHA, 2020, p. 202) pode ocorrer a busca entre as cinco e vinte uma horas é criar espaço para a arbitrariedade ao deixar para o agente público a discricionariedade sobre se ainda existe a luz solar ou não entre às dezoito e vinte e uma horas e entre às cinco e seis horas – e o processo penal é limite contra a arbitrariedade (LOPES JR., 2012, p. 1133); deixar a discricionariedade do agente público decidir se a busca é ilegal ou não, por ainda existir iluminação solar ou não, é interpretação contrária à própria razão de existência do processo penal. Em quarto lugar, essa analogia vai contra a inviolabilidade de domicílio (Constituição, artigo 5º, inciso XI) por expandir o horário de execução da busca domiciliar, assim, é uma interpretação que aumenta a ofensa a direito fundamental – em sentido contrário ao sistema constitucional brasileiro, que limita ao máximo qualquer medida que possa ofender direito fundamental[196]; as analogias devem ser utilizadas para aumentar a efetividade dos direitos fundamentais, não para restringi-los. Em quinto lugar, a interpretação endossada por Greco e Cunha é contrária ao investigado e, por isso, ofende o *favor rei* – vez que na divergência de interpretações deve ser escolhida a mais favorável ao investigado (TOURINHO FILHO, 1992, p. 69) – sendo, também por essa razão, incorreta.

Portanto, a busca deve se iniciar entre às seis e às dezoito horas; se não for executada nesse prazo é ilegal (Código de Processo Penal, artigo 245); e, se for iniciada entre às vinte e uma e cinco horas, existirá também crime de abuso de autoridade, pela especial intensidade de ofensa à inviolabilidade do domicílio (Lei 13.869, de 2019, artigo 22, § 1º, inciso III).

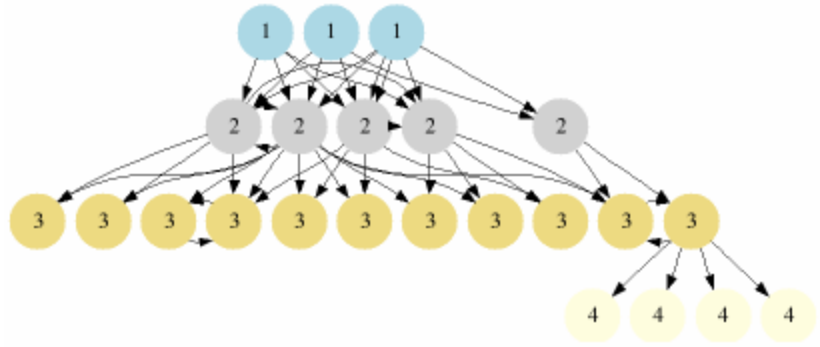
Sobre os elementos de prova digitais apreendidos, destaca-se, finalmente, uma particularidade quanto ao seu horário registrado no sistema informático: o tempo só será registrado no sistema informático se ele for programado para fazê-lo; além disso, é possível alterar os registros do tempo no sistema. Na situação de ligação de dois (ou mais) sistemas informáticos em rede[197], é possível, também, que os relógios dos sistemas não estejam

[196] "Cabe ao Judiciário a tarefa clássica de defender os direitos violados ou ameaçados de violência (art. 5º, XXXV, CF). A defesa dos direitos fundamentais é da essência da sua função. Os tribunais detêm a prerrogativa de controlar os atos dos demais Poderes, com o que definem o conteúdo dos direitos fundamentais proclamados pelo constituinte. A vinculação das cortes aos direitos fundamentais lega a doutrina a entender que estão elas no dever de conferir a tais direitos máxima eficácia possível." (MENDES, Gilmar; BRANCO, 2015, p. 153).
[197] Vide o item 3.2.3, *supra.*

sincronizados. Se isso ocorrer, quando alguém realizou determinada conduta pode estar registrado em horários divergentes nos sistemas informáticos, o que prejudica a compreensão da sequência dos eventos.

Não há solução infalível para esta situação. Ao Observatório Nacional, unidade de pesquisa do Ministério da Ciência e Tecnologia, compete gerar e disseminar a Hora Legal do Brasil (artigo 6º do Decreto da Presidência da República n. 10.546, de 1913, repristinado pelo Decreto Presidência da República n. 4.264, de 2002). O Observatório Nacional estabelece diretrizes de sincronismo do tempo no Brasil, com base em protocolos nacionais e internacionais, inclusive no uso da internet. Exemplificadamente, o *Network Time Protocol*, um dos protocolos utilizados, funciona do seguinte modo:

Figura 6 – Arquitetura do NTP



Fonte: NTP.br

A arquitetura do *Network Time Protocol* foi projetada para funcionar numa estrutura hierárquica em dezesseis níveis numerados de 1 a 16. O nível 0 corresponde a um sistema de GPS ou a um relógio atômico e não integra propriamente a estrutura, ele é o referencial primário de tempo. A partir desse referencial, o nível 1 transmite dados para o 2, o 2 para o 3, e assim sucessivamente na rede de servidores, numa dinâmica em que há obtenção e fornecimento de dados sobre o tempo, simultaneamente (NTP.br, 2022).

Órgãos públicos, empresas e até as pessoas privadas podem sincronizar o relógio de seus sistemas informáticos pela Hora Legal do Brasil, sob os protocolos do Observatório Nacional. Contudo, todo este aparato burocrático e logístico é facilmente burlado com um simples *proxy*, que utiliza servidor intermediário para mascarar na rede o IP do sistema informático, sua localização específica e seu horário real.[198]

Assim, deve existir cautela na análise do horário de um evento no sistema informático apreendido, tanto pela programação do registro do tempo no sistema, como pela possibilidade

[198] O endereço https://www.proxysite.com/, por exemplo, possibilita sua criação gratuita.

de alterar os registros, pela eventual situação de assincronia entre sistemas informáticos em rede e pelas tecnologias que conseguem mascarar o horário.

4.10 Observações sobre o local do elemento digital

Onde ocorreu a conduta e o resultado compõem o lugar do delito (teoria da ubiquidade, CP, art. 6º). Aos delitos cometidos no território nacional é aplicada a Lei penal brasileira (CP, art. 5º), assim como aos delitos cometidos em território estrangeiro, nas situações especificadas no artigo 7º, do Código Penal[199]. A competência do juízo é determinada pela pessoa (prerrogativa de função), pela matéria e pelo lugar. Como regra, é competente o juízo do lugar onde se consumou o delito, ou, se for tentado, o juízo do lugar onde ocorreu o último ato de execução. Se o lugar for incerto, a competência é determinada pela prevenção (CPP, artigos 69 a 91).[200] A lei processual penal brasileira é aplicada em todo o território nacional (CPP, art. 1º). Para a busca e a apreensão de elementos de prova digitais, estas determinações da lei penal e da lei processual penal no espaço devem ser interpretadas considerando as suas especificidades.

O espaço virtual é diferente do real e a internet, principalmente, é um espaço construído por protocolos em que o *Internet Protocol* (IP) não tem referência necessária a um local geográfico (LESSIG, 2006, p. 58).[201] A tecnologia de computação em nuvem ilustra isso. Por ela, os usuários têm acesso global a dados, *hardware*, programação e armazenamento com um custo muito inferior à compra do *hardware* e do *software* requeridos para fazer as mesmas operações de outro modo. Xiaodong Lin (2018, p. 8) compara a computação em nuvem com o aluguel de um apartamento num prédio, mas com a diferença de não ser o aluguel de uma unidade específica; o dispositivo de armazenamento utilizado para a computação em nuvem é

[199] "Art. 7º – Ficam sujeitos à lei brasileira, embora cometidos no estrangeiro: I – os crimes: a) contra a vida ou a liberdade do Presidente da República; b) contra o patrimônio ou a fé pública da União, do Distrito Federal, de Estado, de Território, de Município, de empresa pública, sociedade de economia mista, autarquia ou fundação instituída pelo Poder Público; c) contra a administração pública, por quem está a seu serviço; d) de genocídio, quando o agente for brasileiro ou domiciliado no Brasil; II – os crimes: a) que, por tratado ou convenção, o Brasil se obrigou a reprimir; b) praticados por brasileiro; c) praticados em aeronaves ou embarcações brasileiras, mercantes ou de propriedade privada, quando em território estrangeiro e aí não sejam julgados. § 1º – Nos casos do inciso I, o agente é punido segundo a lei brasileira, ainda que absolvido ou condenado no estrangeiro. § 2º – Nos casos do inciso II, a aplicação da lei brasileira depende do concurso das seguintes condições: a) entrar o agente no território nacional; b) ser o fato punível também no país em que foi praticado; c) estar o crime incluído entre aqueles pelos quais a lei brasileira autoriza a extradição; d) não ter sido o agente absolvido no estrangeiro ou não ter aí cumprido a pena; e) não ter sido o agente perdoado no estrangeiro ou, por outro motivo, não estar extinta a punibilidade, segundo a lei mais favorável. § 3º – A lei brasileira aplica-se também ao crime cometido por estrangeiro contra brasileiro fora do Brasil, se, reunidas as condições previstas no parágrafo anterior: a) não foi pedida ou foi negada a extradição; b) houve requisição do Ministro da Justiça." (BRASIL, 2022g).

[200] A Constituição especifica no artigo 109 a competência da Justiça Federal.

[201] Vide a nota n. 129, *supra.*

variável: se num momento os dados estão armazenados num local, no outro estão armazenados em local diferente, sem qualquer obrigação de serem mantidos num servidor determinado.

Além da dificuldade criada por esta tecnologia para se conhecer o local de armazenamento dos dados, a computação em nuvem proporciona ao usuário que ele apague seus dados com facilidade, a partir de qualquer lugar do mundo, o que pode prejudicar a apuração da materialidade e autoria de delitos que dependa dos elementos digitais (RAMALHO, 2019, p. 78).

Giuseppe Vaciago (2021, p. 7) explica existirem quatro abordagens diferentes quanto ao problema da localização dos elementos digitais no espaço virtual e, consequentemente, da competência na persecução penal: a primeira considera que os elementos digitais estão no local do armazenamento, *e.g.* onde se encontra o *hark disk*, e é competente o juízo dessa localidade; a segunda considera que é competente o juízo do país do usuário; a terceira utiliza o "princípio da bandeira", pelo qual os delitos cometidos em aviões, navios e naves espaciais são de competência do Estado da bandeira, seja qual for a sua localização no momento do delito; a quarta utiliza o poder de disposição, em que qualquer país que conseguir acesso aos elementos digitais é competente para julgamento, o que pode ser obtido com a descoberta do nome do usuário e senha, ou pelo consentimento voluntário de quem pode acessar aos elementos digitais (vide o item 4.4, *supra*).

O processo penal brasileiro é regido pelo princípio da territorialidade (CPP, artigo 1º). Contudo, o Código admite ressalvas feitas em tratados, convenções e regras de direito internacional (inciso I); e a Convenção de Budapeste prevê a territorialidade nos artigos 18 a 21 ("busca e apreensão de dados de computador" e "obtenção de dados de computador em tempo real"); a nacionalidade (artigo 22.1.d); o "princípio da bandeira" (artigo 22.1.b e c) – quanto aos crimes dos artigos 2 a 11 –; e a extraterritorialidade pelo poder de disposição no artigo 32.b (acesso transfronteiriço com consentimento voluntário) (BRASIL, 2021c).

A busca e a apreensão de elementos digitais, especificamente, são recomendadas no artigo 19 da Convenção de Budapeste. Esse artigo restringe a busca e a apreensão ao território do Estado-Parte; portanto, ele não excepciona o princípio da territorialidade previsto no artigo 1º, do Código de Processo Penal.

Com isso, a territorialidade continua a reger a busca e a apreensão de elementos de prova digitais. Não poderia ser de outro modo sem se ofender à soberania das nações (Constituição, artigo 1º, inciso I):

> […] no plano internacional, a soberania será configurada como o atributo jurídico de uma comunidade política territorialmente circunscrita que goza de completa integração num sistema internacional e que, nesse plano, goza de igualdade em relação aos demais Estados. É, aliás, este princípio da igualdade soberana entre Estados, definido por Roth como «princípio fundacional da ordem jurídica internacional», que se impõe que os membros de uma ordem jurídica internacional se reconheçam reciprocamente enquanto tal em termos idênticos. Nas palavras de Vattel, «um anão é tão homem como um gigante. Uma pequena república não é um Estado menos soberano do que o mais poderoso reino» (RAMALHO, 2019, p. 61).

Apesar de ser questionável, a manutenção da territorialidade como critério de competência para atos no espaço virtual (notadamente a internet, que é desterritorializada), os demais critérios também apresentam problemas significativos: o critério do país do usuário não responde às ameaças transnacionais; o "princípio da bandeira" pode estimular que criminosos armazenem os elementos digitais em lugares que não realizem cooperação internacional; e o poder de disposição pode levar a graves ofensas à privacidade por facilitar demasiadamente o acesso aos elementos digitais, o que deveria atender à proporcionalidade (já que bastaria obter legalmente o nome de usuário e a senha, o que poderia ser feito, se a lei autorizasse a busca por ingresso remoto, por ataque de força bruta, por exemplo) (VACIAGO, 2021, p. 7) (SPOENLE, 2022, p. 7-12).

Finalmente, pela manutenção do critério da territorialidade na determinação da competência, a cooperação internacional ganha importância na persecução penal que busque elementos de prova digitais (tema do item 4.10.2, *infra*).

4.10.1 Inviolabilidade do domicílio

Os romanos cultuavam na casa aos deuses *Lares*, as almas dos mortos que influenciam a família, e a casa (principalmente o altar, que continha o fogo sagrado[202]) era um local sacro. A violação de domicílio era injúria contra o morador. O direito germânico medieval também puniu a invasão de domicílio;

> Com a subversão, porém, dos estatutos municipais, o âmbito doméstico decaiu de sua prerrogativa, notadamente em face dos delegados do Príncipe. Os criminalistas

[202] "Portanto, o deus do fogo era a providência da família. Seu culto era muito simples. A primeira regra era manter continuamente sobre o altar alguns carvões acesos, porque, se o fogo se extinguia, um deus deixava de existir. Em certas horas do dia alimentavam-no com ervas secas e lenha; então o deus se manifestava em chamas brilhantes. Ofereciam-lhe sacrifícios, mas a essência de qualquer sacrifício era manter e aliviar o fogo sagrado, nutrir e fazer crescer o corpo de deus. É por isso que, antes de mais nada, ofereciam-lhe ramos; é por isso que derramavam sobre o altar o vinho quente da Grécia, óleo, incenso e gordura animais. O deus recebia essas ofertas, e as devorava; satisfeito e radiante levantava-se sobre o altar, e iluminava com seus raios a seu adorador. Era esse o momento próprio para invocá-lo; o hino da oração saía do coração do homem." (COULANGES, 2006, p. 36-37).

> do século XVII silenciam sobre a inviolabilidade do domicílio. Ocorreu a tal respeito uma verdadeira involução: tal como no primitivo direito oriental, só se fazia referência à violação do domicílio como *meio* para outro malefício especialmente incriminado. Somente com a vitória do *individualismo* sobre o *hiperestatismo* medieval é que se cuidou, novamente, de atribuir à turbação do direito doméstico um posto especial entre os crimes. (HUNGRIA, 1980, p. 204-206).

Na Inglaterra do século XVII, a partir do caso de Peter Semayne contra Richard Gresham, julgado pelo *King's Bench* em 1604,[203] Edward Coke escreveu que o dono da casa deve defendê-la como castelo e maior refúgio – "*domus sua cuique est tutissimum refugium*" –, até contra o *sheriff* do rei (COKE, [1605]/2003, p. 137). A partir de Coke, foi desenvolvida a "doutrina do castelo" (*castle doctrine*). Segundo Blackstone, por exemplo, a casa é protegida com imunidade, é para seu dono um castelo e nunca pode ser violada com impunidade; fazendo referência a Cícero e aos comentários de Coke, o autor defende que na proteção da casa, o dono e sua família podem agir além dos limites ordinários, vez que, além do terror, a violação da casa é ofensa ao direito de moradia (BLACKSTONE, 1770, p. 220-224).[204]

O Código Criminal do Império do Brasil de 1830 incriminou a entrada em casa alheia nos artigos 209 a 214. O Código Penal dos Estados Unidos do Brasil, de 1890, nos artigos 196 a 203. E o atual Código Penal incrimina a violação de domicílio no artigo 150.

Posto isso, nos termos do Código Penal (artigo 150): "[…] § 4º - A expressão 'casa' compreende: I – qualquer compartimento habitado; II – aposento ocupado de habitação coletiva; III – compartimento não aberto ao público, onde alguém exerce profissão ou atividade". Em noção clássica, o domicílio penal é "a *habitação* particular, o local reservado à vida íntima do indivíduo ou à sua atividade privada, seja ou não coincidente com o domicílio civil" (HUNGRIA, 1980, p. 207).

A entrada em domicílio para a busca do dispositivo de armazenamento do elemento digital é frequente na persecução penal.[205] Ocorre que, como ensina Nélson Hungria, o domicílio penal não é o domicílio civil (residência com ânimo definitivo[206]), "É o lugar que,

[203] Neste caso, Peter Semayne tinha uma casa com George Beriford, que faleceu devendo Semayne. Para satisfazer a dívida, Peter buscou apossar-se das terras e bens de Beriford, que estavam sob a administração de Richard Gresham. Os *sheriffs* de Londres se ofereceram para entrar na casa de Gresham para apreender bens. Gresham se opôs. No julgamento, foram discutidos os direitos contra a entrada e busca pelos *sheriffs* do rei. Foi reconhecido que Gresham estava legalmente autorizado a trancar sua porta (COKE, [1605]/2003, p. 136-141).

[204] João Gualberto Garcez Ramos (2006, p. 128-129) explica que, nos Estados Unidos, a *castle doctrine* foi utilizada pela Suprema Corte para analisar a aplicação da Quarta Emenda à Constituição: "A autoridade estatal deve respeitar os limites físicos da casa do cidadão e de seu patrimônio. Não deve invadi-la, pois a casa de um cidadão equivale ao castelo de um rei. Dentro dessa casa há como que um governo soberano, e uma outra 'soberania' não deve nela penetrar, a não ser em situações excepcionais."

[205] Vide os requisitos no item 4.3.2, *supra*.

[206] Código Civil, artigo 70.

embora sem conexão com a casa de moradia propriamente dita, serve ao exercício da atividade individual privada" sendo que "A atividade do cidadão, nos tempos modernos, é múltipla e não se exerce apenas no limite estrito da casa de moradia, e há necessidade de tutelar essa atividade em todos os lugares onde ela se abriga." (HUNGRIA, 1980, p. 217).

Manuel da Costa Andrade (2009, p. 152-153), citando o Tribunal Constitucional Federal da Alemanha, sustenta que tanto a vigilância do domicílio por tecnologias inseridas no interior do domicílio quanto a vigilância externa do espaço físico da habitação – como por microfone direcionado, câmera, drone – viola o domicílio. E que o mesmo se aplica para o ingresso remoto em computador localizado na casa e na "abertura" de sua câmera e microfone.

Em relação aos elementos digitais, parte da literatura jurídica tem defendido que a privacidade não deve ser considerada apenas em relação ao local territorial, pois o exercício da privacidade, principalmente no contexto criado pelas novas tecnologias, alcança múltiplas localidades e o espaço virtual, o que demanda, também, nova noção de domicílio, que inclua o domicílio digital (destaca-se que o crime de invasão de domicílio é localizado no Código Penal no Capítulo dos Crimes Contra a Liberdade Individual, e que a inviolabilidade do domicílio é indissociável da privacidade). Sobre este tema, Geraldo Prado (2020, p. 60) afirma que:

> O domicílio digital e a identidade digital configuram um contínuo à semelhança de uma sombra de dados que vai deixando seus rastros – invisíveis a olho nu, mas plenamente detectáveis pelo emprego da Inteligência Artificial (IA) – que, se beneficiam o titular que encarna a identidade e está ao abrigo deste domicílio, terminam por ser mais facilmente devassáveis e atingíveis que o domicílio territorial e a identidade tradicional.

Citando o julgamento do caso Katz vs. Estados Unidos pela Suprema Corte, Eloy Velasco Núñez (2016, p. 27-28) ressalta que a Quarta Emenda à Constituição dos Estados Unidos – contra buscas e apreensões arbitrárias e que assegura a privacidade e a inviolabilidade do domicílio – protege pessoas, não lugares. Somado a isso, há expectativa de privacidade nos dispositivos de uso privado – como celular, *smartphone* e *notebook* – fazendo com que seja necessária prévia autorização judicial para acessá-los (em função da reserva de jurisdição).

O Superior Tribunal de Justiça já decidiu que o acesso a elementos digitais armazenados em aparelhos celulares sem prévia autorização judicial ofende a privacidade.[207]

[207] Agravo Regimental no *Habeas Corpus* n. 542.940/SP, relator ministro Nefi Cordeiro, publicado em 10 de março de 2020; Recurso em *Habeas Corpus* n. 51.531/RO, relator ministro Nefi Cordeiro, publicado em 09 de maio de 2016. A questão será julgada pelo Supremo Tribunal Federal no Recurso Extraordinário com Agravo n.

Com relação ao domicílio digital, a noção de que ele engloba qualquer compartimento não aberto ao público onde alguém exerce atividade não é incompatível com o espaço virtual e é o conceito do Código Penal, artigo 150, § 4º, inciso III. Em primeiro lugar, grande parte da atividade diária das pessoas, incluindo o exercício profissional e comunicações privadas, é exercida no espaço virtual; e o que o artigo 150, § 4º, inciso III, visa proteger é a atividade individual privada "em todos os lugares onde ela se abriga" (HUNGRIA, 1980, p. 217). Em segundo lugar, essa noção não ofende à taxatividade penal e não aumenta quais condutas são incriminadas pelo artigo 150, sendo que, inclusive, a invasão de dispositivo informático é incriminada no tipo específico do artigo 154-A, do Código Penal – nesta leitura, o domicílio digital também é bem jurídico protegido pelo artigo 154-A[208], que tem pena de reclusão de um a quatro anos, muito superior à do artigo 150, de detenção de um a três meses, ocorrendo consunção. Em terceiro lugar, "O termo *domicílio* deve ser interpretado com a maior amplitude possível" (NUCCI, 2011, p. 211); e, por tratar de direito fundamental (Constituição, artigo 5º, inciso XI), sua eficácia deve ser a máxima (MENDES, Gilmar; BRANCO, 2015, p. 153).[209]

Para Martínez-Villalba (2014, p. 38), são consequências práticas da proteção do domicílio digital a proteção do armazenamento de dados em espaço virtual e da associação de um nome ao IP numérico (*Domain Name System*). Além disso, obviamente, somado à privacidade e à autodeterminação informativa,[210] o domicílio digital é mais um fundamento para a necessidade de prévia autorização judicial para acessar elementos digitais não abertos ao público (reserva de jurisdição; Constituição, artigo 5º, incisos XI e XXXV).

As únicas exceções à inviolabilidade do domicílio, que é garantia constitucional, estão previstas, como não poderia deixar de ser,[211] na própria Constituição (artigo 5º, inciso XI): se existir consentimento do morador; em situação de flagrante delito; em situação de desastre; para prestação de socorro; se existir prévia determinação judicial, durante o dia. O mesmo deve ser aplicado ao domicílio digital, com as observações: fora as situações de flagrante (como em crimes permanentes), as situações de desastre ou prestação de socorro são de difícil aplicação para o domicílio digital; de que o consentimento deve ser voluntário e daquele que é

1.042.075 (tema 977 de repercussão geral).

[208] Somado à "inviolabilidade dos dados informáticos" (VIANNA; MACHADO, 2013, p. 94).

[209] Martínez-Villalba (2014, p. 38) conceitua o domicílio digital como o lugar onde alguém permanece virtualmente e ninguém acessa sem seu consentimento (como páginas em redes sociais, *e-mail*, sites próprios e serviços de armazenamento em nuvem).

[210] Tratada no item 4.5, *supra.*

[211] Vez que "Os direitos fundamentais enquanto direitos de hierarquia constitucional somente podem ser limitados por expressa disposição constitucional (*restrição imediata*) ou mediante lei ordinária promulgada com fundamento na própria Constituição (*restrição mediata*)." (MENDES, Gilmar; BRANCO, 2015, p. 200).

legalmente autorizado a acessar os elementos digitais[212]; e que, diferente do lugar físico, que a polícia pode cercar e esperar amanhecer, o espaço virtual pode desaparecer definitivamente à noite, por isso e pela segurança (Constituição, art. 5º, *caput*) na acepção de ausência de perigos (SOUZA NETO, 2013, p. 231-232), a determinação judicial que autorize o acesso ao domicílio digital deve poder ser executada em qualquer horário, não somente ao dia, para compatibilizar o artigo 5º, *caput*, com o inciso XI, da Constituição (o que também viabiliza a assistência imediata pelo Sistema de Plantão 24 por 7 previsto no artigo 35 da Convenção de Budapeste).[213]

Em síntese, todo compartimento não aberto ao público onde alguém exerce atividade individual privada é protegido pela inviolabilidade do domicílio, seja no espaço real ou virtual, como já consta no artigo 150, § 4º, inciso III, do Código Penal, em interpretação conforme à Constituição, artigo 5º, inciso XI, que assegura a inviolabilidade de domicílio como direito fundamental e, consequentemente, faz com que seja interpretada com a máxima eficácia possível.

4.10.2 Cooperação internacional

Ian Brownlie sustenta que a jurisdição exclusiva sobre um território e uma população, o dever de não ingerência em outros Estados e a subordinação às obrigações criadas pelas relações internacionais apenas com o consentimento do Estado obrigado são as principais consequências da soberania e da igualdade dos Estados (BROWNLIE, 1997, p. 309).

Perante o Direito Internacional, todos os Estados são iguais, como consta na Carta das Nações Unidas, de 1945, artigo 2.1. Segundo Valerio de Oliveira Mazzuoli, são elementos dessa igualdade:

> 1) a igualdade em direitos; 2) o gozo dos direitos inerentes à plenitude da soberania; 3) o respeito à personalidade dos outros Estados; 4) a integridade territorial e a independência política; 5) a livre escolha do Estado de seu sistema político, social, econômico e cultural; e 6) o dever dos Estados em respeitar seus compromissos e de viver em paz com os outros Estados. (MAZZUOLI, 2015, p. 564).

Em respeito à soberania e à igualdade, os Estados têm o dever de não intervir na gestão interna dos outros Estados (MAZZUOLI, 2015, p. 573-575). Estes princípios das relações internacionais são previstos na Constituição, artigo 4º, incisos III, IV, V e VII. Na

[212] Tal como prevê, também, o artigo 32.b, da Convenção de Budapeste.
[213] Vide o item 4.10.2.1, *infra.*

Carta da Organização dos Estados Americanos, de maneira bastante explícita, consta que (artigo 19):

> Nenhum Estado ou grupo de Estados tem o direito de intervir, direta ou indiretamente, seja qual for o motivo, nos assuntos internos ou externos de qualquer outro. Este princípio exclui não somente a força armada, mas também qualquer outra forma de interferência ou de tendência atentatória à personalidade do Estado e dos elementos políticos, econômicos e culturais que o constituem. (ORGANIZAÇÃO DOS ESTADOS AMERICANOS, 2022).

Em função do respeito à soberania, à igualdade e à não intervenção, a realização de atos judiciais em território estrangeiro demanda a cooperação[214] entre os Estados, como por cartas rogatórias, auxílio direto e procedimento de extradição (Constituição, art. 4º, IX; art. 102, I, *g*; art. 105, I, *i*). Isso implica na inconstitucionalidade da atuação brasileira em território estrangeiro sem o cumprimento dos procedimentos de cooperação internacional (MADRUGA; FELDENS, 2015, p. 56).

A busca e a apreensão de elementos digitais em território estrangeiro obedecem aos mesmos pressupostos; com as particularidades detalhadas na sequência.

Como visto (item 4.10, *supra*), o direito nacional e o direito internacional mantêm o critério da territorialidade na determinação da competência da busca e da apreensão de elementos digitais. Em respeito às normas regentes das relações internacionais e pela manutenção do critério da territorialidade, a apreensão do dispositivo material de armazenamento de elementos digitais localizado em território estrangeiro exige a cooperação internacional (MADRUGA; FELDENS, 2015, p. 64).

Já o acesso aos elementos digitais armazenados em território estrangeiro pode ocorrer sem a necessidade de cooperação internacional se: existir o consentimento voluntário daquele legalmente autorizado a acessá-los; ou se esses elementos estiverem disponibilizados ao público (Convenção de Budapeste, artigo 32) – temas tratados nos itens 4.4 e 4.5, *supra*.

Destaca-se que o Marco Civil da Internet reconhece a escala mundial da rede (art. 2º, I) e obriga a observância da legislação brasileira a todos os atos de "coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território

[214] "[…] a cooperação judicial penal internacional pode ser esquematizada funcionalmente como um *conjunto de atividades processuais* (cuja proteção não se esgota nas simples formas), *regulares* (normais), *concretas e de diverso nível, cumpridas por órgãos jurisdicionais* (competentes) *em matéria penal, pertencentes a distintos Estados soberanos, que convergem* (funcional e necessariamente) *em nível internacional, na realização de um mesmo fim, que não é senão o desenvolvimento* (preparação e consecução) *de um processo* (principal) *da mesma natureza* (penal), *dentro de um estrito marco de garantias, conforme o diverso grau e projeção intrínseco do auxílio requerido*." (CERVINI; TAVARES, 2000, p. 51, grifo dos autores).

nacional" (art. 11, *caput*) (BRASIL, 2022b). Contudo, o Brasil não pode unilateralmente obrigar provedor sediado no estrangeiro a enviar os elementos digitais para o Brasil sem procedimento de cooperação internacional – assim como, em reciprocidade, o Estado estrangeiro não pode requerer elementos digitais de provedor sediado em território nacional sem cooperação internacional. Em função da livre iniciativa (Constituição, art. 1º, IV, e art. 170, *caput* e parágrafo único; Marco Civil da Internet, art. 2º, V), o Estado brasileiro também não pode obrigar o provedor estrangeiro a ter estabelecimento no Brasil. E:

> Autoridade judiciária brasileira tampouco pode usar de meios indiretos, igualmente à margem da cooperação jurídica internacional, para forçar o cumprimento no exterior de suas ordens judiciais ou diligências. Assim, não é dado ao juiz brasileiro poder de coagir representante ou pessoa jurídica do mesmo grupo econômico do provedor estrangeiro para, indiretamente, forçá-lo a compartilhamento dos dados eletrônicos que armazene ou hospede no exterior. Destaque-se que o representante comercial brasileiro, ainda que integrante do mesmo grupo econômico, não necessariamente tem – e a legislação brasileira não exige que o tenha – controle ou poder de acesso aos dados armazenados no exterior. (MADRUGA; FELDENS, 2015, p. 65).

A cooperação internacional, como todas as manifestações públicas e privadas, deve estrita obediência à legalidade (Constituição, artigos 4º, IX, e 5º, II). A Lei determina em normas nacionais e internacionais os procedimentos de cooperação internacional. Como requisitos gerais, o Código de Processo Civil, artigo 26, aplicado subsidiariamente ao processo penal, estabelece: o respeito ao devido processo legal no Estado requerente; a igualdade de tratamento entre nacionais e estrangeiros; a publicidade dos atos, exceto nas situações de sigilo previstas na legislação brasileira ou do Estado requerente; a existência de autoridade central para receber ou transmitir os pedidos de cooperação (se não existir prévia determinação em contrário, será o Ministério da Justiça, § 4º); a espontaneidade na transmissão de informações para Estados estrangeiros. Na ausência de tratado entre os Estados, a cooperação internacional é realizada pela via diplomática, com base na reciprocidade (§ 1º). A reciprocidade é dispensada na homologação de sentença estrangeira (§ 2º). E são inadmissíveis os atos que contrariem as normas fundamentais do Brasil, como a prova ilícita. Como observam Humberto Theodoro Júnior, Dierle Nunes, Alexandre Bahia e Fávio Quinaud Pedron (2016, p. 170): "Com tal entendimento normativo, o Brasil adota um reconhecimento dos princípios formadores do devido processo para também as relações de cooperação, bem como o tratamento isonômico (no sentido processual) e o dever de publicidade do procedimento."

Especificamente em relação à busca e à apreensão de elementos de prova digitais, são destacadamente importantes os procedimentos de carta rogatória, auxílio direto e assistência imediata pelo Sistema de Plantão 24 por 7.

No que importa a esta pesquisa, a carta rogatória passiva é procedimento para o cumprimento de ato de judiciário estrangeiro pelo judiciário brasileiro, após juízo de delibação do Superior Tribunal de Justiça sobre os requisitos procedimentais (Constituição, artigo 105, inciso I, alínea *i*; CPC, artigos 36 e 963; Regimento Interno do Superior Tribunal de Justiça, artigos 216-O a 216-X). No projeto original, o CPC previa a carta rogatória ativa no artigo 35, mas o dispositivo foi vetado pela existência de vários tratados internacionais que já preveem a cooperação direta, que é mais rápida que a carta rogatória por ser menos burocrática e não exigir juízo de delibação (MENEGUETTI PEREIRA, 2015, p. 29).

O auxílio direto é procedimento de cooperação internacional por autoridades centrais dos Estados na situação de não ser necessário o juízo de delibação do judiciário brasileiro. Pode ser pedido pela autoridade central do Brasil (auxílio direto ativo) ou ser pedido por autoridade central estrangeira (auxílio direto passivo). O auxílio direto passivo pode envolver ato judicial – situação em que a autoridade central deve instaurar o procedimento na Justiça Federal (Constituição, art. 109, III) – ou extrajudicial – em que a autoridade central deve tomar as providências administrativas cabíveis (CPC, art. 32). O auxílio direto ativo é requerido diretamente à autoridade central brasileira, que se comunica sem intermediários com a autoridade central estrangeira.

> No âmbito do auxílio direto um Estado não pede a outro que se reconheça e execute um ato jurisdicional seu, mas que se profira ato jurisdicional referente a uma determinada questão de mérito que advém de litígio em curso em seu território. Desse modo, não há, como consequência, o exercício de jurisdição pelos dois Estados envolvidos na cooperação, mas apenas pelo Estado requerido. Assim, no auxílio direto, o pleito do Estado estrangeiro será necessariamente verificado quanto ao mérito, buscando-se produzir uma decisão judicial doméstica e, como tal, não sujeita ao juízo de delibação. (MENEGUETTI PEREIRA, 2015, p. 27).

Como ressalta Ivan Jezler Júnior (2019, p. 101-103), todos os procedimentos de cooperação internacional devem utilizar canais oficiais de comunicação e seguir os requisitos estabelecidos nas normas nacionais e internacionais. A Convenção de Palermo (Convenção das Nações Unidas contra o Crime Organizado Transnacional), por exemplo, exige como requisitos do pedido de cooperação por auxílio direto (artigo 18.13) que: o pedido seja feito por escrito, em língua aceita pelo Estado requerido[215], de maneira tal que possibilite atestar a

[215] Destaca-se que o Código de Processo Civil, aplicado subsidiariamente ao processo penal, determina: "Art. 192. Em todos os atos e termos do processo é obrigatório o uso da língua portuguesa. Parágrafo único. O

sua autenticidade (artigo 18.14); a indicação do emitente; o objeto da investigação; o nome e as funções do órgão competente para a investigação; resumo dos fatos relevantes; descrição detalhada da cooperação pretendida; se possível, identidade, endereço e nacionalidade das pessoas investigadas; e descrição da finalidade da cooperação (artigo 18.15).

4.10.2.1 Convenção de Budapeste: medidas prévias à apreensão e o Sistema de Plantão 24 por 7

A Convenção de Budapeste (Convenção sobre o Cibercrime) padronizou procedimentos de cooperação internacional relacionados aos elementos digitais para facilitar a sua obtenção, conservação e comunicação rápida entre os Estados signatários.[216]

Este item tem como objeto normas gerais de cooperação internacional previstas na Convenção de Budapeste e medidas prévias à apreensão que ela prevê (o procedimento dos artigos 19.1.b e 31 será objeto do próximo item).

A Convenção exige comunicação formal pelo Estado para o requerimento de todos os procedimentos de cooperação, salvo na situação de urgência, em que é aceita a comunicação por *e-mail*, desde que com adequado nível de segurança (por exemplo, com uso de criptografia) e possibilidade de autenticação da comunicação (artigo 25.3); neste caso, o Estado requerido também pode exigir posterior confirmação formal.

Especificamente sobre o auxílio direto, a Convenção de Budapeste prevê situações em que a cooperação pode ser recusada (artigo 27.4): se o Estado requerido considerar ser relacionado a delito político ou conexo, ou se o Estado requerido considerar que a cooperação pode prejudicar sua soberania, segurança ou outros interesses (o que abre margem para várias situações de recusa – como não poderia deixar de ser, já que a cooperação é um ato espontâneo de exercício da soberania). O pedido também pode ser adiado se sua execução puder prejudicar os procedimentos do próprio Estado requerido e pode ser atendido apenas parcialmente (artigo 27.5). E o Estado requerido pode condicionar a cooperação à manutenção de sigilo e à não utilização em procedimento diverso do indicado no pedido (artigo 28).

A Convenção de Budapeste trata nos artigos 16 e 29 de um procedimento de auxílio direto específico, prévio a outras medidas como a busca e a apreensão: a conservação expedita de dados armazenados em computador. Nos artigos 17 e 30 ela trata do procedimento de

documento redigido em língua estrangeira somente poderá ser juntado aos autos quando acompanhado de versão para a língua portuguesa tramitada por via diplomática ou pela autoridade central, ou firmada por tradutor juramentado." (BRASIL, 2022c).

[216] Vide o item 4.2.1, *supra.*

revelação dos dados. Por esses procedimentos, dados específicos de computador, incluindo dados de tráfego (dados referentes a uma comunicação por computador, que indicam IP, rota do envio dos pacotes, horário, duração da comunicação e tipo de serviço utilizado; artigo 1.d), facilmente eliminados e modificados, visam ser preservados por ordem a um provedor de serviços ou pessoa que tenha a posse do dispositivo ou controle de acesso. Diferente da busca por ingresso remoto do artigo 19.1.a, que não tem previsão legal no sistema jurídico brasileiro[217], a preservação expedita de dados armazenados e a sua revelação são previstas no Marco Civil da Internet.

