UNIVERSIDADE DE BRASÍLIA
FACULDADE DE DIREITO
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO

THALES CASSIANO SILVA

Os dados pessoais como objeto da pretensão acusatória: a finalidade como critério limitador das ações de aquisição, uso e reúso de informações na investigação preliminar

Brasília
2026

Thales Cassiano Silva

Os dados pessoais como objeto da pretensão acusatória: a finalidade como critério limitador das ações de aquisição, uso e reúso de informações na investigação preliminar

Tese de Doutorado apresentado ao Programa de Pós-Graduação em Direito, da Faculdade de Direito da Universidade de Brasília, como requisito para obtenção do grau de Doutor em Direito.

Orientador: Prof. Dr. Evandro Charles Piza Duarte

Brasília

2026

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

Cassiano Silva, Thales
C345d Os dados pessoais como objeto da pretensão acusatória: a finalidade como critério limitador das ações de aquisição, uso e reúso de informações na investigação preliminar / Thales Cassiano Silva; orientador Evandro Charles Piza Duarte. Brasília, 2026.
239 p.

Tese(Doutorado em Direito) Universidade de Brasília, 2026.

1. Processo Penal. 2. Proteção de Dados. 3. Finalidade Probatória. I. Piza Duarte, Evandro Charles, orient. II. Título.

Thales Cassiano Silva

Os dados pessoais como objeto da pretensão acusatória: a finalidade como critério limitador das ações de aquisição, uso e reúso de informações na investigação preliminar

Tese de Doutorado apresentado ao Programa de Pós-Graduação em Direito, da Faculdade de Direito da Universidade de Brasília, como requisito para obtenção do grau de Doutor em Direito.

Orientador: Prof. Dr. Evandro Charles Piza Duarte

Aprovada em: __/__/2026

Banca Examinadora:

_____

Professor Doutor Evandro Charles Piza Duarte – orientador (UnB)

_____

Professor Doutor Ney de Barros Bello Filho (UnB)

_____

Professor Doutor Marcelo Stopanovski Ribeiro (IDP)

_____

Professor Doutor Rafael de Deus Garcia (IDP)

_____

Professor Doutor Fernando Nascimento dos Santos (UnB)

À minha mãe, Graça, e ao meu pai, Altino, que são a base de todos os sonhos que realizo.

AGRADECIMENTOS

Eu refleti muito sobre o que deveria constar nos agradecimentos desta tese e ainda não sei ao certo o que escrever. Muitas pessoas fizeram parte da minha caminhada e foram essenciais para que eu chegasse até aqui, mas hoje vou destacar quem mais me faz falta.

Meu avô Manuel não me viu ingressar na Faculdade de Direito da UnB; partiu antes disso. Ele sempre dizia que, na nossa família, nunca tinha "dado" doutor, referindo-se às profissões tradicionalmente prestigiosas. Só consigo pensar na falta que ele me faz e em como eu queria que estivesse vivo para saber que, enfim, serei doutor. Sou profundamente grato por sempre ter me sentido tão amado por ele, que, na simplicidade de quem foi candango em Brasília, inspira muito da minha visão humanista; tinha horror ao utilitarismo, mesmo sem nunca ter aprendido a ler.

O apoio que recebi para chegar até aqui me envaidece – ainda que talvez não devesse ser dito dessa forma –, mas ter me sentido tão amado é um privilégio pelo qual só posso agradecer.

Agradeço à minha mãe e ao meu pai por terem me permitido sonhar.

Agradeço à minha Yasmin por dividir comigo os bons e os maus momentos dessa trajetória.

“Tu não devias ter ficado velho antes de ter ficado sábio.”
Rei Lear, William Shakespeare

RESUMO

Esta tese examina a utilização de dados pessoais como objeto da pretensão acusatória no processo penal, situada no contexto do uso crescente dessas informações na investigação criminal e da inadequação da racionalidade processual para assegurar direitos fundamentais, como o devido processo legal, a privacidade e a autodeterminação informacional. O descompasso entre a realidade tecnológica e as justificativas teóricas do direito motivou a pesquisa. A pergunta orientadora indaga se a racionalidade jurídico-processual brasileira é adequada para garantir a licitude da aquisição, do uso e do reúso de dados pessoais no âmbito penal, em conformidade com o princípio da finalidade. A hipótese formulada sustenta que esse princípio, originalmente desenvolvido no campo da proteção de dados, possui conteúdo normativo aplicável ao processo penal, atuando como critério limitador do potencial epistêmico do uso e do reúso de informações frente a desvios da função que justificou sua coleta. Para respondê-la, a tese retoma a criminologia do risco para analisar as infraestruturas informacionais disponíveis a Estados e empresas na coleta de dados em ambientes digitais e físicos. A pesquisa teórica revisitou categorias de vigilância da criminologia e as utilizou para analisar criticamente a arquitetura informacional da segurança pública e da persecução penal brasileiras, o que culminou na identificação de uma unidade informacional entre as referidas atividades. Em um segundo momento, foram abordadas as categorias dogmáticas do processo penal sobre atos de investigação que visam ao reúso de dados privados e de segurança pública como objeto da pretensão acusatória, identificando-se as principais estratégias regulatórias e práticas jurídicas, que são marcadas pela ausência de critérios definidos legalmente para sua transferência à investigação preliminar. Ao final, a hipótese foi confirmada: a racionalidade processual penal brasileira não vincula o uso e o reúso de dados à finalidade delimitada pela hipótese investigativa, enquanto o princípio da finalidade demonstra conteúdo jurídico apto a limitar a utilização dessas informações.

Palavras-chave: Processo Penal. Proteção de Dados. Finalidade Probatória.

ABSTRACT

This thesis examines the use of personal data as the object of the prosecutorial claim in criminal proceedings, situated within the context of the increasing use of such information in criminal investigations and the inadequacy of procedural rationality to ensure fundamental rights, such as due process of law, privacy, and informational self-determination. The disconnect between technological reality and legal theoretical justifications motivated this research. The guiding question asks whether Brazilian legal-procedural rationality is adequate to guarantee the lawfulness of the acquisition, use, and reuse of personal data in the criminal sphere, in compliance with the purpose limitation principle. The formulated hypothesis maintains that this principle, originally developed in the field of data protection, possesses normative content applicable to criminal procedure, acting as a limiting criterion for the epistemic potential of the use and reuse of information regarding deviations from the function that justified its collection. To answer this, the thesis draws upon risk criminology to analyze the informational infrastructures available to States and companies for data collection in digital and physical environments. The theoretical research revisited surveillance categories from criminology and used them to critically analyze the informational architecture of Brazilian public security and criminal prosecution, culminating in the identification of an informational unity between said activities. Subsequently, the dogmatic categories of criminal procedure regarding investigative acts aimed at the reuse of private and public security data as the object of the prosecutorial claim were addressed, identifying the main regulatory strategies and legal practices, which are marked by the absence of legally defined criteria for their transfer to the preliminary investigation. In the end, the hypothesis was confirmed: Brazilian criminal procedural rationality does not bind the use and reuse of data to the purpose delimited by the investigative hypothesis, while the purpose limitation principle demonstrates legal content capable of limiting the utilization of such information.

Keywords: Digital evidence. Criminal Procedure. Data Protection. Evidentiary Purpose.

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABIN - Agência Brasileira de Inteligência

ACLU - American Civil Liberties Union

ADC - Ação Declaratória de Constitucionalidade

ADPF - Arguição de Descumprimento de Preceito Fundamental

ANPD - Autoridade Nacional de Proteção de Dados

API - Interface de Programação de Aplicações

LAPIN - Laboratório de Políticas Públicas e Internet

ARE - Agravo em Recurso Extraordinário

ASSESPRO - Federação das Associações das Empresas Brasileiras de Tecnologia da Informação

CCBE - Council of Bars and Law Societies of Europe

CCGD - Comitê Central de Governança de Dados

CF - Constituição Federal

CGDI - Comitê de Governança de Dados e Sistemas da Informação

CNH - Carteira Nacional de Habilitação

CNMP - Conselho Nacional do Ministério Público

COAF - Conselho de Controle de Atividades Financeiras

COEC - Certificado de Ordem Europeia de Conservação

COEP - Certificado de Ordem Europeia de Produção

CORTEX - Plataforma Integrada de Operações e Monitoramento de Segurança Pública Córtex

CPP - Código de Processo Penal

DEI - Decisão Europeia de Investigação

DEI - Decisão Europeia de Investigação

DENATRAN - Departamento Nacional de Trânsito

DEP - Decisão Europeia de Produção

DF – Distrito Federal

DJO - Departamento de Justiça - dos Estados Unidos

DOJ - Department of Justice

ECA - Estatuto da Criança e do Adolescente

ECPA - Electronic Communications Privacy Act

EFF - Electronic Frontier Foundation

ELENA - E-card de saúde na Alemanha

ERB - Estação Rádio Base

FBI - Federal Bureau of Investigation

FIPs - Fair Information Practices

FTC - Federal Trade Commission

GDPR - General Data Protection Regulation - Regulamento Geral sobre a Proteção de Dados da União Europeia

GIS - Geographic Information System

GPS - Global Positioning System

IAGRO-MS - Agência Estadual de Defesa Sanitária de Mato Grosso do Sul

IBCCrim – Instituto Brasileiro de Ciências Criminais

ICN - Identificação Civil Nacional

IMEI - International Mobile Equipment Identity

IP - Internet Protocol

IRIS - Instituto de Referência em Internet e Sociedade

ISO - International Organization for Standardization

JAI - Justiça e Assuntos Internos (referente a decisões do Conselho da UE).

LED - Law Enforcement Directive

LGPD - Lei Geral de Proteção de Dados

LLM - Large Language Model

MCI - Marco Civil da Internet

MJSP - Ministério da Justiça e Segurança Pública

MLATs - Mutual Legal Assistance Treaties

MP - Ministério Público

NFC - Near Field Communication

NSA - National Security Agency

OEC - Ordem Europeia de Conservação

OEP - Ordem Europeia de Produção

PbD - Privacy by Design

PDF - Portable Document Format

PETs - Privacy Enhancing Technologies

PL - Projeto de Lei

PLC - Projeto de Lei da Câmara.

PNSPDS - Política Nacional de Segurança Pública de Defesa Social

RAIS - Relação Anual de Informações Sociais

RE - Recurso Extraordinário

REsp - Recurso Especial

RHC - Recurso em Habeas Corpus

RMS - Recurso em Mandado de Segurança

SCA - Stored Communications Act

SEDEC - Secretaria Nacional de Proteção e Defesa Civil

SENAD - Secretaria Nacional de Política de Drogas

SENASP - Secretaria Nacional de Segurança Pública

SERP - Sistema Eletrônico de Registros Públicos

SERPRO - Serviço Federal de Processamento de Dados

SINESP - Sistema Nacional de Informações de Segurança Pública, Prisionais e sobre Drogas

SISBIN - Sistema Brasileiro de Inteligência

SISCOAF - Sistema de Controle de Atividades Financeiras

SR/PF/MS - Superintendência da Polícia Federal no Mato Grosso do Sul

STF - Supremo Tribunal Federal

STJ - Superior Tribunal de Justiça

SUS - Sistema Único de Saúde

SUSP - Sistema Único de Segurança Pública

TCU - Tribunal de Contas da União

TEI - Técnicas Especiais de Investigação

TFUE - Tratado de Funcionamento da União Europeia

TJRS - Tribunal de Justiça do Rio Grande do Sul

TJSP - Tribunal de Justiça de São Paulo

TJUE - Tribunal de Justiça da União Europeia

TOMs - Technical and Organisation Measures

TP - Tutela Provisória

VPI - Verificação Preliminar de Informação

SUMÁRIO

INTRODUÇÃO

A proteção de dados e o processo penal têm, pelo menos, uma característica em comum: são ramos do direito que estabelecem limites ao próprio Estado no controle da informação, impedindo que agências estatais detenham conhecimento ilimitado e, consequentemente, poder ilimitado[1]. O poder informacional é uma característica da atual conjuntura histórica e é transversal para as diversas relações jurídicas, sendo claramente visível nas relações econômicas[2], mas nem sempre devidamente abordado no campo das ciências criminais, que é o objeto desta tese.

Apesar das diferenças entre esses campos de estudo no que tange à limitação do poder informacional, eles convergem em um ponto-comum, as garantias fundamentais impedem que as pessoas sejam tratadas como objetos no uso de seus dados pessoais por terceiros. Essa afirmação é válida tanto para o poderio econômico das *Big Techs* quanto para o controle das atividades das agências estatais de persecução penal e segurança pública, visto que o Estado-penal atua como um grande agente de coleta, tratamento e transmissão de dados pessoais.

A resposta jurídica a esse estado de coisas é a autodeterminação informacional, elevada ao status de garantia fundamental com a inclusão do inciso LXXIX no artigo 5º da Constituição Federal[3]. Ela se incorpora ao âmbito dos direitos fundamentais, visando limitar atividades estatais com relevância penal, como a vigilância automatizada. O conteúdo jurídico dessa norma consiste na exigência de que os indivíduos disponham de meios jurídicos para controlar as informações pessoais conhecidas a seu respeito, isto é, exercer controle sobre os dados coletados e utilizados por particulares ou pelo poder público[4].

Os dados digitais são a base do processamento estruturado de informações nas ações investigativas automatizadas e autônomas, constituindo o insumo de todas as formas de processamento[5]. Não por outra razão, há algumas décadas, essa base passou a ser defendida como

---

[1] GRECO, Luís. Organização e introdução. 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. Tradução Alaor Leite, Eduardo Viana e Luís Greco. 1. ed. São Paulo: Marcial Pons, 2018, p. 45.
[2] SRNICEK, Nick. Platform capitalism, 2017, p. 39.
[3] BRASIL. Constituição da República Federativa do Brasil de 1988. Art. 5º, inc. LXXIX.
[4] ESTELITA, Heloisa. O RE 1.055.941: um Pretexto para Explorar Alguns Limites à Transmissão, Distribuição, Comunicação, Transferência e Difusão de Dados Pessoais pelo COAF. Direito Público, 2021, p. 613.
[5] FERGUSON, Andrew Guthrie. Big Data and Predictive Reasonable Suspicion. University of Pennsylvania Law Review, v. 163, n. 2, p. 353, jan. 2015.

valor jurídico autônomo de proteção constitucional, notoriamente originada na Alemanha[6]. Nessa linha, a tese aborda as ações de coleta[7], uso e reúso de dados por agências de persecução penal e os limites processuais penais da produção de provas digitais.

No Brasil, a referida alteração constitucional, era fortemente defendida academicamente, e o que justifica a opção da tese por projetar conteúdo normativo da autodeterminação informacional em dois objetos: i) nas ações de compartilhamento de dados pessoais entre os órgãos de segurança pública e persecução penal; ii) na racionalidade jurídica brasileira sobre os atos de investigação e meios de obtenção de provas. Tal estratégia tem o objetivo de identificar o potencial normativo que o princípio da finalidade do tratamento de dados pode aportar à racionalidade processual penal.

Em outras palavras, o objetivo é contribuir para o campo de estudos com a identificação do potencial hermenêutico que a referida garantia constitucional confere ao sistema processual brasileiro. Isso não significa que a aplicação de outros raciocínios tenha perdido a relevância, mas apenas que esta tese se propõe a testar os limites e as contribuições do princípio da finalidade do tratamento nos dois objetos acima indicados. Para tanto, a pesquisa enfrenta o persistente conflito entre a autodeterminação informacional e o legítimo interesse do Estado em acessar dados pessoais para cumprir suas funções legais[8].

Para cumprir o propósito de pesquisa mencionado, antes de expor o problema de pesquisa, apresenta-se sucintamente a progressão do trabalho, capítulo por capítulo, para antecipar o racional desenvolvido. Busca-se, assim, orientar a leitura de modo mais didático, considerando que se trata de um tema complexo e, em geral, abordado de forma não sistematizada na pesquisa jurídica.

O Capítulo 1 retoma categorias criminológicas fundamentais sobre controle e vigilância para fundamentar a análise crítica do que a tese conceituou como arquitetura informacional. O estudo engloba os dispositivos de coleta de dados utilizados pelas agências públicas e por particulares, evidenciando que existe um espaço de decisão política no uso de estratégias que visam à maximização dos registros de dados pessoais, justificada pela segurança pública. Em sequência, o processo legislativo que altera essa arquitetura é analisado como um objeto de política criminal. Defende-se que a legitimidade do uso de tecnologias da informação depende da observância de

---

[6] GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo. O direito de proteção de dados no processo penal e na segurança pública. 1. ed. Rio de Janeiro: Marcial Pons, 2021, p. 78

[7] A coleta marca o início do controle sobre o dado, que é precedido por um corolário de direitos já previstos na legislação brasileira no âmbito do direito privado, tais como exigir o apagamento e a retificação de informações incorretas, por exemplo.

[8] GLEIZER; MONTENEGRO; VIANA, 2021, p. 80.

dois critérios de validade: a adequação legal e a adequação funcional, os quais devem condicionar o próprio processo legislativo e a aquisição das tecnologias pelo Estado.

Após analisar a infraestrutura citada, o Capítulo 2 se aprofunda no nível da aquisição de dados, examinando ações estatais e privadas. Explora-se a permeabilidade entre a coleta realizada por particulares e o legítimo interesse do Estado em reutilizá-la, o que configura um paradoxo: ao mesmo tempo em que o Estado exige a minimização da coleta pelas empresas – alcançada por princípios como o *privacy by design* – ele demanda acesso aos mesmos dados para seus usos legítimos. A partir dessa tensão, a tese propõe uma taxonomia das bases de dados, subdividindo-as em três categorias que exigem regimes jurídicos próprios: (i) bases privadas; (ii) bases privadas criadas por deveres regulatórios; e (iii) bases públicas. Cada uma delas se conecta ao processo penal por formas distintas, isto é, por compartilhamento ou atos investigativos específicos.

Posteriormente à análise das formas de aquisição, o Capítulo 3 desloca o foco para os usos, ou seja, o processamento computacional com utilidade para o direito. O estudo se concentra no tratamento de dados realizado na segurança pública, operado sob uma lógica de maximização pela consolidação de informações de diversas agências. Com efeito, o atual modelo de gestão brasileiro é analisado por meio do Sistema Único de Segurança Pública (SUSP), com aprofundamento nas técnicas de monitoramento e vigilância à disposição do Ministério da Justiça (como o Córtex). Em razão dos achados da pesquisa, discute-se a necessidade de observância da separação informacional de funções como dimensão institucional da autodeterminação informacional, contrapondo-se à "unidade informacional" vigente no atual modelo brasileiro.

O Capítulo 4 é especificamente focado no início da investigação preliminar e tem a função de definir as características essenciais do elemento informativo digital (imaterialidade, volatilidade e replicabilidade), destacando seus aspectos técnicos diferenciadores em relação às provas analógicas, a fim de propor novas interpretações jurídicas e criticar a leitura atual da doutrina e da jurisprudência. Subsequentemente, a tese revisita as categorias de produção probatória anteriores ao contraditório (provas irrepetíveis e antecipadas), correlacionando a taxonomia das bases de dados descrita anteriormente com os meios de ingresso desses elementos, como a apreensão de dispositivos e as requisições de dados.

N sequência, o Capítulo 5 expõe os atos investigativos em espécie, momento em que se identifica o maior déficit da dogmática processual para lidar com os elementos digitais. A análise abrange desde as formas mais simples, como a apreensão de provas entregues voluntariamente, até

os meios ocultos situados na fronteira do debate jurídico, como o uso de *malwares* para infiltração. Examina-se o regime de requisições de dados na sistemática brasileira, criticando a proteção jurídica estática conferida às informações, baseada apenas na nomenclatura, em detrimento da análise dos possíveis reúsos do dado. Por fim, abordam-se os meios ocultos, que envolvem as interceptações, a infiltração digital e a legalidade dos *softwares* espiões.

As análises do Capítulo 5 sobre o regime de requisições conduziram, no Capítulo 6, à comparação com os modelos internacionais estabelecidos para enfrentar esse desafio jurídico. Nesse sentido, a pesquisa examina o modelo legal americano (Cloud Act) e o sistema da União Europeia (Pacote de Provas Digitais), com o objetivo de aumentar a consciência situacional sobre a territorialização de dados como fundamento de jurisdição. A relevância desse comparativo reside na constatação de que, embora o Supremo Tribunal Federal tenha reconhecido a constitucionalidade da obrigação de entrega de dados por empresas sediadas no exterior, a ausência de critérios legais para instrumentalizar essa obrigação, além da falta de legitimidade, reduz a eficácia das decisões judiciais e potencializa conflitos jurisdicionais.

O Capítulo 7 também condensa as críticas realizadas ao longo da tese e apresenta modelos prescritivos para a superação da dogmática processual penal brasileira, tomando como base o potencial normativo da autodeterminação informacional aplicada à produção probatória. A discussão é balizada pela análise crítica das Técnicas Especiais de Investigação (TEI), tais como algoritmos para análise de *Big Data*, o cercamento digital (*geofencing*), a varredura de torres (*tower dumps*) e a busca generalizada em buscadores online. Contrapondo-se à jurisprudência que valida varreduras coletivas sem individualização prévia, a tese testa a hipótese de inclusão do princípio da finalidade no dispositivo processual como critério limitador dogmático.

1.1. Recorte temático e pergunta de pesquisa

É pressuposto do discurso científico a impossibilidade de se falar sobre tudo ou o todo. Naturalmente, as pesquisas estabelecem seus recortes [9], que devem ser orientados para a resposta ao problema de pesquisa. Em outras palavras, todo discurso científico reduz a complexidade dos

[9] O recorte é uma categoria epistemológica indispensável às questões teóricas e linguística, segundo Orlandi: *"*é preciso determinar, através dos recortes, como as relações textuais são representadas, e essa representação não será, certamente, uma extensão da sintaxe da frase". (ORLANDI, E. Recortar ou segmentar? In: Linguística: Questões e Controvérsias. Série Estudos. Uberaba: Faculdades Integradas de Uberaba, 1984. p. 11-25.)

fenômenos estudados, e quanto menor for essa redução, melhor o resultado.

A inquietação com o tema da pesquisa surgiu das reflexões sobre o uso de algoritmos de mineração de textos em grandes volumes informacionais armazenados em suportes eletrônicos, em um curso organizado na Universidade de Brasília em 2016. Naquela oportunidade, o exemplo era a possibilidade de usar uma base de dados de uma multinacional, obtida no contexto de crimes contra a administração pública, para rodar algoritmos de mineração de texto com parâmetro de busca para crimes sexuais. A pergunta feita provocativamente na época era se essa ação do investigador estaria limitada pelas regras processuais penais, o que gerou debate entre o dever de punir e a desvinculação do ato investigativo em relação à apreensão realizada.

A primeira reflexão pessoal foi que a ação do investigador não poderia ser ilimitada para buscar elementos de informação sobre infrações penais, influenciada pela vinculação causal defendida teoricamente por Lopes Junior sobre as buscas e apreensões, especificamente sobre o encontro fortuito de provas durante buscas e apreensões[10].

Apesar de aquela provocação se situar no limiar do absurdo, ela não tem resposta peremptória pela racionalidade processual penal brasileira. Tal ausência é o fator motivador desta pesquisa. A partir dela, aprofundou-se no tema para amadurecê-lo, momento em que a proteção de dados no âmbito público surgiu, conjuntamente à teoria da prova, para aprofundar o estudo dessa hipótese.

Nesse contexto, a tese visa a responder: a racionalidade jurídico-processual brasileira é adequada para assegurar a licitude da aquisição, uso e reúso de dados pessoais no âmbito processual penal, em observância ao princípio da finalidade?

A hipótese de resposta é que a finalidade na aquisição, uso e reúso de dados pessoais tem conteúdo normativo para se opor frontalmente à teoria da prova penal majoritária aplicada ao digital, que analisa o potencial epistêmico dos elementos de informação estaticamente, desprezando-se o entorno correlacional para fazer inferências probatórias, a partir do *nomen iuris* dos dados pessoais como critério de hierarquização da proteção jurídica.

1.2. Marco teórico

[10] LOPES JUNIOR, Direito Processual Penal, 2020, p. 617-627

Conforme visto na primeira parte da introdução, o tema da pesquisa está situado no campo das ciências criminais, com foco na disciplina processual penal, com aplicação da garantia constitucional da autodeterminação informativa no âmbito público. Portanto, essa abordagem implica no estudo dos limites do poder de punir[11], que são impostos aos órgãos de persecução no cumprimento do dever legítimo de proteção de bens jurídicos tutelados penalmente. Tal limitação é projetada no principal objeto do processo penal, que é a pretensão acusatória[12], que se legitima na tutela jurisdicional racionalizada na prova penal, elemento indispensável à condenação.

No entanto, ainda que a prova penal seja o critério legitimador da condenação criminal, ela não é entendida na tese como a finalidade institucional do processo penal[13]. Essa afirmação pode ser lida como um afastamento do conceito de verdade como correspondência, que é muito presente na doutrina processual penal brasileira[14], que é utilizada e justificada por Badaró, tal como no trecho a seguir: "sendo o processo um mecanismo cognitivo, é preciso que as atividades processuais voltadas a investigação, admissão, produção, valoração da prova e a própria decisão final sejam, na máxima medida, possível, voltadas para a descoberta da verdade."[15]

O problema prático dessa visão é que a busca pela verdade se torna um fator sacralizante dos atos de processuais. Com efeito, o não reconhecimento da falibilidade da reconstrução dos fatos da passados pode levar à flexibilização de limites investigatórios na tentativa de cumprir lacunas, que são características intrínsecas a quaisquer métodos de investigação. Nessa linha, a verdade deve ser vista como o limite do processo, jamais como o objetivo. O produto da atividade processual não é verdade, mas "uma narrativa produzida pelo juiz"[16], marcada pela precariedade.

A reconstrução histórica do passado é sempre aquém da verdade. O processo penal é um dispositivo ritualizado de contenção do poder punitivo e redução de danos, cujo centro cognitivo

---

[11] Segundo Lopes Jr. (2020, p. 159), "[...] os princípios Constitucionais do Processo Penal são constitutivos das chamadas 'regras do jogo', ou do devido processo (*due process of law*), servindo, ao mesmo tempo, como mecanismos de limitação e legitimação do poder de punir. Pensamos o processo penal a partir da 'instrumentalidade constitucional', ou seja, um instrumento a serviço da máxima eficácia do sistema de garantias da Constituição e um caminho necessário para chegar-se a uma pena (ou não pena), permeado por regras que limitam o exercício do poder punitivo. Os princípios gozam de plena eficácia normativa, pois são verdadeiros normas (Bobbio)".

[12] LOPES JUNIOR, 2020, p. 72-75.

[13] GLOECKNER, Ricardo Jacobsen; KHALED JR., Salah H.; DIVAN, Gabriel. Verdade, processo penal e epistemologia: da pretensa fundamentação filosófica aos efeitos jurídicos e políticos da adoção de premissas racionalistas. Revista Brasileira de Ciências Criminais, São Paulo, v. 31, n. 199, nov./dez. 2023, p. 79.

[14] GLOECKNER; KHALED; DIVAN, 2023, p. 75.

[15] BADARÓ, Gustavo H. Editorial dossiê "Prova penal: fundamentos epistemológicos e jurídicos". Revista Brasileira de Direito Processual Penal, 2018, p. 50.

[16] COUTINHO, Jacinto Nelson de Miranda. Verdade e fake news. Revista Brasileira de Ciências Criminais, n. 198. 2023.

deve estar centrado nas garantias processuais derivadas da presunção de inocência[17]. A ideia de que a prova é buscada no processo transmite uma ideia de movimento que inexiste na situação processual, na medida que o passado que se pretende reconstruir já ocorreu, de modo que esse lugar de busca retira o poder judicial da imparcialidade, para a supressão das citadas lacunas.

Como se nota, a tese adere a posição de que o centro do processo não é a busca pela verdade. O centro cognitivo são as garantias processuais que decorrem da presunção de inocência, cuja preservação depende da observância aos limites impostos aos atos processuais, ou seja, a legalidade processual[18]. Tal assertiva, para os autores que não usam o conceito de verdade, sustenta a afirmação de que o processo penal é contraintuitivo, na medida em que oferece obstáculos à evidência. Para aqueles que trabalham com o conceito de epistemologia e verdade judicial no processo, a legalidade é um controle contra epistêmico de ingresso de elementos informativos[19].

Na síntese da discussão para a tese, a legalidade dos meios de prova ocupa posição central na dogmática penal, pois constitui garantia indispensável à preservação da presunção de inocência, cuja pretensão acusatória tende a questionar. Como dito, a depender da abordagem teórica adotada, esses limites podem parecer contraintuitivos, pois oferecem obstáculos à evidência, diante da ideia de reconstrução necessariamente precária do passado, ou podem funcionar como um limite contra epistêmico à noção de verdade como correspondência. O essencial com adoção da última é o reconhecimento de que o racionalismo não é subterfúgio válido para a superação de limites legais[20].

A era informacional reforça a exigência de reflexão sobre a verdade no processo, uma vez que o tratamento em massa de dados alimenta uma ideia de futuro, onde é possível se conhecer tudo e, consequentemente, reconstruir fidedignamente o passado em todas as hipóteses. A arte já entregou diversos exemplos disso, tais como a série brasileira *Onisciente* ou o clássico filme *Minority Report*. Entretanto, esse futuro só é possível em sociedades em que o direito ao devido processo, à privacidade e à autodeterminação informacional deem lugar a busca da verdade como

---

[17] GLOECKNER; KHALED; DIVAN, 2023, p. 101.
[18] GLOECKNER; KHALED; DIVAN, 2023, p. 101.
[19] A exemplo da obra de Geraldo Prado intitulada de Prova Penal e Sistemas de Controles Epistêmicos: a quebra da cadeia de custória das provas obtidas por métodos ocultos. (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.)
[20] Nessa linha, Gloeckner cita exemplos práticos: "Como síntese final, pode ser dito que uma teoria racionalista favorece o desaparecimento das regras de exclusão, em homenagem ao máximo rendimento epistêmico do processo. Regras que proíbem o ingresso de provas indiretas não se justificam diante da perspectiva de maximização da informação processual. A limitação da introdução do inquérito policial no processo penal seria uma atividade certamente contraepistêmica e não justificada a partir dessas correntes. Tampouco preclusões probatórias seriam bem-vindas pelos teóricos racionalistas." (GLOECKNER; KHALED; DIVAN, 2023, p. 101.)

objetivo central das atividades públicas, que é uma premissa com a qual a tese não trabalha.

Apesar dessas considerações, a tese utiliza a noção de potencial epistêmico em alguns momentos, comumente atrelada a autores que usam o conceito de verdade como correspondência[21], para qualificar situações jurídicas nas quais o conteúdo informacional de dispositivos ou bases de dados não é determinável previamente. Isso é feito porque a análise de dados de *big data* opera principalmente em correlação contextual de informações e não por causalidade científica, de modo que o produto da análise é sempre inferencial[22]. Assim, um algoritmo de mineração de palavras pode correlacionar informações que, para humanos, são desconectadas para inferir causalidade. Tal resultado pode ser científico, mas não necessariamente aproveitável ao direito.

O uso do conceito de potencial epistêmico visa à superação da visão estática da dogmática processual penal brasileira para descrever bancos de dados e dispositivos eletrônicos. Em termos de maturidade crítica, o sistema brasileiro ainda lida com os dados de entrada – os *inputs* – como quaisquer informações analógicas, desconsiderando o potencial correlacional com o entorno. Isso é visualizado na hierarquização da proteção aos dados pessoais pelo *nomen iuris* (cadastral, conteúdo etc.). O erro é precisamente apontado por Wachter e Mittelstadt: "non-sensitive data can reveal information about sensitive category attributes through linkage and inference"[23].

A depender do espaço amostral, metadados podem configurar intervenção informacional mais ampla que a análise mais isolada de dados de conteúdo[24]:

> […] The reality is that the metadata, when aggregated, is far more revealing than content data. Content data may reveal a fragment of an individual's life at a particular date and time, whereas the metadata collected, stored, analysed and disclosed about an individual can create a detailed map of an individual's personal life. For these reasons, big data, which incorporates content and metadata are very valuable to private and public agencies when aggregated and analysed.

Por isso, a tese adotou o princípio da finalidade probatória, como critério limitador a ser

---

[21] MATIDA, Janaina; HERDY, Rachel. As inferências probatórias: compromissos epistêmicos, normativos e interpretativos. Revista do Ministério Público do Estado do Rio de Janeiro, Rio de Janeiro, n. 73, p. 133-155, jul./set. 2019, p. 141-143.
[22] WACHTER, Sandra; MITTELSTADT, Brent. A right to reasonable inferences: re-thinking data protection law in the age of Big Data and AI. Columbia Business Law Review, [S. l.], n. 2, 2019, p. 497.
[23] WACHTER; MITTELSTADT, 2019, p. 564.
[24] AGUIAR, Thaís et al. Rastreabilidade, metadados e direitos fundamentais: nota técnica sobre o Projeto de Lei 2360/2020. São Paulo: Data Privacy Brasil, 2021, p. 161.

internalizado ao dispositivo processual penal[25]: se não é possível antever o resultado da análise automatizada, a busca inferencial deve se limitar a atos investigativos que guardem coerência com o motivo da coleta da informação. Como dito, a origem desse princípio está no direito à proteção de dados alemão[26], no qual se reconheceu que a utilização de informações pessoais deve guardar coerência com o motivo que justificou a sua coleta, permitindo controle pelo do titular.

No âmbito privado, o controle dessa utilização é exercido por meio do consentimento contratual do titular. Entretanto, essa lógica não se aplica aos atos processuais penais: não faz sentido falar em consentimento para meios de investigação invasivos[27]. Assim, o controle, que nas relações privadas, se realiza pelo consentimento, é substituído, no processo penal, pela reserva de lei[28]. Desse modo, a finalidade do uso da informação deve ser projetada em todas as fases do ciclo de vida dos dados pessoais no processo penal. A pergunta que poderia ser feita partir dessa afirmação é o porquê essa importação se justifica para o âmbito público.

A justificativa reside no fato que determinadas ações investigativas na era digital se assemelham mais ontologicamente ao tratamento de dados do que aos tradicionais atos de investigação. Essa contestação se evidencia, por exemplo, na pretensão de utilizar dados em massa – relativos a um número indeterminado de pessoas – para identificar autores, coautores e partícipes, bem como no acesso a bancos de dados públicos ou privados com alto volume, variedade, velocidade de dados pessoais. Tais características ampliam o potencial de desvio de finalidade da investigação, em níveis que a dogmática processual penal não alcança e não pode mais ignorar.

Ademais, esse recorte de disciplina processual penal retira sua fundamentação da teoria dos direitos fundamentais, especificamente dos deveres de abstenção do Estado em relação ao particular, que são descritos historicamente como direitos de primeira geração. Nesse sentido, Virgílio aponta que "as liberdades públicas(...) constituem a primeira geração de direitos

---

[25] GIACOMOLLI, Nereu José; EILBERG, Daniela Dora. Coleta e tratamento de dados na transformação tecnológica da investigação criminal. GALILEU - REVISTA DE DIREITO E ECONOMIA, Lisboa, v. 24, n. 1-2, jan./dez. 2023, p. 126-128.

[26] GRECO, Luís, 2018, p. 22.

[27] A respeito do âmbito público em geral: "A propósito, a aplicação das bases legais do legitimo interesse e do consentimento é bastante restrita quando se trata da atuação do poder público. Afirma-se que cabe à legislação estabelecer a ponderação entre as expectativas dos titulares e o interesse público, vez que o desenho legal deve, como se salientou outrora, se circunscrever ao exercício das competências legais ou ao cumprimento das obrigações legais inerentes ao serviço público, particularmente na seara da segurança, da inteligência e da persecução penal)". (SARLET, Ingo; SARLET, Gabrielle. *Separação informacional de poderes no Direito Constitucional brasileiro*. São Paulo: Associação Data Privacy Brasil, 2022, p. 44.)

[28] ESTELLITA, Heloisa. O RE 1.055.941: um pretexto para explorar alguns limites à transmissão, distribuição, comunicação, transferência e difusão de dados pessoais pelo COAF, 2022.

fundamentais e consistem nos direitos que garantem uma esfera de liberdade de atuação dos indivíduos contra as ingerências estatais"[29]. O outro lado da moeda da liberdade individual é a obrigação do Estado em se abster de condutas para violá-la desproporcionalmente[30].

No âmbito da dogmática constitucional-penal, Greco conceitua que os direitos fundamentais têm um objeto de proteção, que exigem que uma conduta estatal, que afete ou intervenha nesse âmbito, seja justificada[31]. Seguindo essa linha, o tema da tese está no âmbito de proteção do devido processo legal, à autodeterminação informacional e à privacidade, sendo que a intervenção que se pretende é a produção probatória com utilização de dados pessoais coletados por empresas e pelo estado na segurança pública para a investigação preliminar. A regra, portanto, é o dever de abstenção do Estado em relação a esse objeto.

A formulação teórica de Greco, que sucede à avaliação, é precisa: "toda intervenção em direito fundamental demanda uma justificação, e um componente necessário dessa justificação, seu pressuposto formal, é o atendimento da exigência de reserva de lei"[32], que, no Brasil, encontra fundamento no artigo 5º, II, da Constituição Federal. Nesse contexto, as normas que autorizam intervenções informacionais devem ser específicas e determinadas, ressalvadas as ações corriqueiras – bagatelares –, como a busca em fontes abertas sobre informações de pessoas suspeitas.[33]

Os critérios de validade da norma de autorização se sustentam em três pilares: previsão em lei que não atinja o núcleo do direito fundamental, proporcional (necessária, adequada, e proporcional em sentido estrito) e visar um fim legítimo[34]. Nesse particular, a teoria dos direitos fundamentais se alinha à defesa de que os meios de obtenção de prova invasivos sejam necessariamente típicos processualmente, que refuta a existência de poder geral de cautela no processo penal[35], e posiciona a autorização procedimental como critério constitucional.

---

[29] SILVA, Virgílio Afonso da. A evolução dos direitos fundamentais. Revista Latino-Americana de Estudos Constitucionais, [S. l.], n. 6, p. 541-558, 2005, p. 547.
[30] SILVA, 2005, p. 551.
[31] GRECO, Luís: "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, 2018, p. 32.
[32] GRECO, 2018, p. 36.
[33] GRECO, 2018, p. 39.
[34] GRECO, 2018, p. 41.
[35] LOPES JUNIOR, Aury. A (in)existência de poder geral de cautela no processo penal. Boletim IBCCrim, n. 203, out. 2009.

A conjugação dos argumentos acima leva à refutação, desde o primeiro momento, de que a investigação envolva uma ponderação entre o direito de punir do Estado e os direitos individuais dos réus ou suspeitos. Primeiro, não existe direito de punir[36], o Estado tem o dever/poder de punir, sendo que os direitos individuais funcionam exatamente como filtro a esse exercício. Nessa equação, dizer-se que há ponderação do interesse legítimo do Estado com garantias tem sempre como resultado a fragilização da última: intervenção sem autorização legal.

Por fim, essa interação entre a teoria das garantias fundamentais, o processo penal enquanto dispositivo de controle do poder de punir e a autodeterminação informacional está no cerne das posições teóricas desenvolvidas ao longo da tese. Naturalmente, esses elementos foram essenciais para a delimitação da pergunta e da hipótese de pesquisa.

[36] JR KHALED, Salah Hassan. "A idéia de jurisdição como poder (mais ou menos condicionado, dependendo do contexto histórico jurídico em questão) tem preponderado. No bojo desta noção de poder, no que se refere à jurisdição penal, está a idéia (acolhida por Carnelutti) de que o poder jurisdicional se conheça sob o nome de direito de punir, coincidindo o poder de punir e o poder de jurisdição penal" (2010. p. 65-66).

1. ARQUITETURA INFORMACIONAL

A arquitetura física de cidades, escolas, locais de trabalho e ambientes públicos em geral foi analisada por Foucault como expressão de dispositivos de controle característicos da sociedade disciplinar, concebidos pelo Estado moderno para vigiar coletividades e prevenir desvios comportamentais.[37]. Nesse contexto, pode-se dizer que o autor inaugura um debate sobre as racionalidades que orientam o espaço físico como um método relevante para entender as formas de vigilância adotados por governos, o qual pode ser projetado em diversas as quadras históricas.

As câmeras de segurança em locais públicos e privados, como condomínios fechados, passaram a fazer parte da paisagem brasileira a partir dos anos 80, primeiramente para funções de trânsito e, depois, para fins de segurança pública[38]. Atualmente, o uso é praticamente onipresente, discutindo-se, em algumas situações, a instalação em banheiros escolares[39]. Melgaço tem razão ao afirmar que essa "busca por segurança é muita das vezes uma busca pela diminuição e controle dos medos"[40], que gera uma racionalização da segurança pública com base em emoções, em que a vigilância constante por dispositivos informáticos é vista como um mal necessário.

Uma das dimensões dessa racionalização é a propaganda sobre as *smart cities*, que são defendidas publicamente como a resposta política adequada para lidar com os riscos das grandes cidades no Brasil e no mundo, a exemplo dos projetos implementados em São Paulo no ano de 2017 e no Rio de Janeiro em 2012[41]. Ainda que a efetividade dessas soluções seja questionável, a cidade inteligente funciona como uma performance de política pública, para a qual a percepção de atuação dos agentes estatais é mais importante que os resultados atingidos[42].

A *smart city* é precisamente um exemplo do que a tese denomina de arquitetura informacional, isto é, a instalação de dispositivos eletrônicos que captam dados digitais para processamento automatizado, justificados na finalidade legítima de segurança pública. Como se

---

[37] FOUCAULT, Michel. Microfísica do poder. Trad. e Org. de Roberto Machado. 13. ed. Rio de Janeiro: Graal, p. 291, 1998.
[38] MELGAÇO, Lucas. Estudantes sob controle: a racionalização do espaço escolar através do uso de câmeras de vigilância, 2012, p. 195.
[39] MELGAÇO, 2012, p. 202.
[40] MELGAÇO, 2012, p. 195.
[41] MELGAÇO, Lucas; VAN BRAKEL, Rosamunde. Smart Cities as Surveillance Theatre. Smart Cities as Surveillance Theatre. Surveillance & Society, 2021, p. 245-246.
[42] GARLAND, David. The Culture of Control: Crime and Social Order in Contemporary Society. Chicago, IL: University of Chicago Press, 2001.

verá adiante no texto, a criação dessa arquitetura deve observar diversas condicionantes jurídico-normativas, tendo em visto o potencial de atingimento a direitos fundamentais, que tende a não ser adequadamente observado pela racionalidade jurídica brasileira, permitindo-se a criação de repositórios de informação sem regras próprias para uso e reúso de dados pessoais.

Num segundo momento, a tese se dedica a investigar a transposição das informações desses repositórios para o processo penal, ou seja, como os dados coletados por arquiteturas informacionais são utilizados como fonte prova, que podem ter origem em soluções implementadas por agências estatais e por particulares. Antes disso, é necessário retomar algumas categorias criminológicas neste primeiro capítulo, que contribuem para com o entendimento sobre as racionalidades que dão origem vigilância digital, mais especificamente das ideias naturalizadoras de intervenções informacionais como soluções necessárias para a segurança pública.

Deve ser ressaltado que antes das modernas tecnologias da informação, o deslumbre com as possibilidades da capacidade computacional e suas técnicas já haviam levado a mudanças substanciais na forma de pensar as soluções de política criminal. Um exemplo que evidencia a afirmação é que os primeiros algoritmos implementados foram criticados por opositores da criminologia atuarial por serem enviesados por raça, por classe social, por credo religioso, isto é, apresentavam resultados ilícitos[43]. Exatamente o mesmo objeto das mais relevantes críticas acadêmicas sobre implementação de inteligência artificial pelo Estado.

Evidentemente, a escala, a velocidade, a variedade e qualidade no processamento de dados foram alteradas entre a análise dos primeiros algoritmos e o atual uso de inteligência artificial por agências estatais. Entretanto, a justificativa para implementá-los permaneceu semelhante, qual seja: a tecnologia permite que a coletividade seja controlada sem a necessidade de individualização das formas de controle, na medida em que os dispositivos de disciplina físicos foram substituídos por soluções informacionais[44]. Por essa razão, a tese se ancora na crítica à racionalidade implementada pela criminologia atuarial e da sociedade do controle porque o racional burocrático não se alterou.

Dieter conceitua que a política criminal atuarial se caracteriza por "diferentes discursos e técnicas em função de um só objetivo. A retórica do risco legitima o uso de instrumentos de cálculo

---

[43] FEELEY, Malcolm; SIMON, Jonathan. The New Penology: Notes on the Emerging Strategy of Corrections and Its Implications, p. 449-474, 1992.

[44] Nesse sentido, Deleuze afirma "deixamos para trás as sociedades disciplinares, [...] não somos mais isso"[44]. Assim, os dispositivos de disciplina (restrição física, horários rígidos etc.) foram substituídos por dispositivos de controle, que têm como principal característica a possibilidade de utilização de códigos e linguagens que tornam os indivíduos em divisíveis por seus dados.

atuarial para reorientação do sistema de justiça criminal, cujo fim imediato é o controle social de coletivos sociais, não de pessoas concretas"[45], a preocupação não está mais na causalidade entre o ilícito cometido e a proporcionalidade da punição a ser dada individualmente. Ao que parece, é uma lógica semelhante a que orienta o capitalismo dos dados, no qual o comportamento de consumo individual é menos importante do que a inferência sobre o consumo coletivo[46].

Esse racional criminológico se popularizou a partir da execução penal americana[47], passando a orientar a política criminal secundária, produzida por agências reguladoras, e é uma das bases utilizada por o Garland para definir a emergência de uma nova cultura do controle[48]. Tanto a cultura do controle quanto a criminologia atuarial apresentam fundamentos para interpretar as justificativas da implementação de tecnologias de monitoramento como condição *sine qua non* para soluções de política criminal, viabilizadas pelo aumento substancial da capacidade de processamento para realizar monitoramentos populacionais, justificados na prevenção ao risco[49].

Portanto, o risco permanece como a principal categoria de análise para as atuais soluções de política criminal, o que muda é o *locus* da projeção da predição, que recai atualmente na implementação de uma arquitetura informacional preditiva e, em alguns casos, automatizada. Logo, o Estado justifica a implementação de tecnologia para a finalidade de prevenir e predizer à criminalidade, por meio do processamento computacional, como condição imposta pela realidade, e não como uma escolha de política criminal. Essa forma de justificação esconde exatamente aquilo que deveria fundamentar: a legitimidade da intervenção informacional[50].

Sobre a sociedade do controle, Garland definiu-a com base em três elementos: i) a recodificação do direito penal do Estado de bem-estar social; ii) uma criminologia do controle; e iii) um estilo econômico de raciocínio[51]. A recodificação do direito penal do Estado de bem-estar

---

[45] DIETER, Maurício S. Política Criminal Atuarial: A Criminologia Do Fim Da História. 2012. 309 f. Tese (Doutorado em Direito do Estado) – Universidade Federal do Paraná, Curitiba, 2012.
[46] MAYER-SCHÖNBERGER, Viktor; RAMGE, Thomas. Reinventing Capitalism in the Age of Big Data, 2018.
[47] FEELEY; SIMON, 2006, p. 449-474.
[48] GARLAND, David. The Culture of Control: Crime and Social Order in Contemporary Society. Chicago: The University of Chicago Press, 2001, p. 175.
[49] Sobre o risco na modernidade, Beck aponta que a sociedade dos riscos é resultado da crescente automação da vida em direção a tornar a sociedade industrial cada vez mais obsoleta. Nesta nova fase, o conhecimento social, a economia pública e os riscos individuais escapam das formas de disciplina da era industrial.
[50] Esse ponto é central para a tese, na medida em que a autodeterminação informacional é uma garantia fundamental, cuja intervenção deve ocorrer por previsão legal. Isso significa que os particulares não podem ter os dados coletados ilimitadamente, mesmo que esse volume permita inferências estatísticas mais apuradas para a segurança pública. Em outras palavras, o cumprimento da finalidade legítima de segurança pública não pode ocorrer às expensas de garantias fundamentais de pessoas indeterminadas para que modelos atuarias funcionem adequadamente.
[51] GARLAND, 2001, p. 175.

colocou a reabilitação individual em segundo plano, se tornando mais punitivista e securitária, com tratamento rígido ao desviante e preocupação central na proteção da coletividade. O segundo se tornou mais silencioso, condicionado ao tipo de ofensa e ao risco do agente para a sociedade[52]. Por fim, o estilo econômico, para o autor, tem viés neoliberal, visando a gestão em termos de eficiência econômica e alocação adequada de recursos com foco no custo-benefício.

Além disso, o autor descreve que a cultura do controle tem duas formas de tratar a prevenção ao crime: a criminologia do outro e a criminologia da vida cotidiana. A criminologia do outro desumaniza os apenados e no defende o incremento da crueldade das penas, ou seja, o caráter retributivo da pena é menosprezado, e os criminosos são descritos publicamente como "'marginais', 'predadores', 'monstros sexuais', 'maus' ou 'malvados', membros de uma 'subclasse', cada um deles sendo o 'inimigo marcado', em uma cultura dominante que exalta os valores da família"[53].

Na Europa, a criminologia do outro apresenta um caráter de negação da modernidade, que reage às inúmeras falhas do modernismo penal e aos arranjos da sociedade moderna tardia, reafirma as práticas de lei e ordem a partir de padrões morais absolutos, protegidos pelo discurso da tradição e do bom senso[54]. O autor exemplifica essa lógica de pensamento na fala do Primeiro-Ministro Britânico John Major de que estava na hora de "condenar mais e entender menos"[55]. Ainda que se tenha passados quase trinta anos dessa afirmação, ela continua atual no ocidente.

Já as ideias de criminologia da vida cotidiana justificam a criminalidade com base na teoria da escolha racional, que é uma teoria da atividade de rotina, o crime como oportunidade e a prevenção da criminalidade situacional[56]. Para o autor, existe uma insistência na criminologia da vida cotidiana em afirmar que os criminosos fazem cálculos de utilidade – que realizam análises

---

[52] "In the course of these developments, both 'penal' and 'welfare' modalities have changed their meaning. The penal mode, as well as becoming more prominent, has become more punitive, more expressive, more security minded. Distinctively, the condemnation and hard treatment of offenders, and the protection of the public have been prioritized. The welfare mode, as well as becoming more muted, has become more conditional, more offence-centred, more risk conscious" (*Ibid.)*.

[53] GARLAND, 2001, p. 180.

[54] "Today's other emergent criminology – the criminology of the other – might properly be described as anti-modern in character. It reacts to the failures of penal modernism and to the social arrangements of late modern society by questioning that society's normative codes and seeking to transform the values upon which they are built." […] This criminology is decidedly anti-modern in its central themes: the upholding of order and authority, the assertion of absolute moral standards, the affirmation of tradition and common sense. It is also deeply illiberal in its assumption that certain criminals are 'simply wicked' and in this respect intrinsically different from the rest of us" (*Ibid.*, p. 184).

[55] *Ibid*., 2001, p. 18, "*to condemn more and to understand less*", tradução nossa.

[56] GARLAND, 1999, p. 64-65.

de custo e benefício – de suas ações. Nesse sentido, a argumentação evidencia a transposição de doutrinas econômicas, que prescrevem o comportamento de consumidores como maximizadores de utilidade, na lógico do como o "eu" agiria em determinadas situações.

A própria racionalidade do agente econômico como pilar da teoria neoclássica é debatível, sendo que, no mínimo, há pesquisas que apontam limites no referido paradigma. Como exemplo, o autor Richard Thaler ganhou o Prêmio Nobel da Economia em 2015 por pesquisas sobre economia comportamental, que desmistificam a ideia da existência de agentes econômicos racionais que medem suas atitudes por cálculos de utilidade diretos e relativos. Segundo ele, um cidadão de classe média americana não consegue escolher sequer o melhor plano de saúde para suas necessidades[57].

A conexão que Garland faz ao pensamento econômico na cultura do controle é contemporânea ao *law and economics*, de Gary Becker e Richard Posner, os quais obtiveram êxito em demonstrar que era possível a criação de modelos econômicos para analisar os mais diversos ramos do direito, recentemente utilizada como bastante marco teórico para alteração do direito brasileiro[58]. Contudo, essas análises desconectadas de discussões valorativas de cada área do conhecimento podem se demonstrar extremamente empobrecedoras, já que tem "pouca adequação com a racionalidade substantiva de fazer justiça"[59], uma vez que o foco não são as garantias fundamentais.

Neste contexto, Garland vê uma fuga do pensamento social para o econômico, mas, talvez, a forma mais apurada de análise seria identificar que os elementos centrais das teorias econômicas foram sendo transpostos às demais ciências sociais. Apesar desta divergência sutil de perspectiva, o autor apresenta uma descrição muito precisa do fenômeno[60].

> [...] Por racionalidade "econômica", não quero dizer simplesmente que as considerações da relação qualidade/preço e de coerção fiscal tornaram-se, hoje em dia, excessivamente determinantes, ao ponto de se explicitarem nos aspectos do discurso e da prática da repressão criminal — embora este seja certamente um traço característico da cena contemporânea. Quero, com isso, chamar a atenção para a dependência crescente para

[57] THALER, Richard H.; SUNSTEIN, Cass R. Nudge: Improving Decisions about Health, Wealth, and Happiness. New Haven: Yale University Press, p. 292-294, 2008.
[58] Art. 20 da Lei de Introdução às normas do Direito Brasileiro: "Nas esferas administrativa, controladora e judicial, não se decidirá com base em valores jurídicos abstratos sem que sejam consideradas as consequências práticas da decisão". *(*BRASIL. Decreto-Lei nº 4.657, de 4 de setembro de 1942. Lei de Introdução às normas do Direito brasileiro. Diário Oficial da União, Rio de Janeiro, RJ, 9 set. 1942, art. 20).
[59] GARLAND, 2001, p. 190, "*though its poor fit with the substantive rationality of 'doing justice*'", tradução nossa.
[60] GARLAND, 1999, p. 65.

> com uma linguagem analítica do risco, da racionalidade, da escolha, da probabilidade, da determinação de alvos, da oferta e da demanda de ocasiões — uma linguagem que transfere as formas "econômicas" de raciocínio e de cálculo para o campo da criminologia; para a importância crescente de objetivos como a compensação, o controle do custo e a redução dos danos; e, enfim, para o recurso crescente a tecnologias como o auditoria, o controle fiscal, a competição de mercado e a gestão restrita à tomada de decisão do controle penal.

Como se pode ver, a consequência dessa racionalidade econômica é que o crime passou a ser debatido pela lógica de redução das oportunidades para sua ocorrência. Assim, "[a] nova abordagem dedica-se a substituir o dinheiro vivo por cartões de crédito, embutir travas nas colunas de direção dos automóveis, contratar vigias nos estacionamentos e colocar circuitos internos de televisão nos shoppings"[61]. O objetivo dos adeptos a essa corrente é o fomento à criação de engenharias situacionais para a prevenção ao crime, afastando-se da discussão do problema social, que era uma característica da criminologia do Estado de bem-estar social europeu.

É importante ressaltar que criação de engenharias situacionais é a lógica mais facilmente privatizável, de modo que cada particular pode criar pequenas soluções para resolver problemas cotidianos. Dito de outra forma, traz-se o particular para o âmbito da solução da criminalidade para além do Estado. Assim, abre-se a possibilidade de endereçar as políticas criminais às organizações, às instituições e aos indivíduos da sociedade civil[62], que é marcador do surgimento do terceiro setor, para além das tradicionais agências de criminalização, é formado por experts em predição e análise de risco[63].

Quanto maior o risco, mais intensa é a defesa da necessidade de metrificá-lo para orientar decisões econômicas e políticas[64]. Assim, o risco, a eficiência, a probabilidade e a estatística passam a ser manifestações de um giro epistemológico, na qual a impossibilidade de gerir múltiplas variáveis – aspectos não são reconhecidos pelos experts – geram mais controle com o discurso da predição. Neste sentido, todo setor que lide com muitos riscos deve implementar soluções

---

[61] GARLAND, 1999, p. 66.
[62] GARLAND, 1999, p. 66.
[63] O primeiro mercado a aderi-lo foi o setor de seguros, que desenvolveu formas de analisar a possibilidade do lucro e a probabilidade de ocorrências de gravames. A utilização dessa forma de racionalidade economicista no pensamento criminológico começa no terceiro setor, particulares que exercem estratégias de política criminal por terceirização estatal, e retornam as discussões públicas.
[64] "[...] The crime control field – from crime prevention work and policing to the prison regime and the practice of parole – has become sutured with technologies of audit, fiscal control, measured performance, and cost-benefit evaluation. The old language of social causation has been displaced by a new lexicon (of 'rick factors', 'incentive pricing') that translates economic forms of calculation into the criminological field" (*Ibid.*, p. 188-189).

preditivas para que, caso ocorra o gravame, possa-se debater a responsabilização por assunção ilegal desses riscos.

Os deveres jurídicos criados pelo Estado desenvolveram o terceiro setor, que passou a auxiliar na política criminal preventiva, por meio das estratégias situacionais, a exemplo do registro de movimentações financeiras em espécie por bancos e outros. Em sequência, o Estado passa a utilizar do mesmo padrão para organizar a burocracia informacional, passando a ser um agente de coleta de informações em massa para exercer as funções legítimas de segurança pública e persecução penal, servindo-se da aquisição de tecnologia privada para tanto, como se verá adiante.

No que se relaciona com a atuação como o terceiro setor, as empresas criam arquiteturas informacionais como condição regulatória para atuar em determinados âmbitos econômicos, isto é, a coleta de dados pessoais é realizada em função da política criminal. A esse fenômeno, soma-se a alteração nas relações de produção, para as quais os dados são ativos econômicos, o que comumente se denomina economia movida a dados[65]; nesse particular, as arquiteturas são criadas por interesses próprios e, eventualmente, interessam ao Estado para a função de persecução penal, mas não existem em razão da política criminal.