Nos termos da Lei n. 12.965, de 2014 (BRASIL, 2022b), os registros de conexão (informações sobre a data e horário de início e de término, duração e endereços de IP de uma conexão à internet; art. 5º, VI) devem ser guardados em sigilo, num ambiente controlado e de segurança, pelo período – prorrogável – de um ano (art. 13), pelo administrador de sistema autônomo (pessoa física ou jurídica que administra blocos de endereço de IP específicos e sistema autônomo de roteamento, cadastrada no Núcleo de Informação e Coordenação do Ponto BR[218]; art. 5º, IV). Os registros de acesso a aplicações de internet (informações sobre a data e hora do uso de uma aplicação de internet por um IP; art. 5º, VIII), consentidos pelo usuário (art. 16, I), devem ser guardados pelo provedor de aplicações de internet[219] (constituído como pessoa jurídica, que exerça atividade organizada, profissional e com finalidade econômica) em sigilo, num ambiente controlado e de segurança, pelo período de seis meses (art. 15, *caput*). Mediante ordem judicial, outros provedores de aplicações de internet (que não sejam constituídos como pessoa jurídica, não exerçam atividade organizada ou profissional ou com finalidade econômica) podem ser obrigados a guardar registros de acesso a aplicações de internet, desde que relativos a fatos específicos em período determinado (art. 15, § 1º). Após guardados, o acesso aos registros depende de ordem judicial específica (art. 13, § 5º, e art. 15, § 3º) sobre pedido que contenha indícios concretos da ocorrência de ilícito, demonstração da necessidade dos registros solicitados para a investigação ou instrução probatória, e indicação do período ao qual se referem os registros (art. 22).

[217] Vide o item 4.3.2, *supra.*

[218] O Decreto da Presidência da República n. 4.829, de 3 de setembro de 2003, art. 1º, II, atribuiu ao Comitê Gestor da Internet no Brasil o registro e distribuição de endereços de IP ".br". Pela Resolução n. 001/2005, art. 1º, o Comitê Gestor da Internet no Brasil atribuiu ao Núcleo de Informação e Coordenação do Ponto BR a operacionalização do registro e distribuição de endereços de IP ".br".

[219] É vedado que o provedor da conexão (o responsável pela transmissão, comutação ou roteamento de pacotes de dados pela internet; art. 9º) bloqueie, monitore, filtre ou analise o conteúdo dos pacotes de dados e, também, é vedado que ele guarde os registros de acesso a aplicações de internet (artigos 9º, § 3º, e 14, da Lei n. 12.965, de 2014).

A Convenção de Budapeste (artigo 29.2) determina que o pedido de cooperação para a conservação expedida de dados armazenados em computador deve especificar: o órgão requerente; o crime investigado ou objeto de ação penal; breve resumo dos fatos; os dados armazenados a serem conservados; a relação desses dados com o crime; informações que identifiquem o detentor dos dados ou a localização do armazenamento; a necessidade de conservação; que o Estado requerente pretende apresentar pedido futuro de cooperação para busca, acesso, apreensão, guarda ou revelação dos dados armazenados em computador.

Como a Convenção de Budapeste deve ser interpretada em conjunto com o Marco Civil da Internet, apenas os registros de conexão e os registros de acesso a aplicações de internet podem ser objeto da cooperação internacional pelo procedimento do artigo 29 da Convenção de Budapeste, vez que os demais dados armazenados por computador não são objeto do dever de guarda na Lei n. 12.965, de 2014, e "ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei" (Constituição, artigo 5º, inciso II [BRASIL, 2020a]).

Pela mesma razão, a ausência de previsão legal (Constituição, artigo 5º, inciso II) – somada às potenciais ofensas à privacidade, à autodeterminação informativa e à proteção contra a autoincriminação[220] –, é inconstitucional a recomendação do artigo 18.1.a da Convenção de Budapeste, sobre o procedimento de ordem de exibição "a qualquer pessoa residente em seu território a entregar dados de computador especificados, por ela controlados ou detidos, que estejam armazenados num sistema de computador ou em qualquer meio de armazenamento de dados de computador" (BRASIL, 2021c, p. 18) – procedimento direcionado para que qualquer pessoa que tenha o acesso imediato aos dados (pela detenção física do dispositivo de armazenamento) ou acesso remoto (pelo controle do seu conteúdo) seja obrigada a exibi-los (RAMALHO, 2019, p. 268-269).

A recomendação do artigo 18.1.b da Convenção de Budapeste, de criação de procedimento para que o provedor de serviço forneça informações cadastrais de seus assinantes em situações específicas (para a Convenção, artigo 18.3, qualquer informação relativa ao assinante, exceto dados de tráfego e de conteúdo da comunicação), tem previsão legal para o fornecimento da qualificação pessoal, filiação e endereço, independente de autorização judicial: Código de Processo Penal, artigo 13-A; Lei 9.613, de 1998, artigo 17-B; Lei 12.850, de 2013, artigo 15; Lei 12.965, de 2014, artigo 10, § 3º.[221] Sobre isso, são devidas

[220] Vide os itens 4.5 e 5.3.1.

[221] A inconstitucionalidade da Lei 13.344, de 2016, que inseriu os artigos 13-A e 13-B no CPP, por ofensa à privacidade, está sob julgamento do Supremo Tribunal Federal na Ação Direta de Inconstitucionalidade n. 5.642. Com base no julgamento do Recurso Extraordinário n. 418.416, que entendeu que o art. 5º, XII, da Constituição, protege a comunicação das informações e não as informações, o Supremo Tribunal Federal firmou

as observações de Gustavo Badaró e Pierpaolo Bottini (2012, p. 356), em relação à Lei 9.613, de 1998, mas também aplicável às demais, por todas restringirem[222], nos artigos mencionados, o fornecimento de informações cadastrais sem prévia autorização judicial à qualificação pessoal, filiação e endereço:

> Ter acesso aos dados cadastrais de sicrano, não se confunde com solicitar informação se sicrano tem alguma conta de *e-mail* ou que é o titular e quais são os dados cadastrais de que utiliza um determinado *e-mail* ou criou um site específico. Em suma, nos estritos limites dos elementos cadastrais especificados no art. 17-B, e apenas para as entidades nela mencionadas, poderão ser que obtidos dados que "informam qualificação pessoal, filiação e endereço".

A Convenção de Budapeste também criou o Sistema de Plantão 24 por 7 para a cooperação internacional (artigo 35). Esse Sistema consiste no estabelecimento de um órgão de contato em cada Estado Parte, composto por pessoal treinado e equipado, disponível vinte e quatro horas por dia, sete dias por semana, para promover a assistência imediata para procedimentos relacionados a crimes cometidos por computador ou para obter elementos digitais sobre um delito. Entre as medidas de assistência, a Convenção elenca o fornecimento de suporte técnico, a preservação de dados, a obtenção de elementos de prova, o fornecimento de informações jurídicas do Estado requerido e a localização de suspeitos (RAMALHO, 2019, p. 72).[223]

Finalmente, nem a conservação expedida de dados armazenados em computador (artigo 29, da Convenção), nem o Sistema de Plantão 24 por 7, nem quaisquer outros atos de cooperação internacional podem ofender a proteção contra a autoincriminação ou qualquer outra garantia componente do modelo constitucional do processo (Constituição, artigo 5º, LIV; Código de Processo Civil, artigo 26, inciso I).

4.11 Modalidades de busca de elementos de prova digitais

jurisprudência no sentido da constitucionalidade do fornecimento das informações de informações cadastrais pelos provedores de serviço (por exemplo: julgamentos do *Habeas Corpus* n. 91.867 e do Agravo Regimental em *Habeas Corpus* n. 124.322). O tema será detalhado no item seguinte.

[222] Em exceção apenas o CPP em relação ao tráfico de pessoas, sequestro e cárcere privado, que não especifica as informações no artigo 13-A.

[223] A assistência mútua na interceptação de dados de tráfego em tempo real (artigos 20 e 33 da Convenção de Budapeste) e assistência mútua em relação à interceptação do conteúdo de comunicações (artigos 21 e 34) não são objetos desta tese. Sobre a interceptação telemática, vide: Sidi (2016). A medida dos artigos 19.1.b e 31 da Convenção será tratada no próximo item.

A premissa jurídica sobre a busca, a apreensão e a multiplicidade de técnicas relacionadas aos elementos digitais é a distinção entre o armazenamento dos elementos e a sua comunicação.

Para Tércio Sampaio Ferraz Júnior (1993, p. 446-448) a proteção do inciso XII, do artigo 5º, da Constituição, não é referente ao conteúdo da comunicação, mas à ação de comunicar-se. Dividindo o inciso XII em dois blocos, um composto pelo sigilo da correspondência e das comunicações telegráficas e o outro pelo sigilo de dados e das comunicações telefônicas, Ferraz Júnior defende que a instantaneidade da comunicação por telefone demanda, para atendimento de interesse público da persecução penal, a violação do sigilo da comunicação enquanto ela ocorre, de maneira a preservar a comunicação, mas, ao mesmo tempo, conhecer o seu conteúdo que não deixa vestígios.

O Supremo Tribunal Federal endossou esta noção no julgamento do Recurso Extraordinário n. 418.416/SC, ocasião em que entendeu: "A proteção a que se refere o art. 5º, XII, da Constituição, é da comunicação de 'dados' e não dos 'dados em si mesmos', ainda quando armazenados em computador" (BRASIL, 2022h).[224]

A distinção entre as técnicas de obtenção de elementos digitais parte daí: para a sua obtenção durante a comunicação, é necessária a interceptação telemática (a telemática é a resultante da união da telecomunicação[225] com a informática[226] [SIDI, 2016, p. 69]) prevista na Lei 9.296, de 1996; para a obtenção dos elementos digitais em dispositivo de armazenamento ou pela internet, são necessárias outras técnicas, como a busca e a apreensão (de situação legislativa descrita no item 4.2, *supra*).

A busca de elementos de prova digitais é meio oculto de investigação consistente na procura do elemento por técnicas operadas sem conhecimento do investigado; pode envolver coerção ou não e ser cautelar ou não (conceito construído no item 4.1, *supra*).

A Convenção de Budapeste, artigo 19, prevê que a busca de elementos digitais pode ocorrer por ingresso remoto no computador ou materialmente (nesta última modalidade, visando o dispositivo de armazenamento dos elementos digitais).

Manuel da Costa Andrade (2009, p. 150, 160, 168) pontua que a busca *online* por ingresso remoto não pode ser feita sem lei prévia baseada em "fortes e extremamente

[224] Lawrence Lessig (2006, p. 202-203) também distingue a vigilância entre duas dimensões, a do monitoramento dos eventos efêmeros e a da procura pelos registros dos eventos, que interagem entre si.
[225] "[…] Telecomunicação é a transmissão, emissão ou recepção, por fio, radioeletricidade, meios ópticos ou qualquer outro processo eletromagnético, de símbolos, caracteres, sinais, escritos, imagens, sons ou informações de qualquer natureza." conforme o artigo 60, § 1º, da Lei 9.472, de 1997 (BRASIL, 2022i).
[226] "A ciência que tem como objeto de estudo as informações automatizadas (dados) é a Informática" (VIANNA; MACHADO, 2013, p. 21).

exigentes critérios de *proporcionalidade*"; a mesma consideração é pertinente ao sistema jurídico brasileiro. E, como dito no item 4.3.2, *supra*, em respeito à legalidade e ao processo legislativo, apenas com lei futura de iniciativa da União será válida a busca por ingresso remoto recomendada pela Convenção de Budapeste no artigo 19.1.a.

Outra modalidade sem previsão legal é o espelhamento. Essa modalidade consiste na sincronização do uso de uma aplicação em mais de um sistema informático. Um caso concreto envolvendo o espelhamento foi analisado pelo Superior Tribunal de Justiça no julgamento do Recurso em *Habeas Corpus* n. 99.735/SC, de relatoria da ministra Laurita Vaz:

> No caso dos autos, o Poder Judiciário deferiu pedido da Autoridade Policial no sentido de apreender o celular de A. C. DA C. Diante da autorização judicial, o Recorrente foi abordado em 17/11/2017 pelo Delegado de Polícia e por policiais, os quais operacionalizaram a medida (fl. 175, nota de rodapé). O espelhamento das mensagens do WhatsApp ocorre em sítio eletrônico disponibilizado pela própria empresa, denominado WhatsApp Web (https://web.whatsapp.com/). Na referida plataforma, é gerado um tipo específico de código de barras, conhecido como Código QR (*Quick Response*), o qual só pode ser lido pelo celular do usuário que pretende usufruir do serviço. Daí a necessidade, enfatizada pela Autoridade Policial, de apreensão, ainda que por breve período de tempo, do aparelho telefônico de A. C. DA C. A leitura do Código QR pode ser realizada com a opção "Mantenha-me conectado", hipótese em que o emparelhamento entre o celular e o computador ocorrerá por tempo indeterminado, até que o usuário, via celular ou via WhatsApp Web, decida encerrar o mencionado aparelhamento. Na hipótese dos autos, após a apreensão do celular, a Autoridade Policial procedeu em sigilo – isto é, sem comunicar ao Recorrente – ao emparelhamento das plataformas, tendo, logo após, devolvido a ele a posse do aparelho. Isso permitiu aos investigadores não apenas o acesso a todas as conversas – conteúdo das mensagens e dados anexados – que já estavam registradas no WhatsApp do Recorrente (*ex tunc*), independentemente da antiguidade ou do destinatário, como também o acompanhamento, dali para frente (*ex nunc*), de todas as conversas que fossem iniciadas pelo Recorrente ou por algum de seus contatos. Mas não é só. Para além de permitir o acesso ilimitado a todas as conversas passadas, presentes e futuras, a ferramenta WhatsApp Web foi desenvolvida com o objetivo de possibilitar ao usuário a realização de todos os atos de comunicação a que teria acesso no próprio celular. O emparelhamento entre celular e computador autoriza o usuário, se por algum motivo assim desejar, a conversar dentro do aplicativo do celular e, simultaneamente, no navegador da internet, ocasião em que as conversas são automaticamente atualizadas na plataforma que não esteja sendo utilizada. Ainda mais relevante para a discussão presente nestes autos é o seguinte detalhe: tanto no aplicativo, quanto no navegador, é possível, com total liberdade, o envio de novas mensagens e a exclusão de mensagens antigas (registradas antes do emparelhamento) ou recentes (registradas após), tenham elas sido enviadas pelo usuário, tenham elas sido recebidas de algum contato. Não bastasse, eventual exclusão de mensagem enviada (na opção "Apagar somente para Mim") ou de mensagem recebida (em qualquer caso) não deixa absolutamente nenhum vestígio, seja no aplicativo, seja no computador emparelhado, e, por conseguinte, não pode jamais ser recuperada para efeitos de prova em processo penal, tendo em vista que a própria empresa disponibilizadora do serviço, em razão da tecnologia de encriptação ponta-a-ponta, não armazena em nenhum servidor o conteúdo das conversas dos usuários. (BRASIL, 2022j).

Esta técnica não obtém apenas elementos digitais armazenados (por exemplo, os registros das comunicações por uma aplicação), ela também possibilita a interceptação da comunicação enquanto ela ocorre, que um agente se passe pelo investigado ou por terceiro e que registros antigos sejam excluídos sem deixar rastros. Ou seja, é uma Quimera que mistura a busca, a apreensão, a interceptação telemática e a infiltração de agentes, sem confiabilidade, integridade, disponibilidade (completude, autenticidade, reprodutibilidade), transparência técnica, rastreabilidade e auditabilidade.[227]

No caso, o Superior Tribunal de Justiça entendeu que: não há previsão legal do espelhamento no sistema jurídico brasileiro; por possibilitar que o agente atue não como observador, como na interceptação, mas como participante da conversa, com engano a terceiro, não é admissível a analogia da técnica de espelhamento com a interceptação; pela possibilidade de exclusão de mensagens sem deixar vestígios, o espelhamento impede a produção de contraprova pelo investigado – o que ofende a ampla defesa –; como o espelhamento possibilita o acesso ao registro de comunicações ocorridas antes da autorização judicial, ele viabiliza o acesso a registros de qualquer comunicação e de períodos em que não existia autorização judicial – o que viola a inafastabilidade da jurisdição e a proporcionalidade –. Por isso, a técnica do espelhamento configura prova ilícita (BRASIL, 2022j) (MACHADO, 2020, p. 210).

Cleunice Pitombo (2005) elenca cinco modalidades lícitas de busca.

Primeira, a busca domiciliar (CPP, art. 240, § 1º). Frente à inviolabilidade do domicílio (Constituição, art. 5º, inciso XI), o ingresso domiciliar só pode ocorrer com consentimento livre, expresso e informado do morador[228]; em situação de flagrante delito (CPP, art. 302); em caso de desastre ou para prestar socorro; com prévia autorização judicial (que cumpra os requisitos legais, descritos no item 4.3.2, *supra*); ou, em estado de sítio[229] (Constituição, art. 139, inciso V). O artigo 293 do Código de Processo Penal trata, também, da situação em que pessoa cuja prisão foi determinada em mandado entrou ou se encontra em alguma casa. Neste caso, o morador deve ser intimado a entregá-la (se não o fizer, pode responder pelo crime de favorecimento pessoal do artigo 348, do Código Penal). Contudo, o morador que recusa o ingresso em seu domicílio à noite age em exercício regular do direito à inviolabilidade do

[227] Conceitos tratados no item 5.1.1, *infra.*
[228] Vide o item 4.4, *supra.*
[229] "O *estado de sítio* consiste, pois, *na instauração de uma legalidade extraordinária, por determinado tempo e em certa área* (que poderá ser o território nacional inteiro), *objetivando preservar ou restaurar a normalidade constitucional, perturbada por motivo de comoção grave de repercussão nacional ou por situação de beligerância com Estado estrangeiro*. A aplicação de medidas coercitivas e a suspensão de direitos e garantias constitucionais são apenas meios para a consecução de seus objetivos." (AFONSO DA SILVA, 1999, p. 742, grifo do autor).

domicílio (CP, art. 23, III; Constituição, art. 5º, XI; CPP, art. 293) e o morador é isento de pena se o fugitivo for seu ascendente, descendente, cônjuge ou irmão (CP, art. 348, § 2º). Ressalta-se que "tão só, mandado de prisão, não autoriza a entrada em casa alheia" (PITOMBO, Cleunice, 2005, p. 137-138), e que o executor – necessariamente agente público (CPP, arts. 6º, II, e 250)[230] – deve ter certeza de que a pessoa procurada se encontra na casa, apenas a suspeita não é suficiente, já que o Código exige ao executor "verificar, com segurança" (art. 293) (BRASIL, 2021a).

Segunda, a busca pessoal (CPP, art. 240, § 2º). Se existir fundada suspeita de que a pessoa oculta arma proibida, coisa obtida por meio criminoso, instrumento do crime ou elemento de prova, é válida a busca pessoal mediante prévia autorização judicial, em função da inafastabilidade da jurisdição nas potenciais ofensas à dignidade, à privacidade, à proibição da tortura, à vedação de autoincriminação e à proteção dos dados pessoais (Constituição, artigos: 1º, III; 5º, III, X, XXXV, XLIX, LXIII e LXXIX). Os mesmos requisitos da busca domiciliar devem ser cumpridos na busca pessoal[231]; somado a eles, a busca feita em mulher deve ser executada por mulher (CPP, art. 249). Excepcionalmente, a busca pessoal pode ser executada sem mandado nas situações de: prisão[232]; fundada suspeita, em elementos de informação concretos, de que a pessoa possua arma proibida ou elementos que constituam o corpo de delito; durante a realização da busca domiciliar; ou com o consentimento livre, expresso e informado da pessoa que sofrerá a busca (CPP, art. 244). Em todas as situações, obviamente, os direitos fundamentais devem ser respeitados (PITOMBO, Cleunice, 2005, p. 144, 149, 152, 158-159).[233]

Terceira, a busca em veículos. Cleunice Pitombo (2005, 160-163) explica que esta modalidade é regida em acordo com o uso do veículo: se a pessoa utiliza o veículo como habitação privada, como a cabine de caminhão ou o trailer, as normas referentes à busca

[230] "Como providência de natureza coercitiva, a busca e a apreensão só pode ter como *sujeitos ativos* as autoridades públicas incumbidas da investigação e da persecução penal, bem como os seus respectivos agentes." (GRINOVER, 2000, p. 480, grifos da autora).

[231] "Recorde-se de que as regras para a busca domiciliar e pessoal estão disciplinadas em conjunto. O legislador, quando quis excepcionar, o fez expressamente (art. 249 do CPP)" (PITOMBO, Cleunice, 2005, p. 150). Vide os itens 4.3.2 e 4.8, *supra.*

[232] Sendo que "[...] a autorização excepcional, conferida ao cidadão para prender quem esteja em situação de flagrante delito, não implica a extensão ao particular de outros poderes, senão aqueles essencialmente necessários para realizar o ato permitido pelo art. 301, CPP, o que não inclui, evidentemente, o direito de acesso ao domicílio alheio para *investigar* a possível ocorrência de crime. Fora da permissão legal, sua atuação será *ilegal*, senão até mesmo *criminosa*." (GRINOVER, 2000, p. 483, grifos da autora).

[233] Conforme Francisco Cangerena Neto (2018, p. 36): "A experiência do policial na localização de determinado objeto relacionado ao crime auxilia na escolha, bem como o uso de ferramentas eletrônicas ou mecânicas como aparelhos de raio x, bastões detectores de metal e scanners corporais ajudam a evitar revistas invasivas e desnecessárias."

domiciliar são aplicáveis (conceito consonante com o Código Penal, art. 150, § 4º); se o veículo é utilizado para transporte, devem ser aplicadas as normas da busca pessoal.

Quarta, busca em lugar público. O processo penal não regulamenta especificamente a matéria. Segundo o Código Civil (art. 99), são bens públicos os de uso comum de todos (como estradas, ruas, praças, mares e rios), os de uso especial (como imóveis que servem à administração dos entes da federação, inclusive os das autarquias) e os dominicais (patrimônio das pessoas jurídicas de direito público) (BANDEIRA DE MELLO, 2009, p. 904). Nos locais de uso comum, não é necessária prévia autorização judicial. Nos de uso especial é exigida a autorização judicial prévia ou o consentimento do representante do órgão competente – "Lembre-se que a categoria abrange as repartições públicas, navios de guerra, aeronaves oficiais, mercados municipais, teatros públicos e os cemitérios" (PITOMBO, Cleunice, 2005, p. 165-166) –; assim como nos dominicais (como em terras devolutas).

Quinta, busca em lugar resguardado pelo sigilo. Existem atividades cujo sigilo é dever, como a advocatícia, a médica, a psicológica e a sacerdotal. Cada uma delas têm regulamentação específica do dever de sigilo e proteção legal distinta.

No geral, o artigo 246 do Código de Processo Penal determina que para a busca no lugar não aberto ao público onde alguém exerce profissão ou atividade (conceito consonante ao do art. 150, § 4º, III, do Código Penal) são necessários os mesmos requisitos da busca domiciliar.[234]

Cabe destacar os limites da busca relacionados ao exercício advocatício. O dever de sigilo da advocacia (Lei 8.906, de 1994, art. 34, VII; CP, art. 325) é protegido por diversas normas (Constituição, art. 133; CPP, art. 243, § 2º; Lei 8.906, de 1994, art. 7º, II[235], XIX e §§ 6º a 6º-I). A advocacia é especialmente protegida por ser serviço público e função social (Lei 8.906, de 1994, art. 2º, §§ 2º e 2º-A) indispensável para a jurisdição[236]; ao proteger seu exercício o legislador assegura não os interesses de uma entidade de classe, mas a possibilidade do exercício da ampla defesa (SOARES, 2016, p. 43). Por isso, a legislação supracitada proíbe a apreensão de documento em posse do defensor, exceto se consistir elemento do corpo de delito, e somente autoriza a busca e a apreensão em advogado por

[234] Portanto, os estabelecimentos empresariais estão sujeitos à proteção contra o ingresso não consentido; como já decidiu o Supremo Tribunal Federal nos julgamentos dos *Habeas Corpus* n. 106.566/SP e *Habeas Corpus* n. 93.050/RJ.

[235] "Tal inciso impede que policiais por exemplo possam grampear as ligações telefônicas do advogado para que possa prender o[u] provar determinado crime praticado pelo cliente do advogado. Também seu escritório de advocacia, sua pasta ou outros documentos que o advogado possua são invioláveis e não podem ser utilizados para produção da prova ou qualquer questão que importe em prejuízo do direito de defesa." (SOARES, 2016, p. 43).

[236] "[…] a expressão 'administração da justiça', destituída de sentido técnico, só pode ser entendida como a função jurisdicional ou a jurisdição […]" (BRÊTAS, 2016c, p. 18).

decisão judicial fundamentada em elementos informativos concretos e prévios de autoria e materialidade de que ele tenha cometido crime – sendo que apenas elementos produzidos por colaboração premiada são insuficientes –; situação em que os atos de execução da decisão judicial devem ser cumpridos na presença de representante da Ordem dos Advogados do Brasil e em que é proibido o uso posterior de documentos, mídias e objetos pertencentes aos clientes do advogado, assim como dos dispositivos que contenham informações relacionadas aos clientes. Somado a isso, a data, o horário e o local da análise dos elementos apreendidos devem ser comunicados à seccional da OAB com ao menos vinte e quatro horas de antecedência (exceto em casos de urgência devidamente fundamentados pelo juízo); e, em qualquer momento que ocorram, todos os atos de análise podem ser acompanhados pelo investigado e por representante da OAB, para fiscalizar a análise e assegurar que elementos não relacionados à investigação não sejam analisados.

Cabe destaque, também, a vedação da busca e da apreensão em função da imunidade diplomática. Amparadas na Constituição (artigo 5º, § 2º) e no Código de Processo Penal (artigo 1º, inciso I), certas relações internacionais têm regulamentação própria. A Convenção de Viena sobre Relações Diplomáticas, de 1961 (promulgada pelo Decreto n. 56.435, de 1965), assegura que o agente diplomático tem imunidade de jurisdição penal do Estado acreditado (art. 31.1), não pode ser preso e é inviolável (art. 29)[237] – o que não o isenta da jurisdição do Estado acreditante (art. 31.4) –. Agente diplomático é o chefe da missão[238] e demais diplomatas que a componham (art. 1, alíneas *a*, *d* e *e*). E os locais da missão (edifícios e terrenos utilizados para as finalidades da missão, e a residência do chefe da missão, art. 1.i) são invioláveis; sem o consentimento do chefe da missão, os agentes do Estado acreditado não podem adentrar-lhes. Tanto os locais da missão, como os bens nele situados, a residência particular do agente diplomático e os veículos de transporte da missão não podem ser objeto de busca, requisição, embargo ou medida executiva (arts. 22, 30, 45.a). A Convenção de Viena sobre Relações Consulares, de 1963 (promulgada pelo Decreto n. 61.078, de 1967), também protege os locais consulares (art. 31) – que só podem ser adentrados com o consentimento do chefe da repartição consular (art. 31.2) –, os documentos consulares (art. 33) e os funcionários consulares (art. 41) contra buscas e apreensões; sendo que os funcionários e empregados consulares tem imunidade de jurisdição penal no exercício de suas funções (art. 43.1) (PRADO, Luiz, 2010, p. 204-206).

[237] Assim como os membros da família do agente diplomático que com ele vivam (arts. 37 e 39.3, da Convenção de Viena sobre Relações Diplomáticas, de 1961).

[238] Embaixadores, núncios (representantes religiosos), enviados, ministros, internúncios e encarregados de negócios acreditados perante os ministros das relações exteriores (art. 14, da Convenção de Viena sobre Relações Diplomáticas, de 1961).

A busca específica de elementos digitais pode ocorrer a partir da procura pelo dispositivo de armazenamento dos elementos digitais pelas modalidades descritas acima e, também, pode ocorrer por mais quatro modalidades.

Pode ocorrer pelo consentimento voluntário de quem legalmente pode acessar e revelar os elementos digitais (Convenção de Budapeste, artigo 32.b); tratada no item 4.4, *supra*.

Pode ocorrer em elementos digitais disponibilizados ao público (Convenção de Budapeste, artigo 32.a) – respeitada a autodeterminação informativa (tratada no item 4.5, *supra*) –; o que é viabilizado, por exemplo, pelo uso de buscadores (como o Google) ou aplicações específicas (como o Maltego).[239]

Pode ocorrer pela requisição das informações cadastrais de qualificação pessoal, filiação e endereço; tratada no item 4.10.2.1, *supra*.

E pode ocorrer pela requisição de registros de conexão ou de acesso a aplicações de internet (art. 22 do Marco Civil da Internet); também tratada no item 4.10.2.1, *supra.*

Esta última modalidade tem possibilitado uma das técnicas de vigilância de maior escala na sociedade de controle (item 2.2, *supra*): a quebra do sigilo em massa.

A quebra do sigilo em massa consiste na revelação, pelos provedores de conexão e de aplicações de internet, dos registros de atividade de usuários não identificados previamente pelos órgãos oficiais, a partir de critérios arbitrários de procura, como transitar num certo lugar num determinado período ou pesquisar alguma palavra em mecanismo de busca (MOURA; MARCHIONATTI, 2020, p. 459-460).

No julgamento do Recurso em Mandado de Segurança n. 61.302, a maioria dos ministros do Superior Tribunal de Justiça entenderam que não há necessidade de especificação da pessoa cujos dados são requeridos e que a medida é lícita:

> Os arts. 22 e 23 do Marco Civil da Internet, que tratam especificamente do procedimento de que cuidam os autos, não exigem a indicação ou qualquer elemento de individualização pessoal na decisão judicial. Assim, para que o magistrado possa requisitar dados pessoais armazenados por provedor de serviços de internet, mostra-se satisfatória a indicação dos seguintes elementos previstos na lei: a) indícios da ocorrência do ilícito; b) justificativa da utilidade da requisição; e c) período ao qual se referem os registros. Não é necessário, portanto, que o magistrado fundamente a requisição com indicação da pessoa alvo da investigação, tampouco que justifique a indispensabilidade da medida, ou seja, que a prova da infração não pode ser realizada por outros meios, o que, aliás, seria até, na espécie – se houvesse tal obrigatoriedade legal – plenamente dedutível da complexidade e da dificuldade de identificação da autoria mediata dos crimes investigados. (BRASIL, 2022k).

[239] Vide a Figura 4, *supra.*

Obtidos os elementos digitais requeridos, eles são cruzados com outros dados e informações para encontrar suspeitos, utilizando-se inteligência artificial ou não.[240]

Como observou o ministro Sebastião Reis Júnior no voto vencido do julgamento do Recurso em Mandado de Segurança n. 61.302 (BRASIL, 2022k, p. 34-35), a medida: ofende a privacidade de vários usuários [inclusive de terceiros em nada relacionados ao caso penal]; descumpre o art. 11, § 3º, do Decreto n. 8.771, de 2016 (regulamentação do Marco Civil da Internet) que proíbe pedidos que não especifiquem os indivíduos e as informações requeridas, e veda expressamente pedidos coletivos, genéricos ou inespecíficos[241]; é ilegal se não existir fundamentação concreta sobre a sua necessidade e extensão.

Somado a isso, em primeiro lugar, deve ser entendido que os registros de conexão e de acesso a aplicações da internet, segundo o Marco Civil da Internet (Lei 12.965, de 2014), são, respectivamente: informações sobre a data e horário de início e de término, duração e endereços de IP de uma conexão à internet (art. 5º, VI); e informações sobre a data e hora do uso de uma aplicação de internet por um IP (art. 5º, VIII), consentidos pelo usuário (art. 16, I). Nem a Lei impõe como dever a guarda do registro de termos procurados em mecanismos de busca ou registro de geolocalização, nem a medida do artigo 22 trata disso. O *caput* do artigo é expresso:

> A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet (BRASIL, 2022b)

Assim, por ausência de previsão legal, a quebra de sigilo de dados em massa com base em critérios arbitrários de procura é inadmissível no Direito Brasileiro. A medida do artigo 22 só pode ser utilizada para a requisição de data, hora, duração e endereço de IP guardadas pelo provedor da conexão ou de aplicação de internet. E sua requisição deve ser específica. É o que determina o artigo 5º, incisos VI e VIII, em cúmulo ao artigo 22 da Lei 12.965, de 2014, somados ao art. 11, § 3º, do Decreto n. 8.771, de 2016, e à Constituição, artigo 5º, inciso II.

Em segundo lugar, a medida ofende a dignidade[242], vez que o terceiro não é considerado como um fim em si, mas como meio para que o Estado persiga outra pessoa.

[240] Vide o item 4.6, *supra.*
[241] O que é previsto no Decreto n. 8.771, de 2016, art. 11, § 3º, para a requisição de informações cadastrais, mas também deve ser exigido para as demais requisições de informações dos usuários (registros de conexão e de acesso a aplicações de internet), mais íntimas e protegidas pela Lei n. 12.965, de 2014, arts. 22 e 23, e que exigem prévia autorização judicial.
[242] Vide o item 5.3.1, *infra.*

Em terceiro lugar, a medida ofende a autodeterminação informativa, vez que não há consentimento prévio do usuário para que suas informações e dados sejam utilizados pela persecução penal (item 4.5, *supra*).

Em quarto lugar, a Lei (além de não regulamentar) não restringe a quebra do sigilo em massa a um catálogo restrito de crimes, o que configura ofensa à proporcionalidade, vez que medida tão ofensiva à privacidade não pode ser autorizada para crimes que não sejam graves (item 4.3.2, *supra*).

Finalmente, como Deleuze explicitou: "Num regime de controle nunca se termina nada" (DELEUZE, 2008a, p. 216). Acreditar que a tecnologia de quebra do sigilo em massa será utilizada para situações pontuais é ingenuidade inadmissível e autocontradição lógica: por ser em massa ela não distingue investigados ou acusados de todos os demais e, também, não obtém elementos digitais apenas de um evento específico, mas, sim, *big data* sobre uma multidão de eventos que, em maioria, em nada se relacionam com o caso penal. Poucas tecnologias apresentam tanta magnitude de vigilância. Seu uso – já presente – pela sociedade de controle é uma das maiores ameaças à privacidade da história. Não há critérios de proporcionalidade que a justifiquem. Ainda que não reconhecido pelo Superior Tribunal de Justiça (até este momento), a quebra do sigilo em massa é inconstitucional, por ofensa à legalidade, à dignidade, à privacidade, à autodeterminação informativa e à proporcionalidade.[243]

4.12 O agente público

O "Roteiro de atuação sobre crimes cibernéticos" do Ministério Público Federal recomenda:

> Quatro dicas para o bem do anonimato
> • Utilizar uma rede externa à da instituição responsável pela investigação. Isto pode ser feito a partir de contratação de um link doméstico exclusivo para os procedimentos; • Utilizar serviços de proxies anônimos na Internet, de preferência tecnologias mais avançadas, como se vê na rede TOR; • Não utilizar email institucional para cadastros online em serviços quando for necessário algum tipo de registro para coleta de informações; • Não utilizar palavras-chave que indiquem a motivação da investigação em buscadores online para se chegar ao serviço investigado. (BRASIL, 2013, p. 171).[244]

[243] Garantias tratadas nos itens 4.3.2, 4.5 e 5.3.1.

[244] A citação é da edição de 2013 porque, mesmo após requisição do pesquisador, a 2ª Câmara de Coordenação e Revisão do Ministério Público Federal expressamente negou acesso à sua última edição (publicação institucional financiada com o dinheiro público) em novembro de 2021, que permanece oculta.

Contudo, o Código de Ética do Ministério Público da União (Portaria n. 98, de 2017) determina a transparência como fundamento de atuação no artigo 3º, inciso V – assim como a Lei Orgânica do Ministério Público do Estado de Minas Gerais (Lei Complementar n. 34, de 1994) no artigo 110, inciso XIII; o Código de Ética da Polícia Federal (Resolução n. 4 do Conselho Superior de Polícia, de 2015) no artigo 5º, inciso II; a Lei Orgânica da Polícia Civil do Estado de Minas Gerais (Lei Complementar n. 129, de 2013) no artigo 3º, inciso VII; e o Código de Ética e Disciplina dos Militares do Estado de Minas Gerais (Lei n. 14.310, de 2002) no artigo 14, incisos IX, XVII e XVIII. A Constituição determina a publicidade como princípio (artigo 37, *caput*);

> Consagra-se nisto o dever administrativo de manter plena transparência em seus comportamentos. Não pode haver em um Estado Democrático de Direito, no qual o poder reside no povo (art. 1º, parágrafo único, da Constituição), ocultamento aos administrados dos assuntos que a todos interessam, e muito menos em relação aos sujeitos individualmente afetados por alguma medida. (BANDEIRA DE MELLO, 2009, p. 114)

No Estado de Democrático de Direito, o exercício das funções públicas deve estrita obediência às premissas legais democraticamente constituídas pelo devido processo legislativo e esse exercício deve poder ser fiscalizado pelos destinatários normativos (BRÊTAS, 2018b, p. 74). Só se fiscaliza aquilo que se conhece, por isso "O homem invisível não teme ao Estado" (LESSIG, 2006, p. 38, tradução nossa[245]). O agir anônimo, sem transparência e, consequentemente, não fiscalizável do agente público assemelha-se à instauração de um Estado de Exceção (no sentido de Agamben[246]) em que os direitos são suspensos ao arbítrio da autoridade (DEL NEGRI, 2016, p. 109-110) – o que é evidentemente inconstitucional no Brasil, vez que o povo é soberano (Constituição, artigo 1º, parágrafo único)[247] e o Estado Democrático de Direito não pode ser suspenso.

No sistema processual penal brasileiro, para investigar de maneira disfarçada na internet, o agente deve requerer autorização judicial para a infiltração virtual, nos termos do artigo 10-A, § 4º, da Lei 12.850, de 2013, ou do artigo 190-A, inciso I, da Lei 8.069, de 1990, e registrar todos os atos eletrônicos praticados (artigo 10-D, da Lei 12.850, de 2013; artigo 190-E, da Lei 8.069, de 1990). Somado a isso, a cadeia de custódia deve ser preservada desde o reconhecimento de um elemento como de potencial probatório (CPP, artigo 158-B, inciso I).

[245] "The invisible man doesn't fear the state".
[246] "Em todos os casos, o estado de exceção marca um patamar onde lógica e práxis se indeterminam e onde uma pura violência sem *logos* pretende realizar um enunciado sem nenhuma referência real." (AGAMBEN, 2004, p. 63).
[247] Vide as notas n. 170, *supra*, e 287, *infra.*

Portanto, é ilegal a recomendação do Ministério Público Federal para que se busque elementos de prova digitais sem transparência, sem cadeia de custódia e sem o devido registro das atividades, por redes externas, serviço de *proxy* anônimo ou uso da rede Tor, sem utilizar o e-mail institucional ou "indicar a motivação da investigação" (BRASIL, 2013, p. 171). Não é admissível que a instituição criada para a fiscalização não se submeta à possibilidade de ser fiscalizada.[248]

A legalidade democrática é regente de todas as atuações dos agentes públicos. Certo é que as novas tecnologias fornecem para o agente público um novo ferramental; todavia, a Constituição jurídica deve ter primazia sobre qualquer uso desse ferramental; principalmente pelos agentes públicos que, voluntariamente, ingressaram nas funções estatais e juraram cumprir os deveres funcionais, inclusive os de transparência e respeito com a Lei (*e.g.*, artigo 5º, inciso I, alínea *h*, em cúmulo aos artigos 195, parágrafo único, e 236, inciso IX, da Lei Complementar n. 75, de 1993).

4.13 Procedimento

O procedimento é sequência de normas, atos e posições subjetivas (lícitas, facultadas ou devidas), em que a realização do ato posterior tem como pressuposto[249] a realização do ato anterior válido (FAZZALARI, 1996, p. 77-78). Neste item, a sequência procedimental da busca e da apreensão de elementos de prova digitais será explicitada, a partir das proposições expostas.

[248] Como decidido pelo Supremo Tribunal Federal, no julgamento do *Habeas Corpus* n. 94.173/BA, de relatoria do ministro Celso de Mello: "O Ministério Público, sem prejuízo da fiscalização intra-orgânica e daquela desempenhada pelo Conselho Nacional do Ministério Público, está permanentemente sujeito ao controle jurisdicional dos atos que pratique no âmbito das investigações penais que promova '*ex propria auctoritate*', não podendo, dentre outras limitações de ordem jurídica, desrespeitar o direito do investigado ao silêncio ('*nemo tenetur se detegere*'), nem lhe ordenar a condução coercitiva, nem constrangê-lo a produzir prova contra si próprio, nem lhe recusar o conhecimento das razões motivadoras do procedimento investigatório, nem submetê-lo a medidas sujeitas à reserva constitucional de jurisdição, nem impedi-lo de fazer-se acompanhar de Advogado, nem impor, a este, indevidas restrições ao regular desempenho de suas prerrogativas profissionais (Lei nº 8.906/94, art. 7º, v.g.). - O procedimento investigatório instaurado pelo Ministério Público deverá conter todas as peças, termos de declarações ou depoimentos, laudos periciais e demais subsídios probatórios coligidos no curso da investigação, não podendo, o '*Parquet*', sonegar, selecionar ou deixar de juntar, aos autos, quaisquer desses elementos de informação, cujo conteúdo, por referir-se ao objeto da apuração penal, deve ser tornado acessível tanto à pessoa sob investigação quanto ao seu Advogado." (BRASIL, 2022m).

[249] "Pressuposto, em linguagem filosófica e da lógica, é premissa não explícita, e essa […] é a proposição da qual são extraídas outras proposições, pelo processo de inferência, e [...] as conclusões podem se tornar novas premissas de novas conclusões, na cadeia de proposições, no raciocínio dedutivo." (GONÇALVES, 1992, p. 110).

Cabe ressaltar que a cadeia de custódia deve ser preservada em todo o procedimento (CPP, arts. 158-A a 158-F)[250] e que sempre deve existir prévia intervenção judicial na situação de possibilidade de ofensa aos direitos (Constituição, art. 5º, XXXV) (VALENTE, 2008, p. 171-173)[251].

Posto isso, a sequência é: requerimento pela parte, em acordo com os requisitos legais e com base em elementos concretos (item 4.3.2, *supra*); decisão fundamentada do juízo competente (Constituição, arts. 5º, XXXVII e LIII, e 93, IX); se autorizada a busca e a apreensão, deve ser expedido mandado (CPP, art. 243), redigido pelo escrivão (CPC, art. 152, I)[252], que demarca o alcance da tarefa dos agentes. Após, durante o dia[253], ocorre a execução da busca, com os atos de (CPP, art. 245): leitura do mandado; se for em domicílio, intimação para que o morador abra a porta; se não for aberta, coação para a entrada forçada; intimação para seja indicado onde se encontra o dispositivo de armazenamento do elemento de prova digital; se necessário, emprego de força na procura do dispositivo; a busca domiciliar deve ser assistida pelo morador ou, na sua ausência, por vizinhos. Reconhecido como de potencial probatório, o dispositivo deve ser isolado e identificado; seguidamente, o dispositivo de armazenamento deve ser coletado pelo perito – ligado ou desligado – ou os elementos digitais devem ser imediatamente adquiridos (Figuras 5 a 7 do item 5.1.2, *infra*) (CPP, arts. 158-B, I a IV, 158-C e 169; NBR ISO/IEC 27037:2013 [ABNT, 2013b]). Toda a execução da busca e da apreensão deve ser registrada em auto circunstanciado assinado por duas testemunhas presenciais (CPP, art. 245, § 7º).

Apreendido, o dispositivo de armazenamento deve ser acondicionado, transportado e recebido pelo agente público responsável (CPP, art. 158-B, V a VII).

Neste ponto, se atingiu a obtenção do dispositivo de armazenamento do elemento de prova digital. A produção probatória baseada nele exige a realização do meio de prova perícia para acessar e tratar as informações (CPP, art. 158).

4.14 Acesso e tratamento das informações

[250] "Transversalmente a cada uma das etapas destaca-se um factor fundamental do procedimento forense, cuja importância é tanto maior quanto for o carácter central e determinante da prova digital num processo de natureza criminal: o registro de todos os passos do procedimento forense que tenham relevo para a aferição da integridade, fidedignidade, autenticidade e, em última análise, validade da prova" (RAMALHO, 2019, p. 117). Vide o item 5.1.1, *infra*, e seguintes.
[251] Item 4.3.2, *supra.*
[252] Vide o item 4.8, *supra.*
[253] Vide o item 4.9, *supra.*

O sistema jurídico demarca os limites de atuação de cada um dos sujeitos do processo, isso é básico para o processo acusatório (MIRANDA COUTINHO, 2010). Ocorre que essa demarcação não diz respeito apenas ao acusador, ao acusado, ao defensor e ao juiz; ela é prevista para todos aqueles que atuam no procedimento (*e.g.* delegado, investigador de polícia, oficial de justiça, escrivão, servidor, vítima, assistente de acusação, testemunha, perito, assistente técnico, intérprete). Isso é importante para o procedimento da busca e da apreensão, principalmente pela configuração dos institutos técnico-científicos como órgãos de polícia levar a confusões conceituais e práticas – como é o caso do Instituto de Criminalística de Minas Gerais (Constituição do Estado de Minas Gerais, artigo 139, inciso I), que integra a Polícia Civil, e do Instituto Nacional de Criminalística (Lei n. 4.483, de 1964, artigo 2º), que integra a Polícia Federal[254]. Como observa Manuel Valente (2020, p. 55):

> A Autoridade de Polícia Criminal ou o Delegado de Polícia não é perito técnico-científico – perito criminal –, logo não lhe cabe quaisquer funções de polícia científica como examinar os vestígios e indícios probatórios, como os constantes de uma mídia informática, que havia sido apreendida [...].

Por isso, e em respeito ao modelo constitucional do processo, as normas, atos e posições subjetivas determinadas pela Lei[255] para o acesso e tratamento das informações são indispensáveis para a produção da prova sobre os elementos digitais.

Destaca-se que a decisão que autoriza a busca e a apreensão é limite rígido sobre o alcance dos atos realizados (itens 4.3.2 e 4.8, *supra*) e que os atos de apreender o dispositivo de armazenamento e o de acessar os elementos digitais lá contidos são distintos. Logo, e pela potencial ofensa à privacidade e à proteção dos dados pessoais (Constituição, art. 5º, X, XXXV e LXXIX), o acesso ao dispositivo de armazenamento demanda decisão judicial específica (MACHADO, 2020, p. 209).

Nos termos do artigo 158, inciso VIII, a "manipulação do vestígio de acordo com a metodologia adequada às suas características" deve ser realizada por perito em exame pericial (BRASIL, 2021a) (VALENTE, 2020, p. 56-60). Portanto, obtido o dispositivo de armazenamento dos elementos digitais, o acesso a esses elementos deve seguir o procedimento descrito nos artigos 159 e 160 do Código, que não fazem restrição à sua aplicação na fase de investigação e devem ser aplicados também nela.

[254] O Departamento Federal de Segurança Pública, referido na Lei n. 4.483, de 1964, passou a chamar-se Departamento de Polícia Federal no artigo 210 do Decreto-lei n. 200, de 1967, e Polícia Federal no artigo 144, inciso I, da Constituição de 1988.
[255] Vide a nota n. 70, *supra.*

Em função da inércia da jurisdição, o exame pericial no dispositivo de armazenamento apreendido deve ser requerido pela parte legitimada (proposição). O exercício da ampla defesa deve ser respeitado e a Defesa pode apresentar razões, quesitos e indicar assistente técnico (Constituição, artigo 5º, inciso LV; Código de Processo Penal, artigo 159, § 3º; e Lei 8.906, de 1994, artigo 7º, inciso XXI, alínea *a*). No juízo de admissibilidade da produção do meio de prova, os requisitos legais devem ser observados, principalmente a proporcionalidade, a relevância e a fundamentação[256]. Admitida, a perícia deve ser feita por perito oficial, portador de diploma de curso superior, ou por duas pessoas idôneas, portadoras de diploma de curso superior na área específica do exame (após prestarem compromisso) (CPP, art. 159). A produção da perícia é composta pelos seguintes atos[257]: acesso ao dispositivo de armazenamento – ligado ou desligado (Figuras 8 e 9, do item 5.1.2, *infra*; NBR ISO/IEC 27037:2013 [ABNT, 2013b]) –; análise científica em metodologia adequada de tratamento das informações; e relatório contendo a descrição da metodologia e as respostas aos quesitos da perícia em laudo pericial (CPP, art. 160). Após o exame por perito oficial, o assistente técnico admitido poderá examinar o elemento de prova digital (CPP, art. 159, §§ 4º e 6º)[258]. O dispositivo de armazenamento deve ser adequadamente guardado (CPP, art. 158-B, IX). E, finalmente, se o dispositivo não interessar mais à instrução, deve ser descartado (CPP, art. 158-B, X), com sua devolução ao dono (CPP, art. 118); exceto se for instrumento do crime cuja fabricação, alienação, uso, porte ou detenção constitua fato ilícito, ou proveito do crime (CPP, art. 119).[259]

Após a produção da perícia, as partes podem requerer a oitiva dos peritos para o esclarecimento dos atos realizados ou para responderem a quesitos encaminhados ao menos dez dias antes da audiência; sendo que o perito pode apresentar as respostas em laudo complementar (CPP, art. 159, § 5º, I). Esta previsão legal deve ser lida em harmonia com o direito ao confronto[260]: é direito do acusado de examinar qualquer pessoa de potencial probatório incriminador, também de arguir impedimentos e suspeições; e é dever do juízo de agir ativamente para fazer com que essa pessoa compareça em audiência para ser

[256] Vide o item 4.3.2, *supra.*
[257] Vide o item 3.5, *supra.*
[258] Todos os elementos de prova já documentados devem ser acessíveis à Defesa, como, inclusive, determina a Súmula Vinculante n. 14, do Supremo Tribunal Federal.
[259] Situações em que, após decisão judicial transitada em julgado, o dispositivo pode ser: confiscado em favor da União (CP, art. 91, II) e posteriormente destruído (CPP, art. 124), leiloado (CPP, arts. 122, 123 e 133) ou recolhido em museu criminal, se existir interesse na sua conservação (CPP, art. 124); ou, se existir interesse público, o juízo pode autorizar o uso do dispositivo por órgão público (CPP, art. 133-A).
[260] Pacto Internacional dos Direitos Civis e Políticos, artigo 14.3.e; Pacto de São José da Costa Rica, artigo 8, 2, f; Constituição, artigo 5º, § 1º; Código de Processo Penal, artigos 203, 204, 205, 206, 212, 214, 217, 218, 260, 261 e 792. Vide: Cordero (1963, p. 236-237), Malan (2009) e Zappalà (2008, p. 129-140).

confrontada.[261] Assim, ainda que o perito apresente laudo complementar, o acusado tem direito de insistir na oitiva do perito e de confrontá-lo em audiência; e, na situação de não comparecimento, o perito pode ser multado e conduzido (CPP, arts. 277, parágrafo único, alínea *a*, e 278).

4.14.1 Perícia sobre o elemento digital apreendido

Pela sua importância e complexidade, em seguida serão destacados mais alguns aspectos sobre a perícia no elemento digital apreendido.

A perícia:

> […] põe presente feitos imperceptíveis aos olhos do profano (por exemplo, análise histológica, sobre uma morte presumida); ou enuncia teses sobre premissas hipotéticas (quais são os sintomas do envenenamento por arsênico); e também (é a hipótese mais frequente) combina observações experimentais com princípios, elaborando conclusões indutivas (que o fator mortal é o arsênico encontrado no cadáver). (CORDERO, 2000b, p. 119, tradução nossa[262]).

A preparação especial do perito é que o qualifica para auxiliar o esclarecimento das questões de fato complexas (CARNELUTTI, 1950, p. 266). Por isso, o artigo 465 do Código de Processo Civil determina que o perito nomeado deve ser especializado no objeto da perícia. Essa especialização não é presumida, exige comprovação (CPC, art. 465, § 2º, II) e pode ser impugnada pelas partes, no exercício da ampla defesa e do contraditório (BRÊTAS, 2016b, p. 174).

O saber que possibilita a enunciação do discurso científico (FOUCAULT, 2014a, p. 105, 220), como todos, é mutável. O que é saber científico num momento é erro grosseiro no outro (como a indivisibilidade do átomo e o geocentrismo). Os saberes que apresentam validade científica devem ser diferenciados dos que não apresentam; "Não se trata somente da cartomancia ou da leitura de borras de café […] A questão concerne também às outras técnicas" (TARUFFO, 2012, p. 245). Para buscar admitir somente as provas cientificamente válidas, a Suprema Corte dos Estados Unidos, no julgamento do caso *Daubert*, elencou como critérios de validade: a possibilidade de criticar a teoria que orientou o exame; o conhecimento da porcentagem de erro; a revisão por pares da metodologia utilizada; a

[261] Vide os itens 5.2.1 e 5.2.1.1, *infra*.

[262] "[…] pone de presente hechos imperceptibles a los ojos del profano (por ejemplo, análisis histológicos, respecto a una muerte presunta); o enuncia tesis sobre premisas hipotéticas (cuáles son los síntomas del envenenamiento con arsénico); y también (es la hipótesis más frecuente) combina observaciones experimentales con principios, elaborando conclusiones inductivas (que el factor mortal es el arsénico encontrado en el cadáver).".

aceitação da metodologia pela comunidade científica. A prova científica só deve ser admitida se satisfizer esses critérios de validade e for relevante no caso concreto (TARUFFO, 2014, p. 96-97) – no Brasil, o Supremo Tribunal Federal endossou o "padrão Daubert", *e.g.*, julgamentos do Agravo Regimental no *Habeas Corpus* n. 174.400/DF e do Recurso Extraordinário n. 363.889/DF.

A aferição do cumprimento dos critérios de validade científica é possível, principalmente, a partir do laudo pericial. Nos termos do art. 473 do CPC (aplicado subsidiariamente ao processo penal):

> O laudo pericial deverá conter: I – a exposição do objeto da perícia; II – a análise técnica ou científica realizada pelo perito; III – a indicação do método utilizado, esclarecendo-o e demonstrando ser predominantemente aceito pelos especialistas da área do conhecimento da qual se originou; IV – resposta conclusiva a todos os quesitos apresentados pelo juiz, pelas partes e pelo órgão do Ministério Público. § 1º No laudo, o perito deve apresentar sua fundamentação em linguagem simples e com coerência lógica, indicando como alcançou suas conclusões. § 2º É vedado ao perito ultrapassar os limites de sua designação, bem como emitir opiniões pessoais que excedam o exame técnico ou científico do objeto da perícia. § 3º Para o desempenho de sua função, o perito e os assistentes técnicos podem valer-se de todos os meios necessários, ouvindo testemunhas, obtendo informações, solicitando documentos que estejam em poder da parte, de terceiros ou em repartições públicas, bem como instruir o laudo com planilhas, mapas, plantas, desenhos, fotografias ou outros elementos necessários ao esclarecimento do objeto da perícia. (BRASIL, 2022c).

Além da especialização do perito no objeto da perícia e da validade científica da metodologia do exame, também se destaca que qualquer perícia é a versão humana da aplicação de um saber a um exame (MAIER, 2011, p. 148). Portanto, a perícia pode ser influenciada pelos mesmos vieses a que os demais seres humanos estão sujeitos[263]. Para combater a parcialidade do perito, o Código de Processo Penal determina que não pode ser perito quem tenha vínculo objetivo (arts. 112 e 279, II) ou subjetivo (arts. 105 e 280) com o caso penal, cabendo a arguição de impedimento ou suspeição.

Com isso, apesar da supracitada[264] configuração dos institutos técnico-científicos como órgãos de polícia, o exercício da função dos peritos deve ser independente (VALENTE, 2009, p. 387; 2020, p. 58-59). Não há sentido e nem relevância na perícia se ela for manipulada por fatores estranhos aos científicos.

Finalmente, a perícia sobre elementos digitais apreendidos, pelas razões expostas, deve ser executada por especialista que, na NBR ISO/IEC 27037:2013 (ABNT, 2013b, p. 2), é aquele autorizado, treinado e qualificado para agir no local do incidente, na coleta e na

[263] Sobre os vieses cognitivos, vide: Nunes, Lud e Pedron (2018).
[264] Item 4.14, *supra.*

aquisição do elemento digital, responsabilizando-se pelo seu manuseio e que tem conhecimento especializado, habilidade e aptidão para lidar com os problemas técnicos envolvidos. Esse especialista deve ser portador de diploma de curso superior (CPP, art. 159) especializado no objeto da perícia (CPC, art. 465) – como ciência da computação ou engenharia de *software* – e pode aprofundar seu conhecimento num segmento. Xiaodong Lin (2018, p. 27-29), exemplificadamente, elenca os segmentos forenses de: sistemas de arquivos, memória, sistemas operacionais, multimídia, redes, *malware*, dispositivos móveis, *e-mail*, *firewall* e fraudes financeiras.

Na execução do exame pericial sobre os elementos digitais, o marco teórico e a operacionalização devem ser cientificamente válidos (operacionalização sem transparência técnica é inválida, por exemplo – por não ser criticável e, portanto, não ser científica). A cadeia de custódia dos elementos digitais deve ser preservada – item 5.1.1, *infra* – (o que não ocorrerá se a operacionalização alterar o elemento digital e comprometer a sua integridade, *exempli gratia*). E os atos do exame devem ser registrados no laudo pericial que responda a todos os quesitos específicos formulados, segundo os requisitos do artigo 473 do Código de Processo Civil.

4.15 Consequências do não cumprimento dos requisitos: inadmissibilidade

Damaška explica que a Revolução Francesa combateu o sistema das provas legais[265] do *ancien régime* e não apenas a valoração da prova, como também as regras de exclusão probatórias foram preteridas em favor do livre convencimento do juiz. Enquanto nos países influenciados pela França[266] predominou a crença na racionalidade e desinteresse do julgador na análise da prova, a situação foi diversa nos países influenciados pela Inglaterra[267]: para que

[265] No sistema das provas legais, a valoração da prova é determinada antes de sua produção e o juízo é resultado de um cálculo: "[…] os juízes, examinando os autos, deviam apreciar o caráter de cada prova e extrair dela o respectivo valor, formulando numericamente a sua *quantidade*, para fins de decisão; assim, as provas podiam resultar *plenas* ou *semiplenas*, ou ainda *manifestas, consideráveis* e *imperfeitas* (ou *ligeiras*). A regulamentação de cada meio de prova também era minuciosa e complexa: com relação à testemunhal, por exemplo, para que fosse considerada *completa*, exigia-se um mínimo de duas testemunhas (*testis unus, tesis nullus*), mas era indispensável que fossem oculares, firmes e tivessem seus depoimentos tomados em três inquirições sucessivas;" (GOMES FILHO, 1997, p. 23-24, grifo do autor). Apesar de parecer benéfica ao investigado, na inquisitoriedade em que se torturava para obter a confissão, e que a confissão era prova suficiente, o cálculo era um fingimento (CORDERO, 2000b, p. 29). Sobre o processo penal francês revolucionário, vide: Pimenta (2019, p. 90-95) e Esmein (1882; 1908).

[266] Como a Alemanha (ROXIN, 2003, p. 565-566).

[267] Como os Estados Unidos (COSTA ANDRADE, 2013, p. 137).

os jurados, leigos, não valorassem equivocadamente o conjunto probatório, a preocupação com as regras de exclusão probatórias foi maior (DAMAŠKA, 2015, p. 37-38, 44-45).[268]

Apesar do Brasil ter sido mais influenciado pela França e pelos países da Europa continental (PIERANGELLI, 1983, p. 99), em primeiro lugar, ambas as tradições não são mais tão distintas e convergiram para destacar a importância do caso concreto e dos precedentes e para, à sua maneira, proteger os direitos substantivos e procedimentais (COSTA ANDRADE, 2013, p. 183-187). Em segundo lugar, a Constituição de 1988 determinou serem inadmissíveis as provas ilícitas (artigo 5º, inciso LVI), instituindo novo regime de exclusão probatória. Em terceiro lugar, ocorreram reformas no processo penal brasileiro para melhor regulamentar a exclusão da prova, em adequação à Constituição, como as operadas pela Lei n. 11.690, de 2008, e pela Lei n. 13.964, de 2019.

As regras probatórias são limites na construção do juízo, por isso são garantias contra a arbitrariedade na cognição, que não deve ocorrer por meios que não esclareçam os fatos e nem por meios que ofendam os direitos fundamentais (BINDER, 2009, p. 77-84). O tratamento constitucional da irregularidade probatória é expresso: a prova ilícita é inadmissível. Essa noção, pela expansividade do modelo constitucional do processo (ANDOLINA; VIGNERA, 1997, p. 9), orienta todo o direito probatório brasileiro. Com isso, desde a obtenção do elemento de prova até a produção da prova, se existir algum ato irregular, a prova é inadmissível; o que implica a impossibilidade de o ato ser saneado. Por determinação constitucional, a prova ilícita não pode integrar o procedimento e deve ser: declarada inadmissível o quanto antes; desentranhada dos autos; e inutilizada (Constituição, artigo 5º, inciso LVI[269]; Código de Processo Penal, artigo 157[270]) (PRADO, Geraldo, 2019, p. 126-127) (VALENTE, 2020, p. 89-90) (GIACOMOLLI, 2022, p. 141-142).[271]

[268] Segundo Bettiol, no processo de proveniência inglesa: "Implícito é o reconhecimento dos limites do conhecimento humano, e por conseguinte do caráter convencional da verdade. Não a impossível e fantástica verdade material do Inquisidor é procurada, quando, ao invés, mais se procura uma decisão além de qualquer outra dúvida. Daí a importância das *Rules of Evidence* e das *Exclusionary Rules* visando a garantir a aquisição da prova, e em particular o contraditório na formação da mesma. No fundo, transparece o conceito científico moderno de que a verdade de uma afirmação é essencialmente construída pela seriedade dos processos." (BETTIOL, 2008, p. 168).

[269] "são inadmissíveis, no processo, as provas obtidas por meios ilícitos" (BRASIL, 2020a).

[270] "São inadmissíveis, devendo ser desentranhadas do processo, as provas ilícitas, assim entendidas as obtidas em violação a normas constitucionais ou legais. (...) § 3º Preclusa a decisão de desentranhamento da prova declarada inadmissível, esta será inutilizada por decisão judicial, facultado às partes acompanhar o incidente." (BRASIL, 2021a).

[271] "[…] o magistrado responsável pelo juízo de admissibilidade, como destinatário da prova produzida em desconformidade com o tipo legal, exerce desde a etapa da investigação criminal a função de *Gatekeeper*. A relevância que a etapa de investigação criminal assume na atualidade requisita do juiz responsável pelo juízo de admissibilidade da prova que a filtre tão pronto constate a sua ilegalidade […]" (PRADO, Geraldo, 2021, p. 141).

Parte da literatura jurídica diferencia a prova ilícita da ilegítima. A proveniência dessa diferenciação é o trabalho de Ada Grinover que, com base no italiano Nuvolone, conceituou: "Quando a proibição for colocada por uma lei processual, a prova será ilegítima (ou ilegitimamente produzida); quando, pelo contrário, a proibição for de natureza material, a prova será ilicitamente obtida" (GRINOVER; FERNANDES; GOMES FILHO, 1996, p. 116). No modelo constitucional do processo, a distinção não tem sentido, já que o direito processual tem fundamento nos institutos processuais constitucionais (direitos processuais substantivos ou "materiais") (ANDOLINA; VIGNERA, 1997, p. 8-11). Somado a isso, como ressalta Jacinto Nelson de Miranda Coutinho (2016, p. 249-250, grifo do autor): "*na Itália e nos EUA não há a previsão constitucional que se tem no Brasil!*", portanto, desde 1988 a distinção não tem qualquer sentido também noutro marco teórico, vez que a inadmissibilidade da prova ilícita é previsão constitucional de direito "material" no Brasil[272]; assim, toda prova que viola norma "processual" – "prova ilegítima" – também ofende norma constitucional "material" – "prova ilícita" – (BARROS, 2008b, p. 36-37).[273]

Em todos os procedimentos jurídicos, a validade de cada um dos atos depende da regularidade de seus antecessores (GONÇALVES, 1992, p. 111). A busca e a apreensão de elementos de prova digitais e a perícia decorrente irregulares são inadmissíveis, não podem integrar o procedimento, contaminam os atos delas derivados e não servem para a construção do juízo; por expressa determinação da Constituição (artigo 5º, inciso LVI) e do Código de Processo Penal (artigo 157).

4.16 Os frutos da árvore envenenada

O § 1º do artigo 157 do Código de Processo Penal determina que também são inadmissíveis as provas derivadas das ilícitas. A ilicitude por derivação no Brasil foi influenciada pela teoria dos frutos da árvore envenenada (*fruits of the poisonous tree*) estadunidense (BARBOSA MOREIRA, 1996, p. 149-150). João Gualberto Garcez Ramos pontua que, nos Estados Unidos, essa teoria foi construída a partir dos julgamentos dos casos *Boyd* v. *United States* (1886), *Weeks* v. *United States* (1914) e *Silverthorne Lumber Co.* v. *United States* (1920)[274]:

[272] Constituição, artigo 5º, inciso LVI.
[273] A redação de norma "processual" e norma "material" entre aspas decorre da impropriedade dessa distinção no modelo constitucional do processo, já que o direito processual substantivo ("material") é o fundamento do direito procedimental. Destaca-se que não há um direito "material" superior ao "processual" (num sentido adjetivo ou secundário) e o processo também é direito "material" (Constituição, artigo 5º, inciso LIV).

> […] em resumo, se em *Boyd* a Suprema Corte fixou a ideia de que a prova ilícita é írrita, em *Weeks* deixou assentado que a produção de provas ilícitas não contamina a validade do processo, mas leva à exclusão dessas provas do processo. Um terceiro julgado, Silverthorne Lumber Co. v. United States, 251 US 385 (1920), consolidaria a doutrina dos frutos da árvore envenenada e a formularia em termos célebres, ao escrever que "a essência da norma que proíbe a aquisição de uma prova uma certa maneira não se limita a dizer que ela não pode ser utilizada em juízo, mas reza que ela não pode ter efeito algum". (RAMOS, 2006, p. 122-123, grifo do autor).

A teoria dos frutos da árvore envenenada estadunidense tem exceções, incompatíveis com o sistema jurídico brasileiro, como será demonstrado no subitem seguinte.

4.16.1 Inconstitucionalidade da descoberta inevitável no Brasil

Nos Estados Unidos, a ilicitude por derivação apresenta três exceções: a atenuação, a fonte independente e a descoberta inevitável. Na primeira, apesar da ilicitude na prova original contaminar as derivadas, pode existir atenuação na exclusão da prova derivada pela sua distância da original. Pela segunda, não há exclusão da prova derivada se a acusação demonstrar que não há vínculo entre ela e a original.[275] Pela terceira, a prova derivada não deve ser excluída se a acusação demonstrar que, hipoteticamente, ela seria inevitavelmente obtida (RAMOS, 2006, p. 124) (COSTA ANDRADE, 2013, p. 171-172).

A atenuação (e toda a arbitrariedade nela envolvida, já que é resultado de juízo discricionário em que são ausentes as premissas legais quanto ao tamanho da distância da prova derivada da originária para não existir a exclusão) não tem ressonância no processo penal brasileiro. Existe previsão legal para a admissibilidade da prova produzida por fonte independente (CPP, art. 157, § 1º); o que é lógico, vez que não há derivação nesta situação e, portanto, não há razão para a contaminação.[276]

A descoberta inevitável é inconstitucional. Prevista com redação ruim no § 2º do art. 157 do CPP[277], que confunde as noções de "fonte independente" com "descoberta inevitável" (PACELLI DE OLIVEIRA, 2010, p. 375), esta exceção à ilicitude por derivação foi aplicada no julgamento do caso *Nix* v. *Williams*, de 1984, pela Suprema Corte dos Estados Unidos.

[274] Não há menção à Bíblia nos julgamentos da Suprema Corte dos Estados Unidos. Curiosamente, contudo, no Evangelho segundo Mateus (Mt. 7,18) consta que: "Não pode a árvore boa produzir frutos maus, nem a árvore má produzir frutos bons." (MATEUS, 1999, p. 638).

[275] "Mas o que valorar para considerar a existência ou inexistência do nexo causal? Um dos critérios é o temporal, ou seja, verificar se aprova discutível (derivada) foi produzida antes, após ou concomitantemente à prova considerada ilícita. A regularidade da produção da prova e os meios probatórios são outros critérios considerados e desenvolvidos." (GIACOMOLLI, 2014, p. 169).

[276] Lembra-se que: "Sempre que houver conexão ou dúvida acerca desta (*in dubio pro reo*), há contaminação." (GIACOMOLLI, 2014, p. 169-170).

[277] "Considera-se fonte independente aquela que por si só, seguindo os trâmites típicos e de praxe, próprios da investigação ou instrução criminal, seria capaz de conduzir ao fato objeto da prova." (BRASIL, 2021a).

Nesse caso, um suspeito de matar uma criança, que estava desaparecida, sofreu violações pela polícia, em oitiva sem a presença de advogado, para que revelasse onde a criança estava. Paralelamente, ocorreu uma busca pela criança por mais de duzentos voluntários. A acusação argumentou que apesar da oitiva do suspeito configurar prova ilícita, inevitavelmente a busca por voluntários encontraria a criança e que, por isso, não era ilícita a descoberta do corpo da criança derivada das informações obtidas na oitiva do suspeito (ROSA, 2020, p. 692-693).

Ocorre que, imbuído de boas intenções ou não, a descoberta inevitável é exercício de raciocínio hipotético indemonstrável. No caso *Nix* v. *Williams*, a busca dos voluntários terminou antes do local onde o corpo foi enterrado. A busca não o encontrou. E, como destaca Jacinto Nelson de Miranda Coutinho, ainda que a busca tivesse continuado, bastava um instante de desatenção de um voluntário que também não o encontraria; "Logo, *dizer da descoberta que ela era inevitável não passa de mera elucubração mental*" (MIRANDA COUTINHO, 2016, p. 267, grifo do autor).

Somado à fragilidade da noção da descoberta inevitável para a construção do juízo, não se pode importar a teoria estadunidense sem se considerar o sistema jurídico brasileiro. No Brasil, os direitos fundamentais assegurados na Constituição somente podem ser limitados por disposição expressa da Constituição (restrição imediata) ou por lei ordinária que tenha fundamento na Constituição (restrição mediata) (MENDES, Gilmar; BRANCO, 2015, p. 200). E a Constituição não prevê qualquer restrição à inadmissibilidade da prova ilícita. Na ausência de previsão constitucional que autorize a restrição, não é possível que a legislação infraconstitucional excepcione o direito fundamental expressamente protegido no inciso LVI, do artigo 5º, da Constituição. Como observa Jacinto Nelson de Miranda Coutinho:

> Por isso, *em se tratando de preceito que expressa um direito individual referente ao devido processo legal (*pelo *"são inadmissíveis, no processo) e limita a conduta de quem quer que seja, dos servidores públicos aos privados* (*pelo "as provas obtidas por meios ilícitos"*), não pode receber, de forma alguma, *interpretação restritiva*, como insistentemente vêm alguns querendo fazer, sem esquecer que se tratam das *provas obtidas* e, por isso, *todas!* (MIRANDA COUTINHO, 2016, p. 267, grifo do autor).

Por criar exceção não autorizada pela Constituição, o § 2º do artigo 157 do Código de Processo Penal, que admite a descoberta inevitável, é inconstitucional (BARROS, 2008b, p. 39). Isto tem relação com a busca e a apreensão de elementos de prova digitais e com todos os atos probatórios.

4.16.2 Encontro fortuito

Antes da obtenção do objeto da apreensão – já que após sua obtenção a execução deve encerrar-se, pelo cumprimento da finalidade demarcada na decisão e pela vedação do abuso em sua execução (ROSA, 2020, p. 695) – pode ocorrer o encontro fortuito de elementos que não eram previstos na decisão judicial, mas que são relacionados a possíveis crimes. A literatura jurídica diverge sobre a validade do uso desses elementos. Este ponto é especialmente importante na busca e na apreensão de elementos de prova digitais, que envolvem volumes imensos de dados referentes a vários aspectos distintos das atividades dos sujeitos.

Manuel Valente sintetiza que, no Direito alemão, parte da literatura jurídica (Prittwitz e Knauth) defende a irrelevância dos conhecimentos fortuitos: pela ausência de previsão legal para a restrição de direito fundamental, esses conhecimentos não podem ser valorados. Parte (Schünemann) entende que todos os conhecimentos fortuitos podem ser valorados se não forem proibidos. Outra parte (Roxin, Wolter, Meyer) sustenta que, em respeito à legalidade, somente os conhecimentos conexos a um catálogo de crimes[278] podem ser valorados – esta corrente também conta com autores que advogam a aplicação da proporcionalidade tanto na autorização da medida quanto na valoração (Rudolphi, Rogall),

> ou seja, impõe-se uma exegese da *necessidade ou desnecessidade* da valoração dos conhecimentos fortuitos para a investigação e, tendo em conta a excepcionalidade deste meio de obtenção de prova, da hipotética admissibilidade da escuta telefônica para a investigação dos crimes objeto do conhecimento fortuito. (VALENTE, 2006, p. 115-117, grifo do autor).

No Brasil, não é possível valorar provas ilícitas por serem inadmissíveis e não integrarem os autos do processo (Constituição, artigo 5º, LVI; CPP, artigo 157; item 4.15, *supra*). Todavia, a discussão acadêmica também conta com uma corrente que considera válido o uso de qualquer elemento obtido em encontro fortuito (NUCCI, 2012, p. 379), uma corrente que considera esse uso inválido (LOPES JR., 2012, p. 584-588), além de uma terceira corrente que entende que o elemento obtido em encontro fortuito é notícia de crime para nova investigação (GOMES; MACIEL, 2012, p. 108).

A primeira corrente despreza a vinculação da execução da busca e da apreensão à demarcação da finalidade, dos meios e do alcance da tarefa dos agentes na decisão judicial e

[278] "Desta constelação retira-se que se o conhecimento fortuito respeitar a um crime exta-catálogo, aquele não pode ser valorado por respeito ao princípio da legalidade – pois seria inadmissível permitir-se valorar provas de um crime que o legislador não admitiu ter dignidade para ser colocado na balança da ponderação entre verdade material e inviolabilidade das comunicações e da vida privada [...]" (VALENTE, 2006, p. 116-117).

no mandado (Constituição, arts. 5º, XXXV, e 93, IX; CPP, arts. 240, § 1º, e 243) e que a atuação do executor fora do demarcado na decisão judicial pode configurar abuso de autoridade (Lei 13.869, de 2019, art. 22). Somado a isso, essa corrente facilita a prática ilegal da pescaria probatória (item 4.7, *supra*). Portanto, deve ser rejeitada.

A segunda corrente respeita a vinculação causal entre a decisão judicial que defere a busca e a apreensão e a obtenção do elemento. A execução pelos agentes deve atender à finalidade demarcada na decisão judicial fundamentada em indícios prévios e concretos. Ao invés da devassa arbitrária, a realização da busca e da apreensão, que envolve restrição a direitos fundamentais (como a privacidade e a inviolabilidade do domicílio), tem como limite a reserva de jurisdição. É ilegal a obtenção de elemento desvinculado da decisão sobre o caso penal específico (LOPES JR., 2012, p. 585-587) – e se a decisão judicial não limita devidamente a busca e a apreensão, ela é viciada por descumprir os requisitos legais, principalmente a fundamentação, o que contraminará todos os atos decorrentes (ROSA, 2020, p. 696).[279]

Ressalta-se que a prisão em flagrante delito – como em crimes permanentes (CPP, art. 303) – não demanda prévia autorização judicial (Constituição, art. 5º, XI), é dever do agente policial (CPP, art. 301) e é seguida de busca pessoal (CPP, art. 244). Pela prisão em flagrante ser dever legal do agente policial nas situações do artigo 302 do CPP e não exigir prévia autorização judicial, obviamente ela não é vedada pela vinculação causal da execução à decisão judicial (LOPES JR., 2012, p. 589). Igualmente, pela busca pessoal poder ser executada sem mandado também nas situações de fundada suspeita, em indícios concretos, de que a pessoa possua arma proibida ou elementos que constituam o corpo de delito ou durante a busca domiciliar ou com o consentimento livre, expresso e informado da pessoa que sofrerá a busca (CPP, art. 244), essas situações não são limitadas pela vinculação causal à decisão judicial, a permissão de sua realização independente de decisão judicial está na lei.[280]

Compondo a terceira corrente, Luiz Flávio Gomes e Silvio Maciel (2012, p. 108) entendem que se a obtenção do elemento tem conexão ou continência com o fato investigado, a prova é lícita; se a conexão ou continência for ausente, a prova é ilícita, mas pode ser utilizada como notícia de crime. Esse posicionamento apresenta os mesmos problemas da primeira corrente na primeira situação e, na segunda, incorre em autocontradição: ao mesmo tempo em que é prova ilícita no procedimento originário, serve para iniciar nova persecução.