A cultura do controle manifesta-se tanto na criminologia do outro quanto na criminologia da vida cotidiana, para dar respostas à criminalidade. Apesar das diferenças que as distinguem, ambas se estruturam em três pilares: (i) foco no controle preventivo do crime; (ii) metrificação estatística dos índices de criminalidade; (iii) implementação de medidas de esvaziamento das políticas criminais de bem-estar social. De forma geral, a descrição da cultura do controle é muito precisa, e permite compreender o lugar dos particulares na prevenção ao crime.

Discutir formas de racionalidade, remontando as críticas ao pensamento atuarial, e a Garland, marcado pela influência de Foucault, objetiva a revisitação de categorias de pensamento que já não recebem a devida atenção. Esse percurso serve de base para a discussão da arquitetura informacional do disponível ao Estado, estudado em regra como um ente despersonificado de ideologia, implementador de soluções que criam riscos, devendo ser regulado. Tal perspectiva, porém, tende a naturalizar escolhas racionais como alteração objetiva de paradigma tecnológico, o que pode é muito prejudicial para um sistema de garantias fundamentais.

Nesse movimento, as próprias pesquisas acadêmicas passam a discutir as novas tecnologias

---

[65] SRNICEK, Nick. Platform capitalism, 2017, p. 39.

e se afastam das razões que justificam a vigilância estatal e empresarial, ainda que a última não seja o objeto principal da tese. As perguntas de pesquisa passam a discutir "como" as tecnologias devem ser reguladas, e não mais se devem ser utilizadas em primeiro momento, como se o monitoramento de populações fosse só mais uma fase de evolução tecnológica, como se a eventual proibição estivesse alheia ao debate democrático.

Como já articulado, lógica atuarial na política criminal se capilarizou a partir da execução penal americana. Posteriormente, a ideia se desloca para o eixo dos agentes secundários de repressão, inclusive com a criação de agências governamentais com este objeto precípuo. Contemporaneamente, o desafio passou a ser controlar o uso de medidas invasivas pelos agentes secundários de criminalização, já que seu uso é tão normalizado que parece ser só mais uma etapa de melhoramento da burocracia, que dispensaria debate democrático, cujo argumento justificador é a eficiência estatal.

Não há possibilidade de predição de criminalidade isenta de vieses, uma vez que a própria definição de infração penal já decorre de escolhas políticas. As modernas tecnologias da informação apenas ampliam os desafios que os primeiros algoritmos computacionais, aplicados às ciências sociais para fenômenos multivariados, já evidenciavam. O deslumbre pelo aumento da capacidade computacional cria uma falsa promessa de panaceia e, nesse movimento, desloca ou neutraliza o espaço de deliberação democrática sobre a legitimidade da arquitetura informacional para vigilância de populações inteiras. Por isso, a tese não se vincula a essa racionalidade, que trata o sujeito de garantias fundamentais como objeto de política criminal informacional.

O produto dessa racionalidade é uma arquitetura informacional que possui três camadas de atuação: i) os dispositivos informacionais implementados como política de segurança pública por agências estatais, ii) as bases de informação formadas pelo terceiro setor que opera em segmentos sujeitos à regulação econômica e; iii) o acesso, pelo processo penal, à arquitetura informacional das empresas de tecnologia. Cada uma dessas camadas recebe um tratamento jurídico diferente, conforme será extensamente abordado na tese, mas em termos de arquitetura permite que as agências de persecução façam intervenções informacionais a nível individual e coletivo.

A primeira camada de arquitetura é instalada pelo Estado, a exemplo das câmeras de segurança para vigilância em tempo real de massas populacionais, conjugada com processamento automatizado para identificação de padrões e riscos. Como visto anteriormente, a *smart city* é o exemplo ideal da racionalidade atuarial aplicada às cidades brasileiras, integrando-se a diversos

sistemas como bilhetagens de transporte públicos, *cookies* em sites públicos, entre outros, para realizar vigilância preventiva e preditiva de populações inteiras. Geralmente, o ingresso dessas informações na persecução penal ocorre por transferência de dados entre órgãos.

Na mesma linha, a segunda camada é criada por dever legal, empresas recolhem informações por determinação prévia, que geralmente ingressam na persecução por comunicação espontânea ou provocação. É nessa fase que a estratégia de retenção de metadados de conexão da política brasileira opera seus principais efeitos, na medida que, mesmo sem critérios de inteligência, as informações de tráfego de todos os usuários de internet são armazenadas por prazos definidos legalmente. Assim, a consequência prática é a criação de vastos repositórios informacionais para a eventualidade de que sejam úteis para processos cíveis e criminais.

A terceira camada possibilita que toda a arquitetura informacional criada para fins econômicos por empresas sejam objeto da persecução criminal. Nesse contexto, a vigilância estatal e privada se comunica e tudo que foi produzido para gerar valor econômico pode vir a ser objeto probatório em ações penais. Os exemplos são variados e contemplam desde metadados de localização de um relógio inteligente aos dados de conteúdo armazenados em nuvem, em suma, não existe uma separação legal absoluta entre informação coletada privadamente, com a consequente impossibilidade que seu uso venha a ser feito na persecução penal.

Por fim, os tópicos seguintes traçam critérios gerais para a implementação da arquitetura informacional estatal, que perpassa a decisão de política criminal e avança aos critérios para a escolha de tecnologias da informação a serem implementadas. No mesmo sentido, analisa-se os deveres legais impostos aos setores regulados e aos agentes econômicos de forma geral. Para ambas, o enfoque é feito em relação às técnicas que intituladas de *big data*, na medida em que se configuram complexamente com etapas de funcionamento, na medida que configuram intervenções informacionais mais graves, da perspectiva das garantias fundamentais.

1.1. Política criminal informacional: a decisão de implementar tecnologias

O crime não é um dado pré-existente. O objeto da persecução penal é decidido

politicamente por Estados que, na modernidade[66], buscam a legitimidade das restrições penais por ideais liberais. A afirmação não significa que a categoria crime seja uma abstração absoluta, mas que as tipificações penais não tendem a ser óbvias como a proibição do homicídio; em um Estado complexo, a apropriação de uma linha de crédito pública, com finalidade específica, para fim diverso pode configurar infração penal, um claro espaço da escolha de política criminal[67].

O Estado que fomenta determinada política pública, potencialmente subsidiada, também positiva a antinormatividade de utilizar-se do recurso para finalidade não referida inicialmente. O exemplo é para demonstrar que há espaços de decisão de política criminal mais complexos que as infrações penais do direito penal clássico. Ademais, o Estado moderno é autolimitado, na medida em que se constitui criando limites aos próprios poderes, a reserva de lei para tipificar conduta é um deles e, o eventual excesso, pode vir a ser revisitado por controle de constitucionalidade.

Naturalmente, o Estado não existe no vácuo, sendo condicionado por seu tempo histórico e pelas escolhas racionais que dele decorrem. Em termos mais amplos, a mudança de paradigma sociológico altera a forma de organização da burocracia jurídico-institucional[68]. Trata-se de uma análise estruturalista à luz das categorias weberianas de dominação. Essa categoria sociológica permite compreender que a revolução das novas tecnologias da informação[69] transforma o Estado e influencia suas respostas a novos problemas, como a tipificação de condutas enquanto decisão de política criminal.

Novas tipificações são a epiderme dessas mudanças. A tendência passa a ser o Estado-informacional, que desenvolve e implementa tecnologia, pública ou privada, e exerce poder por meio do controle da informação[70], assim como as grandes empresas de tecnologia. Nesse sentido,

---

[66] HEGEL, Georg F. Wilhelm. O princípio do mundo moderno em geral é a liberdade da subjetividade. In: HABERMAS, Jürgen. *O Discurso filosófico da Modernidade*. Trad. Ana Maria Bernardo et al. Lisboa: Dom Quixote, p. 27, 1991.

[67] Por exemplo, o art. 20 da lei nº 7.492/1986 (BRASIL. Lei nº 7.492, de 16 de junho de 1986. Define os crimes contra o sistema financeiro nacional, e dá outras providências. *Diário Oficial da União*, Brasília, DF, 18 jun. 1986. Art. 20.)

[68] Esse novo tipo de Estado (moderno), com uma administração impessoal e racional e no qual a burocracia (funcionalismo militar e civil) é capaz de realizar tarefas amplas e complexas, tendo em vista a manutenção da ordem pública, concentraria os recursos políticos necessários para exercer o monopólio legítimo da coação física. (BUGIATO, Caio; TRINDADE, Thiago. O Estado nas Relações Internacionais. Rio de Janeiro: Revista Oikos, v. 16, n. 3, p. 40-42, 2017.)

[69] "Meu ponto de partida, e não estou sozinho nesta conjetura, é que no final do século XX estamos vivendo um desses raros intervalos na história. Um intervalo cuja característica é a transformação de nossa "cultura material" pelos mecanismos de um novo paradigma tecnológico que se organiza em torno da tecnologia da informação uma referência sobre isso"(CASTELLS, Manuel. A sociedade em rede. São Paulo: Paz e Terra, p. 49, 1999.)

[70] BRAMAN, Sandra. Change of State: Information, Policy, and Power. Cambridge, Mass.: The MIT Press, 2006. p. 10.

a burocracia cria e gere bancos de dados para cumprir funções legítimas – saúde, segurança pública, persecução penal etc. – tornando-se um grande agente de coleta, uso e transmissão de dados para finalidades legalmente definidas. Esse movimento de mudança informacional não é isento de tensões, já que ele recai necessariamente sobre garantias fundamentais.

O conflito que se apresenta consiste no fato de que as finalidades legítimas do Estado são alcançadas mediante o atingimento de garantias constitucionais dos particulares, tais como a inviolabilidade do domicílio, o sigilo de dados e comunicações, proteção contra buscas pessoais e a autonomia informacional. Frisa-se que a questão não reside em ponderar abstratamente poderes/deveres do Estado em relação a garantias individuais, mas sim em verificar a legitimação da medida em abstrato e, posteriormente, sua adequação fática a casos concretos.

É por isso que principal garantia cidadã é que as restrições a direitos fundamentais possuam fundamento legal. Assim, as normas autorizadoras, que atingem esses direitos, têm duplo conteúdo[71]: de um lado, asseguram a garantia geral de abstenção do Estado; de outro, autorizam a limitação do direito, desde que respeitado o seu núcleo essencial. O fundamento da garantia de abstenção encontra-se no art. 5º, II, da Constituição, que consagra a reserva legal em sentido amplo, e outras específicas encontradas em expressões como "nos termos da lei"[72] ou "nas hipóteses e na forma que a lei estabelecer".[73]

Esse é o caso do sigilo de correspondência, telegráfico e telefônico, para os quais a Constituição exige decisão judicial, na forma que a lei estabelecer. Desse modo, esses atos de prova invasivos exigem dispositivo legal autorizador, uma vez que seus levantamentos são a exceção constitucional, a regra é, como dito, a abstenção em relação a eles – o sigilo. Em outras palavras, o constituinte determinou qual política criminal deveria ser implementada infraconstitucionalmente, por lei proporcional e adequada, para que a garantia constitucional ao sigilo pudesse ser excepcionada.

O mesmo raciocínio aplica-se à autodeterminação informativa[74], de modo que todas as camadas de intervenção informacional invasiva com dados pessoais para fins de persecução penal devem estar amparadas por norma autorizadora. Antes da persecução individualizada, a referida

---

[71] MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. Curso de Direito Constitucional. 7ª ed. São Paulo: Saraiva, 2012, p. 291-292.
[72] BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, art. 5º, VI e XV.
[73] *Ibid.,* art. 5º, XIII.
[74] *Ibid*., art. 5º, LXXIX.

garantia fundamental determina como a burocracia jurídico-institucional deve ser organizada para o cumprimento das funções legais relativas ao uso de dados abstratamente, de forma a não exceder os limites da decisão política, que, inclusive, podem ser objeto de controle já nessa fase.

Especificamente sobre separação informacional de funções, Sarlet e Sarlet afirmam que ela é consequência constitucional da separação de poderes[75]:

> [...] a separação informacional de poderes consiste em uma ressignificação, tanto lógica quanto necessária, da semântica do princípio da divisão de poderes (artigo 2º CF) à luz do constitucionalismo digital, tendo em vista o atual estado de compartilhamento dos dados em poder do Estado brasileiro que, como se verá, implica uma separação nítida entre as diversas áreas de atuação estatal sob pena de descumprimento de um preceito fundamental e, consequentemente, uma violação das exigências do Estado Democrático de Direito.

Consequentemente, as decisões administrativas somente são lícitas se se conformarem a estrutura burocrática às finalidades públicas definidas constitucionalmente. No âmbito do Estado-informacional, a formação de bancos de dados, as aquisições de dispositivos informáticos, soluções, aplicativos, contratação de prestadores de serviço, depende da aderência às decisões de política criminal, sem espaços para voluntarismos setoriais. Em outras palavras, a decisão de implementação política criminal informacional é transversal na organização burocrática.

Em que pese a força e obviedade da argumentação, ela não encontra respaldo prático nas ações do governo brasileiro, que, por exemplo, iniciou pregão eletrônico para a compra de dispositivo de invasão zero-clique em 2021, suspenso liminarmente pelo TCU, porém autorizado com cumprimento de condições em 2022[76]. O objeto era a compra de tecnologia de invasão de dispositivos eletrônicos, tal como a solução *Pegasus*, oferecida pela empresa *NSO group*, capaz de controlar de câmeras e microfones remotamente, sem a necessidade *click bait*[77]. Esqueceu-se, entretanto, de um detalhe: não há autorização legal para uso desse tipo de tecnologia, logo qual seria o motivo legitimador da compra dessa tecnologia.

Diante da repercussão midiática negativa, o *NSO group* se retirou do processo licitatório, de modo que o *Pegasus* não chegou a ser comprado. Entretanto, a licitação foi concluída com a

---

[75] SARLET, Ingo Wolfgang; SALES SARLET, Gabrielle. Separação informacional de poderes no direito constitucional brasileiro. São Paulo: Associação Data Privacy Brasil de Pesquisa, p. 27, 2022.
[76] Pregão eletrônico nº 03/2021 do Ministério da Justiça e da Segurança Pública, suspenso pelo acórdão n. 2.678/2012-TCU, em plenário. Decisão definitiva no acórdão 1331/2022 no TC 014.760/2021-5.
[77] A legalidade desse tipo de tecnologia está sendo debatido no STF na ADPF nº 1143.

compra de tecnologia que contém funcionalidades semelhantes, produzida pela empresa *Harpia Tech*. Como se pode ver, a inexistência de previsão legal para o uso de *spyware* não impediu que o Ministério da Justiça e Segurança Pública conseguisse autorização para a compra dessa solução, podendo-se presumir, com certo grau de certeza, que haverá uso sem permissivo legal.

A ausência de autorização não é inércia, podendo ser a própria opção legislativa, já que os Estados podem optar por refutar a utilização de técnicas investigativas em razão de riscos. Ademais, o direito penal não é propriamente âmbito da regulamentação. Esse conceito é aplicável limitadamente ao processo penal, pois aquilo que não é objeto de lei autorizadora, e afeta direitos fundamentais, está proibido[78]. O ato de regular pressupõe que a atividade seja lícita em si, discutindo-se como fazê-lo, já os atos de prova e de investigação, devem ser tipificados, tendo em vista que é abstenção é a regra constitucional.

Portanto, mais amplamente, a implementação de medidas tecnológicas que atinjam a autodeterminação informacional deve ser prevista em lei, para que se opere o duplo efeito constitucional esperado das normas de abstenção. A teses sustenta que o primeiro critério de validade material é a verificação de sua adequação legal, que analisa o objeto a medida em relação ao direito positivado e constitucional. O segundo critério é a adequação funcional, em que se analisa se o dispositivo ou aplicativo tecnológico é apto a cumprir a finalidade legal.

Em outras palavras, a funcionalidade das soluções constitui um critério para verificar a adequação legal da política criminal informacional, especialmente no que diz respeito ao processo legislativo e à organização administrativa do Estado. Trata-se, portanto, de um parâmetro aplicável às medidas ainda em fase de debate e destinadas à implementação futura. Essa conceituação possibilita identificar o cumprimento dos critérios pertinentes a cada fase de implementação da política informacional, bem como os contrapesos legais destinados a seu debate, ambas são antecedentes à persecução penal.

A primeira fase deve analisar o objeto da medida. Por exemplo, Greco e Gleizer perguntaram se a infiltração online era autorizada pelo ordenamento brasileiro: a resposta foi

---

[78] GRECO, Luís: "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, p. 40, 2018.

negativa[79]. Diante dela, eles poderiam ter se perguntado se ela poderia ser positivada, debatendo os critérios para tanto. Esse debate é de política criminal informacional, inserido na fase de adequação legal. Mendes, por outro lado, pesquisou se a utilização de *malware* como dispositivo de invasão é adequado funcionalmente com foco na obrigatoriedade da cadeia de custódia[80], isto é, se a funcionalidade técnica permite o cumprimento do referido requisito legal.

Esse ponto é relevante porque os trabalhos sobre provas digitais[81], proteção de dados, uso de tecnologias invasivas, inteligência artificial[82] e cooperação internacional[83], partem dos institutos probatórios das ciências criminais, tais como meios de prova, valoração, cadeia de custódia, para debater as consequências legais de suas inobservâncias. A discussões são pertinentes, mas antes da coleta de dados, a burocracia informacional é organizada por interesses de política criminal, definindo-se a arquitetura de dados disponíveis para a persecução penal futura. Até porque o contraditório na ação penal não terá por objeto discutir o critério utilizado para a compra de uma tecnologia, utilizada para na produção probatória.

A estrutura de dados disponíveis para as agências de investigação também deve se adequar legal e funcionalmente, configurando-se como primeiro lugar de debate da tese. Veja-se, portanto, que falar em adequação legal é mais amplo que tratar dos institutos de processuais e penais, requer análise interdisciplinar com outros campos de estudo, identificando-se riscos à vida privada, à isonomia, à privacidade, à proteção de dados, ao devido processo, os quais influenciam os limites a serem estabelecidos à arquitetura de dados disponível ao Estado-informacional.

Por fim, a prescrição de critérios adicionais à política criminal relacionada intervenções informacionais é um contraponto à racionalidade automatizada e atuarial, criticada anteriormente, para lidar com as alterações de arquitetura informacional que possibilitam intervenções informacionais coletivas, que vai além da discussão sobre novos tipos penais. Nesse sentido, o

---

[79] GLOECKNER, Ricardo Jacobsen. A (in)admissibilidade do interrogatório por videoconferência: a necessária releitura a partir da garantia da presença física e da revalorização do contato pessoal. Revista Brasileira de Direito Processual Penal, Porto Alegre, v. 5, n. 3, p. 1215-1250, 2019.

[80] MENDES, Carlos Hélder Carvalho Furtado. Malware do Estado e Processo Penal: a proteção de dados informáticos face à infiltração por software na investigação criminal. 218 f. Dissertação de Mestrado - Escola de Direito, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2018.

[81] VAZ, Denise Provasi. Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório. 2012. Tese (Doutorado em Direito Processual) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2012.

[82] GLOECKNER, p. 1215-1250, 2019.

[83] DANIELLE, Marcello. La prova digitale nel processo penale. Rivista di Diritto Processuale. v. 66, n. 2, mar/abr. 2011, p. 283-298.

próximo tópico aprofunda de que forma o processo legislativo deve ser alterado para que as decisões sobre a arquitetura informacional sejam bem-informadas, para as quais as categorias de adequação legal e funcional exercem a função de aprofundar o debate e permitir controle da atuação legislativa, especialmente porque o conhecimento técnico não exigido dos juristas.

1.2. Validade material da arquitetura informacional do Estado

A arquitetura de dados do Estado depende de lei para ser criada, tanto sob a perspectiva técnica quanto jurídica, uma vez que a aquisição de tecnologias para finalidades não definidas em lei é ilícita. Sem essa estrutura, a existência de tecnologias de vigilância ou de quaisquer outras intervenções informacionais relevantes não é possível ou, pelo menos, não deveria ser. Portanto, a análise de como a arquitetura informacional é criada e modificada é imprescindível para a compreensão dos condicionantes jurídico-normativos que lhe são aplicáveis.

A autora belga, Élise Degrave, defende a necessidade de que a implementação de algoritmos que processam dados pessoais passe por um teste de impacto de legalidade, em analogia aos procedimentos para certificação de segurança em veículos. Segundo a autora, o teste deve ocorrer em três etapas[84]: i) objetivo determinado e legítimo, ii) lei clara e previsível e, iii) proporcionalidade (equilíbrio no uso dos meios necessários à consecução da finalidade, proporcionalidade em sentido estrito da utilização e dados necessários, que estão englobados pelo conceito de minimização).

Não se trata, contudo, de abordar somente a mera legalidade formal, ou seja, a existência de lei que decorra de processo legislativo. Ao contrário, partindo do pressuposto de que o conhecimento técnico não é exigido do legislador, tampouco dos juristas, os riscos relativos a cada tipo de processamento pretendido devem encontrar regramento no processo legislativo para identificá-los e publicizá-los adequadamente. No plano da validade material da legislação, é incontornável que a arquitetura observe critérios legais, convencionais e constitucionais.

Em fase posterior à autorização legal, a adequação funcional das tecnologias da informação implementadas pelas agências estatais também deve ser analisada. Isso significa que o próprio produto tecnológico é objeto de escrutínio jurídico, na medida em que, caso o funcionamento exceda os limites do ordenamento jurídico, seu uso será ilícito.

---

[84] DEGRAVE, Élise. L'Etat numériques et les droits humains. Ed. Académie Royale de Belgique, 2024, p. 51-54.

Um bom ponto de partida para orientar o debate sobre a arquitetura informacional é tipo de dado pessoal que se pretende usar e para qual finalidade. Esse recorte é necessário porque as tecnologias da informação são muito amplas, podendo englobar até o uso de computadores pelas agências estatais. Logicamente, esse uso instrumental não é de interesse da tese que, como dito, se dedica às formas de uso que permitem o monitoramento individualizado e coletivo de particulares, e sua influência na produção probatória na persecução penal.

A partir da análise do tipo de dado que se pretende coletar e usar para fins penais, especialmente as informações sensíveis e/ou as sigilosas, prescreve-se a adequação do processo legislativo retrospectivamente, isto é, a legitimidade da intervenção informacional (coleta por estruturas físicas, deveres de retenção, entre outros). Num segundo momento, deve-se abordar em concreto a adequação funcional das tecnologias em relação ao permissivo legal. Em outras palavras, a arquitetura informacional deve ser válida, tanto formal quanto materialmente, sendo que ambas possuem aspectos próprios a serem observados, ainda não positivados no Brasil.

As informações sigilosas já estão positivadas na legislação penal e constitucional. Aliás, Abreu tem razão ao afirmar que o direito dos sigilos é bem-reconhecido na construção jurisprudencial do STF, mas deve ser expandido para abranger proteção jurídica da informação que não é necessariamente sigilosa[85]. Por outro lado, não há definição legal para os dados sensíveis para fins de persecução penal, mas por coerência sistêmica, é possível utilizar o conceito trazido no art. 5º, II, da Lei Geral de Proteção de Dados (LGPD)[86], em suma, informações sobre raça, religião, posicionamento político, sindicalização, relativos à saúde, genético e biométrico.

A política criminal informacional deve considerar o conteúdo normativo da proteção de dados, na medida que as intervenções informacionais têm potencial de restringir direitos já identificados por esse ramo do direito. Devido ao seu caráter principiológico, ainda que não positivado expressamente, a governança de dados é um dos condicionantes jurídico-normativo que orientam e limitam as escolhas penais, desempenhando um papel análogo ao clássico debate sobre a legitimidade do bem jurídico tutelado pela norma penal[87]; não basta ser crime, deve proteger bem

---

[85] ABREU, Jacqueline de Souza. Comunicação de dados, não dados em si: origens e problemas do atual paradigma de proteção constitucional do sigilo de dados. Revista de Investigações Constitucionais, Curitiba, vol. 11, n. 1, p. 6, 2024.
[86] II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
[87] GRECO, Luís. Modernização do direito penal, bens jurídicos coletivos e crimes de perigo abstrato. Rio de Janeiro: Lumen Juris, 2011.

jurídico legítimo.

Portanto, a não observância aos limites à coleta, processamento e transmissão de dados são razões para invalidação de atos jurídicos já realizados e, pela mesma razão, devem orientar previamente decisões de política criminal. Deve-se notar, entretanto, que esse fenômeno ainda não é observado no Brasil, uma vez que inexiste normativa específica para o processo legislativo que crie ou altere a infraestrutura informacional do Estado. No mesmo sentido, também não há histórico de precedentes jurisprudenciais em matéria penal que tenha aplicado os princípios da proteção de dados para debater excesso de coleta por agências de persecução.

Para o âmbito cível, o STF já aplicou esse racional, especificamente na ADPF 685/DF, e deu interpretação conforme ao decreto 10.046/2019 sobre a transferência de dados para a ABIN. Nesse julgamento, identificou-se, entre outros atos administrativos, o Termo de Autorização n. 7 do DENATRAN (Departamento Nacional de Trânsito) que permitia que a ABIN acessasse os dados de CNH (Carteira Nacional de Habilitação) de todos os condutores registrados no país (76 milhões pessoas), cujo armazenamento fica a cargo do SERPRO. Talvez em razão da má repercussão pública, o termo foi revogado alguns dias antes do início julgamento, o que, logicamente, impediu eventual anulação judicial por perda de objeto.

O limite imposto pelo STF é precisamente um exemplo de controle de arquitetura informacional. Naquele julgamento, a atuação foi bem justificada, os dados de todas as CNHs brasileiras não podem integrar a base de dados que a ABIN utiliza para a realização de suas funções legais. Não é somente mais um documento que permite a identificação civil e confere licença para condução; há particularidades a serem observadas como condição à transmissão, por exemplo, as restrições de saúde que influenciam na condução de veículos são registradas nele, dados que, pela legislação são de natureza sensível, e o acesso deve ter finalidade específica.

No contexto do direito da União Europeia, o Tribunal de Justiça da União Europeia (TJUE) invalidou a Diretiva 2006/24/CE, que estabelecia a retenção de dados de tráfego e de navegação pelo setor de comunicação eletrônicas acessíveis ao público, por inadequação aos direitos à privacidade e à proteção de dados, previstos no direito primário do bloco[88]. No mesmo sentido, o TJUE declarou a incompatibilidade de uma lei sueca que criava o dever de retenção de dados de

[88] UNIÃO EUROPEIA. Tribunal de Justiça (Grande Secção). Acórdão de 8 de abril de 2014. Processos apensos C-293/12 e C-594/12. *Digital Rights Ireland Ltd contra Ministro das Comunicações, Recursos Marinhos e Naturais e o. e Kärntner Landesregierung e o*. [S. l.]: EUR-Lex, 2014.

tráfego e localização para prestadores de serviço de comunicação para persecução penal[89], que tinha internalizado a Diretiva invalidada previamente pelo tribunal.

O caso brasileiro e os dois julgados do TJUE demonstram potencial normativo da proteção de dados, na dimensão principiológica, para limitar a arquitetura informacional, ainda que tenham ocorrido contenciosamente. Em ambos os casos, agências estatais foram proibidas de acessar informações. No primeiro, informações à disposição de uma agência pública não puderam ser transferidas, sem justificativa legal. Nos casos do bloco europeu, o tribunal impediu que Estados-membro obrigassem o setor regulado a reter dados em caráter preventivo, que poderiam ser acessados na persecução penal individualizada no futuro.

A principal ideia jurídica que se pode retirar das decisões europeias é que a retenção de dados indiscriminada de todos os usuários de determinados sistemas configura uma intervenção informacional indevida, isso porque o Estado não deve obrigar particulares a fazerem registros coletivos para a eventualidade de que possam a ser úteis a investigações criminais. Entretanto, vale lembrar que esse racional é inexistente no ordenamento e decisões brasileiras, o que se evidencia com a utilização da retenção geral como estratégia de informações em diversos diplomas, com ênfase no Marco Civil da Internet, que prevê amplos deveres de retenção[90].

A retenção indiscriminada se diferencia das práticas de prevenção anteriormente previstas no ordenamento brasileiro, especificamente sobre branqueamento de capitais, na medida em que o COAF recebe informações já identificadas previamente como atípicas por padrões de inteligência, que são publicados. No caso da retenção das informações da internet, a opção legislativa é pelo arquivamento completo sem a observância de critérios de inteligência, em outras palavras, a política informacional é orientada para a formação de repositórios, o que não é visualizado como uma intervenção em direitos fundamentais pela prática jurídica brasileira.

Isso ocorre porque a arquitetura informacional disponível ao Estado é estabelecida com a utilização de múltiplas estratégias, regulatórias para o setor privado, com de deveres inerentes à atividade econômica, ou de política públicas implementadas para e pelos entes públicos. Independentemente do setor, riscos de excesso de coleta, abuso de processamento e transmissão

---

[89] UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia. Acórdão de 21 de dezembro de 2016. Tele2 Sverige AB c. Post- och telestyrelsen e Secretary of State for the Home Department c. Tom Watson e o. Processos apensos C-203/15 e C-698/15. ECLI:EU:C:2016:970. Luxemburgo, 2016.

[90] Todos dados de conexão devem ser retidos por um ano por provedores de internet (Art. 13, § 2º) e os dados de acesso a aplicativos devem ser retiros por seis meses. Respetivamente previstos pelos artigos 13, § 2º e 15, § 3º, do Marco Civil da Internet.

inadequadas de dados devem são objetos da política criminal informacional, que além de invalidar juridicamente o ato já praticado, deve funcionar como critério de validade formal para orientar as escolhas futuras, mais precisamente com critérios específicos para o processo legislativo.

A política criminal define os elementos de informação que podem ser objeto de persecução penal antes da existência do fato-crime, permitindo que o Estado cumpra o poder/dever de perquirir criminalmente, tendo em vista que a jurisdição penal é necessária[91]. Entretanto, o poder estatal de fazê-lo – caracterizado pelo exercício jurisdicional –, não pode instituir uma arquitetura que exceda, por desenho institucional, os limites impostos, pelas condicionantes jurídicas aplicáveis. Em outras palavras, a arquitetura informacional deve observar critérios de validade material, tais como a separação informacional e a adequação legal das soluções tecnológicas.

Como se pode ver, ao se falar na validade material das leis que versam sobre a arquitetura informacional, é necessário recorrer ao conteúdo normativo da proteção de dados, aos menos na dimensão principiológica, na medida em que esse ramo do direito já identificou riscos e aspectos legais formais e materiais para intervenções informacionais. Nesse sentido, a descrição do teste de legalidade de Degrave leva invariavelmente a interconexões com esse ramo, a exemplo da proporcionalidade, cuja aplicação prática remete diretamente ao princípio da minimização, isto é, usar a menor quantidade de dados pessoais para gerar inferências corretas.

Esse racional, que introduz a proteção de dados principiologicamente, ficou muito claro da decisão do STF sobre compartilhamento com a ABIN, na qual a finalidade abstrata de inteligência estatal não superou o caráter abrangente e ilimitado da transferência em questão, notoriamente securitária. Entretanto, a aplicação enquanto princípio não é suficiente para adicionar etapas de validade para o processo legislativo, com adição etapas procedimentais a serem cumpridas, que são necessárias em razão do tipo de intervenção informacional em questão. Naturalmente, não ideal que as inovações só possam ser controladas contenciosamente após a alteração legal.

Em conclusão, não há critérios para a validade formal do processo legislativo, que implementa intervenções informacionais. Por essa razão, toda a discussão dos limites à arquitetura informacional é prescritiva, quando muito, é possível recorrer-se a experiência internacional, para

---

[91] "A idéia de jurisdição como poder (mais ou menos condicionado, dependendo do contexto histórico jurídico em questão) tem preponderado. No bojo desta noção de poder, no que se refere à jurisdição penal, está a idéia (acolhida por Carnelutti) de que o poder jurisdicional se conheça sob o nome de direito de punir, coincidindo o poder de punir e o poder de jurisdição penal" (KHALED JR., Salah Hassan. O problema da prevalência do poder na jurisdição penal: rumo ao estabelecimento de uma jurisdição penal como poder-dever e direito fundamental. Revista da Faculdade de Direito da UFG, v. 34, n. 01, p. 65-66, jan./jun. 2010.)

afirmar a invalidade material das leis em razão dos excessos de coleta, uso e reúso pela arquitetura informacional do Estado, que é uma consequência da mora legislativa em relação à proteção de dados no âmbito público brasileiro.

No próximo subtópico, os critérios de uma metalei para o processo legislativo no contexto informacional são propostos.

1.2.1. Adição de critérios formais para o processo legislativo que visa a implementar e/ou alterar a arquitetura informacional

Como abordado no tópico anterior, alguns critérios adicionais devem ser observados para alterações legislativas que visam a implementação de tecnologias da informação invasivas. Para instrumentalizar essa obrigação, o próprio processo legislativo deve assumi-los, uma função que poderia ser exercida por uma lei geral de proteção de dados para finalidade pública. Entretanto, o Brasil não aprovou lei nesse sentido, apesar de apresentação de anteprojeto por uma de juristas convidados pela Presidência da Câmara dos Deputados, que deu origem ao projeto ao PL 1515/2022. Ainda que o texto possa servir como fonte comparativa, não é fonte de direito.

Em relação a inclusão de critérios formais na decisão política, é necessária a produção de relatórios de impacto e a realização de audiências públicas processo legislativo que altera a arquitetura informacional do Estado. Essas estratégias almejam aumentar o conhecimento público sobre o que se pretende autorizar, abrindo-se a possibilidade de questionamentos pela sociedade civil, academia e outros atores sociais. No âmbito do exercício das pretensões processuais desses entes, as ações para garantia de direitos difusos e as ações constitucionais devem ser lidas como instrumentos para efetivar as condicionantes jurídicas da arquitetura informacional do Estado.

Partindo-se do trabalho da referida comissão, os juristas propuseram que exigência da elaboração de Relatório de Análise de Impacto Regulatório como condição para implementação de tecnologias de monitoramento[92]. O relatório englobaria a definição da natureza dos dados envolvidos, as finalidades específicas de processamento, risco de uso discriminatório, as medidas previstas para dirimir os riscos e a política de uso e as garantias dos titulares dos dados[93]. O objetivo

[92] A definição de tecnologia de monitoramento no anteprojeto é: *"*XXIII - tecnologia de monitoramento: equipamento, programa de computador ou sistema informático que possa ser usado ou implementado para tratamento de dados pessoais captados ou analisados, entre outros, em vídeo, imagem ou áudio".
[93] Art. 42, § 2º, do anteprojeto.

era que os diversos resultados ilícitos decorrentes desse tipo de vigilância fossem previamente mensurados para se verificar concretamente se o risco é tolerável.

Por exemplo, não é aceitável que a tecnologias de vigilância incidam com maior ênfase em determinados grupos étnicos, esse é um resultado ilícito como esse poderia afastar a implementação de determinadas tecnologias, caso identificada em relatório de risco. Vale mencionar que a revisão bibliográfica identificou fontes sobre utilização de *softwares* com vieses discriminatórios para seleção profissional de pessoas, distinguindo ilicitamente entre brancos e pretos[94], reconhecimento facial para segurança pública e persecução e alta taxa de erro[95], tratamento não isonômico entre homens e mulheres[96], o que indica o acerto da prescrição etapas legislativas adicionais.

Essas fontes apontam resultados ilícitos[97], que constituem risco inerente do uso de soluções algorítmicas para predição de comportamentos. É necessário saber que é impossível erradicá-los, então é necessário o manejo legislativo para reduzi-los no âmbito público. Assim, o processo legislativo que cria a intervenção informacional deve observar critérios específicos que permitam a identificação dos riscos informacionais. Nesse sentido, o relatório de impacto se apresenta como a solução gerencial de risco mais adequada para esse cenário, que serve, em linhas gerais, para orientar o debate político com critérios técnicos.

A definição do conteúdo dos relatórios de impacto gerou diversas divergências nas últimas décadas, sendo que a forma mais adequada de os caracterizar é como conceito guarda-chuva de várias soluções. Clarke define-o como "um processo sistematizado que identifica e avalia, sob as perspectivas de todas as partes interessadas, os potenciais efeitos sobre a privacidade de um projeto, iniciativa ou sistema ou esquema proposto, incluindo a busca por maneiras de evitar ou mitigar impactos negativos à privacidade". Na segurança pública, a análise deve anteceder qualquer alteração que tenha como objetivo realizar monitoramento de pessoas.

---

[94] SOUSA, Pedro. Direito penal nos tempos da inteligência artificial: uma análise da responsabilidade dos agentes envolvidos no desenvolvimento e na operação de algoritmos de seleção e recrutamento em relação ao crime de racismo previsto no art. 4° da Lei 7.716/1989. 2022. Dissertação (Mestrado em Direito Constitucional) – Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, Brasília, 2022.

[95] ALMEIDA, Eduarda Costa. Os grandes irmãos: o uso de tecnologias de reconhecimento facial para persecução penal. Revista Brasileira de Segurança Pública, São Paulo, v. 16, n. 2, p. 264-283, fev./mar. 2022

[96] COLLETT, Clementine; NEFF, Gina; GOMES, Livia Gouvea. Os efeitos da inteligência artificial na vida profissional das mulheres. Brasília: UNESCO: BID: OCDE, 2023.

[97] Igualdade de tratamento entre homens e mulheres é norma constitucional com força normativa, e o fato da ilicitude ser no ambiente digital, não altera o efeito jurídico atribuído legalmente. Deve haver, portanto, formas de evitá-los. Nesse sentido, uma das estratégias é a obrigação de impacto regulatório como etapa essencial do processo legislativo para edição de medidas que geram os referidos riscos, especialmente quando se tratar de dados sensíveis e sigilosos.

Nessa linha, a participação da sociedade civil organizada e da academia no processo legislativo é essencial para identificar riscos não toleráveis na adoção de medidas de processamento de dados de alto risco; por exemplo, na persecução penal, a capacidade técnica de desvio de finalidade. Por isso, o chamamento e publicização de audiências pública são o primeiro contrapeso legal nesse processo decisório de política criminal informacional, que possibilita a contestação dos testes apresentados ou a demonstração de que o risco foi indevidamente mensurado.

Entretanto, em que pese a justificativa do anteprojeto legislativo feito pela comissão, o projeto de Lei 1515/2022, apresentado com base nele, retirou a obrigatoriedade de produção de Análise de Impacto Regulatório como etapa do processo legislativo, bem como os procedimentos de controle público. Nesse contexto, analisando o projeto apresentado, o instituto Lapin concluiu corretamente que a versão apresentada enfraquece "direitos e proteções referentes a decisões automatizadas, como exigência de autorização prévia e de relatórios de impacto adequadamente procedimentalizados, em favor de disposições genéricas e de aplicabilidade limitada"[98].

A defesa de que medidas de intervenção informacional sejam previstas em lei em desajuste a um processo legislativo sem critérios específicos é uma proteção legal deficiente à autodeterminação informacional como garantia fundamental. O relatório de impacto serve para jogar luz do debate público em questões técnicas não facilmente compreendidas, evitando-se decisões legislativas movidas somente pelo interesse legítimo de persecução penal, mas em completa inobservância aos riscos de sua implementação.

Como se pode ver, o atual arcabouço legal é limitado e a proposta concreta para alterá-lo não privilegia uma política criminal informacional orientada para garantia de direitos fundamentais. Ao tudo indica, a organização da burocracia informacional não foge do lugar-comum da política criminal do combate à criminalidade, cujos direitos são debatidos como reveses ao endurecimento da lei, quando muito mencionados após conjunções adversativas, entendidos pejorativamente como brechas utilizadas pelos inimigos públicos[99].

O projeto de lei n. 1515/2022 e a lógica de política criminal que o orienta lidam mal com os riscos do monitoramento de alto risco, a exemplo da vigilância em tempo real, que sabidamente

---

[98] AZEVEDO, Cynthia Picolo Gonzaga de et al. Nota técnica: análise comparativa entre o anteprojeto de LGPD penal e o PL 1515/2022. Belo Horizonte: Instituto de Referência em Internet e Sociedade (IRIS); Brasília: Laboratório de Políticas Públicas e Internet (LAPIN), p. 4, 2022.

[99] SILVA, Thales Cassiano. Como a Petrobras foi de vítima à ré? Lava Jato vs. Vaza Jato: instrumentalidade processual e limites penais da assistência direta. 237 f. Dissertação de Mestrado - Faculdade de Direito, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, p. 39, 2021.

ocorrem no Brasil, mesmo sem previsão em norma autorizadora. À vista disso, a realidade prática brasileira é que as intervenções informacionais geralmente são autorizadas sem definição de finalidade e com conteúdo amplo, para serem regulamentadas por decretos e portarias, como se abordará adiante na implementação dos sistemas de monitoramento públicos no Brasil. Deve-se concluir, portanto, que a praxe é diametralmente oposta às prescrições aqui realizadas.

1.2.2. Adequação funcional e legal das tecnologias implementadas

A adequação funcional dos métodos tecnológicos aplicados é geralmente defendida para implementação de soluções que envolvam *big data*[100], essenciais ao monitoramento, e compõe a validade material da arquitetura informacional. Dessa forma, um programa específico, que pode ser uma tecnologia privada comprada pelo Estado, deve ser testado de acordo com seus objetivos declarados, em outras palavras, se o programa cumpre o que se propõe a fazer. Essa fase é especialmente relevante em países que são predominantemente consumidores de tecnologias produzidas em outros países[101].

Em regra, os objetivos declarados informam a utilização de dois tipos de algoritmos[102]: os de triagem, que classificam cidadãos em função de critérios – condicionantes a acesso a direitos – e os de predição que fazem a perfilagem para lidar com riscos, que são os mais relevantes paras as funções de segurança pública e persecução criminal. Diante disso, a análise funcional deve identificar quais dados o programa computacional necessita para gerar inferências estatisticamente corretas, isto é, o processamento computacional útil. A depender do tipo de dado pessoais necessário, determinadas soluções podem ser consideradas inadequadas legalmente.

Por exemplo, uma tecnologia que objetive identificar passageiros perigosos para aviação não poderá depender de dados de credo religioso para gerar inferências (*no-fly list*). Caso seja esse o caso, ainda que a referida finalidade fosse autorizada legalmente, a tecnologia em específico não poderá ser utilizada por inadequação funcional. O exemplo pode parecer absurdo, mas a depender do país de origem da tecnologia, isso pode ser exigido por design. Pode-se dizer, portanto, que a

---

[100] GRAY, David. The Fourth Amendment in an Age of Surveillance. [S. l.]: Cambridge University Press, 2017, p. 267, 2017.
[101] LEMOS, Alessandra et al. Comentários ao Anteprojeto de Lei de Proteção de Dados para a Segurança Pública: Tecnologia de Reconhecimento Facial. [S. l.]: Instituto de Tecnologia & Sociedade do Rio, p. 6, 2021.
[102] DEGRAVE, 2024, p. 21.

origem da informação, o tipo e uso são critérios para aferição da adequação funcional, tendo em vista que os usos não podem depender de qualquer tipo de dados pessoais.

A fonte da informação digital e a coleta de dados serão trabalhadas em capítulos específicos no decorrer da tese. Entretanto, não é possível falar de adequação funcional sem distinguir que a coleta por agências estatais não pode recair sobre dados sensíveis sem previsão legal, assim como seu reúso para finalidade distinta da aquisição inicial. No caso da informação religiosa, não há permissivo legal para a retenção dessa informação individualizada[103] e, ainda que houvesse, o acesso para gerar inferências sobre risco à segurança é inconstitucional, por violação ao núcleo essencial liberdade de credo religioso com uma intervenção informacional.

O reconhecimento dos resultados ilícitos também orienta a análise do cumprimento dos objetivos declarados, isto porque um sistema que coleta mais dados que o necessário ou apresenta grande taxa de erro de processamento não é adequado funcionalmente. Nesse ponto, a adequação está conectada com a fase de processamento de dados, que constitui o objetivo-fim das ações de coleta, transmissão etc. Assim, se na fase de testes da tecnologia da informação for verificada a disfuncionalidade no uso declarado, ela deve ser descartada.

Prescritivamente, a verificação da adequação funcional é intuitiva, mas a principal questão que se impõe a partir da afirmação é o momento adequado para a verificação dos objetivos declarados[104]. No caso brasileiro, e de outros países do sul global, nos quais grande parte das tecnologias são adquiridas já desenvolvidas, o momento de identificar esses critérios de inadequação é prévio à contração, em testes de revisão, a serem realizados pela agência destino da tecnologia, que, no caso da persecução, seriam principalmente as polícias judiciárias. Outra questão pertinente é que os testes deveriam ocorrer publicamente para a realização de controle[105].

A publicidade dos testes encontra dois problemas. O primeiro deles é que, ao tratar das funções de inteligência da segurança nacional, o sigilo estatal tende a ser privilegiado. Em segundo lugar, o funcionamento do algoritmo é constantemente protegido como propriedade intelectual das empresas criadoras. Nesse contexto, a possibilidade de controle público é limitada, devendo-se confiar que o processo de aquisição tenha levantado os pontos relevantes para a tomada de decisão

---

[103] A única razão para retenção de informação sobre credo religioso é por razões acadêmicas e censitárias, que não necessariamente exigem que a pessoa que cedeu a informação seja individualizada.
[104] Será explicado adiante as preocupação e limitações das políticas de privacidade e segurança no projeto das tecnologias da informação.
[105] GRAY, p. 268, 2017.

a respeito da adequação da solução à sua proposta, o que não defensável juridicamente.

Algumas medidas podem ser tomadas para endereçar esse desafio: a obrigatoriedade de apresentação de relatórios de usos em outros países, que guardem semelhança com as características sociais e econômicas brasileiras; a realização de monitoramento de resultados pós implementação como motivo contratual para rescisão sem custos ao erário em caso de inadequação. Ademais, os processos de compra devem ser publicados por meios oficiais para que, os órgãos de controle difuso e sociedade civil possam questioná-los judicialmente, nas hipóteses necessárias.

No entanto, a tendência no sistema brasileiro, tendo em vista o modelo implementado de proteção de dados na seara cível, é o controle por agência independente, conjuntamente ao dever de produzir relatórios de impacto regulatório para implementação de novas tecnologias durante o processo legislativo. No âmbito das atividades investigação e de repressão a infrações penais, a única previsão vigente é que a possibilidade de a Autoridade Nacional de Proteção de Dados (ANPD) de emitir opiniões técnicas e recomendações[106]. Logicamente, esse controle está aquém do necessário, o que é relativamente um consenso político.

Atualmente, a verificação da adequação funcional das tecnologias da informação implementadas por órgãos públicos ocorre em um ambiente opaco, em razão do direito de propriedade das empresas e da invocação de sigilo por se tratar de ações de segurança ou de inteligência estatal. Contudo, esses argumentos não devem prevalecer, na medida em que há instrumental para o controle público, como os testes funcionais realizados antes e depois da aquisição, ou ainda o controle por agência independente. Por fim, quanto aos critérios a serem utilizados nos testes, o excesso de processamento, a produção de resultados ilícitos e os tipos de dados necessários constituem as principais métricas para analisar os objetivos declarados.

1.3. Entre as prescrições feitas e a realidade brasileira

Como vem sendo abordado no capítulo, não é necessário citar as modernas tecnologias da informação para identificar os riscos da utilização acrítica de algoritmos pela burocracia estatal, as análises sobre criminologia atuarial evidenciaram o potencial deletério aos direitos fundamentais desse tipo de racionalidade há bastante tempo. Se consideradas a capacidade computacional de

[106] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2025]. Art. 4º, III, § 3º.

armazenamento e processamento de dados, aqueles algoritmos eram processados rudimentarmente, com baixa eficácia. Ainda assim, projetava-se neles, o gerenciamento do risco penal[107] [108].

Deve-se entender que o processamento de alto risco não se assemelha às análises humanas tradicionais e manualizadas, pois permite correlações e inferências que só são possíveis mediante a inserção de dados em larga escala. Essa capacidade possibilita "*to extract new insights or create new forms of value, in ways that change markets, organizations, the relationships between citizens and governments*"[109]. Para sua existência, é indispensável a disponibilidade de vastas bases de dados, alimentadas por múltiplas fontes, aliada ao alto processamento computacional, em outras palavras, a constituição de uma ampla arquitetura informacional.

Esse tipo de processamento pode englobar variadas tecnologias da informação, tais como a inteligência artificial, *big data*, *machine learning*, que podem ser utilizadas isoladas ou conjuntamente. Uma das suas possibilidades que é mais atrativa para segurança pública e persecução penal é o reconhecimento facial automatizado, que talvez seja a principal técnica na qual se projeta a panaceia tecnológica pela política brasileira, o que Melgaço chamou de performance de política pública[110], que é pouco comprometida com a efetividade das medidas, e pode ser visualizada na propaganda da cidade inteligente como resposta penal.

Essa técnica está, ou já esteve, em funcionamento em diversas cidades do mundo, a exemplo de Nova Iorque[111], Oakland e São Francisco [112]. A última baniu a utilização em razão do uso indevido para controle de protestos políticos [113]. Nessa linha, o banimento do uso não é

---

[107] Utiliza-se a expressão trazida pela obra de Maurício Dieter, que é *Política Criminal Atuarial: A Criminologia do Fim da História,* 2012.

[108] Gloeckner aponta que: "na modernidade, sob o governo da técnica e da ciência, a natureza era vista como objeto. Na modernização reflexiva, com o surgimento da sociedade de risco, os primeiros efeitos, via de consequência, serão observados naquilo que era a preocupação moderna: a natureza. Os riscos são constata- dos mais facilmente no meio-ambiente" (GLOECKNER, 2008, p. 110).

[109] MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. Big Data: a revolution that will transform how we live, work, and think. Boston: Houghton Mifflin Harcourt, 2013.

[110] MELGAÇO; VAN BRAKEL, 2021, p. 245-246.

[111] AMNESTY INTERNACIONAL. Ban the Scan, 2021. Disponível em: https://banthescan.amnesty.org/nyc/index.htmlMNISTIA.

[112] GUARIGLIA, Matthew. The Movement to Ban Government Use of Face Recognition. Electronic Frontier Foundation, 2 maio 2022. Disponível em: https://www.eff.org/deeplinks/2022/05/movement-ban-government-use-face-recognition. Acesso em

[113] KOKKONEN, Bolívar. BARNIR OU REGULAR: Reconhecimento Facial e Racismo nas Polícias do Berço das Big Techs, 2022.

particularidade de São Franciso, a proibição já foi identificada em outras cidades americanas[114], ou seja, é uma possibilidade jurídica em discussão que apresenta bons pontos de reflexão.

Em território brasileiro, encontrou-se fontes descentralizadas que confirmam a utilização nos estados do Acre e da Bahia[115], no cidades do Rio de Janeiro e de São Paulo[116], e em Recife[117]. É importante mencionar que é possível identificar outras cidades, a exemplo de Curitiba, por meio de fontes jornalísticas, mas a tese priorizou as cidades em que mapeadas por pesquisas acadêmicas sobre proteção de dados e tecnologia da informação.

Entretanto, essa não é a única tecnologia de monitoramento identificada no Brasil. A pesquisa de Tsunoda, Candido e Guimarães identificou o uso de tecnologias invasivas para função de segurança pública com implementação de GIS (*Geographic Information System*) em Alagoas e no Distrito Federal[118]. Um outro achado de pesquisa relevante é que alguns estados responderam aos pesquisadores não fazer o uso de nenhuma das tecnologias inseridas na pesquisa, mas publicaram oficialmente o uso de inteligência artificial para finalidade de segurança, especificamente Paraná e Alagoas.

Enquanto se discute academicamente o estabelecimento de critérios prévios a implementação de tecnologias invasivas, a realidade que se impõe é a implementação estatal, em tal grau de opacidade, que se responde a pesquisadores que não se faz uso, apesar de já ter havido implementação. Talvez por isso, a opinião pública costuma tomar conhecimento dessas medidas pela divulgação de testes realizados por organizações sem fins lucrativos, que se dedicam a temática da privacidade, como a Data Privacy Brasil, *a American Civil Liberties Union* (ACLU), *Amnesty International*, a *Electronic Frontier Foundation* (EFF).

A ACLU testou um software de reconhecimento facial, produzido pela *Amazon*, que identificou falsamente o rosto de 28 congressistas americanos com base num banco de dados de atiradores. Os falsos positivos eram o dobro para pessoas pretas, demonstrando um viés

---

[114] *Electronic Frontier Foundation* (EFF) identificou as seguintes cidades: Berkeley (CA); Boston (MA); Brookline (MA); Cambridge (MA); King County (WA); Madison (WI); Minneapolis (MN); New Orleans (LA); Northampton (MA); Oakland (CA); Pittsburgh (PA); Portland (ME); Portland (OR); San Francisco (CA); Santa Cruz (CA); Somerville (MA); Springfield (MA). Disponível em https://www.eff.org/aboutface/bans-bills-and-moratoria

[115] TSUNODA, Denise Fukumi; CANDIDO, Ana Clara; GUIMARÃES, André José Ribeiro. Tecnologias disruptivas em segurança pública: uma análise situacional brasileira. Revista Tecnologia e Sociedade, Curitiba, v. 20, n. 61, p. 327, 2024.

[116] MELGAÇO; VAN BRAKEL, 2021, p. 245-246.

[117] LEANDRO; DE, M.; GUILHERME, F. Cidades inteligentes e inovação: a videovigilância na Segurança Pública de Recife, Brasil. Cadernos Metrópole, 2023.

[118] TSUNODA; CANDIDO; GUIMARÃES, 2024, p. 327.

discriminatório[119]. É inegável o papel da sociedade civil na definição dos contornos da adequação funcional de tecnologias que processam em massa dados sensíveis. Naturalmente, a adequação funcional da arquitetura informacional não pode depender exclusivamente de testagens da sociedade civil. Ao contrário, ela começa com o dever de publicidade do Estado.

O processo de aquisição de tecnologias da informação para a composição da arquitetura informacional do Estado brasileiro é bastante opaco, sem critérios para o momento em que as testagens prévias devem ocorrer ou das entidades que devem participar. O exemplo do pregão eletrônico que culminou na compra de *spyware* da *Harpia Tech* sem previsão legal é somente uma das aquisições, num contexto de implementação de projetos de cidades inteligentes em diversos municípios brasileiros, como já identificado nas pesquisas citadas acima. Dito de outra forma, houve a implementação de projetos de monitoramento em diversas cidades sem previsão legal, sem testagem pública da adequação funcional e sem produção relatórios de risco.

Não há, de fato, conhecimento público sobre as tecnologias que vêm sendo implementadas, tampouco um processo legislativo que identifique e avalie os riscos envolvidos. O que chega ao conhecimento da sociedade são apenas os casos de falso negativo – quando uma pessoa inocente é identificada por *software* e presa indevidamente. É preciso, contudo, compreender que esse resultado decorre de uma cadeia de eventos que inclui a implementação de tecnologias sem amparo legal, sem transparência, sem verificação de funcionalidade e sem fiscalização quanto ao uso por parte dos agentes responsáveis pelo treinamento. Em sentido mais amplo, não é suficiente reconhecer o resultado do processamento de dados que são ilícitos, deve-se prescrever instrumentos legais que possibilitem o contrapeso legal em todas as etapas que o precedem, o que se dá, em primeiro momento, em na definição dos contornos da arquitetura informacional.

Ademais, o cenário tende a se agravar. Diz-se isso porque a arquitetura informacional passa, gradualmente, a incorporar tecnologias capazes de coletar dados de forma autônoma, o que potencialmente aumenta os processamentos ilícitos – tanto por erros técnicos quanto por atuações ilegais de agentes de persecução penal. Nesse contexto, a arquitetura informacional brasileira é constituída com base em decisões políticas locais, orientadas por um viés cientificista, e é implementada em grande medida sem autorização legal em sentido amplo.

---

[119] GERCHICK, Marissa; CAGLE, Matt. When it comes to facial recognition, there is no such thing as a magic number. ACLU, 7 fev. 2024. Disponível em: https://www.aclu.org/news/privacy-technology/when-it-comes-to-facial-recognition-there-is-no-such-thing-as-a-magic-number. Acesso em: .

Portanto, a tese central de que Estado só deve implementar a soluções de arquitetura tecnológica que realizem a função declarada após averiguar os riscos inerentes e possíveis excessos em sua utilização não encontra ressonância na prática brasileira. Naturalmente, a não observância dessa diretriz impede a efetividade dos contrapesos legais para a proteção dos direitos difusos[120].

O capítulo abordou os dois principais usos da categoria adequação funcional, o teste em concreto da função declarada pela solução tecnológica com seus resultados práticos – o cumprimento do objetivo declarado – e os critérios de validade material e formal necessários a alteração da arquitetura informacional do Estado. Ademais, não há critérios legais para estabelecer o momento e a forma para realização de testes de adequação que, com dito, em países consumidores das tecnologias, deve ocorrer preferencialmente antes da aquisição da solução tecnológica pela agência destinatária, para as quais se defendeu a necessidade de comprovação de efetividade por meio de relatórios de uso em outros países ou fase de teste posterior a contração como possibilidade de rescisão contratual.

Por fim, a política criminal informacional é condicionante jurídico-normativa da arquitetura informacional disponível para persecução penal, que deve orientar o debate legislativo *ex ante* sobre deveres de retenção para setores, criação de bancos de dados por entes de direito público e métodos de investigação. Nesse processo, as previsões legais e constitucionais impõem que, especialmente no regramento de dados sensíveis e sigilosos, o debate legislativo ocorra com apoio em evidências e participação pública. Como se viu, adequação legal da arquitetura não se exaure na promulgação de lei, que deve se adequar a critérios de validade formal e material específicos.

[120] A exemplo da ação popular, da ação civil pública ou do mandado de segurança.