[279] "A vinculação causal da prova (especialidade) é decorrência natural da adoção de um processo penal minimamente evoluído, como forma de recusa ao substancialismo inquisitorial e às investigações abertas e indeterminadas." (LOPES JR., 2012, p. 586). Sobre os requisitos legais, vide o item 4.3.2, *supra.*
[280] Vide o item 4.11, *supra.*

Além disso, como a Constituição determina que a prova ilícita é inadmissível (art. 5º, LVI), não há como aceitar que ela integre persecução alguma. Apesar desse entendimento ser aceito na Espanha[281], não há como aceitá-lo no Brasil, onde existe previsão constitucional específica no sentido de total inadmissibilidade da prova ilícita.[282]

Pelas razões expostas acima – e considerando que a busca e a apreensão de elementos de prova digitais não são restritas a um catálogo de crimes no Brasil, o que facilita a sua vulgarização[283] – esta tese endossa a segunda corrente.

4.17 Observações sobre o cúmulo com outros meios de investigação

A subsidiariedade[284], derivada da proporcionalidade, restringe o uso de meios ocultos, como a busca, às situações em que o conhecimento sobre o caso penal não tem como ser obtido de outra maneira. Como as invenções tecnológicas aumentam muito o potencial de controle e acesso a informações sensíveis sobre o indivíduo (item 2.5, *supra*), o progressivo uso de novas tecnologias pela sociedade de controle deve, ainda mais incisivamente, ser limitado pela subsidiariedade: entre dois ou mais meios que possibilitem o cumprimento da finalidade da decisão, deve ser preferido o menos gravoso aos direitos fundamentais.

Com a possibilidade de quebra de sigilo de dados fiscais e bancários, interceptação telefônica, interceptação telemática, ação controlada, captação ambiental de sinais eletromagnéticos, agente infiltrado, agente infiltrado virtual e o progressivo aumento do uso de novas tecnologias pela persecução (ERICSON; HAGGERTY, 2007, p. 37), o cúmulo da busca e da apreensão de elementos de prova digitais com outros meios deve ser evitado; a subsidiariedade veda que, desnecessariamente, vários meios ocultos de investigação sejam utilizados simultaneamente (COSTA ANDRADE, 2009, p. 115).

Ressalta-se que é inadmissível a burla à legislação pelo uso incorreto de analogia. Tourinho Filho (1992, p. 150) entende que, na analogia "a lei estabelecida para um determinado fato a outro se aplica, embora por ela não regulada, dada a semelhança ao primeiro". A analogia relaciona fatos, não cria premissas legais[285]. Com isso, as normas sobre

[281] Sobre o posicionamento dos autores espanhóis, vide: Valente (2006, p. 122).
[282] "É que ou ela será ilícita, podendo gerar efeitos jurídicos, ou ilícita e, nesse caso, não há que ser admitida para nenhum fim, nem como notícia de crime e nem como fonte de prova para nova investigação, sob pena de se estar concebendo um raciocínio contraditório e frontalmente violador da vedação constitucional às provas ilícitas (art. 5º, LVI) e até mesmo do artigo 157 do CPP." (SIDI, 2016, p. 292).
[283] Vide a nota n. 65, *supra.*
[284] Vide o item 4.3.2, *supra.*
[285] "A analogia não passa nem do geral para o particular (dedução), nem do particular para o geral (indução), mas de um particular para outro particular, do caso previsto para o caso não-previsto." (TORNAGHI, 1977, p. 157).

os diversos meios ocultos não podem ser combinadas para criar uma nova. Na situação presente da inexistência de lei que autorize a busca por ingresso remoto, por exemplo, não é possível utilizar-se de analogia para combinar o que é determinado para o agente infiltrado virtual (arts. 10-A a 10-D, da Lei 12.850, de 2013; arts. 190-A a 190-E, da Lei 8.069, de 1990) com o que é determinado para a busca e a apreensão (arts. 240 a 250, do CPP) e entender que seria possível a busca por ingresso remoto. Isso não é analogia entre fatos, é legislar.

A mesma premissa legal pode ser aplicada a situações diversas, mas semelhantes (CPP, art. 3º), como a aplicação dos requisitos do recurso extraordinário, normatizados nos artigos 1.029 a 1.035 do Código de Processo Civil, aos recursos extraordinários criminais. Contudo, isso não possibilita a edição de novas premissas legais (como uma nova modalidade de recurso).

Feitas essas observações, destaca-se que, excepcionalmente, o cúmulo de meios ocultos pode ser necessário – por exemplo, o uso do agente infiltrado para descobrir onde está um computador e a posterior busca e apreensão para obtê-lo. Todavia, somente no juízo sobre o meio oculto no caso concreto (explicitado na fundamentação, considerando a ofensa às garantias envolvidas, como à privacidade e à vedação de autoincriminação[286]) é possível aferir a proporcionalidade, não em abstrato (VALENTE, 2008, p. 64).

4.18 Limiar

A realização concreta da busca e da apreensão de elementos de prova digitais em consonância ao modelo constitucional do processo exige diversas releituras sobre a cautelaridade, os seus requisitos de admissão, o seu procedimento e a ilicitude probatória.

Mormente pelo imenso potencial de vigilância possibilitado pelas novas tecnologias e a virtualização da sociedade atual, o respeito ao modelo constitucional do processo é indispensável no controle racional da atuação dos sujeitos na persecução penal.

[286] Vide o item 5.3.1, *infra*.

5 TÉCNICAS PARA A PARTICIPAÇÃO ATIVA DO ACUSADO NA PERSECUÇÃO QUE UTILIZA O MEIO OCULTO DE INVESTIGAÇÃO DA BUSCA E A MEDIDA CAUTELAR DE APREENSÃO DE ELEMENTOS DE PROVA DIGITAIS

A persecução penal que utiliza os novos meios de investigação atrai o foco da construção do juízo para os atos realizados na fase investigativa, sem a participação prévia e consciente do investigado e visando a sua autoincriminação (introdução e capítulo 2, *supra*).

Após tratar da tecnologia (capítulo 3, *supra*) e dos limites legais (capítulo 4, *supra*) relacionados à busca e à apreensão de elementos de prova digitais no modelo constitucional do processo, a pesquisa pode enfrentar melhor como assegurar a participação do acusado na persecução que utiliza o meio oculto da busca e a medida cautelar de apreensão de elementos de prova digitais.

Destaca-se que a pesquisa é também orientada pela teoria do caso (BENAVENTE CHORRES, 2011, p. 48).[287] O que, neste trabalho, significa que seu objetivo é otimizar a participação ativa do acusado na produção da prova nas situações concretas da persecução que utiliza a busca e a apreensão de elementos de prova digitais.

Posto isso, ressalta-se que a participação ativa do acusado na persecução penal é determinação constitucional. Numa democracia, as decisões são fruto da atuação dos destinatários normativos e da consideração com esta atuação (GONÇALVES, 1992, p. 171-173). O Estado Democrático de Direito une a legitimidade pela participação do cidadão na construção das decisões políticas (que se reconhece como coautor das decisões) com os compromissos democraticamente criados que vinculam e estimulam essa participação,[288] afirmando o Direito e fazendo cumprir a determinação da Constituição em seu art. 1º, parágrafo único: "[...] Todo o poder emana do povo" (BRÊTAS, 2018a).

É o processo que possibilita a construção do Estado Democrático de Direito:[289]

> […] o processo constitucional concorre para o fortalecimento dessa legitimação democrática do Estado, seja o processo constitucional legislativo, seja o processo

[287] Vide a introdução, *supra.*

[288] "Em tal processo legislativo democrático, a soberania popular e os direitos humanos, concebidos, desde o início, como princípios jurídico-constitucionais, fazem valer o nexo interno entre autonomia pública e autonomia privada dos cidadãos, essas, também, consideradas, desde o início de forma jurídica, cooriginária e com igual relevância, em contraponto com as tradições republicana e liberal que relevam apenas uma delas e as compreendem inicial e respectivamente ou como autodeterminação ética ou como autonomia moral. Essa compreensão buscará também desfazer o que parece ser um paradoxo acerca dos fundamentos de legitimidade do Direito moderno, porque, para uma Teoria Discursiva do Direito, os destinatários das normas jurídicas, enquanto sujeitos privados, pelo processo democrático, enquanto cidadãos, tornam-se autores dos seus próprios direitos e deveres." (CATTONI DE OLIVEIRA, 2016, p. 212-213).

[289] Eixo que dá nome à linha de pesquisa do Programa de Pós-graduação em Direito Processual da PUC Minas, onde este trabalho foi desenvolvido.

> constitucional jurisdicional. Por meio do primeiro, o povo pode fiscalizar e participar do controle democrático de constitucionalidade da elaboração da norma jurídica. Por meio do segundo, como destinatário da norma jurídica produzida, qualquer do povo (sujeito constitucional) poderá provocar a jurisdição estatal, visando a controlar em concreto sua constitucionalidade, quando posta em vigor, notadamente se a norma jurídica estiver em colisão com os direitos e garantias fundamentais positivados no texto constitucional (BRÊTAS, 2018b, p. 30).

Pelo exercício do contraditório, especialmente, é conferida legitimidade[290] à decisão jurídica; é por ele que as partes expressam suas razões e influenciam na construção do procedimento (NUNES, 2008, p. 227).[291] Portanto, a participação do acusado na persecução penal é determinação constitucional (Constituição, artigo 1º, inciso II e parágrafo único, e artigo 5º, inciso LV) e exigência para a legitimidade das decisões.

Somado a isso, nas palavras de José Alfredo de Oliveira Baracho:

> O exercício da função jurisdicional leva em conta os princípios gerais estabelecidos na Constituição expressamente e que afetam a todo tipo de jurisdição. É princípio básico o que garante o *direito e ação e de defesa*. Na primeira situação, exclui-se toda limitação injustificada à possibilidade de se apresentarem em juízo as situações jurídicas subjetivas, atribuídas pela lei ao particular, protegendo-o de eventuais violações. Assegura-se a todos os que são parte em juízo o direito de fazer valer suas razões, através da defesa pessoal, por meio da defesa técnica. (BARACHO, 1995, p. 60).

A participação do acusado viabilizada pelas garantias de defesa alcança a perfectibilidade por técnicas adaptadas às especificidades do processo penal (BARROS, 2008b, p. 14-17).

Como pontua Agamben, a técnica é um agir humano que visa uma finalidade e:

> enquanto nos limitarmos a olhar para a técnica pela perspectiva da instrumentalidade, não perceberemos a sua verdadeira natureza e continuaremos presos à ilusão de a dominarmos. Só se compreendermos o instrumento como um modo de causalidade, então a técnica se revelará por aquilo que é, ou seja, como 'destino de um desvelamento'. (AGAMBEN, 2017, p. 91-92).

[290] "[…] legítima é a decisão advinda não de um *a priorismo* racional conceitual, mas de uma atividade construtora que se projeta no mundo vivido (agir comunicativo) juridicamente democrático, que tem como seus autores aqueles que sofrerão sua incidência, ou seja: provimento atingido através de atividade processual." (CARVALHO, 2009, p. 279).

[291] Atrelado a isso, o contraditório exige não surpresa sobre todas as questões: a resolução de qualquer questão, mesmo as de conhecimento oficioso, exige a provocação do juiz para que as partes se manifestem previamente (NUNES, 2008, p. 229). Conforme Dierle Nunes (2008, p. 230): "Em relação às partes, o contraditório aglomera um feixe de direitos dele decorrentes: a) direito a uma cientificação regular durante todo o procedimento, ou seja, uma citação adequada do ato introdutivo da demanda e a intimação de cada evento processual posterior que lhe permita o exercício da defesa no curso do procedimento; b) o direito à prova, possibilitando-lhe sua obtenção toda vez que esta for relevante; c) em decorrência do anterior, o direito de assistir pessoalmente a assunção da prova e de se contrapor às alegações de fato ou às atividades probatórias da parte contrária ou, mesmo, oficiosas do julgador; e d) o direito de ser ouvido e julgado por um juiz imune à ciência privada (*private informazioni*), que decida a causa unicamente com base em provas e elementos adquiridos no debate contraditório."

Toda técnica racional[292] é influenciada por um saber organizado (por isso Abbagnano [2007, p. 942] afirma que tecnologia é "O mesmo que técnica").

A hipótese deste trabalho é de que determinadas técnicas racionais (regidas pelo Direito) asseguram a participação ativa do acusado na persecução que utiliza a busca e a apreensão de elementos de prova digitais – que é diferente da do direito penal repressor tradicional (introdução e capítulo 2, *supra*).

Estas técnicas são diretamente relacionadas às mudanças causadas pelos meios ocultos de investigação na persecução: em relação à diminuição da fronteira entre repressão e prevenção de delitos, a cadeia de custódia de elementos digitais, por possibilitar perceber se a investigação foi prospectiva ou baseada em elementos concretos preexistentes; em relação ao aumento do espaço da polícia e da importância da fase investigativa, o direito de confrontar os agentes públicos e privados envolvidos em audiência; em relação à tendência para a privatização da recolha estatal de informação, a proteção contra a autoincriminação por medidas antiforenses e pela atuação judicial na proteção preventiva das garantias processuais; e em relação ao progressivo aumento do uso de novas tecnologias na persecução penal, a paridade entre as partes no espaço virtual pela ampliação do uso dessas tecnologias pelo acusado.

Na sequência, isso será aprofundado.

5.1 Relacionada à diminuição da fronteira entre prevenção e repressão de delitos

Para a perfectibilidade (ANDOLINA; VIGNERA, 1997, p. 9) das garantias processuais do contraditório, da ampla defesa, da paridade entre as partes, da fundamentação e do estado de inocência – principalmente em sua acepção probatória – e da inadmissibilidade das provas ilícitas, a cadeia de custódia é técnica indispensável e está diretamente relacionada à diminuição da fronteira entre prevenção e repressão dos delitos: ela possibilita a fiscalização sobre se os meios de investigação foram realizados amparados em elementos concretos preexistentes ao ato investigador, para apurar um evento pretérito, ou se foram realizados sem justa causa e para investigar prospectivamente (PRADO, Geraldo, 2019, p. 107).

Ferir a intimidade, a vida privada, a honra, a imagem, o sigilo de dados e das comunicações telefônicas e a dignidade da pessoa humana de maneira extrema como na

[292] Como demonstra Aroldo Plínio Gonçalves (1992, p. 22-26), baseado em Weber, historicamente a técnica antecede à ciência. Nem toda técnica é organizada racionalmente, mas, influenciada pela ciência, a técnica pode ser modificada em acordo com finalidades previamente estabelecidas. Ou seja, as técnicas podem ser racionais ou irracionais. São racionais se influenciadas por um saber organizado previamente demarcado que possibilita a sua modificação (como o Direito baseado na legalidade); e são irracionais as influenciadas por crenças que não possibilitam a sua modificação (como os ritos religiosos). Vide: Abbagnano (2007, p. 939-941).

realização dos meios ocultos de investigação não é algo banal. É medida de *última ratio* somente justificada na investigação de crimes graves, na situação de impossibilidade demonstrada de investigação por outros meios (subsidiariedade), com proibição do excesso, se for adequado para obter resultado relevante, com limite de tempo e espaço, com demarcação clara do evento do passado objeto da investigação, demonstrada por elementos concretos, com prévia autorização judicial e respeito absoluto à legalidade (VALENTE, 2009).

O Código de Processo Penal obriga que a busca e a apreensão de elementos de prova digitais investiguem apenas eventos do passado (artigo 240, §§ 1º e 2º)[293] em decorrência da exigência de suspeita do cometimento de crime grave fundamentada em elementos concretos prévios para se invadir extremamente a vida privada e lesar garantias processuais.

Somente com a técnica da cadeia de custódia é possível fiscalizar se os atos investigativos foram repressivos ou prospectivos.

5.1.1 Cadeia de custódia

A cadeia de custódia tem como marco histórico no Brasil o julgamento do *Habeas Corpus* n. 160.662, pelo Superior Tribunal de Justiça. No caso objeto desse julgamento, segundo a ministra Assusete Magalhães (2014, p. 518-520, 533):

> Em Habeas corpus apreciado recentemente, tive a oportunidade de me manifestar, em voto submetido ao Colegiado da 6ª Turma do Superior Tribunal de Justiça, favoravelmente à pretensão da defesa, no sentido de anular as provas obtidas mediante a quebra dos sigilos telefônico e telemático, por sua inidoneidade como fonte de prova, em face de sua fragmentação e do extravio de parte do produto das interceptações, ainda no âmbito policial. Os elementos de prova questionados foram apurados na denominada Operação Negócio da China, deflagrada para investigar a eventual ocorrência de negociações fictícias, com o objetivo de dissimular a natureza de valores supostamente provenientes da prática do delito de descaminho, mediante a ilusão parcial do tributo devido na importação de produtos, por sociedade empresária, resultando na denúncia de 14 agentes. No writ impetrado no Superior Tribunal de Justiça, discutia-se, entre outras teses defensivas, a ilicitude do produto das interceptações telefônica e telemática, em virtude da sua fragmentariedade e perda de sua unidade, dada a existência de áudios telefônicos descontínuos e mensagens eletrônicas não sequenciais, inclusive vinculadas à conta de e-mail do principal denunciado, as quais, após captadas, não foram armazenadas pelo provedor EMBRATEL, nem preservadas pela autoridade policial à qual direcionadas, com a perda irreparável da aludida fonte de prova de interceptação telemática. Ponderou o impetrante, na ocasião, que a ausência de preservação integral dos elementos informativos impedia os acusados de exercerem, de forma ampla, o contraditório e a ampla defesa, dada a impossibilidade de refutarem a tese acusatória, apresentando interpretação diversa do conjunto probatório. Restou demonstrado, no aludido processo, que, apesar de franqueado, aos acusados, o acesso aos autos, parte das provas obtidas, a partir da interceptação telemática, foi

[293] Assim como a Lei n 9.296, de 1996, artigo 2º, I, e a Lei 12.850, artigo 10, § 2º.

> extraviada, ainda na Polícia Judiciária, e o conteúdo dos áudios telefônicos não foi disponibilizado da forma como captado, havendo descontinuidade nas conversas e na sua ordem, não sendo, portanto, tais provas encartadas nos autos do Inquérito Policial e da Ação Penal. Na impetração, demonstrou-se, mediante prova pré-constituída, a impossibilidade de rastreamento da origem da prova, em razão do extravio de parte significativa do produto das interceptações telemáticas, mantidas sob custódia da Polícia Judiciária, fato atestado pela autoridade policial, pelo provedor de internet e pelo Juízo. […] Portanto, constatada, na situação ora em exame, a ilicitude da prova resultante das interceptações telefônica e telemática, por inobservância do método probatório constitucionalmente adequado (art. 5º, LVI, da CF), em razão do desaparecimento parcial do material informativo e de sua seleção unilateral, no âmbito da Polícia Judiciária, o que afetou a unidade e a comunhão da prova, revelando uma atuação estatal fora dos limites legais e constitucionais, na tutela da prova, restou caracterizada a violação aos direitos fundamentais dos acusados, não havendo outro caminho senão determinar o seu integral desentranhamento (arts. 5º, LVI, da CF e 157 do CPP) e a verificação da existência de eventual prova ilícita por derivação, nos termos do art. 157, §§ 1º e 2º, do CPP.

A argumentação das partes é corroborada – ou não – pela prova. O elemento de prova submetido, em contraditório, ao meio de prova, produz a prova (LEAL, Rosemiro, 2021, p. 197). Somente após a realização, em contraditório, do meio de prova sobre o elemento de prova existe a prova apta a corroborar – ou a refutar – um discurso sobre um evento e a produzir efeitos de um discurso "verdadeiro" ou de um "falso":

> Chamamos «prova» a um método estabelecido para controlo das hipóteses históricas: quando nenhuma é experimentável, nem mesmo através de longas meditações, o enunciado escapa aos que qualificam o verdadeiro e o falso; os sermões sobre o inferno têm um sentido, tão truculento que a pedagogia religiosa neles construiu poderosas instituições, mas, com base nas técnicas experimentais conhecidas, não são verificáveis nem refutáveis, se bem que alguns argumentos (por exemplo, a história psicológica das respectivas imagens) os assinalem como algo improváveis. (CORDERO, 1999, p. 16).

Um elemento de prova obtido pela polícia e utilizado pela acusação numa denúncia não é apto a, por si, corroborar o discurso do acusador – lhe falta a realização do meio de prova em contraditório que cria a prova (no juízo natural da causa, com oralidade e imediação).[294]

Sem a possibilidade de a defesa participar da construção da prova sobre um elemento de prova, produzir novas provas sobre o mesmo elemento de prova (como a perícia sobre um *hard drive*) e fiscalizar a licitude na obtenção do elemento de prova, ocorre evidente ofensa à ampla defesa. Para realizar esses atos, o elemento de prova deve estar preservado na instrução judicial e deve ter sido demonstrada a totalidade da sua cadeia de custódia.

Nos termos do art. 158-A, do Código de Processo Penal: "Considera-se cadeia de custódia o conjunto de todos os procedimentos utilizados para manter e documentar a história

[294] Vide o item 4.1, *supra.*

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" (BRASIL, 2021a). Um procedimento é uma sequência de normas, atos e posições subjetivas (lícitas, facultadas ou devidas), em que a realização do ato posterior tem como pressuposto[295] a realização do ato anterior válido (FAZZALARI, 1996, p. 77-78). Como conceituado pelo Código, a reunião de todos os procedimentos que preservem a autenticidade e demonstrem a integridade do elemento de prova é a cadeia de custódia. No conjunto de procedimentos que compõem a cadeia de custódia, o art. 158-B expressamente normatiza: a) o reconhecimento (distinção de um elemento como de potencial probatório para a construção do juízo sobre o caso penal); b) o isolamento (preservação do elemento de prova e do ambiente da sua coleta); c) a fixação (identificação do elemento de prova, inclusive com fotos, filmagens e croqui); d) a coleta (recolhimento do elemento); e) o acondicionamento (procedimento de embalagem, registro da identificação e anotação da data, hora e nomes daqueles que coletaram e acondicionaram o elemento de prova); f) o transporte (mudança de local do elemento de prova); g) o recebimento (transferência da posse do elemento de prova); h) o processamento (perícia); i) o armazenamento (guarda e preservação do elemento de prova); e j) o descarte (despojamento do elemento de prova) – sendo que cada elemento de prova é diferente e exige metodologia diferente de tratamento.

Na lição de Geraldo Prado (2014, p. 86), a finalidade da técnica da cadeia de custódia é "assegurar a fiabilidade do elemento probatório, ao colocá-lo sob proteção de interferências capazes de falsificar o resultado da atividade probatória". Com a notícia do crime já torna-se possível o reconhecimento de um elemento de prova e deve ser iniciada a cadeia de custódia (como uma ligação para a Polícia Militar em que o agente orienta o noticiante a não alterar o local do suposto crime).[296] Do reconhecimento do elemento ao seu descarte, a cadeia de custódia assegura que o elemento de prova coletado num momento é o mesmo que será periciado e influenciará a construção do juízo (mesmidade); ela possibilita o controle sobre quem, como, quando, onde e porquê teve contato com o elemento de prova; preserva o elemento de prova para contraprovas; aumenta a credibilidade das provas produzidas; possibilita o rastreamento da relação entre as provas para aferir a ilicitude por derivação; e

[295] "Pressuposto, em linguagem filosófica e da lógica, é premissa não explícita, e essa […] é a proposição da qual são extraídas outras proposições, pelo processo de inferência, e [...] as conclusões podem se tornar novas premissas de novas conclusões, na cadeia de proposições, no raciocínio dedutivo." (GONÇALVES, 1992, p. 110).

[296] CPP, art. 158-A, §§ 1º e 2º. Lembra-se que: "Com a notícia do crime inicia-se o processo verdadeiramente […] E deste fato – instituição do *processo* desde a notícia do crime – são extraídas diversas consequências tanto no âmbito da atividade probatória quanto na influência sobre os estatutos jurídicos dos diversos sujeitos que são personagens obrigatórios" (PRADO, Geraldo, 2019, p. 37-38).

rejeita presunções, pela desconfiança da fiabilidade probatória[297] e exigência de demonstração concreta do cumprimento dos procedimentos que mantêm e documentam a história cronológica do elemento de prova. Enfim, a técnica da cadeia de custódia é indispensável para a perfectibilidade da ampla defesa, sendo que a defesa técnica tem direito de acesso a todos os seus registros e ao elemento de prova preservado[298] (PRADO, Geraldo, 2019, p. 37-38, 65-66, 95-96, 103) (VALENTE, 2020, p. 51-54) (EDINGER, 2016).

Mitigando a inquisitoriedade do inquérito, a cadeia de custódia impede a arbitrária seleção do que integrará o processo ao viabilizar à defesa – e ao judiciário – o conhecimento e fiscalização dos atos investigativos (PRADO, Geraldo, 2019, p. 120, 130). Somado a isso, a possibilidade de controle da ilicitude da investigação desestimula os agentes públicos a desrespeitarem o Direito (MARINHO MARQUES, 2016).

Todos os atos dos procedimentos que compõem a cadeia de custódia devem ser realizados pelos agentes públicos (CPP, art. 158-C, § 1º) – a posição subjetiva dos agentes públicos nos procedimentos da cadeia de custódia é de dever, não de faculdade; não lhes cabe a possibilidade válida de não realizar os atos da cadeia de custódia e violar as garantias do modelo constitucional do processo, como a ampla defesa e a inadmissibilidade das provas ilícitas. Sempre que a cadeia de custódia for irregular – independente da boa-fé ou má-fé dos agentes públicos[299] –, a prova resultado do meio de prova sobre o elemento custodiado é inadmissível, o elemento torna-se imprestável para novas provas e tanto o elemento deve ser descartado como todas as provas produzidas a partir dele devem ser desentranhadas dos autos, assim como todas as dele derivadas (Constituição de 1988, art. 5º, LVI; CPP, art. 157).[300] Mais rigoroso que o regime de nulidades, que analisa o prejuízo do ato, o descumprimento da cadeia de custódia implica inadmissibilidade, a prova não pode sequer integrar o procedimento e deve ser imediatamente excluída (PRADO, Geraldo, 2019, p. 124-131).[301]

[297] "A fiabilidade probatória refere-se ao esquema de ingresso do elemento probatório no procedimento em cujo âmbito, posteriormente, este elemento poderá ser objeto de avaliação e diz muito especificamente com a questão dos controles epistêmicos, compreendidos nesta etapa como 'controles de entrada'." (PRADO, Geraldo, 2019, p. 88).

[298] Constituição de 1988, art. 5º, LIV e LV. Convenção Americana sobre Direitos Humanos, art. 8, 2, *c.* Lei n. 8.906, de 1994 (Estatuto da Ordem dos Advogados do Brasil), art. 7º, XIV. Lei n.º 13.869, 2019 (abuso de autoridade), art. 32. Súmula Vinculante n. 14, do Supremo Tribunal Federal.

[299] *E.g.*, no caso *Brady v. Maryland*, de 1963, a *Supreme Court of the United States* (UNITED STATES, 2021), julgando um caso de latrocínio, decidiu que a supressão de elementos de prova pela acusação, independentemente de sua boa-fé ou má-fé, viola o devido processo legal. "A supressão indevida de elementos informativos opera efeito impeditivo de emprego das informações remanescentes, que carecem de «suficiência probatória». O material probatório remanescente está afetado pela referida quebra e configura prova ilícita, pois não há como sujeitá-lo, adequadamente, aos procedimentos de comprovação e refutação. A decisão política que proscreve provas ilícitas escuda-se em experiência de «preenchimentos posteriores de lacunas» relacionadas aos requisitos legais para as providências cautelares. Trata-se de algo equivalente à «lavagem de provas ilícitas», que em concreto sabota o sistema normativo de controles epistêmicos do processo." (PRADO, Geraldo, 2014, p. 87).

[300] Vide o item 4.16, *supra.*

É dever da acusação cumprir a cadeia de custódia. O estado de inocência, como norma probatória, implica na carga probatória que busque alterar esse estado caber à acusação; por óbvio, somente por provas lícitas (PRADO, Geraldo, 2014, p. 81) (MORAES, 2010, p. 461-468) (GIACOMOLLI, 2014, p. 96-97, 102-103). O estado de inocência e a opção legislativa de estabelecer a posição subjetiva do agente público no cumprimento da cadeia de custódia como dever (CPP, art. 158-C, § 1º) implicam o dever de a acusação cumprir e demonstrar a cadeia de custódia. Todos os atos dos procedimentos que compõem a cadeia de custódia devem ser documentados[302] pelos agentes responsáveis e demonstrados pela acusação: não se presume o cumprimento da cadeia de custódia, cada singular cumprimento de seus atos, incluindo a preservação do elemento de prova (CPP, art. 158-B, IX), deve ser demonstrado pelo órgão acusador, a quem cabe a carga probatória. Caso assim não se faça, a cadeia de custódia é considerada inexistente:

> A cadeia de custódia não só deve ser feita, como deve ser provada. O formato da cadeia de custódia prova o que se realizou e daí uma de suas cardeais finalidades. Isto não é mais que desenvolvimento do milenar apotegma, o que não se prova não existe; então, se não se prova a cadeia de custódia, esta não existe. (BAUTISTA, 2021, p. 3, tradução nossa[303]).

Finalmente, pelos registros dos procedimento que compõem a cadeia de custódia é possibilitada a fiscalização sobre se os meios ocultos de investigação tinham como objeto fatos do passado, cumpriram os requisitos legais e foram autorizados judicialmente, fundamentados em elementos prévios de risco concreto, iminente e substancial à futura participação das partes ou se a investigação foi prospectiva, ilegal e sem justa causa:[304] basta confrontar a cadeia de custódia com os demais atos da persecução penal, considerando, por exemplo, o momento de realização dos atos.

[301] Sendo cabível, também, a responsabilidade criminal, administrativa e civil dos agentes públicos (como por prevaricação: CP, art. 319). Sobre a responsabilidade do Estado, vide: Brêtas (2004, p. 13-60).

[302] Na lição de Geraldo Prado (2021, p. 168-169), a documentação "[…] deve descrever: a) os protocolos de coleta/extração do dado ou elemento probatório, de sorte a comprovar que não houve supressão, inclusão ou alteração de elementos que afete a qualidade de «prova autêntica e íntegra», em atenção ao princípio da «mesmidade»; b) os cuidados que foram adotados, voltados à transparência do processo anterior, que igualmente demonstrem que houve controle por terceiros da coleta/extração, acondicionamento, transporte e preservação do elemento probatório, isso em reverência ao princípio da «desconfiança»; c) a cadeia de pessoas que tiveram contato com o elemento probatório e os respectivos títulos e motivos, se funcionário público ou terceiro à administração, se para transporte ou exame do vestígio etc."

[303] "La cadena de custodia no solo debe hacerse, sino que debe probarse. El formato de cadena de custodia prueba que se realizó y de ahí una de sus cardinales finalidades. Esto no es más que desarrollo del milenario apotegma, lo que no se prueba no existe; entonces, si no se prueba la cadena de custodia, ésta no existe."

[304] Como dito (item 5.1), os meios ocultos só podem ser autorizados para investigar fatos passados (art. 2º, I, da Lei n. 9.296, de 1996; art. 10, § 2, da Lei 12.850; CPP, art. 3º), em função da exigência de suspeita do cometimento de crime grave fundamentada em elementos concretos prévios; somente com essa demonstração por elementos prévios é possível, legalmente e, após decisão judicial, devassar a vida privada e lesar direitos fundamentais pelos meios ocultos de investigação.

A resistência de uma hipótese no processo só pode ser aferida se a prova que corrobora uma argumentação puder ser fiscalizada em todos os atos que a construíram (desde a obtenção do elemento de prova, passando pela realização do meio de prova e pelo registro do resultado probatório). Deve ser possibilitado tanto o rastreamento probatório, como a fiscalização sobre a maneira pela qual foi obtido o elemento de prova que possibilitou a criação de uma prova; e esse elemento de prova deve ser preservado para contraprovas futuras. Isso só tem como ser obtido pela cadeia de custódia.

Portanto, a cadeia de custódia é técnica que aumenta a efetivação do modelo constitucional do processo (BARROS, 2008b) e barreira contra o controle constante ultrarrápido e preferencialmente preventivo da sociedade de controle. Em função da investigação por meios ocultos exigir suspeita do cometimento de crime grave, fundamentada em elementos concretos prévios para se invadir extremamente a vida privada e lesar direitos fundamentais, qualquer medida investigativa ou probatória que se valha de prospecções pode ser rastreada pela cadeia de custódia e considerada inadmissível para a construção do juízo.

5.1.2 Cadeia de custódia de elementos digitais

Especificamente em relação aos elementos de prova digitais, a cadeia de custódia possibilita fiscalizar se a busca e a apreensão foram realizadas com base em elementos concretos prévios ao seu deferimento, sobre evento do passado, ou em pescaria probatória.[305] Por isso, ela é estrategicamente importante contra a diminuição da fronteira entre a repressão e prevenção de delitos na sociedade de controle.[306]

A cautelar probatória existe para preservar a confiabilidade, integridade e disponibilidade do elemento de prova contra riscos concretos, iminentes e substanciais à futura atuação das partes (item 4.1, *supra*). Não há sentido em realizar a apreensão cautelar do elemento digital e não o preservar. A sua preservação, assim como a documentação de sua história cronológica, ocorre pela realização dos procedimentos componentes da cadeia de custódia.[307]

Qualquer suspeita concreta de violação à cadeia de custódia (como o rompimento de um lacre ou o apagamento de metadados) compromete a sua confiabilidade e torna o elemento de prova inadmissível para o procedimento (VALENTE, 2020, p. 46-47, 88-90).

[305] Vide o item 4.7, *supra.*
[306] Vide o item 2.2, *supra.*
[307] "A preservação das fontes de prova é concebida como remédio jurídico-processual contra o desequilíbrio inquisitório, caracterizado pela seleção e uso arbitrário de elementos pelas agências repressivas." (PRADO, Geraldo, 2019, p. 120).

Ressalta-se novamente que a demonstração do cumprimento da cadeia de custódia de elementos com potencial incriminador é dever probatório da acusação (PRADO, Geraldo, 2014, p. 81). Na denúncia, toda a documentação relacionada à cadeia de custódia deve ser anexada para que a defesa possa exercer o contraditório quanto a isso na resposta à acusação e o juízo possa deferir ou indeferir a realização do meio de prova sobre o elemento de prova objeto da cadeia de custódia. Se a demonstração da realização dos procedimentos da cadeia de custódia não ocorrer, a prova é inadmissível e os elementos de prova devem ser desentranhados e inutilizados (Constituição, art. 5º, LVI; CPP, art. 157).[308]

Como os elementos digitais são *bits*, "1" ou "0" na notação binária utilizada pelo computador (item 3.1.1.1, *supra*), e como é muito fácil alterá-los e apagar os registros da alteração, a importância da cadeia de custódia do elemento digital é colossal.

Em função da busca e da apreensão na legislação brasileira dirigirem-se, principalmente, para a apreensão do dispositivo eletrônico de armazenamento, ganha destaque a necessidade da criação de cópia de segurança do dispositivo apreendido. Como recomenda a Associação Brasileira de Normas Técnicas na NBR ISO/IEC 27037:2013 (ABNT, 2013b, p. 10):

> Convém que o método de aquisição utilizado produza uma cópia de evidência digital da potencial evidência digital ou do dispositivo digital que pode conter a potencial evidência digital. Recomenda-se que ambas as fontes originais e a cópia da evidência digital sejam verificadas com uma função de verificação comprovada (comprovada precisão, naquele determinado momento) que é aceitável para o indivíduo que utilizará a evidência. É recomendado que a fonte original e cada cópia de evidência digital produzam o mesmo resultado de função de verificação.

As cópias, em primeiro lugar, asseguram que não existiu adulteração do elemento digital original, vez que a perícia ocorrerá nelas e não no elemento original. Em segundo lugar, os elementos originais não são modificados. Em terceiro lugar, os elementos originais permanecem disponíveis para novas perícias. Ou seja, é garantida a confiabilidade, a integridade e a disponibilidade (NÚÑES, 2016, p. 89).[309]

Pela cadeia de custódia dos elementos digitais são percebidos os atos ilegais de investigação prospectiva e pescaria probatória. Ela também auxilia a aferição da ilicitude por

[308] "A etapa de admissibilidade da acusação está concebida para, estrutural e funcionalmente, impedir essas distorções inquisitórias e para isso é essencial que o juiz, no lugar de preservar na 'cultura das corporações', de matriz inquisitorial, que para além das mais elementares objeções metodológicas, acredita em uma magistratura 'depositária da função de busca da verdade', assuma a função de fiscal da legalidade das práticas investigatórias, dos elementos informativos e da própria fiabilidade da acusação, que não pode ser leviana ou temerária." (PRADO, Geraldo, 2019, p. 75).

[309] No julgamento do Agravo Regimental no Recurso em *Habeas Corpus* n. 143.169, o Superior Tribunal de Justiça decidiu que a inexistência de cópia dos elementos digitais apreendidos e que a possibilidade de que perícias tenham ocorrido com o acesso direto dos peritos aos elementos originais – e não a cópias – configuram quebra da cadeia de custódia.

derivação.[310] Por isso, ela é fundamental contra a vigilância ininterrupta da sociedade de controle.

Padrões internacionais de identificação, coleta, aquisição e preservação dos elementos digitais são demarcados na ISO/IEC 27037 (ABNT, 2013b), que orienta como assegurar a confiabilidade, integridade e a disponibilidade (completude, autenticidade, reprodutibilidade) dos elementos apreendidos, com transparência técnica, rastreabilidade e auditabilidade.

A confiabilidade é a fiabilidade do elemento digital, resultado da limitação de acesso a ele somada aos demais comportamentos que impeçam a sua adulteração. A integridade é a ausência de modificação do elemento digital, sua sequência de *bits* (informações, dados e metadados) não pode ser alterada, o elemento digital apreendido deve ser o mesmo que será periciado, disponibilizado às partes e influenciará o juízo. A disponibilidade consiste na gestão do elemento digital caber não apenas ao juiz, mas também às partes, que devem poder ter acesso à totalidade dos elementos (completude), conferir a sua integridade (autenticidade) e reproduzir os métodos utilizados pela computação forense, em condições diferentes e em qualquer tempo permitido pelo procedimento (reprodutibilidade) (ABNT, 2013b) (KIZZA, 2017, p. 46-47) (LIN, 2018, p. 18).