2. COLETA DE DADOS DIGITAIS

No capítulo anterior, a tese debateu os critérios de adequação legais e funcionais para que a arquitetura informacional do Estado seja legítima, estabelecendo que o controle *ex ante* da política criminal é determinante para reduzir impactos ilícitos em direitos pela implementação de tecnologias da informação. A preocupação com a arquitetura informacional deriva do potencial de produção de conhecimento a partir do dado digital – entendido como a mínima unidade de informação quantificada e quantificável[121]– que pode gerar informações inteligíveis.

O dado digital é a base de todas as formas de processamento computacional, isso não é novidade alguma na era computacional[122]. A novidade está na escala[123], uma das principais variáveis é a estrutura de captação, disponíveis na navegação online, por meio de hardwares, dispositivos sem fio e na interação automática entre dispositivos. Neste contexto, dados pessoais são coletados e armazenados a todo momento, tal como bem-observou Solove: "we are becoming a society of records, and these records are not held by us, but by third parties."[124]

Os terceiros mencionados pelo autor são geralmente as empresas de tecnologia da informação, mas se aplica igualmente ao Estado. Indubitavelmente, a coleta de dados pessoais é a primeira ingerência na esfera individual de direitos, que pode ser ilegítima por desvio de finalidade, excesso, reutilização secundária, erros de processamento e acessos indevidos[125]. Esses ilícitos na coleta minam a autodeterminação informacional, chegando-se ao ponto de possibilitar a predição de comportamentos alheios ao escopo do consentimento dos titulares dos dados.

Antes de expor os potenciais problemas, define-se a coleta de dados como "the process of gathering, filtering and cleaning data before it is put in a data repository or any other storage solution on which data analysis can be carried out (…) [que é baseado] on fast and massive data

---

[121] CUNHA, M. B.; CAVALCANTI, C. R. O. Dicionário de Biblioteconomia e Arquivologia. Brasília: Briquet de Lemos, p. 112-113, 2008.
[122] FERGUSON, Andrew Guthrie. Big Data and Predictive Reasonable Suspicion. University of Pennsylvania Law Review, v. 163, n. 2, p. 353, jan. 2015.
[123] "The growth in the volume of data collected, the ability to connect previously discrete data networks, and the analytical capabilities made possible by faster computer processors and more data storage capacity, however, are new developments" (*Ibid.*)
[124] SOLOVE, Daniel J. The Digital Person: Technology and Privacy in the Information Age. New York: New York University Press, p. 181-192, 2004.
[125] RUBINSTEIN, Ira S. Regulating Privacy by Design. Berkeley Technology Law Journal, [s. l.], v. 26, n. 3, p. 1431, 2011.

collection"[126]. Ademais, a aquisição de dados também é alterada pela evolução das tecnologias da informação, ou seja, ocorre em alto volume, alta velocidade e alta variedade, alta veracidade e tem alto valor[127]; esses 5Vs determinam a forma como essa fase ocorre, e se caracteriza por ser escalável.

Como já visto, a tradicional solução jurídica para endereçar os desvios de finalidade no processamento de dados é a defesa do consentimento, isto é, o titular do dado permite que terceiros processem seus dados para obter informações úteis, melhor rota para o destino, predição de gosto musical etc. O referido princípio também é aplicável à coleta: só deve ser coletado aquilo que foi permitido pelo titular, que deve ter meios para essa tomada de decisão. No direito público, adequação legal opera o mesmo efeito, limita o que é registrado (conhecido) pelo Estado.

Usando-se o direito europeu como base jurídica comparada, a Diretiva (EU) 2016/680 determina que o Estados-membros legislem sobre tratamento de dados para fins de persecução, com a definição das finalidades[128]. Na sequência, o artigo 9º do referido diploma especifica que todas as formas de processamento não previstos para as referidas finalidades não podem ser realizadas. Em outras palavras, a intervenção informacional no âmbito público só é válida materialmente se atender a finalidades de uso definidas previamente.

O sistema brasileiro de proteção de dados oferece a mesma solução para o processamento no âmbito cível, usando-se consequentemente o consentimento como categoria de controle. Por essa razão, cita-se a experiência internacional para o tipo de processamento estudado na pesquisa. Como tese geral, a afirmação é que dados que excedam a finalidade legal não devem ser coletados. Esta é a primeira etapa de controle, o momento-chave, e o mais eficaz, para evitar processamentos

---

[126] SOLOVE, 2004, p. 166.

[127] De acordo com Wandt e Maras: "*There are five dimensions of big data: volume, which refers to the amount of data (i.e. quantity of data); variety (i.e. different types of data collected about users) that can be divided into structured data (i.e. traditional forms of data, such as financial data, geolocation data, and call data) and unstructured data (i.e. weblogs, social media posts, video recordings, audio recordings, images, and app usage logs); velocity, which refers to the speed with which data is generated, processed and transferred; veracity (i.e. the accuracy and reliability of data); and value, which refers to the gains from data collection and analysis, and the measurable improvements that the collection and analysis of the data provide*". (MARAS, Marie-Helen; WANDT, Adam Scott. Enabling mass surveillance: data aggregation in the age of big data and the Internet of Things. Journal of Cyber Policy, [s. l.], v. 4, n. 2, p. 161, 17 mar. 2019).

[128] UNIÃO EUROPEIA. Parlamento Europeu e Conselho. Diretiva (UE) 2016/680, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revogação a Decisão-Quadro 2008/977/JAI do Conselho. *Jornal Oficial da União Europeia*, L 119, Luxemburgo, 4 maio 2016. p. 89-131. Art. 8º.

ilícitos de dados, que é não permitindo sua coleta no primeiro momento[129].

Degrave aponta no mesmo sentido a respeito do direito belga: "se for possível prescindir de um tratamento de dados para atingir o objetivo perseguido, é preciso fazê-lo, sendo a melhor forma de proteger os dados dos cidadãos a de não os coletar"[130]. À vista disso, a autora menciona a opinião n. 37/2003, da autoridade belga de proteção de dados sobre estacionamentos públicos, que afirmou que é preferível que as prefeituras instalem catracas físicas do que coletar os dados de todas as placas de automóveis com utilização de leitores automáticos.

Nos casos em que a coleta é imprescindível, o princípio adjacente é a minimização, que consiste no desenho dos sistemas de informação de dados para realizar o processamento "with the aim of collecting, processing and using no personal data at all or as little personal data as possible"[131]. O princípio é bastante intuitivo, combate-se o excesso com a métrica da necessidade em razão finalidade – objetivo de utilização. É nesta fase que se insere a problemática do uso de tecnologias que aprendem autonomamente a coletar e processar mais dados que o programado.

Mais uma vez, o direito da União Europeia pode servir como exemplo de inserção legislativa do referido princípio, tanto o processamento para fins cíveis quanto penais[132] [133], ambas, com a mesma redação, preveem que o processamento deve ser "limitado ao mínimo necessário relativamente às finalidades". Essa leitura deve ser ampliada à fase de coleta, na medida que o adequado só pode ter como base a finalidade, funcionando com a métrica desse limite, logo a aquisição de dados não é legítima se orientada à maximização da coleta de dados "supérfluos"[134].

De forma geral, tem-se um consenso a respeito da resposta jurídica aos apontados riscos com a implementação de tecnologias da informação. Contudo, o reconhecimento jurídico não encerra o debate. Ainda que os referidos princípios, que nascem em resposta ao avanço tecnológico, sejam condicionantes jurídico-normativas, positivadas em diversos ordenamentos, a implantação

---

[129] SHANMUGAM, Divya et al. Learning to Limit Data Collection via Scaling Laws: A Computational Interpretation for the Legal Principle of Data Minimization. *In*: ACM CONFERENCE ON FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY (FAccT '22), 2022, Seoul. Anais [...]. New York: ACM, 2022. p. 839-849.
[130] DEGRAVE, Élise. L'Etat numériques et les droits humains. 1 Ed. Académie Royale, p. 57-58, 2024, tradução nossa.
[131] SCHAAR, Peter. Privacy by Design. IDIS, [s. l.], v. 3, n. 3, p. 271, 1 abr. 2010.
[132] UNIÃO EUROPEIA. Parlamento Europeu. Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). *Jornal Oficial da União Europeia*, Luxemburgo, L 119, p. 1-88, 4 maio 2016. Artigo 5º alínea C.
[133] UNIÃO EUROPEIA, Diretiva (UE) 2016/680, 2016. Art. 4º alínea C.
[134] O excesso de processamento tem valor econômico, logo a superficialidade é relacionada à métrica da necessidade.

deles nas tecnologias, concretamente, não é trivial[135]. Neste ponto, amplia-se o debate de como as garantias jurídicas podem/devem ser implementadas por desenvolvedores de tecnologia.

Todavia, ainda que o princípio da finalidade seja aplicável aos âmbitos público e privado, a camada de intervenção informacional é distinta, conforme explicado no Capítulo 1. Por essa razão, este capítulo é subdividido em dois grandes tópicos: a coleta privada e a coleta pública. Isso decorre do fato de que a primeira camada de intervenção, fundada na finalidade de segurança pública, não pode coletar quaisquer dados pessoais, na medida em que eles precisam ser previamente úteis; por exemplo, o Estado não consegue justificar a coleta de dados sobre o gosto musical dos cidadãos.

Por outro lado, a coleta privada é justificada por interesses econômicos de empresas e particulares, sendo derivada do consentimento. Por paralelismo, utilizando o mesmo exemplo acima, particulares podem ceder dados sobre seus gostos musicais a empresas de streaming que, eventualmente, podem ser acessados no âmbito do processo penal, a depender da hipótese investigativa. Como mencionado, esse tipo de acesso pressupõe uma investigação individualizada e deve ocorrer por meio de instrumentos investigativos específicos, isso significa que a arquitetura privada não é separada, em absoluto, da persecução criminal.

Em suma, a arquitetura de dados privada também pode ser útil para investigações criminais, por isso é importante entender em linhas gerais como ela é criada, especialmente porque ela é objeto de política regulatória. No mesmo sentido, a arquitetura pública existe em razão da política de segurança pública e se conecta logicamente ao processo penal quando infrações penais são cometidas, portanto, a utilidade é aspecto imprescindível para sua criação legal em primeiro momento.

2.1. A coleta privada como intervenção informacional

Os grandes agentes de tratamento privados coletam uma gama de dados pessoais a fim de permitir "construct profiles of people, learn about their preferences, habits, and purchases, and use this information to conduct targeted marketing campaigns designed to get the customers/consumers

---

[135] "*The apparent solution proposed by regulators now, but barely specified, is Privacy by Design (PbD). At first sight, the powerful term seems to suggest we simply need to take a few Privacy-Enhancing Technologies (PETs) and add a good dose of security, thereby creating a fault-proof systems' landscape for the future. But the reality is much more challenging*.". SPIEKERMANN, Sarah. The Challenges of Privacy by Design. Communications of the ACM, v. 55, n. 7, p. 26-28, July 2012.

to make more purchases that benefit companies"[136]. Nesse sentido, o objetivo das empresas é coletar o dado como um ativo econômico, que sirva como elemento de vantagem competividade no mercado, que é um marcador da economia movida a dados.

Nesse âmbito, os particulares cedem suas informações para empresas para que elas ofereceram produtos e serviços, cuja base jurídica é o consentimento, mas essa relação jurídica não está alheia a problemas jurídicos, especialmente em razão risco à privacidade dos usuários. A quantidade de dados produzida e armazenada por *Big Techs* permitem a vigilância privada, que é uma intervenção informacional tão grave quanto a vigilância estatal[137]. Esse risco decorre principalmente da coleta e consolidação de dados desconectados da finalidade inicial de coleta pelas empresas.

Diante do cenário econômico, em que a autonomia individual é privilegiada, a tese optou por descrever a coleta privada negativamente, isto é, pela descrição dos limites principiológicos e jurídicos que são impostos às empresas. Ao fazer isso, o objetivo é que os inúmeros exemplos de coleta sejam medidos por essa métrica, ao contrário de criticar especificamente como cada tipo de coleta pode significar uma intervenção informacional indevida.

Além disso, a discussão é colocada na intersecção entre direito e ciência da informação, de modo que a aplicabilidade dos preceitos jurídicos seja analisada levando em consideração os limites tecnológicos. O enfoque é no desenvolvimento de produtos digitais online, que se justifica, como se verá adiante, no interesse das agências de persecução de acessar dados de conteúdo e metadados de comunicação vinculado a esse uso dos usuários.

O conceito-referência para fazer esse debate é a privacidade por design, "privacy by design" (PbD), que é atribuído à Ann Cavoukian. A autora defendeu a ideia de que sistemas de tecnologia deviam ser concebidos/produzidos com preocupações sobre privacidade no desenho do produto. Para tanto, ela desenvolveu sete princípios fundamentais: i) proativo, não reativo; ii) privacidade como padrão; iii) privacidade embutida no design; iv) funcionalidade total, v) proteção ponta a ponta; vi) visibilidade e transparência e; vii) respeito pela privacidade do usuário[138].

Antes de adentrar no significado prático de cada um dos princípios, é necessário reconhecer,

---

[136] MARAS, Marie-Helen; WANDT, Adam Scott. Enabling mass surveillance: data aggregation in the age of big data and the Internet of Things. Journal of Cyber Policy, [s. l.], v. 4, n. 2, p. 160, 17 mar. 2019.
[137] MARAS; WANDT, 2019, p.160.
[138] CAVOUKIAN, Ann. Privacy by Design: The 7 Foundational Principles. Toronto: Information & Privacy Commissioner of Ontario, 2011.

que apesar das limitações e variadas críticas, o PbD serviu como elo de contato entre pesquisas em tecnologias da informação e do campo jurídico. Um exemplo nítido é que o excesso de dados é metrificado por físicos estatísticos, matemáticos e outras áreas, para discutir o ponto ideal de coleta, que tecnicamente é aquele que permite inferências corretas, alinhado juridicamente com a necessidade de processar a menor quantidade de dados[139]. É, portanto, um paradigma.

Outra necessária a distinção a ser feita é entre segurança e privacidade, que são trabalhados indistintamente por alguns autores; segurança é uma das formas de efetivação da privacidade, logo é impensável PbD sem governança de segurança. Não são sinônimos, mas retroalimenta-se conceitualmente, Spiekermann elucida a questão[140]:

> […] Security and privacy in this view are clearly distinguished. Security means the confidentiality, integrity, and availability of personal data are ensured. From a data protection perspective security is one of several means to ensure privacy. A good PbD is unthinkable without a good Security by Design plan. The two approaches are in a "positive sum" relationship.

O objetivo do PbD deve ser entendido como a tentativa de que as prescrições jurídicas encontrem ressonância nas práticas no *design-thinking* de soluções tecnológicas. A proteção à privacidade e segurança devem ser os padrões de desenvolvimento de *softwares*. Assim, o direito também deve ser permeável aos limites apontados por outras áreas do conhecimento, e caso o risco não seja tolerável, regular pode não ser suficiente, devendo-se proibir determinada utilização. Para facilitar a compreensão, estruturaram-se os sete princípios, na tabela abaixo[141]:

Tabela 1 - Princípios do Privacy by Design

Princípio	**Conteúdo**
i) Proativo, não reativo	o PbD deve antecipar e prevenir os riscos à privacidade, não deve, portanto, esperar que os riscos se materializem. O PbD ocorre antes do fato ilícito.

[139] SHANMUGAM, Divya et al., 2022, p. 11.
[140] SPIEKERMANN, 2012, p. 40.
[141] CAVOUKIAN, 2011, p. 1-5.

ii)	Privacidade como padrão	PbD almeja entregar o máximo de privacidade, assegurando que os dados pessoais são protegidos automaticamente em qualquer tecnologia da informação ou prática comercial. Nenhuma ação do titular dos dados é necessária para a manutenção da privacidade, essa é a forma que o sistema funciona por definição, que se implementa como com as seguintes FIPs (*Fair Information Practices)*: finalidades, limitação de coleta, minimização, retenção e limitação ao acesso.
iii)	Privacidade embutida	PbD deve estar no desenho e arquitetura dos sistemas de informação, que é implementada sem diminuição das funcionalidades.
iv)	Funcionalidade total	PbD tem como objetivo que todos os interesses legítimos e objetivos sejam acomodados em uma soma positiva, sem fazer-se desnecessários *trade-offs.* Evita especialmente a falsa dicotomia entre privacidade e segurança, demonstrando que é possível ter ambos.
v)	Proteção ponta a ponta	A privacidade deve ser implantada com PbD antes que o primeiro do dado seja coletado, estendendo segurança ao longo de todo o ciclo dos dados, com técnicas apropriadas para garantir a privacidade. Isso garante que todo dado retido está seguro e deve ser apagado ao fim do tratamento.
vi)	Visibilidade e transparência	PbD busca assegurar a todos os *stakeholders* que, independente da política comercial e tecnologia envolvida, as tecnologias implementadas estão operando conforme as promessas e objetivos.
vii)	Respeito pela privacidade do usuário	PbD exige que a arquitetura de sistemas e os operadores mantenham o interesse em proteção da privacidade dos usuários, oferecendo privacidade como padrão, a exemplo de notificações e fortalecendo interfaces amigáveis para tomada de decisão (consentimento, revogação).

Fonte: elaborado pelo autor

Como se pode ver, alguns dos princípios são muito amplos, a exemplo do quinto, que

prescreve a funcionalidade total das tecnologias da informação com a proteção da privacidade e segurança no desenho do produto. A afirmação teórica é a proposição de um modelo ideal, mas deve-se discutir a possibilidade técnica de implementá-la, até porque a primeira proteção é a coleta zero de dados, que pode ser conseguida por meio da organização informacional das soluções (*Technical and Organizational Measures*): que permitem anonimização, pseudonimização etc.[142]

Apesar das críticas, geralmente vinculadas à vagueza dos princípios, o PbD é reconhecido como boa prática para limitar a coleta e processamento de dados, sua lógica está presente em vários contextos, como no conceito "*security by design*", que é utilizado como padrão de certificação pela ISO[143]. A respeito da normatividade do PbD, a União Europeia aplica a regulação por princípios, que permite adaptabilidade com novas tecnologias, e as ideias gerais do PbD estão claramente presentes no artigo 25º da GDPR e art. 20º da LED, ideia que já era presente na Diretiva 95/46/EC[144].

Ambos os dispositivos legais preveem que a proteção de dados é implementada "by design" e "by default". O modelo brasileiro, que é inspirado no direito do bloco europeu, também fez escolhas legislativas semelhantes, que podem ser encontradas no artigo 50 da LGPD, que estabelece as boas práticas para o desenvolvimento e implementação de tecnologias da informação. Ademais, o anteprojeto da comissão de juristas também introduziu essa ideia no eixo a respeito da segurança da informação, prescrevendo a privacidade e segurança por desenho e padrão.

Assim, discutir o alcance das práticas de PbD não é um debate puramente acadêmico e teórico, foi imposto legislativamente como um dever jurídico ao setor interessado, e será objeto de manifestações de agências especializadas, tanto para autorizar determinadas tecnologias quanto para punir empresas por descumprimento legal. Diante disso, é incontornável a discussão sobre atual estágio de desenvolvimento técnico de PbD para discutir a eficácia jurídica da regulação por princípio, que vedam ao excesso de coleta e do desvio de finalidade em relação a ela.

2.1.1. Paradoxo do PbD como estratégia de regulação

---

[142] RUBINSTEIN, 2011, p. 1420.
[143] ISO/IEC/27001, International Organization for Standardization.
[144] UNIÃO EUROPEIA. Parlamento Europeu. Conselho. Diretiva 95/46/CE, de 24 de outubro de 1995. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. *Jornal Oficial das Comunidades Europeias*, Luxemburgo, L 281, p. 31-50, 23 nov. 1995.

Os exemplos de modelos regulatórios citados são por princípios. A demonstração do conteúdo dos sete princípios de PbD são criticados por serem vagos. Esse estado de coisas exige um debate em concreto das ferramentas técnicas que efetivam o PbD: as PETs (*Privacy Enhancing Technologies*). Por questões didáticas, a discussão será orientada pela implementação do cartão eletrônico de saúde na Alemanha, cujo nome gera o acrônimo ELENA, que será usado a partir de agora como *case* para endereçar as discussões práticas sobre privacidade por padrão.

Uma premissa inicial que deve estar presente no ideário dos juristas ao discutir os padrões de privacidade e segurança é que não se pode presumir que os desenvolvedores de soluções sabem como o fluxo de dados ocorre. Ao contrário, "data is like water: it flows and ripples in ways that are difficult to predict. As a result, even a well-conceived, general, and sustainable privacy regulation (…) struggles to ensure its effectiveness"[145]. Naturalmente, a compreensão dessa premissa não deve impedir a verificação concreta de responsabilização.

As empresas também têm interesse em desenvolver produtos que estão nos limites da regulação, com objetivo de não restringir seus modelos de negócios[146], especialmente porque as consequências do dano reputacional são pequenas economicamente[147]. Além disso, os produtos de tecnologia cuja privacidade é o principal modelo de negócios não atraem muitos usuários[148]. Assim, se o dano reputacional é baixo e os produtos com esse modelo não atraem, pode-se inferir que privacidade e segurança não são os principais fatores de escolha dos usuários[149].

Voltando ao caso de estudo, ELENA é um cartão eletrônico (*e-card*) de saúde implementado na Alemanha, que tem um microprocessador com interoperabilidade com outros sistemas, a exemplo de verificar a identidade do usuário com planos de saúde[150]. Os dados relacionados à prescrição médica, prontuário eletrônico, histórico de emergências, dentre outros, poderiam ser adicionados a esse *e-card*. ELENA, portanto, é um sistema crítico de processamento de dados porque coleta principalmente dados sensíveis relacionados à saúde dos cidadãos.

---

[145] SPIEKERMANN, 2012, p. 38.
[146] SPIEKERMANN, 2012, p. 39.
[147] De acordo com Spiekermann, "*Unfortunately, we still have too little knowledge about the real damage that is being done to brands and a company's reputation when privacy breaches occur. The stock market sees some negligible short-term dips, but people flock to data-intensive services (such as social networks); so far, they do not sanction companies for privacy breaches*", (*Ibid.,* p. 40).
[148] GOLDBERG, Ian. *Privacy Enhancing Technologiesfor the Internet III.- Ten Years Later, in* DIGITAL PRIVACY: THEORY, TECHNOLOGIES, AND PRACTICES 3, 2007, p. 4-5.
[149] Outra hipótese é que o dano reputacional seja baixo porque há pouco debate sobre direitos e as violações coletivas.
[150] SCHAAR, 2010, p. 268.

A primeira observação a ser feita é que a implementação de um novo sistema deve gerar, no mínimo, o mesmo grau de proteção existente no modelo existente – tal como exemplo citado do estacionamento na Bélgica. Essa questão geralmente não é colocada, partindo-se somente da premissa que o ganho de eficiência justificaria a implementação de tecnologias. Dessa forma, a constatação de que a coleta desses dados de saúde teria padrões inferiores de limitação à coleta do sistema anterior teria de levar a decisão política de não o implementar por inadequação funcional.

Outra premissa do desenvolvimento da ELENA foi que os usuários devessem ter controle sobre os dados em todas as funcionalidades escolhidas, sendo capazes de decidir a quantidade de dados relativos à saúde deveriam ser armazenados no *e-card*[151]. Essa premissa implica que o desenvolvimento priorize uma interação com usuário para que ele possa entender as decisões que está tomando sobre seus dados, para tanto, a interface deve ser amigável; um exemplo técnico é abas de seleções de *cookies*, em que se pode optar, entre *opcionais, obrigatório e todos os cookies*.

De acordo com Peter Shaar, todos os atores envolvidos no projeto aceitaram desenvolvê-lo a partir dos seguintes princípios: soberania dos dados, voluntariedade, extensão dos dados, limite de acesso, direito à informação e checagem de acessos[152]. Isso significa que os provedores de serviços devem permitir, por meio técnicos, a proteção dos dados dos usuários, com utilização de criptografia, controle de acessos e disposições de uso anônimo. O desenho do produto partiu da concepção que o usuário tem o controle sobre a informação, permitindo-se ou não a coleta.

Ademais, a segurança do sistema foi um elemento central, na medida em que falhas nessa etapa vulneram todos os controles anteriores. Assim, o prazo de validade de certificados não deve ser muito longo, considerando que os sistemas computacionais ganham capacidade de processamento, o que faz com que a força das barreiras de segurança decaia relativamente[153]. Por essa razão, os sistemas devem ser desenvolvidos de forma a permitir a optimização e inclusão de novas técnicas de segurança, sob pena de se tornarem obsoletos pelos apontados riscos.

Um outro princípio que orientou o desenvolvimento da ELENA é relevante para a discussão da coleta no âmbito público, que é a utilização de técnicas que garantam que “that data are used only for the purpose for which they were collected, and in particular that no access is given to the security authorities, tax authorities, Customs, and the like”. No trecho, há a clara preocupação com

---

[151] SCHAAR, 2010, p. 268.
[152] SCHAAR, 2010, p. 269.
[153] SCHAAR, 2010, p. 271.

o conceito de separação informacional, que é essencial na coleta de dados para persecução penal porque o Estado não deve ser visto unitariamente ao se tratar de tratamento de dados.

Em outras palavras, o reúso de dados pessoais coletados para finalidades diversas não pode ser ilimitado, tendo em vista que as agências estatais exercem diferentes finalidades. Neste ponto, pode-se fazer a diferenciação entre as ações de prevenção e persecução penal, que olham para o futuro para prevenir riscos e para o passado para responsabilizar por ilícitos, respectivamente. Assim, o dado fiscal sob custódia da Receita Federal não pode ser acessado livremente pelas autoridades de persecução, o que só deve ocorrer nas hipóteses legais.

No âmbito penal, algumas restrições se aplicariam aos princípios que orientaram a ELENA, por exemplo, o controle sobre os dados não pode ser total, na medida que o consentimento não é o conceito que rege a coleta por agências de persecução, e sim a autorização legal. Ademais, a voluntariedade estaria conectada à faculdade processual de produzir provas, mas em regra, a prova penal se produz sem a sua observância, tais como os meios de ocultos de prova. Portanto, há informações que devem ser coletados e armazenadas por imperativo legal, que não permitem as referidas características.

Os princípios de PbD que orientaram o *e-card* alemão são implementados em produtos digitais por meio de TOMs (*Technical and Organisation Measures*). Como o nome indica, as TOMs podem ser tecnologias da informação (criptografia, direitos de acesso de sistema) ou medidas organizacionais (políticas de privacidade, compliance com a legislação cogente, treinamento das equipes envolvidas). Especificamente a respeito de coleta de dados pessoais, as técnicas mais relevantes para o *privacy by design* são as PETs (*Privacy-Enhancing Technologies*) [154].

O objetivo dos desenvolvedores ao implementar PETs no desenvolvimento de produtos é permitir que as empresas que dependem de processamento de dados como modelo de negócio tenham práticas informacionais justas, as FIPs em inglês[155]. Comumente, autores trabalham PbD e PETs como sinônimos, o que é impreciso teoricamente, estas são técnicas que implementam aquela, que passaram a ser dever legal, tendo em vista sua adoção em modelos regulatórios de dados[156]. Portanto, a boa compreensão das técnicas permite a discussão do objetivo regulatório.

Rubinstein defende que que as PETs devem ser diferenciadas em dois tipos, substitutivas e

---

[154] Conceitualmente, toda PET é uma TOM, esta, portanto, é gênero daquela.
[155] Fair Information Practices (FIPs)
[156] RUBINSTEIN, 2011, p. 1410.

complementares. As primeiras são usadas para "to protect privacy by blocking or minimizing the collection of personal data, thereby making legal protections superfluous"[157], que objetivam a coleta-zero de dados. Já as PETs complementares permitem a coleta de dados "as long as these activities are consistent with privacy laws and related statutory requirements"[158], enfatizam o controle sobre o dado e garantem técnicas de segurança do sistema de informação.

A utilização de PETs como estratégia regulatória ocorre pelo menos desde 1995. Em regra, elas refletem avanços tecnológicos, a criptografia é um ótimo exemplo dessas possibilidades, que protege o conteúdo de aplicativo de mensagens de ponta a ponta, pagamentos anônimos, proteção da identidade online, dentre outros[159]. De forma geral, as PETs substitutivas permitem o anonimato do usuário de produtos de tecnologias, logo a proteção relativa à coleta abusiva é a impossibilidade de tratá-lo individualizadamente em primeiro lugar; o dado coletado não seria pessoal juridicamente.

Como visto, as PETs não se resumem à garantia de anonimato. As PETs complementares aumentam a possibilidade de conhecimento e controle sobre a coleta com estratégias de usabilidade amigável e preservação da segurança dos sistemas de informação. Por exemplo, a interface gráfica do aplicativo deve ser pensada para informar o tipo de processamento que será feito e conseguir o consentimento válido do usuário do produto. A não observância de ambas as fases leva a um consentimento inválido, por derivar de uma decisão não informada do usuário.

Mais estruturalmente, PETs complementares podem ser utilizadas na infraestrutura de processamento e transmissão de dados (*back-end infrastructure*), que permitem que agente de tratamento gerencie a identidade de usuários, direitos de acesso, políticas de privacidade etc. [160] Essas soluções são imprescindíveis para que exista interoperabilidade entre sistemas de diferentes empresas, tal como ocorreu com as linhas de celulares no Brasil e, mais recentemente, com o *open finance* – transferência de dados bancários entre instituições brasileiras.

A síntese da argumentação é que os sistemas de informação devem ser projetados com preocupações inerentes à privacidade e à segurança desde a concepção, princípio identificado como PbD. O enfoque é reduzir a coleta de dados ao mínimo operacional. Nesse sentido, as TOMs (tecnologias e medidas organizacionais) são instrumentos para alcançar esses objetivos, que são

---

[157] RUBINSTEIN, 2011, p. 1417.
[158] RUBINSTEIN, 2011, p. 1417.
[159] RUBINSTEIN, 2011, p. 1415.
[160] RUBINSTEIN, 2011, p. 1418.

empregadas pelo setor regulado para se adequar à regulação setorial sobre privacidade e segurança. Naturalmente, cada ordenamento pode adotá-las distintamente em suas estratégias.

O direito da União Europeia apresenta a tendência de avaliar as PETs como "a useful complement to existing regulatory and self-regulatory approaches", enquanto as autoridades americanas as veem como opção à intervenção regulatória[161]. A divergência está centrada na defesa da autorregulação ou regulação estatal. Tomando o debate de boa-fé, parece que há poucos incentivos de mercado para que a autorregulação seja efetiva, já que não há evidência de que haja impacto financeiro relevante em razão de falhas de segurança e brechas de privacidade.

Ademais, a opção de mercado tende a ser a utilização de PETs complementares, na medida em que permitem comunicar aos clientes preocupações de segurança e privacidade, sem perder a possibilidade de processar dados não anonimizados. O custo de oportunidade de não coletar é injustificável em razão da baixa demanda por produtos de privacidade baseados em PETs substitutivas[162], que pode ter como hipótese de explicação o baixo letramento do cliente-médio de como as empresas de tecnologia captam dados para oferecer produtos customizados.

Os princípios orientadores da implementação da ELENA na Alemanha derivam, em primeiro plano, dos deveres jurídicos impostos aos entes públicos e privados. Idealmente, tais deveres são alcançados com a utilização do PbD no desenho de produtos. No mesmo sentido, as técnicas adotadas por desenvolvedores permitem diferentes graus de privacidade e segurança, que podem ser objeto de regulação setorial ou de escolhas empresariais. Contudo, como articulado, não parece haver incentivos de mercado para orientá-las a mais proteção.

Se não há incentivos de mercado, a privacidade como elemento necessário das estruturas de captação de dados constitui um dever regulatório do Estado, na medida em que a autorregulação, nesse particular, é antieconômica, pois limita a aquisição de dados pessoais enquanto ativos econômicos. No mesmo sentido, a utilização do consentimento não é suficiente para evitar intervenções informacionais injustificadas, especialmente porque o usuário não tem conhecimento do ecossistema de dados de que as empresas dispõem, de modo que não pode prever as correlações possíveis com os dados cedidos, mesmo considerando um cenário de elevado letramento digital.

Por fim, a regulação pelos princípios de PbD foi qualificada como paradoxal no título do

---

[161] BENNETT, Colin J.; RAAB, Charles D. The Governance of Privacy: Policy Instruments in Global Perspective. [s.l.]: MIT Press, p. 180-202, 2006.
[162] RUBINSTEIN, 2011, p. 1444.

tópico. Isso decorre do fato de que a regulação da proteção de dados no âmbito privado visa a garantir que os produtos captem apenas o mínimo de dados necessários e que as empresas utilizem estratégias organizacionais de privacidade. Contudo, ao mesmo tempo, as agências estatais almejam acesso a essas informações em investigações criminais, além de criar contrapontos jurídicos para sua completa anonimização, com se verá adiante. De certo modo, o mesmo Estado que protege o cidadão contra as empresas, utiliza as bases informacionais destas como instrumento probatório.

2.2. A coleta pública como intervenção informacional

Os cidadãos cedem informações pessoais ao Estado desde o nascimento até a morte[163]. Não há exagero nessa afirmação, pois o exercício dos direitos civis depende, invariavelmente, do reconhecimento estatal: não basta nascer, é necessário o registro público desse nascimento. Essa é a principal distinção entre a privacidade no âmbito privado e no público: no primeiro, a cessão de dados pessoais é, em alguma medida, opcional; no segundo, é obrigatória. Entre as razões dessa obrigatoriedade, destaca-se o dever/poder do Estado de exercer a persecução penal.

Ainda que seja virtualmente impossível não ceder dados pessoais às empresas de *Big Techs*, dadas as limitações que isso traria à vida diária, é possível afirmar, teoricamente, que há um espaço de escolha. Afinal, nenhum exercício de direito depende do acesso a redes sociais para sua eficácia. Por outro lado, o Estado exige a coleta de dados de trabalho, renda, localização, seguridade social, registros públicos de diversas naturezas como condição para os exercícios de direitos. Essa exigência, porém, conflita com os ideais de PbD, discutidos no tópico acima.

Como visto, as PETs substitutivas têm como finalidade de garantir o anonimato dos usuários de serviços de tecnologia, configurando-se como a forma mais eficaz de preservação da privacidade, já que impedem a coleta de informações individualizáveis. Spierkamann conceitua a privacidade digital justamente como a escassez da coleta e reúso de dados, aliada à maximização do controle individual[164]. Nesse ponto, o PbD vai de encontro ao interesse legítimo do Estado-penal em estabelecer deveres de coleta por órgãos públicos e setores privados regulados.

O conflito fica evidente quando se observa o modelo de práticas proibidas pela FTC

---

[163] DEGRAVE, 2024, p. 11.
[164] SPIEKERMANN, 2012, p. 39.

(*Federal Trade Commission*) nos Estados Unidos no desenvolvimento de produtos digitais. O conteúdo de PbD também pode ser depreendido a partir das práticas indesejáveis, que são precisamente aquelas que ensejam debate para uso pelo Estado para fins penais[165]:

> […] Also instructive are some half-dozen "spyware" and "adware" enforcement actions suggesting prohibited design practices or required disclosure practices. In the prohibited category, the FTC [Federal Trade Commission] has brought several cases involving the alleged practices of (1) installing software without a user's consent by exploiting security vulnerabilities; (2) bundling software with malware; and (3) installing root kit software. In the required category, several additional cases concern allegations of failing to clearly and conspicuously disclose (4) the bundling of free software with malware; (5) all the features of a program (such as content protection or "phone home" features); (6) the types of data that certain tracking software will monitor, record, or transmit; and (7) the means by which consumers may uninstall any adware or similar programs that monitor internet use and display frequent, targeted pop-up ads.

O trecho destaca a instalação de softwares sem o consentimento do usuário, especificamente o uso de *malware* e a instalação de *rootkit*. O que o autor está afirmando é que empresas não devem aplicar técnicas que maximizem a coleta de dados dos usuários, com a utilização de programas que invadem dispositivos eletrônicos. Entretanto, este é precisamente o conteúdo do que a invasão de dispositivos eletrônicos pode significar. Esse tema será aprofundado no Capítulo 5, dedicado aos debates sobre a legalidade da infiltração digital, mais especificamente sobre o use de *spywares* como método oculto de obtenção de provas em investigações criminais.

A reflexão permite concluir que mesmo que a política regulatória do setor privado objetivasse o uso de PETs de forma obrigatória sempre que possível, ela seria incongruente com os determinados objetivos legítimos do Estado. A assertiva não está subordinada ao âmbito de coleta na internet, que é ponto mais conectado com produtos digitais. Por exemplo, a lei n. 14.478/22 regulamentou o mercado de criptomoedas que, entre seus efeitos, exige autorização para atuar no setor e regulação da lei para identificação de proprietários e valores movimentados[166].

Do ponto de vista técnico, as criptomoedas não dependem de identificação dos proprietários para funcionarem. Sua operação ocorre por cadeias de *blockchain*, validadas descentralizadamente por diversos computadores autônomos. Entretanto, a possibilidade de que sejam usadas para fins

---

[165] RUBINSTEIN, 2011, p. 1428.

[166] Inserção do inciso XIX, parágrafo único, do art. 9º, da lei 9.613/1998. (BRASIL. Lei nº 9.613, de 3 de março de 1998. Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras - COAF, e dá outras providências. *Diário Oficial da União*, Brasília, DF, 4 mar. 1998).

ilícitos gera o interesse do Estado em impor o registro público, que passa a determinar, portanto, que as empresas coletem informações de identidade e transações. Em outras palavras, a criação das bases de dados sobre essas informações é uma escolha de política criminal informacional.

Adiante será discutida em detalhes a formação de bases de dados por órgãos do poder público e por particulares, mas o que interessa nesse momento é que a solução dada aos criptoativos não serve para todas as hipóteses em que o Estado tem legítimo interesse de acesso. Assim, mesmo que os produtos de tecnologia devam ser pensados desde a concepção para garantir privacidade e segurança, por exigência legal, as ações estatais conflitam com o uso de determinadas ferramentas para o aumento de privacidade; o uso da criptografia é elucidativo.

De acordo com Liguori Filho e Salvador[167]:

> […] Esse cenário ensejou um debate sobre a necessidade ou não de regular, por meio do Direito, o desenvolvimento, implementação e utilização da criptografia, de forma a viabilizar o acesso a dados por autoridades de investigação em determinados casos, resguardando, assim, a segurança pública. A questão é que esta restrição pode gerar severas consequências na integridade dos sistemas criptográficos, fragilizando sua segurança e potencialmente viabilizando violações à privacidade (novamente) por parte de criminosos e governos.

Há muito se conhece o debate entre Estados e empresas de tecnologia sobre utilização de criptografia forte para impedir o acesso a dados de conteúdo coletados por empresas[168]. Nos anos noventa, a política americana usava os regimes de exportação para proibir a venda de produtos criptográficos[169], solução que dependia, naturalmente, de hegemonia tecnológica. A nova página dessa discussão se deu com a ascensão das *Big Techs,* que passaram a utilizar a criptografia por padrão em sistemas operacionais e em produtos digitais, reavivando as *crypto wars*[170].

Essa situação se refere a dados custodiados por agentes privados, que são coletados, retidos e tratados por finalidades econômicas que, presumindo-se a aderência legal, foram coletados com consentimento dos clientes. É inevitável que essas informações possam ser elementos úteis para

---

[167] LIGUORI FILHO, Carlos Augusto; SALVADOR, João Pedro Favaretto. Crypto wars e bloqueio de aplicativos: o debate sobre regulação jurídica da criptografia nos Estados Unidos e no Brasil. Revista da Faculdade de Direito UFPR, [S. l.], v. 63, n. 3, p. 137, 2018.

[168] MCCARTHY, H. J. Decoding the encryption debate: Why legislating to restrict strong encryption will not resolve the "going dark" problem. Journal of Internet Law, 20(3), 2016.

[169] LIGUORI FILHO; SALVADOR, 2018, p. 140.

[170] De acordo com Liguori e Salvador: "*Nos Estados Unidos, esse debate surge na década de 1990, no início da popularização da internet como principal meio de comunicação e da popularização de instrumentos criptográficos para uso privado nas interações online–estas ficaram conhecidas como crypto wars*". (LIGUORI *Ibid*., p. 137)

persecução penal na medida em que empresas coletam grandes volumes de dados comportamentais e registros comunicacionais. Entretanto, o acesso a elas por terceiros, inclusive o Estado, pode ser tecnicamente impossível a depender da utilização de PETs pelas empresas desenvolvedora do produto. Esse fato ensejou o debate regulatório de proibir o uso criptografia no Estados Unidos, que foi superado politicamente após o escândalo de espionagem do *Wikileaks.*

Os aplicativos de mensagens instantâneas com criptografia forte de ponta a ponta estão no centro desse debate, a exemplo do *Whatsapp* e do *Telegram*. Nesse contexto, as empresas sustentam que é tecnicamente impossível ter acesso aos dados de conteúdo dos clientes, que só é disponível os usuários das pontas da comunicação que possuem a chave de decriptação. No Brasil, esse tipo de resposta levou a bloqueios do *Whatsapp* entre 2015 e 2016. Nos Estados Unidos, a problemática opôs as *Big Techs* e o FBI, que tentam exigir abertura de dados ou disponibilização de acesso por *backdoor* nos aplicativos para investigações criminais[171].

Os modelos regulatórios da criptografia variam amplamente, incluindo proibições de criptografia forte, autorizações prévias para o uso de mecanismos criptográficos, imposições de assistência e estímulos ao uso de criptografia[172]. Como se pode ver, a variação dessas escolhas são um preciso exemplo da política criminal informacional trabalhado no capítulo anterior, uma decisão *ex ante* que determina quais tipos de tecnologia podem ser utilizadas para desenvolvimento de produtos digitais para os quais é imprescindível tratamento de dados pessoais.

A privacidade que os sistemas possibilitam são defendidos como ativos econômicos das empresas que as utilizam, de modo que o acesso do Estado poderia ser visto como desincentivo à privacidade e ao desenvolvimento de novas tecnologias. A situação opõe os interesses econômicos das empresas aos interesses/deveres legítimos dos Estados em relação à segurança pública e à persecução penal. Assim, as exigências de política criminal informacional também condicionam a forma como as empresas de tecnologia devem organizar suas estruturas de dados.

No limite, isso quer dizer que o desenvolvimento de soluções digitais que coletam e tratam dados pessoais deve considerar a política regulatória setorial de como implementar segurança e privacidade no desenho do produto, a exemplo da LGPD no Brasil. Ao mesmo tempo, a depender do setor econômico que operem, ou o tipo de solução fornecida aos consumidores, também devem

---

[171] ENDELEY, Robert E. End-to-End Encryption, Backdoors, and Privacy. 2019. Dissertação (Doutorado em Cibersegurança) - Capitol Technology University, Laurel, 2019 p. 5-6.
[172] LIGUORI, 2023, p. 214-231.

se ater à política criminal informacional, que pode se manifestar com o dever de criar banco de dados ou limites à utilização de determinadas tecnologias.

Por fim, no tópico a seguir, a tese passa a expor as características das bases de dados que o Estado pretende acessar, as quais incluem: as privadas, as privadas criadas por dever legal e as públicas. O objetivo é demonstrar as diferentes estratégias regulatórias disponíveis ao Estado para a produção probatória cujo objeto são dados pessoais.

2.3. Pretensão de reúsos de dados pessoais pelo Estado

Até o momento, este capítulo analisou de que forma a política regulatória setorial pretende garantir a privacidade dos clientes de produtos de tecnologia, que pressupõe que a coleta de dados está sendo realizada por empresas para finalidades econômicas. Ademais, verificou-se que a política criminal informacional pode ser responsável por cria contrapesos aos referidos interesses regulatórios, na medida em que a identificação de usuários pode ser de interesse penal, o que leva à limitação de instrumentos técnicos para garantir o anonimato digital.

O dado digital de interesse de persecução penal é o pessoal, uma vez que a identificação do usuário por trás do hardware é etapa imprescindível em investigações criminais. Isso reforça a necessidade de tutela penal dos dados para garantir direitos fundamentais. Os exemplos citados nos tópicos anteriores, a cessão de informação para registros públicos e o acesso a dados retidos por empresas, correspondem a formas de coleta feitas pelo poder público. Contudo, deve ser destacado que tais dinâmicas exemplificam somente a uma das estratégias disponíveis.

O ingresso de dados pessoais no processo penal varia conforme a origem dos repositórios informacionais, e essas diferentes fontes influenciam tanto as formas de acesso quanto, em alguns casos, a sua própria impossibilidade. Neste contexto, a tese diferencia o repositório de dados coletados em três tipos: base de dados gerida pelo poder público – única em que a coleta é realizada diretamente por agências estatais –, base de dados criada por entes privados por dever legal, base de dados privada. Essa separação objetiva a possibilidade de realizar prescrições gerais de como meios de investigação devem ocorrer a partir dessas características centrais.

Tecnicamente, base de dados pode ser definida como “[...] uma coleção de informações

armazenadas como dados num sistema informático"[173], que se subdividem em dados relacionais – lidos estruturadamente por uma linguagem computacional – ou não relacionais – que suportam uma variedade de dados diferentes entre si. Parte dessas coleções de informações são úteis como fonte de prova digital no processo penal, por seguirem uma "lógica que procura proporcionar a extração de do máximo de proveito possível a partir de um conjunto de informações"[174].

Nos Capítulos 4 e 5, o acesso a esses bancos de dados será detalhado, quando se versará especificamente sobre os meios de obtenção de provas digitais para a investigação preliminar. Neste momento, o objetivo é entender a arquitetura informacional do Estado, que como dito anteriormente, utiliza informações coletadas por suas próprias agências e por particulares, especificamente empresas de setores econômicos relevantes. Dito de outra forma, todo acesso a dados coletados, público ou privadamente, para finalidade distinta é reúso de dados e configuram uma nova intervenção informacional.

Naturalmente, o interesse penal de acesso a essas informações nasce do fato-crime, e os critérios de legalidade e legitimidade para tanto dependem de diversos fatores, inclusive a gravidade em abstrato da infração penal, isto é, a descrição da existência desses repositórios informacionais não se confunde com a defesa de que são necessariamente acessíveis na investigação preliminar. Ademais, para cada tipo de banco de dados, haverá um meio jurídico distinto para garantir acesso, ressalvando-se as hipóteses a impossibilidade técnica.

Antes de explicar cada tipo especificamente, é importante ressaltar que as bases são constituídas com dados digitais e informações. No texto, a utilização da terminologia base de dados decorre do fato de que, com a digitalização das atividades estatais, a forma de organizá-las passa a ser em linguagem estruturada de dados. Assim, ainda que o acesso às informações cartorárias seja através de certidão pública (informação), sua estruturação digital ocorre com a criação de bases unificadas em formato de linguagem legível por máquina, armazenados em banco de dados.

2.3.1. Base de dados públicas

[173] Conceito utilizado comercialmente pela Microsoft (MICROSOFT. O que são bases de dados? [S. l.: s. n., s. d.]. Disponível em: https://azure.microsoft.com/pt-pt/resources/cloud-computing-dictionary/what-are-databases. Acesso em: 05 jan. 2025.

[174] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. Espaço Jurídico Journal of Law [EJJL], [S. l.], v. 12, n. 2, p. 92, 2011.

As bases de dados geridas pelo poder público são criadas por lei para o cumprimento de finalidades públicas, registro civil das pessoas e de propriedade de imóveis[175], informações fiscais[176], propriedade de bens móveis[177]. Essas bases não existem em razão das finalidades penais, elas estão conectadas com os inúmeros direitos cuja fruição depende da linguagem do direito, logo os particulares cedem essas informações como condição da vida cidadã. Ademais, a criação desses registros deve ser entendida em conjunto às leis que determinam a digitalização do Estado.

Os exemplos dessas bases são inúmeros, por isso a tese foca nas que são de interesse para fins de prevenção e persecução penal. Desde 2020, os cartórios de registros de imóveis passaram a ser setor obrigado a comunicar ao COAF movimentações em espécie acima de R$ 30.000,00 em operação de compra de imóveis, por meio da Provimento 88/2019 do Conselho Nacional de Justiça[178]. Esse é um caso a gestão informacional, exige-se o registro de propriedade para fruição de direitos e, a partir dela, empresta-se finalidade penal, no caso, com normativo infralegal.

Dito de outra forma, é condição da administrativização do direito econômico que haja uma gestão informacional que crie mecanismos de comunicação entre as agências estatais, característica inerente ao conceito de prevenção. Nesse caso, os registradores de imóveis passaram a ser entes obrigados a comunicar informações para compor o acervo do COAF. Na mesma linha, outro exemplo pertinente, também da lei de lavagem de dinheiro, é dever legal imposto de manutenção de dados fiscais dos contribuintes pela Receita Federal, pelo prazo mínimo de cinco anos[179].

O padrão de acesso a essas informações é tradicionalmente trabalhado no direito constitucional e processo penal pelo critério do sigilo. A Constituição Federal enumera diversos

---

[175] BRASIL. Lei nº 6.015, de 31 de dezembro de 1973. Dispõe sobre os registros públicos, e dá outras providências. *Diário Oficial da União*, Brasília, DF, 31 dez. 1973.

[176] BRASIL. Lei nº 4.862, de 29 de novembro de 1965. Altera a legislação do imposto de renda, adota diversas medidas de ordem fiscal e fazendária, e dá outras providências. *Diário Oficial da União*, Brasília, DF, 30 nov. 1965.

[177] BRASIL. Lei nº 9.503, de 23 de setembro de 1997. Institui o Código de Trânsito Brasileiro. *Diário Oficial da União*, Brasília, DF, 24 set. 1997.

[178] ”Os notários e registradores comunicarão à Unidade de Inteligência Financeira – UIF, por intermédio do Sistema de Controle de Atividades Financeiras – Siscoaf, quaisquer operações que, por seus elementos objetivos e subjetivos, possam ser consideradas suspeitas de lavagem de dinheiro ou financiamento do terrorismo.“ (CONSELHO NACIONAL DE JUSTIÇA. Corregedoria Nacional de Justiça. Provimento n. 88, de 1º de outubro de 2019. Dispõe sobre a política, os procedimentos e os controles a serem adotados pelos notários e registradores visando à prevenção dos crimes de lavagem de dinheiro [...]. *Diário da Justiça Eletrônico*, Brasília, DF, n. 187, 2 out. 2019. Caderno Administrativo, p. 14-22. Art. 6º.)

[179] "A Secretaria da Receita Federal do Brasil conservará os dados fiscais dos contribuintes pelo prazo mínimo de 5 (cinco) anos, contado a partir do início do exercício seguinte ao da declaração de renda respectiva ou ao do pagamento do tributo. Lavagem de Dinheiro.” (BRASIL. Lei nº 9.613, de 3 de março de 1998. Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores. *Diário Oficial da União*, Brasília, DF, 4 mar. 1998. Seção 1, p. 1. Art. 17-E.)

dados que são sigilosos, exigindo reserva de jurisdição para a acesso de terceiros. Recentemente, a ideia de dados protegidos juridicamente passou a receber mais atenção, isto é, aquelas informações que não são sigilosas, mas que não devem ser tratadas sem motivo idôneo. Por exemplo, os dados de consumo colhidos pelos setores obrigados do COAF – joias, obras de arte, direitos esportivos.

O registro de imóvel constitui informação pública, em posição diametralmente oposta à ideia de sigilo. Isso não significa, entretanto, que o dado deixe de ser protegido, considerando que determinados processamentos podem afetar direitos fundamentais. Isoladamente, o registro de imóvel permite o conhecimento acerca da cadeia dominial, de direitos de preferência e de eventuais gravames. Por outro lado, seu tratamento combinado com outras informações por entes públicos somente será lícito quando destinado a finalidades legais, estando, assim, protegido juridicamente.

No que se refere à ascensão do direito penal econômico, ele é especialmente relevante, pois não apenas a norma penal tem seu conteúdo complementado pela regulação setorial econômica, como também se estabelece, por paralelismo, uma dependência informacional das agências de persecução em relação aos órgãos detentores de competência específica, o que não exclusividade desse campo. Mais amplamente, há um o padrão de identificação das bases de dados públicas: leis que determinam o dever de registro por órgão público e a informação a ser retida.

Esse padrão fica claro na criação do Sistema Eletrônico de Registros Públicos (SERP), criado pelo art. 37 da lei 11.977/2009, que unifica o padrão de registro cartorário:

> Art. 37. Os serviços de registros públicos de que trata a Lei nº 6.015, de 31 de dezembro de 1973 (Lei de Registros Públicos) promoverão a implantação e o funcionamento adequado do Sistema Eletrônico dos Registros Públicos (Serp), nos termos da Medida Provisória nº 1.085, de 27 de dezembro de 2021.

Na sequência, o artigo 41 descreve os acessos aos bancos de dados pelo judiciário e executivo federal:

> Art. 41. A partir da implementação do sistema de registro eletrônico de que trata o art. 37, os serviços de registros públicos disponibilizarão ao Poder Judiciário e ao Poder Executivo federal, por meio eletrônico e sem ônus, o acesso às informações constantes de seus bancos de dados, conforme regulamento.

O exemplo é bastante elucidativo do modelo geral, o legislador complementa a lei de registros públicos, obrigando o setor cartorário a alimentar um sistema unificado com as

informações conhecidas em razão da atividade, com a finalidade de criar base única de informações a nível nacional. Dessa forma, soma-se ao acesso descentralizado por certidões cartorárias, uma base de dados pública e estruturada. Destaca-se que o uso dessa informação dependerá das formas autorizadas de tratamento, não servindo a qualquer ação que seja possível

Além da cessão de dados para o exercício da vida cidadã, as agências estatais criam estruturas de captação física para funções de segurança pública, tais como a instalação de câmeras e dispositivos de leitura de placa. Esse tipo de medida exige lei que defina o objeto e a finalidade da coleta, o que, na prática, não se concretiza. O Estado de São Paulo, por exemplo, autorizou a captura de imagens em locais públicos com uma lei de apenas quatro artigos – um deles vetado –, que se limita a autorizar a coleta, sem dispor sobre o modo de sua ocorrência[180].

Esse é um exemplo de criação de bases de dados públicas para segurança que se conecta com o uso probatório no processo penal, na medida que se houver registro do cometimento de infração penal, ela será transferida para a polícia judiciária como elemento de informação. No Capítulo 1, a tese já expôs a preocupação com arquitetura informacional que permite vigilância. Caso a prática seja repetida em todos os entes federativos, após consolidação, é possível falar-se em inúmeras bases de dados criadas sem definição de objetivo de uso, intervindo no direito à autodeterminação informacional dos cidadãos coletivamente.

Em conclusão, a criação de bases de dados públicas por lei exige a exposição clara da finalidade da coleta e a definição da autoridade competente para realizá-la. Isso é essencial para manter a legitimidade estatal - do registro civil ao monitoramento de segurança pública - e evitar o risco de vigilância não justificada. É necessário ressaltar que esse o único exemplo em que as próprias agências estatais captam os dados pessoais, que eventualmente são compartilhados com outras órgãos, observância a pertinência legal para tanto.

2.3.2 Base de dados privadas criadas por dever legal

As bases de dados privadas criadas por dever legal são as que se comunicam diretamente

[180] A Lei nº 15.518/14 afirma: Artigo 1º - Serão instaladas câmeras de monitoramento e vigilância nas áreas com índice de ocorrências policiais no Estado de São Paulo. Artigo 2º - Vetado. Artigo 3º - As despesas decorrentes da execução desta lei correrão à conta de dotações orçamentárias próprias, suplementadas se necessário. Artigo 4º - Esta lei entra em vigor na data de sua publicação. (SÃO PAULO (Estado). Lei nº 15.518, de 17 de julho de 2014. Dispõe sobre a afixação de aviso com o número do Disque Denúncia da Violência contra a Mulher em estabelecimentos que especifica. *Diário Oficial do Estado*, São Paulo, SP, 18 jul. 2014)

com a regulação de setores econômicos, na medida em que determinadas atividades podem ser meios, instrumento ou lugar do cometimento de infrações penais. Esse tipo de banco de informações é criado em razão da política criminal informacional, uma vez que se elegem as atividades econômicas que são comumente utilizadas em infrações criminais ou que permitem a identificação de suspeitos, para reter informação para a gestão de risco penal.

Nesses casos, as informações não são cedidas como condicionante ao exercício de direitos, elas se referem à utilização de produtos e serviços disponibilizados por empresas para fins pessoais, cujo acesso é livre e disponível por regras de mercado aos particulares. Da perspectiva das empresas, a legislação impõe a formação de bancos de dados como dever legal, condicionante jurídico-normativa para o oferecimento de serviços, que englobam a totalidade do setor financeiro e outros ramos específicos como a telefonia, aviação civil, setor viário, dentre outros.

As informações são variadas e previstas em legislações especiais. Como dito anteriormente, o direito brasileiro lida bem com os direitos dos sigilos, que é para os quais há critérios mais bem-definidos para acesso na persecução penal. Entretanto, no que se refere ao dever de retenção de informações, permanece no ideário que se o dado não for de conteúdo, não há riscos em determinar a coleta e armazenamento para possível acesso das agências de persecução. Como regra, os dados cadastrais são livremente requisitados por Ministérios Públicos e Polícias Judiciárias.

O padrão de identificação das bases de dados privadas é: lei que determine a retenção de dados por empresas, com a definição do dado pessoal que deve ser coletado. Mais uma vez, recorre-se a lei de lavagem de dinheiro para o expor o ponto, no art. 10, II e § 2º:

> [...] Da Identificação dos Clientes e Manutenção de Registros
> I - identificarão seus clientes e manterão cadastro atualizado, nos termos de instruções emanadas das autoridades competentes;
> II - manterão registro de toda transação em moeda nacional ou estrangeira, títulos e valores mobiliários, títulos de crédito, metais, ativos virtuais, ou qualquer ativo passível de ser convertido em dinheiro, que ultrapassar limite fixado pela autoridade competente e nos termos de instruções por esta expedidas;
> § 2º Os cadastros e registros referidos nos incisos I e II deste artigo deverão ser conservados durante o período mínimo de cinco anos a partir do encerramento da conta ou da conclusão da transação, prazo este que poderá ser ampliado pela autoridade competente.

Como se pode ver, os setores obrigados pela lei de branqueamento de capitais devem manter registro dos clientes e de todas as movimentações financeiras por eles realizadas pelo prazo mínimo de cinco anos. Solução semelhante é encontrada na lei das organizações criminosas, que determina

que as concessionárias de telefonia fixa e móvel devem manter registros de identificação de números dos terminais de origem e destino de ligações por cinco anos, mantendo-os à disposição das polícias judiciárias e dos ministérios públicos[181] e no marco civil da internet.

O fato dessas bases existirem em razão da política criminal gera previsibilidade quanto às informações que podem ser conhecidas quando acessadas. Por isso, pode-se dizer que possuem um potencial epistêmico limitado, já que o conteúdo informacional não é variado. Por exemplo, o acesso a registros telefônicos permite saber quem se comunicou, quando e por quanto tempo, para o qual o atual controle judicial é bem dimensionado. Essa mesma característica é observada nos bases públicas, que também coletam dados com potencial limitado, desde que o dado não seja correlacionado com outros e tratados para finalidades distintas.

Ademais, outra característica que aproveitada por ambas é que as agências de persecução sempre terão meio para acessos a esses bancos de dados, tendo em vista que existem para possibilitar a persecução penal em primeiro momento, a lei que cria também prevê a forma de acesso – a requisição administrativa e judicial. Assim, os problemas advindos da computação em nuvem para armazenamento de informações em outras jurisdições não são relevantes para os objetos do tópico "a" e "b", por se tratar de setores econômicos regulados.

2.3.3. Base de dados privada

Os bancos de informação privados existem em razão da atuação de entes privados no fornecimento de produtos no mercado, ao contrário dos analisados acima que são criados por lei. Essa característica impede que se possa identificá-los exaustiva e antecipadamente. Dessa forma, a coleta pelos particulares se dará em independência dos objetivos de política criminal informacional, que só serão relevantes quando as agências de persecução pretenderem acessá-las, isto é, após a instauração de alguma espécie de investigação preliminar.

A discussão colocada sobre criptografia ajuda a orientar a compreensão. Na hipótese desse tópico, nem mesmo o interesse de política criminal expressado por lei autorizadora garantem-no

[181] "As concessionárias de telefonia fixa ou móvel manterão, pelo prazo de 5 (cinco) anos, à disposição das autoridades mencionadas no art. 15, registros de identificação dos números dos terminais de origem e de destino das ligações telefônicas internacionais, interurbanas e locais." (BRASIL. Lei nº 12.850, de 2 de agosto de 2013. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal. *Diário Oficial da União*: seção 1, Brasília, DF, ed. extra, p. 1, 5 ago. 2013. Art. 16.)

eficácia jurídica. Os conflitos entre Estados e empresas de tecnologia se dão geralmente nesse campo, em que os dados de conteúdo de comunicações via aplicativos de conversas, e-mails, metadados de tráfegos, de multidões de pessoas são requisitadas a fim de produzir provas em ações penais[182]. O interesse decorre da possibilidade de reconstruir fato do passado para investigações.

Na categoria de dados privados, pode-se dizer que qualquer processamento de dados pessoais pode servir à função probatória, tendo em vista que os usos são os mais diversos, mas a depender da hipótese criminal, eles podem permitir a conclusão de que um fato no passado ocorreu. É, portanto, essencial estabelecer o ponto fulcral: justamente porque dados pessoais são utilizados em todas as atividades diárias, a coleta irrestrita que permita a vigilância, pública ou privada, da vida íntima viola a garantia constitucional à vida privada e autodeterminação informativa[183].

Tanto a vigilância privada quanto a pública são indesejadas[184], logo os argumentos de cada setor devem ser bem-compreendidos, uma vez que as razões públicas podem não coincidir com as motivações reais. É o tipo de discussão em que os dois lados não parecem ter razão. As empresas não querem o custo adjacente de permitir acessos individualizados para agências de persecução penal, o movimento de rebanho é o que lhes interessa[185], que requer a existência de equipes dedicadas, mais procedimentos de abertura de dados, o que foge ao interesse comercial.

Por outro lado, o poder público, pouco limitado sobre a perspectiva da investigação, cujos atos são definidos para era analógica de maneira muito abrangente, pretende maximizar o acesso às informações que sabem estar à disposição das grandes empresas de tecnologia. O valor do acesso está na quantidade, variedade, velocidade e veracidade das informações, a combinação disso é um material de *big data*[186], que permite que o Estado possa dar as mais diversas formas de tratamento, integrando-as com as bases públicas, para endereçar hipóteses criminais.

As bases privadas são mais variadas que as públicas, sendo que a acesso pode ser a dados não estruturados, como *weblogs,* postagens em redes sociais, gravações de vídeos, imagens e registros de aplicativos. Para analisá-los automatizadamente, as polícias utilizam algoritmos para colocá-los em linguagem estruturada. No caso dos *weblogs*, a pesquisa identificou o uso de *link analysis* para escalar a criação de vínculos sociais a partir do conteúdo, algoritmos de mineração

---

[182] GIACOMOLLI; EILBERG, 2023, p. 126
[183] LAPIN; IRIS, 2022, p. 22.
[184] MARAS; WANDT, 2019, p. 165.
[185] ZUBOFF, 2020, p. 153-154.
[186] MARAS; WANDT, 2019, p. 161.

de texto[187] para e-mail e PDFs para melhorar os resultados de investigação[188].

Somente em relação a *link analysis* e *text mining*, a pesquisa identificou dezoito soluções algorítmicas para uso criminal[189], o que significa que o gargalo para a utilização está no acesso aos dados, e não propriamente na capacidade de tratamento. Por isso, trabalhar com base em exemplos de possibilidade é tarefa especulativa ineficaz, tendo em vista que a integração de diversas fontes de dados permite inferências que nem os agentes de tratamento preveem, já que criam padrões multivariados, virtualmente impossíveis para o cérebro humano.

A título de exemplo, um iphone tem os seguintes hardwares instalados para coleta de dados: microfone, câmera, barômetro, termômetro, giroscópio de três eixos, acelerômetro, sensor de proximidade, sensor de luz ambiente, *wifi*, NFC, bluetooth, gps, monitor de frequência cardíaca[190]. Se considerarmos que cada pessoa no mundo tem quatro dispositivos conectados, e que eles se conectam automaticamente em várias situações – internet das coisas[191] –, é possível em falar em vigilância pelas empresas e pelo Estado, caso acesse indiscriminadamente esses materiais.

Além das dos hardwares citados acima, deve-se levar em consideração a cessão voluntária para utilização de produtos digitais na internet e as estruturas físicas de captação em ambientes públicos ou privados (monitoramento de placas, rede de telefonia com antenas). Como dito, é virtualmente impossível descrever as estruturas digitais de captação de dados. De toda maneira, é necessário descrever ontologicamente a capacidade de empresas de tecnologia de captar e armazenar dados de interesse comercial e comercial.

Para quantificar o argumento que vem sendo trabalhado, apresenta-se os dados dos pedidos de agentes de persecução brasileiros à Apple – primeiro semestre de 2024. Conforme a Tabela 2, o Brasil realizou 12.519 pedidos de aberturas de dados àquela empresa, para os quais foram fornecidas informações em 78%. De acordo com os dados da empresa americana, as informações são relativas aos aparelhos, aos identificadores financeiros, às contas, a *push tokens* e a

---

[187] Tecnologias encontradas: Perilog, Autonomy, Clairvoyance, ClearForest, Klarity, iCrossReader, Lextek, Leximancer, Quenza, VantagePoint, and Readware.
[188] PRAMANIK, M. I. et al. Big data analytics for security and criminal investigations. WIRES Data Mining and Knowledge Discovery, v. 7, jul./ago, p. 8-9, 2017.
[189] PRAMANIK, M. I. et al, 2017, p. 2-5.
[190] MARAS; WANDT, 2019, p. 165.
[191] De acordo com Maras e Wandt, "*The Internet of Things (IoT) is a term used to describe a network of interconnected everyday devices to the internet, which enable the real-time and remote monitoring and massive collection and sharing of data about people, animals, plants and property, to provide users of these devices with some form of service (Maras 2015). IoT technology is already deployed in homes, vehicles, buildings, roads and cities, constantly monitors energy levels, structural health and the quality of air and water, and regulates waste management".* P. 162.

emergências[192]. A maioria deles se referem a identificação de IMEI – causa provável roubo e furto de celulares – e dados de contas Appel para identificação de usuários.

Tabela 2 - Pedidos realizados pelo Brasil à Apple no primeiro semestre de 2024

Tipo de Pedido	Pedidos recebidos	Pessoas identificadas por pedido	Abertura de dados	Abertura em %
Dispositivo	8776	42276	6808	78%
Identificador financeiro	12	68	2	17%
Conta	3664	17884	2619	71%
Push token	0	0	0	
Emergência	67		55	82%
Total	12519	60228	9484	

Fonte: elaborada pelo autor

A tabela 2 demonstra que há acesso a informações pelas agências de persecução a dados cadastrais e metadados de utilização de dispositivos e contas de empresas privadas. Esse mecanismo é chamado de cooperação voluntária, que como se verá no Capítulo 6, não é um termo adequado para tratar a matéria. De toda forma, essa forma de acesso demonstra a dependência das agências de persecução em relação a empresas para acessar tais informações, o que configura uma situação não ideal para as agências de persecução, na medida em que a verificação da legalidade de intervenções informacionais não é função de agentes privados.

No contexto da América latina, com divisão de países feitos pela fonte, o Brasil se destaca como o país que realizou 98% dos pedidos relativos à identificação de dispositivos, conforme se pode visualizar na Tabela 3. Essa informação permite inferir o alto grau de utilização desses

[192] Tradução própria do site da Apple: Dispositivo: Solicitações recebidas de uma agência governamental buscando dados de clientes relacionados a identificadores de dispositivos, como número de série ou número IMEI. Identificador financeiro: Solicitações recebidas de uma agência governamental buscando dados de clientes relacionados a identificadores financeiros, como cartão de crédito ou cartão-presente. Conta: Solicitações recebidas de uma agência governamental buscando dados de clientes relacionados a identificadores de conta, como Apple ID ou endereço de e-mail. Push Token: Solicitações recebidas de uma agência governamental buscando dados de clientes relacionados a tokens do serviço de Notificação Push da Apple. Emergência: Solicitações recebidas de uma agência governamental buscando dados de clientes em uma questão de emergência, acessado em 17.09.2025.

mecanismos por agências brasileiras de persecução penal, isto é, o acesso a bases de dados privadas para fins de investigação criminal, o que não vem recebendo a devida atenção pelas ciências criminais, especialmente a teoria da prova do processo penal.

Tabela 3 - Pedidos de identificação de dispositivos na América Latina

América Latina	Pedidos por dispositivo	Total de dispositivos identificados	Abertura de dados por dispositivo	Abertura de dados por dispositivo (%)
Argentina	6	9	1	17%
Brasil	8776	42276	6808	78%
Chile	61	81	31	51%
Colômbia	47	94	31	66%
Costa Rica	1	2	0	0%
Equador	1	1	0	0%
Jamaica	1	1	0	0%
Total	8893	42464	6871	77%

Fonte: elaborado pelo autor

O principal objetivo ao quantificar o número de pedidos brasileiros realizados a uma única empresa é demonstrar que a arquitetura informacional privada e, consequentemente, seus bancos de dados, ingressam cotidianamente nas investigações criminais, ainda que não haja critérios legais claros para isso. Nesse sentido, o barulho que se faz sobre alguns pontos de debate, a exemplo da recusa a ceder dados de conteúdo, não é representativa da realidade, ainda que seja importante para os debates jurídicos[193]. Como dito anteriormente, não há garantia de que um dado cedido sobre o gosto musical não venha a ser utilizado em investigações criminais.

O ponto fulcral sobre as bases de dados e as respectivas capacidades técnicas de coleta de dados permanece inalterado: a coleta irrestrita de informações pessoas permite vigilância em massa tanto por Estado quanto por empresa[194], que devem ser rechaçados juridicamente pelo mesmo

[193] A exemplo das negativas de acesso a dados de conteúdos de *WhatsApp* que deram origem a ADPF 403 e ADI 5527. CORDEIRO, 2024, p. 74.
[194] MARAS; WANDT, 2019, p. 160-161.

motivo, ou seja, pela violação a garantias fundamentais. Como se viu ao longo do tópico, as potencialidades tecnológicas de coleta geram bancos de informações volumosos e multivariados para possibilitar inferências sobre padrões de consumo. Paralelamente, esses bancos de dados privados não estão alheios à ingerência do Estado-penal, o que é evidente na Tabela 2.

Finalmente, a experiência brasileira, demonstrada com os pedidos feitos a Appel, para guardar paralelismos com os hardwares de captação do Iphone, demonstra que as agências recorrem sistematicamente a empresas de tecnologia para subsidiar investigações criminais.

3. USO DE DADOS PESSOAIS NA SEGURANÇA PÚBLICA

O uso de dados pessoais para a finalidade de segurança pública antecede a existência de uma infração penal, de modo que essas informações não são tratadas com a utilização da categoria processual penal de suspeição, mas sim de evitamento de perigos[195], isto é, objetiva assegurar que a população esteja livre de riscos a bens jurídicos tutelados. Nessa linha, a primeira característica da segurança pública é que ela tem um olhar para o futuro, ainda que se relacione fortemente com a persecução penal[196], que tem sempre uma olhar retrospetivo para o passado.

O fato da segurança pública recair sobre perigos futuros faz com que a intervenção informacional realizada por esse ramo do direito tenha, como destinatário das normas, coletivos de pessoas indeterminados, com a função de reconhecimento daqueles que podem perturbar a ordem pública. O primeiro passo, portanto, é expor o que são perigos à segurança pública e delimitar o grupo de destinatários da norma, o que na linha do marco teórico deve ser feito com base em norma autorizadora[197], ressalvadas as intervenções bagatelares, como a identificação civil.

Como ficou claro no tópico sobre a constituição das bases de dados públicas – a única hipótese em que as próprias agências estatais realizam a coleta de dados – essa atividade deve estar orientada por finalidades públicas previamente previstas em lei autorizadora, uma vez que implica restrição ao direito fundamental à autodeterminação informacional. Isso não significa, porém, que todos os usos posteriores sejam automaticamente permitidos às agências de segurança. Ao contrário: a finalidade é condição da validade material da norma autorizadora e, portanto, determina os usos que podem ser feitos da informação.

A consequência dessa afirmação é que se a lei autoriza a instalação de câmeras de segurança com a finalidade de prevenir o risco à vida em avenidas movimentadas, as imagens coletadas não devem ser armazenadas para usos diversos, a exemplo de monitorar em tempo real protestos políticos, identificar seus líderes e rastrear pessoas determinadas. Dito de outra forma, a implementação da arquitetura informacional da segurança pública não serve à finalidade de realizar atos investigativos retrospetivamente, recaindo necessariamente sobre pessoas não suspeitas.

A tese central é que o uso de dados pelas agências estatais deve ser restrito à finalidade que

---

[195] GLEIZER; MONTENEGRO; VIANA, 2021, p. 77-82.
[196] PRADO, 2024, p. 246
[197] GLEIZER; MONTENEGRO; VIANA, 2021, p. 86

autorizou a sua coleta, o que pressupõe que as leis autorizadoras tenham objeto definido. Esse raciocínio retira fundamento dos princípios gerais de proteção de dados da União Europeia, mais precisamente da Diretiva (UE) 2016/680[198]. Tal diploma prescreve a finalidade do tratamento como um dos pilares da autodeterminação informacional, na medida em que vincula as agências de segurança ao motivo que legitimou a coleta para evitar excessos de processamento.

Adiante, a tese vai expor, em tópico próprio, o conteúdo jurídico da separação informacional, que fez uma escolha de política de segurança de separar rigidamente as funções de inteligência, segurança pública e persecução penal, para evitar a unicidade informacional. Reconhecidamente, a Alemanha é um bom exemplo da internalização da Diretiva mencionada acima, já que "adotou o princípio da separação informacional entre órgãos de inteligência e persecução penal para evitar abusos de poder decorrentes da onisciência informacional"[199]. O que se opõe às escolhas adotadas no Brasil.

Na mesma linha, as finalidades devem ser legítimas e explícitas[200]. Evidentemente, a lei autorizadora não deve prever normas gerais que sirvam para quaisquer situações, a exemplo de leis que determinem abstratamente a instalação de câmeras para "fins de segurança" pública. Em relação à legitimidade, espera-se que a arquitetura informacional do Estado não seja empregada para perseguição a inimigos políticos, ou para limitar o direito de reunião[201], de manifestação[202], ou seja, não objetive o descumprimento deliberado de outras garantias constitucionais.

Ao nosso ver, as escolhas de política de segurança pública brasileiras não se orientam por uma principiologia jurídica centrada na teoria das garantias fundamentais, a exemplos dos princípios e exigências legais adotadas na tese. De maneira oposta, a escolha brasileira usa as capacidades tecnológicas como fundamento para a alteração do arcabouço jurídico, em uma espécie de presunção de que se é possível tecnicamente, pode ser implementado. Essa afirmação se justifica na análise das alterações legislativas realizadas no Brasil.

Em oposição à ideia de norma autorizadora com objeto definido, com exceção das leis que disciplinam os levantamentos de sigilo, o modelo comum é que o legislador imponha arquitetura informacional, inclusive para segurança pública, sem afirmar para qual finalidade. Veja-se o

---

[198] UNIÃO EUROPEIA. Diretiva (UE) 2016/680, art. 4º, (1)(b).
[199] BALDISSERA, Rafaela. Construindo um Modelo Brasileiro de Proteção de Dados para a Segurança Pública: Lições da Europa no Combate à Lavagem de Dinheiro, 2025, p. 201.
[200] BALDISSERA, 2025, p. 71.
[201] BRASIL. Constituição Federal, art. 5º, XVI.
[202] BRASIL. Constituição Federal, art. 5º, IV e IX.

exemplo da legislação paulista, artigo 1º, da lei estadual 15.518/04 estabelece que "serão instaladas câmeras de monitoramento e vigilância nas áreas com índice de ocorrências policiais no Estado de São Paulo"[203]. É impossível depreender a finalidade do uso previsto pelo legislador com a análise dessa norma.

A questão que se coloca é se uma norma como essa é materialmente válida, ou seja, se define um uso lícito, finalisticamente vinculado, adequado e necessário – critérios que poderiam vir a ser exigidos por uma LGPD penal[204], a exemplo do anteprojeto apresentado pela Comissão de Juristas. Invariavelmente, a resposta deve ser negativa: a única função do referido artigo é permitir a aquisição do material a ser instalado, enquanto toda a fase de uso e reúso posterior ocorre em ambiente opaco e sem limitações, geralmente justificada pelo amplo e indeterminado conceito de poder de polícia[205].

A tese é orientada pela o modelo europeu de proteção de dados no âmbito público e, assim como muitos outros trabalhos, poderia se dedicar a explicar os princípios aplicáveis àquela realidade jurídica para prescrever como deveria ocorrer no Brasil. Entretanto, o recorte do texto é como o fluxo dessas informações ingressam no processo penal, somadas aos outros tipos de base dados disponíveis às agências de persecução – as privadas –, sendo que o problema imediato é que se há um sistema de segurança público implementado legalmente, ele deve ser analisado. Assim, é preciso retomar a fundamentação desse sistema e como ele opera.

Como característica geral, o modelo de segurança público brasileiro é orientado pela consolidação de dados, que é alcançado dentro as agências estatais com uso de tecnologias da informação com protocolos semelhantes para maximizar a quantidade de informações, em outras palavras, é a capacidade técnica que molda o sistema jurídico. Ainda que essa orientação seja justificada computacionalmente, ela é juridicamente oposta a um sistema que pretenda limitar a

---

[203] SÃO PAULO. Lei 15.518/04, Art. 1º.

[204] A lógica da meta lei serve para regular as relações privadas de coleta, uso e reuso de dados pessoais porque funciona para excepcionar as ações que não podem ser tomadas por controladores e operadores no âmbito privado. No caso do tratamento para finalidades penais, essa perspectiva reguladora pode criar etapas de cumprimento de obrigações pelas agências de persecução, mas as atividades de tratamento em si devem ser autorizadas por atos de investigação e de prova, mesmo que previsto em legislações especiais e não sistematizadas.
Acrescenta pouco ou quase nada dizer que o tratamento para fins penais imprescinde do consentimento do titular, isso é uma obviedade em se tratando de meios de obtenção de prova ocultos. O potencial limitador está no preenchimento do conteúdo jurídico das medidas de investigação após a análise e entendimento da realidade tecnológica. Nesse sentido, a afirmação que a coleta do dado deve ocorrer para fim específico para evitar *fishing expedition* é correto, mas vai de encontro com toda a arquitetura informacional já implementada pelo Estado brasileiro.

[205] GLEIZER; MONTENEGRO; VIANA, 2021, p. 82

onisciência informacional estatal, isto é, não é orientada pela axiologia da proteção de dados.

A partir dessa constatação, o capítulo se subdivide em três tópicos que versam sobre: i) a separação informacional como garantia institucional; ii) a estratégia consolidação de dados pelo Estado brasileiro, ii) e; iii) a análise do sistema único de segurança pública, da perspectiva do uso de dados pessoais.

3.1 A separação informacional como garantia institucional

A proteção de dados no âmbito público é mais que uma garantia individual, na medida que sua observância depende de que o Estado adote medidas processuais e procedimentais para garanti-la em dimensão institucional, como vendo sendo explicado na tese. A separação informacional é também uma garantia institucional, que decorre da instrumentalização da proteção individual do direito individual, assim como defende Greco, com base no modelo alemão[206]:

> [...] A vinculação à finalidade, conjugada à separação entre inteligência, polícia e justiça, significa também que é inadmissível uma base de dados comum a todos os órgãos estatais. "Toda tentativa de enxergar a administração pública como uma unidade informacional é incompatível com uma proteção eficiente de dados". Se saber é poder, o Estado não pode saber tudo, porque um Estado que tem conhecimentos ilimitados tem também um poder ilimitado. O direito de proteção de dados, que começa como direito subjetivo, mostra-se, ao menos em boa parte, como garantia institucional, relativa à própria estrutura da sociedade e do Estado. Nesse nível macro o direito se transforma em uma exigência de separação informacional de poderes

O autor tem razão ao afirmar que a unidade informacional confere poderes ilimitados ao Estado, o que é incondizente com o Estado moderno, que é desenhado para ser autolimitado. Isso significa que a arquitetura informacional em todas as funções de estatais deve ser pensada para evitar que esse fenômeno, o que exige que as agências públicas tenham acesso às informações pertinentes para o cumprimento de suas funções legais. Tal argumento perpassa transversalmente a organização da burocracia estatal, conforme já trabalho.

Nesse sentido, a Bélgica é um excelente exemplo. Desde a primeira cessão de dados pessoais ao Estado, o sistema é pensado para que ela feita uma única vez, e ocorra descentralizadamente conforme as atribuições legais das agências estatais[207]. Esse modelo evita a

---

[206] GRECO, 2018, p. 45.
[207] DEGRAVE, 2024, p. 18.

duplicação de informações e a unicidade informacional; não há porque agências de saúde terem acesso a informações de trânsito, uma vez que as funções legais são complemente diferentes, isto é, se a agência não poderia coletar o dado, pela mesma razão, não deve ter acesso.

O objetivo é garantir que a arquitetura informacional espelhe as atribuições legais vinculativas das agências do Estado. Vale dizer que isso não é uma novidade da era digital, que geralmente ficava abrangida pela ideia de sigilo, por exemplo os dados fiscais não ficam sob custódia da polícia – que é a primeira garantia para evitar o uso indevido desses dados. Dito de outra forma, a unidade informacional potencialmente viola direitos fundamentais, mesmo que consideradas situações exclusivas do direto analógico, por assim dizer.

O primeiro passo do sistema belga consiste na identificação de órgãos com funções comuns, que são organizados em redes setoriais de informação, cuja arquitetura da informação funciona com interoperabilidade entre as agências[208]. O acesso aos registros administrativos ocorre por meio de um sistema que concede acessos à fonte autêntica – base de dados primária. Nesse caso, o acesso às informações é controlado e armazenado sob custódia de outra agência[209]. Essa solução visa a assegurar mais governança no acesso e discussão das funções comuns antes da transferência.

Como se pode perceber, os problemas atinentes à unicidade informacional não são restritos à segurança pública e à persecução penal. Por exemplo, países com economias fortes tendem a atrair mão de obra em situação irregular. Essas pessoas constituem famílias e têm acesso a determinados direitos. Para garanti-los, é indispensável a proteção das informações pessoais. Assim, hospitais não devem comunicar o atendimento de pessoas sem documentação às autoridades migratórias, pois o efeito imediato seria a resistência ao atendimento médico.

O exemplo acima parece é mais facilmente compreendido porque o raciocínio sobre sigilos está bem-sedimentado nos ordenamentos jurídicos ocidentais, no caso concreto, o sigilo médico. Entretanto, a mesma *ratio* deve servir ao acesso à educação, as escolas não devem comunicar as crianças indocumentadas às autoridades migratórias. Nessa situação, não há um direito de sigilo sobre estar matriculado, pelo menos em termos tradicionais, ainda assim, é necessário entender que as agências de imigração e as escolares não devem compartilhar bases de dados, já que realizam funções independentes. Em suma, o Estado não deve ser uma unidade informacional[210].

---

[208] DEGRAVE, 2024*,* p. 19.
[209] DEGRAVE, 2024, p. 20.
[210] ZUBOFF, Shoshana. A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder. Tradução: George Schlesinger. Rio de Janeiro: Intrinseca, 2020, p. 153-154.

Se diversas agências estatais coletam dados para finalidades específicas, autorizadas por lei, o compartilhamento também deve observá-la. É, portanto, essencial que dados e informações não circulem livremente entre agências do Estado sem atenção a esse risco.

O ponto é justamente entender que a capacidade técnica não significa possibilidade jurídica, que deve primeiro encontrar adequação legal antes de ser implementada concretamente. Evidentemente, os exemplos apresentados colocam casos fáceis para exemplificar a questão, até porque o objetivo é fundamentar as categorias que serão utilizadas para analisar os casos limítrofes adiante, nomeadamente, aqueles que envolvem sobreposição de funções e necessária comunicação entre agências de segurança pública e persecução penal. Nesse contexto, a separação é um critério de validade material das leis que alterem a arquitetura informacional do Estado.

É claro que existe uma diferença ontológica entre hospitais públicos que, por meio de registros em papel, comunicam às agências policiais possíveis infrações penais, e o uso de API (interface de programação de aplicações) que integra os dados de prontuários do Sistema Único de Saúde (SUS) ao Sistema Nacional de Informações de Segurança Pública (SINESP) para gerar alertar de cometimento infrações penais. Essa diferença ontológica reside na escala e na velocidade proporcionadas por informação estruturada entre agências de diferentes funções, na medida em que o volume de informações deixa de ser um problema, tendo em vista os métodos automatizados de análise, logo o potencial da violação à autonomia informacional é incrementado.

Retomando a diferenciação feita no início deste capítulo, as funções de segurança pública e persecução penal são, no mínimo, complementares, de modo que as agências estatais se organizam para lidar com perigos futuros que, caso não evitados, devem idealmente iniciar a fase de investigação preliminar. Nesse contexto, a infraestrutura preventiva é útil à atividade probatória do processo penal quando o risco que a segurança visa a evitar, é efetivado com a infração penal. Logo, não há modelo ideal que separe absolutamente os dois campos.

Diante dessa constatação, a pergunta que deve ser respondida é como esse fluxo deve ocorrer, em outras palavras, como os dados levantados para a função "x" podem ser legitimamente reutilizados para "y". Por paralelismo argumentativo, se é necessária autorização legal para intervir informacionalmente, também deve ser para compartilhar. Dessa forma, argumentam Gleizer, Montenegro e Viana no sentido de que não só a coleta depende de lei[211]:

---

211 GLEIZER; MONTENEGRO; VIANA, 2018, p. 136,

> [...] Todas as considerações anteriores são desenvolvidas a partir de único fio condutor: cada uma das formas de tratamento de dados pessoais por órgãos de segurança pública e persecução penal demanda autorização em lei e tem sua legitimidade avaliada separadamente em face da natureza de cada uma dessas atividades estatais. Por conseguinte, deve haver normas de direito de segurança pública que autorizem respectivamente levantamento, armazenamento, alteração e utilização, assim como também devem fazê-lo as normas atinentes ao processo penal. Essa ideia é tratada no direito alemão como o "modelo das duas portas".

O modelo de duas portas impõe foi a solução encontrada pelo Tribunal Constitucional Alemão. A ideia é a necessidade de que exista duplo fundamento legal, isto é, o controlador primário deve ser autorizado legalmente a compartilhar, e o controlador secundário de ser autorizado a acessar originariamente o tipo de dado que se pretende obter por compartilhamento[212]. Nesse sentido, as duas portas deveriam estar abertas para que o compartilhamento e o reuso de dados seja legalmente válido.

Utilizando-se o exemplo brasileiro, se as guardas municipais não poderiam, mesmo que autorizados legalmente – por inconstitucionalidade –, coletar informações relativas a amostras de DNA, já que não exercem função de polícia judiciária[213], tampouco podem receber essa informação por compartilhamento da Polícia Federal, a primeira porta estaria fechada. Entretanto, a prática brasileira é a consolidação de bases de inúmeras agências, que coletam dados por meio de leis que não estabelecem critérios de validade para interferir na autodeterminação informacional

No direito americano, houve a compreensão de que a consolidação de dados sem limitação constitui um risco à 4ª emenda da Constituição dos Estados Unidos[214], que veda buscas colocava buscas desmotivas e apreensões. Sobre isso, David Gray afirma que "aggregation is often what makes Big Data searches broad and indiscriminate, and therefore what threatens the right of the people to be secure against unreasonable searches and seizures"[215]. Uma das razões para justificar a afirmação é que a partir do momento que se faz o *input* de bases multivariadas em grande volume, o agente de tratamento perde o controle sobre o resultado.

O autor afirma que algum grau de reflexão sobre isso foi dado pelo Congresso dos Estados unidos. Segundo ele, o caso paradigmático foi restrição que a *National Security Agency* (NSA) em reter diretamente os metadados de todas as telecomunicações telefônicas que, a partir do USA

---

[212] GLEIZER; MONTENEGRO; VIANA, 2018, p.137-138.
[213] BRASIL. Supremo Tribunal Federal, Recurso Extraordinário 608.588.
[214] ESTADOS UNIDOS. Constituição (1787). Emenda n. 4. 1791. In: The Bill of Rights. Washington, D.C.: National Archives.
[215] GRAY, 2017, p. 269.

Freedom Act de 2015, ficam retidos pelas empresas telefônicas, acessáveis mediante decisão judicial, com especificação do objeto[216]. O caso é pertinente, a legislação americana separou a base de dados e a agência que pretende o acesso por decisão judicial.

A prática brasileira está em direção oposta. Como se verá adiante, os critérios de consolidação são dados por atos infralegais, cujo pedágio consolidação de novas bases pode ser um Acordo Cooperação Técnica com o Ministério da Justiça. Assim, ainda que bem definido academicamente, a separação informacional como limite institucional é uma desconhecida no Brasil[217]. A consequência é a política pública do quanto mais dados, melhor, e caso haja vazamento, agente de tratamento deve ser responsabilizado, o que não é impeditivo da vigilância como política estatal.

Este tópico explorou prescritivamente o potencial da separação informacional como limite institucional; os próximos, abordam descritivamente a realidade brasileira.

3.2. Unidade informacional e segurança pública brasileira

O Estado pode aumentar a capacidade de gerar inferências a partir de dados pessoais com a consolidação de variados bancos de dados, possibilidade que alimenta o mito que unidade informacional como panaceia da segurança pública, a moda *minority report*. Nesse sentido, a consolidação de dados é tão relevante para as tecnologias da informação quanto a aquisição inicial da informação, na medida em que permite alterar o entorno correlacional de informações pessoais; a câmera de segurança de um aeroporto e o acesso a um site público, analisados integradamente, permitem inferências sobre a localização de forma mais assertiva.

A consolidação de dado, tradução de *data aggregation*, constitui uma etapa maximizadora da intervenção informacional a partir das informações coletadas[218], provenientes de múltiplas fontes, ao apresentá-las de forma compilada e inteligível para a interpretação humana. Seu objetivo é possibilitar que grandes bases de dados, de diferentes origens e conteúdos heterogêneos, possibilitem ao agente de tratamento conhecer aspectos da realidade, isto é, extrair potencial epistêmico de informações que, isoladamente, não teriam valor prático.

---

[216] GRAY, 2017, p. 270.
[217] SARLET; SARLET, 2022, p. 8-16.
[218] MARAS; WANDT, 2019, p. 160-163.

O ponto central é que, quanto maior o número de bases agregadas, maior é o potencial de extração de conhecimento inferencial. Esse aspecto tecnológico tem sido utilizado no Brasil para implementar a estratégia de uniformização dos dados pessoais coletados por entes públicos, com o objetivo final de consolidá-los e produzir inferências de diversas naturezas, alinhadas às obrigações legais dos órgãos de segurança estatal, que desempenham finalidades distintas, como a repressão e a prevenção da criminalidade.

Como articulado, o fundamento jurídico não se confunde com as possibilidades técnicas, na medida em que a maximização da consolidação leva a uma unidade informacional, que é deontologicamente desorientada da proteção de dados no âmbito público, apesar da insistência brasileira nesse tipo estratégia, visualizada concretamente na implementação do Sistema Único de Segurança Pública (SUSP)[219], que é analisado no próximo tópico. Se somente a lógica técnica for levada em consideração, o Estado passa a se organizar para gerar mais utilidade de uso e reúso de dados, isto é, o que se coleta para fazer "x" também é útil para "y".

Suponha-se que a coleta "x" é a imagem de uma placa de carro em um local de alta incidência de roubo de veículos em uma *smart city*, logo todos os veículos que passarem no local têm o descolamento registrado. Na hipótese "a", um veículo é furtado, e essa imagem é compartilhada com a polícia judiciária, num fluxo de informação lógico. Na hipótese "b", nenhum veículo foi furtado durante uma semana, mas a informação é armazenada em um sistema integrado entre polícias ostensiva e judiciária para possível utilidade probatória, por prazo indeterminado.

Na hipótese "a", o uso realizado é o que justificou a coleta finalisticamente, logo é lícito. Entretanto, na hipótese "b", pretende-se usar a informação para comprovação de infração penal que pode ocorrer futuramente, o que rompe com o motivo inicial da coleta, por isso a utilização é ilícita. Dessa forma, o problema que surge dessa situação é que se as bases da prevenção e da apreensão são agregadas, em uma unidade informacional, é impossível identificar o uso que será realizado, isto é, a coleta "x" não opera efeitos limitadores nos potenciais usos futuros.

A segurança pública não deve ser utilizada como fundamento para realizar registros massificados de movimentos populacionais, sobretudo quando, mesmo sem a concretização de riscos a bens jurídicos, as informações são retidas apenas pelo potencial de utilidade probatória. Do ponto de vista jurídico, a consolidação deve ser lida como compartilhamento de dados entre

---

[219] BRASIL. Lei nº 13.675/2018. Art. 9º, § 1º.

agências estatais que, por paralelismo, exige lei, tendo em vista é que um ato semelhante à coleta[220].

Ademais, há critérios materiais a serem observados para validade da autorização de compartilhamento, especificamente sobre os limites: não se deve franquear acesso a agências que não autorizadas realizar a coleta diretamente, num primeiro momento. Assim, se a polícia judiciária necessita de autorização judicial para rastrear um suspeito por vários dias – tal como ocorre na postergação do flagrante –, não é admissível que sistemas integrados de segurança pública sejam utilizados para essa finalidade sem o mesmo controle judicial.

O compartilhamento é a forma como a segurança pública se conecta ao processo penal, de modo que, se há onisciência informacional na primeira, o resultado é a deflagração de investigações preliminares com base nesse paradigma de intervenções ilegítimas. A depender do grau de intervenção informacional, o axioma processual da presunção de inocência é afastado, na medida em que a prevenção aos riscos antecipa os registros de qualquer ação humana coletivamente, que possa vir a ser criminosa. Esse exemplo é paralelo à gravação de todas as ligações telefônicas para que, na eventualidade de uma ação penal, pudessem servir de elemento de prova.

Por fim, a síntese do argumento é que as intervenções informacionais para segurança pública não servem à finalidade de antecipar a atividade probatório do processo penal, e sim para lidar com os riscos concretos à ordem pública. A garantia de que esse cenário não ocorra depende da observância da separação informacional, institucionalizamente, entre segurança pública e persecução penal, mas essa não foi a escolha legislativa brasileira que, como se explica no tópico abaixo, fez a opção por uma unidade informacional na segurança pública.

3.3. O modelo informacional implementado pelo Sistema Único de Segurança

Ainda em 2018, o autor Luís Greco comentava que o Brasil estava optando por um sistema de segurança pública estruturado contrariamente à separação informacional entre agências do Estado, como consequência das inobservâncias da proteção de dados no âmbito público. Em texto introdutório da obra do jurista Jurgen Wolter sobre a proteção de dados no processo penal alemão, ele comentava que o PLC 19/2018, que deu origem à lei 13.675/2018, sobre os riscos de se

[220] Sarlet e Sarlet argumentam que "*O compartilhamento de dados pessoais entre os órgãos estatais, por sua vez, deve ser devidamente regulado por lei, sendo pautado por uma repartição de competências (separação informacional de poderes), ademais de guiado pela finalidade da coleta e tratamento dos dados, porquanto somente assim o poder público estará atuando no âmbito de seus deveres constitucionais e legais"*. (SARLET; SARLES SARLET, p. 37-38)

integrarem diversas agências públicas em um Sistema Único de Segurança Pública (SUSP)[221]:

> [...] No Brasil, na contramão desses princípios, vejo com preocupação enquanto escrevo as presentes linhas que o Senado acaba de aprovar um Sistema Único de Segurança Pública (PLC 19/2018), que eleva a integração de informações de inteligência e de segurança pública obtidas por autoridades dos mais diversos níveis (polícias, bombeiros, órgãos penitenciários, agentes de trânsito etc., federais, estaduais e municipais) a uma de suas bandeiras centrais. O fato de que esses esforços não tenham provocado um escândalo público é prova da urgência de uma reflexão mais aprofundada sobre os princípios que acabo de expor.

A ideia tanto não gerou um escândalo público que atualmente é o marco legal da segurança pública brasileira. A única imprecisão do autor no comentário é que a criação do SUSP era o a consolidação do da estrutura legal anterior do Sistema Nacional de Informações de Segurança Pública (SINESP), previsto inicialmente na lei 12.681/2012[222]. Ela foi formalmente revogada pela lei posterior, mas teve o conteúdo normativo replicado na legislação posterior, o que permite afirmar que a unicidade informacional da segurança pública brasileira data de 2012.

O SUSP é constituído pelas a seguintes órgãos públicos: polícia federal, polícia rodoviária federal, polícias civis, polícias militares, corpo de bombeiros militares, guardas municipais, órgãos do sistema penitenciário, institutos oficiais de criminalística, medicina legal e identificação, Secretaria Nacional de Segurança Pública, secretarias estaduais de segurança pública ou congêneres, Secretaria Nacional de Proteção e Defesa Civil, Secretaria Nacional de Política de Drogas, agentes de trânsito, guarda portuária, polícia legislativa[223].

O SINESP, desde sua criação, a função "proceder à coleta, análise, atualização, sistematização, integração e interpretação de dados e informações relativos às políticas de que trata o art. 1º "[224]. Para o objeto da tese, o foco deve ser ações de integração, que é o que potencialmente cria riscos à separação institucional de funções, na medida em que agências estatais com funções muito distintas fazem parte do mesmo sistema, como órgão de trânsito e a guarda portuária, que não guardam correlação legal entre suas atribuições legais.

Nesse ponto, a prática brasileira se distancia do exemplo belga, uma vez que se pretende integrar toda a informação que já foi coletada pelas agências citadas acima. No país europeu, por

---

[221] GRECO, 2018, p. 45-46.
[222] BRASIL. Lei nº 12.681/2012, Art. 1º ao art. 5º.
[223] BRASIL. Lei nº 13.675/2018, Art. 9º, § 1º.
[224] BRASIL. Lei nº 12.681/2012, Art. 2º, I.

outro lado, os dados pessoais foram cedidos uma única vez porque já se sabia, desde a concepção do sistema, a quais dados cada agência poderia ter acesso em razão do setor de atuação[225]. Como dito anteriormente, a política brasileira se orienta pelo critério técnico de maximizar os usos de dados, sem a devida atenção aos princípios jurídicos que limitam a implementação.

De acordo com a legislação, a finalidade do SINESP é "armazenar, tratar e integrar informações*"* relacionadas à segurança pública, defesa social, sistema prisional, execução penal, rastreabilidade de armas e munições, banco de perfis genéticos e digitais, tráfico de drogas e violência doméstica[226]. Claramente, o critério de que a finalidade deve ter conteúdo objetivo não é verificada na lei de regência desse sistema, na medida em que se limita a citar fases do ciclo de vidas dos dados digitais, vinculando-o à função de segurança pública.

Entretanto, o que mais chama atenção é que não houve positivação dos procedimentos para o cumprimento para realizar a integração das informações entre os diferentes órgãos. Nesse contexto, a opção legislativa foi delegar por decreto presidencial essa função, que deu origem a Decreto 9.489/2018[227]. Tal escolha legislativa é representativa de que a política brasileira não enxerga a proteção de dados como uma garantia fundamental, que delega temas que intervém diretamente em direito fundamentais, apesar do consenso doutrinário sobre normas de abstenção[228].

Nesse sentido, especificamente sobre padrões de consolidação e interoperabilidade, nos termos do referido decreto, compete ao Conselho Gestor do SINESP, regrado pelo referido decreto, a competência para "propor procedimentos sobre coleta, análise, sistematização, integração, atualização, interpretação de dados e informações*"*. Portanto, é um conselho administrativo que propõe os padrões técnicos para garantir a compatibilidade de dados entre órgãos.

De acordo com o art. 19, II, do Decreto nº 9.489/2018, o Conselho proporá:

> [...] a) metodologia, padronização, categorias e regras para tratamento dos dados e das informações a serem fornecidos ao Sistema Nacional de Informações de Segurança Pública, Prisionais, de Rastreabilidade de Armas e Munições, de Material Genético, de Digitais e de Drogas;
> b) dados e informações a serem integrados ao Sistema Nacional de Informações de Segurança Pública, Prisionais, de Rastreabilidade de Armas e Munições, de Material Genético, de Digitais e de Drogas, observado o disposto no art. 18;
> c) padrões de interoperabilidade dos sistemas de dados e informações que integrarão o

[225] DEGRAVE, 2024, p. 18-21.
[226] BRASIL. Lei nº 13.675/2018, Art. 35, I-VI.
[227] BRASIL. Decreto Presidencial nº 9.489/2018/2018.
[228] MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. Curso de Direito Constitucional. 7ª ed. São Paulo: Saraiva, 2012, p. 291-292

> Sistema Nacional de Informações de Segurança Pública, Prisionais, de Rastreabilidade de Armas e Munições, de Material Genético, de Digitais e de Drogas;
> d) critérios para integração e gestão centralizada dos sistemas de dados e informações a que se refere o art. 18;
> e) rol de crimes de comunicação imediata; e
> f) forma e condições para adesão dos Municípios, do Poder Judiciário, da Defensoria Pública, do Ministério Público, e dos demais entes públicos que considerar pertinentes;

O Gestor do SINESP é responsável por propor os critérios técnicos de consolidação e compatibilidade de sistemas de informações, a forma e as condições para que outros entes públicos adiram ao sistema. A alínea "f" se refere a municípios, Defensoria Pública, Ministério Público e demais entes que sejam pertinentes. Há, claramente, um contraste entre o tipo de dado à disposição e a abertura institucional para acessá-los, especialmente porque os critérios legais são insuficientes, permitindo-se inclusive o "acesso recíproco aos bancos de dados"[229].

Em síntese, a integração dos dados nacionais de segurança pública ocorre pelo SINESP, regrado por decretos e portarias administrativas. Logo, é impossível se falar em previsão legal para tratamento de dados quando a legislação permite acesso aos bancos de dados para múltiplos órgãos, cujo limite é a porosa expressão[230] "nos limites das respectivas competências". A crítica à expressão se justifica na realidade: o STF teve se manifestar em repercussão geral se guardas municipais poderiam fazer policiamento ostensivo e judiciário, isto evencia que a interpretação sobre as competências legais na segurança pública é relevante[231].

É difícil compreender uma política informacional que inclua agentes de trânsito em um sistema que contém dados de perfil genético e digitais. Esse tipo de solução se justifica na crença de que o tratamento de dados pelo poder público é indene de problemas, tendo-se por objetivo integrar a maior quantidade de dados. Diante dessa abrangência, a forma escolhida para a realização da gestão do SINESP se torna uma questão de primeira ordem, já que tem o condão de dizer qual órgão administrativo tem acesso ao quê. Em outras palavras, o que separa as guardas municipais de dados de biométricos é uma decisão administrativa, cuja competência é estabelecida por decreto.

O SINESP não é exceção. Ao contrário, é mais um dos exemplos de uma estratégia

---

[229] *Ibid*., art. 10, VI, § 4º.
[230] Afirma-se que a expressão é insuficiente porque existem dúvidas relevantes a respeito de quais sãos esses limites legais numa federação com múltiplos entes e sobreposição de deveres legais. Esse debate foi recorrente sobre as guardas municipais, que inclusive deu origem ao tema de repercussão geral 656 no STF no início de 2025, a tese final do julgamento permitiu policiamento ostensivo e comunitária, pelas forças municipais, com a exclusão de qualquer atividade de policiamento judiciário. Logo a linha de competências não é tão clara.
[231] BRASIL. Supremo Tribunal Federal, Recurso Extraordinário 608.588.

informacional que se repete para uso e reúso de dados pessoais, incluindo as sensíveis e os sigilosos; cria-se um sistema único de informações para finalidades legítimas e, posteriormente, permite-se amplo acesso para fins indefinidos, cujo limite do compartilhamento é encontrado por expressões que ensejam mais debates do que entendimentos firmados. Nessa linha, Sartet e Sarlet identificaram o mesmo problema quanto em relação ao programa Identificação Civil[232]:

> [...] Outra discrepância diz com o problema da Identificação Civil Nacional (ICN) que se baseia na Lei 13.444/2017 e que evoca questões acerca da centralização de dados que compõe o sistema de identificação civil nacional. Por sua vez, a lei 13673/2018, em seu artigo 6º (aqui citado em caráter meramente ilustrativo), sem a devida cautela para com a Governança de dados exigida pela LGPD e tampouco vinculada ao guia orientativo da ANPD, listou dentre os objetivos da Política Nacional de Segurança Pública: a promoção da interoperabilidade dos sistemas de segurança pública, o estímulo ao intercâmbio de informações de inteligência de segurança pública com instituições congêneres, a entrega e o compartilhamento das informações de segurança pública, prisionais e sobre drogas, dentre outros. Merece atenção especial o artigo 10, parágrafo 2º, do referido diploma legal, quando prescreve que o "compartilhamento de informações será feito preferencialmente por meio eletrônico com acesso recíproco aos bancos de dados, nos termos estabelecidos pelo Ministério extraordinário de segurança pública. No que se refere ao funcionamento do SISBIN assume importância o posicionamento do STF outrora mencionado e o flagrante desrespeito ao princípio da separação informacional.

A citação dos autores é precisa: a política de centralização da informação é materializada, no caso, por meio de um sistema nacional de identificação civil, cuja administração cabe a um comitê, conselho gestor ou órgão equivalente, responsável por propor critérios de funcionamento e de interoperabilidade para edição futura de atos normativos. Ademais, somente a possibilidade de compartilhamento de dados com as agências de persecução penal é definida por lei, sendo que as outras ficam a cargo da gestão da base de dados.

Assim, na sistemática brasileira identificada, a previsão legal cumpre somente a função de conferir competência normativa para regulamentar o assunto em nível infralegal. Num segundo momento, quando os órgãos são questionados a respeito legalidade e finalidade dos tratamentos que estão realizando, apontam como fundamento a norma de competência, e não da norma autorizadora para o tratamento[233]. A consequência dessa política informacional é a necessidade de

---

[232] SALES; SALES SARLET, 2022, p. 62.

[233] A diferenciação entre norma de competência e autorizadora é realizada por Estelita: Mais concretamente: se se entendesse que normas (ainda que constitucionais) de competência consubstanciassem uma "carta branca" aos agentes

analisar normas administrativas para compreender o funcionamento de sistemas que, em última caso, permitem vigilância coletiva para a segurança pública.

Como dito acima, o conceito de separação informacional como limite institucional é inexiste a nível legal, tendo em vista que lei de regência usa variações da expressão "nos limites das respectivas competências*"* para determinar as diferenças de finalidades entre os órgãos públicos, com a delegação da regulação para normas infralegais. Em resumo, o Brasil optou por uma governança digital baseada na unicidade informacional, e o pior, o regramento é realizado a nível infralegal, que para além do déficit de legitimidade, cria outros problemas práticos.

A delegação da organização informacional a decretos cria riscos reais de que a troca de governo tenha capacidade de modificá-la complemente, implementando-se um viés mais securitário, por exemplo. Como se abordará no próximo subtópico, as bases de dados do SINESP alimentam a plataforma de inteligência Córtex, que permite vigilância em tempo real de carros, pessoas e deslocamentos populacionais. Assim, a gestão por decreto pode ser instrumentalizada para permitir perseguições políticas a pessoas expostas, em um ambiente opaco.

Por fim, a estratégia da inteligência de segurança pública brasileiras autoriza medidas de intervenção informacional por lei, mas todos os critérios de funcionamentos dos sistemas são criados por decretos administrativos, isto é, a legislação não tem objeto definido. Com efeito, o alerta realizado por Greco em 2018 estava correto: a ideia de sistemas unificados não é motivo de escândalo, tampouco a implementação de uma política informacional que desconsidera complemente o limite institucional imposto pela separação de funções, em decorrência da observância da proteção de dados enquanto garantia fundamental.

A ideia é criar grandes repositórios unificados de informações para prevenir à criminalidade, o efeito prático é a vigilância ilegal da população. Para aprofundar os riscos, antes de concluir o capítulo, o próximo subtópico analisa as intervenções informacionais do sistema CORTEX, conectando-o com o problema de pesquisa.

3.3.1. O problema de pesquisa e a plataforma CÓRTEX

---

estatais para que, a pretexto de "bem" cumpri-las, por exemplo, aplicassem uma sanção penal sem o devido processo legal (art. 5º, LIV, da CF) ou privassem o cidadão de parte de seu patrimônio (art. 5º, caput e XXII, da CF), o sistema constitucional de proteção de direitos fundamentais ruiria duas ou três páginas à frente de sua consagração, pois as regras de competência se sobreporiam às normas garantidoras de direitos fundamentais. ESTELITA. 2021, p. 612.

O Ministério da Justiça implementou a plataforma de inteligência Cortex, criado pela portaria 218/2021 que, segundo preâmbulo, "Dispõe sobre a Plataforma Integrada de Operações e Monitoramento de Segurança Pública – Córtex"[234]. A abrangência da medida informacional não é definida objetivamente na portaria, ou seja, quais as ações de monitoramento são possíveis – o que, como já se disse, deveria ser previsto legalmente, em linha com o marco teórico do teórico da tese. Entretanto, mais uma vez, mesmo se tratando de portarias administrativas, não há previsão de procedimentos detalhados para a implementação da intervenção informacional.

A portaria limita o uso do Córtex para a segurança pública[235], mas não há informação suficiente a respeito de quais órgãos são considerados como parte desse setor de atuação, podendo-se presumir que o artigo se refere aos integrantes do SUSP. Esse rol já seria muito abrangente, tendo em vista que compreende órgãos que não realizam atividades próprias de segurança pública, a exemplo dos bombeiros e a guarda portuária. Além disso, o Conselho Nacional do Ministério Público (CNMP) aderiu à utilização do sistema[236], de modo que, ainda que se reconheça os poderes investigatórios dessa carreira, eles não se confundem com a segurança pública.

Avançando sobre as funcionalidades do sistema de inteligência, o Córtex realiza monitoramento de alvos móveis com utilização da leitura de placas automatizadas no território nacional, que são cruzadas com outras bases disponíveis pelo SINESP, para identificar civilmente os alvos e cercamentos digitais[237]. Barreto e Dias descrevem aspectos desse monitoramento[238]:

> [...] o "alvo móvel" é cadastrado ao passar por uma câmera com capacidade de leitura de placas e é necessário apenas dois segundos para que agentes de inteligência ou policiais interessados sejam avisados por meio de push no aplicativo do celular. Assim, é possível continuar monitorando o alvo, mandar o policial mais próximo tentar abordá-lo ou cruzar as informações do veículo e seu proprietário com diversas outras à disposição do governo federal.

A plataforma é alimentada por bases de dados do SINESP e outras à disposição do SUSP,

---

[234] BRASIL. Ministério da Justiça e Segurança Pública. Portaria nº 218/ 2021.
[235] BRASIL. Ministério da Justiça e Segurança Pública. Portaria nº 218/ 2021. Art. 6º.
[236] Disponível em: https://www.cnmp.mp.br/portal/todas-as-noticias/15672-cnmp-mpf-e-ministerio-da-justica-firmam-acordo-para-acesso-a-plataforma-integrada-de-operacoes-e-monitoramento-de-seguranca-publica. Acessado em 10/10/2025.
[237] BRASIL. Ministério da Justiça e Segurança Pública. Portaria nº 218/ 2021, Art. 5º, IV e art. 4º, VIII.
[238] BARRETO, Alana; DIAS, Clara. A exposição da privacidade diante da falta de transparência: um estudo sobre o Córtex, 2023, p. 713.

somada à realização de acordos de cooperação técnica com outros órgãos de todos os entes federativos. Nesse contexto, o monitoramento é efetivado com o reúso de variadas de informações coletadas por órgãos públicos, a exemplo do compartilhamento do "Rais (Relação Anual de Informações Sociais, do Ministério da Economia), que possibilita o acesso às informações sobre salários, trabalhos e deslocamentos junto ao monitoramento das placas de veículos"[239].

O grau de opacidade do sistema, que é consequência da constituição por meio de atos administrativas infralegais, impossibilita o dimensionamento do poder computacional do Córtex, que só pôde ser mensurado após vazamentos à imprensa. Nesse sentido, segundo informações de fontes abertas, o Córtex é capaz de realizar a vigilância em tempo real com a utilização de 36 mil câmeras de segurança, que podem ser acessados por mais de 55 mil agentes de segurança pública[240]. Além disso, o sistema conta com dados de bilhetagem do transporte público, cadastro de empregados, notas fiscais, cadastro do SUS, restrições judiciais sobre veículos, manifesto de cargas rodoviárias, lista de pessoas politicamente expostas, cookies de sites públicos etc.[241]

Esse reúso é normalizado por parte da doutrina. Com tal viés, Aras comenta com acriticamente que o Córtex: "ao longo dos anos, o sistema se ampliou e passou a ser usado largamente pela Polícia Rodoviária Federal e pela Receita Federal em suas atividades fiscalizatórias, mediante acesso pela Rede Infoseg, da Secretaria Nacional de Segurança Pública (SENASP)"[242], sem comentários adicionais a respeito da legalidade na implementação e utilização. Assim, para parte da doutrina, o monitoramento só parece ser polêmico quando se utiliza reconhecimento facial com inteligência artificial[243].

Da perspectiva tecnológica, o sistema consolida bases de dados de órgãos de todos os entes federativos e por isso é tão capilarizado e abrangente, ou seja, realiza vigilância nacionalmente. Juridicamente, o objetivo é alcançado com a criação do SUSP e a realização de acordos de

---

[239] BARRETO; DIAS, 2023, p. 713

[240] VALENTE, Rubens; FREITAS, Caio de. Ata revela 'consultas irregulares' em sistemas de vigilância do Ministério da Justiça. Agência Pública, 21 jan. 2025. Disponível em: https://apublica.org/2025/01/ata-revela-consultas-irregulares-em-sistemas-de-vigilancia-do-ministerio-da-justica/. Acesso em: 9 out. 2025.

[241] Disponível em: https://www.cnmp.mp.br/portal/todas-as-noticias/15672-cnmp-mpf-e-ministerio-da-justica-firmam-acordo-para-acesso-a-plataforma-integrada-de-operacoes-e-monitoramento-de-seguranca-publica. Acessado em 10/10/2025.

[242] ARAS, Vladimir. Cerco Digital ("Geofence") e Varredura Terminológica: Balizas Constitucionais e Legais. In: SALGADO, Daniel de Resende; BECHARA, Fábio Ramazzini; GRANDIS, Rodrigo de (Coords.). 10 Anos da Lei das Organizações Criminosas: Aspectos Criminológicos, Penais e Processuais Penais. Almedina, p. 614, 2023.

[243] ARAS, 2023, p. 614 "Muito mais polêmicos são os sistemas automatizados de reconhecimento facial, por meio de modelos de machine learning. O Pacote Anticrime introduziu no art. 7º-C da Lei 12.037/2009".

cooperação técnica, que têm como fundamento jurídico a portaria de criação do Córtex, conforme já explorado. Por essa razão, a tese analisa um exemplo de acordo de cooperação para conferir compreensão completa sobre o tema, antes de concluir e fazer as considerações sobre as perguntas de pesquisa.