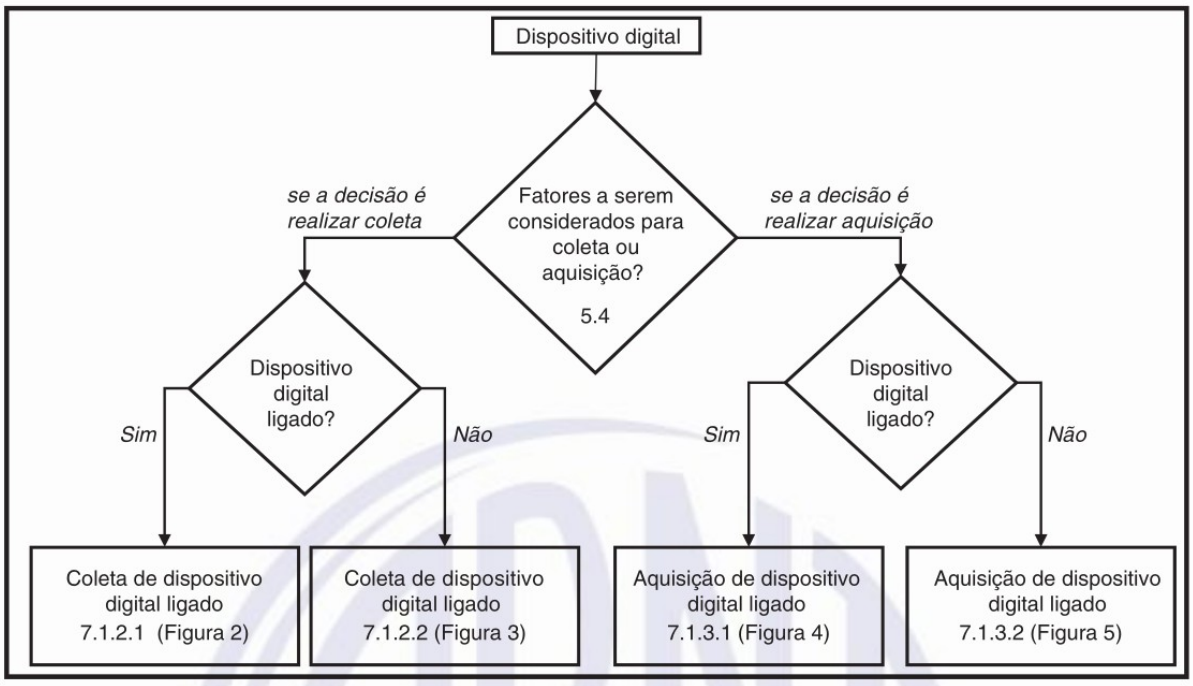
O requisito da transparência técnica é configurado pela demarcação explícita da metodologia utilizada pela computação forense, ou seja, do marco teórico – conjunto de enunciados teóricos utilizados para o teste das hipóteses – e da operacionalização – conjunto de atos concretos realizados, incluindo como, por que, onde e quando (GALUPPO, 2003, p. 116-117). A rastreabilidade é a possibilidade de identificar os atos relacionados ao elemento digital, desde seu reconhecimento ao descarte. A auditabilidade é a possibilidade de terceira pessoa avaliar as atividades realizadas, fiscalizando o método, a aplicação de técnicas e os resultados obtidos; o que só é viável com acesso aos elementos digitais e a todos os registros dos atos (ABNT, 2013b, p. 7).

Para efetivar estes requisitos, a cadeia de custódia de elementos digitais deve ser composta por procedimentos específicos adequados às suas particularidades.

A Associação Brasileira de Normas Técnicas (ABNT) endossou integralmente o ISO/IEC 27037 na Norma Brasileira (NBR) 27037:2013 e sintetizou determinados procedimentos de coleta (apreensão material do dispositivo que armazena os elementos digitais) e aquisição (criação de cópia dos elementos digitais em dispositivo externo) nas figuras seguintes:

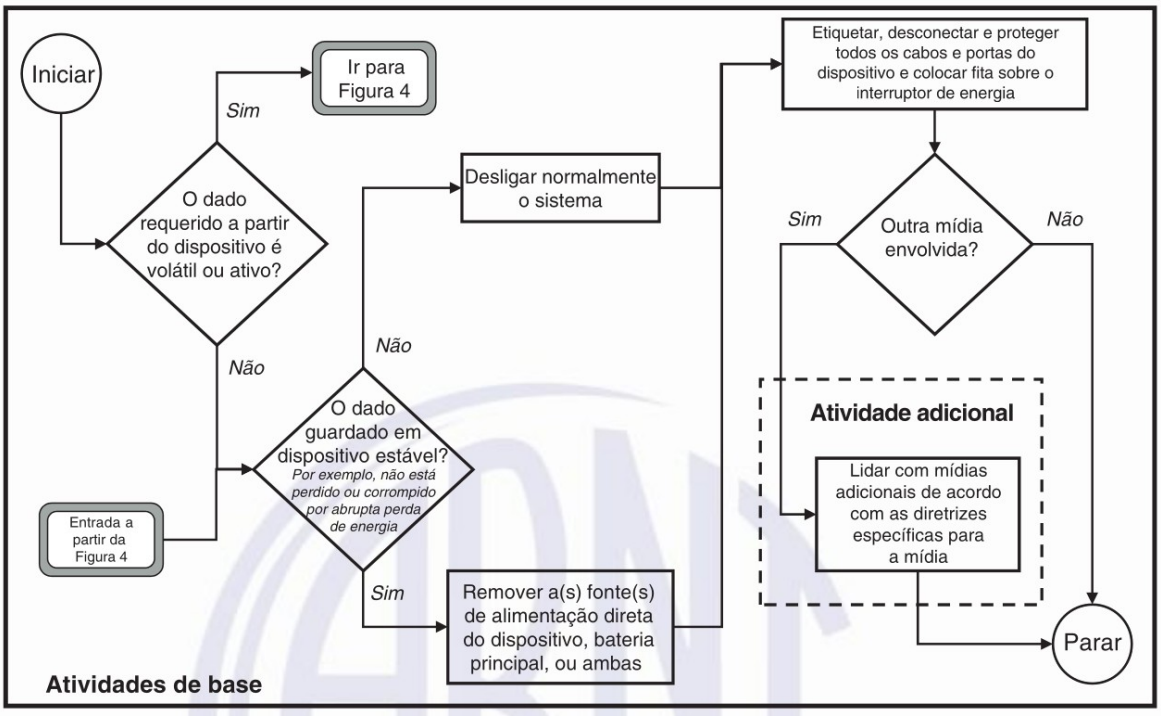
[310] Vide o item 4.16, *supra.*

Figura 7 – Diretrizes para tomada de decisão para coleta ou aquisição da potencial evidência digital



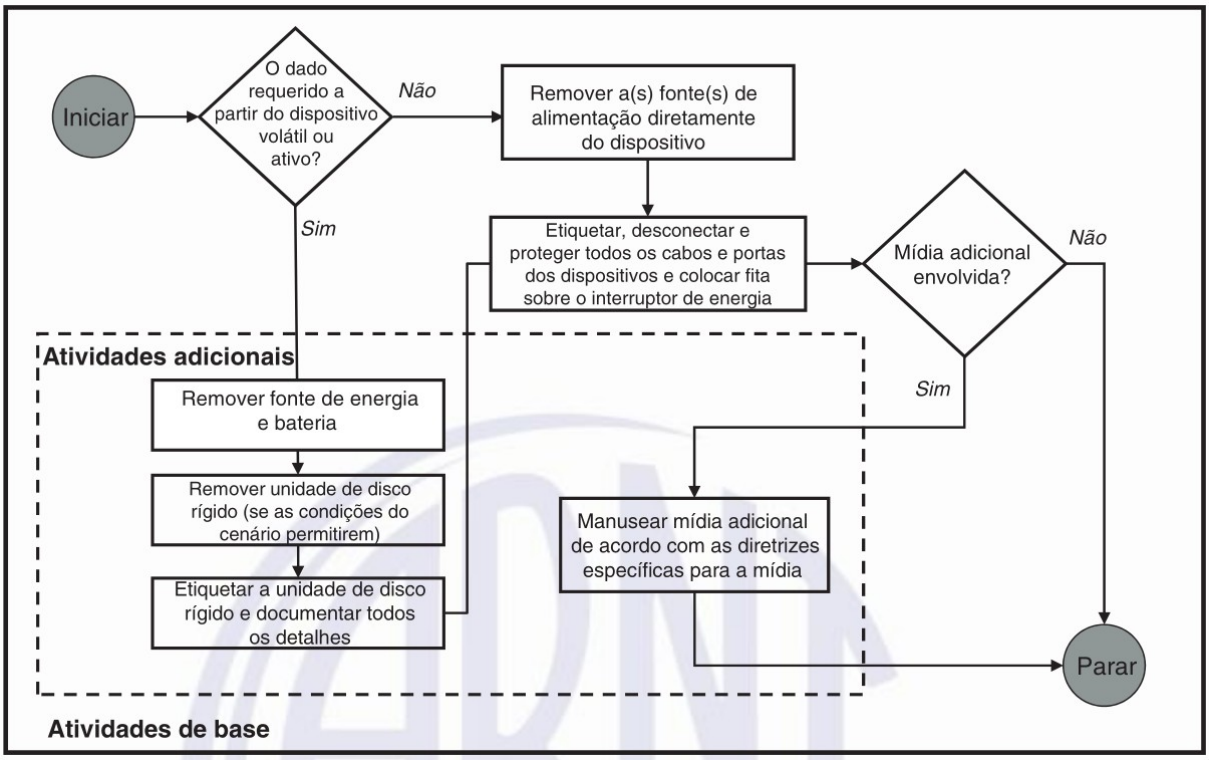
Fonte: ABNT (2013b, p. 24)

Figura 8 – Diretrizes para coleta de dispositivo digital ligado



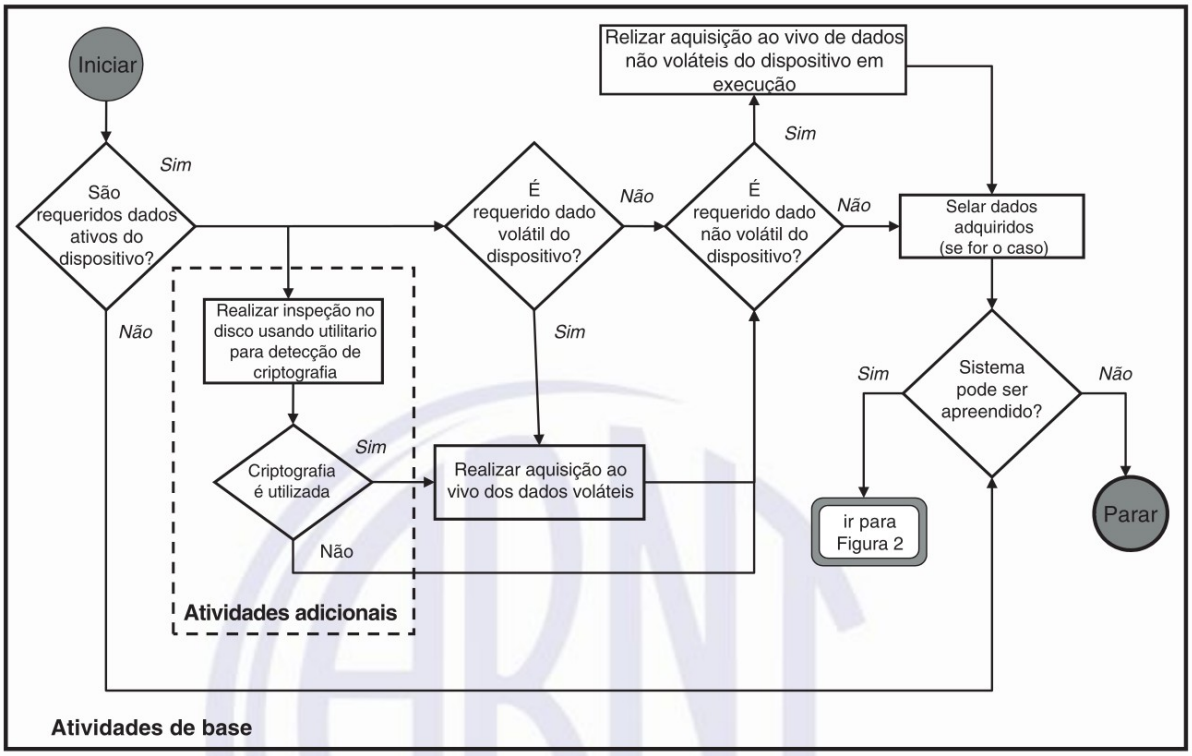
Fonte: ABNT (2013b, p. 25)

Figura 9 – Diretrizes para coleta de dispositivo digital desligado



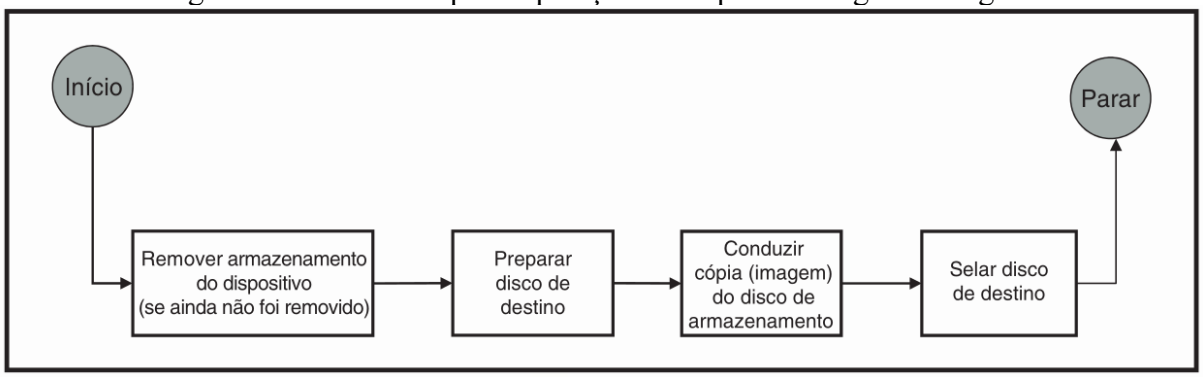
Fonte: ABNT (2013b, p. 27)

Figura 10 – Diretrizes para aquisição de dispositivo digital ligado



Fonte: ABNT (2013b, p. 29)

Figura 11 – Diretrizes para aquisição de dispositivo digital desligado



Fonte: ABNT (2013b, p. 31)

Em resumo, a cadeia de custódia de elementos digitais – conforme o art. 158-B do CPP (BRASIL, 2021a) e a NBR ISO/IEC 27037:2013 (ABNT, 2013b) – é composta, em abstrato, pelos seguintes atos sequenciais: busca e distinção de um elemento como de potencial probatório (reconhecimento); isolamento (preservação do dispositivo de armazenamento, do elemento digital e do ambiente da sua coleta); fixação (identificação do dispositivo, inclusive com fotos, filmagens e croqui); decisão sobre se é melhor a coleta do dispositivo de armazenamento ou a imediata aquisição dos elementos digitais (Figura 7, considerando a volatilidade do elemento digital – que pode desaparecer na situação de desligamento de aparelho encontrado ligado, por exemplo –, situações concretas – como o tamanho de armazenamento necessário – e os requisitos legais); coleta do dispositivo ligado (Figura 8) ou desligado (Figura 9); acondicionamento (procedimento de embalagem, registro da identificação e anotação da data, hora e nomes daqueles que coletaram e acondicionaram o dispositivo que armazena o elemento digital); transporte do dispositivo; recebimento do dispositivo pelo agente público responsável; aquisição dos elementos digitais armazenados no dispositivo ligado (Figura 10) ou desligado (Figura 11); perícia nos elementos digitais adquiridos; guarda e preservação de cópia de segurança do elemento digital; e descarte do elemento digital irrelevante ou que não atenda aos requisitos legais – como confiabilidade, integridade e disponibilidade. Todos os atos devem atender à transparência técnica, rastreabilidade e auditabilidade.

5.1.2.1 Cadeia de custódia de elementos digitais e logs

Para aferir se a cadeia de custódia dos elementos digitais foi cumprida, os *logs* são destacadamente importantes.

Reginald Morrish, com base em Edmond Locard[311], formulou clássico princípio da ciência forense: no contato entre dois itens, haverá uma troca; um criminoso na cena do crime deixa sempre algo e leva algo consigo (FÜSZTER, 2016, p. 24). No espaço virtual, o "princípio da troca" também é aplicável, não apenas em relação a atos criminosos, mas a quaisquer atos digitais (como de peritos, investigadores *etc.*). Nos crimes violentos, os vestígios das trocas são físicos, como as marcas num cadáver. Nos atos digitais, os *logs* estão entre os principais vestígios das trocas.

O *log* é um arquivo de registro de eventos específicos do sistema, como das atividades do usuário, das medições dos sensores da máquina e das suas operações (LIN, 2018, p. 305-306). Esses arquivos são criados automaticamente pelo sistema e são relevantíssimos para a instrução; qual usuário usou o dispositivo num determinado momento, por exemplo, pode estar registrado no *log*.

A Associação Brasileira de Normas Técnicas recomenda, para a segurança da informação (NBR ISO/IEC 27002:2013), os registros de:

> a) identificação dos usuários (ID); b) atividades do sistema; c) datas, horários e detalhes de eventos-chave, como, por exemplo, horário de entrada (log-on) e saída (log-off) no sistema; d) identidade do dispositivo ou sua localização, quando possível, e o identificador do sistema; e) registros das tentativas de acesso ao sistema, aceitas e rejeitadas; f) registros das tentativas de acesso a outros recursos e dados, aceitas e rejeitadas; g) alterações na configuração do sistema; h) uso de privilégios; i) uso de aplicações e utilitários do sistema; j) arquivos acessados e o tipo de acesso; k) endereços e protocolos de rede; l) alarmes provocados pelo sistema de controle de acesso; m) ativação e desativação dos sistemas de proteção, como sistemas de antivírus e sistemas de detecção de intrusos; n) registros de transações executadas pelos usuários nas aplicações. (ABNT, 2013a, p. 54-55).

Somado a isso, os agentes públicos não podem desativar ou apagar os registros de suas próprias atividades. No processo penal, em função do estado de inocência como norma probatória, a demonstração do cumprimento da cadeia de custódia cabe à acusação (PRADO, Geraldo, 2014, p. 81), e os *logs* são demonstrações importantes de que os atos da cadeia de custódia foram cumpridos pelos agentes públicos. Sem os registros das atividades dos agentes é impossível demonstrar a cadeia de custódia; além de impossibilitar a rastreabilidade e a auditabilidade, não será possível aferir se existiu modificação no elemento digital, o que compromete sua confiabilidade e impede a comprovação da sua integridade. Consequentemente, sem os *logs* das atividades dos agentes os elementos digitais serão inadmissíveis.

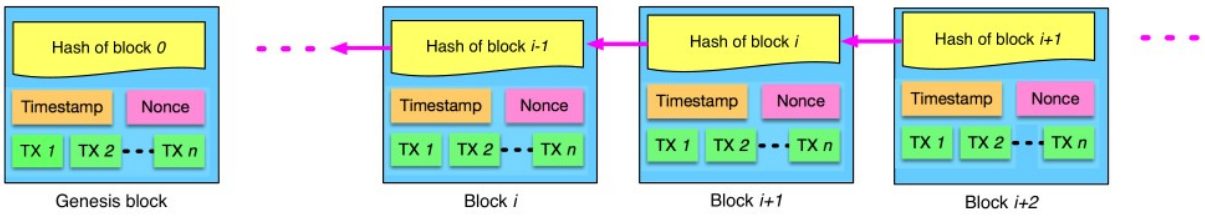
[311] Médico e jurista, Locard foi um dos principais cientistas forenses do século XX e o pioneiro na utilização de laboratórios forenses (FÜSZTER, 2016, p. 22).

5.1.2.2 Cadeia de custódia de elementos digitais e blockchain

Finalmente, destaca-se que outra tecnologia, o *blockchain*, pode ser de grande utilidade para a demonstração da confiabilidade e integridade do elemento digital, assim como para a transparência da operacionalização da busca e apreensão.

O *blockchain* é uma cadeia de blocos sequenciais criptografados em que cada bloco seguinte tem valor de *hash* único, baseado no do último bloco (ZHENG *et al*., 2018, p. 355).

Figura 12- An example of blockchain which consists of a continuous sequence of blocks



Fonte: Zheng *et al*. (2018, p. 355)

Cada bloco é composto por dados de versão, valor do *hash* do bloco anterior, valor do *hash* da estrutura de todas as operações da cadeia[312], marcação do tempo de existência do bloco, valor do *hash* do bloco atual e o número de controle da quantidade de cálculos de *hash* na cadeia (ZHENG *et al*., 2018, p. 355).

Cada um desses blocos de dados, ao ser submetido ao algoritmo de criptografia (ver o item 3.2.2.1), resulta num valor de *hash*. Esta operação faz com que uma sequência arbitrária de *bits*, de qualquer comprimento, seja transformada (pelo algoritmo) numa sequência de *bits* de comprimento fixo (o valor de *hash*) – por exemplo, um bloco de dados, com qualquer conteúdo, submetido ao algoritmo de criptografia SHA-256, tem como resultado sequência de 256 *bits* (o *hash*); ou seja, tanto um arquivo de texto contendo uma letra e de sequência de 2 *bytes*, como a Bíblia em PDF de sequência de muitos *megabytes*, ao serem submetidos ao SHA-256, resultam num valor de *hash* de 256 *bits* de comprimento (assim, arquivos de comprimentos variados resultam num arquivo de comprimento padronizado). Somado a isso, pela própria programação da criptografia, o bloco de dados pode ser convertido num valor de *hash*, mas não é possível fazer a operação reversa (inserir o *hash* no algoritmo e obter o bloco de dados) (SMART, 2016, p. 271, 279).

No *blockchain*, cada bloco seguinte tem o valor de *hash* baseado no valor de *hash* do bloco anterior (o algoritmo de criptografia utiliza o *hash* do bloco anterior como uma das

[312] O *Merkle tree root hash* (ZHENG *et al*., 2018, p. 355) (SMART, 2016, p. 276-280).

variáveis da função matemática). Com isso, é possível rastrear qual o bloco anterior e qual o seguinte, e assim sucessivamente. Como cada alteração no bloco de dados resulta num valor de *hash* distinto, também é possível saber se existiu alteração de um bloco de dados para outro (NOFER *et al.*, 2017, p. 183-184).

Pelo *blockchain*, a autenticação da integridade do arquivo é facilitada. Cada arquivo passa a ter uma "identidade digital", assim como eventual modificação no arquivo. Os benefícios que esta tecnologia pode proporcionar para a cadeia de custódia do elemento digital são evidentes, tanto a inexistência de alteração no arquivo poderá ser demonstrada, como os atos dos agentes públicos poderão ser rastreados e auditados.

5.2 Relacionada à tendência de aumento do espaço da polícia

Como dito (item 2.3, *supra*), a polícia é a porta de entrada da persecução penal; centraliza a análise de informações na rede de vigilância alimentada por agentes públicos e privados; e é à polícia a quem cabe a maior parte dos atos relacionados à realização dos meios ocultos de investigação. Cada vez mais, é confirmada a tendência de aumento do espaço da polícia na sociedade de controle.

Elementar que o fundamento da atividade policial é a legalidade democrática – e parte-se da premissa de que os agentes policiais são comprometidos com o respeito ao Estado Democrático de Direito. A questão que se põe é que mesmo em investigações ocultas que observem ao máximo as garantias processuais, os atos investigativos não são realizados em contraditório oral e, portanto, não são construídos com influência da defesa técnica que, *e.g.*, pode levantar pontos não cogitados pelos investigadores e controlar a regularidade na realização dos atos (impedindo falsidades nos seus registros, por exemplo). Sem contraditório oral – e, também sem paridade entre as partes, publicidade e imediação judicial – os atos ocultos investigativos enviesados pelas hipóteses construídas antes do debate são inquisitórios e frágeis em credibilidade.

Em relação à busca e à apreensão de elementos de prova digitais e os demais meios ocultos de investigação atraírem o foco da persecução penal para os atos policiais realizados sem a participação prévia e consciente do acusado, o direito ao confronto é técnica relevantíssima.

Para demonstrar o potencial do direito ao confronto para a participação do acusado e a dinâmica de poder envolvida, o próximo item utilizará novamente da história. A genealogia[313]

[313] Item 2.1, *supra.*

do direito ao confronto demonstrará que um indivíduo acusado de um crime pode superar o líder inglês se puder confrontar seus incriminadores "face a face" e exercer melhor a argumentação.[314] Com a mesma estratégia, o acusado pode enfrentar os autores do acervo investigativo construído pelos novos meios de investigação.

5.2.1 Direito ao confronto

No início da acusatoriedade inglesa, os jurados tinham conhecimento dos fatos ocorridos no local onde viviam. A necessidade de produção de prova sobre fatos do passado estranhos ao conhecimento do júri surgiu nos séculos XV e XVI, com a expansão populacional e do número de casos submetidos a julgamento (MIRANDA COUTINHO, 2010, p. 6). Neste momento em que se passou a exigir a produção da prova perante o *jury* foram aperfeiçoadas as regras probatórias, principalmente com a intenção proteger os juízes leigos de erros no julgamento, e ocorreu o primeiro caso de que se tem notícia relacionado ao direito ao confronto na Inglaterra (WIGMORE, 1923, p. 11-14) (DAMAŠKA, 2015, p. 44).

Em 1552, o Parlamento inglês estabeleceu que em acusações de traição o acusado tinha o direito de ter ao menos duas testemunhas que o acusavam trazidas perante si. Contudo, a Coroa desprezava este direito e formava a maior parte da cognição sobre acusações de traição por torturas. No ano de 1603, *Sir* Walter Raleigh foi acusado de traição por ter conspirado para que Arabella Stuart se tornasse a rainha da Inglaterra. A única prova contrária a Raleigh era um documento escrito por *Lord* Cobham – após ser torturado – desmascarando a conspiração. Raleigh exigiu que Cobham fosse trazido para um confronto "face a face". Sua exigência foi negada, ele foi condenado e executado. Posteriormente, o documento escrito por Cobham foi provado como falso – o próprio Cobham escreveu outra carta a Raleigh, buscando se retratar (PERRY, 2008, p. 568-569) (FRIEDMAN, 1998, p. 1024) (SHAVIRO, 1991, p. 341).

Depois de mais de trinta anos desses eventos, em 1637, o ministro religioso quaker John Lilburne foi acusado de traição por contrabandear livros que atacavam bispos da Igreja Anglicana. Na instrução, Lilburne se recusou a responder perguntas até que aqueles que o acusavam fossem trazidos à sua presença para serem confrontados "face a face". A *Star Chamber* determinou o açoite de Lilburne e sua prisão até que se dispusesse a responder às perguntas. O Parlamento interveio junto a Charles I, defendeu que o julgamento foi ilegal e tirânico e, no ano de 1640, conseguiu a liberdade de Lilburne.[315] Foi o primeiro caso inglês em

[314] Caso do ministro religioso quaker John Lilburne, de 1637.
[315] A *Star Chamber*, que julgava infrações contra a Coroa, foi abolida no ano seguinte, 1641.

que o direito de confrontar "face a face" as testemunhas da acusação impediu a injustiça. Em 1649, Lilburne foi acusado de traição novamente, desta vez por supostamente ter escrito panfletos contrários ao regime da *Commonwealth* (liderado por Cromwell e estabelecido como regime oficial no mesmo ano). Na sessão de julgamento, Lilburne exerceu seu direito de confrontar as testemunhas de acusação e, em sua fala final, demonstrou que a acusação falhou em provar, por ao menos duas testemunhas presentes no tribunal, que ele era o autor dos escritos. O veredito foi unânime pela absolvição (MALAN, 2009, p. 68-71) (PERRY, 2008, p. 570).

O conteúdo do direito ao confronto, atualmente, é demarcado por Zappalà (2008, p. 129-140) como o direito do acusado de examinar as testemunhas contrárias a si, também de arguir impedimentos e suspeições, somado ao dever do juízo de agir ativamente para fazer com que a testemunha compareça em audiência para ser confrontada. Para a efetivação desse direito, a identidade da testemunha deve ser revelada à defesa; deve ser garantida a presença do acusado no ato da produção da prova, que ele entenda o que ocorre e que possa agir e reagir durante a audiência (no que é fundamental a participação efetiva da defesa técnica) (RAMOS, 2006, p. 147-148).

É importante, ainda, destacar que a "testemunha" que deve ser submetida ao direito ao confronto não é exclusivamente o elemento de prova do meio de prova testemunho, é todo aquele que tenha o potencial probatório incriminador; não importa a qualificação da pessoa que presta a declaração (vítima, informante, testemunha, perito, corréu *etc.*), qualquer pessoa que funcione como elemento de prova é aqui abrangida pelo conceito de "testemunha" e deve ser submetida ao direito ao confronto, como defendido por Diogo Malan (2009, p. 78-80).

Previsto no Pacto Internacional dos Direitos Civis e Políticos (artigo 14.3.e) e no Pacto de São José da Costa Rica (artigo 8, 2, f), e incorporado no sistema jurídico brasileiro como direito fundamental de aplicação imediata (Constituição de 1988, artigo 5º, § 1º), o direito ao confronto entrelaça-se de maneira indissociável às técnicas de produção da prova oral previstas no Código de Processo Penal: oralidade (artigo 204); publicidade (artigo 792); presença do acusado e de seu defensor (artigos 217, 260 e 261); presença do juiz do mérito da causa (artigo 212); dever de depoimento da testemunha (artigos 206 e 218); dever de compromisso juramentado da testemunha em dizer a verdade (artigo 203); direito do acusado conhecer a identidade da testemunha (artigos 203 e 205); direito de exercer o *cross examination* (exame cruzado) (artigo 212); direito de contraditar a testemunha por impedimento, suspeição ou proibição de depor (artigo 214). O desrespeito ao direito fundamental ao confronto implica em ilicitude probatória, o que torna o ato inadmissível para

integrar o procedimento e causa a exclusão de seus registros dos autos do processo – assim como os dele derivados – (Constituição de 1988, artigo 5º, LVI; Código de Processo Penal, artigo 157) (MALAN, 2009, p. 90-91).

A cadeia de custódia também tem relação direta com o direito ao confronto: somente com os registros da cadeia de custódia é possível conhecer a identidade dos autores dos atos ligados aos elementos de prova obtidos na investigação e arrolá-los para serem confrontados na instrução em juízo.

Antes de explicar a importância do direito ao confronto contra a tendência de aumento do espaço da polícia na sociedade de controle, urge, finalmente, ressemantizar a relação do direito ao confronto com o contraditório no Direito brasileiro para compreender melhor seu lugar no sistema jurídico nacional. Malan (2009, p. 99-105) afirma que, enquanto o contraditório é proveniente da tradição de *civil law*, é de titularidade de ambas as partes e alcança todas as suas participações; o direito ao confronto provém da *common law*, é de titularidade exclusiva do acusado e alcança apenas a produção da prova oral. Contudo, a semelhança entre eles é significativa, principalmente no marco teórico desta tese que é o contraditório como influência e não surpresa (NUNES, 2008) e que, no processo penal acusatório, deve respeitar a oralidade como técnica de construção dos atos.

Apesar da proveniência da *common law*, o direito ao confronto foi internalizado como direito fundamental no sistema jurídico brasileiro pelos Decretos ns. 592 (Pacto Internacional sobre Direitos Civis e Políticos) e 678 (Pacto de São José da Costa Rica), ambos de 1992. Portanto, ele é direito internalizado e seu espaço no processo penal brasileiro deve ser bastante claro. Partindo daí, defende-se a ressemantização de que o princípio do contraditório, que deve influenciar a construção de todos os atos decisórios do procedimento, além de ser mais amplo que o direito ao confronto, também o engloba. Defende-se que toda participação do acusado no processo penal é exercício do contraditório, e que a sua participação na produção da prova oral é tanto exercício do princípio do contraditório como do subprincípio do direito ao confronto.[316] Essa ressemantização, além de aclarar a distinção acadêmica entre o contraditório e o direito ao confronto no sistema jurídico brasileiro, é mais adequada à semelhança entre os dois institutos e atende à variabilidade da efetivação do contraditório no processo penal (ANDOLINA; VIGNERA, 1997, p. 9).[317]

[316] Na lição de Antonio Marçal (2007, p. 34): "O princípio é uma construção *teórica integradora*, na medida em que é resultado de uma generalização, que reúne e organiza outros e anteriores conhecimentos e, como tal, permite compreender e explicitar a correlação entre conhecimentos e realidade conhecida. O princípio é, neste processo, também uma construção conceitual *operativa*, na medida em que os conhecimentos nele reunidos e expressos possibilitam *progredir* na produção de novos conhecimentos e também *orientar* a forma e o curso da ação humana voltada para fins.".

[317] Sobre a diferença da *hearsay rule* para o direito ao confronto, aquela trata da proibição de "informações de segunda mão" (DAMAŠKA, 1992, p. 425, tradução nossa: "second-hand information"), como os testemunhos de

A colocação do direito ao confronto como subprincípio do contraditório no sistema jurídico brasileiro, além de adequar a produção da prova oral às especificidades do processo penal, faz com que o direito ao confronto seja respeitado não como simples argumento retórico (o que ocorre, entre outras razões,[318] pela não demarcação de seu lugar no sistema jurídico nacional em relação ao contraditório), mas como direito internalizado, vigente, com lugar claro no processo penal e que, inclusive, pode orientar o controle de convencionalidade[319] da legislação relacionada.

Posto isto, torna-se possível a compreensão sobre a importância do direito ao confronto contra a tendência de aumento do espaço da polícia na persecução penal na sociedade de controle.

Na sociedade de controle, é a polícia quem tem o primeiro contato com o caso penal, quem centraliza a análise de informações na rede de vigilância alimentada por agentes públicos e privados e quem realiza a maior parte dos atos relacionados aos meios ocultos de investigação. A persecução penal é desenvolvida partindo, principalmente, das informações produzidas pela polícia.

Óbvio que os meios ocultos de investigação teriam sua relevância esvaziada na situação de conhecimento prévio do investigado de que sofre interceptação telefônica, por exemplo (evidente que o investigado não utilizaria o telefone neste caso e a investigação seria inútil). Partindo deste contexto, reconhecendo a relevância dos meios ocultos, principalmente para investigar a criminalidade organizada, deve se efetivar o modelo constitucional do processo também na persecução penal que utilize meios ocultos. Para isso, o direito ao confronto emerge como garantia de especial relevância: ele possibilita que todos os que produziram o acervo investigativo sejam confrontados "face a face" na instrução judicial. A carência de fiscalização dos meios ocultos no momento de sua realização é mitigada pelo direito ao confronto exercido em juízo. E essa matéria é relacionada não somente à

ouvir dizer; o direito ao confronto é composto pelo dever de o tribunal fazer comparecer as testemunhas e pela faculdade do acusado contraditar e examinar as testemunhas. A *hearsay rule* trata do conteúdo da declaração; o direito ao confronto trata do direito fundamental de participação do acusado na produção da prova oral (MANTHEY; SIMONETTI, 1979, p. 579) (COSTA ANDRADE, 2013, p. 161-162).

[318] A não demarcação sistêmica do direito ao confronto em relação aos demais institutos processuais confunde o intérprete. Além disso, são causas da pouca consideração do direito ao confronto na prática forense a quantidade reduzida de publicações científicas brasileiras relacionadas ao tema e à raridade da realização do controle de convencionalidade no Brasil, o que torna escassa a sua discussão.

[319] "A compatibilidade do direito doméstico com os tratados internacionais de direitos humanos em vigor no país faz-se por meio do controle de convencionalidade, que é complementar e coadjuvante (jamais subsidiário) do conhecido controle de constitucionalidade. […] O controle de convencionalidade tem por finalidade compatibilizar verticalmente as normas domésticas (as espécies de leis, *lato sensu*, vigentes no país) com os tratados internacionais de direitos humanos ratificados pelo Estado e em vigor no território nacional." (MAZZUOLI, 2011, p. 132).

credibilidade e legitimidade da persecução – apesar de envolver também isso –, ela trata da dignidade da pessoa humana.

Cada sujeito é um fim em si e deve ser tratado como tal mesmo se acusado de crimes gravíssimos, por imposição constitucional.[320] O Estado deve servir ao homem, não o homem ao Estado (CANOTILHO, 2003, p. 225). Apenas no saber inquisitório o investigado é objeto da investigação; no saber acusatório ele é sujeito que tem o direito de influenciar efetivamente o provimento que pode alterar radicalmente a sua liberdade (CORDERO, 2000a, p. 21-23, 87-88) (GOLDSCHMIDT, 1935, p. 69).

É inadmissível que o investigado seja objeto dos meios ocultos de investigação e jamais possa sequer ter a oportunidade de confrontar aqueles que atuaram na persecução. O investigado deve ser tratado como sujeito, digno e ativo na construção do provimento de que é o principal interessado.

Especialmente em relação aos investigadores e peritos, os que mais atuam na realização dos atos ocultos e na análise dos elementos obtidos, o direito ao confronto deve ser respeitado para que eles sejam questionados, por exemplo, quanto ao reconhecimento, isolamento, fixação, coleta, acondicionamento, transporte, recebimento, armazenamento e descarte do elemento de prova; assim como para serem confrontados quanto ao seu currículo, especialização no objeto da perícia, conhecimento científico, metodologia de investigação (incluindo o marco teórico, as hipóteses avaliadas, os procedimentos adotados, o desenvolvimento e o resultado), duração dos atos, local em que foram realizados, hierarquia no local de trabalho *etc.* Assim, o direito ao confronto efetiva a dignidade do acusado: depois de anos de atos de terceiros suspeitando de suas condutas, pelo exercício do direito ao confronto, o acusado tem a possibilidade de refutar as hipóteses da investigação e examinar "face a face" as pessoas envolvidas na persecução penal (MASSARO, 1988, p. 897-907).

Derradeiramente, lembra-se, novamente, que o direito ao confronto envolve o dever do juízo de fazer com que todo aquele que tenha função probatória incriminadora compareça em audiência para ser confrontado (ZAPPALÀ, 2008, p. 138-140).[321] E, no cumprimento desse dever, falas como "dificuldade de o perito encontrar tempo", "dificuldade em intimar uma testemunha", "dificuldade de logística para ouvir grande número de testemunhas pela pluralidade de acusados" *etc.*, são completamente irrelevantes, ilegais e ofendem à garantia fundamental do direito ao confronto – mormente pelas possibilidades criadas pelas novas

[320] Constituição de 1988, artigo 1º, III; e artigo 5º, LVII (estado de inocência como norma de tratamento [GIACOMOLLI, 2014, p. 99-100]).
[321] Dever também previsto no Código de Processo Penal, artigos 159, § 5º, I; 202, § 1º; 206 e 218.

tecnologias.[322] É da liberdade e da vida de alguém que se trata. Não se pode transigir com a dignidade da pessoa humana, a legitimidade do provimento e com o respeito ao modelo constitucional do processo para se realizar um utilitarismo[323] inconstitucional.

Assim, o direito ao confronto é técnica eficiente em mitigar a tendência de aumento do espaço policial na persecução da sociedade de controle que, cada vez mais, utiliza os meios ocultos de investigação. No mínimo, é possibilitado um tratamento digno ao acusado e que ele refute as hipóteses construídas antes do debate.

5.2.1.1 Direito de confrontar os agentes públicos e privados envolvidos na execução da busca e da apreensão de elementos de prova digitais

A busca e a apreensão de elementos de prova digitais é realizada principalmente no inquérito, pela polícia, e produz informações sensíveis que influenciarão significativamente toda a sequência da persecução.[324] Por meio de novas tecnologias – predominantemente privadas (itens 2.4, 3.3 e 4.6, *supra*) –, a polícia obtém imensa quantidade de elementos digitais, que podem ser relevantes para a apuração da autoria e materialidade dos delitos, principalmente de organizações criminosas, e que aumentam ainda mais a importância de atos realizados fora do espaço processual de conhecimento.

Para assegurar a possibilidade de participação ativa do acusado na construção do juízo, o direito ao confronto assume destacada importância.

Lembra-se que a busca e a apreensão não obtêm provas, mas elementos de prova que, submetidos aos meios de prova (como a perícia e o testemunho) resultarão na prova – após as fases procedimentais de proposição, admissão e produção orientadas pelos institutos processuais constitucionalizados, principalmente o contraditório.[325]

Em nome da variabilidade do modelo constitucional do processo (ANDOLINA; VIGNERA, 1997, p. 9), defende-se (item 5.2.1, *supra*) que a participação do acusado na produção da prova oral é exercício do contraditório e do direito ao confronto, o que implica no direito do acusado examinar todas pessoas que tenham potencial incriminador – seja qual for o nome que se dê à pessoa (como testemunha, perito, auxiliar, vítima, intérprete *e.g.*)

[322] O *International Criminal Tribunal for the former Yugoslavia* reconheceu, por exemplo, a possibilidade do uso da videoconferência para cumprir o direito ao confronto (ZAPPALÀ, 2008, p. 139).
[323] O utilitarismo "substitui a consideração do *fim* [...] pela consideração dos *móveis* que levam o homem a agir. Nisto, liga-se à tradição hedonista, que vê no prazer o único móvel a que o homem ou, em geral, o ser vivo, obedece" (ABBAGNANO, 2007, p. 986).
[324] Vide a introdução e o item 2.6, *supra*.
[325] Vide o item 4.1, *supra*.

(MALAN, 2009, p. 78-84) – e arguir impedimentos e suspeições; e no dever do juízo agir ativamente para fazer com que a pessoa compareça em audiência para ser confrontada.

O comparecimento em audiência para ser confrontado, se requerido pelo acusado, é dever: o Código de Processo Penal expressamente determina a condução coercitiva da vítima, da testemunha, do perito e do intérprete que não comparecerem (artigos 201, § 1º, 218, 278 e 281).

Ocorre que a busca e apreensão de elementos digitais pode utilizar tecnologias privadas que intencionalmente são mantidas sob sigilo pelas empresas (BARROS; BOLZAN DE MORAIS, 2021, p. 359). E, como destacado no item 4.6, *supra*, o funcionamento da tecnologia pode ser incompreensível. Por isso, o confronto aos agentes privados envolvidos também ganha relevância. Perito oficial algum terá como explicar o funcionamento de determinadas tecnologias se o algoritmo de programação não for revelado.

Não tem cabimento considerar que alguém é culpado ou inocente em função de prova produzida a partir de elemento digital sem se conhecer qual a tecnologia envolvida na obtenção, acesso e tratamento do elemento digital. Se somente o programador da tecnologia pode responder como um algoritmo chegou a um resultado, das duas uma: ou ele deve comparecer em juízo como testemunha[326] para ser confrontado e explicar o funcionamento da tecnologia de potencial incriminador, ou a prova é ilícita por ofensa à ampla defesa (Constituição, artigo 5º, LV) – vez que a contraprova sobre o funcionamento da tecnologia será impossível –, por ofensa à cadeia de custódia (CPP, artigos 158-A a 158-F) – pela inexistência de demonstração da história cronológica do elemento de prova digital, por ter sido utilizada a tecnologia com opacidade no reconhecimento, coleta ou processamento – e por ofensa ao direito ao confronto (Pacto Internacional dos Direitos Civis e Políticos, artigo 14.3.e, e Pacto de São José da Costa Rica, artigo 8.2.f[327]) – pelo não comparecimento da testemunha.

5.3 Relacionadas à proteção contra a autoincriminação

Em interceptações de conversas telefônicas, revelações a agentes infiltrados, captações ambientais, leniências, delações, comunicações rotineiras a órgãos oficiais, colaboração das

[326] Toda pessoa pode ser testemunha (Código de Processo Penal, artigo 202); a gestão da prova é regida pelo princípio dispositivo no processo acusatório (MIRANDA COUTINHO, 2001, p. 37); e o testemunho é relevante pela sua realização poder alterar o juízo (vide o item 4.3.2, *supra*).

[327] "2. Toda pessoa acusada de delito tem direito a que se presuma sua inocência enquanto não se comprove legalmente sua culpa. Durante o processo, toda pessoa tem direito, em plena igualdade, às seguintes garantias mínimas: f) direito da defesa de inquirir as testemunhas presentes no tribunal e de obter o comparecimento, como testemunhas ou peritos, de outras pessoas que possam lançar luz sobre os fatos." (BRASIL, 2022o).

empresas de tecnologia com o Estado *etc.*, ocorre a autoincriminação de indivíduos, atendendo à pressão por controle ultrarrápido, constante e em qualquer lugar da sociedade de controle.[328]

Neste contexto, a dignidade, o direito ao silêncio, à privacidade e à proibição da tortura, são garantias que afirmam ao máximo a acepção de garantia como "sinônimo de proteção jurídico-política" (BARACHO, 1984, p. 138) – não apenas em relação à busca e à apreensão de elementos de prova digitais, mas em relação a todos os meios de investigação.

5.3.1 Respeito à dignidade, ao direito ao silêncio, à privacidade, à proibição da tortura e a vedação de autoincriminação

Primeiro, nas palavras de Canotilho (2003, p. 225):

> Perante as experiências históricas da aniquilação do ser humano (inquisição, escravatura, nazismo, stalinismo, polpotismo, genocídios étnicos) a dignidade da pessoa humana como base da República significa, sem transcendências ou metafísicas, o reconhecimento do *homo noumenon*, ou seja, do indivíduo como limite e fundamento do domínio político da República. Neste sentido, a República é uma organização política que serve o homem, não é o homem que serve os aparelhos político-organizatórios.

Sem metafísica[329] ou direito natural, a dignidade da pessoa humana como fundamento do Estado brasileiro é uma escolha política feita pelo constituinte no artigo 1º, inciso III, da Constituição de 1988. Após séculos de escravidão, colonialismo, golpes militares, ditaduras, pobreza extrema e outras várias mazelas, em 1988 o Brasil foi constituído sob o fundamento de que o indivíduo é um fim em si e que o Estado existe para efetivar a sua dignidade.

Segundo, o direito ao silêncio[330] não é diretamente ligado apenas à posição subjetiva do investigado ou do acusado nos atos do procedimento, ele é diretamente ligado às posições subjetivas de todos os sujeitos processuais. O investigado ou acusado tem a faculdade de não confessar ou prestar qualquer declaração (o interrogatório é meio de defesa).[331] A testemunha

[328] *Supra*, item 2.4.
[329] Vide a nota n. 17, *supra.*
[330] Constituição de 1988, art. 5º, LXIII.
[331] A luta pela noção do interrogatório como meio de defesa é centenária. João Barbalho, por exemplo, escreveu nos comentários à Constituição de 1891: "No empenho de rodear das mais solidas garantias a liberdade individual, e de assegurar a imparcialidade do julgamento, entre as providencias mais salutares ficou estabelecido um limite para a interrogatorio dos accusados. Com effeito, nada pòde ser mais prejudicial á causa da justiça do que este duello pungente, de argucias e subtilezas, de subterfugios e ciladas, qiue commummente se vê travado em pleno tribunal, entre o juiz e o accusado, e em que, não raro, aquelle que devera ser o orgam circumspecto e severo da austera magestade da lei, tem no emtanto como o mais appetecido triumpho a confissão do accusado, extorquida á força de uma sagacidade criminosa. No systema adoptado para os processos criminaes, quer se trate da formação da culpa, que se trate do julgamento o accusado tem o direito de responder laconicamente – sim ou não – e o juiz tem o dever de respeitar o laconismo. E' a instalação definitiva do regimen

tem o dever de declarar, salvo na hipótese em que sua declaração pode levar à autoincriminação, situação em que seu dever de declaração é convertido em faculdade. Os agentes públicos, por sua vez, têm o dever de informar o declarante do direito ao silêncio em momento anterior ao início da declaração, de não estimular a fala do declarante que quer permanecer em silêncio e de não valorar o exercício deste direito (COSTA ANDRADE, 2013, p. 86) (GIACOMOLLI, 2014, p. 193).[332]

Terceiro, Warren e Brandeis (1890) foram pioneiros na conceituação do direito à privacidade, distinguindo-o da propriedade material (como a propriedade de imóveis) e imaterial (como a propriedade intelectual). Diferente da propriedade material, seu foco de proteção não é a proteção física; diferente da propriedade imaterial, ela não exige a expressão linguística e está associada à própria escolha de se expressar. Para os autores, a privacidade é direito de estar só (*the right to be let alone*) e seu foco de proteção é o desenvolvimento da personalidade do indivíduo (WARREN; BRANDEIS, 1890, p. 193-205, 213). Vianna (2007, p. 109-116), após analisar o desenvolvimento do direito à privacidade na Suprema Corte dos Estados Unidos,[333] defende que, nos dias atuais, a privacidade[334] é garantia contra a arbitrariedade de agentes públicos; alcança o direito de não ser monitorado, registrado ou reconhecido (proibição de divulgação de informações privadas); entrelaça-se ao exercício de direitos políticos como o voto secreto, a liberdade de associação e a liberdade de manifestação do pensamento; e configura não mais apenas um direito individual, mas um direito público indissociável do exercício democrático.

Quarto, ao analisar as torturas cometidas na investigação da peste milanesa de 1630, Pietro Verri (1992, p. 80) escreveu:

> Qual é o sentimento que nasce no homem, ao sofrer uma dor? Este sofrimento é *o desejo de que a dor pare*. Quanto mais violento for o suplício, tanto mais violento será o desejo e a impaciência de que chegue ao fim. Qual é o meio com que um homem torturado pode acelerar o término da dor? Declarar-se culpado do crime pelo qual é investigado. Mas é verdade que o torturado cometeu o crime? Se a verdade é sabida, é inútil torturá-lo; se a verdade é duvidosa, talvez o torturado seja inocente, e o torturado inocente, tal como o culpado, é igualmente levado a se acusar do crime.

estabelecido pelas praticas dos tribunaes inglezes e americanos: ahi está consagrada na sua maior pureza o principio da inviolabilidade do direito da defesa." (BARBALHO, 1924, p. 436). Hoje, é pacífico na jurisprudência do Superior Tribunal de Justiça que o interrogatório é meio de defesa; no julgamento do *Habeas Corpus* n. 703.978/SC, o tribunal reconheceu, inclusive, que o investigado ou acusado pode exercer o silêncio parcial e responder apenas às perguntas de seu advogado.

[332] A conduta de prosseguir com o interrogatório de quem decidiu exercer o direito ao silêncio é crime de abuso de autoridade (Lei 13.869, de 2019, artigo 15, parágrafo único, inciso I).

[333] Do voto divergente do então *justice* Brandeis de 1928 (Olmstead *vs.* United States), passando pela analogia da privacidade com a inviolabilidade de domicílio (Katz *vs.* United States) à proteção da liberdade individual contra o Estado (Stanley *vs.* Georgia) e à proteção da privacidade contra o monitoramento e registro do indivíduo (National Association for the Advancement of Colored People *vs.* Alabama).

[334] Constituição de 1988, art. 5º, X.

> Portanto, os tormentos não constituem um meio para descobrir a verdade, e sim um meio que leva o homem a se acusar de um crime, tenha-o ou não cometido.

Baseado na hipótese acrítica que já aceitou, o torturador busca enquadrar o procedimento da tortura em seu quadro mental paranoico (CORDERO, 1985, p. 651; 1986, p. 51-52). Em nada ela esclarece sobre o fato e seus efeitos concretos ferem drasticamente a dignidade humana. Por essas razões, a tortura é proibida pela Constituição de 1988, em seu artigo 5º, inciso III.

Quinto, reunidos, a dignidade e os direitos ao silêncio, à privacidade e à proibição da tortura relacionam-se diretamente com a vedação de autoincriminação. Na inquisição é que o investigado é um objeto, "animal da confissão", obrigado a se incriminar (CORDERO, 1985, p. 639; 1986, p. 48, tradução nossa[335]). Na acusatoriedade, o investigado ou acusado é sujeito de direitos que deve ter sua dignidade respeitada (GOLDSCHMIDT, 1935, p. 69) e não pode ser compelido a participar de qualquer ato investigativo ou de prova; isso implica: a) a vedação de qualquer estímulo ou engano aptos a alterar a vontade do indivíduo e incliná-lo à autoincriminação; b) a consideração do indivíduo como um fim em si; c) a faculdade do indivíduo de não colaborar com a persecução (seja permanecendo em silêncio ou se negando a participar passiva – como no reconhecimento de pessoas – ou ativamente – como no fornecimento de padrão grafotécnico –); d) o direito de declarar a própria narrativa dos fatos e não sofrer punição pela mentira;[336] e) a proteção contra a invasividade do corpo humano (seja a interna – como na inserção de agulha para retirada de sangue – ou a externa – como a retirada de fio de cabelo –); f) a proibição de monitoramento, registro ou divulgação de informações privadas de maneira arbitrária; g) na proibição da tortura (física ou psicológica) (GIACOMOLLI, 2014, p. 193) (GOMES; MAZZUOLI, 2010, p. 127) (BOTTINO, 2009, p. 205).

Consequentemente, isso também implica que, na realização dos meios ocultos de investigação na sociedade de controle, a vedação de autoincriminação seja especialmente considerada pelos magistrados na decisão que os autoriza ou indefere. Neste ato, ganha especial relevância a atuação judicial na proteção preventiva das garantias ligadas à vedação de autoincriminação, para que a investigação por meios ocultos só seja autorizada em último

[335] "animale da confessione".

[336] A um, como anotam Luiz Flávio Gomes e Valerio de Oliveira Mazzuoli (2010, p. 127): "não existe o crime de perjúrio no direito brasileiro". A dois: o investigado ou acusado não presta juramento de dizer a verdade. A três: "verdade" ou "mentira" depende dos critérios de veridição, que podem ser interpretados diferentemente pelo declarante e outro sujeito. A quatro: se existisse punição pela mentira, existiria um desestímulo para que o declarante exercesse a autodefesa no interrogatório, vez que qualquer fala sua que não coincidisse com a de outrem poderia ser punida, o que é inadmissível numa democracia. A cinco: o que alguém entende por "mentira" em primeira instância, pode ser considerado "verdade" em instância recursal; não existe "verdade" metafísica.

caso, na situação de impossibilidade demonstrada – no momento em que é requerida a investigação por meio oculto (informações ulteriores são inaptas a justificar a decisão pretérita) – de investigação por outros meios (subsidiariedade); em crimes graves; proibido o excesso; com a utilização do meio adequado para obter resultado relevante; com tempo e lugar preestabelecidos, explicitação clara do objeto da investigação, dos elementos concretos que a justifiquem e observância plena da legalidade em todos os momentos (COSTA ANDRADE, 2011, p. 547-550) (VALENTE, 2009). A ofensa à vedação de autoincriminação causada pelos meios ocultos de investigação exige especial cuidado e fundamentação dos juízes que atuam na fase de investigação (que não são ratificadores dos atos investigativos, mas garantidores do cumprimento do Direito e devem indeferir a realização de atos ocultos ilegais e sem justa causa).

Finalmente, na situação de realização de investigação oculta ilegal, a ofensa à vedação de autoincriminação deve ser considerada pelos juízos superiores para declarar a investigação como inadmissível para integrar o procedimento e excluir todos os seus registros – observada a ilicitude por derivação.[337]

5.3.1.1 Proteção contra a autoincriminação e medidas antiforenses

Sem lesão a direito de terceiro, o Estado não pode intervir punitivamente (ROXIN, 1997, p. 51-57).[338] Existindo, ou não, suspeita de alguém ter lesionado direito de terceiro, é vedada a autoincriminação (tema desenvolvido no item anterior). Mormente na sociedade de controle, onde agências públicas e privadas acumulam uma imensidão de elementos digitais sobre os indivíduos, numa rede de vigilância que busca ser ininterrupta (capítulo 2, *supra*), o agir do indivíduo contra a autoincriminação é direito seu; assim como a defesa de sua privacidade.

Com o aumento da influência tecnológica na persecução penal, ganham importância as tecnologias que podem ser utilizadas, propositadamente ou não, como medidas antiforenses.

As medidas antiforenses são técnicas que prejudicam a atuação da computação forense[339] nos elementos digitais armazenados no sistema informático e técnicas que dificultam sua localização (RAMALHO, 2019, p. 151-152).

[337] Constituição de 1988, art. 5º, LVI; CPP, art. 157. Para tanto, principalmente no sistema recursal brasileiro em que a regra é a irrecorribilidade das decisões interlocutórias, é fundamental a impetração de *Habeas Corpus*.
[338] "No direito penal essa opção se traduz no princípio da lesividade, segundo o qual nenhum direito pode legitimar uma intervenção punitiva quando não medeie, pelo menos, um conflito jurídico, entendido como a afetação de um bem jurídico total ou parcialmente alheio, individual ou coletivo." (ZAFFARONI; BATISTA, 2011, p. 226).
[339] Vide o item 3.5, *supra.*

Como exemplos de medidas antiforenses que prejudicam a atuação da computação forense nos elementos digitais armazenados, são citadas: a eliminação dos dados, principalmente pelo seu apagamento em definitivo[340] (já que "enviar para a lixeira" não remove o arquivo do sistema, ele continua armazenado no *hard drive*, o computador apenas é comandado para reconhecer o espaço daquele arquivo como livre para uma gravação futura); a dissimulação dos dados, como por criptografia[341] (tratada no item 3.2.2.1, *supra*); e a adulteração dos dados, como a alteração de metadados[342].

Como exemplo de medidas antiforenses que dificultam a localização do elemento digital, cita-se: esconder o dispositivo de armazenamento (o que é facilitado pela redução dos tamanhos dos dispositivos, como um *pen drive*), o uso de *proxy*[343] (um servidor intermediário que esconde o endereço do IP na internet) ou do Tor.

O Tor merece destaque especial por ser uma das principais tecnologias para a navegação anônima na internet. O Tor Project foi iniciado em 2006 por uma organização sem fins lucrativos para possibilitar a navegação privada e sem censura na internet. O Tor é um navegador em *software* livre[344] (logo, também aberto) que funciona por um "roteamento onion": os pacotes enviados pela internet passam por vários servidores diferentes e são criptografados em cada roteador (TOR PROJECT, 2022).[345] Além de impedir o rastreamento da atividade na internet, a aplicação possibilita a navegação nos endereços que não aparecem nos buscadores (como no Google) – contudo, outras aplicações ou o próprio sistema operacional podem automaticamente armazenar dados, como o Windows, e a navegação pelo Tor pode ficar registrada[346].

Posto isto, lembra-se, novamente, Deleuze (2008a, p. 216): "as máquinas não explicam nada", é necessário entender o uso delas pelos sujeitos. Utilizar uma tecnologia não explica o porquê do uso, e qualquer pessoa pode licitamente utilizar as tecnologias aqui referidas. Afinal, há de se considerar o dolo do sujeito, que pode estar apenas em busca da proteção de sua privacidade e, ainda, que queira prejudicar a atuação da computação forense, não pode ser punido por isso, em função de o indivíduo não ter o dever de colaborar com a investigação, pela vedação da autoincriminação, e de, no Direito brasileiro, somente a

[340] Como pelo *software* CCleaner.
[341] Como o BitLocker e o AESCrypt.
[342] Possível de ser feita pelo mat2, por exemplo.
[343] Como o ProxySite.com.
[344] Sobre o conceito de *software* livre, vide a nota n. 184, *supra.*
[345] Vide a nota 129, *supra.*
[346] O que não ocorre, *e.g.*, com a distribuição Linux Tails, que é um sistema operacional que funciona por *pen drive*, não utiliza o *hard drive* do computador, apaga automaticamente tudo o que é feito durante a sessão no desligamento do sistema e permite a comunicação de qualquer aplicação pela internet apenas pelo Tor (o Linux Tails é disponibilizado gratuitamente em: https://tails.boum.org/index.pt.html).

obstrução da investigação de organização criminosa ser tipificada como crime (art. 2º, § 1º, da Lei 12.850, de 2013); ilícito que exige conduta dolosa contra investigação em andamento e só pode ser cometido por terceiro, vez que o investigado estaria no exercício regular do direito de não se autoincriminar[347] (BITENCOURT, 2016, p. 693-701).

O ponto é que, contra a vigilância do espaço virtual na sociedade de controle por várias agências públicas e privadas, existem tecnologias que, propositadamente utilizadas como medidas antiforenses ou não, podem proteger a privacidade do indivíduo e contra a sua autoincriminação.[348]

5.4 Relacionadas ao progressivo aumento do uso de novas tecnologias

O computador é a máquina mais utilizada na sociedade de controle e influencia diversas técnicas de investigação (DELEUZE, 2008a, p. 216). A imagem do investigador com fone de ouvido ouvindo a interceptação telefônica no momento em que ela ocorre, por um "grampo" na linha telefônica, por exemplo, só permanece plausível nos filmes de *Hollywood*; as polícias utilizam sistemas de interceptação que operam pelo computador (ERICSON; HAGGERTY, 1999, p. 237-244) – como o Sistema Guardião, o Sistema Sombra e o Sistema Wytron, das empresas privadas Dígitro Tecnologia Ltda., Federal Tecnologia de Software Ltda. e Wytron Technology Corp. Ltda., respectivamente (SANTORO; TAVARES; GOMES, 2017, p. 621-622, 625-627).

5.4.1 Paridade entre as partes no espaço virtual

[347] "Eventuais empecilhos que o investigado possa apresentar aos investigadores caracterizará, no mínimo, um *post factum* impunível. Portanto, membro da organização criminosa que oferecer dificuldades à investigação criminal ou apresentar empecilhos à sua desenvoltura não responderá por este crime, estará exercendo sua ampla defesa e o direito de não se autoincriminar." (BITENCOURT, 2016, p. 694). Ainda que não se considerasse aplicável a excludente de ilicitude do exercício regular do direito de não se autoincriminar, a conduta não seria punível em função da inexigibilidade de conduta diversa, vez ser inexigível que alguém não realize todos os esforços possíveis para evitar a prisão nas penitenciárias brasileiras, que "de alguma maneira, são campos de concentração social" (ZAFFARONI, 2017, p. 7).

[348] "É verdade que, mesmo antes das sociedades de controle terem efetivamente se organizado, as formas de delinquência ou de resistência (dois casos distintos) também aparecem. Por exemplo, a pirataria ou os vírus de computador, que substituirão as greves e que no século XIX se chamava de 'sabotagem' (o tamanco – *sabot* – emperrando a máquina). Você pergunta se as sociedades de controle ou de comunicação não suscitarão formas de resistência capazes de dar novas oportunidades a um comunismo concebido como 'organização transversal de indivíduos livres'. Não sei, talvez. Mas isso não dependeria das minorias retomarem a palavra. Talvez a fala, a comunicação, estejam apodrecidas. Estão inteiramente penetradas pelo dinheiro: não por acidente, mas por natureza. É preciso um desvio de fala. Criar foi sempre coisa distinta de comunicar. O importante talvez venha a ser vacúolos de não-comunicação, interruptores, para escapar do controle." (DELEUZE, 2008a, p. 216-217).

Um dos maiores problemas causados pelo aumento do uso da tecnologia pelos órgãos oficiais na persecução penal é a ampliação da diferença entre as partes habituais e as eventuais.

Galanter destaca as vantagens das partes habituais (*repeat players*) – que atuam frequentemente em vários casos semelhantes – sobre as eventuais (*one-shotters*) – que apenas ocasionalmente estão envolvidas em certa tipologia de casos. As partes habituais têm as vantagens de: ter experiência sobre as eventualidades que podem ocorrer; utilizar especialistas; conhecer as pessoas que atuam nas instituições; desenvolver uma reputação junto a um grupo específico; planejar em longo prazo, visando um grande conjunto de casos, não apenas um caso isolado; provocar o tribunal por vários casos diferentes para estimular o debate de determinadas teses; contar com maior orçamento para investir na atuação nos casos (GALANTER, 1974, 97-104).

Dierle Nunes e Nathália Medeiros pontuam que o uso das novas tecnologias pelos profissionais do Direito tende a aumentar as vantagens das partes que contam com maior orçamento para acessar essas novas tecnologias, "uma vez que as decisões estratégicas de parcela destes e de seus advogados serão tomadas com base em poder e acesso desiguais às informações de modo que a capacidade econômica ampliará a disparidade de poder argumentativo" (NUNES; MEDEIROS, 2022).

O acesso das pessoas em geral à tecnologia é muito precário. A *Organization for Economic Co-operation and Development* (OECD) – composta, por exemplo, por Alemanha, Austrália, Áustria, Bélgica, Canadá, Dinamarca, Espanha, Estados Unidos, Finlândia, França Islândia, Itália, Japão, Noruega, Nova Zelândia, Portugal, Reino Unido, Suécia e Suíça – pesquisou um grupo de cerca de 166.000 pessoas, com idade entre 16 e 65 anos, em 24 dos países da OECD, de 2013 a 2015, sobre habilidades relacionadas à alfabetização, uso de números e resolução de problemas tecnológicos. 14,2% das pessoas não conseguiram realizar tarefas simples que demandam um único ato, como apagar um e-mail; 28,7% das pessoas conseguiram realizar apenas tarefas simples, como responder um e-mail para várias pessoas simultaneamente utilizando a função "responder a todos"; 25,7% das pessoas conseguiram realizar tarefas que exigem mais de um ato, como procurar por um determinado documento anexado em um e-mail antigo; e apenas 5,4% das pessoas conseguiram realizar tarefas mais complexas, que exigem o uso de mais de uma aplicação simultaneamente e vários atos, como agendar uma reunião online, a partir de informações contidas em e-mails e em aplicação de agenda. O restante, 26% da população, sequer conseguiu utilizar o computador (OECD, 2016, p. 20, 53).

A pesquisa foi sobre a população no geral, nos países da OECD, não foi sobre os atores jurídicos do Brasil, e foi apresentada apenas para ilustrar o problema do acesso à tecnologia como um todo. Contudo, frente à situação econômica brasileira e à ausência de treinamento em tecnologia na maioria dos currículos acadêmicos do bacharelado em Direito, não há como ser demasiadamente otimista sobre a situação de grande parte dos atores jurídicos do Brasil.

Enquanto o Ministério da Justiça e Segurança Pública, o COAF, o Ministério Público Federal, a Polícia Federal e demais órgãos da persecução utilizam de vultoso orçamento público para investir em novas tecnologias e em treinamento (BARROS; BOLZAN DE MORAIS, 2021) (STOPANOVSKI, 2020) (BRASIL, 2013), o uso de novas tecnologias por advogados de defesa treinados é restrito a poucos profissionais; o que restringe o número de investigados e acusados que podem contar com o uso das novas tecnologias em seu favor, principalmente pelos altos custos envolvidos.

No saber inquisitório que apenas alguns privilegiados podem acessar a ordem do discurso da salvação e o investigado é um estranho que não entende o que ocorre (FOUCAULT, 2014b, p. 35-39). Não é admissível que em persecução penal cada vez mais influenciada pelas novas tecnologias, o investigado ou acusado não as conheça e utilize. Sua influência na construção do juízo deve ser em paridade.

Concomitante a esta situação, em primeiro lugar, há notória desigualdade econômica entre as partes do processo penal. Em segundo lugar, o inquérito exerce grande influência na instrução e no julgamento do caso penal.[349] Em terceiro lugar, a mídia exerce grande pressão punitiva nos sujeitos do processo.[350] Em quarto lugar, as Defensorias Públicas não são estruturadas como os órgãos de acusação. Contudo, deve-se agir para que "a desigualdade real não desemboque em desigualdade processual" (PRADO, Geraldo, 1999, p. 131). Por isso, o sistema jurídico assegura vantagens à defesa e ao investigado ou acusado, como: a carga probatória caber à acusação (Constituição, art. 5º, LVII); *in dubio pro reo* (CPP, art. 386, VI); o direto da defesa falar por último (CPP, arts. 403 e 476, § 3º); recursos exclusivamente defensivos (CPP, art. 609, parágrafo único); revisão criminal apenas em favor do acusado (CPP, art. 621); entre outras. A paridade no processo penal, portanto, não significa igualdade – evidentemente impossível, já que há "desigualdade real", principalmente econômica, e as posições subjetivas das partes são distintas, como quanto à carga probatória, por exemplo –; a paridade é configurada pelo "equilíbrio global" entre as partes, o que é alcançado com

[349] Vide a introdução e o item 2.6, *supra.*
[350] Vide a nota n. 24, *supra.*

técnicas que aumentam a influência defensiva na construção do juízo (GOMES FILHO, 2001, p. 42-44).

Apesar da situação do progressivo aumento do uso de novas tecnologias pelos órgãos responsáveis pela persecução penal poder ampliar a diferença entre as partes, defende-se que a tecnologia também pode ser utilizada para mitigar essa diferença.

No processo penal, o direito do investigado participar da construção da persecução inicia-se na fase investigativa (SAAD, 2018, p. 70-71); que pode lhe atingir diretamente em seu patrimônio e liberdade pelas cautelares e que cria acervo relevante para a formação da opinião do titular da ação penal, que pode arquivar o inquérito, e para o juízo de conhecimento do caso.[351] Desde a notícia do crime[352] é direito da defesa acessar os autos investigativos, conhecer o que ocorre e atuar para o cumprimento do modelo constitucional do processo.[353]

Neste ponto, a investigação defensiva apresenta especial importância para a paridade entre as partes.[354]

A Constituição (art. 5º, LV) assegura a ampla defesa, com os meios e recursos a ela inerentes. A ampla defesa é indissociável do tempo: sem ser assegurado ao investigado o tempo necessário para o planejamento e execução de sua defesa, não há como acreditar que ela será ampla e efetiva (BARROS, 2008b, p. 20). Frequentemente, o inquérito policial dura anos. E o prazo para responder à acusação é de dez dias (CPP, art. 396).[355] Somente isso já justifica a realização da investigação defensiva em todos os casos penais. Em conjunto à previsão constitucional, o Pacto Internacional dos Direitos Civis e Políticos (art. 14.3.b) e a Convenção Americana de Direitos Humanos (art. 8.2.c) asseguram à defesa o tempo e meios necessários para preparar-se. A investigação defensiva deriva do direito fundamental à ampla defesa e se concretiza pelas investigações realizadas pelo defensor para obter elementos de prova relacionados ao exercício da defesa em qualquer momento da persecução penal; tal

[351] Vide a introdução e o item 2.6, *supra*.

[352] "Com a notícia do crime inicia-se o processo verdadeiramente, com independência de o direito processual brasileiro convergir para a conclusão de que o processo se inicia somente quando a acusação formal é admitida pelo juiz, no recebimento da denúncia ou queixa. É fato. E deste fato – instituição do *processo* desde a notícia crime – são extraídas diversas consequências tanto no âmbito da atividade probatória quanto na influência sobre os estatutos jurídicos dos diversos sujeitos que são personagens obrigatórios em um contexto formado por elementos 'discursivos' e 'não discursivos'." (PRADO, Geraldo, 2019, p. 37-38).

[353] Constituição, artigos 5º, LV, e 133; Lei 8.906, de 1994, artigo 7º, incisos XIV e XXI; Lei n.º 13.869, 2019 (abuso de autoridade), artigo 32; Súmula Vinculante n. 14, do Supremo Tribunal Federal.

[354] Como defende Marta Saad (2004, p. 202): "É preciso, pois, garantir a defesa efetiva do acusado quando esta realmente importa, estendendo-se o exercício do direito de defesa ao inquérito policial. Mas não só a autodefesa, insuficiente em face do próprio comprometimento emocional e do desconhecimento técnico do acusado. Este deve poder contar, pois, com assistência de advogado, legalmente habilitado, zeloso e competente, na real defesa dos interesses de sua liberdade jurídica."

[355] "[…] os prazos fixados para se responder às acusações são, hoje, totalmente desproporcionais e, se poderia afirmar, desleais." (DIAS, 2019, p. 22).

como regulamentado pelo Provimento n. 188/2018, do Conselho Federal da Ordem dos Advogados do Brasil (CFOAB).[356]

Nos casos que envolvem elementos de prova digitais, a defesa pode agir ativamente pela investigação defensiva.[357] Vários dos *softwares* mencionados nos capítulos 3 e 4 desta tese (como: Maltego, FOCA, ExifTool, Metapicz, Metashield, IANA WHOIS, hostip.info, MaxMind, Tor, Nmap, Fern Wifi, Kismet e aplicações de criptografia)[358] são úteis e de uso gratuito. O investigado ou acusado também é legitimado para requerer a busca e a apreensão de elementos digitais (CPP, art. 242) e pode valer-se delas para a elaboração de sua defesa.

Outrossim, tanto na obtenção dos elementos digitais quanto no acesso a esses elementos, o advogado pode contar com profissionais especializados, como detetives, auxiliares, técnicos e peritos (art. 4º do Provimento n. 188/2018, do CFOAB).

Questão problemática é o uso de elemento de prova digital obtido ilicitamente, por *hacker*[359], por exemplo. Parte da literatura jurídica admite o uso da prova ilícita em favor do investigado em função da dignidade da pessoa humana, da liberdade (Constituição, arts. 1º, III, e 5º, *caput*) e da proporcionalidade[360]:

> Aliás, não deixa de ser, em última análise, manifestação do princípio da proporcionalidade a posição praticamente unânime que reconhece a possibilidade de utilização, no processo penal, da prova favorável ao acusado, ainda que colhida com infringência a direitos fundamentais seus ou de terceiros (GRINOVER; FERNANDES; GOMES FILHO, 1996, p. 120).[361]

Outra parte sustenta que o sistema jurídico é um só e, se o ato de obtenção do elemento de prova é permitido pelo Direito como um todo, não há como ele ser considerado ilícito (mormente pela admissão da analogia pelo art. 3º do CPP e pelo *favor rei*); exatamente o que ocorre na situação do investigado, acusado ou terceiro em seu benefício agir amparado em excludente de ilicitude, como a legítima defesa ou o estado de necessidade (Código Penal, arts. 23 a 25). Exemplificadamente: se o investigado realiza intercepção telefônica sem prévia autorização judicial para demonstrar sua inocência e manter sua liberdade, ainda que

[356] Para a comparação da investigação defensiva no Direito estadunidense e no Direito brasileiro, vide: Malan (2012). Sobre aspectos práticos, vide: Dias (2019).
[357] Afinal, "Defender-se o acusado fazendo uso exclusivo do material probatório selecionado pelo acusador é o sonho que todo inquisidor nutre relativamente à posição de seu adversário processual" (PRADO, Geraldo, 2019, p. 85); e o defensor que age ativamente assegura que todas as possibilidades de defesa sejam realizadas.
[358] O Kali Linux conta com dezenas de outros *softwares* úteis pré-instalados.
[359] Um *hacker* de computador é alguém que explora as possibilidades desta tecnologia; já um *cracker* é um *hacker* que quebra barreiras de segurança (STALLMAN, 2022).
[360] Vide o item 4.3.2, *supra.*
[361] "[…] ao próprio Estado não pode interessar a punição do inocente, o que poderia significar a impunidade do verdadeiro culpado; é nesse sentido, aliás, que a moderna jurisprudência norte-americana tem afirmado que o direito à prova de defesa é *superior.*" (GOMES FILHO, 1997, p. 107).

sacrificando a privacidade de terceiro, ele age em estado de necessidade e sua conduta é lícita (JARDIM, 2003, p. 316) (RANGEL, 2012, p. 467).

Certo é que ambas as correntes admitem o uso do elemento de prova irregularmente obtido em favor do investigado ou acusado. Quanto à situação acima suscitada de *hacker* obter irregularmente elemento de prova favorável ao investigado ou acusado, pelas razões expostas, o elemento pode ser utilizado para aquele caso específico[362]. E a conduta do *hacker* não é ilícita se agir amparado em excludente de ilicitude.

Finalmente, destaca-se que somente com o conhecimento do funcionamento das novas tecnologias é possível fiscalizá-lo. Sem isso é impossível a qualquer ator jurídico relacionar o Direito com a tecnologia e contribuir de maneira qualificada para a construção do procedimento que assegure efetivamente a primazia da Constituição. Portanto, para a paridade entre as partes no espaço virtual, o conhecimento transdisciplinar sobre o funcionamento das novas tecnologias é fundamental.

5.5 Limiar

Não há como negar as diferenças da persecução penal que utiliza novos meios de investigação em relação à persecução penal tradicional. E o aumento da importância dos atos investigativos e das cautelares (realizadas principalmente no inquérito) para a construção do juízo modifica radicalmente a dinâmica da atuação das partes.