Em um dos documentos disponíveis em buscas abertas, encontrou-se a Ata da 46ª Reunião do CGDI (Comitê de Governança de Dados e Sistemas da Informação), que tem como objeto acordos de cooperação técnica com contrapartida do Ministério da Justiça. No referido documento, o item 4, referente ao processo 08335.002225/2023-2, dispõe sobre a parceria entre a Agência Estadual de Defesa Sanitária de Mato Grosso do Sul e a Superintendência da Polícia Federal daquele estado nos seguintes termos[244]:

> [...] cooperação técnica e operacional entre os partícipes, pelo qual a SR/PF/MS disponibilizará vagas em ações de capacitação para servidores do IAGROMS e possibilitará a doação de bens móveis, inclusive veículos, conforme disponibilidade; por seu turno, o IAGRO-MS concederá acesso aos sistemas de monitoramento e análise das propriedades das propriedades rurais, bem como acesso aos registros de passagens de veículos nas câmeras da instituição.

Em contrapartida por vagas de capacitação e pela possível doação de bens móveis e imóveis, o órgão sanitário estadual concede acesso aos sistemas de monitoramento por câmeras da instituição. Trata-se de uma hipótese clara de reúso de dados, uma vez que a norma – se houver e for materialmente válida – que autorizou a instalação de câmeras no Estado de Mato Grosso do Sul não o fez com a finalidade de permitir o compartilhamento das imagens para funções de segurança pública. O segundo ponto relevante é que o acordo foi firmado com a Polícia Federal, órgão de polícia judiciária que, portanto, não realiza policiamento preventivo e não deveria liderar iniciativas voltadas à obtenção de dados destinados à alimentação de sistemas de inteligência.

Diante do cenário exposto no subtópico, o Córtex é a materialização da conclusão realizada no Tópico 3.3., um sistema que funciona com base em unicidade informacional entre órgãos de competências distintas, sem observância à separação informacional como um limite institucional imposto pela proteção de dados no âmbito público. Ademais, a arquitetura informacional que permite a vigilância, em tempo real e retrospectiva, é de livre acesso para milhares de agentes de

---

[244] VALENTE, Rubens; FREITAS, Caio de. Ata revela 'consultas irregulares' em sistemas de vigilância do Ministério da Justiça. Agência Pública, 21 jan. 2025. Disponível em: https://apublica.org/2025/01/ata-revela-consultas-irregulares-em-sistemas-de-vigilancia-do-ministerio-da-justica/. Acesso em: 9 out. 2025.

segurança pública, prescindindo em todas as hipóteses de autorização judicial.

Especificamente em relação à pergunta de pesquisa, a racionalidade jurídico-processual brasileira é adequada para assegurar a licitude da aquisição, uso e reúso de dados pessoais no âmbito processual penal, em observância do princípio da finalidade?

A resposta é negativa. No que se refere a função de segurança pública, necessariamente anterior ao processo penal, a norma autorizadora da criação do SUSP é inválida materialmente pela inobservância da proteção de dados para regras as ações de coleta, uso e reúso de dados pessoais, especificamente a finalidade. Essa conclusão é confirmada pela análise dos sistemas de monitoramento empregados pelo Ministério da Justiça e Segurança Pública.

Para superar essa invalidade, a lei que autoriza a criação do sistema unificado deve prever: i) quais órgãos podem ter acesso a vigilância em tempo real, orientada à prevenção de perigos; ii) os critérios para o reúso de dados de órgãos públicos distintos não podem ser realizados por atos infralegais; iii) o fluxo informacional, sem autorização judicial, deve ser da segurança pública para a persecução penal; iv) a realização de cercamentos digitais depende de análises concretas de perigos a serem evitados pela segurança pública[245]; v) o monitoramento individual só é legítimo na situação flagrancial para garantir a efetividade da persecução penal futura[246].

Em relação ao processo penal, momento posterior para qual a vigilância identificou infrações penais, a resposta à pergunta de pesquisa também é negativa, tendo em vista que o acesso é unificado em tempo real e retrospectivo, sem diferenciação pelas funções exercidas pelos órgãos de persecução, ou seja, é impossível respeitar os limites da finalidade. Além disso, as agências de persecução não devem ter acesso à plataforma para realizar as medidas descritas nos pontos de i) a iv), descritas no parágrafo anterior.

O compartilhamento deve ser lido como uma nova intervenção que requer previsão legal, em razão disso, a autorização para uso retrospectivo e em tempo real da arquitetura informacional da segurança pública, para fins probatórios, depende previsão legal que preveja a reserva de jurisdição, na medida em que a vigilância individualizada é medida que atinge à autodeterminação individual do suspeito, e a observância dos critérios das medidas cautelares do processo penal.

---

[245] É o que se verifica, por exemplo, quando fontes abertas revelam que torcidas organizadas de futebol planejam um confronto. Nessa hipótese delimitada, o Estado pode recorrer previamente à arquitetura informacional disponível para monitorar a situação, de modo a garantir que a intervenção seja mais efetiva e segura, podendo fazer um cercamento digital da área.

[246] Um exemplo prático seria a detecção de um veículo roubado e o monitoramento em tempo real de seu trajeto, permitindo a prisão em flagrante do suspeito e a apreensão do bem.

Por fim, o entendimento em contrário sobre o monitoramento pessoal em tempo real e retrospectivo leva a possibilidade de que milhares de agente de segurança pública e de persecução penal possam obter informações relativas à vida privada de pessoas insuspeitas e ou contingentes populacionais inteiros, que são intervenções informacionais legítimas. Entretanto, o que a pesquisa encontrou como resultado não espelha as prescrições feitas acima, ao contrário, revelam o uso da coleta, uso e reúso de dados pessoais desmedidamente, baseada em atos infralegais.

4. ELEMENTO INFORMATIVO DIGITAL

Até agora, a tese abordou o uso de dados na segurança pública, desde a fase de arquitetura informacional para captá-los até o uso e reúso das informações. Contudo, não se utilizou a expressão "prova digital" para defini-los. Isso porque, conceitualmente, a ação penal é imprescindível para que elementos informativos possam ser classificados como prova, isto é, para serem apresentados como meio de prova em ação penal em contraditório, com observância aos demais axiomas do processo penal[247]. Por essa razão, os capítulos anteriores aplicaram o conceito de dados pessoais para se referir às informações úteis na segurança pública.

Neste e nos próximos capítulos, passa-se a utilizar o conceito de elemento informativo digital, na medida o "lugar" de análise da tese é depois da suspeição, mas anterior à ação penal: na fase investigação preliminar[248]. Essa escolha decorre do recorte axiológico do processo penal em sociedades democráticas que, como dito, a prova é produto do contraditório judicial. É claro, entretanto, que da perspectiva computacional, é possível a afirmar que os dados digitais são provas digitais desde a verificação da sua existência. o que não afasta a normatividade necessária para que se possa falar em prova como o produto da atividade processual.

O entendimento doutrinário mais comum para as provas digitais é analisá-las comparativamente em relação às tradicionais. Esse esforço é válido e permite corretas conclusões, mas deve-se reconhecer que, diante de realidades anteriormente inexistentes, o acréscimo do adjetivo "digital" não é garantia de adequação conceitual[249]. Dentre as características dessa nova realidade, tem-se a imaterialidade, a volatilidade, a replicabilidade e a necessidade de intermediação, que são categorias que se destinam a analisar o fenômeno digital à luz do direito.

A utilização dessas características permite a compreensão do objeto estudado estaticamente, o que, por óbvio, não é suficiente para regrar as situações processuais dinâmicas do processo penal[250]. A exemplo da afirmação, saber que as provas digitais dependem de suporte físico não permite nenhuma conclusão sobre como apresentar esse conteúdo na ação penal, apesar de ser uma abstração intelectual interessante. Desse modo, tais atributos servem para entender a realidade

---

[247] A exceção a essa regra são as hipóteses de produção cautelar, antecipada e irrepetível, que são trabalhadas adiante.
[248] LOPES JUNIOR, 2020, p. 181.
[249] RAMALHO, David da Silva. Métodos Ocultos de Investigação Criminal em Ambiente Digital. 1. ed. Coimbra: Almedina, 2017, p. 102.
[250] GOLDSCHMIDT, James. Prozess als Rechtslage: Eine Kritik des Prozessualen Denkens. [S.l.]: Springer, 1925, p. 268; 277; 280.

digital dos elementos digitais, mas oferecem pouco da perspectiva teórico-processual.

A imaterialidade é o aspecto menos controverso. De acordo com Danielle[251], o conteúdo do elemento digital não é palpável como um objeto físico. Ele é fruto do processamento computacional de sequências numéricas, que depende de um suporte informático para se tornar inteligível[252]. Assim, a prova digital existe independentemente do suporte, ainda que dependa dele para ser visualizada, como uma mensagem enviada em um código que não pode ser compreendida pelo destinatário; nesse caso, ela existe e não tem função probatória para o processo.

Já Denise Vaz, a respeito da volatilidade, conecta-a à fragilidade, pois esta "facilmente se submete a alterações ou desaparecimentos, bastando a modificação da sequência numérica"[253]. A alteração de um arquivo digital pode ocorrer até culposamente, dado que o manuseio de um arquivo pode alterar a composição e, eventualmente, a possibilidade de comprovação de sua veracidade. Para lidar com a volatilidade, é necessária a existência de remédios processuais adequados, que estão conectados com a urgência, já que podem deixar de existir tão rapidamente quanto foram criados. Talvez por isso seja conveniente falar-se da requisição em tempo real.

A respeito da replicabilidade, essa característica rompe com a ideia de originalidade. Não é possível dizer que um documento digital é original, pois todo arquivo que tiver a mesma sequência numérica será idêntico. Isso significa que as provas digitais podem ser reproduzidas infinitamente e, se não houver alteração, todas serão idênticas. Nesse sentido, para a função processual, a comprovação de que a cópia foi realizada de maneira adequada é suficiente para emprestar-lhe utilidade probatória, ou seja, transladá-la ao processo por meio de prova. Isso significa que a mesma prova pode estar dispersa em mais de um lugar ao mesmo tempo[254].

Entre o código digital e a compreensão pelo cérebro humano, é necessária a intermediação técnica de um *hardware*. Essa estrutura decodifica a sequência produzida por dispositivos eletrônicos e a entrega em formato inteligível, como música, documento de texto, áudio etc. O interessante é que o acesso à prova pode depender do acesso ao meio em que ela está armazenada, uma vez que o suporte é necessário para traduzi-la, mas, além disso, é imprescindível para a existência do conteúdo informacional. Diante disso, a apreensão dos dispositivos que geraram

---

[251] DANIELE, Marcello. La prova digitale nel processo penale. Rivista di Diritto Processuale, v. 66, n. 2, 2011, p. 284.
[252] MASON, Stephen; SENG, Daniel. Electronic Evidence. Londres: Queen Mary Univeristy of London, 2017, p. 26.
[253] VAZ, 2012, p. 69.
[254] Nessa linha, nada impede que o elemento seja utilizado como em um remédio constitucional e na ação penal, ao mesmo tempo, sem ter por que falar-se em cópia ou original.

determinado arquivo ou que somente armazenaram a informação pode ser útil a investigações, situação jurídica que Geraldo Prado denomina de prova digital offline[255].

Como dito, a descrição dessas características estaticamente contribui muito pouco para o campo de estudo, tendo em vista que o processo penal é uma situação processual dinâmica. A pergunta correta a se fazer é como esses elementos se conectam com a teoria da prova, em outras palavras, sua conexão com as formas de produção e de ingresso no processo penal. Dessa forma, quais são os problemas práticos que essas características criam e as maneiras conceitualmente adequadas de endereçá-las? Algumas delas foram rapidamente inseridas após a descrição das características doutrinárias, e serão aprofundadas adiante.

Na dimensão estática, os dados de conteúdo são inteligíveis diretamente pelo cérebro humano, a mensagem de texto, o vídeo, a foto são o produto da comunicação ou do registro de pensamento do usuário de dispositivos eletrônicos. Já os dados cadastrais permitem a identificação do usuário de produtos digitais, assim como os proprietários de domínios de sites. Por fim, os dados brutos são registros digitais que não permitem a compreensão sistematizada do conteúdo sem análise; são o resultado, por exemplo, da cópia de um dispositivo eletrônico; em princípio, antes de mineração e análise, eles não permitem inferências nem comprovação de assertivas.

O metadado é a informação sobre um dado digital. Sua conceituação costuma aparecer na legislação vinculada à função que exerce. Por exemplo, a definição de dados de tráfego pelo Marco Civil da Internet refere-se aos metadados que a navegação na internet produz[256], o mesmo acontece com os dados de acesso a aplicativos. A informação mais relevante é que ele está associado à sua principal característica: ele existe antes do dado de conteúdo como condição para a "comunicação" entre dispositivos eletrônicos, na linguagem computacional, os protocolos de comunicação[257]. Para a função probatória, os metadados estão no cerne da cadeia de custódia[258].

Avançando para as situações dinâmicas processuais, há duas observações a serem feitas. A primeira questão é temporal. O contraditório na ação penal é considerado o momento ideal para a

---

[255] Segundo o autor, "A prova digital off line é aquela coletada no âmbito de buscas que apreendem fisicamente os dispositivos informáticos visados – smartphones, desktops, notebooks". PRADO, 2024, p. 249.
[256] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. Espaço Jurídico Journal of Law, 2011, p. 92.
[257] DONEDA, Danilo. Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados, 2019, p. 130-135.
[258] PRADO, 2024, p. 251.

produção da prova, de modo que o que existe antes dele deve ter impacto cognitivo reduzido[259], constituindo o que se denomina elemento de informação, ainda que produzido mediante as exceções legais. O resultado probatório, que pressupõe o encerramento da instrução processual, é o conjunto de informações que se pode inferir com segurança das provas produzidas, as quais podem confirmar assertivas a respeito de fatos passados, para a realização de juízos de previsibilidade, que são precários e contingentes[260].

A segunda questão é de hipótese. Só é possível que exista um elemento de informação penal se houver uma hipótese investigativa– relativa à fase pré-processual – ou acusatória – própria da ação penal. Antes dessas formulações, as informações servem à finalidade extraprocessual para a qual foram criadas. Essa compreensão dinâmica é de utilidade ímpar para as provas digitais, na medida em que as correlações possíveis de serem feitas com os dados são imprevisíveis. Por isso, não se pode hierarquizar de forma absoluta o acesso às informações conforme sua função imediata, a exemplo do uso irrestrito de dados cadastrais[261].

Essas proposições, em conjunto com a nomenclatura de dados utilizada pelo direito da União Europeia[262], permitem definir elemento informativo digital como gênero das seguintes espécies: dados de conteúdo, dados cadastrais, dados brutos e metadados. A diferenciação é oportuna porque permite uma utilização adaptável a cada situação. Por exemplo, o metadado pode ser a prova em si da localização ou a metaprova de que um documento é verídico. O uso, portanto,

---

[259] Ideia semelhante é trabalhada por Assis Moura, com a utilização da nomenclatura indícios. (MOURA, Maria Thereza Rocha de Assis. A prova por indícios no processo penal. Rio de Janeiro: Lumen Juris, 2009, p. 99)

[260] Partimos de uma epistemologia que concebe o processo penal como um espaço cujo centro cognitivo reside nas garantias processuais. Nessa perspectiva, reconhecem-se os limites da cognição humana e, por conseguinte, a impossibilidade de reconstrução integral dos fatos pretéritos, de modo que a atividade probatória produz apenas uma aproximação contingente e incompleta da denominada verdade real. Trata-se de uma orientação de matriz subjetivista, na qual a certeza judicial se funda na coerência e na aceitabilidade racional das afirmações probatórias, em linha com as doutrinas de Aury Lopes Jr. e Paolo Ferrua. Em sentido oposto, situam-se as correntes objetivistas, que pressupõem a correspondência entre enunciados probatórios e a realidade fática, admitindo, ao menos em tese, o atingimento da verdade no processo penal. Para essas correntes, modelos racionalistas são úteis para assegurar a controlabilidade racional da atividade probatória, sendo as doutrinas de Gustavo Badaró, em certa medida, e Michele Taruffo representativas dessa orientação.

[261] Dora Eilberg aduz que: "A tradicional relação do grau de proteção às diferentes categorias (cadastrais, de tráfego, de conteúdo) para determinação da reserva jurisdicional proveniente da dogmática alemã possui respaldo na Convenção de Budapeste e, na perspectiva nacional, no Marco Civil da Internet, mas é uma concepção ultrapassada que não dá conta dos desafios atuais das novas tecnologias. (EILBERG, Daniela Dora. Fluxo de dados, prova e processo penal. Revista da Faculdade Mineira de Direito, v. 27, n. 54, 2024, p. 29-54.)

[262] Art. 3º, 8: «Prova eletrónica», dados de assinantes, dados de tráfego ou dados de conteúdo, conservados em formato eletrónico, por um prestador de serviços ou em seu nome, no momento da receção de um certificado de ordem europeia de produção (COEP) ou de um certificado de ordem europeia de conservação (COEC). (UNIÃO EUROPEIA. Regulamento (UE) 2023/1543, cit., art. 3º, n. 8.).

é determinado pela hipótese, que será determinado pelas informações analisadas conjuntamente pelo investigador. Amplamente, o valor epistêmico da prova deriva de uma rede de inferências[263].

Por último, o capítulo visa a descrever e debater outras categorias dogmáticas processuais quando necessário para a superação de pontos específicos. Cabe destacar que o método utilizado é o de debater as categorias processuais em razão da sua finalidade dinâmica. Ademais, o não abandono completo das categorias estáticas, formuladas paras as provas analógicas, justifica-se pelo fato de que algumas delas são previstas legalmente, devendo-se analisá-las.

4.1. A deflagração da investigação preliminar

A partir da suspeita de que uma infração penal tenha sido cometida, o poder-dever de punir do Estado deve ser exercido dentro dos limites e das formas estabelecidos pelo direito processual penal[264]. A prisão em flagrante, realizada por órgãos de segurança pública, e a notícia-crime são as formas mais comuns de dar início à fase pré-processual[265]. Contudo, a investigação também pode ser instaurada de ofício, especialmente em casos de conhecimento público ou notório dos fatos. Igualmente, a persecução penal pode ser iniciada por provocação, seja da vítima, de autoridade competente ou de testemunha. Em qualquer hipótese, a investigação deve ser formalizada, marcando o início da investigação preliminar, que atua como filtro para a fase processual.

No modelo brasileiro, o inquérito policial constitui a forma ordinária de investigação preliminar, mas não é o único. O sistema jurídico admite outras modalidades, tais como as comissões parlamentares de inquérito, os procedimentos investigatórios conduzidos pelos Ministérios Públicos e as investigações realizadas por órgãos com atribuições específicas[266]. Naturalmente, os elementos informativos produzidos nessa fase estão conectados à hipótese investigativa. Assim, quando se trata de um cibercrime, é inevitável que os meios de prova e os

---

[263] Esse conceito é trabalhado na teoria da prova de Anderson e Twining, que defende que o valor epistêmico da prova deriva na rede de conexões inferenciais interligadas, isto é, a informação isolada é somente um nó na cadeia de informações para a realização de inferências seguras. (ANDERSON, Terence; TWINING, William; SCHUM, David A. *Analysis of Evidence: How to Do Things with Facts*. 2. ed. New York: Cambridge University Press, 2005.)

[264] De acordo com Vasconcellos, "variando desde um mero instrumento para realização do direito material até um mecanismo de resolução de conflitos e pacificação social, o processo penal é um dispositivo inerente à racionalidade e à concretização do poder punitivo na sociedade. (VASCONCELLOS, Vinicius Gomes de. Fundamento e função do processo penal: a centralidade do juízo oral e sua relação com as demais fases da persecução penal para a limitação do poder punitivo. Revista Eletrônica de Direito Processual, Rio de Janeiro, v. 19, n. 2, 2018, p. 230-231.)

[265] FERNANDES, Antonio Scarance. Teoria Geral do Procedimento, 2005, p. 35.

[266] BADARÓ, Gustavo Henrique. Processo Penal. 2ª ed. Rio de Janeiro: Elsevier, 2013, p. 65.

dados necessários à verificação de autoria e materialidade tenham natureza digital.

Ainda que não se trate de um cibercrime, é virtualmente impossível que as investigações preliminares não dependam de elementos informativos digitais para o cumprimento de sua função processual[267]. Isso se evidencia já na prisão em flagrante, em que, entre os objetos apreendidos durante a busca pessoal, podem conter dispositivos eletrônicos. Da mesma forma, no primeiro ato de desenvolvimento da investigação preliminar[268] – a ida ao local da infração penal e o isolamento da área para preservação de vestígios –, é comum que se encontrem aparelhos eletrônicos sujeitos à apreensão e à análise pericial, como câmeras, sensores e outros dispositivos digitais.

Em regra, os atos de iniciação e de desenvolvimento da investigação preliminar não dependem de autorização judicial, uma vez que encontram prévia autorização legal para conferir o impulso oficial às investigações. Contudo, com o avanço das tecnologias da informação, o legislador passou a prever expressamente determinadas medidas investigativas de natureza informacional já nos atos iniciais da persecução penal como resposta à mudança social também ocorrida, criando-se situações em que a reserva de juiz pode ser imprescindível para o levantamento de sigilos. Exemplos disso são a requisição de dados e o acesso aos dados que permitam a geolocalização em tempo real de suspeitos e vítimas de determinados crimes[269].

A estruturação teórica do processo penal está lidando com uma nova realidade: a emergência da apreensão do elemento digital na fase de investigação preliminar, o que antecipa para a investigação o objeto da ação penal. Vale lembrar que a cognição realizada na investigação preliminar é instrumental e limitada quanto à existência do fato[270]. Assim, o alerta de Vasconcellos é adequado, a fase pré-processual cumpre função de "assegurar a produção de eventuais provas irrepetíveis, além de propiciar elementos para eventuais decisões judiciais em sede cautelar"[271].

---

[267] DANIELE, Marcello. La prova digitale nel processo penale. Rivista di Diritto Processuale, Padova, v. 66, n. 2, mar./abr. 2011, p. 283.

[268] A diligência ao local do crime foi colocada conjuntamente aos meios de obtenção de provas digitais por paralelismo explicativo do texto, na medida em que permite a apreensão de dispositivos digitais após o isolamento da área e de sua liberação por peritos. Contudo, é mais adequado conceituá-la como atos de desenvolvimento do inquérito, previsto nos artigos 6º e 7º, do CPP. De acordo com a legislação de regência, a autoridade policial deve se dirigir ao local, isolá-lo, apreender objetos que tenham relação com o crime, e colher todas as provas que servirem ao esclarecimento de infração penal, segundo leitura conjunta dos incisos I, II e III do artigo 6º, do CPP. Neste ponto, trata-se de mais um exemplo no qual se faz a leitura de dispositivos digitais como "objetos" ou "provas" sem haver diferenciação para as fontes de prova digital.

[269] BRASIL. Código de Processo Penal, art. 13-B.

[270] GLOECKNER, Ricardo; LOPES JR., Aury. Investigação Preliminar no Processo Penal. 6ª ed. São Paulo: Saraiva, 2014, p. 176.

[271] VASCONCELLOS, 2018, p. 233.

Os atos procedimentais realizados no âmbito da investigação preliminar têm por finalidade fundamentar uma hipótese sobre um fato aparentemente típico e ilícito, bem como identificar seus autores, coautores e partícipes[272]. Nesse contexto, a investigação preliminar, dotada de dupla função pré-processual, destina-se tanto a possibilitar a propositura da ação penal quanto a evitá-la, na hipótese de ausência de elementos mínimos de materialidade e autoria. Tais elementos são encaminhados ao titular da ação penal – no sistema brasileiro, aos membros do Ministério Público – a fim de subsidiar a decisão de oferecer denúncia ou arquivamento[273].

Outra função da investigação preliminar que deve ser destacada é o acautelamento de elementos de informação[274], sobretudo no que se refere a dados digitais, que são voláteis. Contudo, tal preservação pode culminar num recorte informacional irreversível para a ação penal, em prejuízo ao direito de defesa. Portanto, a universalidade da prova digital exige a superação de entendimentos restritivos a respeito do direito de defesa na fase preliminar[275], uma vez que um simples critério técnico apresentado por investigados pode alterar o recorte informacional realizado por investigadores. Esse argumento leva em consideração a alteração de uma variável nas investigações: o volume de dados disponíveis exige recortes automatizados.

No contexto de expansão do direito de defesa na fase preliminar, é possível observar alterações na cultura processual penal brasileira, a exemplo da consolidação do direito de acesso aos autos pelo STF, especialmente com o enunciado da Súmula 14[276]. Esse entendimento permite o conhecimento e faculta a reação da defesa, que pode requerer diligências e questionar a condução de atos de investigação, contribuindo com suas funções. Ademais, a consolidação das investigações defensivas[277] também servem a acautelar informações para a ação penal.

A universalidade da prova digital[278], cujos elementos são essencialmente voláteis[279], revela também que o contraditório mitigado, como fundamento teórico do processo penal para justificar a ausência de defesa na fase pré-processual, tem como consequência a necessidade de criação de

---

[272] Artigos 4º e 12 do Código de Processo Penal.
[273] SAAD, Marta. Editorial do dossiê "Reformas da investigação preliminar e a investigação defensiva no processo penal" - Investigação preliminar: desafios e perspectivas. Revista Brasileira de Direito Processual Penal, Porto Alegre, v. 6, n. 1, jan./abr. 2020, p. 29-40.
[274] SAAD, Marta. Direito de defesa na etapa preliminar da apuração penal: reconhecimento, novas perspectivas e desafios. Boletim IBCCRIM, São Paulo, v. 32, n. 381, 2024, p. 14.
[275] VASCONCELLOS, 2018, p. 234.
[276] BRASIL. Supremo Tribunal Federal, 2029, Súmula 14.
[277] MACHADO, André. Investigação criminal defensiva. 1. ed. São Paulo: Revista dos Tribunais, 2010, p. 111.
[278] DANIELE, 2011, p. 284.
[279] VAZ, 2012, p. 69.

critérios sistêmicos adicionais para admissão do elemento digital na ação penal. Por outro lado, pode-se defender que o ideal é que haja direito de defesa contínua e ampla na fase preliminar[280], o que exigira o direito a representação técnica. Independente da solução, os argumentos colocados demonstram que o momento de maior relevância epistêmica do elemento digital está situado, por razões da natureza informacional ou prática, na fase investigativa. Entretanto, é precisamente nessa fase em que há menos limites cognitivos definidos legal ou doutrinariamente, com a indefinição de direitos dos investigados, em relação à atividade cognitiva e à representação técnica.

Os produtos da investigação preliminar são base para outras medidas investigativas, inclusive aquelas sujeitas à reserva de jurisdição. Contudo, em razão da mitigação dos princípios reitores do processo penal na fase pré-processual, especialmente o contraditório – seja por razões teóricas, seja em virtude da realidade da grande maioria das investigações preliminares –, o resultado das diligências realizadas nessa fase consiste em um conjunto de elementos informativos que não se confundem, do ponto de vista principiológico, com provas, aqui entendidas como os elementos aptos a fundamentar uma sentença penal condenatória isoladamente.

Por último, como adverte Taruffo, "a teoria das provas é rica de vocábulos, mas é bastante pobre de conceitos confiáveis e rigorosamente formulados"[281], que é precisamente o estado da arte sobre os elementos digitais, caracterizado pela ausência de regra para a arquitetura informacional, pela fragilidade nos limites de ingresso na investigação preliminar e pela falta de critérios para admissão e valoração na ação penal. Portanto, o texto aborda numa ordem cronológica prática, os dilemas impostas na busca e, eventualmente, da produção probatória na fase pré-processual.

4.2. O elemento informativo no tempo processual

Os atos de investigação não têm como função o convencimento do julgador, uma vez que não servem a um juízo de certeza na ação penal[282]. Essa diferenciação entre os produtos da investigação e da ação penal foi inserida, tardia e laconicamente, na legislação brasileira, a qual

---

[280] Nesse sentido é a defesa de Marta Saad, "o exercício do direito de defesa, eficaz e tempestivo, deve se iniciar no inquérito policial, permitindo-se então a defesa integral, contínua e unitária. Há de se garantir ao investigado em inquérito policial o exercício do direito de defesa, possibilitando a ele o direito de conhecimento do teor do inquérito policial, de contraposição a todas as acusações, com a assistência de advogado, com a possibilidade de manter-se silente e a admissibilidade de produção das provas por ele requeridas". SAAD, 2024, p. 14.
[281] TARUFFO, Michele. La prova dei fatti giuridici - nozioni generali. Milano: Giuffrè, 1992, p. 413-414.
[282] GLOECKNER; LOPES JUNIOR, 2014, p. 207.

dispôs que o convencimento será livre sobre o que for produzido em contraditório judicial, não podendo fundamentar-se exclusivamente em elementos informativos da investigação[283]. A outra consequência da alteração é a permissão expressa para que determinadas provas sejam produzidas em momento anterior ao contraditório, que devem ser justificadas factualmente na urgência ou emergência[284].

A redação do artigo é questionável. A utilização do adjetivo "livre", vinculado ao convencimento, é uma porta hermenêutica ampla, que somada ao "exclusivamente", permite a utilização do produto na investigação para o convencimento do julgador. É óbvio, entretanto, que a interpretação gramatical do dispositivo, se filtrada constitucionalmente, não seria um problema, já que o contraditório é um imperativo axiológica do modelo acusatório, de modo que sua força normativa afastaria a interpretação literal inadequada. Essa não observância serve, muitas vezes, a legitimar condenações da criminalidade de rua baseadas apenas nas palavras dos policiais[285].

Ainda que timidamente, pode-se afirmar que houve a introdução do conceito de "elementos de informação" na legislação brasileira, o que deve derrogar a utilização dos "indícios" como meio de prova, como erroneamente previsto na legislação processual penal[286]. O fato é que a distinção obtida pela doutrina internacional e nacional recebeu algum amparo legislativo, distinguindo os atos de prova dos atos de investigação, além de limitar sua força valorativa pelo destinatário da prova, o julgador da ação penal, que se convencerá da culpa ou não. Por outro lado, dá lugar a diferenciações doutrinárias pouco aplicáveis, especialmente aos elementos digitais.

Os atos de prova cabem às partes processuais e constituem ônus para acusação e faculdade processual para a defesa. Ambos se destinam à captação do convencimento motivado do julgador da causa. O resultado processual desses atos compõe o quadro fático que será valorado na sentença, conforme o atingimento do *standard* probatório: certeza para condenação e dúvida para absolvição. Nesta fase, com acusação formal recebida, aplicam-se plenamente as garantias do réu, tais como

---

[283] O art. 155 do Código de Processo Penal (CPP) afirma: "O juiz formará sua convicção pela livre apreciação da prova produzida em contraditório judicial, não podendo fundamentar sua decisão exclusivamente nos elementos informativos colhidos na investigação, ressalvadas as provas cautelares, não repetíveis e antecipadas". BRASIL. Decreto-Lei nº 3.689, de 3 de outubro de 1941. Código de Processo Penal. Brasília, DF: Presidência da República, art. 155.
[284] CORDEIRO, 2024, p. 114-115.
[285] Em pesquisa de Haber e Maciel, que analisou um universo de 3.700 sentenças proferidas entre 2014 e 2016 no Rio de Janeiro, as testemunhas policiais foram as únicas em 62,33% dos casos; dentre esses, 80% resultaram em sentenças condenatórias. HABER, C. D.; MACIEL, N. C. A. As sentenças judiciais por tráfico de drogas na cidade e Região Metropolitana do Rio de Janeiro. Cadernos de Segurança Pública, v. 10, n. 10, p. 1–16, 2018.
[286] Capítulo X do CPP, posicionado topograficamente no Título VII, destinado a provas (BRASIL, 1941).

direito a advogado, o conhecimento de todos os elementos, a imediaticidade na reação e o contraditório processual. Lopes Junior e Glockener nomeiam seis características próprias dos atos de prova: a) estão dirigidos a convencer o juiz da verdade de uma afirmação; b) estão a serviço do processo e integram o processo penal; c) dirigem-se a formar um juízo de certeza - tutela de segurança; d) servem à sentença; e) exigem estrita observância da publicidade, contradição e imediação; f) são praticados ante o juiz que julgará o processo.[287]

Esses atos não se confundem com os atos de investigação, cuja finalidade e instrumentalidade estão conectadas à investigação preliminar, geralmente o inquérito conduzido por polícias judiciárias ou por magistrados de instrução, a depender da característica do sistema processual. Os atos de investigação são próprios das autoridades policiais e dos órgãos administrativos com competências específicas, realizados de ofício ou mediante comunicação, por qualquer meio idôneo, que utilizam as prerrogativas legais, principalmente o poder de requisição[288], para averiguar a probabilidade de que um fato-crime tenha ocorrido.

Parte da doutrina entende que há atos de instrução nos inquéritos policiais[289], a consequência dessa argumentação é a necessidade de trasladar características dos atos de provas aos atos de investigação, a exemplo da imediaticidade, publicidade e contradição por defesa técnica, em outras palavras, defender o direito de defesa pré-processualmente. Não se desconhecem as exceções que justificam tal posição, mas é necessário estabelecer um modelo ideal diferenciador das fases pré-processual e processual, que permita a justificação criteriosa das exceções aplicadas. Ao nosso ver, a melhor forma de diferenciar os referidos atos é por suas finalidades, tal como visto acima nas seis características dos atos de prova e das funções da investigação preliminar.

Nesse contexto, o exemplo da confissão do investigado ou réu é elucidativo para o argumento apresentado. De acordo com Lopes Junior e Gloeckner, "eventual confissão obtida nesse momento [inquérito] tem um valor endoprocedimental, como típico ato de investigação e não ato de prova"[290]. Ainda que não haja diferença ontológica entre confessar na polícia ou em juízo, à

---

[287] GLOECKNER; LOPES JUNIOR, 2014, p. 206.
[288] A prerrogativa conferida por lei à autoridade policial e ao Ministério Público para exigir, de forma direta, informações, dados, documentos e a realização de perícias de órgãos públicos ou entidades privadas para instruir uma investigação criminal. GLOECKNER; LOPES JUNIOR, 2014.
[289] Pitombo e Saad utilizam da categoria de atos de instrução, conceitos utilizados no direito brasileiro desde o império. Para essa vertente, as autoridades administrativas produzem atos de instrução ao longo da investigação preliminar que servem para aparelhar a decisão judicial de recebimento da acusação ou deferimento cautelar. Diz-se, portanto, que haveria atos de investigação (procura de fontes) e instrução (formulação de conhecimento) na fase preliminar.
[290] GLOECKNER; LOPES JUNIOR, 2014, p. 210.

primeira faltam características principiológicas e formais para se constituir como uma prova[291]. É dizer, de outra maneira, que a forma processual – e a consequente garantia para cada ato –alteram a interpretação jurídica sobre uma situação semelhante ontologicamente.

De forma geral, os atos de prova na fase preliminar devem estar conectados à proteção da fase processual ou do bem jurídico tutelado pela norma penal material. Por configurarem exceção sistêmica, dependem de justificação legal específica e, em razão dessa natureza, exigem critérios adicionais de admissibilidade na ação penal. Isso porque, como articulado anteriormente, o produto do ato de investigação é o elemento informativo que serve para fundamentar a acusação e as medidas de investigação ocultas – ou cautelares reais e pessoais –, atividade sobre a qual deve incidir o contraditório admissão e valoração na ação penal subsequente.

Não é viável, portanto, a separação absoluta entre as categorias de atos de prova e atos de investigação. Entretanto, a antecipação de produção de provas requer a identificação de motivo específico, com fundamento legal de caráter excepcional. A afirmação em sentido contrário levaria a defesa de investigações exaurientes do objeto, excedendo-se a função de ministrar os elementos informativos mínimos para a acusação ou arquivamento, em outras palavras, à burla sistemática do momento ideal da produção probatória. Diante disso, reafirma-se que a principal função da fase pré-processual é ser um filtro para que acusações infundadas não cheguem ao judiciário.

Essa filtragem preliminar pode ser identificada em três funções: a busca do fato oculto, a função simbólica da investigação e a redução de acusações infundadas[292]. A primeira delas toca diretamente o objeto da tese porque, no ambiente digital, a regra é a presunção de sigilo dos atos praticados na internet; os clientes de empresas de tecnologia têm interesse, justificado nos contratos de uso e no Marco Civil da Internet, que suas informações sejam protegidas por políticas de privacidade. Em segundo lugar, as infrações penais quando são publicadas nas redes tendem a contar com pseudônimos e contas falsas para dificultar a real identificação dos autores.

Um simples crime cibernético dependerá da identificação usuários e, não raramente, o elemento informativo mínimo que confirme a probabilidade de um fato, aparentemente típico e ilícito, está sob custódia de empresas. É da natureza dessa criminalidade que certos atos de prova

---

[291] A diferença entre o ato de prova na investigação e o ato de instrução processual é principiológica, pois não é prova em razão da ausência de contraditório, condição imposta pelo devido processo legal para a formação dos elementos valoráveis. Essa distinção ganha relevância no contexto da prova digital, em que as fontes eletrônicas permitem o acesso direto a dados inteligíveis, como imagens e vídeos, que dispensam interpretação especializada, ao lado de dados brutos, cuja compreensão exige processamento técnico, isto é, são constituídas tecnicamente.

[292] GLOECKNER; LOPES JUNIOR, 2014, p. 210.

ocorram na investigação preliminar, a exemplo do acesso a dispositivos e tratamento de dados como condição à sua continuação, sob pena de que a função de acautelamento de elementos voláteis perca a eficácia. Naturalmente, isso não autoriza investigações exaurientes com a finalidade de produzir juízo de certeza, mas permite a antecipação de atos de prova em razão de urgência e emergência, protegendo-se a lógica sistêmica de separação em fase pré-processual e processual.

Antes de avançar na especificação dos fundamentos legais que autorizam atos de prova na investigação, explica-se resumidamente que a tese se dedica ao problema posto na investigação preliminar, razão pela qual não articula de forma exauriente os critérios de admissão probatória pertinentes à ação penal. Contudo, deve ficar claro que os atos judiciais antecipados e o respectivo produto probatório dependem da observância do contraditório para ingressarem posteriormente na fase processual, ocasião em que se realizará o controle dos atos decisórios e do próprio ato de prova, a exemplo da verificação da cadeia de custódia, da observância ao princípio da finalidade no tratamento de dados e de quaisquer outras exigências cogentes.

Retomando a lógica da separação de fases e a necessidade de fundamento específico, somente em três situações, atos de prova na fase de investigação preliminar são justificáveis. Elas se referem a contingências da vida que são incontroláveis, a enfermidade da testemunha, o desaparecimento de um vestígio do delito com o decurso do tempo, a contemporaneidade da infração penal etc. Nestes casos, a finalidade da prova estará presente na investigação preliminar porque haverá um motivo idôneo a flexibilizar as garantias próprias da ação penal. Fala-se, portanto, em prova irrepetível, prova antecipada e prova cautelar[293] – conceito este afastado na tese.

Para parte da doutrina, a essas três espécies, que excepcionam o contraditório para a produção da prova, englobam também as provas pré-constituídas, "elementos de prova legitimamente preexistentes ao momento procedimental ótimo do ponto de vista do princípio do contraditório, na maioria das vezes anteriores ao eventual processo que lhes corresponda"[294]. Esse entendimento decorre da adoção das categorias conceituais de provas pré-constituídas e pós-constituídas, para o qual todo o tratamento de dados anterior ao processo se equipararia, para todos os efeitos, a um documento que existia antes da ação penal.

A primeira imprecisão desse raciocínio é que não se pode fazer uma conceituação estática

---

[293] LOPES JUNIOR, 2020, p. 180-187.

[294] SOARES, Gustavo Torres. Investigação criminal e inovações técnicas e tecnológicas: perspectivas e limites. 2014. 307 f. Tese (Doutorado em Direito Processual Penal) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2014, p. 45.

para uma situação dinâmica. Tem razão Badaró ao afirmar que a maioria dos elementos de informação existe para além do processo penal[295], pois foram elaborados para razões quaisquer que não a comprovação de hipóteses criminais. Ademais, considerar como pré-constituído algo que foi produzido para a investigação preliminar, para concluir uma hipótese ou permitir outros atos de investigação, é desconsiderar que ela seja sempre instrumental à ação penal, ou seja, exerça função de possibilitá-la ou inviabilizá-la. Esse erro advém da utilização de categorias conceituais da processualística civil a casos penais[296] [297], sem observar a dinâmica própria da investigação, que processa informações de diversas fontes para formar uma tese sobre determinado fato.

O elemento pré-constituído refere-se àquele que existe independentemente da hipótese criminal. Já as provas produzidas antecipadamente, sob o prisma do contraditório, surgem em razão da hipótese criminal, constituindo-se instrumentalmente em função de uma possível ação penal, ainda que na fase investigativa. A diferença deontológica se manifesta no âmbito da ação penal: tudo aquilo que foi produzido de forma instrumental a ela deve respeitar os meios típicos de investigação e, tratando-se de uso ou reúso de dados, deve observar o requisito de licitude, sob pena de invalidade. Naturalmente, os elementos pré-constituídos são trasladados à ação penal pelos meios de prova, sendo inaplicável falar em formas típicas de produção na investigação.

A aplicação dessa conceituação, criticável no contexto da universalidade da prova digital, equivale a sustentar que a ação penal teria como função apenas valorar o que foi produzido na fase pré-processual, considerando que boa parte das provas digitais depende de análise técnica especializada para se tornar inteligível, mas seria avaliada apenas pelo resultado obtido. Tal raciocínio é inadequado: é o meio processual que legitima o resultado, e não o contrário. Por isso, as provas pré-constituídas, antes da hipótese, não são exceções ao contraditório.

Por fim, antes de avançar para a análise dos meios de investigação em espécie, a tese reforça que as hipóteses em que a produção da prova é autorizada ainda na investigação preliminar devem

---

[295] BADARÓ, 2013, p. 276.

[296] A defesa de que as provas irrepetíveis, cautelares, são espécies do gênero pré-constituído, assim como um documento, foi replicada por Gustavo Torres com fundamento em obra do professor Piero Calamandrei, sobre o estudo sistemático dos procedimentos cautelares para processos cíveis e criminais, mais especificamente, Introduzione allo estudio sistematico dei provvedimenti cautelari.

[297] Jacinto Coutinho dedicou uma obra própria sobre o tema. (COUTINHO, Jacinto. *O papel do novo juiz no processo penal*. Crítica a Teoria Geral do Direito Processual Penal. Rio de Janeiro: Renovar, 2000). Da mesma forma, Aury Lopes cunhou, em ambiente jornalístico, pergunta que ilustra simbolicamente essa perspectiva (ROSA, Alexandre Morais da; LOPES JR., Aury. Limite Penal: Quando a Cinderela do Processo Penal ganha novas roupas. Consultor Jurídico, 28 jul. 2017. Disponível em: https://www.conjur.com.br/2017-jul-28/limite-penal-quando-cinderela-processo-penal-ganha-novas-roupas/. Acesso em 10 fev. 2021).

ser compreendidas como exceções sistêmicas. Por opção legislativa, as três categorias conceituais que excepcionam o contraditório judicial – sob a perspectiva do momento ideal de produção da prova – foram inseridas em um mesmo dispositivo do Código de Processo Penal. Com efeito, o artigo 155 estabelece o contraditório judicial como regra e ressalva "as provas cautelares, não repetíveis e antecipadas". A economia legislativa na descrição dessas categorias transferiu à doutrina o ônus de sua delimitação conceitual, como se passa a examinar nos subtópicos seguintes.

4.2.1. Elemento probatório cautelar

O elemento probatório cautelar é exceção à produção sob contraditório, em razão do risco de perder a oportunidade de produzi-lo contemporaneamente. Os meios de obtenção de prova autorizados judicialmente conectam-se a elementos que dependem de infraestrutura para captação e que, por sua própria natureza, não deixariam vestígios. A regra é que as pessoas façam ligações telefônicas protegidas pelo sigilo; logo, se houver necessidade de investigar pessoas específicas por esse meio de comunicação, é imprescindível a existência de uma estrutura prévia de registro.

O lugar-comum é chamar esse procedimento de prova cautelar por duas razões principais: a exigência de reserva de juiz – a decisão não é de mérito – e a proteção de um resultado útil para a ação penal. Nessa linha, esse tipo de prova faria o asseguramento cautelar de informações[298], utilizando-se a *ratio* das cautelares reais. Em concreto, o sequestro impede que o proveito da infração penal seja alienado, assegurando a efetividade de eventual perdimento definitivo. A comparação, contudo, evidencia a fragilidade do argumento majoritário, pois o sequestro é provisório e revogável a qualquer tempo, a prova cautelar, não.

Quando a interceptação telefônica confirma a hipótese da investigação, o que se tem é um elemento de prova pré-constituído, que pode ser apresentado na denúncia e que não será substituído posteriormente. Assim, caso seja admitido, o mesmo elemento que justificou a acusação poderá ser valorado na sentença. Parece, portanto, mais adequado dizer que a prova foi produzida antecipadamente na fase pré-processual e que ela já existe no mundo jurídico[299]. Ela não pode ser revogada, apenas excluída; e, se verificadas causas de ilicitude, deve ser desentranhada.

---

[298] DIAS, Fernando Gardinali Caetano. Prova cautelar, antecipada e irrepetível e o contraditório na investigação criminal. Revista Fórum de Ciências Criminais - RFCC, Belo Horizonte, v. 5, n. 10, jul./dez, 2018, p. 122.
[299] DIAS, 2018, p. 122.

No exemplo acima, do sequestro e perdimento, tem-se a cautelar que efetiva o principal. Apesar de a interceptação ser contemporânea, serve à finalidade de convencer o julgador – ato de prova. Explicadas as razões de discordância em relação ao conceito doutrinário majoritário, expresso explicitamente no direito posto, o que se chama de prova cautelar será, aqui, considerado como prova antecipada. O tema é relevante para a tese, pois os métodos ocultos e invasivos de investigação computacional antecipam a produção de provas digitais.

O termo "prova cautelar" só aparece uma vez em toda a legislação processual brasileira, exatamente como exceção à prova produzida em contraditório. Não há, portanto, conteúdo jurídico de prova cautelar, que é dado exclusivamente pela doutrina, com utilização por analogia da processualística civil. É, no mínimo, indesejável que um dos conceitos usados pela legislação para excepcionar um dos pilares essenciais do processo penal tenha o conteúdo depreendido a partir de um único artigo. Ademais, não há um procedimento para os processos cautelares, por isso, fala-se em provimento cautelar, mas não existem regras instrumentais para o processo cautelar[300].

Por fim, a assunção de que a prova cautelar deva ser tratada como prova antecipada gera consequências sistêmicas, isso porque a produção antecipada exige certo grau de contraditório. Nesse contexto, vale mencionar que tal defesa está em linha com o regramento do juiz das garantias, especificamente o art. 3-B, VII, do CPP, que exige audiência pública em contraditório para a antecipação probatória, quando não haja prejuízo à diligência investigativa.

4.2.2. Elemento probatório irrepetível

O tempo da vida e do processo não coincidem, o conceito de irrepetibilidade comprova essa afirmação. Quando a urgência pelo perecimento normal das coisas inviabilizar a produção da prova sob contraditório judicial na ação penal, a autoridade responsável pela investigação preliminar deverá adotar as medidas necessárias para produzi-la imediatamente. Assim, ao descobrir, de ofício ou mediante manifestação, um elemento informativo que potencialmente comprove a ocorrência de uma infração penal, devem ser tomadas diligências necessárias para resguardá-lo.

É um motivo intrínseco ao elemento de informação, isto é, próprio do objeto analisado. Nesse caso, é o regramento jurídico que se adequa aos limites naturais. Pode-se falar do hematoma

[300] BADARÓ, Gustavo. Ônus da prova no Processo penal. 1. ed. Revista dos Tribunais, 2003, p. 414-417.

da lesão corporal, cujo potencial epistêmico será resguardado como exame de corpo de delito[301], ou das evidências do local de um crime violento, das quais se fará a perícia dos elementos encontrados imediatamente[302], dentre outras muitas possibilidades. Ambos os exemplos têm meios de prova explícitos na legislação processual por se tratar de situações comuns.

Entretanto, como dito anteriormente, toda forma de produção antecipada de provas deve encontrar fundamento legal, o que não quer dizer que todas as formas de irrepetibilidade devam ser tipificadas. Isso porque a autorização legal para a produção dessas provas é dada na parte final do artigo 155 do CPP, disciplinando todas as hipóteses em que, em razão da característica do objeto, possa haver o risco de se perder a prova que seja útil para instrução processual. Portanto, a situação justificada de perecimento permitirá a produção mesmo que o ato não esteja tipificado processualmente.

O perecimento é geralmente trabalhado como uma das características dos dados digitais, inclusive como categoria que os constitui, isto é, os dados são voláteis e passíveis de apagamento. Então, o elemento digital pré-constituído deverá ser armazenado imediatamente após sua descoberta – e coleta – para que possa ser utilizado na fase processual[303]. Por outro lado, a situação não é tão simples a respeito dos dados que necessitam de processamento, elemento informacional a ser constituído, na medida em que a produção poderia vir a ocorrer somente na fase processual.

No caso dos dados que devem ser processados para produzir uma informação inteligível, sua preservação para posterior uso processual requer a existência de uma medida cautelar própria de congelamento de dados, inexistente na legislação brasileira. Entretanto, em razão da adesão à Convenção de Budapeste sobre o cibercrime, o Brasil se obrigou a inserir no ordenamento tal medida de preservação de dados digitais[304]. A questão de fundo será saber quando o processamento

---

[301] Art. 158 do CPP: "Quando a infração deixar vestígios, será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado". (BRASIL, 1941, art. 158).

[302] Art. 169 do CPP: "Para o efeito de exame do local onde houver sido praticada a infração, a autoridade providenciará imediatamente para que não se altere o estado das coisas até a chegada dos peritos, que poderão instruir seus laudos com fotografias, desenhos ou esquemas elucidativos" (BRASIL, 1941, art. 169).

[303] O dado bruto descoberto na investigação, como um vídeo da prática criminosa, será juntado aos autos como documento pré-constituído, sendo necessária a comprovação de sua origem e integridade por meio de metaprova de extração para que seja admitido no processo - situação claramente delimitada pelo conceito de cadeia de custódia. Já a informação processada, resultante da análise ou do tratamento técnico desses dados, será apresentada como elemento de informação indireto (laudos periciais, relatórios investigativos), cuja admissibilidade depende da observância do contraditório quanto aos limites da produção da informação e da interpretação especializada.

[304] Art. 16 da Convenção de Budapeste: Conservação expedita de dados informáticos armazenados. (BRASIL. Decreto nº 11.491, de 12 de abril de 2023. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. Brasília, DF: Presidência da República, art. 16.)

na fase pré-processual será considerado ato de investigação ou de prova.

A ressalva do artigo 155 do CPP não afasta o contraditório para a admissão das provas irrepetíveis, ao contrário, reforça-o. Se foram produzidas na investigação preliminar, é natural a exigência de metaprova que comprove a autenticidade, a veracidade, a confiabilidade e a integralidade na ação penal. Por essa razão, a interpretação contrária parece equivocada[305], pois o contraditório exercido para a admissão da prova possibilita sua exclusão dos autos pelas razões acima citadas, verificáveis pelo descumprimento de limites formais do ordenamento.

Não há prova sem contraditório, ainda que diferido e em menor extensão. A afirmação contraria a doutrina de Badaró nesse ponto; segundo esse autor, o rompimento da cadeia de custódia da prova digital reduziria o valor probatório, mas não levaria à sua inadmissão[306]. Nessa linha, se o contraditório diferido não puder impedir a admissão da prova produzida, por exemplo, mediante processamento de dados proibido por lei, de fato não há contraditório nessa prova, que, por essa razão, seria epistemologicamente fraca. A conclusão é errada porque a premissa também o é.

4.2.3. Elemento probatório antecipado

O conceito de prova antecipada foi ressalvado no artigo 155 do CPP como aquelas provas que não são produzidas sob contraditório pleno. Esse dispositivo reproduz a orientação predominante na doutrina à época de sua inclusão, com a minirreforma de 2008, que também alterou a redação do artigo 156 para permitir que o juízo ordene a produção de prova antecipada quando houver urgência e relevância, desde que observada a proporcionalidade da medida[307]. Assim, positivou-se como faculdade do juízo determinar, de ofício, a produção probatória na fase de investigação preliminar.

Não é difícil perceber o viés inquisitorial dessa faculdade processual atribuída ao

---

[305] BADARÓ, Gustavo Henrique Righi Ivahy. O valor probatório do inquérito policial. Polícia e investigação no Brasil. Tradução. Brasília, DF: Gazeta Jurídica, 2016. p. 276.

[306] Gustavo Badaró defende que se trata de uma questão valorativa, de modo que o juízo deve realizar a valoração da prova cuja cadeia de custódia tenha sido violada. Portanto, a prova é admitida e valorada em conjunto com os outros elementos de cognição, podendo o rompimento da cadeia de custódia reduzir sua força epistêmica. Em outra vertente, Aury Lopes Junior, Geraldo Prado e Janaina Matida defendem que a violação da cadeia de custódia está conectada ao momento de admissão. Se não é possível aferir a autenticidade, a inalterabilidade e a integralidade do elemento de informação, este deve receber o tratamento constitucional de prova ilícita.

[307] Art. 156 do CPP: "A prova da alegação incumbirá a quem a fizer, sendo, porém, facultado ao juiz de ofício: I – ordenar, mesmo antes de iniciada a ação penal, a produção antecipada de provas consideradas urgentes e relevantes, observando a necessidade, adequação e proporcionalidade da medida." BRASIL, 1941, art. 156.

magistrado. Em vez de apenas complementar as provas apresentadas pelas partes em contraditório, o juiz, com base no artigo 156, assume a iniciativa de produzi-las ainda antes da ação penal, desempenhando atividade probatória típica de investigação[308]. O sistema, ao não estabelecer limites adequados ao controle probatório judicial, revela sua permissividade, admitindo até mesmo a produção de provas, que deveria ser tratada de forma estritamente excepcional.

Além disso, a proporcionalidade constitui um limite imanente – verdadeiro "limite dos limites" – imposto pela Constituição Federal e aplicável a qualquer ato público, judicial, legislativo ou administrativo[309]. Desse modo, inseri-la na legislação infraconstitucional representa, no melhor dos cenários, apenas uma tentativa de conferir aparência de ponderação ao dispositivo, sem respaldo principiológico no sistema acusatório. Assim, a autorização para a produção antecipada de provas por iniciativa do juízo na fase pré-processual requer filtragem constitucional.

Os dispositivos que positivam hipóteses de produção antecipada de prova merecem análise crítica. O artigo 225 do CPP disciplina a situação da testemunha enferma ou idosa, permitindo que seja ouvida de forma antecipada sobre os fatos que conheça[310]. Já no caso do réu citado por edital[311], o artigo 366 autoriza o juízo a determinar a produção das provas urgentes. Em ambos os casos, repete-se o mesmo defeito apontado anteriormente: o juiz é colocado como ator central na delimitação da iniciativa probatória em razão da urgência e do risco de perecimento do elemento informativo.

Esses dispositivos, contudo, como dito, devem ter a interpretação filtrada constitucionalmente[312]. Sempre que houver necessidade de antecipar a produção probatória, o contraditório deve ser assegurado, desde que não comprometa a efetividade da diligência. Assim, ainda que a legislação processual penal seja omissa quanto à forma de instrumentalização da prova antecipada, deve-se interpretar que a testemunha enferma seja ouvida perante acusação e defesa; e, no caso do réu foragido, que a Defensoria Pública participe do ato, garantindo o contraditório

---

[308] LOPES JUNIOR, 2020, p. 62-64.
[309] MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. Curso de Direito Constitucional. 17ª ed. São Paulo: Saraiva Jur, 2022, p. 312.
[310] Art. 225 do CPP: "Se qualquer testemunha houver de ausentar-se, ou, por enfermidade ou por velhice, inspirar receio de que ao tempo da instrução criminal já não exista, o juiz poderá, de ofício ou a requerimento de qualquer das partes, tomar-lhe antecipadamente o depoimento" (BRASIL, 1941, art. 225).
[311] Art. 366 do CPP: "Se o acusado, citado por edital, não comparecer, nem constituir advogado, ficarão suspensos o processo e o curso do prazo prescricional, podendo o juiz determinar a produção antecipada das provas consideradas urgentes e, se for o caso, decretar prisão preventiva, nos termos do disposto no art. 312" (BRASIL, 1941*,* art. 366*).*
[312] LOPES JUNIOR, 2020, p. 285-286

judicial.

A efetividade da diligência se refere aos casos em que o desconhecimento da medida seja essencial para sua finalidade, tais como escutas telefônicas e infiltração de agentes, que, como dito, a doutrina majoritária define como prova cautelar, erroneamente. Nessas hipóteses, contraditório é necessariamente diferido, e é requisito para a admissão desse resultado na ação penal.

Neste ponto, chega-se à tradicional dicotomia entre a prática e direito posto como a causa do problema apontado. A introdução do artigo 156 remonta à racionalidade da sua época de inclusão, que teve a eficácia não questionada judicialmente, portanto, é vigente e aplicado corriqueiramente. Logo, seria razoável dizer que a prática inquisitorial decorre do direito posto, o qual deve ser alterado.

Pois bem, o legislador realizou a alteração no sentido doutrinário e principiologicamente apontado acima. Introduziu-se o artigo 3º-B, VII, no CPP[313], que outorgou a competência ao juiz das garantias para decidir sobre a produção de provas antecipadas urgentes e não repetíveis, com o dever de assegurar o contraditório e a ampla defesa em audiência pública e oral. Houve, portanto, um alinhamento com a axiologia do sistema acusatório, privilegiando-se o direito de defesa e a possibilidade de reagir imediatamente aos pedidos acusatórios.

O juiz das garantias foi inserido pelo pacote anticrime, promulgado em 24 de dezembro de 2019. A Associação dos Magistrados do Brasil ajuizou ação direta de inconstitucionalidade e obteve liminar que suspendeu a eficácia dos artigos 3º-A a 3ª-F[314], menos de um mês após o ajuizamento. Sobre o artigo 3º-B, a decisão de mérito do plenário, de 25 de agosto de 2023, concluiu que o dispositivo "deve ser interpretado à luz da Constituição, para estabelecer que o juiz pode deixar de realizar a audiência quando houver risco para o processo, ou diferi-la em caso de necessidade"[315].