Em nome da perfectibilidade das garantias de defesa, a participação do investigado ou acusado na persecução que utiliza os novos meios de investigação deve ser assegurada por determinadas técnicas.

Em relação especificamente à busca e à apreensão de elementos de prova digitais, a cadeia de custódia virtual deve ser utilizada contra investigações prospectivas e a diminuição da fronteira entre repressão e prevenção de delitos; o direito ao confronto deve ser exercido contra os agentes públicos e privados envolvidos; a proteção contra a autoincriminação, utilizando-se medidas antiforenses ou não, deve ser destacadamente protegida contra a tendência para a privatização da recolha estatal de informação; e as novas tecnologias devem ser utilizadas para a paridade entre as partes no espaço virtual.

Pela realização destas técnicas é possibilitado ao investigado ou acusado a participação ativa na persecução que pode impactar diretamente em sua liberdade.

[362] "Essa prova ilícita, que excepcionalmente está sendo admitida para evitar o absurdo que representa a condenação de um inocente, não pode ser utilizada contra terceiro." (LOPES JR., 2012, p. 598).

6 CONSIDERAÇÕES FINAIS

A necessidade de resposta rápida no combate ao crime estimula a redução da fronteira entre a repressão e a prevenção aos delitos. Essa resposta rápida ocorre principalmente por investigações protagonizadas pela polícia, que atua antes da fase iniciada com a ação penal, executa os meios ocultos e cruza as informações da rede de vigilância composta por agências públicas e privadas.

Os meios ocultos obtêm, em grande maioria, informações e dados criados pelos próprios investigados, como e-mails, conversas telefônicas e arquivos de computador; o que configura autoincriminação e não pode ser ignorado.

A persecução penal que utiliza esses meios ocultos é distinta da persecução do direito penal repressor tradicional. Os meios de investigação operados sem o conhecimento do investigado, realizados predominantemente no inquérito e viabilizados pelas novas tecnologias, atraem o foco dos sujeitos do processo por obterem informações sensíveis, relevantes e que são frequentemente inacessíveis por outro modo.

Essas características exigem mudanças na dinâmica de atuação do acusado para que ele não seja um objeto de investigação passivo nas persecuções que utilizam os novos meios ocultos, mas, sim, um sujeito de direitos que participa ativamente na construção do juízo.

Esta tese pesquisou o problema de como assegurar a participação do acusado na persecução penal que utiliza o meio oculto da busca de elementos de prova digitais e a apreensão desses elementos. A hipótese da pesquisa foi de que frente a cada uma das principais características da persecução que utiliza meios ocultos, devem ser realizadas técnicas específicas que cumpram a perfectibilidade do contraditório dinâmico; tendo por marcos teóricos o modelo constitucional do processo (que exige que a lei infraconstitucional aperfeiçoe o cumprimento dos institutos processuais constitucionalizados) e a teoria do caso (que reúne, simultaneamente, considerações fáticas, jurídicas e probatórias com o objetivo de auxiliar a participação ativa e estratégica das partes, para que sejam entendidas e melhor argumentem sobre as questões relevantes para o julgamento do caso; especificamente nesta tese, dos casos em que a persecução utiliza a busca e a apreensão de elementos de prova digitais).

Em outras palavras, foi proposto que a participação ativa do acusado na persecução que utiliza a busca e a apreensão de elementos de prova digitais é assegurada por determinadas técnicas diretamente relacionadas às mudanças causadas pelos meios ocultos de investigação: em relação à diminuição da fronteira entre repressão e prevenção de delitos, a

cadeia de custódia de elementos digitais, por possibilitar perceber se a investigação foi prospectiva ou baseada em elementos concretos preexistentes; em relação ao aumento do espaço da polícia e da importância da fase investigativa, o direito de confrontar os agentes públicos e privados envolvidos em audiência; em relação à tendência para a privatização da recolha estatal de informação, a proteção contra a autoincriminação por medidas antiforenses e pela atuação judicial na proteção preventiva das garantias processuais; e em relação ao progressivo aumento do uso de novas tecnologias na persecução penal, a paridade entre as partes no espaço virtual pela ampliação do uso dessas tecnologias pelo acusado.

O recorte do tema pela pesquisa da persecução que utiliza a busca e a apreensão de elementos de prova digitais exigiu transdisciplinaridade, vez que elementos digitais são *bits* operados por computador e que sem o conhecimento de noções da tecnologia envolvida é impossível entender a busca e a apreensão desses elementos.

A demarcação da realização lícita da busca e da apreensão de elementos de prova digitais em consonância ao modelo constitucional do processo também exigiu releituras sobre cautelaridade, requisitos, local, horário, modalidades de busca e de apreensão, procedimento, acesso aos elementos digitais e ilicitude probatória. Foi demonstrado que apenas a situação concreta permite classificar em que consiste a busca de elementos digitais, sendo que a maior parte configura meio oculto de investigação, e que a apreensão de elementos digitais é medida cautelar de obtenção de elemento de prova.

Finalmente, o objetivo da tese de possibilitar o controle do exercício do poder nas persecuções que utilizam a busca e a apreensão de elementos de prova digitais pelo exercício do processo foi, obviamente, alcançado apenas parcialmente – o que é importante de ser destacado, vez que a pesquisa não visa a confirmação da hipótese, mas ao teste da hipótese. Foi corroborado que a cadeia de custódia possibilita identificar investigações prospectivas e ilegais; que o direito ao confronto mitiga o aumento do espaço da polícia; que medidas antiforenses e a atuação judicial preventiva podem proteger o investigado contra a autoincriminação; e que a ampliação do uso de tecnologias pelo acusado pode contribuir para a paridade entre as partes no processo penal. Todavia, a ambição por controle ininterrupto, rápido e em todos os lugares da sociedade de controle nem sempre respeita os limites do Direito; o que faz com que qualquer proposta de controlar o exercício do poder seja necessariamente uma proposta de controlar parte do exercício desse poder. A hipótese da tese apenas possibilita a redução da arbitrariedade e da ilegalidade na persecução que utiliza a busca e a apreensão de elementos de prova digitais. Ela, em primeiro lugar, pressupõe que os vícios vão ocorrer e que para combatê-los são necessários cadeia de custódia, direito ao

confronto, medidas antiforenses, atuação judicial preventiva e aumento do uso de tecnologia pelo acusado; em segundo lugar, novas leis e tecnologias demandarão novas conjecturas. A construção do Estado Democrático de Direito pelo processo é permanente e a cada nova tentativa de expansão irracional do poder punitivo serão exigidas outras proposições que assegurem a legalidade democrática.

REFERÊNCIAS

ABBAGNANO, Nicola. **Dicionário de filosofia.** 5. ed. São Paulo: Martins Fontes, 2007.

AFONSO DA SILVA, José. **Curso de direito constitucional positivo.** 16 ed. São Paulo: Malheiros, 1999.

AGAMBEN, Giorgio. **Estado de exceção.** São Paulo: Boitempo, 2004.

AGAMBEN, Giorgio. **O uso dos corpos.** São Paulo: Boitempo, 2017.

AMODIO, Ennio. **Estetica della giustizia penale:** prassi, media, fiction. Milano: Giuffrè, 2016.

ANDOLINA, Italo; VIGNERA, Giuseppe. **I fondamenti costituzionali della giustizia civile.** 2. ed. Torino: Giappichelli Editore, 1997.

ANGWIN, Julia; LARSON, Jeff; KIRCHNER, Lauren. **Machine Bias:** There's software used across the country to predict future criminals. And it's biased against blacks. Disponível em: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing. Acesso em: 13 jul. 2021.

ARENDT, Hannah. **Origens do totalitarismo.** São Paulo: Companhia das Letras, 2012.

ARISTÓTELES. **Metafísica:** volume 2: texto grego com tradução ao lado. São Paulo: Edições Loyola, 2002.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002:** Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação. Rio de Janeiro: ABNT, 2013a.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27037:** Tecnologia da informação - Técnicas de segurança - Diretrizes para identificação, coleta, aquisição e preservação de evidência digital. Rio de Janeiro: ABNT, 2013b.

BADARÓ, Gustavo Henrique; BOTTINI, Pierpaolo Cruz. **Lavagem de capitais:** aspectos penais e processuais penais. São Paulo: RT, 2012.

BADARÓ, Gustavo Henrique. **Processo penal.** 3. ed. São Paulo: RT, 2015.

BANDEIRA, Leonardo Costa. **Do direito constitucional de recorrer em liberdade.** Belo Horizonte: Del Rey, 2003.

BANDEIRA DE MELLO, Celso Antônio. **Curso de direito administrativo.** 26. ed. São Paulo: Malheiros, 2009.

BARACHO, José Alfredo de Oliveira. **Processo constitucional.** Rio de Janeiro: Forense, 1984.

BARACHO, José Alfredo de Oliveira. **Teoria geral da cidadania:** a plenitude da cidadania e as garantias constitucionais e processuais. São Paulo: Saraiva: 1995.

BARACHO, José Alfredo de Oliveira. Teoria geral da soberania. **Revista Brasileira de Estudos Políticos,** v. 63, n. 64, p. 7-138, 1987.

BARBALHO, João. **Constituição federal brasileira:** commentarios. 2.ed. Rio de Janeiro: F. Briguiet, 1924.

BARBOSA MOREIRA, José Carlos. A Constituição e as provas ilicitamente obtidas. **Revista de Processo,** a. 21, n. 84, p. 144-155, 1996.

BARILLI, Raphael Jorge de Castilho. **Teoria do caso e sua aplicação ao processo penal brasileiro.** Curitiba: CRV, 2019.

BARROS, Flaviane de Magalhães. A atual crise do processo penal brasileiro, direitos fundamentais e garantias processuais. **Duc In Altum Cadernos de Direito**, v. 10, n. 21, mai.-ago., 2018. p. 5-33.

BARROS, Flaviane de Magalhães. **A participação da vítima no processo penal.** Rio de Janeiro: Lumen Juris, 2008a.

BARROS, Flaviane de Magalhães; PIMENTA, Marcus Vinícius. A secularização da inquisitoriedade no processo penal vista pela imagem da audiência de instrução e julgamento. **Revista Brasileira de Ciências Criminais**, v. 171, p. 225-249, 2020.

BARROS, Flaviane de Magalhães; BOLZAN DE MORAIS, José Luis. Compartilhamento de dados e devido processo: como o uso da inteligência artificial pode implicar em uma verdade aleteica. In: NUNES, Dierle *et al.* [org.]. **Inteligência artificial e direito processual:** os impactos da virada tecnológica no direito processual. 2. ed. Salvador: JusPodivm, 2021. p. 343-367.

BARROS, Flaviane de Magalhães. O inimigo no processo penal: uma análise a partir da relação entre direito e política. In: CATTONI, Marcelo; MACHADO, Felipe [coords.]. **Constituição e processo:** entre o direito e a política. Belo Horizonte: Fórum, 2011. p. 87-113.

BARROS, Flaviane de Magalhães. O modelo constitucional de processo e o processo penal: a necessidade de uma interpretação das reformas do processo penal a partir da Constituição. In: MACHADO, Felipe Daniel Amorim; CATTONI DE OLIVEIRA, Marcelo Andrade [Coords.]. **Constituição e processo:** a contribuição do processo ao constitucionalismo brasileiro. Belo Horizonte: Del Rey, 2009. p. 331-345.

BARROS, Flaviane de Magalhães; MACHADO, Felipe Daniel Amorim. **Prisão e medidas cautelares.** Belo Horizonte: Del Rey, 2011.

BARROS, Flaviane de Magalhães Bolzan de Morais; DALLE, Ulisses Moura. Prisão preventiva: em busca de uma noção para garantia de direitos fundamentais. **Revista de Estudos Criminais,** n. 81, p. 89-114, 2021.

BARROS, Flaviane de Magalhães Bolzan de Morais. Processo penal cautelar: remédio e veneno. In: BOLZAN DE MORAIS, Jose Luis. (org.). **A democracia sequestrada.** São Paulo: Tirant lo Blanch, 2019. p. 207-224.

BARROS, Flaviane de Magalhães. **(Re)forma do processo penal:** comentários críticos dos artigos modificados pelas leis n. 11.690/08 e n. 11.719/08. Belo Horizonte: Del Rey, 2008b.

BARROSO, Luís Roberto. **Constituição da República Federativa do Brasil anotada.** 3. ed. São Paulo: Saraiva, 2001.

BAPTISTA DA SILVA, Ovídio Araujo. **Do processo cautelar.** 3. ed. Rio de Janeiro: Forense, 2001.

BATISTA, Nilo. **Introdução crítica ao direito penal brasileiro.** 12. ed. Rio de Janeiro: Revan, 2011.

BAUTISTA, Juan Carlos Urazán. **La cadena de custodia en el nuevo Codigo de Procedimiento Penal.** Disponível em: https://fundacionluxmundi.com/custodia.php. Acesso em: 12 jan. 2021.

BBC NEWS. **Henry Borel:** Como polícia teve acesso a mensagens de WhatsApp apagadas por casal. Disponível em: https://www.bbc.com/portuguese/brasil-56703187. Acesso em: 30 jul. 2021.

BEALE JR., Joseph H. Contempt of court, criminal and civil. **Harvard Law Review,** v. 21, n. 3, p. 161-174, 1908.

BENAVENTE CHORRES, Hesbert. **La aplicación de la teoría del caso y la teoría del delito en el proceso penal acusatorio.** Barcelona: J.M. Bosch Editor, 2011.

BETTIOL, Giuseppe. **Instituições de direito e processo penal.** São Paulo: Pillares, 2008.

BEMERS-LEE, Tim; CAILLIAU, Robert. **WorldWideWeb:** Proposal for a HyperText Project. Disponível em: https://cds.cern.ch/record/2639699/files/Proposal_Nov-1990.pdf. Acesso em: 12 mai. 2021.

BENTHAM, Jeremy. **O panóptico.** 2. ed. Belo Horizonte: Autêntica, 2008.

BENTO DE FARIA. **Código de processo penal.** 2. ed. Rio de Janeiro: Record, 1960. v. 1.

BERNAYS, Edward. **Propaganda.** New York: Ig Publishing, 2005.

BINDER, Alberto M. **El incumplimiento de las formas procesales.** Buenos Aires: Ad-Hoc, 2009.

BINDER, Alberto M. **Introducción al derecho procesal penal.** 2. ed. Buenos Aires: Ad-Hoc, 1999.

BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2019. *E-book*.

BITENCOURT, Cezar Roberto. **Tratado de direito penal econômico:** volume 2. São Paulo: Saraiva, 2016. recurso online.

BLACKSTONE, William. **Commentaries on the laws of England:** book the fourth. 4. ed. Oxford: Clarendon Press, 1770.

BLANCO CORDERO, Isidoro. **El delito de blanqueo de capitales.** 4. ed. Cizur Menor: Aranzadi, 2015.

BLIKSTEIN, Izidoro. **Kaspar Hauser ou a fabricação da realidade.** 3. ed. São Paulo: Cultrix, 1990.

BLOCH-WEHBA, Hannah. Process without procedure: national security letters and First Amendment rights. **Suffolk University Law Review**, v. 49, p. 367-408, 2016.

BOFF, Leonardo. Inquisição: um espírito que continua a existir. In: EYMERICH, Nicolau; LA PEÑA, Francisco de. **Manual dos inquisidores.** Rio de Janeiro: Rosa dos Tempos; Brasília: Ed. UnB, 1993. p. 09-28.

BOLZAN DE MORAIS, José Luis; FESTUGATTO, Adriana Martins Ferreira. **A democracia desinformada:** eleições e *fake news*. Porto Alegre: Livraria do Advogado, 2021.

BOLZAN DE MORAIS, José Luis; MENEZES NETO, Elias Jacob de. Análises computacionais preditivas como um novo biopoder: modificações do tempo na sociedade dos sensores. **Revista Novos Estudos Jurídicos - Eletrônica,** v. 24, n. 3, p. 1129-1154, 2018.

BOTTINO, Thiago. **Direito ao silêncio na jurisprudência do STF.** Rio de Janeiro: Elsevier, 2009.

BRANDOM, Robert B. **Articulating reasons:** an introduction to inferentialism. 2. ed. Cambridge: Harvard University Press, 2001a.

BRASIL. **Código de Processo Civil.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em 21 jan. 2022c.

BRASIL. **Código de Processo Penal Militar.** Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del1002.htm. Acesso em: 13 jan. 2022a.

BRASIL. **Código Penal.** Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 07 fev. 2022g.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 09 dez. 2020a.

BRASIL. **Decreto de 13 de maio de 1809.** Disponível em: http://www.planalto.gov.br/ccivil_03/Atos/dim/1809/DIM-13-5-1809-3.html#view. Acesso em: 13 dez. 2020b.

BRASIL. **Decreto nº 5.015, de 12 de março de 2004.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/decreto/d5015.htm. Acesso em: 28 jan. 2022e.

BRASIL. **Decreto n. 73.332, de 19 de dezembro de 1973.** Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/antigos/d73332.htm. Acesso em: 08 dez. 2020c.

BRASIL. **Decreto n. 8.420, de 18 de março de 2015.** Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2015/Decreto/D8420.htm. Acesso em: 18 dez. 2020d.

BRASIL. **Decreto-lei n. 317, de 13 de março de 1967**. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/1965-1988/Del0317.htm. Acesso em: 20 dez. 2020h.

BRASIL. **Decreto-lei n. 3.689, de 3 de outubro de 1941.** Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em: 11 jan. 2021a.

BRASIL. **Decreto-lei n. 6.378, de 28 de março de 1944.** Disponível em: https://www2.camara.leg.br/legin/fed/declei/1940-1949/decreto-lei-6378-28-marco-1944-389489-publicacaooriginal-1-pe.html. Acesso em: 13 dez. 2020f.

BRASIL. **Decreto-lei n. 667, de 2 de julho de 1969.** Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del0667.htm. Acesso em: 08 dez. 2020e.

BRASIL. **Decreto nº 678, de 06 de novembro de 1992.** Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/d0678.htm. Acesso em: 01 abr. 2022o.

BRASIL. **Exposição de Motivos do Código de Processo Penal.** Disponível em: https://honoriscausa.weebly.com/uploads/1/7/4/2/17427811/exmcpp_processo_penal.pdf. Acesso em: 04 dez. 2020g.

BRASIL. **Lei n. 9.472, de 16 de julho de 1997.** Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9472.htm. Acesso em 17 fev. 2022i.

BRASIL. **Lei n. 12.965, de 23 de abril de 2014.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 19 jan. 2022b.

BRASIL. **Lei n. 13.869, de 05 de setembro de 2019.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13869.htm. Acesso em 02 mar. 2022l.

BRASIL. Câmara dos Deputados. **EXPOSIÇÃO DE MOTIVOS:** Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. Disponível em:

https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/documentos/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf. Acesso em: 10 dez. 2021d.

BRASIL. Conselho Nacional de Justiça. **Resolução n. 332, de 21 de agosto de 2020.** Disponível em: https://atos.cnj.jus.br/files/original191707202008255f4563b35f8e8.pdf. Acesso em 18 mar. 2022n.

BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 2. **Roteiro de atuação:** crimes cibernéticos. 2. ed. Brasília: MPF/2ªCCR, 2013.

BRASIL. Senado Federal. **Projeto de Decreto Legislativo nº 255, de 2021.** Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9026819&ts=1641833584084&disposition=inline. Acesso em: 28 dez. 2021c.

BRASIL. Superior Tribunal de Justiça. **Agravo Regimental no Recurso em Mandado de Segurança nº 62.562/MT.** Relator: ministro Jesuíno Rissato. Brasília, 13 dez. 2021. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201903741193&dt_publicacao=13/12/2021. Acesso em: 02 fev. 2022f.

BRASIL. Superior Tribunal de Justiça. ***Habeas Corpus*** **nº 598.051/SP.** Relator: ministro Rogerio Schietti Cruz. Brasília, 15 mar. 2021. Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=2027533&num_registro=202001762449&data=20210315&formato=PDF. Acesso em: 25 jan. 2022d.

BRASIL. Superior Tribunal de Justiça. **Recurso em *Habeas Corpus* nº 51.531/RO.** Relator: ministro Nefi Cordeiro. Brasília, 09 mai. 2016. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201402323677&dt_publicacao=09/05/2016. Acesso em: 25 jan. 2022c.

BRASIL. Superior Tribunal de Justiça. **Recurso em *Habeas Corpus* nº 99.735/SC.** Relatora: ministra Laurita Vaz. Brasília, 12 dez. 2018. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201801533498&dt_publicacao=12/12/2018. Acesso em: 23 fev. 2022j.

BRASIL. Superior Tribunal de Justiça. **Recurso em Mandado de Segurança nº 49.349/RJ.** Relator: ministro Rogerio Schietti Cruz. Brasília, 02 mar. 2021. Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=2024477&num_registro=201502370206&data=20210302&peticao_numero=-1&formato=PDF. Acesso em: 27 jul. 2021b.

BRASIL. Superior Tribunal de Justiça. **Recurso em Mandado de Segurança nº 61.302/RJ.** Relator: ministro Rogerio Schietti Cruz. Brasília, 04 set. 2020. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201901991320&dt_publicacao=04/09/2020. Acesso em: 28 fev. 2022k.

BRASIL. Supremo Tribunal Federal. ***Habeas Corpus*** **nº 94.173/BA.** Relator: ministro Celso de Mello. Brasília, 27 nov. 2009. Disponível em:

https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=606303. Acesso em: 03 mar. 2022m.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário nº 418.416/SC.** Relator: ministro Sepúlveda Pertence. Brasília, 19 dez. 2006. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=395790. Acesso em: 17 fev. 2022h.

BRENNAN, Tim; DIETERICH, William. Correctional offender management profiles for alternative sanctions (COMPAS). In: SINGH, Jay P. *et al.* [org.]. **Handbook of recidivism risk/need assessment tools.** New Jersey: Wiley-Blackwell, 2018. p. 49-75.

BRÊTAS, Ronaldo de Carvalho Dias. Aspectos técnicos e teóricos da prova no Novo Código de Processo Civil. In: BRÊTAS, Ronaldo de Carvalho Dias *et al.* (org.). **Direito probatório:** temas atuais. Belo Horizonte: D'Plácido, 2016a. p. 99-122.

BRÊTAS, Ronaldo de Carvalho Dias *et al.* **Estudo sistemático do NCPC.** 2. ed. Belo Horizonte: D'Plácido, 2016b.

BRÊTAS, Ronaldo de Carvalho Dias. O Processo Constitucional na construção do Estado Democrático de Direito. In: VILELA, Alexandra; GODINHO, Inês Fernandes; LEITE, Jorge; MEIRA, José Boanerges [orgs.]. **As novas fronteiras do direito.** Porto: Edições Universitárias Lusófonas, 2018a. p. 91-106.

BRÊTAS, Ronaldo de Carvalho Dias. Prefácio. In: SOARES, Carlos Henrique. **Estatuto da advocacia e processo constitucional.** 2. ed. Belo Horizonte: Del Rey, 2016c. p. 17-20.

BRÊTAS, Ronaldo de Carvalho Dias. **Processo constitucional e Estado Democrático de Direito.** 4. ed. Belo Horizonte, Del Rey, 2018b.

BRÊTAS, Ronaldo de Carvalho Dias. **Responsabilidade do Estado pela função jurisdicional.** Belo Horizonte: Del Rey, 2004.

BROWNLIE, Ian. **Princípios de direito internacional público.** Lisboa: Fundação Calouste Gulbenkian, 1997.

BURKE, Colin. Digital sousveillance: a network analysis of the US surveillant assemblage. **Surveillance & Society,** v. 18, p. 74-89, 2020.

CALAMANDREI, Piero. Introduzione allo studio sistematico dei provvedimenti cautelari. In: CALAMANDREI, Piero. **Opere giuridiche:** volume IX: esecuzione forzata e procedimenti speciali. Roma: Roma TrE-Press, 2019. p. 157-254.

CALVET DE MAGALHÃES, Theresa. Da arqueologia do saber ao ensaio filosófico: a problemática de uma ontologia do presente em Foucault. **Síntese,** n. 40, p. 59-83, 1987.

CÂMARA LEAL, Antônio Luiz da. **Comentários ao Código de Processo Penal Brasileiro.** Rio de Janeiro: Freitas Bastos, 1942. v. 1.

CANÊDO, Carlos Augusto; LEMOS, Carolina Barreto. **Crime e risco. Os novos rumos do Direito Penal:** uma política criminal de defesa social. Disponível em: https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad82d9b000001802306d4bd5b3a35e9&docguid=Ie9458a30e11f11e19781010000000000&hitguid=Ie9458a30e11f11e19781010000000000&spos=1&epos=1&td=1&context=20&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1. Acesso em: 13 abr. 2021.

CANGERENA NETO, Francisco Alves. **Meios de obtenção de prova no processo penal:** busca pessoal e ações policiais. Curitiba: Juruá, 2018.

CANOTILHO, J. J. Gomes. **Direito constitucional e teoria da Constituição.** 7. ed. Coimbra: Almedina, 2003.

CAPPELLETTI, Mauro. **La giurisdizione costituzionale delle libertà.** Milano: Giuffrè, 1976.

CARNELUTTI, Francesco. Cenerentola. **Rivista di diritto processuale,** v. 1, n. 1, p. 73-78, 1946.

CARNELUTTI, Francesco. **Lecciones sobre el proceso penal.** Buenos Aires: EJEA, 1950. v. 1.

CARVALHO, Carlos Eduardo Araújo de. **Legitimidade dos provimentos:** fundamentos da ordem jurídica democrática. Curitiba: Juruá, 2009.

CATTONI DE OLIVEIRA, Marcelo Andrade. **Processo constitucional.** 3. ed. Belo Horizonte: Fórum, 2016.

CELLEBRITE. **Premium access to all iOS and high-end Android devices.** Disponível em: https://cf-media.cellebrite.com/wp-content/uploads/2020/07/ProductOverview_CellebritePremium.pdf. Acesso em: 30 jul. 2021.

CERVINI, Raúl; TAVARES, Juarez. **Princípios de cooperação judicial penal internacional no protocolo do Mercosul.** São Paulo: RT, 2000.

CHESWICK, William R.; BELLOVIN, Steven M.; RUBIN, Aviel D. **Firewalls and Internet security:** repelling the wily hacker. 2. ed. Boston: Addison-Wesley, 2003.

CHIOVENDA, Giuseppe. **Instituições de direito processual civil.** 3. ed. São Paulo: Saraiva, 1969. v. 1.

CHIOVENDA, Giuseppe. **Principii di diritto processuale civile.** 2. ed. Napoli: Editrice N. Jovene E C, 1923.

CHOUKR, Fauzi Hassan; BACILA, Carlos Roberto (colaborador). Polícia e Estado de Direito na América Latina: relatório brasileiro. In: AMBOS; COLOMER; VOGLER [orgs.]. **La policía en los estados de derecho latinoamericanos:** un proyecto internacional de investigación. Bogotá: Ediciones Jurídicas Gustavo Ibáñez C., Ltda., 2003. p. 115-156.

COKE, Edward. **The selected writings and speeches of Sir Edward Coke.** Indianapolis: Liberty Fund, 2003. v. 1.

COMISSÃO NACIONAL DA VERDADE (Brasil). **Relatório.** Brasília: CNV, 2014. v. 1. t. 2.

COMOGLIO, Paulo. **Nuove tecnologie e disponibilità della prova:** l'accertamento del fatto nella diffusione delle conoscenze. Torino: Giappichelli, 2018.

CORDEIRO LEAL, André. **Instrumentalidade do processo em crise.** Belo Horizonte: Mandamentos, 2008.

CORDERO, Franco. Direito. In: GIL, Fernando [coord.]. **Enciclopédia Einaudi:** volume 39: Direito – Classes. Lisboa: Imprensa Nacional-Casa da Moeda, 1999. p. 11-128.

CORDERO, Franco. **Gli osservanti:** fenomenologia delle norme. Milano: Giuffrè, 1967.

CORDERO, Franco. **Guida alla procedura penale.** Torino: UTET, 1986.

CORDERO, Fanco. **Ideologie del processo penale.** Milano: Giuffrè, 1966.

CORDERO, Franco. **Procedimiento penal.** Santa Fe de Bogotá: Temis, 2000a. t. 1.

CORDERO, Franco. **Procedimiento penal.** Santa Fe de Bogotá: Temis, 2000b. t. 2.

CORDERO, Franco. **Riti e sapienza del diritto.** Roma: Laterza, 1985.

CORDERO, Franco. **Tre studi sulle prove penali.** Milano: Giuffrè, 1963.

COSTA ANDRADE, Manuel da. **"Bruscamente no verão passado", a reforma do código de processo penal:** observações críticas sobre uma lei que podia e devia ter sido diferente. Coimbra: Coimbra Editora, 2009.

COSTA ANDRADE, Manuel da. Métodos ocultos de investigação (*Plädoyer* para uma teoria geral). In: BONATO, Gilson (org.). **Processo penal, constituição e crítica.** Rio de Janeiro: Lumen Juris, 2011. p. 531-550.

COSTA ANDRADE, Manuel da. **Sobre as proibições de prova em processo penal.** Coimbra: Coimbra Editora, 2013.

COTTA, Francis Albert. **Uma polícia para o império:** historiografia e iconografia sobre a polícia no Rio de Janeiro - primeira metade do século XIX. Disponível em: http://www.fafich.ufmg.br/pae/apoio/umapoliciaparaoimperio.pdf. Acesso em: 13 dez. 2020.

COULANGES, Fustel de. **A cidade antiga.** Tradução de Frederico Ozanam Pessoa de Barros. São Paulo: EDAMERIS, 2006.

COUNCIL OF EUROPE. **Convention on Cybercrime.** Disponível em: https://rm.coe.int/1680081561. Acesso em: 19 jan. 2022a.

COUNCIL OF EUROPE. **T-CY Guidance Note # 3:** Transborder access to data (Article 32). Disponível em: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726a. Acesso em: 25 jan. 2022b.

CUNHA, Rosa Maria Cardoso da. **O caráter retórico do princípio da legalidade.** Porto Alegre: Síntese, 1979.

DAMAŠKA, Mirjan R. **El derecho probatorio a la deriva.** Madrid: Marcial Pons, 2015.

DAMAŠKA, Mirjan R. Of hearsay and its analogues. **Minnesota Law Review,** v. 76, p. 425-458, 1992.

DEI SEGNI, Lotario (pope Innocent III). **De miseria condicionis humane.** Athens: The University of Georgia Press, 1978.

DEL NEGRI, André. **Controle de constitucionalidade no processo legislativo:** teoria da legitimidade democrática. Belo Horizonte: Fórum, 2008.

DEL NEGRI, André. **Segredo de Estado no Brasil.** Belo Horizonte, D'Plácido, 2016.

DELEUZE, Gilles. Controle e devir. In: **Conversações.** São Paulo: Ed. 34, 2008a. p. 209-218.

DELEUZE, Gilles. Post-scriptum sobre as sociedades de controle. In: **Conversações.** São Paulo: Ed. 34, 2008b. p. 219-226.

DIAS, Gabriel Bulhões Nóbrega. **Manual prático de investigação defensiva:** um novo paradigma na advocacia criminal brasileira. Florianópolis: EMais, 2019.

EDGE, Charles; O'DONNELL, Daniel. Introduction to cryptography. In: **Enterprise mac security.** Berkeley: Apress, 2016. p. 497-499.

EDINGER, Carlos. Cadeia de custódia, rastreabilidade probatória. **Revista Brasileira de Ciências Criminais,** v. 120, p. 237-257, 2016.

EGBERT, Simon; LEESE, Matthias. **Criminal Futures:** predictive policing and everyday police work. New York: Routledge, 2021.

ERICSON, Richard V.; HAGGERTY, Kevin D. El control policial del riesgo. **Delito y Sociedad**, v. 16, n. 24, p. 27-61, 2007.

ERICSON, Richard V.; HAGGERTY, Kevin D. The militarization of policing in the information age. **Journal of Political and Military Sociology,** v. 27, p. 233-255, 1999.

ESMEIN, Adhémar. **Histoire de la procédure criminelle en France et spécialement de la procédure inquisitoire, depuis le XIIe siècle jusqu'à nos jours.** Paris: L. Larose et Forcel, 1882.

ESMEIN, Adhémar. **Précis élémentaire de l'histoire du droit français de 1789 à 1814:** révolution, consulat & empire. Paris: L. Larose et L. Tenin, 1908.

ESPÍNOLA FILHO, Eduardo. **Código de processo penal brasileiro anotado.** 6. ed. Rio de Janiero: Editora Rio, 1980. v. 3.

EUROPEAN COMMISSION. **Study on the use of innovative technologies in the justice field** – Final Report. Disponível em: https://orbi.uliege.be/bitstream/2268/252237/1/DS0220605ENN.en.pdf. Acesso em: 17 mar. 2022.

EVANCICH, Nick; LI, Jason. Attacks on industrial control systems. In: COLBERT, Edward JM; KOTT, Alexander [orgs.]. **Cyber-security of SCADA and other industrial control systems.** Cham: Springer, 2016.

FACEBOOK. **Política de Dados.** Disponível em: https://www.facebook.com/about/privacy/update. Acesso em: 20 dez. 2020.

FARIA, Maria Auxiliadora. **A Guarda Nacional em Minas:** 1831-1873. 1977. Dissertação (Mestrado em História) - Universidade Federal do Paraná, Curitiba, 1977.

FAZZALARI, Elio. **Istituzioni di diritto processuale.** 8. ed. Padova: Cedam, 1996.

FERGUSON, Andrew G. Policing predictive policing. **Washington University Law Review,** v. 94, n. 5, p. 1109-1189, 2017.

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

FIGUEIREDO DIAS, Jorge de. A criminalidade organizada: do fenómeno ao conceito jurídico-penal. **Revista Brasileira de Ciências Criminais,** n. 71, p. 11-30, 2008.

FIGUEIREDO DIAS, Jorge de. **Direito processual penal.** Coimbra: Coimbra Editora, 1974.

FINANCIAL ACTION TASK FORCE (FATF). **International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation.** Disponível em: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF %20Recommendations%202012.pdf. Acesso em: 17 dez. 2020.

FLORIAN, Eugenio. **Delle prove penali.** 3. ed. Milano: Istituto Editoriale Cisalpino, 1961.

FOLHA DE S. PAULO. **Nem o FBI consegue decifrar arquivos de Daniel Dantas.** Disponível em: https://www1.folha.uol.com.br/fsp/poder/po2506201015.htm. Acesso em: 27 jul. 2021.

FOUCAULT, Michel. **A arqueologia do saber.** 8. ed. Rio de Janeiro: Forense Universitária, 2014a.

FOUCAULT, Michel. **A ordem do discurso:** aula inaugural no Collège de France, pronunciada em 2 de dezembro de 1970. 24. ed. São Paulo: Edições Loyola, 2014b.

FOUCAULT, Michel. A tecnologia política dos indivíduos. In: **Ética, sexualidade, política.** Rio de Janeiro: Forense Universitária, 2004. (Ditos e escritos; V).

FOUCAULT, Michel. **A verdade e as formas jurídicas.** 4. ed. Rio de Janeiro: Nau, 2013.

FOUCAULT, Michel. **Do governo dos vivos:** curso no Collège de France, 1979-1980 (excertos). 2. ed. São Paulo: Centro de Cultura Social; Rio de Janeiro: Achiamé, 2011.

FOUCAULT, Michel. **História da sexualidade 1:** a vontade de saber. 3. ed. São Paulo: Paz e Terra, 2015a.

FOUCAULT, Michel. **Malfazer, dizer verdadeiro:** função da confissão em juízo: curso em Louvain, 1981. São Paulo: Martins Fontes, 2018.

FOUCAULT, Michel. **Microfísica do poder.** 2. ed. Rio de Janeiro: Paz e Terra, 2015b.

FOUCAULT, Michel. **Os anormais:** curso no Collège de France (1974-1975). São Paulo: Martins Fontes, 2001.

FOUCAULT, Michel. **Segurança, território, população:** curso dado no Collège de France (1977-1978). São Paulo: Martins Fontes, 2008a.

FOUCAULT, Michel. **Vigiar e punir.** 35. ed. Petrópolis: Vozes, 2008b.

FRAGA, Bruno. **Técnicas de invasão:** aprenda as técnicas usadas por hackers em invasões reais. São Paulo: Labrador, 2019.

FRAGOSO, Heleno Cláudio. **ILEGALIDADE E ABUSO DE PODER NA DENÚNCIA E NA PRISÃO PREVENTIVA.** Disponível em: http://www.fragoso.com.br/wp-content/uploads/2017/10/20171003005647-ilegalidade_abuso_poder.pdf. Acesso em: 23 nov. 2022.

FRANÇA. **Code des délits et des peines du 3 brumaire, an 4 (25 octobre 1795).** Disponível em: https://ledroitcriminel.fr/la_legislation_criminelle/anciens_textes/code_delits_et_peines_1795/code_delits_et_peines_1795_1.htm. Acesso em: 03 dez. 2020.

FREDERICO MARQUES, José. **Elementos de direito processual penal.** Campinas: Bookseller, 1998a. v. 1.

FREDERICO MARQUES, José. **Elementos de direito processual penal.** Campinas: Bookseller, 1998b. v. 2.

FRIEDMAN, Richard D. Confrontation: the search for basic principles. **Georgetown Law Journal,** v. 86, p. 1011-1043, 1998.

FUNDAÇÃO GETÚLIO VARGAS. **Projeto "Panaceia universal ou remédio constitucional? Habeas corpus nos Tribunais Superiores".** Disponível em: https://www.conjur.com.br/dl/radiografia-habeas-corpus.pdf. Acesso em: 20 jan. 2022.

FÜSZTER, Erzsébet Balláné. Edmond Locard – "Father of the Crime Lab". **Magyar Rendészet,** v. 16, n. 2, p. 21-26, 2016.

GALANTER, Marc. Why the haves come out ahead: speculations on the limits of legal change. **Law & Society Review,** v. 9, p. 95-160, 1974.

GALUPPO, Marcelo Campos. **Da idéia à defesa:** monografias e teses jurídicas. Belo Horizonte: Mandamentos, 2003.

GEIST, Michael. Cyberlaw 2.0. **Boston College Law Review**, v. 44, p. 323-358, 2003.

GIACOMOLLI, Nereu José. **A fase preliminar do processo penal:** crises, misérias e novas metodologias investigatórias. 2. ed. São Paulo: Tirant lo Blanch, 2022.