A interpretação conforme dada não parece efetiva. O risco a ser evitado não é explicitado; presume-se que seja a proteção do elemento de informação sobre o qual a atividade probatória da

---

[313] Art. 3º-B: "O juiz das garantias é responsável pelo controle da legalidade da investigação criminal e pela salvaguarda dos direitos individuais cuja franquia tenha sido reservada à autorização prévia do Poder Judiciário, competindo-lhe especialmente: (...) VII - decidir sobre o requerimento de produção antecipada de provas consideradas urgentes e não repetíveis, assegurados o contraditório e a ampla defesa em audiência pública e oral" (BRASIL, 1941, art. 3º-B).

[314] Medida cautelar na Ação Direta de Inconstitucionalidade 6298/DF (BRASIL. Superior Tribunal de Justiça. Recurso Especial nº 1.962.275/GO, 2022.

[315] Trecho da ementa da ADI 6298/STF (BRASIL, REsp nº 1.962.275/GO, 2022.)

ação penal deve recair. A possibilidade de diferir a audiência em caso de necessidade sem a determinação dos critérios pode significar, no limite, a impossibilidade por carga de trabalho ou qualquer outro argumento consequencialista. Ademais, logicamente, o diferimento do ato se daria apenas após a produção da prova, quando eventual violação já teria ocorrido, restando somente a inadmissão ou a exclusão do elemento informativo.

O argumento vencedor foi consequencialista. Ninguém argumentaria que a existência dessa audiência é inconstitucional, mas o ato exigiria a presença dos magistrados, já que é ato indelegável, o que encontra resistência pela categoria. A conclusão é que, quando o legislador limita a prática legalmente, a autorização para descumpri-la é jurisprudencial. É um ciclo da cultura jurídica que despreza o processo penal, orientado racional e humanisticamente, para evitar erros e violações de direitos, que está evidente tanto no direito posto quanto na prática.

A prova digital exige mais aprofundamento nas categorias de provas urgentes – desconsiderando-se o conceito de cautelar –, na medida em que os limites ao processamento de dados em massa em investigações se aplicam, geralmente, na fase preliminar, em que se produz a prova, e não somente busca-a, como a doutrina costuma trabalhar confortavelmente. Como se viu, o ordenamento permite a centralidade do papel do juiz, e a hipótese de um contraditório imediato e público foi transformada em faculdade processual dos magistrados, tornando-a débil. Em conclusão, o melhor conteúdo que se pode atribuir àquilo que o Código denomina "prova antecipada" é compreendê-la como antecipada do ponto de vista do contraditório próprio da ação penal, o momento ótimo, como dito acima. Nesse sentido, sua justificativa repousa na emergência, caracterizada pela perda iminente da janela temporal adequada à produção da prova, ou na urgência, fundada na contemporaneidade da infração penal. De todo modo, o fato é que a previsão da prova antecipada se encontra expressamente positivada como um tipo específico.

Adiante, os atos de investigação começam a ser estudos em espécie e as bases definidas neste capítulo passam a se materializarem em limites efetivos para antecipação e produção probatória do elemento digital no processo penal.

5. ATOS DE INVESTIGAÇÃO DA PROVA DIGITAL

A tese sustenta que o sistema processual brasileiro não se adequou às exigências tecnológicas contemporâneas, de modo que as investigações e os atos processuais ainda se realizam, em grande parte, por analogia a situações analógicas. Por outro lado, observa-se o uso recorrente de categorias tradicionais, como os meios de obtenção de prova e as requisições, para viabilizar as investigações de provas digitais. O problema é que essa prática pode distorcer o enquadramento do debate, levando à aplicação de analogias simplificadoras e à falta de reconhecimento de um estado fático que demanda abstrações e prescrições jurídicas específicas.

Este capítulo descreve o uso atual de cada instrumento processual empregado na obtenção de elementos informativos digitais, com foco na aquisição da informação pelos investigadores e na avaliação da adequação de sua utilização pelo poder judiciário. Nos casos em que se conclui pela inadequação do instrumento, a tese propõe um modelo ideal para a situação específica, acompanhado da justificação teórica correspondente. Ademais, a análise tem por objetivo sistematizar as formas de ingresso dos elementos digitais na investigação preliminar, ainda que o caráter de universalidade imponha um desafio para esse objetivo.

Em linha com a conceituação utilizada por Prado, as fontes de prova digital estudadas adiante se dividem em estáticas – *offline* – e dinâmicas – *online*[316]. Respectivamente, o acesso à fonte estática depende da apreensão física do dispositivo eletrônico em que as fontes de prova estão armazenadas[317] ou da aquisição de bases de dados públicas e privadas; o acesso às provas dinâmicas depende de métodos ocultos de investigação[318], que incluem interceptações, infiltração digital, o uso de *malwares* e vigilância em tempo real.

Naturalmente, sendo as fontes distintas, devem ser aplicados meios processuais diferenciados para cada situação, os quais não se encontram previstos de forma adequada no ordenamento jurídico nacional. E, mesmo com integração completa da Convenção de Budapeste, essa lacuna não seria adequadamente suprimida, uma das razões para tanto reside na falta de compreensão plena do fenômeno digital, o que dificulta a formulação de modelos ideais para o

---

[316] PRADO, Geraldo. Esboço de Proposta sobre Dispositivo de Controle da Investigação Digital: O "Aspecto Dinâmico da Prova Digital". Revista do Sistema Único de Segurança Pública (Revista SUSP), Brasília, DF, v. 3, n. 1, p. 240-261, jul./dez. 2024, p. 106.

[317] No caso das fontes estáticas, a fonte da prova é o dado digital, cuja apreensão física do dispositivo é condição para o acesso.

[318] PRADO, 2024, p. 253.

regramento pelo direito processual penal e controle da aplicação prática.

5.1. Apreensão, busca pessoal e encontro de dispositivos eletrônicos

Os elementos informativos digitais estão presentes na investigação preliminar desde o primeiro momento em que se verifica a ocorrência de infrações penais. Como abordado anteriormente, já na fase de diligência ao local do crime, em um dos primeiros atos de investigação, é possível encontrar dispositivos eletrônicos potencialmente relevantes para a apuração. Diante disso, caso haja suspeita de que o dispositivo tenha funcionado como instrumento do crime, ele deve ser apreendido para posterior análise pericial, em razão do seu potencial probatório.

É importante mencionar que a apreensão de suporte eletrônico decorrente da busca pessoal na flagrância e aquela que resulta do encontro da coisa no local do crime configuram situações juridicamente idênticas no âmbito processual penal. Em ambas, há a apreensão de bens independentemente de decisão judicial, mas o posterior acesso e análise do conteúdo não são disciplinados especificamente no ordenamento jurídico. Dessa forma, a resposta normativa a ser dada a tais situações deve ser a mesma, razão pela qual foi trazida conjuntamente neste tópico.

A apreensão desses itens funciona bem para as coisas corpóreas, mas é problemática no contexto numérico. O primeiro obstáculo é de ordem prática: como saber se um computador constitui instrumento da infração penal sem tê-lo acessado? Esse conhecimento pressupõe o acesso ao dispositivo. O segundo problema é de ordem jurídica, dado que a apreensão é do suporte físico, que contém todos os tipos de dados e informações, se dá por analogia a regras gerais, uma vez que não há regras no ordenamento que discipline a invasão ao dispositivo eletrônico.

Esse é o primeiro desafio imposto pelo uso por analogia de dispositivos corpóreos para a realidade digital, que é bem explorado por Ramalho[319]:

> [...] Para uma correta compreensão da geral inadequação das normas processuais penais tradicionais à realidade digital, é necessário compreender as especificidades da prova digital. Com efeito, ao passo que certos tipos de prova são imediatamente compreendidos como sendo dotados de características individualizadoras que os autonomizam e que reivindicam especiais meios e/ou conhecimentos técnicos para a sua

[319] RAMALHO, David da Silva. Métodos Ocultos de Investigação Criminal em Ambiente Digital. 1. ed. Coimbra: Almedina, 2017. David da Silva Ramalho é mestre em Ciências Jurídico-Criminais pela Faculdade de Direito da Universidade de Lisboa e investigador no Centro de Investigação em Direito Penal e Ciências Criminais (CIPDCC), vinculado à Faculdade de Direito da Universidade de Lisboa.

> recolha, a prova digital tende a ser relegada para o domínio da analogia com meios de obtenção de provas de cariz não especialmente técnicos, como as buscas e apreensões.

A comparação é, todavia, descabida por ignorar o grau de lesividade a garantias fundamentais ao se comparar um *smartphone* a um objeto qualquer. Nesse sentido, Zilli afirma que "se por um lado os avanços tecnológicos propiciam novos meios de realização de práticas ilícitas, por outro é inegável a carga lesiva à intimidade que o acesso ilimitado ao conteúdo armazenado nesses aparelhos pode trazer"[320]. Logo, a apreensão de suportes eletrônicos deve ser pensada por regras procedimentais próprias na sistemática brasileira, não só em razão da intimidade, mas para observar diversas garantias constitucionais, tal como o devido processo.

A jurisprudência costuma apontar que a decisão que autoriza a busca, por consectário lógico, abrange a análise do material apreendido[321]. Tal entendimento é parcialmente coerente para investigações analógicas, especialmente quando o mandado de busca cumpre o requisito da especificidade. Entretanto, quando um computador ou um celular são apreendidos por estarem no local do crime ou em posse do preso em flagrante, inexiste decisão judicial prévia que tenha autorizado a apreensão. Nesses casos, o ponto de discussão é se o acesso ao dispositivo deve observar a reserva de jurisdição.

Na nossa visão, o *locus* do debate não reside na identificação de quais sigilos poderiam ser violados, tal como se perguntar se olhar os registros telefônicos constitui levantamento do sigilo, nos termos da Constituição. O acesso aos dados armazenados no suporte físico é uma intervenção informacional, que implica restrição ao direito fundamental à autodeterminação informacional. Portanto, há um dever de abstenção estatal em acessá-los, que só pode ser excepcionado com autorização legal que estabeleça o procedimento de controle, que pode ser uma autorização judicial.

---

[320] ZILLI, Marcos. A prisão em flagrante e o acesso de dados em dispositivos móveis: nem utopia, nem distopia: apenas a racionalidade. In: ABREU, Jacqueline de Souza; ANTONIALLI, Dennys (ed.). Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate. Vol. I. São Paulo: InternetLab, 2018. p. 86.

[321] A tese é sumarizada da seguinte forma: "Segundo o entendimento desta Corte Superior, o mandado de busca e apreensão dos bens autorizados judicialmente, já pressupõe a autorização da extração dos dados dos celulares apreendidos, e que foram objeto do mandado. Ademais, o mesmo entendimento aplica-se à violação de intimidade, tendo em vista que a quebra de sigilo telefônico foi previamente autorizada". (BRASIL. Superior Tribunal de Justiça. Agravo Regimental no Recurso em Habeas Corpus n. 167.634/PA. Relator: Min. Joel Ilan Paciornik. Quinta Turma. Julgado em 15 mai. 2023. Publicado no DJe em 18 mai. 2023. O precedente foi citado em diversos processos, a exemplo do HC 834.268/SC e do AgRg no RHC 181.846/RS.)

Sobre a restrição à autodeterminação informacional nessa hipótese, Gleizer afirma que[322]:

> [...] Um outro exemplo são os dados oriundos de telecomunicação já encerrada, como os e-mails salvos em um dispositivo informático. Nesse caso, o direito ao sigilo da telecomunicação também não é afetado pela captura desses dados. Porque, com o fim do processo de telecomunicação, esses dados estão sob domínio do indivíduo, que pode, por exemplo, eliminá-los. Por isso, esses documentos em nada diferem de outros documentos quaisquer. A captura desses dados afeta um outro direito fundamental, que protege também a personalidade do indivíduo: a autodeterminação.

A afirmação anterior está em linha com a Emenda Constitucional 115/2022, que elevou a proteção de dados a status de garantia fundamental. Entretanto, antes disso, houve intenso debate sobre a exigência da reserva de jurisdição para o acesso a dispositivos eletrônicos. De um lado, houve a defesa de que a Constituição elegeu quais informações estavam protegidas por reserva de jurisdição, aquelas que são identificadas como sigilosas e, por consequência, os demais dados não ostentavam a mesma garantia, o que permitiria o acesso automático pelas agências penais. Esse entendimento é securitário e coloca em risco o núcleo essencial da proteção de dados.

No sentido contrário, diversos trabalhos se dedicaram a fazer analogias das intervenções informacionais com sigilos previstos na Constituição. Nesse contexto, Silva Rodrigues e Dezem defenderam a ideia de domicílio digital; o primeiro escreveu sobre a espiritualização do domicílio[323], e o segundo apresentou a ideia da casa digital[324]. Buscava-se uma analogia com sigilos previstos constitucionalmente para que fosse defendida a reserva de jurisdição. Essa analogia não resolve um problema crucial: a inviolabilidade do domicílio é excepcionada pela flagrância.

Outra linha argumentativa muito desenvolvida defendia o sigilo de comunicação, uma vez que se assemelharia à interceptação telefônica. Sobre esse ponto, será apresentado especificamente no Tópico 4.6, que debate em detalhes os meios de obtenção de prova ocultos. Adianta-se, por oportuno, que não faz sentido utilizar a hipótese constitucional de interceptação telefônica, que exige decisão judicial prévia, para itens encontrados no local das infrações criminais ou

---

[322] GLEIZER, Orlandino. A dogmática dos métodos ocultos de investigação no processo penal. In: BRITO CRUZ, Francisco; SIMÃO, Bárbara (eds.). Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate. São Paulo. InternetLab, 2021, v. IV, p. 122.

[323] RODRIGUES, Benjamin Silva. Da prova penal: Tomo II – Bruscamente... A(s) Face(s) Oculta(s) Métodos Ocultos de Investigação Criminal. Editora Rei dos Livros, 2010.

[324] DEZEM, Guilherme Madeira. A Espiritualização do Domicílio: o novo conceito de domicílio e o Marco Civil da Internet. In: Marco Civil da Internet. Lei 12.965/2014. Coordenadores Fabiano Del Masso, Juliana Abrusio e Marco Aurélio Florêncio Filho. São Paulo: Editora Revista dos Tribunais, 2014.

apreendidos durante buscas pessoais. Isso porque a analogia protegeria, no limite, os dados comunicacionais registrados nos dispositivos apreendidos por serem sigilos, ao mesmo tempo em que manteria proteção deficiente aos dados protegidos, inclusive os sensíveis.

Após muitas idas e vindas da jurisprudência, em 24 de setembro de 2025, o STF publicou o acórdão do ARE 1042075[325], que foi julgado no regime de repercussão geral, e deu origem ao tema 977. Nesse julgado, o tribunal constitucional enunciou a tese que versa exatamente sobre as possibilidades de encontro de coisas e apreensão após busca pessoal na situação de flagrante. Em alguns pontos, a decisão está de acordo com a defesa de mérito realizada na tese, em outros, concluiu em sentido diverso; a tese enunciada pelo tribunal é a seguinte[326]:

> [...] 1. A mera apreensão do aparelho celular, nos termos do art. 6º do CPP ou em flagrante delito, não está sujeita à reserva de jurisdição. Contudo, o acesso aos dados nele contidos deve observar as seguintes condicionantes: 1.1 Nas hipóteses de encontro fortuito de aparelho celular, o acesso aos respectivos dados para o fim exclusivo de esclarecer a autoria do fato supostamente criminoso, ou de quem seja o seu proprietário, não depende de consentimento ou de prévia decisão judicial, desde que justificada posteriormente a adoção da medida. 1.2. Em se tratando de aparelho celular apreendido na forma do art. 6º do CPP ou por ocasião da prisão em flagrante, o acesso aos respectivos dados será condicionado ao consentimento expresso e livre do titular dos dados ou de prévia decisão judicial (cf. art. 7º, inciso III, e art. 10, § 2º, da Lei nº 12.965/2014) que justifique, com base em elementos concretos, a proporcionalidade da medida e delimite sua abrangência à luz de direitos fundamentais à intimidade, à privacidade, à proteção dos dados pessoais e à autodeterminação informacional, inclusive nos meios digitais (art. 5º, X e LXXIX, CRFB/88). Nesses casos, a celeridade se impõe, devendo a Autoridade Policial atuar com a maior rapidez e eficiência possíveis e o Poder Judiciário conferir tramitação e apreciação prioritárias aos pedidos dessa natureza, inclusive em regime de plantão. 2. A autoridade policial poderá adotar as providências necessárias para a preservação dos dados e metadados contidos no aparelho celular apreendido, antes da autorização judicial, justificando, posteriormente, as razões de referido acesso. 3. As teses acima enunciadas só produzirão efeitos prospectivos, ressalvados os pedidos eventualmente formulados por defesas até a data do encerramento do presente julgamento.

Segundo o STF, a apreensão de suportes eletrônicos não depende de autorização judicial, que é uma obviedade, na medida em que não se pode exigir decisão judicial prévia para apreensão de instrumentos ou objetos encontrados no contexto flagrância ou em atos de desenvolvimento. Na hipótese de encontro fortuito, o ponto 1.1 determinou que o acesso ao dispositivo pode ser realizado diretamente pelos órgãos de persecução com a finalidade de identificação de autores, coautores e

---

[325] BRASIL. Supremo Tribunal Federal, 2025, ARE 1042075.
[326] BRASIL. Supremo Tribunal Federal, 2025, Tema 977.

partícipes; no caso concreto, o telefone perdido durante a fuga foi enquadrado nessa categoria. Entretanto, o tribunal parece ter confundido a apreensão de instrumentos do crime na situação de flagrância com a figura do encontro fortuito de provas, que pressupõe a descoberta de elementos probatórios diversos daqueles inicialmente autorizados judicialmente. De forma ampla, a situação de flagrância afasta a necessidade de observância à reserva de jurisdição em função do caráter emergencial o risco ao bem jurídico tutelado. Por essa mesma razão, não é adequado qualificar o instrumento ou objeto apreendido como encontro fortuito, uma vez que não há desvio causal.

No ponto 1.2 do tema, o STF estabeleceu que, na apreensão decorrente de prisão em flagrante – isto é, nas situações de flagrância que efetivamente resultem em prisão –, é legítimo o acesso mediante consentimento do usuário, cuja comprovação é, na prática, extremamente difícil [327] . Ademais, o tribunal determinou que as decisões judiciais observem princípios constitucionais como privacidade, autodeterminação informacional e proporcionalidade, sem, contudo, atribuir conteúdo operacional concreto. Na sequência, o ponto 2 autoriza a superação de barreiras de segurança e a cópia de dados, aspecto relevante na medida em que funciona como permissivo legal para a aquisição e utilização de tecnologias de invasão.

Esse precedente tem características de lei – ampla, geral e abstrata –, e poderia facilmente tratar-se de um artigo do capítulo das provas digitais no Código de Processo Penal, que determina o destinatário da norma, a finalidade, a licitude do tratamento e a proporcionalidade. O problema, contudo, não está necessariamente no mérito do que foi decidido, mas na falha do sistema de precedentes, que acaba por criar hipóteses autorizadoras de investigação criminal. Esse fazer jurisprudência mina a lógica sistêmica do direito processual penal, que retira da legalidade estrita, a legitimidade e a previsibilidade para a ação dos órgãos de persecução penal[328].

A tese de repercussão geral menciona que o acesso ao conteúdo atinge os direitos constitucionais à intimidade, à privacidade e à proteção de dados. Logo, a regra é a abstenção em relação a eles, caso não haja autorização legal – enunciado de súmula e tese de repercussão geral

---

[327] É necessário um destaque de ordem criminológica. A discussão sobre o que pode ser analisado em um dispositivo eletrônico durante a apreensão apresenta riscos. Esse debate pode, indiretamente, legitimar práticas de violência policial, na medida em que se afirma que o acesso ao conteúdo seria possível por meio de consentimento do preso em flagrante. Tal construção, além de fragilizar garantias fundamentais, não tem verossimilhança empírica. Não por acaso, o STJ passou adotar posição rigorosa com essa argumentação no contexto das buscas domiciliares, supostamente por convite do morador após prisão em flagrante por crime diverso. A exemplo do afirmado, tem-se o *Habeas Corpus* n. 762932 e do *Habeas Corpus n.* 598.051/SP, ambos do Superior Tribunal de Justiça. No último, se afirma expressamente que o ônus de provar o convite é estatal.

[328] GLOECKNER; EILBERG, 2019, p. 19.

não preenchem esse requisito, evidentemente. Nesse sentido, a constatação é que não há previsão legal para acessar dispositivos eletrônicos após a apreensão, o que também demonstra uma inércia injustificável do legislador. Portanto, os dispositivos eletrônicos, como regra, devem ser acessados por meio de decisão judicial porque o conteúdo informacional é protegido constitucionalmente.

Assim, constata-se que um modelo ideal de disciplina das provas digitais deve conter a diferenciação entre a apreensão do dispositivo eletrônico e o acesso aos dados nele constantes. Na hipótese de encontro no local do crime e nas buscas pessoais, ainda que o item seja apreendido, a análise, como regra, deve depender de autorização. É possível também discutir quais hipóteses autorizam o acesso imediato, tal como feito no ponto 1.2 da tese firmada, quando a urgência exigir comportamento célere, como em casos de crimes em curso, para proteção de bens jurídicos de alta estatura legal, devendo-se, por paralelismo, a consequente forma de controle do ato.

A situação de mora legislativa é tão grave que a tese do STF preencheu ilegitimamente a ausência de norma que discipline a invasão do dispositivo para possibilitar a produção probatória: o rompimento de senhas e as barreiras de segurança. A referida lacuna é a matéria que deve ser regrada por um modelo que contemple a apreensão do suporte, definindo o meio jurídico aceitável para romper barreiras de segurança, a cadeia de custódia e a licitude do uso dos dados, cuja métrica é dada pela decisão judicial autorizada a partir da hipótese investigativa, a serem verificados como critério de admissibilidade do elemento na ação penal[329].

É claro, no entanto, que a ausência de lei não impediu que as polícias judiciárias analisassem o material apreendido. Isso é evidenciado na jurisprudência que já exigia autorização para análise antes do tema 977[330]. Além de decisões judiciais nesse sentido, a tese identificou resultados de pesquisa que comprovam compras públicas de tecnologias de invasão realizadas por órgãos públicos anteriores ao precedente. A Transparência Brasil identificou que as Secretarias de Justiça da Bahia, São Paulo, Paraná e Rio de Janeiro firmaram contratos com a empresa TechBiz – representante da Cellebrite no Brasil – para a aquisição de aplicativos de invasão de celulares [331].

Ainda que não tenha lei autorizadora, as agências penais brasileiras compram e utilizam tecnologia de invasão de dispositivos. Esse ponto é sensível e deveria também ser previsto em uma disciplina própria das provas digitais, na medida em que o acesso é obtido por meio de tecnologias

---

[329] Por exigência do artigo 158-A e seguintes do Código de Processo Penal.
[330] BRASIL. Superior Tribunal de Justiça, 2016, HC 51.531.
[331] BERTI, Bianca. Ausência de proteção de dados na contratação de tecnologias de vigilância para segurança pública. Transparência Brasil, 2024, p. 5.

que exploram fragilidades de sistemas informacionais. Tais métodos podem inviabilizar a verificação dos critérios legais de validade da prova. Por isso, o uso de ferramentas como *spywares* deve ser proibido, já que, além de comprometerem a integridade do processo probatório, tornam-se inúteis para a finalidade pública que justificou sua aquisição. Ademais, a invasão de dispositivo informático é crime[332], de modo que, se não houver autorização legal para essa ação, sob a perspectiva da dogmática penal, a conduta policial é típica e antijurídica.

Evidentemente, o argumento é pelo absurdo, já que a licitude da prática pode ser depreendida implicitamente da jurisprudência do STF e de outros tribunais nacionais. O objetivo é demonstrar que o legislador brasileiro não se atém detidamente a esses fatos e chega ao ponto de colocar os agentes de investigação em risco penal. É claro que a utilização de tecnologia, comprada publicamente, para o exercício de função legal jamais seria considerada antijurídica. Entretanto, a necessidade de formular esse argumento é a prova de que não só a apreensão, mas também o acesso deve ser autorizado legalmente para lidar com as características próprias das provas digitais.

Por fim, as prescrições feitas neste tópico servem para os suportes eletrônicos encontrados no local do crime e para as buscas pessoais permitidas pela legislação processual penal. Nesse sentido, a conclusão mais relevante é que a apreensão não permite automaticamente o acesso e a análise dos dados digitais. Ademais, o modelo ideal de disciplina também deve considerar quais são os meios legítimos para realizar a invasão do dispositivo eletrônico, excluindo-se os que violem a integridade dos sistemas computacionais. Posteriormente, os limites ao uso, por exigência da finalidade no dispositivo processual, são abordados no Capítulo 7, onde se define o conteúdo do pedido e da decisão judicial autorizadora com base na hipótese da tese.

5.1.1. Entrega voluntária da prova digital estática.

O Código de Processo Penal disciplina, em seu artigo 6º, IV e V, que a autoridade policial deve proceder à oitiva da vítima da infração penal e do indiciado[333]. Neste ponto da tese, o objetivo não é discutir as garantias aplicadas às pessoas que serão ouvidas, sejam possíveis vítimas,

---

[332] BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Diário Oficial da União, Rio de Janeiro, 31 dez. 1940. Art. 154-A.

[333] Art. 6º do CPP: Logo que tiver conhecimento da prática da infração penal, a autoridade policial deverá: (...) IV - ouvir o ofendido; V - ouvir o indiciado, com observância, no que for aplicável, do disposto no Capítulo III do Título Vll, deste Livro, devendo o respectivo termo ser assinado por duas testemunhas que lhe tenham ouvido a leitura; (BRASIL, 1941, Art. 6º)

suspeitos, testemunhas, pois naturalmente todas podem trazer elementos informativos digitais aos autos da investigação. Assim, ao se tratar da entrega de suportes eletrônicos por vítimas e testemunhas, fala-se em entrega voluntária[334], e o objeto entregue deve ser apreendido com a respectiva oficialização.

A entrega voluntária se diferencia das buscas pessoais, na medida em que a ideia de consentimento é verossímil, isto porque não há um prejuízo direto aos direitos do quem está consentindo, especificamente do suspeito ou investigado. Por outro lado, aquele que foi vítima de infração penal pode ter o interesse em retirar barreiras de segurança e permitir o acesso às agências policiais, inclusive indicando a fonte pertinente. É dessa forma, por exemplo, que as câmeras privadas de segurança e mensagens de aplicativos ingressam espontaneamente na investigação preliminar sem a necessidade de observância de decisões judiciais.

Uma hipótese pouco explorada de entrega voluntária de dados ocorre na notícia-crime realizada por provedores de armazenamento em nuvem. Estas empresas utilizam tecnologias de escaneamento automatizado para coibir o armazenamento de conteúdo ilícito, notadamente o Material de Abuso Sexual Infantil (CSAM). A política de uso do Google, por exemplo, prevê a desativação da conta e a notificação às autoridades; entre janeiro e junho de 2025, a empresa reportou a detecção de 3.124.107 conteúdos desse gênero[335]. Nesses casos, a plataforma atua de forma proativa, encaminhando às agências de persecução penal dados previamente selecionados.

Já o suspeito tem a faculdade de apresentar elementos informativos digitais que julgue pertinentes na investigação preliminar, vale ressaltar que o CPP utilizar a expressão “indiciado”, mas como se trata dos primeiros atos de investigação, é mais adequado o uso da categoria “suspeição”. Nessa hipótese, com a prova do consentimento válido – que engloba a entrega e o meio de acesso –, os elementos ingressam no inquérito policial sem a necessidade de controle judicial. Vale ressaltar que a hipótese é menos frequente que a juntada pelas vítimas, mas é possível.

Cabe aos órgãos de persecução a análise da pertinência daquilo que se pretende entregar, uma vez que os suportes eletrônicos devem ter relação com o fato em investigação, em outras palavras, devem ter utilidade para a comprovação da hipótese investigativa. Naturalmente, a não

---

[334] BADARÓ, 2013, p. 149.
[335] Disponível em https://transparencyreport.google.com/child-sexual-abuse-material/reporting?hl=pt_BR, acessado em 17/03/2026.

observância da pertinência e da utilidade é causa de apreensão abusiva e extravagante[336], cuja consequência é o desentranhamento por ilicitude.

Além da análise da pertinência, a averiguação da autenticidade, integralidade e confiabilidade desses elementos informativos também é dever das autoridades de investigação, para evitar o ingresso informações adulteradas na investigação preliminar, a exemplo de uma fotografia editada, o registro de uma conversa que tenha sido manipulado, dentre outras. Para tanto, o conceito de cadeia de custódia é o dispositivo de controle mais bem definido para lidar com essas situações, que vem sendo utilizado pelo STJ para impedir que informações inverificáveis sejam utilizadas como fonte de prova, a exemplo de *prints* de *Whatsapp*[337].

Finalmente, a descrição minuciosa de todas as formas de ingresso de elementos digitais na investigação preliminar é impraticável, tendo em vista que os envolvidos nos fatos apurados podem entregá-los voluntariamente ou por interesse defensivo, até porque a prova digital está universalmente dispersa no dia a dia[338]. Ainda assim, o principal ganho da descrição reside na identificação de padrões: nas buscas pessoais e nas entregas realizadas por vítimas, predomina a apreensão de suportes eletrônicos; já nas hipóteses decorrentes de escaneamento por provedores de serviços em nuvem, prevalece a apreensão de dados.

5.2. Requisição de dados, ordem de exibição, injunção, coleta?

A inexistência de um marco normativo para as provas digitais, por vezes, dificulta a própria comunicação técnica pela ausência de conceitos aptos a descrever situações jurídicas de elevada importância, como é o caso da abordagem dos dados pessoais no ambiente processual penal. Essa imprecisão verifica-se na maneira de definir o ingresso das informações digitais no processo penal, para a qual utilizam-se indistintamente vários termos: requisição, ordem, acesso, injunção e coleta. Deles, o mais usado no ordenamento brasileiro é "requisição", que é a nomenclatura do Marco

---

[336] REBELLATO, Luiz Fernando Bugiga. A análise constitucional do sigilo e da privacidade nas investigações criminais: o acesso a dados armazenados em aparelhos celulares. 2021. Dissertação (Mestrado) – Universidade de São Paulo, São Paulo, 2021, p. 151.
[337] BRASIL, Superior Tribunal de Justiça, 2024, HC 828.054.
[338] DANIELE, 2011, p. 284.

Civil da Internet[339].

O problema é que o conceito de "requisição" remete àquelas de natureza administrativa, as quais poderiam ser realizadas sem observância à reserva de jurisdição, por não estarem protegidas por sigilos[340], e que costumam ser positivadas em leis que regem as profissões[341]. Não é esse o caso e, como se verá adiante, o Código de Processo Penal institui requisições que dependem de autorização judicial para o acesso a dados. Ademais, nos primeiros capítulos da tese, foi exposto que é mais adequada a descrição da coleta como ato realizado por particulares e pelo poder público, com prévio estabelecimento de uma arquitetura informacional.

Logo, coleta de dados é um ato independente da investigação criminal, até porque ocorre, cotidianamente, antes da existência de suspeição por infrações penais e à despeito dela; em outras palavras, o objetivo é a sua existência fora do processo penal. As agências estatais pretendem acessar e utilizar as informações previamente produzidas para outros contextos na investigação preliminar, o que se adequa ao conceito de fontes de provas que devem ser buscadas pelos meios de obtenção de provas. Diante disso, parece mais adequada a utilização do termo "coleta" para situações alheias ao processo penal, mantendo a coerência com o que foi defendido anteriormente.

Sobre a utilização de "acesso", concorda-se com Cordeiro, uma vez que seu uso "traria um significado equivocado de entrada. Poder-se-ia passar a impressão de que o Estado teria liberação para acessar todos os dados contidos em determinada base, tornando-se ele também controlador dos dados, o que não condiz com o meio de investigação"[342]. A expressão é coloquial e poderia ser interpretada no sentido de que o acesso não é vinculado, o que não é adequado para os meios de busca, que, teleologicamente, devem se orientar pela hipótese de autorização judicial. Por essas razões, deve-se evitar a utilização dessa expressão dogmaticamente.

---

[339] A lei n. 12.965/2014 dedica a Seção IV ao assunto, que é denominada "Da requisição Judicial de Registros". Em outra oportunidade, a legislação excepciona a proteção de registros cadastrais à proteção, pelas autoridades que tenham competência legal para requisitá-las. (BRASIL, 2014).

[340] CORDEIRO, Pedro Ivo Rodrigues Velloso. O Direito Fundamental à Proteção de Dados Pessoais e a Obtenção de Dados de Provedores de Conexão e de Provedores de Aplicações de Internet no Âmbito Processual Penal. 2024. 320 f. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2024, p. 178.

[341] Cita-se para exemplificar o argumento, o art. 26, II, da Lei n. 8.625/1993 (Lei Orgânica Nacional do Ministério Público), que prevê a possibilidade de requisitar informações a empresas para instrução de processos, ou a requisição de perícia pelo delegado ao perito responsável, previsto na Lei n. 12.850/2013. (BRASIL. Lei nº 8.625, de 12 de fevereiro de 1993. Institui a Lei Orgânica Nacional do Ministério Público, dispõe sobre normas gerais para a organização do Ministério Público dos Estados e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, 15 fev. 1993. p. 1997.) (BRASIL. Lei nº 12.850, de 2 de agosto de 2013. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal [...]. Diário Oficial da União: seção 1, Brasília, DF, 5 ago. 2013. p. 3).

[342] CORDEIRO, 2024, p. 178.

O interesse para a processualística penal é determinar em que situações é legítimo que as agências de persecução obriguem a entrega de dados coletados e os utilizem com função probatória. Nesse sentido, a Convenção de Budapeste do Conselho da Europa propõe o uso de ordem de exibição[343], que remete ao termo *production order* do inglês e é uma nomenclatura mais ampla, a qual permite que os diversos ordenamentos jurídicos compreendidos adequem suas legislações, e expressa a ideia central: o Estado obriga o particular a entregar informações de que tem custódia. O Regulamento n. 2023/1543 da União Europeia replica a Convenção de Budapeste[344].

No direito comparado, observa-se que, em consonância com os compromissos assumidos pela referida convenção internacional, Portugal adota a figura da injunção para a apresentação ou concessão de dados. Ao nosso ver, é uma solução tecnicamente adequada, por consistir em decisão emanada de autoridade judiciária[345] destinada a permitir o acesso a dados sob a custódia de terceiros. Importa destacar que o conteúdo jurídico da "injunção" é suficientemente claro e abrangente para enfrentar o problema a que se propõe: exige decisão judicial, especificação do dado cujo acesso se pretende, indicação do destinatário – aquele custodia a informação – e definição das consequências da resistência. O caput do dispositivo tem a seguinte redação[346]:

> [...] Se no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados que os comunique ao processo ou que permita o acesso aos mesmos, sob pena de punição por desobediência.

A primeira constatação que deve ser feita de cunho normativo é a de que não há norma com

---

[343] BRASIL. Decreto nº 11.491, de 12 de abril de 2023. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. Diário Oficial da União: seção 1, Brasília, DF, 13 abr. 2023. Título III, art. 18.

[344] O regulamento cria dois tipos de ordem a serem enviadas aos provedores de serviço: *European Production Orders* e *European Preservation Orders*. (UNIÃO EUROPEIA. Regulamento (UE) 2023/1543 do Parlamento Europeu e do Conselho, de 12 de julho de 2023. Relativo às ordens europeias de produção e às ordens europeias de conservação para efeitos de prova eletrônica em processos penais e para efeitos de execução de penas privativas de liberdade na sequência de processos penais. Jornal Oficial da União Europeia, L 191, p. 118-180, 28 jul. 2023.)

[345] Em Portugal, o conceito de autoridades judiciárias compreende tanto os magistrados judiciais quanto os membros do Ministério Público, razão pela qual essa faculdade deve ser analisada à luz do sistema judicial português, não se confundindo com a noção estrita de autoridade judicial adotada no Brasil.

[346] PORTUGAL. Lei nº 109/2009, de 15 de setembro de 2009. Aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa. Diário da República, Lisboa, Série I, n.º 179/2009, 15 set. 2009. Art. 14º.

o conteúdo referido acima no ordenamento brasileiro. Por essa razão, o acesso a dados ocorre pela interpretação sistemática de diversas leis, com objetos e limites materiais diversos, às quais, em razão de leis especiais, convencionou-se chamar de requisições. O próprio Código de Processo Penal aderiu recentemente a essa nomenclatura, exigindo, no entanto, decisão judicial para dados de tráfego para localização de pessoas, logo, uma requisição sujeita à reserva de jurisdição[347].

A profusão de normas que variam quanto aos tipos de dados, aos destinatários da norma e aos limites penais é tão relevante que o texto produziu tabelas analíticas para facilitar a compreensão do que se tem positivado no ordenamento. Com efeito, Dezan descreveu essa multiplicidade de normas como um microssistema de legislação penal extravagante[348], que engloba a lei de lavagem, a lei das organizações criminosas, o Marco Civil da Internet e as alterações no CPP, que legitimam o poder de requisição. Contudo, a profusão dessas normas se assemelha mais ao conceito de rizoma[349] do que a um sistema: são heterogêneos, múltiplos não lineares.

Por fim, os tópicos a seguir visam a sistematizar as previsões legais brasileiras sobre requisição de dados, expondo a ausência de previsão legal para o acesso a dados de conteúdo.

5.2.2. Requisição de dados cadastrais de vítimas e suspeitos

O poder de requisição é uma prerrogativa legalmente atribuída a determinados órgãos para medidas administrativas autoexecutórias, que imprescindem pedido ou decisão judicial prévios. No caso da persecução criminal, o poder de requisição preenche o conteúdo normativo dos poderes de investigação das polícias judiciárias, que têm respaldo constitucional e legal, visto amplamente no Código de Processo Penal e em legislações especiais, a exemplo da Lei n. 12.830/2013[350]. Esse entendimento se aplica às investigações do Ministério Público[351].

---

[347] Art. 13-A e 13-B do Código de Processo Penal.

[348] DEZAN, Sandro Lúcio. Documentos e requisição direta de dados e informações pelo delegado de polícia. In: PEREIRA, Eliomar da Silva; ANSELMO, Márcio Adriano (org.). Direito Processual da Polícia Judiciária II: os meios de obtenção de prova. Belo Horizonte: Fórum, 2020, p. 113-131, p. 129.

[349] DELEUZE, 1992. p. 215-216.

[350] Art. 2, § 2º: Durante a investigação criminal, cabe ao delegado de polícia a requisição de perícia, informações, documentos e dados que interessem à apuração dos fatos. (BRASIL. Lei nº 12.830, de 20 de junho de 2013. Dispõe sobre a investigação criminal conduzida pelo delegado de polícia. Diário Oficial da União: seção 1, Brasília, DF, 21 jun. 2013. Art. 2º, § 2º.)

[351] O STF declarou a constitucionalidade dos poderes de investigação autônomos do órgão no RE 593.727, de modo que todas as legislações que conferiam prerrogativa ao órgão para atos de investigação são juridicamente válidas, o

Comparando-se com os institutos visualizados anteriormente, esse é o primeiro que se destina a acessar dados digitais, e não os suportes eletrônicos onde eles possam ser encontrados após análise. Ademais, a utilização da expressão "dados cadastrais" releva a finalidade de acesso e que as informações deverão estar em linguagem estruturada; na perspectiva da LGPD, esses dados são entendidos como dados pessoais[352], cuja utilização permite identificar o usuário, ato de investigação imprescindível para a atribuição de autoria, coautoria e participação.

A primeira inserção legislativa da requisição de dados cadastrais como ato de investigação foi na Lei de Lavagem de Dinheiro, em alteração legislativa ocorrida em 2012, que prevê que[353]:

> [...] A autoridade policial e o Ministério Público terão acesso, exclusivamente, aos dados cadastrais do investigado que informam qualificação pessoal, filiação e endereço, independentemente de autorização judicial, mantidos pela Justiça Eleitoral, pelas empresas telefônicas, pelas instituições financeiras, pelos provedores de internet e pelas administradoras de cartão de crédito.

Esse artigo é replicado no artigo 15 da Lei n. 12.850/2013 (Lei das Organizações Criminosas), que foi promulgada no ano seguinte à mencionada primeira inserção. Diante disso, a aplicação da requisição é restrita aos crimes previstos nos diplomas mencionados.[354] Portanto, na investigação dos referidos crimes, independentemente de autorização judicial, os órgãos de persecução poderão requisitar dados cadastrais às empresas do setor de telefonia, a instituições financeiras, a provedores de internet, às administradoras de cartão de crédito e à Justiça Eleitoral.

Há também hipótese de requisição de dados cadastrais no Marco Civil da Internet, prevista

---

que inclui as requisições que serão descritas. O tese de repercussão geral n. 184 do STF afirma: "O Ministério Público dispõe de competência para promover, por autoridade própria, e por prazo razoável, investigações de natureza penal, desde que respeitados os direitos e garantias que assistem a qualquer indiciado ou a qualquer pessoa sob investigação do Estado, observadas, sempre, por seus agentes, as hipóteses de reserva constitucional de jurisdição e, também, as prerrogativas profissionais de que se acham investidos, em nosso País, os Advogados (Lei 8.906/1994, art. 7º, notadamente os incisos I, II, III, XI, XIII, XIV e XIX), sem prejuízo da possibilidade – sempre presente no Estado democrático de Direito – do permanente controle jurisdicional dos atos, necessariamente documentados (Súmula Vinculante 14), praticados pelos membros dessa Instituição". (BRASIL. Supremo Tribunal Federal (Plenário). Recurso Extraordinário 593.727/MG. Relator: Ministro Cezar Peluso. Redator do acórdão: Ministro Gilmar Mendes. Julgamento em 14 mai. 2015. Publicação em 8 set. 2015. Diário da Justiça Eletrônico, 08 set. 2015. Repercussão Geral – Tema 184.)

[352] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Art. 5º, I.

[353] BRASIL, 1998, art. 17-B.

[354] Os dispositivos possuem limite penal definido para a produção de prova, sendo aplicável somente para infrações penais no contexto de organizações criminosas, às infrações penais previstas em tratados e convenções internacionais, com elemento internacional nas condutas ou resultados, e às organizações terroristas, de acordo com o art. 1º, § 2º, I, II, da lei 12.850/2013. (BRASIL, 2013)

no artigo 10, § 3º, da Lei n. 12.965/2014, "O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição". O parágrafo excepciona o dever de proteção aos dados pessoais e às comunicações privadas dos usuários de serviços de internet. Entretanto, o dispositivo não cria hipóteses, somente mantém as já existentes.

Em 2016, uma requisição semelhante foi inserida no Código de Processo Penal, dando origem ao artigo 13-A, que autorizou, para um rol de crimes gravíssimos (tráfico de pessoas, redução análoga à escravidão, sequestro e cárcere privado, extorsão com restrição de liberdade, extorsão mediante sequestro e tráfico internacional de crianças) [355], que órgãos de persecução requisitem, a quaisquer órgãos e empresas, dados e informações cadastrais de vítimas ou suspeitos. Portanto, a lógica do artigo é permitir a identificação célere dos suspeitos e a rápida ação dissuasiva.

O prazo de cumprimento da requisição é de 24 horas. Ela deve conter: i) o nome da autoridade requisitante; ii) o número do inquérito policial iii) a identificação da unidade de polícia judiciária responsável pela investigação. Dentre os critérios, o que tem potencial para gerar debate é a necessidade de instauração de inquérito – que também compreende o procedimento de investigação criminal do Ministério Público –, mas que deve excluir instrumentos anteriores, a exemplo do VPI (Verificação Preliminar de Informação) ou qualquer outro menos formal.

Diante disso, a conclusão é que, no atual cenário legal, a requisição de dados cadastrais só pode ocorrer no contexto da legislação de repressão à lavagem de dinheiro, às organizações criminosas e ao rol previsto no artigo 13-A. Ademais, a respeito dos destinatários, os setores são especificados nas leis especiais abordadas e indeterminados para o uso do CPP. Com o intuito de facilitar a compreensão, os dispositivos são apresentados compilados na Tabela 3:

Tabela 4 - Consolidação das hipóteses de requisição de dados cadastrais

Dispositivo legal	**Ano**	**Tipo de dado**	**Legitimados**	**Reserva de jurisdição**	**Destinatário**

[355] Art. 13-A do CPP: Nos crimes previstos nos arts. 148, 149 e 149-A, no § 3º do art. 158 e no art. 159 do Decreto-Lei no 2.848, de 7 de dezembro de 1940 (Código Penal), e no art. 239 da Lei no 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), o membro do Ministério Público ou o delegado de polícia poderá requisitar, de quaisquer órgãos do poder público ou de empresas da iniciativa privada, dados e informações cadastrais da vítima ou de suspeitos. Parágrafo único. A requisição, que será atendida no prazo de 24 (vinte e quatro) horas, conterá: I - o nome da autoridade requisitante; II - o número do inquérito policial; e III - a identificação da unidade de polícia judiciária responsável pela investigação. (BRASIL, 1941, art. 13-A)

Lei de Lavagem de Dinheiro (Lei n. 9.613/98, Art. 17-B Alteração Legislativa)	2012	Dados cadastrais: qualificação pessoal, filiação e endereço	Autoridade policial e Ministério Público	Não	Justiça Eleitoral, empresas telefônicas, instituições financeiras, provedores de internet e administradoras de cartão de crédito
Lei das Organizações Criminosas (Lei n. 12.850/2013, Art. 15)	2013	Dados cadastrais: qualificação pessoal, filiação e endereço	Autoridades administrativas que detenham competência legal	Não	Justiça Eleitoral, empresas telefônicas, instituições financeiras, provedores de internet e administradoras de cartão de crédito
Marco Civil da Internet (Lei n. 12.965/2014, Art. 10, § 3º)	2014	Dados cadastrais: qualificação pessoal, filiação e endereço	Autoridades administrativas que detenham competência legal	Não	Provedores de conexão e de aplicação de internet
Código de Processo Penal (Art. 13-A)	2016	Dados e informações cadastrais	Autoridade policial e Ministério Público	Não	Quaisquer órgãos ou empresas privadas

Fonte: elaborada pelo autor

O poder de requisição de dados digitais é uma prerrogativa investigativa proporcional às

necessidades da vida conectada, e, por isso, a tendência é o aumento da importância de sua utilização nas investigações cotidianas. Como visto, o ordenamento jurídico brasileiro contém normas esparsas que permitem o acesso, por requisição administrativa ou judicial, a dados digitais como atos de investigação criminal, que escalonam o grau de proteção conforme o tipo de dado que seja necessário acessar, isto é, quanto mais intrusivo, haverá mais requisitos a serem cumpridos. O que, como se verá adiante, essa proteção estática pode não ser suficiente para garantia de observância da finalidade de tratamento pelas agências de investigação.

Por fim, não é adequado que a matéria seja tratada em legislações especiais somente para determinados tipos de crimes. Nesse sentido, a universalidade da prova digital exige uma disciplina unificada, que poderia contar com a possibilidade de requisição de dados cadastrais como regra geral no Código de Processo Penal, para empresas que tenham porte para atender a esse tipo de pedido. Adicionalmente, essa regra poderia ser limitada por um critério de subsidiariedade, ou seja, sendo aplicável apenas quando os registros públicos não permitirem o acesso a essa informação.

5.2.3. Requisição judicial de dados de metadados para geolocalização

O poder de requisição de dados digitais para localização de suspeitos e vítimas é um ato de investigação típico da fase de investigação preliminar. A Lei 13.344/2016 inseriu o artigo 13-B no Código de Processo Penal[356], permitindo a requisição de metadados de localização (telefônico ou telemático) para identificação de vítimas e suspeitos dos delitos em curso. Quanto à nomenclatura dos dados, o texto usa a expressão "meios técnicos adequados – como sinais, informações e outros", que não é imprecisa da a perspectiva técnica computacional.

A redação do artigo apresenta um limite de âmbito de aplicação claro: a requisição visa à repressão ao tráfico de pessoas. Ademais, o critério de o crime estar "em curso" caracteriza a medida como um ato eminentemente de investigação, de modo que o objetivo-fim da localização é fazer cessar a lesão ao bem jurídico protegido, no caso, a dignidade da pessoa humana. Em suma, nos casos em que houver investigação por esse tipo de delito em curso, os órgãos de persecução

[356] Art. 13-B: Se necessário à prevenção e à repressão dos crimes relacionados ao tráfico de pessoas, o membro do Ministério Público ou o delegado de polícia poderão requisitar, mediante autorização judicial, às empresas prestadoras de serviço de telecomunicações e/ou telemática que disponibilizem imediatamente os meios técnicos adequados – como sinais, informações e outros – que permitam a localização da vítima ou dos suspeitos do delito em curso. (BRASIL, 1941, art. 13-B)

poderão requisitar às empresas prestadoras de telecomunicação e/ou telemática os metadados de localização.

O legislador também exigiu a autorização judicial para a requisição, o que é interessante, na medida em que rompe com a ideia tradicional de que somente a entrega de dados de conteúdo é potencialmente digna de proteção pela reserva de jurisdição. Entretanto, o § 2º do referido artigo permite que, em os casos urgentes, quando o prazo de 12 horas não for atendido pelo Judiciário, a requisição deve ser enviada diretamente às empresas referidas acima. Por essa razão, a requisição para geolocalização é híbrida, uma vez que a decisão judicial é imprescindível, com exceção dos contextos de urgência.

Além disso, é vedado o acesso aos dados de conteúdo, registro da ação ou pensamento humano, que atraem a aplicação de decisão fundamentada na Lei de Interceptação Telefônica. Evidentemente, o objetivo da medida não é ter acesso ao que os suspeitos ou vítimas conversam, e sim a possibilidade de geolocalizá-los para fins de investigação criminal. Em outras palavras, o uso do metadado da comunicação é suficiente para o objetivo de tratamento estabelecido pela legislação processual. Ademais, o prazo máximo da medida é de 30 dias, renováveis por igual período, mediante decisão judicial[357].

Após superar as hipóteses de aplicação e os limites, esse artigo deve ser lido de forma positiva no contexto das provas digitais, uma vez que ele se constitui de maneira única. Isso porque o objeto do tratamento e a finalidade estão claramente expostos, como se percebe na expressão "a localização da vítima ou dos suspeitos" com o uso de metadados que permitam a geolocalização. Trata-se de um raro dispositivo que estabelece o que deve ser feito com os elementos informativos digitais após serem coletados por empresas privadas e entregues a agências de investigação.

O dispositivo expressa claramente o tipo de processamento lícito de acordo com a legislação processual penal, que é um requisito que deveria ser exigido por uma metalei que almeje disciplinar o processamento de dados para fins de persecução penal. Portanto, o artigo 13-B é uma exceção no ordenamento brasileiro de definição da licitude do uso após a aquisição por agência de persecução. Logo, a consequência indireta é a de que qualquer uso fora da hipótese autorizada é ilícito e deve ser descartado da investigação preliminar e/ou inadmitido na ação penal respectiva.

De modo mais amplo, a disciplina das provas digitais deve observar um modelo ideal que

---

[357] BRASIL. Código de Processo Penal, 2016, art. 13-B, § 2º, II.

esse artigo respeita: setor de coleta + hipótese de acesso pelos órgãos de persecução + uso lícito permitido ao investigador = elemento informativo válido. No caso do artigo da requisição para geolocalização, tem-se: empresa de telefonia e comunicação + acesso a metadados telemáticos e telefônicos + uso para localizar suspeito ou vítima = rastreamento individualizado.

A última parcela da soma é o que diferencia o modelo em relação às provas analógicas, já que o potencial epistêmico destas é circunscrito naturalmente. Por outro lado, os dados digitais têm um potencial epistêmico ilimitado – com infinita capacidade de correlação. Contudo, ausência de limite e processo penal se excluem mutuamente, de modo que o tratamento é limitado pela hipótese investigativa, ainda que o entorno de dados permita correlações outras.

A última parcela da soma é o que distingue o modelo em relação às provas analógicas, cujo potencial epistêmico é naturalmente circunscrito. Em contraste, os dados digitais apresentam um potencial epistêmico ilimitado, em razão da sua ampla capacidade de correlação. Contudo, a ausência de limites, ainda que técnicos, é incompatível com a estrutura do processo penal, de modo que o tratamento dos dados deve permanecer vinculado à hipótese investigativa, ainda que o entorno informacional permita correlações diversas.

Esse último fator será trabalhado no Capítulo 7, após a descrição dos meios de entrega (atos de investigação, meios de obtenção de provas etc.). Adiantando-se o ponto, é por essa razão que o acesso ao suporte eletrônico exige decisão judicial, momento no qual deve haver fundamentação no pedido e na decisão do que se pretende provar com o tratamento, permitindo-se, assim, limitar as ações dos órgãos de investigação, o que seria semelhante à regra processual de distribuição dos ônus probatórios no processo civil, ou seja, a delimitação do que se pretende provar com os meios de prova antecipadamente. Em suma, a postulação pelas agências de persecução e a decisão judicial funcionam como limitadoras do potencial epistêmico dos dados acessados, sendo que qualquer reúso desconectado dessa limitação deve ser considerado ilícito.

Ao tratar das bases de dados públicas, o uso lícito deve estar previsto na legislação que autoriza o compartilhamento de informações entre agências estatais, conforme trabalhado no Capítulo 3, sobre o fluxo informacional da segurança pública para a persecução criminal. Em paralelo, a utilização legítima das bases de dados privadas requer previsão legal específica, tanto para a aquisição quanto para o processamento dos dados. Ademais, os dados de conteúdo sob custódia privada devem estar sujeitos à reserva de jurisdição, seguindo o raciocínio aplicado aos dispositivos eletrônicos: a postulação e a decisão judicial delimitam o escopo da utilização do

material apreendido.

Em conclusão, as prescrições acima só encontram respaldo no artigo 13-B do CPP da legislação atual. Assim, a regra é que a apreensão e a requisição, autorizadas ou circunstanciais, não tenham seu uso lícito posterior determinado legalmente, ou restrito por decisão judicial.

5.2.4. Requisição de metadados de internet e telefonia

A pesquisa identificou duas fontes legislativas que permitem aos órgãos de persecução a requisição de metadados de comunicação, que podem ser definidos como "envelope do processo comunicacional e engloba vários tipos de dados (i.e. dados sobre o usuário que realiza a comunicação, localização, tipo de mensagem, a rede utilizada, horário, duração)"[358]. Essas fontes são a Lei das Organizações Criminosas de 2013 e o Marco Civil da Internet de 2014, esta se aplica amplamente, inclusive para processos cíveis, enquanto aquela tem âmbito restrito legalmente.

A primeira característica em comum das legislações é a retenção de metadados pelas empresas como estratégia regulatória[359]. No caso da lei de 2013, as empresas de telefonia devem reter os metadados de comunicação por cinco anos, que poderão ser requisitados pelas agências de persecução penal. Nesse sentido, chama atenção que não haja necessidade de decisão judicial para acessar esses dados por duas razões: os dados são de natureza sensível[360], já que permitem a perfilagem de cidadãos, e o dever de retenção atinge todos os usuários do sistema.

Há, inclusive, uma desproporcionalidade com a hipótese prevista no artigo 13-B do Código de Processo Penal, que exige decisão judicial para acessar dados de localização, em relação os mesmos destinatários, para localizar suspeitos e vítimas, que, como dito anteriormente, foi fruto de alteração legislativa ocorrida em 2012. Portanto, ambas as legislações versam sobre metadados de

---

[358] AGUIAR, Thaís et al. Rastreabilidade, metadados e direitos fundamentais: nota técnica sobre o Projeto de Lei 2630/2020. São Paulo: Data Privacy Brasil, 2021, p. 4.

[359] A escolha política criminal que orienta o tema é anterior à persecução penal, possibilitando a retenção indeterminada de dados sobre comunicações de todos os usuários de telefonia, sem que sejam ao menos investigados por infrações criminais, como medida de segurança pública. Mas a afirmação pode ser feita no sentido processual, isto é, para resguardar eventual meio de prova, são retidos todos os dados de comunicação por telefonia fixa e móvel. Como visto, para os registros de viagens, o acesso é garantido livremente, até mesmo ao juízo.

[360] Abreu "[...] (i) são sensíveis a questões sobre privacidade e sigilo das comunicações e, por outro, (ii) são bastante úteis como instrumentos de investigação e meios de prova. (ABREU, Jacqueline de Souza. Guarda obrigatória de registros de telecomunicações no Brasil: sobre as origens da retenção de dados e as perspectivas para direitos fundamentais. In: SIMPOSIO INTERNACIONAL LAVITS, 4., 2016, Buenos Aires. [IV Simposio Internacional LAVITS]. Buenos Aires: [s.n.], 2016. p. 2.)

comunicação, mas somente em uma das hipóteses o acesso depende de decisão judicial, sendo que a lei posterior é mais permissiva e, claramente, tem viés securitário.

Em relação ao Marco Civil da Internet, o dever de guarda tem a finalidade de instruir processos cíveis e criminais. No contexto da investigação preliminar, o acesso pode se dar por meio de requisição administrativas pelos órgãos de persecução ou por decisão judicial, cujo critério definidor é o tipo de dado que se pretende acessar, replicando-se a ideia de dados cadastrais e outros metadados. Ademais, houve a sistematização de conceitos utilizados internacionalmente, a exemplo da Internet Protocol (IP) como metadado de identificação de dispositivos eletrônicos.

O MCI escalona o grau de proteção de acesso aos dados, exigindo decisão judicial para a entrega de dados de conexão e de acesso à navegação na internet e em aplicativos, com exceção dos dados cadastrais destinados à identificação de acusados. Assim, os dados de cadastro podem ser acessados mediante requisição administrativa para identificação de suspeitos, o que guarda coerência sistêmica com os demais dispositivos das legislações penais esparsas.

A lei de regulação da internet também exige a retenção dos dados de conexão pelo provedor do serviço pelo prazo de um ano.[361] Essa obrigação compreende informações sobre o tempo de acesso, sites acessados, tipo de dispositivo – *smartphone* ou computador –, o IP utilizado para a conexão e a localização aproximada do usuário. Tal dever também recai sobre fornecedores de aplicativos, que devem manter os dados de acesso pelo prazo de seis meses; este tipo de dado revela informações como data e hora de utilização de aplicativo vinculado ao IP.

O legislador optou por diferenciar os dados de acesso dos de conexão[362], ainda que ambos possam ser configurados na categoria de metadados de tráfego. Tal afirmação está alinhada à Convenção de Budapeste, internalizada pelo Decreto n. 11.491/2023, cujo artigo 1º traz a definição de "(...) dados de computador referentes a uma comunicação (...) que indicam sua origem, destino, caminho, hora, data, extensão, duração ou tipo de serviço subordinado". Essa nomenclatura é mais precisa tecnicamente e se adequa melhor a um modelo de disciplina para as provas digitais.

O acesso a essas informações foi protegido pela reserva de jurisdição, o que é coerente com o grau da intervenção informacional a dados sensíveis; o registro de todos os sites acessados por determinado usuário, por exemplo. Entretanto, a finalidade do tratamento não é definida na

---

[361] BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, 24 abr. 2014. Art. 13º.
[362] A diferenciação pode ser encontrada no artigo 5º da MCI. (BRASIL, 2014, art. 5º.)

legislação, que é ponto que enseja o maior debate jurídico e jurisprudencial no Brasil. Atualmente, o STF julga o RE 1.301.250, em regime de repercussão geral, que dará origem ao Tema 1.148, cujo ponto central é saber como esses dados podem ser usados.

A relevância da discussão se materializa em técnicas como o *geofencing* – também chamado de "quebra de sigilos de dados reversa" – e a quebra de sigilo das buscas por palavra no *Google*. Em ambos os casos, falar em quebra de sigilo é mal colocar a discussão, mas tudo indica que é por essa linha que o julgamento vai seguir, que conta inclusive com uma proposta de tese que abraça a referida ideia[363]. Todavia, a questão não reside no acesso permitido pelas legislações aqui discutidas, mas sim no tipo de uso, com observância à finalidade legal ou não, que os agentes de tratamento, os investigadores, podem fazer dele.

Os referidos usos são técnicas de processamento que serão detalhadas no Capítulo 7. Adianta-se, pela pertinência, que a geolocalização só é permitida para localizar suspeitos e vítimas de tráficos de pessoas, logo, o uso em outras hipóteses é ilícito. Em relação às palavras-chave utilizadas no *Google*, também não há permissivo legal para a utilização e, se tratando de intervenção informacional na autodeterminação informacional de um coletivo de pessoas, exige lei para ser implementada como ato de investigação.

Retomando as prerrogativas de investigação, o período de retenção pode ser alterado por meio de requisição da polícia judiciária e do Ministério Público, que terá 60 dias para ingressar com o pedido judicial de acesso quando acreditar que informações relevantes à comprovação da hipótese criminal podem ser perdidas, se não o fizer, a retenção além do prazo legal caduca. Vale mencionar que o artigo 13, § 2º, menciona que os órgãos devem "requerer" a extensão da retenção, devendo-se ler "requisitar". O termo "requerer" foi utilizado atecnicamente, tendo em vista que não cabe ao provedor negar ou aceitar a extensão.

O Marco Civil da Internet não pode ser usado como fundamento para acesso a dados de conteúdo[364], aqueles que se referem ao registro de ações e pensamentos humanos e são inteligíveis

---

[363] No que interessa ao objeto da discussão: "1) É constitucional a requisição judicial de registros de conexão ou de registros de acesso a aplicativos de internet para fins de investigação criminal ou instrução processual penal, inclusive o fornecimento de dados pessoais por provedores, em cumprimento de medida de busca reversa por palavra-chave, com fundamento no art. 10 e no art. 22 da Lei 12.965/2014 (Marco Civil da Internet), desde que preenchidos os requisitos de (a) fundados indícios de ocorrência do ilícito; (b) motivação da utilidade dos registros solicitados para fins de investigação ou instrução probatória; (c) período ao qual se referem os registros" . BRASIL. Supremo Tribunal Federal, 2025. Proposta de tese em repercussão geral, ponto 1, da relatoria do RE 1.301.250.

[364] CORDEIRO, 2024, p. 231.

sem tratamento especializado. A razão é a ausência de permissão legal. Tal possibilidade deveria existir, em linha com os artigos 18 e 21 da Convenção de Budapeste – que o Brasil se obrigou a internalizar –, notadamente a ordem de exibição e a interceptação de dados, respectivamente. Em que pese a ausência de permissivo legal, a ordem de exibição e a interceptação/entrega de dados são comuns na prática judiciária brasileira.

Por fim, o acesso a metadados de comunicação pela Lei das Organizações Criminosas destoa da lógica sistêmica ao permitir a requisição administrativa para dados sensíveis. Por outro lado, o Marco Civil da Internet mostra-se coerente ao permitir o acesso aos dados cadastrais por requisição e exigir a reserva de jurisdição para as hipóteses de metadados de navegação. Ademais, pode haver requisição para extensão do prazo de retenção, com prazo de caducidade exposto taxativamente. Conforme visto, inexiste a possibilidade de utilizar a lei de regulação da internet como fundamento legal para o acesso a dados de conteúdo.

5.2.5. Requisição informações de deslocamento de empresas de transporte

Este tópico, assim como o anterior – que versava sobre a requisição de metadados telefônicos e telemáticos –, está diretamente conectado à formação de bases de dados privadas criadas por dever legal, tal como detalhado no Capítulo 2. Essa hipótese requer que empresas de setores regulados retenham dados para possível acesso por órgãos de persecução. Trata-se de um ponto sensível da perspectiva da proteção de dados, mas é tratado com naturalidade pelo legislador brasileiro[365]. Não é necessário que a tese repita as observações realizadas anteriormente.

No âmbito de aplicação da Lei das Organizações Criminosas, foi inserido como prerrogativa dos órgãos de investigação a possibilidade de acessarem dados relativos aos deslocamentos e reservas em empresas de transporte, que compreende as companhias aéreas e

[365] A não visualização dos dados como objeto de proteção autônoma leva a uma banalização da criação de base de dados com informações sensíveis sobre todos os usuários de serviços. Ainda que se chegue à conclusão de que a medida é adequada em razão dos riscos à segurança pública, o caminho desse convencimento deve levar em consideração a complexidade e os limites a serem impostos, como a obrigação de realização de relatórios de impacto, autorização de uso de técnicas invasivas etc. Em outras palavras, a discussão não se encerra na reserva de jurisdição para o acesso às referidas bases de dados. A título de comparação, no direito comunitário europeu, a retenção de dados é vista como assunto delicado pela Corte de Justiça da União Europeia, pelo risco de violação aos direitos humanos e à privacidade. O tribunal invalidou Diretiva de Retenção de dados em 2014 e uma legislação sueca que obrigava provedores de serviços de comunicações a reter dados de tráfego e a localização para fins de investigações criminais. No caso brasileiro, especialmente na Lei de Organizações Criminosas, chega a haver previsão de livre acesso a dados sensíveis.

viárias. De acordo com o artigo 16 da Lei 12.850/13, há a obrigação de retenção das referidas informações pelo prazo de cinco anos[366]. Sobre o acesso, a redação é peculiar: "acesso direto e permanente do juiz, do Ministério Público ou do delegado de polícia".

O dispositivo trata de acesso direto, e não de requisição por órgãos de investigação. Nesse sentido, a interpretação adequada é a de que o acesso direto é uma força de expressão, devendo ser entendido como a possibilidade de requisição sem autorização judicial. Caso contrário, as empresas deveriam manter bancos de dados com abertura permanente aos inúmeros órgãos de investigação. Essa situação assemelha-se ao caso americano em que os metadados de telefonia eram retidos diretamente pela agência de inteligência daquele país, o que se alterou após o *WikiLeaks*[367].

A separação informacional, que retira o conteúdo jurídico da autodeterminação informacional, é o princípio jurídico a ser aplicado para que uma base de dados privada – ainda que criada por dever legal – não seja de livre acesso a agentes de persecução. De modo mais amplo, os órgãos que têm interesse em acessar a informação não podem ser os mesmos que a retêm, tendo em vista a inexistência de meios efetivos de controle da legalidade do acesso. As empresas não são o *longa manus* das agências estatais para coleta, organização e disponibilização de dados.

Para além da fusão informacional criada no artigo, permitiu-se também o acesso "direto" pelo juízo. A requisição é um ato investigativo, que tem como objetivo-fim reunir indícios que confirmem precariamente uma hipótese criminal. Naturalmente, não compete aos juízes realizar atos de investigação, uma vez que toda ação positiva que se destina a comprovar uma hipótese contribui com a carga acusatória, que é incompatível com a função processual de julgador. Nesse caso, nem mesmo a defesa de atos instrutórios é possível, tendo em vista que se trata de ato investigativo contido na fase de investigação preliminar. Essas afirmações principiológicas foram tardiamente introduzidas na legislação brasileira pelo artigo 3º-A, no CPP, em 2019.

Outro ponto importante refere-se à natureza desses dados de deslocamento e reservas. Em certa perspectiva, eles são dados de conteúdo, na medida em que são inteligíveis sem necessidade de análises técnicas, a pessoa esteve no lugar "x" e se deslocou ao "y", o que enseja claramente um conhecimento a respeito da localização do investigado. Além disso, pode ser utilizado em múltiplas

---

[366] Art. 16: As empresas de transporte possibilitarão, pelo prazo de 5 (cinco) anos, acesso direto e permanente do juiz, do Ministério Público ou do delegado de polícia aos bancos de dados de reservas e registro de viagens. (BRASIL, 2013, art. 16.)

[367] GRAY, David. The Fourth Amendment in an Age of Surveillance. In: The Fourth Amendment in an Age of Surveillance. [S. l.]: Cambridge University Press, 2017, p. 76.

correlações a depender do volume, revelando informações sensíveis, credo religioso, organização política etc. Portanto, a licitude do uso depende da finalidade de tratamento, que, ao contrário da requisição de dados para geolocalização, não está presente na legislação.

Assim, para a limitação do potencial epistêmico desse ato de investigação, as requisições devem ser específicas para a identificação concreta de deslocamentos relevantes para a hipótese criminal. Apesar de ser uma intervenção informacional, não parece ser desproporcional em relação a outros métodos de investigação, a exemplo de campanas e missões de reconhecimento. Contudo, qualquer outro uso para gerar outros tipos de correlação, possíveis com a consolidação com outras bases públicas ou privadas, deveria depender de autorização judicial, a fim de emprestar-se judicialmente o tipo de processamento autorizado aos órgãos de investigação.

Diante dos argumentos apresentados, conclui-se que o artigo 16 da Lei das Organizações Criminosas deve receber interpretação conforme para evitar a fusão informacional entre bases de dados privadas e públicas, em afronta ao direito fundamental à proteção de dados, e à finalidade de tratamento, que é critério infralegal que legitimador da intervenção informacional. Ademais, o dispositivo confere prerrogativa de acesso a juízes na fase preliminar, o que mina as premissas axiológicas do sistema acusatório, especificamente nas funções processuais dos atores processuais, em outras palavras, os juízes não devem agir positivamente para aumentar a carga acusatória.

5.3. Meios ocultos de obtenção de prova digital

A doutrina brasileira que diferencia os meios de obtenção de prova dos meios de prova tornou-se majoritária e tem forte inspiração italiana[368]. O primeiro é um instrumento de pesquisa que permite trazer ao processo elementos que existiam antes dele[369], como um documento lavrado para fins econômicos que, no contexto processual, pode servir como prova direcionada ao convencimento do juízo. Os meios de prova, por sua vez, servem para produzir elementos de convicção para o processo, isto é, são constituídos em ato judicial, tal como o depoimento da

[368] O autor Paolo Tonini influenciou a processualística penal brasileira, aportando a ideia de que um elemento informativo pré-existente poderia ser buscado por um meio de pesquisa. TONINI, Paolo. Manuale di procedura penale. Nona edizione. Milano: Giuffré Editore, 2008, p. 3370). Outro autor italiano que contribuiu com essa diferenciação é Mario Chiavario. (CHIAVARIO, M. Diritto processuale penale. Nuova ediz. [s.l: s.n.]. Editore Giappichelli. 2024, p. 378).

[369] LOPES JUNIOR, 2020, p. 586.

testemunha e a declaração do perito[370].

Essa nomenclatura foi inclusive positivada em alterações legislativas recentes[371], o que justifica o uso no decorrer da tese. Entretanto, ela tem limitações, especialmente quando o meio de obtenção visa a capturar elementos informativos que ainda não existem. Nesses casos, deve-se analisar criteriosamente seu uso; na interceptação telefônica, por exemplo, o objeto não é a pesquisa do que existe, mas descobrir se há um elemento ocorrendo fora do processo que, se acautelado, pode vir a convencer o juízo.

O uso do conceito de "meio de obtenção de prova" deverá ser revisto no futuro, especialmente pelos aportes fáticos trazidos pelos elementos digitais, na medida em que qualquer elemento que precise ser processado para gerar informações inteligíveis não existe antes do processo, logo não pode ser buscado[372]. Ao contrário, o que se busca é o suporte físico que contém dados que devem ser tratados para se tornarem elementos informativos[373]. Tais elementos estão sendo constituídos na investigação preliminar, e não buscados como o conceito majoritário indica. É muito cômodo, no entanto, equiparar o dispositivo à coisa e denominá-lo fonte de prova ou objeto de busca e apreensão, quando a apreensão jurídica recai, na verdade, sobre o elemento digital.

Não é objeto desta tese a discussão da recolocação conceitual a respeito dos meios de obtenção de prova. Contudo, é importante pontuar que os tipos de atos de investigação descritos adiante dependem de autorização judicial para serem implementados. Isso decorre do fato de lidarem diretamente com inviolabilidades e sigilos constitucionalmente estabelecidos, os quais são protegidos por reserva de jurisdição, exigindo-se, como consequência, decisão fundamentada. Na mesma linha, configuram uma intervenção informacional que se conecta à proteção constitucional da autodeterminação informacional[374]. Ademais, os tópicos propõem modelos ideais para cada situação jurídica, os quais poderiam ser introduzidos na disciplina específica das provas digitais.

---

[370] BADARÓ, 2013, p. 270.

[371] A lei n. 12.850/2013 utiliza a expressão meio de obtenção de prova para descrever a natureza jurídica da delação premiada. (BRASIL, 2013).

[372] Em sentido contrário à argumentação exposta, Gustavo Torres argumento sobre o mesmo instituto que: Excepcionalmente, os meios de investigação podem se destinar diretamente à busca de elementos de prova (não repetíveis, cautelares ou legitimamente antecipados) Imagine-se, por exemplo, a interceptação, juridicamente correta, da conversa telefônica entre o investigado "A" e o coinvestigado "B", ambos posteriormente denunciados perante o juízo criminal pela prática do delito "X": os seres humanos "A" e "B"', neste caso, foram fonte (pessoal) de prova, e suas palavras referentes ao delito "X", devidamente captadas e consignadas nos autos do processo penal correlato, são, desde o início, elementos de prova (nesse caso, obtidos diretamente pelo meio investigativo denominado interceptação telefônica). (SOARES, 2014, p. 42-43)

[373] A exceção são os dados de conteúdo, que não precisam de tratamento profissional para serem entendidos por leigos.

[374] GLEIZER, Orlandino. A dogmática dos métodos ocultos de investigação no processo penal, 2021, p. 122.

5.3.1. Busca e apreensão de dispositivos informáticos

É comum que a apreensão seja descrita como consequência da busca, seja ela pessoal ou domiciliar. No entanto, trata-se, na verdade, de instituto cautelar autônomo, voltado ao ingresso de elementos de informação na investigação[375]. No contexto da prova digital, por exemplo, as vítimas podem apresentar à autoridade policial ou ao Ministério Público dados digitais aos quais tenham acesso, com o intuito de dar início à investigação. Esses dados serão apreendidos, ainda que não tenham sido buscados como meio de obtenção de prova oculta ou em situação de flagrância.

A notícia de crime é um meio procedimental que pode ser utilizado por qualquer pessoa, incluídas as pessoas jurídicas, para comunicar às autoridades a ocorrência de infrações penais. Dessa forma, quando vier acompanhada de elementos digitais que corroborem o relato, tais como backup de e-mails utilizados em investigações corporativas, a autoridade deverá formalizar o recebimento dessa entrega voluntária por meio de um termo de apreensão, em observância ao princípio da formalidade dos atos processuais. Nessa hipótese, há apreensão sem busca, demonstrando a independência conceitual.

Por outro lado, deve-se presumir a necessidade de busca nas hipóteses em que haja direito de não produzir provas contra si mesmo[376], ou seja, nas situações em que as agências estatais não possam requisitar informações de pessoas na condição de suspeitas, em razão do direito à não autoincriminação e das demais exceções legais à colaboração com a carga probatória – as imunidades, as relações de parentescos e os deveres profissionais[377].

Entretanto, a busca de elementos digitais não recebeu tratamento diferenciado até o momento pelo ordenamento brasileiro, sendo tratada por analogia a objetos, instrumentos e coisas. Essa é a mesma situação jurídica que ocorre na hipótese da busca como consequência do flagrante, conforme já abordado no Tópico 4.1.

---

[375] Parte da doutrina caracteriza a busca como meio de obtenção de prova e a apreensão como medida cautelar, a exemplo de Lopes Junior. Entretanto, o tratamento dado ao tema, por desenho do tópico, utiliza a segmentação do Código de Processo Penal.

[376] LOPES JUNIOR, 2020, p. 153-155.

[377] Situação jurídica que a dogmática processual penal portuguesas denomina de provas proibidas. DA COSTA ANDRADE, Manuel. Sobre as proibições de prova em processo penal, 2013, p. 286-304.

É certo que os dispositivos eletrônicos são coisas tangíveis[378], mas a intenção jurídica ao apreendê-los é acessar a miríade de informações neles contida – de cunho comunicacional, financeiro, político, religioso, fiscal etc. Como dito anteriormente, essa pretensão de utilização atinge o direito fundamental à autodeterminação informacional, sem prejuízo, contudo, de que no caso concreto haja a indevida intrusão em outros, a exemplo dos sigilos fiscal e bancário, frequentemente armazenados em dispositivos eletrônicos. Assim, a proteção jurídica deve recair centralmente sobre o conteúdo informacional, e não sobre o suporte físico.

A primeira constatação é de cunho ontológico: o elemento que se busca será sempre o suporte eletrônico, que é o que pode ser apreendido fisicamente. Por outro lado, a apreensão útil juridicamente incide sobre os dados digitais que estão nele armazenados[379]. Logo, o que se pretende é realizar o uso dos dados do dispositivo eletrônico apreendido, que deve ser limitado, desde a representação para a busca e apreensão, pela hipótese da investigação e, naturalmente, pela decisão autorizadora, que determina o conteúdo do tratamento lícito autorizado. Essa distinção exige que a legislação discipline diferentemente o procedimento das buscas por elementos físicos.

A tendência é que isso ocorra à luz da Convenção de Budapeste, que prevê a obrigação de os Estados signatários instituírem diversos meios de obtenção de provas digitais, entre eles o disposto no Título IV, acerca da "busca e apreensão de dados de computador"[380], sem, contudo, especificar se tal busca envolve acesso físico ou remoto aos dispositivos. Naturalmente, essa mudança deve vir acompanhada de procedimentos que permitam endereçar as particularidades desse meio de obtenção de prova para os elementos digitais, tais como a cadeia de custódia para a admissão e o registro detalhado das etapas de processamento, de modo a permitir a repetibilidade dos atos como condição de validade para admissão na ação penal.

Para efeitos comparativos, as requisições exigem a entrega do elemento informativo, é uma ordem de abertura de dados, o que implica um pré-tratamento por empresas privadas, que se perfaz com a delimitação do passageiro, da torre de telefonia, isto é, com as informações que permitam a

---

[378] KNIJNIK, Danilo. A triologia Olmstead-Katz-Kyllo: o art. 5º da Constituição Federal do século XXI. Revista Escola da Magistratura do TRF da 4ª Região, ano 2, número 4. Porto Alegre/RS, 2016, p. 84.

[379] Olin Kerr trabalhou ideia semelhante, defendeu que há uma segunda busca eletrônica que se segue à primeira física. (KERR, Orin S., Search Warrants in an Era of Digital Evidence. 75 Mississipi Law Journal 85, 2005, p. 91). Nos parece que a primeira busca é instrumental a primeira, na medida em que a apreensão de dispositivos eletrônicos deveria estar autorizada desde o primeiro momento para que se tenha efetivado.

[380] BRASIL. Decreto nº 11.491, de 12 de abril de 2023. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. *Diário Oficial da União*, Brasília, DF, 13 abr. 2023. Art. 19.

filtragem dos elementos úteis. Já as buscas e apreensões visam ao suporte que pode conter informações úteis a investigação. Em tese, a apreensão é sempre possível, tendo em vista que os dados sempre estão armazenados fisicamente apesar do potencial de ineficácia, é possível a apreensão completa de um *data center.* Essa intervenção informacional, no entanto, seria uma das mais gravosas a ser adotada pelo ordenamento jurídico e criaria conflitos jurisdicionais[381].

Sob a perspectiva de validade, o Código de Processo Penal exige que os mandados de busca e apreensão indiquem: o local da diligência, os nomes do morador e dos investigados, ou meios de identificá-los, e o objetivo probatório a ser alcançado[382]. Soma-se a isso, por exigência constitucional, a fundamentação concreta, que deve indicar elementos de autoria e materialidade para autorizar a medida. Nesse particular, não há divergência relevante sobre esses elementos, mas a situação se complexifica ao inserir os elementos digitais, na medida em que a apreensão almeja elementos digitais desconhecidos no momento da decisão judicial.

O primeiro limite que se aplica é que a busca por dispositivos eletrônicos deve ser expressamente autorizada e justificada em elementos que identifiquem, para determinada hipótese, a possibilidade de existir prova digital a ser produzida. Em segundo lugar, "os fins da diligência", na nomenclatura do CPP, têm de ser interpretados como o tratamento de dados permitido aos investigadores, delimitado pela decisão judicial que autoriza a intervenção informacional no repositório de informações da pessoa suspeita ou investigada, condicionando, inclusive, o emprego de técnicas automatizadas de investigação.

Assim, considerando que o investigador poderá utilizar um algoritmo de palavras-chave, em todo o conteúdo copiado de um celular – técnica orientada por padrões linguísticos associados a tipos penais específicos –, essa utilização deve permanecer vinculada à hipótese investigativa postulada e autorizada judicialmente. Nessa linha, na investigação de um crime ambiental, a utilização do algoritmo para encontrar elementos típicos de crimes sexuais excederia o limite imposto para a intervenção informacional. O argumento pressupõe, necessariamente, que o uso de tecnologias da informação dê origem a relatórios de investigação específicos.

Os dados digitais são produzidos e armazenados por meio de protocolos que organizam a comunicação entre dispositivos, de modo que a informação está organizada em padrões que podem

---

[381] A afirmação é no sentido de que um *data center* no Brasil pode armazenar dados de usuários de diversos países, cujas proteções jurídicas são díspares, logo a apreensão nesse contexto seria extremamente gravosa.
[382] BRASIL, 1941, art. 243.

ser lidos estruturadamente. Mesmo os dados de conteúdo podem ser lidos e estruturados para leitura automatizada (como fotos e vídeos). Em analogia, o repositório digital de um celular se assemelha mais a uma biblioteca profissional do que a um almoxarifado de madeireira: a informação é catalogada desde a entrada para que sejam possíveis os múltiplos usos por diversos usuários.

Portanto, a escala de informações em dispositivos eletrônicos é incomparável ontologicamente à de objetos corpóreos, para os quais a busca e a apreensão, como meios de obtenção de provas, foram positivadas. A variedade e a quantidade de dados armazenados em dispositivos eletrônicos exigem maior controle da atividade de investigação, uma vez que dados desconexos passam a constituir informação inteligível ao observador[383].

Quando forem utilizadas ferramentas avançadas de tecnologia da informação, o relatório de investigação deve expor, pormenorizadamente, os critérios automatizados usados, a exemplo das palavras-chave buscadas ou o racional para o emprego de algoritmos de reconhecimento facial em fotos e vídeos. Caso a investigação tenha seguido uma linha diferente da que foi autorizada na decisão de busca e apreensão, configura-se *fishing expeditons*[384], e o resultado obtido não pode ser utilizado na fase pré-processual, tampouco admitido na ação penal, já que configura um rompimento com a vinculação causal entre a decisão e a prova[385].

O modelo ideal para busca e apreensão de dispositivos eletrônicos exigem que a decisão judicial vincule a busca digital ao fim específico da diligência, com autorização expressa para o rompimento de barreiras de segurança. O ato de investigação subsequente deve registrar quem teve acesso ao material, por quanto tempo, quais ferramentas utilizou e quais critérios aplicou, garantindo a repetibilidade dos resultados e a transparência processual[386].

Em síntese, o tratamento lícito de dados na investigação é determinado, com base na hipótese, pela decisão judicial autorizadora. O desconhecimento prévio dos elementos a serem

---

[383] RIBEIRO, M. S. Características da informação na Teoria Quântica e suas possíveis interpretações para um objeto informacional na Ciência da Informação, 2014, p. 119.

[384] Entendido nos seguintes termos: "como a apropriação de meios legais para, sem objetivo traçado, pescar qualquer espécie de evidência, tendo ou não relação com o caso concreto. Trata-se de uma investigação especulativa indiscriminada, sem objetivo certo ou declarado, que, de forma ampla e genérica, lança suas redes com a esperança de pescar qualquer prova, para subsidiar uma futura acusação ou para tentar justificar uma ação já iniciada". SILVA, Viviani Ghizoni da; MELO E SILVA, Philipe Benoni; MORAIS DA ROSA, Alexandre. Fishing expedition e encontro fortuito na busca e na apreensão: um dilema oculto do processo penal. 2. ed. Florianópolis: Emais, 2022, p. 175.

[385] Aury Lopes JUNIOR trabalha a ideia de vinculação causal, a busca e a apreensão devem ficar restritas às hipóteses autorizadas no pedido e na decisão, mas reconhece que a jurisprudência permite que o é encontrado fortuitamente seja utilizado, sem critérios adicionais. (LOPES JUNIOR, 2020, p. 823)

[386] PRADO, Geraldo. *A cadeia de custódia da prova no processo penal*. 1. ed. São Paulo: Marcial Pons, 2019, p. 87-124.

encontrados não justifica intervenções informacionais indiscriminadas. Esse argumento defende a vinculação causal entre pedido e prova, estabelecida na cooperação jurídica internacional, que se denomina como princípio da especialidade[387], que visa a aumentar o grau de previsibilidade nas relações. O Estado não pode julgar o extraditando por infração que conhecia à época da extradição e não comunicou à outra parte; na mesma linha, as provas recebidas em razão do pedido "a" não podem ser reaproveitadas para outro processo, salvo nova autorização específica da contraparte.

O modelo proposto pode ser resumido pela seguinte equação: autorização da apreensão de dispositivo eletrônico + autorização para o rompimento da barreira de segurança + uso lícito automatizado conforme a hipótese que originou a decisão judicial + produção de relatório de processamento (tratamento) = validade da apreensão do elemento informativo digital, que resulta na admissibilidade na ação penal. As duas primeiras parcelas da soma podem estar em uma única decisão judicial ou podem ocorrer em momentos distintos, diante de novas informações.

Deve ficar claro que a hipótese investigativa é o elemento limitador da intervenção informacional, tendo em vista ser impossível que algum modelo preveja o uso que possa ser dado previamente para todas as situações jurídicas. Também não se trata de exigir um exercício de futurologia da magistratura, mas tão somente de limitar a busca a elementos de informações por meio de critérios racionalizáveis, a partir de informações já conhecidas. Naturalmente, se isso não for possível, a maior probabilidade é a de que a busca e a apreensão do dispositivo eletrônico estejam sendo utilizadas de forma especulativa.

Esta argumentação não se confunde com o conceito de cadeia de custódia. Ainda que os procedimentos técnicos de armazenamento e espelhamento garantam a autenticidade e a integridade do dispositivo, o tratamento de dados pode ser ilegal caso a investigação prossiga além

---

[387] O princípio da especialidade tem origem na extradição e é expressamente previsto pela nova Lei da Imigração, esta norma apresenta evidente caráter de proteção, na medida em que no processo extradicional, o Estado requerente fica subordinado às razões submetidas no pedido de extradição, evitando, portanto, que o extraditado venha a ser julgado posteriormente em hipóteses que os Estados teriam negado o pedido num primeiro momento. Aumenta, assim, a previsibilidade dos atos de cooperação e os interesses fundamentais da pessoa extraditada. Além disso, o fundamento para sua utilização na assistência direta é bastante amplo, tendo em vista estar previsto na Convenção de Viena, de Palermo, no Protocolo do Mercosul e na maior parte dos tratados bilaterais celebrados pelo Brasil. Em se tratando dos atos de cooperação próprios, nos quais os Estados atuam no sentido de instruir processo penal sob jurisdição estrangeira, o princípio da especialidade tem finalidade de reduzir a desconfiança entre os atores cooperantes e evitar que os elementos de informação transitados entre as jurisdições sejam utilizados em processos dos quais o Estado requerido não tenha conhecimento. Assim, em caso de descumprimento deste tipo de norma, regida pela boa-fé objetiva dos agentes públicos, da perspectiva política, o efeito será futuro – impedindo outras relações cooperacionais – e imediato para os visados (investigados ou réus) que poderão arguir, na jurisdição para qual se destinou os elementos, que estes estão sendo utilizados de forma ilícita, com perpetuação de ato ilícito internacional, o que, evidentemente, é causa maculadora da prova, impedindo que sua carga probatória seja incorporada ao processo.

dos limites e hipóteses autorizados pela decisão de busca e apreensão. O conceito de cadeia de custódia vem sendo mais bem tratado jurisprudencialmente[388] e é aplicado por analogia[389].

Antes de concluir, há um elemento da prática judicial brasileira, convalidada pelos tribunais, que põe em risco toda a argumentação realizada sobre a busca e apreensão de elementos digitais, para a qual se traçou um modelo para determinar o tratamento lícito pelos investigadores. O Superior Tribunal de Justiça aplica a teoria da serendipidade para validar as provas encontradas em medidas ocultas de investigação que não tenham conexão com a decisão judicial que autorizou a medida[390]. Essa interpretação mina a defesa da exigência da finalidade no tratamento de dados para a busca da prova digital, que poderia ser superado pela admissibilidade do encontro fortuito.

Giacomolli e Eilberg têm razão ao afirmar que encontro fortuito é inaplicável à dimensão digital, na medida em que tudo é direcionado pelo investigador, especialmente com uso de ferramentas automatizadas, o que inviabiliza o uso de doutrinas justificadoras do desvio causal[391]:

> [...] No mundo digital, não há encontro fortuito com as características justificantes de aproveitamento probatório do encontro fortuito de prova que tenha uma corporeidade no mundo digital, vez que no mundo digital tudo é direcionado, calculado, premeditado com algoritmos. [em outro momento] (...) no que diz respeito à temática de encontro fortuito e, principalmente, aos perigos da prática de *fishing expedition* no acesso de dados não-abertos por meio de ferramentas de raspagem automática, reitera-se a necessidade de atentar aos requisitos de continência e conexão de dados relacionados à infração penal que ensejou a investigação, sob pena de ser contrário à justa causa.

Já Cordeiro, Agosti e Camargo defendem a aplicabilidade da doutrina do *plain view* como limitação adicional à validade do encontro fortuito de provas digitais[392]. Nesse contexto, sustentam que a prova encontrada organicamente poderia ser validada. Esse argumento pressupõe que investigadores analisam dispositivos como usuários, com abertura de aplicativos e o acesso a

---

[388] O informativo de jurisprudência do Superior Tribunal de Justiça aponta o RHC 77.836/PA como *leading case* pertinente à discussão realizada.

[389] Artigos 158-A e 158-B, do Código de Processo Penal, introduzidos pela Lei n. 13.964/2019. (BRASIL. Lei nº 13.964, de 24 de dezembro de 2019. Aperfeiçoa a legislação penal e processual penal. *Diário Oficial da União*, Brasília, DF, 24 dez. 2019)

[390] Ainda que algumas decisões ressalvem o entendimento, o encontro fortuito de provas é validado frequentemente pelo tribunal, cita-se a título de exemplo os seguintes julgados: RHC 98.182/RJ, AgRg no HC 416.098/RS e AgRg no REsp 1.717.551/PA.

[391] GIACOMOLLI, Nereu José; EILBERG, Daniela Dora. Coleta e tratamento de dados na transformação tecnológica da investigação criminal. Galileu - Revista de Direito e Economia, v. 24, n. 1-2, jan./dez. 2023, p. 129; 133-134.

[392] CORDEIRO, Pedro Ivo Rodrigues Velloso; AGOSTI, Francisco Felippe Lebrão; CAMARGO, Pedro Luís de Almeida. Repensando o encontro fortuito de provas na era digital, 2024, p. 24.

diretórios de informação. Entretanto, o que se verifica factualmente é cópia integral dos dados, seguida da organização de fluxos informacionais por meio de ferramentas automatizadas para o tratamento. Na ausência de pesquisas empíricas sobre o ponto da divergência, é conveniente formular uma construção conceitual por exclusão: a utilização ferramentas automatizadas afasta a fortuidade necessária para caracterizar o *plain view*, por ser ato de investigação intencional.

Assim, se usadas as balizas jurisprudenciais atuais para as provas digitais, sem um modelo que exija que o resultado da investigação, ou do tratamento de dados, seja detalhadamente exposto, qualquer elemento de informação constante de um dispositivo poderá ser utilizado em ações penais, independentemente da autorização judicial dada. Isso significa que a decisão autorizadora seria somente uma "licença" aos investigadores para que, a partir do acesso autorizado, possam aplicar qualquer método automatizado de investigação, desvinculado da hipótese investigativa.

Por fim, espera-se que o reconhecimento do potencial epistêmico a partir do tratamento de dados seja um vetor de mudança no entendimento jurisprudencial sobre o encontro fortuito, sob pena de que *fishing expeditions* se tornem a regra sistêmica, ainda que visualizadas em situações intencionais. Para tanto, o modelo proposto para a busca e apreensão da prova digital estática visa a racionalizar a adequação da atividade investigativa, de forma dinâmica, à hipótese investigativa, para a qual a decisão judicial funciona como critério de finalidade do tratamento de dados.

5.3.2. Interceptação telefônica, telegráfica e telemática

A inclusão da interceptação telefônica e telegráfica no capítulo destinado aos meios ocultos de obtenção de prova com relevância digital decorre do histórico da discussão no Brasil. No plano constitucional, assegura-se o direito ao sigilo da correspondência e à inviolabilidade das comunicações telefônicas e telegráficas[393]. Não há, contudo, lei específica acerca do levantamento do sigilo postal ou da quebra da inviolabilidade telegráfica, tendo o legislador optado por disciplinar, segundo o preâmbulo da Lei nº 9.296/1996, o "inciso XII, parte final" do artigo 5º da Constituição.

No âmbito legal, o parágrafo único do artigo 1º da referida lei aumentou o escopo da inviolabilidade das comunicações para inserir aquelas realizadas por sistemas de informática e

[393] BRASIL, 1988, art. 5º, XII.

telemática. Essa ampliação levou alguns doutrinadores a defenderem a inconstitucionalidade do dispositivo[394], o que é incoerente, já que Constituição determina a proteção mínima a direitos, e não a máxima. Em sentido semelhante e complementar, o Marco Civil da Internet consagrou o sigilo do fluxo das comunicações e o sigilo das comunicações privadas armazenadas[395]. Assim, as inviolabilidades das comunicações em fluxo e armazenadas têm status infraconstitucional[396].

A legislação da internet positivou a distinção entre dados em fluxo e armazenados, o que espelha o entendimento jurisprudencial do STF da época da edição da lei, em 2014. Antes de avançar na conceituação, vale retomar que a utilização da expressão "dados" já havia suscitado debate doutrinário após a promulgação da Constituição de 1988[397], o que é indicativo do contexto histórico que deve ser resgatado para a compreensão do tema. O fato é que o entendimento adotado pelo STF recepcionou, em grande maioria, os argumentos expostos por Ferraz Júnior no clássico artigo intitulado "Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado"[398], escrito em 1993.

O autor partia da premissa de que o objeto da proteção constitucional é a ação humana, as liberalidades, de modo que o sigilo seria instrumental à proteção de direitos fundamentais, no caso da comunicação, o direito à privacidade[399]. Dessa forma, o que deveria ser protegido pela inviolabilidade constitucional era o ato de se comunicar, e não o produto da comunicação, materializado nos vestígios deixados. Essa interpretação permitia, por exemplo, que uma carta não aberta não pudesse ser interceptada, mas poderia ser apreendida se encontrada aberta na residência durante uma busca domiciliar.

---

[394] Segundo Grinover, "O dispositivo é de duvidosa constitucionalidade, tendo sido ajuizada ação direta, ainda pendente de julgamento, a seu respeito, sob o fundamento de que violaria o sigilo da comunicação de dados (inc. XII, do art. 5º CF), que é absoluto (...) Desse modo, parece que o dispositivo em questão é efetivamente inconstitucional, salvo se se der ao termo" comunicações telefônicas" a acepção de "comunicações pela via telefônica", o que também é de difícil aceitação. (GRINOVER, A. P. O regime brasileiro das interceptações telefônicas. Revista de Direito Administrativo, [S. l.], v. 207, p. 21–38, 1997, p. 25)

[395] BRASIL, 2014, art. 7.

[396] Em sentido mais amplo, há autores que defendem que o sigilo constitucional "abrange toda a dimensão do preceito: correspondência, comunicação telegráfica, dados e comunicação telefônica – nessa ordem. Assim, tudo isso compõe a esfera da inviolabilidade constitucional". (GIACOMOLLI, Nereu; CANI, Luiz Eduardo. O acesso autorizado a aparelhos smart: burla ao agente infiltrado digital? Boletim IBCCRIM, São Paulo, v. 30, n. 352, 2024, p. 4-5.)

[397] BRITO CRUZ, Francisco; SIMÃO, Bárbara (eds.). Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate. Vol. IV. São Paulo. InternetLab, 2021, p. 8.

[398] FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. Revista da Faculdade de Direito da Universidade de São Paulo, São Paulo, v. 88, 1993.

[399] Segundo o autor, "Sigilo não é o bem protegido, não é o objeto do direito fundamental. Diz respeito à faculdade agir (manter sigilo, resistir ao devassamento), conteúdo estrutural do direito". FERRAZ JUNIOR, 1993 p. 443.

Esse contexto jurídico fomentou a distinção entre dados em fluxo e dados armazenados, sendo o primeiro passível de interceptação e o segundo, de levantamento de sigilo. A inviolabilidade foi entendida, pela doutrina, como proteção ao meio de comunicação, e não ao conteúdo da comunicação[400]. Contudo, a realidade fática foi completamente alterada: uma conversa em tempo real por aplicativo de mensagens instantâneas é armazenada para permitir a comunicação. Mais amplamente, a internet se estrutura no armazenamento e na organização de informações, razão pela qual a distinção deve ser superada.

A lógica sistêmica era a seguinte: o dado armazenado podia ser apreendido e analisado, respeitando-se a reserva de jurisdição, enquanto o dado em fluxo dependeria de decisão de interceptação telefônica, nos termos da lei prevista pela Constituição. Como se sabe, entretanto, essa lei somente foi promulgada em 1996, quase doze anos após o texto constitucional. Nesse intervalo, vale lembrar que o STF entendeu que era lícita a interceptação sem lei autorizadora[401] [402], em outros termos, era lícito o atingimento a direitos fundamentais sem norma específica, que vai de encontro ao marco teórico da tese.

A projeção desse argumento para dispositivos eletrônicos foi automática, equiparando-se microcomputadores a cartas ou quaisquer objetos com dados armazenados. No *leading case* do Recurso Extraordinário n. 418.416[403], o STF manteve esse entendimento para computadores apreendidos, afastando a nulidade da análise após a apreensão, como se lê[404]:

> [...] III. Decreto de busca e apreensão: validade. 1. Decreto específico, que somente permitiu que as autoridades encarregadas da diligência selecionassem objetos, dentre aqueles especificados na decisão e na sede das duas empresas nela indicadas, e que fossem "interessantes à investigação" que, no caso, tinha pertinência com a prática do crime pelo qual foi efetivamente condenado o recorrente. 2. Ademais não se demonstrou que as instâncias de mérito tenham invocado prova não contida no objeto da medida judicial, nem tenham valorado qualquer dado resultante da extensão dos efeitos da decisão determinante da busca e apreensão, para que a Receita Federal e a "Fiscalização do INSS" também tivessem acesso aos documentos apreendidos, para fins de investigação e cooperação na persecução criminal, "observado o sigilo imposto ao feito". IV - Proteção constitucional ao sigilo das comunicações de dados - art. 5º, XVII, da CF: ausência de violação, no caso. 1. Impertinência à hipótese da invocação da AP 307 (Pleno, 13.12.94, Galvão, DJU 13.10.95), em que a tese da inviolabilidade absoluta de dados de computador não pode ser

[400] FERRAZ JUNIOR, 1993, p. 439-459.
[401] BRASIL. Supremo Tribunal Federal. Habeas Corpus n. 69.912/RS. Redator para o acórdão: Min. Carlos Veloso. Tribunal Pleno. Julgado em 30 jun. 1993. Publicado no Diário de Justiça, 26 nov. 1993.
[402] BRASIL. Supremo Tribunal Federal (STF). Tribunal Pleno. Habeas Corpus nº 69.912/RS. Relator: Min. Sepúlveda Pertence. Julgado em 16 dez. 1993. *Diário da Justiça*, Brasília, DF, 01 fev. 1994.
[403] BRASIL. Supremo Tribunal Federal, 2004.
[404] BRASIL. Supremo Tribunal Federal, 2004, Ementa do Julgamento.

> tomada como consagrada pelo Colegiado, dada a interferência, naquele caso, de outra razão suficiente para a exclusão da prova questionada - o ter sido o microcomputador apreendido sem ordem judicial e a conseqüente ofensa da garantia da inviolabilidade do domicílio da empresa - este segundo fundamento bastante, sim, aceito por votação unânime, à luz do art. 5º, XI, da Lei Fundamental. 2. Na espécie, ao contrário, não se questiona que a apreensão dos computadores da empresa do recorrente se fez regularmente, na conformidade e em cumprimento de mandado judicial.

Esse entendimento perdurou até que os tribunais passaram a se deparar com teses defensivas relacionadas à análise de dados armazenados em dispositivos eletrônicos encontrados durante buscas pessoais – tema já abordado em tópico próprio. Como se observa no julgado, a proteção recai sobre o meio de comunicação, sendo possível a análise do conteúdo desde que não haja interceptação em tempo real. Esse entendimento produziu efeitos significativos no sistema processual penal brasileiro e demorou a ser revisado.

Nessa linha de entendimento, todas as conversas de *WhatsApp* registradas no celular de alguém submetido a uma busca pessoal e apreensão estariam acessíveis para a polícia ostensiva, à exceção da conversa em andamento, que não poderia ser colocada no viva-voz, já que configuraria interceptação em tempo real. É óbvio, contudo, que é "falsa a noção de que o fluxo de comunicações só seria violável pelas comunicações telemáticas e telefônicas na forma da Lei nº 9.296/96"[405]. As comunicações por aplicativo são a evidência dessa assertiva.

A tese começou a ser superada pelos Tribunais Superiores em razão de alterações fático-sociais, chegando o STF a reconhecer a ocorrência de mutação constitucional em caso no qual a Polícia Militar acessou dados de *WhatsApp* durante uma busca pessoal no domicílio do paciente, em 2020[406]. Em sentido semelhante[407], o STJ já havia decidido um caso de acesso ao *WhatsApp* por autoridade policial em 2016[408], com destaque para o voto que afirmou que a ação violou a intimidade e a privacidade, ainda que não se enquadrasse nas hipóteses do Marco Civil da Internet e da Lei de Interceptações Telefônicas.

Ambos os precedentes prenunciam uma tese mais ampla: o acesso a dados de conteúdo em

---

[405] INTERNETLAB. O direito das investigações digitais no Brasil: fundamentos e marcos normativos. 3. ed. São Paulo: InternetLab, 2022. p. 301.
[406] BRASIL. Supremo Tribunal Federal (STF). Segunda Turma. Habeas Corpus nº 168.052 São Paulo. Relator: Min. Gilmar Mendes. Julgado em 20 out. 2020.
[407] BRASIL. Superior Tribunal de Justiça (STJ). Sexta Turma. Recurso Ordinário em Habeas Corpus nº 51.531/RO. Relator: Min. Nefi Cordeiro. Julgado em 19 abr. 2016.
[408] BRASIL. Superior Tribunal de Justiça (STJ). Quinta Turma. Recurso em Habeas Corpus nº 89.981/MG. Relator: Min. Reynaldo Soares da Fonseca. Julgado em 05 dez. 2017. *Diário da Justiça Eletrônico*, Brasília, DF, 13 dez. 2017.

investigações criminais não está abrangido pela hipótese de interceptação telemática. O que não significa que o acesso prescinda da reserva de jurisdição; ao contrário, revela a mora na criação de marco normativo que assegure previsibilidade à persecução penal e proteção efetiva ao núcleo essencial do direito à privacidade e à autodeterminação informacional. Nesse contexto, a quebra do sigilo telemático é efeito jurídico não decorrente do ato de interceptar. No limite, a dicotomia entre dados estáticos e em fluxo é uma relativização de garantias fundamentais[409].

A discussão histórica brasileira, em conjunto com as alterações legislativas infraconstitucionais, mal posicionou o debate sobre inviolabilidade e sigilo das comunicações relativas aos dados estáticos de conteúdo produzidos com o uso da internet. O resultado foi a aplicação analógica de conceitos jurídicos inadequados e a replicação de práticas procedimentais inviáveis tecnicamente. Os dados telemáticos são sigilosos, nos termos do MCI, mas o ato jurídico de interceptar é inaplicável a esses casos, razão pela qual não há instrumentalidade adequada para implementação da decisão judicial que quebra o sigilo temático.

Vale lembrar que nem mesmo a lei de interceptação telefônica disciplina como o ato deve ser instrumentalizado nas ligações tradicionais[410]. Na prática policial, as empresas são oficiadas com a decisão judicial e desviam o sinal para as agências de investigação. Aplicando-se o mesmo *modus operandi*, as agências passaram a oficiar as empresas de tecnologia para disponibilizarem os dados que têm sob custódia. Assim, o ato jurídico autorizado judicialmente é uma ordem de abertura de dados de conteúdo, e não uma interceptação de dados telefônicos.

Nesse sentido, a ordem de abertura de dados no ordenamento brasileiro se assemelha mais ao que se convencionou denominar requisições de dados, tal como exposto anteriormente. Contudo, essa solução enfrenta dois problemas práticos: i) a abertura tem que ser tecnicamente possível e ii) o local de armazenagem da informação que se requer pode estar fisicamente em outra jurisdição. A primeira questão comunica-se com a utilização de PET (*privacy-enhancing technologies*); a segunda, com a computação em nuvem, que demanda cooperação jurídica

---

[409] Nesse sentido, aponta Dora Eilberg, "Essa problemática se evidencia quando o objeto da proteção ao sigilo previsto constitucionalmente está em jogo. Disputas sobre o que estaria sob sigilo – o conteúdo em si ou o fluxo das informações comunicadas –, além das exceções previstas no dispositivo que permitem a quebra de sigilo (INTERNETLAB, 2020, p. 20) exigem a valorização da privacidade mesmo de dados telemáticos cujo caráter é estático. A relativização da garantia constitucional é infundada". EILBERG, 2024, p. 35.

[410] Art. 6º da Lei n. 9.296/1996, "Deferido o pedido, a autoridade policial conduzirá os procedimentos de interceptação, dando ciência ao Ministério Público, que poderá acompanhar a sua realização. (BRASIL. Lei nº 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. *Diário Oficial da União*, Brasília, DF, 25 jul. 1996.)

internacional, ou deveria demandar, para a efetivação das decisões judiciais. Essa é precisamente a situação jurídica que envolve as grandes empresas provedoras de comunicação, armazenamento e redes sociais, que será desenvolvida no Capítulo 6.

A constatação doutrinária de que "[...] a legislação não dispõe exaustivamente sobre os parâmetros e o meio de execução da quebra de sigilo de dados armazenados"[411] não pode vir acompanhada da proposição de critérios supletivos doutrinariamente[412], como se estes pudessem complementar aquela. Dessa forma, conclui-se que não há critérios no ordenamento processual penal brasileiro para o levantamento do sigilo de dados armazenados e que, na ausência de autorização legal, o Estado deve se abster de atos que atinjam direitos fundamentais.

Em que pese a posição individual do dever de abstenção como dever constitucional, a defesa majoritária é em outro sentido. Gisela Wanderley sustenta que "não se pode inviabilizar a atividade de persecução penal ao simplesmente cominar de nulo qualquer meio de obtenção de provas ainda não regulamentado em lei específica"[413]. Se for esse o caso, argumentos como os de Sidi também estão corretos, na medida em que importam critérios da lei vigente a uma situação jurídica distinta, por exemplo, a respeito do limite temporal de apreensão: "de mensagens pretéritas armazenadas pelo indivíduo ou por seu provedor não será válida se não datarem do período compreendido pela autorização judicial, que deverá ser concedida nos termos do artigo 5º da Lei nº 9.296/96" [414].

Ainda que fosse possível superar a vedação constitucional – o que não é –, a partir dessas características, a legislação processual deve prescrever o meio próprio de obtenção de provas, sob pena de que esse limite seja flexibilizado e estabelecido por interpretação voluntarista. O segundo argumento é de cunho prático: o uso mais útil desse meio de obtenção por analogia seria em relação a empresas de tecnologias cujas sedes ou áreas de armazenamento estejam em outros países; contudo, as decisões brasileiras não cumpriram o requisito, em eventual conflito de normas internacionais, de demonstrar o fundamento legal da obrigação das empresas.

Por fim, a quebra de sigilo telemático com base nos critérios da Lei de Interceptações

---

411 MOURA, Maria Thereza Rocha de Assis; BARBOSA, Daniel Marchionatti. Dados digitais: interceptação, busca e apreensão e requisição. In: DIREITO, PROCESSO E TECNOLOGIA. 2021, p. 488.
412 MOURA; BARBOSA, 2021, p. 489.
413 WANDERLEY, Gisela. Privacidade e Cidadania: Os Limites Jurídicos da Atividade Investigativa e a Legalidade do Acesso Policial a Aparelhos Celulares. In: ANTONIALLI, Dennys; FRAGOSO, Nathalie (org.). Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate. São Paulo: InternetLab, 2019. v. 2, p. 119.
414 SIDI, Ricardo. A interceptação de e-mails e a apreensão física de e-mails armazenados. Revista Fórum de Ciências Criminais - RFCC, Belo Horizonte, ano 2, n. 4, p. 101-121, jul./dez. 2015.

Telefônicas é insuficiente para garantir a proteção da intimidade[415], da autodeterminação informacional[416] e da proteção de dados. Apesar de acertos jurisprudenciais, em especial do STJ, o levantamento de sigilo dos dados de conteúdo exige autorização legal para que empresas sejam obrigadas a cedê-los a agências de persecução.

5.3.3. Infiltração digital: autorização para o uso de Malware?

A infiltração digital é um meio de obtenção de provas inserido na legislação por duas leis especiais: a Lei das Organizações Criminosas[417] e o Estatuto da Criança e do Adolescente[418]. Ela consiste na infiltração de investigadores no ambiente digital, replicando-se as exigências da infiltração policial tradicional[419], que se utiliza de técnicas para camuflar a real identidade e desenvolver relações pessoais para adquirir elementos de informação. Nesses casos, as informações informáticas que o agente tenha acesso, em grupos de conversas, arquivos compartilhados, fotos, vídeos, dentre outros, podem ser utilizadas na investigação preliminar.

No ambiente digital, infiltração autoriza a criação de *perfis* falsos e a manutenção de comunicação com suspeitos para obtenção de provas, permitindo-se, no limite, a participação em atividade criminosa[420]. O primeiro ponto de destaque é que as legislações não definem a o conteúdo da invasão digital, isto é, um meio de obtenção de provas positivado sem precisar dos procedimentos para a realização da medida. Nesse sentido, entendem Giacomolli e Cani[421]:

---

[415] O livre desenvolvimento da personalidade é expresso na garantia de que haja espaços da vida privada em que os indivíduos se comportem espontaneamente. No ambiente digital, isso implica que a coleta, o tratamento e a transmissão de dados pessoais ocorram em respeito à autodeterminação informacional dos particulares. No Brasil, esse direito foi alçado aos status de garantia fundamental, com a inclusão do LXXIX do 5º da Constituição Federal, e se soma ao âmbito geral de proteção da privacidade e das inviolabilidades acima descritas.

[416] A autodeterminação informacional é o controle sobre a informação pessoal, que é cedido com base na finalidade pré-definida de sua coleta. No direito privado, exerce-se o controle por vontade contratual das partes, enquanto no âmbito do direito público ele é estabelecido por força de lei. Naturalmente, não é possível falar em consentimento em ser alvo de medidas cautelares e/ou investigações criminais, exatamente por isso que, para os casos penais, o controle deve ser exercido pela norma autorizativa sobre a matéria, a exemplo da quebra do sigilo telemático.

[417] BRASIL, 2013, arts. 10-A a 10-D.

[418] BRASIL. Lei nº 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. *Diário Oficial da União*, Brasília, DF, 16 jul. 1990. Arts. 190-A a 190F.

[419] É a leitura que Geraldo Prado faz dos artigos mencionados anteriormente citado. (PRADO, 2024, p. 258)

[420] RIBEIRO, Gustavo Alves Magalhães; CORDEIRO, Pedro Ivo Rodrigues Velloso; FUMACH, Débora Moretti. O malware como meio de obtenção de prova e a sua implementação no ordenamento jurídico brasileiro. Revista Brasileira de Direito Processual Penal, Porto Alegre, v. 8, n. 3, set./dez. 2022. p. 1484.

[421] GIACOMOLLI; CANI, 2023, p. 5.

> [...] Não há regramento específico do meio à execução da infiltração de agentes. Daí porque no Brasil, assim como vem ocorrendo na Europa, para realizar a infiltração de agente digital, as polícias recorrem frequentemente ao uso de malware: programa de computador que se instala no aparelho após a quebra dos protocolos de segurança e permite a devassa do aparelho, inclusive a adulteração dos dados armazenados.

Como alertado pelos autores, a ausência de procedimento, que vem se tornando uma regra nas alterações processuais penais, cria uma zona cinzenta sobre a autorização para o emprego de *malwares*[422]*,* tais como os *softwares* espiões[423], para realizar a infiltração. É uma interpretação, no mínimo, desconectada da estrita legalidade, exigível principiologicamente para o direito público de forma geral. Ademais, retomando-se o que foi abordado no Capítulo 1, não há autorização legal que permita nem mesmo a compra desse tipo de tecnologia.

Esse debate é o maior ponto de interesse, já que "invasão" poderia significar a utilização de técnicas especiais – ocultas, remotas e simultâneas – para adquirir elementos informativos, como já autorizado em algumas experiências internacionais[424]. Tal confusão entre infiltração e utilização de *malwares* não é restrita ao direito brasileiro; em Portugal, há disputa sobre o artigo 19º, ponto n. 2, da Lei do Cibercrime, que positivou as ações encobertas, debatendo-se a permissão par ao uso desse tipo de aplicativo[425]. Na linha de argumentação de que é possível, a interação humana é equiparada ao uso de *softwares* com propósitos iguais.

A defesa da autorização de invasão por *software* espião se justifica pelos resultados práticos

---

[422] Segundo Alves, A pedra de toque do malware é que ele é instalado sub-repticiamente, através de *hacking*, no sistema informático do sujeito alvo (isto é, sem o seu conhecimento) através de diversos meios: (i) infecção via suporte físico removível; (ii) infecção via browser; e (iii) infecção via download voluntário. Existem diversos tipos de malware, desde os célebres cavalos de Tróia ("Trojan horses") até às logic bombs, spyware, rootkits, worms, etc. (ALVES, Daniel Bento. Uso de malware em investigação criminal. Actualidad Jurídica Uría Menéndez, Lisboa, n. 47, 2017, p. 20.)

[423] Os chamados softwares espiões (s*pywares*) são aplicativos que invadem dispositivos informáticos e abrem acesso total ao aparelho infiltrado, podendo o invasor manipular câmeras, microfones, informações, aplicativos etc. O mais conhecido mundialmente é o israelense Pegasus, que permite uma invasão "zero clique" – o usuário nem precisa "morder a isca" para que o dispositivo seja explorado pelo agente/invasor. O diferencial do aplicativo já levou ao menos 14 países da União Europeia a adquiri-lo, segundo recente relatório do Conselho da Europa.

[424] A pesquisa identificou a autorização específica para uso de *spywares* na Itália, na Espanha (Lei orgânica 13/2015), na França (Lei 2011-267).

[425] David Silva Ramalho defende que o n. 2, do artigo 19º autoriza o uso de *malware* (RAMALHO, David Silva. Métodos ocultos de investigação criminal em ambiente digital. Almedina, 2017, p. 344 e 345). No sentido oposto, o catedrático Costa Andrade se opõe a esse entendimento, na medida em que exige que todo meio oculto de investigação criminal são instroponivelmente previstos em lei. (ANDRADE, Manuel da Costa. "Métodos ocultos de investigação (Plädoyer para uma teoria geral)", *in Que futuro para o Direito Processual Penal?: simpósio em Homenagem a Jorge de Figueiredo Dias*, Coimbra Editora, 2009, p. 540).

que o uso possibilita, como se vê no caso francês com cooperação da Holanda[426], em que conversas do aplicativo de mensagens criptografadas, *EncroChat*, foram *hackeadas*, infectando 300 mil telefones em mais de 120 países[427]. O impacto dessas ações é significativo, e a defesa de sua utilização é consequencialista, as agências de persecução poderiam prevenir diversos riscos e adquirir dados protegidos pela opacidade. Contudo, a argumentação de que eles estariam abrangidos pela infiltração digital não é correta, de acordo com a legislação brasileira.