GIACOMOLLI, Nereu José. **O devido processo penal:** abordagem conforme a Constituição Federal e o Pacto de São José da Costa Rica. São Paulo: Atlas, 2014.

GIORGI, Raffaele De. O risco na sociedade contemporânea. **Revista de Direito Sanitário**, v. 9, n. 1, p. 37-49, São Paulo, mar.-jun., 2008.

GLOECKNER, Ricardo Jacobsen. **Autoritarismo e processo penal:** uma genealogia das ideias autoritárias no processo penal brasileiro. Florianópolis: Tirant Lo Blanch, 2018.

GÖDEL, Kurt. **On formally undecidable propositions of Principia Mathematica and related systems**. New York: Dover Publications, 1992.

GOLDSCHMIDT, James. **Problemas jurídicos y políticos del proceso penal:** conferencias dadas en la Universidad de Madrid en los meses de diciembre de 1934 y de enero, febrero y marzo de 1935. Barcelona: BOSCH, 1935.

GOMES FILHO, Antonio Magalhães. **A motivação das decisões penais.** São Paulo: RT, 2001.

GOMES FILHO, Antonio Magalhães. **Direito à prova no processo penal.** São Paulo: RT, 1997.

GOMES FILHO, Antonio Magalhães. Notas sobre a terminologia da prova (reflexos no processo penal brasileiro). In: YARSHELL, Flávio Luiz; MORAES, Maurício Zanoide de. **Estudos em homenagem à professora Ada Pellegrini Grinover.** São Paulo: DPJ, 2005. p. 303-318.

GOMES FILHO, Antonio Magalhães; BADARÓ, Gustavo Henrique Righi Ivahy. Prova e sucedâneos de prova no processo penal. **Revista Brasileira de Ciências Criminais,** v. 15, n. 65, p. 175-208, 2007.

GOMES, Luiz Flávio; MAZZUOLI, Valerio de Oliveira. **Comentários à Convenção Americana sobre Direitos Humanos:** Pacto de San José da Costa Rica. 3. ed. São Paulo: RT, 2010.

GOMES, Luiz Flávio; MACIEL, Silvio. **Interceptação telefônica:** comentários à Lei 9.296, de 24.07.1996. São Paulo: RT, 2012.

GONÇALVES, Aroldo Plínio. **Nulidades no processo.** Rio de Janeiro: Aide, 1993.

GONÇALVES, Aroldo Plínio. **Técnica processual e teoria do processo.** Rio de Janeiro: Aide, 1992.

GONTIJO, Lucas de Alvarenga. **Filosofia do direito.** 2. ed. Belo Horizonte: D'Plácido, 2019.

GONTIJO, Lucas de Alvarenga; PRICE, Jorge Eduardo Douglas. Culture of urban violence: the theory of recognition and creative expansion of rights versus biopolicial practices of safety devices. **Revista Jurídica Unicuritiba,** v. 1, n. 58, p. 244-269, 2020.

GOOGLE. **Como o Google lida com solicitações governamentais de informações de usuários.** Disponível em: https://policies.google.com/terms/information-requests?hl=pt-BR. Acesso em: 20 dez. 2020.

GRAHAM, Kyle. **Overcharging.** Disponível em: http://digitalcommons.law.scu.edu/facpubs/608. Acesso em: 23 dez. 2020.

GRECO, Luís. Introdução – O inviolável e o intocável no direito processual penal: considerações introdutórias sobre o processo penal alemão (e suas relações com o direito constitucional, o direito de polícia e o direito dos serviços de inteligência). In: WOLTER, Jürgen. **O inviolável e o intocável no direito processual penal:** reflexões sobre dignidade humana, proibições de prova, proteção de dados (e separação informacional de poderes) diante da persecução penal. São Paulo: Marcial Pons, 2018. p. 21-82.

GRECO, Rogério; CUNHA, Rogério Sanches. **Abuso de autoridade:** Lei 13.869/2019: comentada artigo por artigo. Salvador: JusPodivm, 2020.

GREENBERG, Andy. **Hacker Lexicon:** What Is the Dark Web?. Disponível em: https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/. Acesso em 28 jul. 2021.

GRINOVER, Ada Pellegrini. Parecer sobre busca e apreensão em caso de flagrante delito. In: GRINOVER, Ada Pellegrini. **A marcha do processo.** Rio de Janeiro: Forense, 2000. p. 477-490.

GRINOVER, Ada Pellegrini; FERNANDES, Antonio Scarance; GOMES FILHO, Antonio Magalhães. **As nulidades no processo penal.** 5. ed. São Paulo: Malheiros, 1996.

HAN, Byung-Chul. **Psicopolítica:** o neoliberalismo e as novas técnicas de poder. Belo Horizonte: Âyiné, 2018.

HASSEMER, Winfried. História das idéias penais na Alemanha do pós-guerra. **Revista de informação legislativa**, v. 30, n. 118, p. 237-282, abr.-jun., 1993a.

HASSEMER, Wilfried. Segurança pública no Estado de Direito. IN: HASSEMER, Wilfried. **Três temas de direito penal.** Porto Alegre: Publicações Fundação Escola Superior do Ministério Público, 1993b. p. 61-81.

HERTZOG, Raphaël *et al*. **Kali linux revealed:** mastering the penetration testing distribution (2021). New York: OffSec Press, 2021.

HILBERT, David. Mathematical problems. **Bulletin of the American Mathematical Society,** v. 8, n. 10, p. 437-479, 1902.

HOLMAN, Leonardo Moreno. **Teoría del caso.** Buenos Aires: Didot, 2012.

HOMERO. **Odisseia.** São Paulo: Hedra, 2011.

HUNGRIA, Nélson. **Comentários ao Código Penal:** volume VI. 5. ed. Rio de Janeiro: Forense, 1980.

HUTCHINS, Eric M.; CLOPPERT, Michael J.; AMIN, Rohan M. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. In: RYAN, Julie [org.]. **Leading issues in information warfare & security research.** London: Good News Digital Books, 2011. p. 80-116.

INTERNATIONAL ORGANIZATION OF STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 11179:** Information technology – Metadata registries (MDR). Geneva: ISO/IEC, 2015.

JAEGER, Paul T.; BERTOT, John Carlo; MCCLURE, Charles R. The impact of the USA Patriot Act on collection and analysis of personal information under the Foreign Intelligence Surveillance Act. **Government Information Quarterly**, v. 20, p. 295-314, 2003.

JARDIM, Afrânio Silva. **Direito processual penal.** 11. ed. Rio de Janeiro: Forense, 2003.

JEZLER JÚNIOR, Ivan. **Prova penal digital:** tempo, risco e busca telemática. Florianópolis: Tirant Lo Blanch, 2019.

KIZZA, Joseph Migga. **Guide to computer network security.** 4. ed. Cham: Springer, 2017.

KROMBHOLZ, Katharina *et al*. Advanced social engineering attacks. **Journal of Information Security and Applications,** v. 22, p. 113-122, 2015.

LEAL, Rosemiro Pereira. **Teoria geral do processo:** primeiros estudos. 15. ed. Belo Horizonte: Fórum, 2021.

LEAL, Victor Nunes. **Coronelismo, enxada e voto:** o município e o regime representativo no Brasil. 7. ed. Editora Companhia das Letras, 2012.

LESSIG, Lawrence. **Code:** version 2.0. New York: Basic Books, 2006.

LIN, Xiaodong. **Introductory computer forensics:** a hands-on practical approach. Cham: Springer, 2018.

LIU, Yunfei; MA, Xingjun; BAILEY, James; LU, Feng. **Reflection backdoor:** a natural backdoor attack on deep neural networks. Disponível em: https://arxiv.org/pdf/2007.02343.pdf. Acesso em: 29 jul. 2021.

LOPES JR. Aury. **Direito processual penal.** 9. ed. São Paulo: Saraiva, 2012.

LOPES JR., Aury. **Fundamentos do processo penal:** introdução crítica. São Paulo: Saraiva, 2015.

LOPES JR., Aury; MENDES, Carlos Hélder Carvalho Furtado. **"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. Acesso em: 13 nov. 2022.

MACHADO, Leonardo Marcondes. **Manual de inquérito policial.** Belo Horizonte: CEI, 2020.

MACKENZIE, Charles E. **Coded character sets, history and development.** Reading: Addison-Wesley Publishing Company, 1980.

MADRUGA, Antenor; FELDENS, Luciano. Dados eletrônicos e cooperação internacional: limites jurisdicionais. In: BRASIL. Ministério Público Federal. Secretaria de Cooperação Internacional. **Temas de cooperação internacional.** Brasília: MPF, 2015. p. 47-67.

MAGALHÃES, Assusete. Quebra de sigilo de dados e das comunicações telefônicas: o dever estatal de preservação da fonte da prova. In: Superior Tribunal de Justiça (org.). **Doutrina:** edição comemorativa, 25 anos. Brasília: Superior Tribunal de Justiça, 2014.

MAIER, Julio B. J. **Derecho procesal penal:** parte general: sujetos procesales. Buenos Aires: Del Puerto, 2003. v. 2.

MAIER, Julio B. J. **Derecho procesal penal:** parte general: actos procesales. Buenos Aires: Del Puerto, 2011. v. 3.

MALAN, Diogo Rudge. **Direito ao confronto no processo penal.** Rio de Janeiro: Lumen Juris, 2009.

MALAN, Diogo. Investigação defensiva no processo penal. **Revista Brasileira de Ciências Criminais,** v. 96, p. 279-309, 2012.

MALTEGO TECHNOLOGIES. **Maltego.** Versão: 4.2.18.13878.deb. Disponível em: https://www.maltego.com/downloads/. Acesso em: 28 jul. 2021.

MANTHEY, Christopher C.; SIMONETTI, Carol G. Sixth Amendment; Right of Confrontation; Unavailalbe Witness; State v. Roberts. **Akron Law Review,** v. 12, n. 3, p. 572-591, 1979.

MARÇAL, Antonio Cota. Princípio: estatuto, função e usos no direito. In: TAVARES, Fernando Horta [org.]. **Constituição, direito e processo.** Curitiba: Juruá, 2007. p. 31-58.

MARINHO MARQUES, Leonardo Augusto. Interceptação telefônica e obscurantismo inquisitório: o que aprender com a Lava Jato?. **Revista Brasileira de Ciências Criminais**, n. 122, p. 206-227, 2016.

MARINHO MARQUES, Leonardo Augusto. Sistemas processuais, a produção da prova e os sujeitos do processo penal. **Boletim Informativo IBRASPP,** Porto Alegre, a. 4, n. 6, p. 25-28, 2014.

MARQUES, Pedro Campanholo. **Busca e apreensão:** juízo de admissibilidade. Florianópolis: Tirant Lo Blanch, 2019.

MARSHALL, Angus M. **Digital forensics:** digital evidence in criminal investigation. Chichester: Wiley-Blackwell, 2008.

MARSHALL, Angus M.; MILLER, Peter. CaseNote: mobile phone call data obfuscation & techniques for call correlation. **Digital Investigation,** v. 29, p. 82-90, 2019.

MASSARO, Toni M. The dignity value of face-to-face confrontations. **University of Florida Law Review,** v. 40, p. 863-918, 1988.

MARTÍNEZ-VILLALBA, Juan Carlos Riofrío. La cuarta ola de derechos humanos: los derechos digitales. **Revista latinoamericana de derechos humanos,** v. 25, n. 1, p. 15-45, 2014.

MATEUS. In: **A Bíblia Sagrada.** Traduzida em português por João Ferreira de Almeida. 2. ed. Barueri, SP: Sociedade Bíblica do Brasil, 1999.

MAZZUOLI, Valerio de Oliveira. **Curso de direito internacional público.** 9. ed. São Paulo: RT, 2015.

MAZZUOLI, Valerio de Oliveira. **O controle jurisdicional da convencionalidade das leis.** 2. ed. São Paulo: RT, 2011.

MCNEFF, Jules G. The global positioning system. **IEEE Transactions on Microwave theory and techniques,** v. 50, n. 3, p. 645-652, 2002.

MEDEIROS, Luciano Frontino de. **Inteligência artificial aplicada:** uma abordagem introdutória. Curitiba: InterSaberes, 2018.

MEDEIROS, Nathália Roberta Fett Viana de. **Uso da inteligência artificial no processo de tomada de decisões jurisdicionais:** uma análise sob a perspectiva da teoria normativa da comparticipação. 2019. Dissertação (Mestrado) - Pontifícia Universidade Católica de Minas Gerais, Programa de Pós-Graduação em Direito, Belo Horizonte, 2019.

MENDES, Carlos Hélder Carvalho Furtado. **Malware do Estado e Processo Penal:** a Proteção de dados informáticos face à infiltração por software na investigação criminal. 2018.

Dissertação (Mestrado) - Programa de Pós-Graduação em Ciências Criminais, PUCRS, Porto Alegre, 2018.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional.** 10 ed. São Paulo: Saraiva, 2015.

MENDES, Laura Schertel Ferreira. Habeas data e autodeterminação informativa: os dois lados da mesma moeda. **Revista Brasileira De Direitos Fundamentais & Justiça,** a. 12, n. 39, p. 185-216, 2018.

MENEGUETTI PEREIRA, Luciano. A cooperação jurídica internacional no Novo Código de Processo Civil. **Revista CEJ,** n. 67, p. 18-34, 2015.

MIAILLE, Michel. **Introdução crítica ao direito.** 3. ed. Lisboa: Estampa, 2005.

MIRANDA COUTINHO, Jacinto Nelson de. **A lide e o conteúdo do processo penal.** Curitiba: Juruá, 1989.

MIRANDA COUTINHO, Jacinto Nelson de. A prova ilícita no processo penal: crítica à luz da Constituição da República de 1988. **Delictae,** v. 1, n. 1, p. 247-277, 2016.

MIRANDA COUTINHO, Jacinto Nelson de; CARVALHO, Edward Rocha de. Acordos de delação premiada e o conteúdo ético mínimo do Estado. **Revista de Estudos Criminais,** v. 6, n. 22, p. 75-84, 2006.

MIRANDA COUTINHO, Jacinto Nelson de. Efetividade do processo penal e golpe de cena: um problema às reformas processuais. **Boletim da Faculdade de Direito – Universidade de Coimbra,** v. 78, p. 687-697, 2002.

MIRANDA COUTINHO, Jacinto Nelson de. O papel do novo juiz no processo penal. In: MIRANDA COUTINHO, Jacinto Nelson de (Coord.). **Crítica à teoria geral do direito processual penal.** Rio de Janeiro: Renovar, 2001. p. 3-55.

MIRANDA COUTINHO, Jacinto Nelson de. Sistema acusatório: cada parte no lugar constitucionalmente demarcado. In: MIRANDA COUTINHO, Jacinto Nelson de; CARVALHO, Luis Gustavo Grandinetti Castanho de (Orgs.). **O novo processo penal à luz da Constituição:** análise crítica do Projeto de Lei n. 156/2009, do Senado Federal. Rio de Janeiro: Lumen Juris, 2010. p. 1-17.

MITNICK, Kevin D. **A arte de enganar:** ataques de hackers: controlando o fator humano na segurança da informação. São Paulo: Pearson Education, 2003.

MOMMSEN, Theodor. **El derecho penal romano.** Madrid: La España Moderna, 1905. v. 1.

MONET, Jean-Claude. **Polícias e sociedades na Europa.** São Paulo: Edusp, 2001.

MORAES, Maurício Zanoide de. **Presunção de inocência no processo penal brasileiro:** análise de sua estrutura normativa para a elaboração legislativa e para a decisão judicial. Rio de Janeiro: Lumen Juris, 2010.

MOURA, Maria Thereza Rocha de Assis; MARCHIONATTI, Daniel. Quebra de sigilo em massa e proteção de dados de terceiros: como minimizar o impacto da medida sem prejudicar a ampla defesa. In: ASSOCIAÇÃO NACIONAL DOS PROCURADORES DA REPÚBLICA (org.). **Proteção de dados pessoais e investigação criminal.** Brasília: ANPR, 2020. p. 457-478.

MUNÁRRIZ, Luis Alvarez. **Fundamentos de inteligencia artificial.** Murcia: Universidad de Murcia, 1994.

NICOLITT, André. **Manual de processo penal.** 5. ed. São Paulo: RT, 2014.

NIETZSCHE, Friedrich. **A genealogia da moral.** 4. ed. Petrópolis: Vozes, 2013.

NIETZSCHE, Friedrich Wilhelm. **O nascimento da tragédia,** ou helenismo e pessimismo. São Pauto: Companhia das Letras, 1992.

NIETZSCHE, Friedrich Wilhelm. **Sobre a verdade e mentira.** São Paulo: Hedra, 2008.

NOFER, Michael *et al*. Blockchain. **Business & Information Systems Engineering,** v. 59, n. 3, p. 183-187, 2017.

NORONHA, E. Magalhães. **Curso de direito processual penal.** 11. ed. São Paulo: Saraiva, 1979.

NTP.br. **Arquitetura do NTP.** Disponível em: https://www.ntp.br/conteudo/ntp/. Acesso em: 03 fev. 2022.

NUCCI, Guilherme de Souza. **Código de processo penal comentado.** 11. ed. São Paulo: RT, 2012.

NUCCI, Guilherme de Souza. **Provas no processo penal.** 2. ed. São Paulo: RT, 2011.

NUNES, Dierle José Coelho; LUD, Natanael; PEDRON, Flávio Quinaud. **Desconfiando da imparcialidade dos sujeitos processuais:** um estudo sobre vieses cognitivos, a mitigação de seus efeitos e o *debiasing*. Salvador: JusPodivm, 2018.

NUNES, Dierle; VIANA, Aurélio. **Deslocar função estritamente decisória para máquinas é muito perigoso.** Disponível em: https://www.conjur.com.br/2018-jan-22/opiniao-deslocar-funcao-decisoria-maquinas-perigoso. Acesso em: 13 jul. 2021.

NUNES, Dierle; MARQUES, Ana Luiza Pinto Coelho. Inteligência artificial e direito processual: vieses algorítmicos e os riscos de atribuição de função decisória às máquinas. **Revista de Processo,** v. 285, p. 421-447, 2018.

NUNES, Dierle; MEDEIROS, Nathália. **Inteligência artificial – litigantes habituais e eventuais.** Disponível em: https://www.conjur.com.br/2018-nov-20/opiniao-tecnologia-direito-litigantes-habituais-eventuais. Acesso em: 29 mar. 2022.

NUNES, Dierle José Coelho. **Processo jurisdicional democrático:** uma análise crítica das reformas processuais. Curitiba: Juruá, 2008.

NUNES, Dierle; BAHIA, Alexandre; PEDRON, Flávio Quinaud. **Teoria geral do processo.** Salvador: JusPodivm, 2020.

NUNES, Dierle. Virada tecnológica no direito processual e etapas do emprego da tecnologia no direito processual. In: NUNES, Dierle et al. [org.]. **Inteligência artificial e direito processual:** os impactos da virada tecnológica no direito processual. 2. ed. Salvador: JusPodivm, 2021. p. 17-54.

NÚÑEZ, Eloy Velasco. **Delitos tecnológicos:** definición, investigación y prueba en el proceso penal. Madrid: Sepín, 2016.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **Skills Matter:** further results from the survey of adult skills. Paris: OECD Publishing, 2016.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS. **Carta da Organização dos Estados Americanos "Protocolo de Buenos Aires", assinado em 27 de fevereiro de 1967, na Terceira Conferência Interamericana Extraordinária.** Disponível em: https://www.oas.org/dil/port/tratados_A-41_Carta_da_Organiza %C3%A7%C3%A3o_dos_Estados_Americanos.htm#ch2. Acesso em: 14 fev. 2022.

ORWELL, George. **1984.** São Paulo: Companhia das Letras, 2009.

OSULA, Anna-Maria. Transborder access and territorial sovereignty. **Computer law & Security review,** v. 31, n. 6, p. 719-735, 2015.

PACELLI DE OLIVEIRA, Eugênio. **Curso de processo penal.** 13. ed. Rio de Janeiro: Lumen Juris, 2010.

PARLAMENTO EUROPEU. Resolução do Parlamento Europeu, de 14 de março de 2017, sobre as implicações dos grandes volumes de dados nos direitos fundamentais: privacidade, proteção de dados, não discriminação, segurança e aplicação da lei. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52017IP0076&from=LV. Acesso em: 13 jul. 2021a.

PARLAMENTO EUROPEU. Resolução do Parlamento Europeu, de 16 de fevereiro de 2017, que contém recomendações à Comissão sobre disposições de Direito Civil sobre Robótica. Disponível em: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_PT.html. Acesso em: 13 jul. 2021b.

PATTERSON, David A.; HENNESSY, John L. **Computer organization and design:** the hardware/software interface. 4. ed. Waltham: Elsevier, 2012.

PEIRCE, Charles Sanders. **Semiótica.** São Paulo: Perspectiva, 2015.

PENROSE, Roger. **A mente nova do rei:** computadores, mentes e as leis da física. Rio de Janeiro: Campus, 1993.

PEREIRA, Eliomar da Silva. **Introdução ao direito de polícia judiciária.** Belo Horizonte: Fórum, 2019.

PERRY, Hadley. Virtually face-to-face: the confrontation clause and the use of two-way video testimony. **Roger Williams University Law Review,** v. 13, p. 565-594, 2008.

PIERANGELLI, José Henrique. **Processo penal:** evolução histórica e fontes legislativas. Bauru: Jalovi, 1983.

PIMENTA, Marcus Vinícius. **Poder-saber inquisitório:** observações sobre o inquérito e a dissonância cognitiva. Florianópolis: Tirant Lo Blanch, 2019.

PIMENTA, Marcus Vinícius. Processo Constitucional: consonâncias e dissonâncias entre as proposições de Couture, Fix-Zamudio, Baracho, Andolina e Vignera. **Revista da Faculdade Mineira de Direito,** v. 23, n. 45, p. 256-274, 2020.

PITOMBO, Cleunice Aparecida Valentim Bastos. **Da busca e apreensão no processo penal brasileiro.** 2. ed. São Paulo: RT, 2005.

PITOMBO, Sérgio M. de Moraes. **Do sequestro no processo penal brasileiro.** São Paulo: José Bushatsky, 1973.

PON, Raymond K.; BUTTLER, David J. **Metadata registry, ISO/IEC 11179.** Disponível em: https://digital.library.unt.edu/ark:/67531/metadc926399/m2/1/high_res_d/973862.pdf. Acesso em 16 jul. 2021.

PONTES DE MIRANDA, Francisco Cavalcanti. **Comentários à Constituição de 1946.** Rio de Janeiro: Henrique Cahen Editor, 1947. v. IV.

POULSEN, Kevin. **Documents:** FBI Spyware Has Been Snaring Extortionists, Hackers for Years. Disponível em: https://www.wired.com/2009/04/fbi-spyware-pro/. Acesso em: 28 jul. 2021.

PRADEL, Jean. **Le juge d'instruction.** Paris: Dalloz, 1996.

PRADO, Geraldo. **A cadeia de custódia da prova no processo penal.** São Paulo: Marcial Pons, 2019.

PRADO, Geraldo. **A cadeia de custódia da prova no processo penal.** 2. ed. São Paulo: Marcial Pons, 2021.

PRADO, Geraldo. A excepcionalidade da prisão provisória – comentários aos artigos 311-318 do CPP, na redação da Lei 12.403/2011. In: FERNANDES, Og (coord.). **Medidas cautelares no processo penal:** prisões e suas alternativas: comentários à Lei 12.403, de 04.05.2011. São Paulo: RT, 2011.

PRADO, Geraldo. **Prova penal e sistema de controles epistêmicos:** a quebra da cadeia de custódia das provas obtidas por métodos ocultos. São Paulo: Marcial Pons, 2014.

PRADO, Geraldo. **Sistema acusatório:** a conformidade constitucional das leis processuais penais. Rio de Janeiro: Lumen Juris, 1999.

PRADO, Geraldo. Tutela contra a geolocalização contínua. In: CRUZ, Francisco Brito; FRAGOSO, Nathalie [eds.]. **Direitos fundamentais e processo penal na era digital:** doutrina e prática em debate: vol. 3. São Paulo: InternetLab, 2020. p. 49-69.

PRADO, Luiz Regis. **Curso de direito penal brasileiro:** volume 1: parte geral, arts. 1º a 120. 10. ed. São Paulo: RT, 2010.

PRATT, John. Dangerousness, risk and technologies of power. **The Australian and New Zealand Journal of Criminology,** v. 28, p. 3-31, 1995.

RAMALHO, David Silva. **Métodos ocultos de investigação criminal em ambiente digital.** Coimbra: Almedina, 2019.

RAMAYANA, Marcos. **Direito eleitoral.** 4. ed. Rio de Janeiro: Impetus, 2005.

RAMIRO, André [coord.]. **Mercadores da insegurança:** conjuntura e riscos do hacking governamental no Brasil. Recife: IP.rec, 2022. *E-book*.

RAMOS, João Gualberto Garcez. **Curso de processo penal norte-americano.** São Paulo: RT, 2006.

RANGEL, Paulo. **Direito processual penal.** 20. ed. São Paulo: Atlas, 2012.

RODRIGUES, Anabela Miranda. A fase preparatória do processo penal. In: NUCCI, Guilherme de Souza; MOURA, Maria Thereza Rocha de Assis (orgs.). **Doutrinas essenciais:** processo penal: volume I: teoria geral do processo penal. São Paulo: RT, 2012. p. 995-1016.

ROSA, Alexandre Morais da. **Guia do processo penal conforme a teoria dos jogos.** 6. ed. Florianópolis: EMais, 2020.

ROXIN, Claus. **Derecho penal:** parte general: tomo I: fundamentos. la estructura de la teoria del delito. Madrid: Civitas, 1997.

ROXIN, Claus. **Derecho procesal penal.** Buenos Aires: Editores Del Puerto, 2003.

SAAD, Marta. Defesa no inquérito policial. **Revista de Direito de Polícia Judiciária,** v. 2, n. 4, p. 59-83, 2018.

SAAD, Marta. **O direito de defesa no inquérito policial.** São Paulo: RT, 2004.

SALOMÃO, Luis Felipe [coord.]. **Inteligência Artificial:** Tecnologia Aplicada à Gestão de Conflitos no Âmbito do Poder Judiciário Brasileiro. Disponível em: https://ciapj.fgv.br/sites/ciapj.fgv.br/files/estudos_e_pesquisas_ia_1afase.pdf. Acesso em: 12 jul. 2021.

SANTIAGO NETO, José de Assis. **A formação inquisitória do processo penal brasileiro:** análise a partir da construção legislativa do direito processual penal no Brasil. 2019. Tese (Doutorado) - Pontifícia Universidade Católica de Minas Gerais, Programa de Pós-Graduação em Direito, Belo Horizonte, 2019.

SANTORO, Antonio E. R.; TAVARES, Natália L. F.; GOMES, Jefferson C. O protagonismo dos sistemas de tecnologia da informação na interceptação telefônica: a importância da cadeia de custódia. **Revista Brasileira de Direito Processual Penal,** Porto Alegre, v. 3, n. 2, p. 605-632, mai./ago. 2017.

SAUSSURE, Ferdinand de. **Curso de linguística geral**. 28. ed. São Paulo: Cultrix, 2012.

SEITZ, Nicolai. Transborder search: a new perspective in law enforcement. **Yale Journal of Law & Technology,** v. 7, p. 23-50, 2004.

SHAVIRO, Daniel. The confrontation clause today in light of its common law background. **Valparaiso University Law Review,** v. 26, p. 337-366, 1991.

SIDI, Ricardo. **A interceptação das comunicações telemáticas no processo penal.** Belo Horizonte, D'Plácido, 2016.

SKEEM, Jennifer L.; LOUDEN, Jennifer Eno. **Assessment of evidence on the quality of the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS).** Disponível em: https://cpb-us-e2.wpmucdn.com/sites.uci.edu/dist/0/1149/files/2013/06/CDCR-Skeem-EnoLouden-COMPASeval-SECONDREVISION-final-Dec-28-07.pdf. Acesso em: 13 jul. 2021.

SMART, Nigel P. **Cryptography made simple.** Cham: Springer, 2016.

SOARES, Carlos Henrique. **Estatuto da advocacia e processo constitucional.** 2. ed. Belo Horizonte: Del Rey, 2016.

SOUZA NETO, Cláudio Pereira de. Comentário ao artigo 5º, *caput.* In: CANOTILHO; MENDES; SARLET; STRECK [Coords.]. **Comentários à Constituição do Brasil.** São Paulo: Saraiva, 2013. p. 229-232.

SPOENLE, Jan. **Cloud Computing and cybercrime investigations:** Territoriality vs. the power of disposal. Disponível em: https://rm.coe.int/16802fa3df. Acesso em: 09 fev. 2022.

STALLMAN, Richard. **Free software, free society:** selected essays of Richard M. Stallman. 3. ed. Boston: Free Software Foundation, 2015.

STALLMAN, Richard. **O Manifesto GNU.** Disponível em: https://www.gnu.org/gnu/manifesto.html. Acesso em: 03 mai. 2021.

STALLMAN, Richard. **On Hacking.** Disponível em: https://stallman.org/articles/on-hacking.html. Acesso em: 30 mar. 2022.

STOPANOVSKI, Marcelo. **Laboratório contra lavagem de dinheiro aumenta complexidade de defesa.** Disponível em: https://www.conjur.com.br/2014-dez-08/suporte-litigios-labortatorio-lavagem-aumenta-complexidade-defesa. Acesso em: 23 dez. 2020.

STRECK, Lenio Luiz. O que é isto, - livre convencimento motivado e livre apreciação da prova? In: NUNES; LEITE; STRECK [Coords.]. **O fim do livre convencimento motivado.** Florianópolis: Tirant Lo Blanch, 2018. p. 11-26.

SULOCKI, Victoria-Amália de Barros Carvalho G. de. **Segurança pública e democracia:** aspectos constitucionais das políticas públicas de segurança. Rio de Janeiro: Lumen Juris, 2007.

TARUFFO, Michele. **A prova.** São Paulo: Marcial Pons, 2014.

TARUFFO, Michele. **Uma simples verdade:** o juiz e a construção dos fatos. São Paulo: Marcial Pons, 2012.

THE GUARDIAN. **Edward Snowden: the whistleblower behind the NSA surveillance revelations.** Disponível em: https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance. Acesso em: 21 dez. 2020a.

THE GUARDIAN. **NSA collecting phone records of millions of Verizon customers daily.** Disponível em: https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order. Acesso em: 21 dez. 2020b.

THE GUARDIAN. **NSA shares raw intelligence including Americans' data with Israel.** Disponível em: https://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents. Acesso em: 21 dez. 2020c.

THE GUARDIAN. **Revealed:** leak uncovers global abuse of cyber-surveillance weapon. Disponível em: https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus. Acesso em: 30 jul. 2021.

THE NEW YORK TIMES. **As facebook raised a privacy wall, it carved an opening for tech giants.** Disponível em: https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html. Acesso em: 20 dez. 2020.

THEODORO JÚNIOR, Humberto; NUNES, Dierle; BAHIA, Alexandre Melo Franco; PEDRON, Flávio Quinaud. **Novo CPC:** Lei nº 13.105, de 16.03.2015: fundamentos e sistematização. 3 ed. Rio de Janeiro: Forense, 2016.

THIBAU, Vinícius Lott. **Presunção e prova no direito processual democrático.** Belo Horizonte: Arraes, 2011.

TOLEDO, Francisco de Assis. **Princípios básicos de direito penal.** São Paulo: Saraiva, 1982.

TOR PROJECT. **Sobre:** História. Disponível em: https://www.torproject.org/pt-BR/about/history/. Acesso em: 01 abr. 2022.

TORNAGHI, Hélio. **Instituições de processo penal.** 2. ed. São Paulo: Saraiva, 1977. v. 1.

TORNAGHI, Hélio. **Instituições de processo penal.** 2. ed. São Paulo: Saraiva, 1978. v. 3.

TOURINHO FILHO, Fernando da Costa. **Código de Processo Penal comentado.** 14 ed. São Paulo: Saraiva, 2012.

TOURINHO FILHO, Fernando da Costa. **Processo Penal.** 13 ed. São Paulo: Saraiva, 1992. v. 1.

TRINDADE, André Karam; BERNSTS, Luísa Giuliani. O estudo do direito e literatura no Brasil: surgimento, evolução e expansão. **Anamorphosis: Revista Internacional de Direito e Literatura,** v. 3, n. 1, p. 225-257, 2017.

TUCCI, Rogério Lauria. Busca e apreensão (Direito Processual Penal). In: NUCCI, Guilherme de Souza; MOURA, Maria Thereza Rocha de Assis (orgs.). **Doutrinas essenciais:** processo penal: volume III: processo em geral II. São Paulo: RT, 2012. p. 1321-1244.

TURING, Alan Mathison. Computing machinery and intelligence. **Mind,** v. LIX, n. 236, p. 433-460, 1950.

TURING, Alan Mathison. On computable numbers, with an application to the Entscheidungsproblem. **Proceedings of the London mathematical society**, v. 2, n. 1, p. 230-265, 1937.

UNITED STATES. Supreme Court of the United States. **Brady v. Maryland, 373 U.S. 83 (1963).** Disponível em: https://supreme.justia.com/cases/federal/us/373/83/. Acesso em: 12 jan. 2021.

VACIAGO, Giuseppe. **Cloud computing and data jurisdiction:** a new challenge for digital forensics. Disponível em: https://www.juridice.ro/wp-content/uploads/2019/09/cyberlaws_2012_1_20_70033-1.pdf. Acesso em 14 mai. 2021.

VACIAGO, Giuseppe. Opportunities and challenges in the legal tech services in the italian and european framework. In: PERUGINELLI, G.; FARO, S. [orgs.]. **Knowledge of the law in the big data age.** Clifton: IOS Press, 2019. p. 208-289.

VALENTE, Manuel Monteiro Guedes. **Cadeia de custódia da prova.** 2. ed. Coimbra: Almedina, 2020.

VALENTE, Manuel Monteiro Guedes. **Conhecimentos fortuitos:** a busca de um equilíbrio apuleiano. Coimbra: Almedina, 2006.

VALENTE, Manuel Monteiro Guedes. **Direito penal do inimigo e o terrorismo.** 2. ed. São Paulo: Almedina, 2016.

VALENTE, Manuel Monteiro Guedes. **Escutas telefônicas:** da excepcionalidade à vulgaridade. 2. ed. Coimbra: Almedina, 2008.

VALENTE, Manuel Monteiro Guedes. Os Direitos e Garantias dos Cidadãos investigados na Era Digital. In: ANTONIALLI, Dennys; FRAGOSO, Nathalie [eds.]. **Direitos fundamentais e processo penal na era digital:** doutrina e prática em debate: vol. 2. São Paulo: InternetLab, 2019. p. 12-22.

VALENTE, Manuel Monteiro Guedes. **Teoria geral do direito policial.** 2. ed. Coimbra: Almedina, 2009.

VALLE, Gabriel; VALLE, Sofia. **Lições de filosofia do direito.** Rio de Janeiro: Forense, 2012.

VALLE, Gabriel. **Metafísica clássica.** Belo Horizonte; 2007. Apostila do Curso de Bacharelado em Filosofia da PUC-Minas, 2007.

VERRI, Pietro. **Observações sobre a tortura.** São Paulo: Martins Fontes, 1992.

VIANNA, Túlio; MACHADO, Felipe. **Crimes informáticos:** conforme a lei nº 12.737/2012. Belo Horizonte: Fórum, 2013.

VIANNA, Túlio. **Transparência pública, opacidade privada:** o Direito como instrumento de limitação de poder na sociedade de controle. Rio de Janeiro: Revan, 2007.

VON NEUMANN, John. First draft of a report on the EDVAC. **IEEE Annals of the History of Computing,** v. 15, n. 4, p. 27-75, 1993.

WARAT, Luis Alberto. **A ciência jurídica e seus dois maridos.** Santa Cruz do Sul: Faculdades Integradas de Santa Cruz do Sul, 1985.

WARREN, Samuel; BRANDEIS, Louis. The right to privacy. **Harvard law review,** v. 4, n. 5, p. 193-220, 1890.

WIGMORE, John Henry. **A treatise on the anglo-american system of evidence in trials at common law including the statutes and judicial decisions of all jurisdictions of the United States and Canada.** 2. ed. Boston: Little, Brown, and Company, 1923. v. 3.

WIKIPEDIA. **Planta da estrutura do Panóptico idealizado por Bentham (desenho do arquiteto inglês Willey Reveley, 1791).** Disponível em: https://pt.wikipedia.org/wiki/Pan-%C3%B3ptico#/media/Ficheiro:Panopticon.jpg. Acesso em: 04 nov. 2020.

XU, Xingyuan et al. 11 TOPS photonic convolutional accelerator for optical neural networks. **Nature,** v. 589, n. 7840, p. 44-51, 2021.

YAGUELLO, Marina. **Alice no país da linguagem:** para compreender a linguística. Lisboa: Estampa, 1991.

ZACCARIOTTO, José Pedro. **A polícia judiciária no Estado Democrático.** Brazilian Books: Sorocaba, 2005.

ZACCONE, Orlando. **Indignos de vida:** a forma jurídica da política de extermínio de inimigos na cidade do Rio de Janeiro. Rio de Janeiro: Revan, 2021.

ZAFFARONI, Eugenio Raúl. **A palavra dos mortos:** conferências de criminologia cautelar. São Paulo: Saraiva, 2012.

ZAFFARONI, Eugenio Raúl; BATISTA, Nilo. **Direito penal brasileiro.** 4. ed. Rio de Janeiro: Revan, 2011. v. 1.

ZAFFARONI, Eugenio Raúl. Entrevista conduzida por Tamires Maria Alves e Gabriela Laura Gusis. **Revista Estudos Políticos,** v. 8, n. 2, p. 04-10, 2017.

ZAPPALÀ, Salvatore. **Human rights in international criminal proceedings.** Oxford: Oxford University Press, 2008.

ZHENG, Zibin *et al*. Blockchain challenges and opportunities: a survey. **International Journal of Web and Grid Services,** v. 14, n. 4, p. 352-375, 2018.

ZULLI, André Luiz Cardoso Azoubel. **Guarda Real da Polícia do Rio de Janeiro:** um estudo sobre as atribuições da primeira instituição policial ostensiva brasileira (1809 – 1831). 2018. Dissertação (Mestrado em História) - Universidade Federal do Estado do Rio de Janeiro, Rio de Janeiro, 2018.