No plano normativo, não há autorização para o uso de tecnologia invasiva, o que é exigência para métodos ocultos invasivos que atinjam a autodeterminação informacional, em alinhamento com a defesa realizada anteriormente na tese. Na mesma linha, Ribeiro, Cordeiro e Fumach[428] afirmam que o princípio da legalidade processual não permite a extensão da infiltração digital:

> [...] a utilização do malware não poderá ser realizada a partir do regime jurídico previsto para o agente infiltrado virtual. Isso porque aquela norma não trata especificamente da implantação de um agente malicioso no dispositivo informático de um terceiro com o objetivo de acessar os dados e informações que estão nele armazenados ou sendo a partir dele produzidos. Diante disso, e em sendo o malware uma técnica investigativa bastante invasiva, não é possível a realização de uma interpretação ampla do conceito de infiltração sem que isso implique uma violação ao princípio da legalidade processual.

No plano dogmático, utilizando-se as categorias propostas por Geraldo Prado, a prova digital pode ser abordada no seu caráter estático (o microcomputador apreendido), também pela necessidade de medidas com propósitos de *online search* – que é o caso da infiltração – e por meio da vigilância em tempo real – *online surveillance*[429]. Com base nessa diferenciação, o uso de

---

[426] De acordo com a Europol, a EncroChat comercializava celulares modificados para garantir segurança, com a desativação de tecnologias que possibilitassem o rastreamento ou a identificação do usuário, bem como a implementação de uma senha de limpeza criptografada para situações de urgência. Em razão dessas características, os dispositivos foram amplamente utilizados por grupos de criminalidade organizada, de modo que a invasão do sistema resultou em mais de 6.500 prisões. Disponível em https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe, acessado em 23.03.2026.

[427] ZARAGOZA TEJADA, Javier Ignacio. La prueba ilícita y prueba tecnológica. Reflexiones a raíz del caso Encrochat. In: ORTIZ PRADILLO, Juan Carlos; ABELLÁN ALBERTOS, Antonio (Dir.). El derecho de defensa en la justicia penal digital. Valencia: Tirant lo Blanch, 2024, p. 309.

[428] RIBEIRO; CORDEIRO; FUMACH, 2022, p. 1485.

[429] O texto adaptou os conceitos para o tema debatido. Por isso, segue a forma como o autor definiu as categorias: "em seu aspecto estático (off line) a prova digital já demanda cuidados extremos para que seja processualmente válida, a prova digital online reclama um reforço de garantias. A execução quer das medidas determinadas com exclusivo propósito de busca (on line search) ou as que compreendem a vigilância à distância (on line surveillance) são passíveis de manipulação e, se não adequadamente fiscalizadas, coletadas e preservadas, tornam ineficaz qualquer esforço de submissão futura ao contraditório, inviabilizando-se como elemento probatório. (PRADO, 2024, p. 251)

malware é uma técnica de *online surveillance*, e não um método de *online search,* o que é mal interpretado por quem defende que a infiltração digital autoriza a utilização de *malware*. Portanto, busca e vigilância não são categorias intercambiáveis, nem abrangidas entre si, de modo a não poderem ser utilizadas para persecução com base no mesmo dispositivo legal autorizador.

Ainda que o uso de *malware* fosse positivado legalmente para a persecução penal, ressalvada a utilização para segurança nacional, essa previsão seria inconstitucional, na medida em que os investigares rompem as barreiras de segurança e agem como se fossem o próprio usuário, o que impede a verificação da cadeia de custódia dos elementos de informação produzidos. Esse argumento é foi amplamente difundido por Prado na dogmática brasileira e parece o mais adequado para lidar com a problemática abordada[430]. Em suma, a infiltração digital não pode ser realizada automatizadamente por *softwares* no Brasil.

Até o momento, o tópico a abordou o conceito de infiltração digital negativamente, isto é, descrevendo o porquê de a invasão por *software* não estar abrangida por ela, mas dedicou pouca atenção ao que foi positivado no ECA, com as alterações promovidas pela Lei n. 13.441/2017, e na Lei das Organizações Criminosas, com as alterações realizadas pela Lei n. 13.964/2019. Ambos os textos são bastante semelhantes e, como dito anteriormente, carecem da descrição de procedimentos para a realização da medida.

Como não há um procedimento a ser analisado, o que limita a crítica à própria inexistência de atos procedimentais e, considerando a semelhança entre as previsões legais, decidiu-se apresentá-las na tabela comparativa a seguir:

Tabela 5 - Infiltração digital no ECA e na Lei das Organizações Criminosas

Critério de Análise	**Estatuto da Criança e do Adolescente**	**Lei das Organizações Criminosas**
Bens jurídicos tutelados	Aplicável a rol taxativo de crimes cuja proteção é a dignidade sexual de crianças, adolescentes e	Aplicável aos crimes definidos e nas hipóteses de aplicação da própria lei, ou por crime que o Brasil se obrigou

[430] Nas palavras do autor, “embora não seja objeto do artigo, faço questão de registrar que em minha opinião o uso de software espião para vigilância – e não para a coleta de arquivos digitais – é inconstitucional a qualquer título, na medida em que, potencializado pelos recursos da inteligência artificial, produz aquele tipo de concentração de poder informacional verificado pela Teoria do Mosaico. (PRADO, 2024, p. 257)

	vulneráveis, à exceção do crime de invasão de dispositivo informático[431].	a reprimir por tratado, com efeito transnacional[432] .
Reserva de jurisdição	Obrigatória. O limite dos atos é definido por decisão judicial (Art. 190-A, I, determina que a decisão "estabelecerá os limites da infiltração").	Obrigatória. Não contém previsão expressa de que a decisão estabelecerá os limites (o que condiz com o "pacote anticrime").
Subsidiariedade	Não será autorizada se houver possibilidade de obtenção da prova por meio menos gravoso (replica previsão da Lei de Interceptação Telefônica).	Não será autorizada se houver possibilidade de obtenção da prova por meio menos gravoso (replica previsão da Lei de Interceptação Telefônica) [433].
Prazo inicial	90 dias[434].	6 meses[435].
Prazo máximo	Renovável até o limite total de 720 dias.	Sem possibilidade de renovação, mas o prazo máximo é de 720 dias (a redação sugere um único período ou um limite total).
Legitimidade para postulação	Ministério Público ou Autoridade Policial (durante a investigação).	Ministério Público ou Autoridade Policial (durante a investigação).
Parecer do Ministério Público	O juízo deve determinar a manifestação do MP na representação policial (opinião lida como não vinculante, conforme tendência jurisprudencial do STJ e	O juízo deve determinar a manifestação do MP na representação policial (opinião lida como não vinculante, conforme tendência jurisprudencial do STJ e STF).

[431] BRASIL. Decreto-Lei nº 2.848/1940, arts. 154-A, 217, 218 a 218-B; e BRASIL. Lei nº 8.069/1990, arts. 240 a 241-D.
[432] BRASIL, Lei nº 12.850/2013, arts. 1º, § 1º e § 2º.
[433] BRASIL, Lei nº 8.069/1990, art. 190-A, III, § 3; BRASIL, Lei nº 12.850/2013, art. 10-A, § 3º.
[434] BRASIL, Lei nº 8.069/1990, art. 190-A, III.
[435] BRASIL, Lei nº 12.850/2013, art. 10-A, § 4º A.

	STF).	
Execução da medida	Agentes de polícia, membros do Ministério Público não estão autorizados a realizar o ato.	Agentes de polícia, membros do Ministério Público não estão autorizados a realizar o ato.
Controle de legalidade	O MP e o juízo que autorizou poderão solicitar relatórios, e a medida poderá ser revogada a qualquer tempo[436].	O MP e o juízo que autorizou poderão solicitar relatórios, e a medida poderá ser revogada a qualquer tempo.
Conceito de dados	Ambas as legislações definem o que é dado cadastral e de tráfego. Os incisos servem, no máximo, para orientar a leitura jurídica do relatório.	Ambas as legislações definem o que é dado cadastral e de tráfego. Os incisos servem, no máximo, para orientar a leitura jurídica do relatório.

Fonte: elaborada pelo autor

As hipóteses de infiltração digital são previstas sem aprofundamentos nos dois dispositivos legais. Em ambos, há o condicionamento à reserva de jurisdição, subsidiariedade com outros meios de obtenção de prova, prazo máximo e a legitimidade para requerer. A postulação desse meio de obtenção de prova pode ser realizada tanto pelo Ministério Público quanto pela autoridade policial durante a investigação. No caso de iniciativa por representação policial, o juízo deve determinar a manifestação do Ministério Público; esta opinião deveria ser lida vinculativamente, mas essa não é a tendência jurisprudencial do STJ[437] e do STF[438]. Além disso, as legislações autorizam a infiltração por "agentes de polícia", de modo que os membros do Ministério Público não estão autorizados a realizar esse ato, que é exclusivo da investigação policial.

O ECA conta com previsão do limite da medida, ainda que seja dado exclusivamente

[436] BRASIL, Lei nº 8.069/1990, art. 190-A, § 2º, I e II; BRASIL, Lei nº 12.850/2013, art. 10-A, § 1º, I e II.
[437] No Recurso Especial n. REsp 2.022.413, a Sexta Turma afirmou que a introdução do art. 3-A, do CPP, não revogou tacitamente o art. 385 do CPP e que o dispositivo está em acordo com o sistema acusatório. (BRASIL. Superior Tribunal de Justiça (STJ). Sexta Turma. Recurso Especial nº 2.022.413/PA. Relator: Min. Sebastião Reis JUNIOR. Relator para acórdão: Min. Rogerio Schietti Cruz. Julgado em 14 fev. 2023. *Diário da Justiça Eletrônico*, Brasília, DF, 07 mar. 2023.)
[438] *Mutatis mutandis*, o STF entende que o art. 385 do CPP é constitucional, logo se pode condenar mediante pedido de absolvição. Na mesma linha, o juízo está autorizado a deferir a representação policial com parecer contrário.

expressa pela decisão judicial "estabelecerá os limites da infiltração para obtenção de prova"[439], o que reforça o argumento anterior da ausência de procedimentos. Por outro lado, a Lei das Organizações Criminosas não contém previsão semelhante.

Como se pode ver, há uma tendência legislativa, e doutrinária, em compreender que os limites mais restritivos aos meios de obtenção de provas ocultos cautelares sejam a reserva de jurisdição e a limitação temporal, o que faz sentido apenas ao se trabalhar com elementos de informação com potencial epistêmico pré-definido e de caráter estático. Contudo, para cada intervenção informacional, deve se atentar a um modelo ideal para se ter acesso, como o que vem sendo proposto nos tópicos próprios desta tese, a exemplo da exigência de que a decisão permita o uso de tecnologia de extração nos casos de apreensão de dispositivos eletrônicos.

Por fim, Greco tem razão ao afirmar que as intervenções informacionais no processo penal e a reserva de lei prevista na Constituição são grandes desconhecidas do direito brasileiro[440]. O acesso policial – não escrutinada devidamente pelo Judiciário – configura-se como uma licença para que se acesse a vida privada de forma indefinida, fenômeno que poderia ser lido como um processo penal não abordado como limitador do poder punitivo.

---

[439] BRASIL, Lei nº 8.069/1990, art. 190-A.

[440] GRECO, Luís. Organização e introdução. 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. Tradução Alaor Leite, Eduardo Viana e Luís Greco. 1. ed. São Paulo: Marcial Pons, 2018, p. 26.

6. A DESTERRITORIALIZAÇÃO DA PROVA DIGITAL: A REQUISIÇÃO UNILATERAL COMO RESPOSTA DOS ESTADOS UNIDOS E DA UNIÃO EUROPEIA

O elemento estruturante da requisição de dados consiste no fato de que a revolução informacional se deu em ambiente internacional, caracterizado pela concentração da oferta de serviços de comunicação e armazenamento por empresas denominadas *Big Techs*. Vale recordar que o Capítulo 4 também abordou o ordenamento brasileiro sobre a requisição de dados, explicando inicialmente que nem mesmo um nome técnico para esse tipo de ato de investigação existe na dogmática processual penal brasileira. Contudo, um elemento essencial não foi debatido: o efeito da ordem de exibição para uma empresa com sede ou armazenamento de dados no exterior.

O debate também se mostra pertinente quando se pretende acessar conversas digitais armazenadas por provedores de serviços de comunicação, bem como conteúdos guardados em nuvem ou por provedores de aplicações de internet. Atualmente, como não existe permissivo legal para a requisição de dados de conteúdo por esse tipo de empresa, situação que se repete em diversos países, passou-se a adotar o conceito de "cooperação voluntária": a entrega de informações pelas empresas quando solicitadas por agências de persecução. Contudo, por razões conceituais, tal prática não é cooperação, tampouco pode ser considerada voluntária.

O ponto mais relevante é que, ao realizarem essas entregas, as empresas acabam desempenhando funções públicas, como analisar a necessidade e a proporcionalidade dos meios de obtenção de provas requisitadas por autoridades públicas, além de avaliar o impacto sobre direitos fundamentais[441]. Tal atribuição não cabe juridicamente a empresas privadas. Além disso, não se trata de um método excepcional: os dados indicam que sua ocorrência é relativamente frequente[442].

Outro aspecto importante é a ausência de regras e, naturalmente, de limites definidos, o que levanta questões relacionadas a proteção jurídica a privilégios, imunidades e sigilo de dados vinculados à abertura de informações. Esse ponto se torna ainda mais evidente ao compararmos o modelo adotado na Europa, que optou por um sistema de territorialização dos dados.

Nos últimos anos, essa problemática foi visualizada em diversas situações. O primeiro

---

[441] TOSZA, Stanislaw. The e-evidence package is adopted end of a saga or beginning of a new one? European Data Protection Law Review. v. 9, n. 2, 2023, p. 166.
[442] EILBERG, 2024, p. 42-43.

exemplo são as liminares de juízes federais que suspendiam o *WhatsApp* em todo o território nacional, uma vez que a empresa proprietária do aplicativo alegava impossibilidade técnica de interceptação ou entrega de dados de conversas para investigações criminais. A relevância do tema é alta, considerando que há modelos de negócios cujas vendas dependem desse tipo de comunicação eletrônica; logo, o impacto econômico e social é relevante.

Atualmente a prática de bloqueio do referido aplicativo está suspensa em razão de liminar deferida na ADPF n. 403, pelo STF, em processo de origem da 2ª Vara Criminal de Duque de Caxias, não podendo ser utilizada como método coercitivo para a entrega de dados pela *Meta*[443]. O caso de fundo é o que mais interessa: há uma ordem de entrega de dados que a empresa alega impossibilidade técnica de cumprir, tendo em vista a utilização de criptografia. O fato é que, mesmo não havendo meio típico para requisitar a abertura de dados de conteúdo, a prática é recorrente, e a decisão foi suspensa para preservar o direito de comunicação da coletividade, e não em razão do uso de método coercitivo para cumprimento decisão atípica da perspectiva probatória.

A impossibilidade técnica é um dos argumentos para o não cumprimento da decisão, mas também poderia ser relacionada à jurisdição do local de armazenamento ou da sede das empresas. Esse segundo argumento foi enfrentado pela ADC n. 51 no STF[444]. A ação utilizada e a pretensão jurídica dela depreendida possuem um fundamento heterodoxo, a Federação das Associações das Empresas Brasileiras de Tecnologia da Informação (ASSESPRO) requereu a declaração da constitucionalidade do acordo de cooperação jurídica em matéria penal entre Brasil e Estados Unidos[445], cuja conclusão indireta seria a impossibilidade de utilizar outros meios, especificamente a atípica requisição de dados de conteúdo armazenados no exterior.

Em primeiro lugar, a ação jamais alcançaria o objetivo intentado, uma vez que os MLATs são uma das formas de cooperação em matéria penal, e não a única. A evidência desse argumento é que o Brasil tem acordos específicos para compartilhar dados na cooperação entre as polícias

---

[443] Acesso ao andamento processual e decisões realizado em 12/11/2025 em https://portal.stf.jus.br/processos/detalhe.asp?incidente=475500.
[444] BRASIL. Supremo Tribunal Federal. ADC 51, 2017.
[445] BRASIL. Decreto nº 3.810, de 2 de maio de 2001. Promulga o Acordo de Assistência Judiciária em Matéria Penal entre o Governo da República Federativa do Brasil e o Governo dos Estados Unidos da América, celebrado em Brasília, em 14 de outubro de 1997. *Diário Oficial da União*, Brasília, DF, 3 maio 2001.

judiciárias, o COAF, a Receita Federal, entre outros[446]. Por esta razão, a pretensão jurídica de declarar constitucionalidade do auxílio mútuo não teria o efeito lógico de interditar outras formas de cooperação previstas no ordenamento brasileiro. Nada impede, inclusive, que o Brasil adira aos acordos executivos do *Cloud Act*[447] em concomitância ao auxílio direto já previsto.

A resposta do julgamento foi a declaração da constitucionalidade do MLAT com os Estados Unidos, ressalvando a possibilidade de requisição direta de dados armazenados no exterior, com utilização do Marco Civil da Internet, independentemente dos outros meios de cooperação[448]. Dessa forma, a ementa da decisão tem dois pontos que interessam à tese:

> [...] 3. As hipóteses de requisição direta previstas no art. 11 do Marco Civil da Internet e no art. 18 da Convenção de Budapeste reafirmam os princípios da soberania e da independência nacional, concretizando o dever do Estado de proteger os direitos fundamentais e a segurança pública dos cidadãos brasileiros ou residentes no país. (...) 5. Dispositivos que convivem com a possibilidade de solicitação direta de dados, registros e comunicações eletrônicas nas hipóteses do art. 11 do Marco Civil da Internet e do art. 18 da Convenção de Budapeste.

O artigo 11 do Marco Civil da Internet não cria a hipótese de requisição de dados, em linha com o que foi argumentado anteriormente. Dora Eilberg explica precisamente a utilização: "[o STF acatou o] fenômeno da "territorialização" do ciberespaço e que, pelo fato de as empresas terem representação no Brasil, as normas de requisição direta de dados e comunicações eletrônicas às empresas do MCI seriam prevalentes, sem a realização de MLAT"[449]. Assim, a partir da obrigação do cumprimento da legislação brasileira, o STF depreendeu a possibilidade de requisição direta de dados de conteúdo, independentemente do local de armazenamento do dado.

A pergunta de fundo desse entendimento é se requisitar dados dependeria de atos próprios

---

[446] Vale mencionar que a cooperação policial encontra previsão no art. 48 da Convenção das Nações Unidas contra a Corrupção e no art. 27 da Convenção das Nações Unidas contra o Crime Organizado Transnacional, de modo que as polícias se estruturam em redes para o compartilhamento de informações relevantes à manutenção da ordem pública. Ademais, o COAF integra o Grupo Egmont, voltado precisamente à cooperação entre unidades de inteligência financeira em âmbito internacional. Tais exemplos são mobilizados para afastar a compreensão de que os MLATs esgotam as formas de transferência de dados, excluindo mecanismos de cooperação tributária ou administrativa. Embora a adesão a organismos intergovernamentais com previsão de intercâmbio de dados sem base legal específica mereça crítica, é fato que esses mecanismos operam, na prática, em paralelo à assistência jurídica mútua.

[447] ESTADOS UNIDOS. Clarifying Lawful Overseas Use of Data Act (CLOUD Act). Pub. L. No. 115-141, div. V, 132 Stat. 1213 (2018).

[448] BRASIL. Supremo Tribunal Federal (STF). Tribunal Pleno. Ação Declaratória de Constitucionalidade nº 51/DF. Relator: Min. Gilmar Mendes. Julgado em 21 jun. 2023. *Diário da Justiça Eletrônico*, Brasília, DF, 28 abr. 2023. Ementa.

[449] EILBERG, 2024, p. 45.

de cooperação jurídica internacional, na medida em que o local de armazenamento dos dados pode ser utilizado como critério para estabelecimento de jurisdição. A resposta a esse tema tão atual não foi dada academicamente, mas a realidade normativa se impôs, sendo comum que países utilizem o processo penal para ter acesso a dados sob jurisdição estrangeira[450]. Com efeito, o que marca a diferença da situação brasileira é que há lei para o fazer em relação aos dados de conteúdo, ainda que defina sua competência em razão do local da coleta, assim como vários países[451].

A superação dos acordos de auxílio direto é discutida amplamente[452], na medida em que se defende que a volatilidade das provas digitais é incompatível com o procedimento de cooperação que, como regra, exige decisão em pelo menos dois países, trânsito por autoridades administrativas e outras exigências práticas que têm um prazo para se efetivar. Esse argumento esteve presente tanto na União Europeia[453] quanto nos Estados Unidos, especialmente nos documentos que antecederam as inovações legislativas realizadas sobre o tema.

Nesse sentido, o efeito jurídico da utilização pela autorização judicial para requisitar dados de conteúdo é semelhante ao que ocorre atualmente nos Estados Unidos e vai passar a acontecer na União Europeia a partir de agosto de 2026. A diferença, no entanto, está na ausência de fundamento legal para requisitar dados de conteúdo, que, como vem sendo defendido, não pode ser relativizada. Assim, para o aprofundamento do debate, as práticas americana e do bloco europeu serão analisadas neste capítulo, para que discussão sobre a requisição de dados de conteúdo no Brasil seja realizada com base em toda a dinâmica criada pelas provas digitais, o que inclui a

---

[450] VERGNOLLE, Suzanne. Understanding the French criminal justice system as a tool for reforming international legal cooperation and cross-border data requests. In: BRÄUTIGAM, Tobias; MIETTINEN, Samuli (ed.). *Data Protection, Privacy and European Regulation in the Digital Age*. Helsinki: Unigrafia, 2016, p. 213.

[451] De acordo com o Departamento de Justiça dos Estados Unidos, os seguintes países utilizam o local da coleta para determinar competência jurisdicional: Austrália, Bélgica, Canadá, Colômbia, Dinamarca, França, Irlanda, México, Montenegro, Noruega, Peru, Portugal, Sérvia, Espanha, Reino Unido. (ESTADOS UNIDOS. Department of Justice. Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act. White Paper. Abr. 2019.)

[452] VERGNOLLE, 2016, p. 219-220.

[453] No relatório de impacto da Comissão Europeia sobre provas digitais afirma textualmente a lentidão dos acordos bilaterais de cooperação: "*judicial cooperation is often too slow for timely access to data and can entail a disproportionate expense of resources*" (UNIÃO EUROPEIA. Comissão Europeia. Commission Staff Working Document – Impact Assessment: Accompanying the document Proposal for a Regulation [...] and Proposal for a Directive [...]. SWD(2018) 118 final. Bruxelas, 17 abr. 2018.). Em sentido semelhante, o Departamento de Justiça dos Estados Unidos publicou que: *"The number of MLAT requests has increased dramatically in recent years, in light of the massive volume of electronic communications that occur daily over the Internet and the enormous amount of electronic data held by companies located throughout the world. While the MLAT process remains a critical evidence-gathering mechanism, the system has faced significant challenges keeping up with the increasing demands for electronic evidence in criminal investigations worldwide*" (ESTADOS UNIDOS. Promoting Public Safety, 2019, p. 3).

dimensão internacional das ordens direcionadas a *Big Techs*.

6.1. Cloud Act: a solução americana para dados armazenados em outros países

A computação em nuvem é um mercado de grande concentração das intituladas *Big Techs,* que funcionam como provedores de internet e gerenciam plataformas de comunicação, cujos dados podem ser relevantes para investigações penais. As quatro maiores empresas no setor representam mais de 90% do mercado e têm suas sedes corporativas nos Estados Unidos[454]. Esse cenário consolidou a posição proeminente dessas empresas na legislação americana sobre provas digitais, como as principais destinatárias de direitos e deveres pelo *Cloud Act.*

Na arquitetura legal americana, essa lei está inserida na legislação de proteção à privacidade das comunicações eletrônicas (ECPA)[455], que se divide em três partes: título I (Lei de Interceptação Telefônica), título II (Lei das Comunicações Armazenadas – SCA) e o título III (Lei sobre o registro de números discados e recebidos). O *Cloud Act* modifica especificamente o título II em dois aspectos principais. A primeira alteração foi a extensão dos efeitos dos mandados para que fossem cumpridos por empresas sob jurisdição americana em "possession, custody, or control" of the data sought "regardless" of whether the data is stored inside or outside of the U.S"[456].

O segundo aspecto está conectado à criação de uma moldura legal para a realização de acordos bilaterais com outros países para o acesso a dados de maneira facilitada. Além disso, inaugura um novo sistema de cooperação, isto é, entre Estados e empresas de tecnologia. Nesse contexto, os países que preencherem os requisitos da legislação americana[457] poderão firmar acordo executivo para ter acesso a provas digitais que estejam sob jurisdição de empresas americanas ou lá sediadas, passando a se enquadrar como governo estrangeiro qualificado, por oposição, os demais são tratados pela legislação como governo estrangeiro não qualificado[458].

O retrospecto da discussão dessa alteração legislativa revela várias características do modelo adotado, em que saiu vencedora a não territorialidade dos dados para jurisdição em nuvem.

---

[454] UNIÃO EUROPEIA, SWD (2018) 118 final, 2018, p. 14.
[455] ESTADOS UNIDOS. *Electronic Communications Privacy Act (ECPA)*. U.S. Code, § 2510 et seq., 1986.
[456] BERENGAUT, Alexander A.; LENSDORF, Lars. The CLOUD Act at Home and Abroad. Computer Law Review International (CRi), v. 20, n. 4, p. 111-117, 2019.
[457] BERENGAUT; LENSDORF, 2019, p. 112.
[458] BERENGAUT; LENSDORF, 2019, p. 114.

O *Cloud Act* foi promulgado na pendência do caso *United States v. Microsoft Corp*[459] perante a Suprema Corte dos Estados Unidos[460], após os debates orais das partes e *amici curiae*, em que se ouviram argumentos sobre a necessidade de manifestação legislativa do Congresso[461]. A matéria de fundo foi a resistência da Microsoft no cumprimento de mandado para entregar dados ao FBI que estavam armazenados em outra jurisdição, afirmando que dever-se-ia utilizar a assistência direta.

O debate legal recaiu sobre a validade do mandado de interceptação de dados baseado na Lei de Comunicações Armazenadas[462] e sobre a natureza jurídica da ordem, se mandado ou intimação[463], na medida em que parte dos dados estava armazenada em outro país. A empresa sustentou que o instrumento utilizado não possuía efeitos extraterritoriais, posição à qual não se opunha o DJO (Departamento de Justiça). Havia concordância a respeito do fato de a lei não prever alcance transnacional[464]. Contudo, na visão do FBI, o acesso aos dados seria possível a partir dos Estados Unidos, não importando o local de armazenamento pela empresa sob jurisdição[465].

O mandado de um juiz do Tribunal Distrital de Nova York foi questionado pela Microsoft, que apresentou um pedido para revogá-lo. O colegiado indeferiu o pedido da empresa e a considerou em desacato ao tribunal por ter recusado a executar a ordem. Com efeito, o argumento central ia ao encontro da visão institucional do DJO, isto é, de que o mandado tinha apenas ordens sujeitas a territorialidade americana[466]. A empresa manteve o argumento e apelou ao Segundo Circuito, que julgou em seu favor, anulando o mandado. Diante das inúmeras interpretações da legislação e da relevância, a Suprema Corte aceitou o caso para julgamento em 2017[467].

Pode-se dizer que as decisões no Tribunal Distrital se baseavam na teoria da não territorialidade dos dados, privilegiando-se a jurisdição pessoal sobre a empresa incorporada ou

---

[459] BILGIC, Secil. Something old, something new, and something moot: the privacy crisis under the CLOUD Act. Harvard Journal of Law & Technology, v. 32, n. 1, 2018, p. 323.
[460] ESTADOS UNIDOS. Suprema Corte. *United States, Petitioner v. Microsoft Corporation*. No. 17-2. U.S. Reports, Washington, D.C., v. 584, 2018
[461] DASKAL, Jennifer. Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0. Stanford Law Review Online, v. 71, p. 9-16, May 2018.
[462] ESTADOS UNIDOS. Stored Communications Act. U.S. Code, Título 18, § 2703. 1986.
[463] The legal discussion of whether an order under the SCA a warrant, subpoena or hybrid is falls outside of the scope of this research. However, it has been a relevant subject of the discussion in the case.
[464] ABRAHA, Halefom H. Regulating law enforcement access to electronic evidence across borders: the United States approach. Information & Communications Technology Law, v. 29, n. 3, 2020, p. 330.
[465] ABRAHA, 2020, p. 330
[466] BILGIC, 2018, p. 331.
[467] BILGIC, 2018, p. 330.

com atividade econômica relevante no local da execução da ordem[468]. Esse argumento não foi aceito pela corte federal após a apelação, e reafirmou-se que o acesso deveria ser franqueado com a utilização de meios judiciais de cooperação, que era o argumento da Microsoft. A opinião da Suprema Corte americana sobre o ponto não será conhecida porque o caso perdeu o objeto[469], mas o receio com o risco de evasão de dados ficou nítido nas audiências[470].

A *Cloud Act* alinhou-se à posição jurídica de que os dados são não territoriais, a qual vinha sendo sustentada judicialmente pelo DOJ em diversos casos, a exemplo de mandados para cumprimento pelo Google[471], e que foi replicada na justificativa oficial da lei[472]. Esse ponto de vista tem respaldo teórico na autora Jennifer Daskal, que defende que a mobilidade, a fungibilidade e as características dos dados fazem com que a discussão sobre territorialidade na nuvem seja anacrônica e potencialmente deletéria para as agências de persecução.

Essa excepcionalidade justificou a alteração sistêmica para a cooperação direta, em oposição aos meios tradicionais de cooperação, que seriam incompatíveis com a era digital, reforçando a impossibilidade de tratar os pedidos de países estrangeiros em tempo adequado pelo alto volume e pelas características dos dados. Neste contexto, os MLATs são tratados como um mecanismo "*a critical evidence-gathering mechanism",* apesar de inaptos a lidar com a velocidade da era digital[473]. Contudo, a legislação mantém sua utilização para os casos em que a cooperação direta for inadequada, a exemplo daqueles que envolvam cidadãos americanos.

A reforma da Lei de Comunicações Armazenadas contou com apoio público das *Big Techs* americanas, que manifestaram apoio às alterações em ambas as fases de votação no Congresso[474]. Na visão delas, o novo marco legal "w*ould require baseline privacy, human rights and rule of law standards in order for a country to enter into an agreement*", além de instrumentos para o questionamento das medidas, especificamente, "*provides mechanisms to notify foreign governments when a legal request implicates their residents, and to initiate a direct legal challenge*

---

[468] DASKAL, Jennifer. The Un-Territoriality of Data. The Yale Law Journal , v. 125, 2015, p. 328.
[469] ABRAHA, 2020, p. 331.
[470] BILGIC, 2018, p. 332.
[471] ABRAHA, 2020, p. 331.
[472] ESTADOS UNIDOS. Promoting Public Safety..., 2019.
[473] ESTADOS UNIDOS. Promoting Public Safety..., 2019, p. 3.
[474] Letter of Support to Senate. Signed by Apple, Facebook, Google, Microsoft and Oath on 06/02/2018. Disponível em: https://cyberlaw.stanford.edu/content/files/datalaw/wp-content/uploads/sites/149/2018/02/tech-companies-letter-of-support-for-senate-cloud-act-020618.pdf. Acesso em: 16 nov. 2025.

when necessary"[475]. É importante notar que a lei vedou qualquer ação civil ou criminal contra o provedor que cumpra ordem judicial para a abertura de dados de boa-fé[476].

Esse breve resumo introduz o ambiente jurídico-político que antecedeu a promulgação do *Cloud Act* e sua vinculação teórica. Neste ponto, passamos a explicar em duas partes, destacando o objeto, os conceitos centrais, os âmbitos de aplicação e as inovações trazidas ao contexto da cooperação jurídica da prova digital. A primeira parte trata das alterações na SCA que dizem respeito à atuação das autoridades americanas no exercício jurisdicional nos Estados Unidos; a segunda parte descreve o sistema de cooperação dentro do *Cloud Act*, ao qual países estrangeiros poderão aderir para demandar provas digitais diretamente às empresas.

6.1.1 Efeito interno do Cloud Act

O *Cloud Act* estabeleceu a obrigação de que empresas que detenham "custody, possession or control" sobre dados de interesse para investigação possam ser demandadas diretamente se estiverem sob jurisdição americana, mas a lei não define o conteúdo jurídico desses termos[477]. No entanto, essa expressão está presente tanto nas regras de processo civil quanto nas de processo penal nos Estados Unidos[478], que engloba o direito das partes ou dos réus de exigir a entrega de documentos e informações jurídicas. Esses dispositivos já fundamentaram o exercício de jurisdição em contextos em que, *prima facie,* atos de cooperação seriam necessários, mas foram ignorados[479].

Ainda que alguns autores considerem que há limites jurisprudenciais bem estabelecidos para a utilização da expressão trazida no Cloud Act e que "the analysis of possession, custody, or control will likely be fact-specific, and based on the totality of the circumstances"[480]. O fato é que a interpretação dos limites dessa obrigação deve ser antecedida pela discussão sobre os critérios para aferição da jurisdição americana, dada a inexistência de critérios de diferenciação entre os prestadores de serviço americanos e estrangeiros, ou seja, quando as empresas estarão

---

[475] Letter of Support (*Ibid.*), p. 1.
[476] ESTADOS UNIDOS. *Clarifying Lawful Overseas Use of Data Act (CLOUD Act)*. Sec. 104, Título 18, U.S. Code. 2018.
[477] HEMMINGS, Justin; SRINIVASAN, Sreenidhi; SWIRE, Peter. Defining the Scope of "Possession, Custody, or Control" for Privacy Issues and the CLOUD Act. Journal of National Security Law & Policy, v. 10, 2020, p. 654.
[478] ESTADOS UNIDOS. Federal Rules of Criminal Procedure: Rule 16 (a)(1) (B, D-F). Washington, D.C.: U.S. Government Publishing Office, 2024.
[479] Bank of Nova Scotia Doctrine. Pode-se citar, como exemplo, o caso Marc Rich.
[480] HEMMINGS; SRINIVASAN; SWIRE, 2020, p. 674.

suficientemente conectadas à legislação americana e ao seu *enforcement*.

Como dito, não há diferenciação na legislação entre os prestadores de serviços americanos e estrangeiros; ao contrário, a lei é aplicável a todas as empresas sob *personal jurisdiction* dos Estados Unidos. Mais uma vez, o conteúdo do exercício da jurisdição deve ser encontrado na legislação nacional, podendo-se esperar que as cortes americanas apliquem o direito nacional de acordo com sua jurisprudência[481]. Na perspectiva nacional, os critérios de atração da jurisdição deverão ser os mesmos aplicados no direito corporativo, que diferencia as empresas sujeitas à jurisdição geral daquelas sujeitas à jurisdição específica para responder a demandas[482].

Portanto, a lei fortalece a tendência global de colocar os provedores de internet no centro da discussão sobre jurisdição na nuvem, o que surge como consequência da adesão teórica à não territorialidade dos dados[483]. Nesse sentido, a relação entre os Estados que possuem jurisdição sobre o fato criminoso e aqueles nos quais os *data centers* estão localizados é substituída pela relação entre Estado e empresa, passando ao servidor a capacidade de resistir à cooperação, não mais interetática, porque não necessariamente envolve dois ou mais países, e não mais vinculada aos critérios de atração de jurisdição tradicionais do direito público internacional.

No lugar da territorialidade do dado, a legislação americana colocou a nacionalidade e a residência das pessoas, que são alvos buscados pelas agências de persecução penal, o que vinha sendo advogado por acadêmicos há bastante tempo, uma vez que "privacy protections should follow the user instead of the data"[484], um exemplo de 2014. Dessa forma, as empresas de tecnologia passam a mediar a cooperação com base em um critério técnico de difícil mensuração, visto que pressupõe que tais informações são de conhecimento do provedor de serviços de comunicação.

Essa escolha endereça a principal preocupação externada pelo DJO e por alguns juízes da Suprema Corte americana, isto é, a de que as empresas nacionais pudessem mudar a localização

---

[481] ESTADOS UNIDOS. Promoting Public Safety..., 2019.
[482] A jurisdição geral existe somente se a empresa tiver sede ou for incorporada nos EUA, recebendo "*any and all claims*", ainda que a matéria seja indiferente à atuação no país, o caso das big techs como Google, Microsoft e Apple. Nas hipóteses que não haja sede ou incorporação, a jurisdição específica é atraída somente se "*the company has sufficient minimum contacts with the United States. Under this doctrine, companies may face only those lawsuits that derive from or are connected with such contacts*". Neste segundo caso, já se considerou contatos mínimos a captação de contratos no valor total de 250 mil dólares nos EUA.
[483]DASKAL, 2015, p. 328.
[484] KERR, Orin S. The Next Generation Communications Privacy Act. University of Pennsylvania Law Review, v. 162, n. 2, 2014, p. 417.

dos dados para se furtarem a cooperar com agências de persecução penal. Por outro lado, a opção de utilização de critérios nacionais para atribuição de jurisdição abriu precedente para que outros países fizessem escolhas semelhantes, tendo em vista que, concomitantemente, o SCA foi reformado para permitir que os provedores entreguem dados de conteúdo por determinação judicial de outros países[485], em interpretação do artigo 18 da Convenção de Budapeste[486].

Um fato distingue a escolha americana de toda a discussão sobre critérios de atribuição de jurisdição penal e, consequentemente, de legitimidade no plano internacional não há vinculação aos tradicionais princípios que se aplicam ao local da conduta, do resultado, do autor ou da vítima[487]. A maximização da escolha pela jurisdição pessoal sobre a empresa, que não é a proprietária do dado, e sim sua controladora, desloca toda essa discussão para a possibilidade de faculdade de obrigar uma pessoa jurídica a produzir provas.

Entretanto, caso a entrega dos dados pelo provedor de comunicação conflite com o direito de um país terceiro, o *Cloud Act* permite dois sistemas para resolução de conflitos legais, que têm como principal critério de diferenciação a definição de se o país é um governo estrangeiro qualificado ou um governo estrangeiro não qualificado [488]. Antes de explicá-los, é importante notar que a realização do acordo por um país estrangeiro também aumenta o grau de proteção e previsibilidade que os tribunais americanos conferirão aos seus ordenamentos em caso de conflito legal.

Caso o país seja qualificado, no prazo de 14 dias, o destinatário da ordem poderá impugná-la pelo risco de violar as leis de um país qualificado, se tiver motivos razoáveis para acreditar que a ordem "would create a material risk that the provider would violate the laws of a qualifying government"[489]. Nessa hipótese, a lei traz os critérios que deverão ser aplicados pelos tribunais

---

[485] ''(j) It shall not be unlawful under this chapter for a provider of electronic communication service to the public or remote computing service to intercept or disclose the contents of a wire or electronic communication in response to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523. (ESTADOS UNIDOS, *Clarifying Lawful Overseas Use of Data Act (CLOUD Act)*, 2018)

[486] Maillart explains the application context to this article "*According to the Explanatory Report of the Convention, the term 'possession or control' refers to 'physical possession of the data concerned in the ordering Party's territory, and situations in which the data to be produced is outside of the person's physical possession but the person can nonetheless freely control production of the data from within the ordering Party's territory*'. (MAILLART, Jean-Baptiste. The limits of subjective territorial jurisdiction in the context of cybercrime. ERA Forum, v. 19, 2019. p. 385.)

[487] BASSIOUNI, M. Cherif. International Extradition: United States Law and Practice. 6. ed. Oxford: Oxford University Press, 2014, p. 497.

[488] HEMMINGS; SRINIVASAN; SWIRE, 2020, p. 653.

[489] ESTADOS UNIDOS. *U.S. Code*. Título 18, § 2703(h)(2)(ii). 2018.

americanos, que, no essencial, ponderam os interesses de ambos os países e a relevância da investigação em seu contexto[490]. A decisão final caberá à autoridade central americana. Ademais, a abertura de dados poderá ser comunicada ao país interessado[491].

Em relação aos países não qualificados, os provedores de serviços de comunicação não podem se opor ao cumprimento de uma ordem com base nas garantias normativas do *Cloud Act*. Entretanto, de acordo com o DJO, em manifestação oficial que explica o funcionamento da legislação, os países devem receber o tratamento tradicional da cortesia internacional consuetudinária [492]. Ressalta-se que, entre as possibilidades de resistência dos dois sistemas, os direitos à privacidade e ao devido processo legal dos investigados e acusados não são critérios de resolução de conflito[493].

Como se pôde ver, a resolução de potenciais conflitos ocorre com base numa lei nacional, reconhecendo-se que a parte legitimada para exercer a resistência não é o titular do dado, mas sim a empresa que o controla. Ademais, o conflito é resolvido em cortes americanas com aplicação do direito local, isto porque o guarda-chuva dos acordos executivos não é uma convenção internacional, mas uma lei americana. Essas características mostram que houve a nacionalização do problema da jurisdição sobre provas digitais na nuvem.

O texto base do *Cloud Act* não previu a forma pela qual os países qualificados podem se opor a uma ordem, constando somente que o provedor de comunicação pode comunicar a abertura de dados às suas autoridades. Tal comunicação pode constituir um direito de conhecimento prévio à reação, mas não há nada disposto na lei a esse respeito. Assim, a regulação de um eventual direito

---

[490] "(A) the interests of the United States, including the investigative interests of the governmental entity seeking to require the disclosure;"(B) the interests of the qualifying foreign government in preventing any prohibited disclosure; "(C) the likelihood, extent, and nature of penalties to the provider or any employees of the provider as a result of inconsistent legal requirements imposed on the provider; "(D) the location and nationality of the subscriber or customer whose communications are being sought, if known, and the nature and extent of the subscriber or customer's connection to the United States, or if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the nature and extent of the subscriber or customer's connection to the foreign authority's country; "(E) the nature and extent of the provider's ties to and presence in the United States; "(F) the importance to the investigation of the information required to be disclosed; "(G) the likelihood of timely and effective access to the information required to be disclosed through means that would cause less serious negative consequences; and "(H) if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the investigative interests of the foreign authority making the request for assistance. (ESTADOS UNIDOS. *U.S. Code*. Título 18, § 2703, 2018.)

[491] ABRAHA, 2020, p. 339.

492 As the White Paper notes, if a particular order is challenged, the U.S. government could "pursue alternate channels, such as narrowing or modifying a request," resolve the conflict through "good faith negotiation," or make the request via an MLAT. (ESTADOS UNIDOS. Promoting Public Safety..., 2019, p. 16.)

493 ABRAHA, 2020, p. 340.

de resistência, da exigência de apagamento de dados por matérias relativas a interesses essenciais do Estado e de outras tradicionais justificativas seria feita nos acordos executivos. Essa condição pode alterar os critérios de resistência entre os países que decidam realizá-los.

6.1.2. Acordos executivos com base no Cloud Act

A legislação americana também criou os critérios para que países terceiros possam realizar acordos bilaterais previstos no *Cloud Act*, de modo a ter acesso direto a dados armazenados por provedores de comunicação na jurisdição americana. A legislação determinou que o Advogado-Geral, com a concordância do Secretário de Estado, submeta ao Congresso o certificado de que "the domestic law of the foreign government, including the implementation of that law, affords robust substantive and procedural protections for privacy and civil liberties in light of the data collection and activities of the foreign government that will be subject to the agreement"[494].

Assim, o primeiro critério de elegibilidade a ser comprovado por um país terceiro é a robustez do sistema legal para a proteção da privacidade, tanto material quanto procedimentalmente. A especificação de alguns desses critérios está expressa: o respeito pelo Estado de Direito, a adesão aos princípios internacionais de proteção dos direitos humanos, a observância de procedimentos legais claros sobre as agências que podem requisitar e usar dados e o estabelecimento de procedimentos de minimização no tratamento de dados, entre outros[495]. Para tanto, a adesão à Convenção de Budapeste sobre cibercriminalidade é prova de adequação do ordenamento jurídico para aderir a um acordo executivo do *Cloud Act*[496].

Além de ser elegível, o país que inicia a negociação de um acordo executivo assume que a discussão é balizada *a priori* por critérios inderrogáveis. Neste particular, a legislação veda que os acordos posteriores criem a obrigação de as empresas descriptografarem dados (cripto neutra)[497]. Outro exemplo é a vedação de utilização da cooperação direta para obter intencionalmente dados de cidadãos americanos ou de residentes nos Estados Unidos; e, em caso de acesso fortuito a eles, os países devem se comprometer impreterivelmente a realizar ações de minimização de retenção,

---

[494] ESTADOS UNIDOS. *U.S. Code*. Título 18, § 2523 (b)(1). 2018.
[495] ESTADOS UNIDOS. *U.S. Code*. Título 18, § 2523 (1)(2). 2018.
[496] ESTADOS UNIDOS. *U.S. Code*. Título 18, § 2523 (1)B. 2018.
[497] (3): "the terms of the [executive] agreement shall not create any obligation that providers be capable of decrypting data or limitation that prevents providers from decrypting data". (ESTADOS UNIDOS. *U.S. Code*. Título 18, § 2523(b)(2)(3). 2018.)

uso dos dados e disseminação a países terceiros[498].

As ordens dos países terceiros devem ter como objeto a abertura de dados com a finalidade de obter provas digitais para fins penais, compreendendo a prevenção, investigação e persecução penal de crimes graves[499]. As ordens devem individualizar as pessoas, usuárias de internet, bem como apresentar "reasonable justification based on articulable and credible facts, particularity, and severity regarding the conduct under investigation" [500] e estarem em conformidade com o ordenamento jurídico do local de emissão[501].

É impreterível que a ordem seja sujeita ao controle judicial ou a outra autoridade judiciária[502]. A inclusão de outras autoridades na lei é um reconhecimento da diversidade de sistemas processuais penais. Outro limite aplicável é o princípio da especialidade, aplicável nas relações cooperacionais, de modo que os países não podem utilizar as ordens diretas para acessar meios de prova com o intuito de cooperar com outros países[503].

O *Cloud Act* limita materialmente a utilização das ordens em investigações que possam infringir a liberdade de expressão[504]. Esta limitação é relevante politicamente, na medida em que a União Europeia e outros países reconhecem a disseminação de *fake news* em redes sociais como um problema de primeira ordem, mas, aparentemente, a resposta do ordenamento americano seguirá sendo àquela tradicionalmente vista nos MLATs, isto é, a impossibilidade de cooperar.

As ordens emitidas podem ter como objeto a interceptação em tempo real de comunicações, para as quais o *Cloud Act* criou critérios adicionais. Nesse sentido, será necessário que a interceptação de dados seja por tempo fixado, não podendo ser mais longa que o necessário para as finalidades de persecução criminal. Além disso, esse meio de produção de prova só deve ser usado caso nenhum outro seja eficaz para o objetivo da investigação[505]. O preenchimento desses critérios será verificado nacionalmente pelo emissor da ordem. Como efeito prático, as empresas devem lidar com diversos padrões de controle para executar ordens de interceptação de comunicação.

---

[498] ESTADOS UNIDOS. *U.S. Code*. Título 18, § 2523(b)(3); (b)(4)(D)(v). 2018.
[499] A legislação não define o conceito de crime grave. (MAILLART, 2019, p. 388)
[500] ESTADOS UNIDOS. *U.S. Code*. Título 18, § 2523(D), IV. 2018.
[501] ESTADOS UNIDOS. *U.S. Code*. Título 18, § 2523(D), III. 2018.
[502] ESTADOS UNIDOS. *U.S. Code*. Título 18, § 2523(D), V. 2018.
[503] ESTADOS UNIDOS. *U.S. Code*. Título 18, § 2523(3)(c). 2018.
[504] ESTADOS UNIDOS. *U.S. Code*. Título 18, § 2523 (b)(4)(E). 2018.
[505] ESTADOS UNIDOS. *U.S. Code*. Título 18, § 2523 (2)(D) I. 2018.

O governo estrangeiro qualificado deve ainda concordar que haverá avaliações periódicas do seu ordenamento para verificar a manutenção dos critérios legais de elegibilidade para cooperar com a utilização do *Cloud Act*[506], bem como deve realizar mudanças no ordenamento interno, tais como as realizadas pelos Estados Unidos, para possibilitar o acesso a provas digitais diretamente por agências de persecução americanas[507]. Assim, os países terceiros terão de provar periodicamente que seus ordenamentos permanecem conformes à legislação americana, em que todo possível conflito legal será julgado, em última análise, por cortes americanas.

6.2. Pacote de provas digitais da União Europeia

O pacote de provas eletrônicas (*e-evidence package*) é composto por dois atos legislativos: o Regulamento (UE) 2023/1543 e a Diretiva (UE) 2023/1544[508], que foi inicialmente proposto dias após a promulgação do *Cloud Act*. Contudo, devido ao necessário debate institucional na União, decorrente da divisão de competência para negociação internacional compartilhada com os Estados-membros[509], o pacote foi promulgado em julho de 2023, com entrada em vigor somente em 18 de agosto de 2026.

No recital do referido regulamento, afirma-se que "*obtaining electronic evidence using judicial cooperation channels often takes a long time, resulting in situations where subsequent leads might no longer be available*"[510]. Diante do desafio de acesso às fontes digitais, a Comissão Europeia propôs uma modernização radical dos meios judiciais de cooperação internacional, que se baseavam nos MLATs e na DEI (Decisão Europeia de Investigação)[511].

---

[506] ESTADOS UNIDOS. *U.S. Code*. Título 18, § 2523 D, J. 2018.
[507] ESTADOS UNIDOS. *U.S. Code*. Título 18, § 2523 G. 2018.
[508] Regulamento do Parlamento Europeu e do Conselho relativo às Ordens Europeias de Produção e Preservação de Provas Eletrônicas em Matéria Penal e Proposta de Regulamento do Parlamento Europeu e do Conselho sobre o Acesso Transfronteiriço a Provas Eletrônicas (Pacote *E-Evidence*).
[509] BLAŽIČ, Borka Jerman; KLOBUČAR, Tomaž. Removing the barriers in cross-border crime investigation by gathering evidence in an interconnected society. Information & Communications Technology Law, v. 29, n. 1, p. 66-81, 2020.
[510] UNIÃO EUROPEIA. Parlamento Europeu e Conselho. Regulamento (UE) 2023/1543, de 12 de julho de 2023. Relativo às ordens europeias de produção e às ordens europeias de conservação [...]. *Jornal Oficial da União Europeia*, Luxemburgo, L 191, p. 118-180, 28 jul. 2023. Recital 8.
[511] A EIO já havia intensificado a abrangência do alcance do reconhecimento mútuo de decisões judiciais em matéria probatória, que vinha sendo aplicado no Decisão-Quadro 2008/978 sobre Mandado Europeu de Obtenção de Provas (MEOP) e a Decisão-Quadro 2003/577/JHA sobre conservação de provas. Entretanto, todos sem aplicação fora da União Europeia, isto é, não permitindo acesso a dados armazenados em países-terceiros (fora do bloco). As autoridades

Esta modernização implica a eliminação do processo tradicional, no qual uma autoridade judicial que emite uma decisão exigia validação por outra autoridade judicial na jurisdição onde a decisão teria efeito para ser executável, modelo padrão dos MLATs. No novo modelo, o Estado de Execução passa a atuar como órgão de supervisão, para aplicação de motivos pré-determinados para a recusa de uma ordem de acordo com o Regulamento, cujas principais variáveis são a urgência, que determina os prazos aplicáveis, e a gravidade, as infrações penais.

Os novos tipos de ordens são a OEP (Ordem Europeia de Produção) e a OEC (Ordem Europeia de Conservação), que permitem o acesso a dados de assinante, de acesso, de transação e de conteúdo diretamente de prestadores de serviços legalmente localizados noutro Estado-Membro – o Estado de Execução[512]. A OEP impõe a produção e a divulgação de provas digitais, enquanto a OEC é uma medida cautelar provisória para a conservação de dados. Complementarmente, a Diretiva (UE) 2023/1544 determina a nomeação de representantes legais para companhias que oferecem serviços digitais no âmbito da União[513].

No que se refere aos destinatários das ordens, quatro setores econômicos são afetados: prestadores de serviços de comunicações eletrônicas (provedores de e-mail); prestadores de serviços da sociedade da informação (redes sociais e outras aplicações de interação); prestadores de serviços de infraestrutura de internet (ligação à internet); e mercados online[514]. A este respeito, o pacote tem um impacto direto nas atividades comerciais das grandes empresas de tecnologia no bloco, particularmente em áreas como as redes sociais e o armazenamento de dados.

Essas obrigações de entrega de dados pelas empresas foram desvinculadas do local de armazenamento[515], o que segue a tendência da legislação americana sobre o assunto. A atração da jurisdição da União Europeia se baseia em dois critérios adicionais à prestação dos serviços a

---

judiciárias, que inclui juízes, cortes, juízes de investigação e procuradores públicos podem emitir a EIO, ou seja, manteve-se a tradicional flexibilidade do sistema de MLAT, reconhecendo-se a autoridade competente do país requerente. O objetivo desse instrumento era possibilitar medidas de investigação em outros Estado-membros, não tratando especificamente de provas digitais. O único dispositivo sobre provas digitais na Directiva 2014/41/EU é o que regula a interceptação de telecomunicações com assistência de outro Estado, em que endereços de IP podem ser o objeto do pedido.

[512] UNIÃO EUROPEIA. Regulamento (UE) 2023/1543, cit., art. 3º, n. 9, 11 e 12.

[513] UNIÃO EUROPEIA. Parlamento Europeu e Conselho. Diretiva (UE) 2023/1544, de 12 de julho de 2023. que estabelece regras harmonizadas aplicáveis à designação de estabelecimentos designados e à nomeação de representantes legais para efeitos de recolha de prova eletrónica em processos penais. *Jornal Oficial da União Europeia*, Luxemburgo, L 191, p. 181-190, 28 jul. 2023. Considerando 7.

[514] STEFAN, Marco; FUSTER, Gloria González. Cross-border Access to Electronic Data through Judicial Cooperation in Criminal Matters: State of the art and latest developments in the EU and the US. [Brussels]: CEPS, 2018. (CEPS Paper in Liberty and Security in Europe, n. 2018-07). p. 25.

[515] UNIÃO EUROPEIA. Diretiva (UE) 2023/1544, n. 21.

pessoas físicas e jurídicas em um Estado-Membro: a) a incorporação de uma sede em um país do bloco[516]; b) a existência de ligação substantiva com a União – a ser analisada com base fática, quantidade de usuários, direcionamento de serviço, idioma e moeda utilizada em transações e possibilidade de encomendar bens[517].

Assim, as empresas que prestarem serviços em qualquer país-membro estarão sujeitas à jurisdição de todos os países da União Europeia, em relação às atividades econômicas realizadas no espaço europeu[518]. Nesse sentido, é irrelevante o fato de os dados estarem armazenados em países terceiros, tampouco a inexistência de sede ou que o serviço seja prestado a partir do exterior, por meio de computação em nuvem[519]. Em comparação ao *Cloud Act*, a diferença central recai no fato de que no âmbito europeu necessariamente haverá dois países envolvidos[520], dado que as regras do pacote vedam a utilização no âmbito nacional, aplicando-se o direito do Estado-Membro.

Portanto, as diferenças centrais entre o pacote de provas digitais e os instrumentos anteriores são o efeito extraterritorial para além da União Europeia e a dispensa da participação do Estado de Execução, ou seja, a nacionalização das decisões. Pela primeira vez, o artigo 82 do Tratado de Funcionamento da União Europeia (TFUE) foi utilizado para dispensar o controle judicial no Estado de Execução, posição jurídica que gera divergências, à medida que instituições[521] e acadêmicos[522] argumentam que o artigo supramencionado fundamenta a cooperação jurídica entre autoridades judiciais, e não entre Estados e empresas.

A cooperação direta, que, para algumas hipóteses, dispensa a atuação completa das autoridades do Estado de Execução, ainda terá de se provar adequada na visão do Tribunal de Justiça da União Europeia (TJUE), já que, na linha da jurisprudência consolidada sobre a operacionalização do princípio da confiança mútua[523], essa exclusiva participação de autoridades judiciais de um Estado-Membro poderá ser considerada insuficiente para resguardar direitos fundamentais atingidos pela abertura de dados[524]. Vale lembrar que, na prática, a corte exerce um

---

[516] UNIÃO EUROPEIA, Regulamento (UE) 2023/1543, cit. art., 3º, 4.
[517] UNIÃO EUROPEIA. Regulamento (UE) 2023/1543, cit., art. 3º, n. 4, alínea "b".
[518] UNIÃO EUROPEIA, Regulamento (UE) 2023/1543, 2023, art. 2º, n. 3.
[519] STEFAN; FUSTER, 2018.
[520] UNIÃO EUROPEIA. Regulamento (UE) 2023/1543, cit., arts. 4, 14 e 16.
[521] COUNCIL OF BARS AND LAW SOCIETIES OF EUROPE. CCBE recommendations on the establishment of international rules for cross-border access to electronic evidence. [Brussels]: CCBE, 2019.
[522] STEFAN; FUSTER, 2018, p. 41.
[523] STEFAN; FUSTER, 2018, p. 28.
[524] STEFAN; FUSTER, 2018, p. 28.

tipo de controle de constitucionalidade da legislação secundária[525].

As funções do Estado de Execução na qualidade de fiscalizador geraram intenso debate, especialmente em razão da divergência sobre a necessidade de comunicação da emissão das ordens pelo Estado de Emissão. O tema opôs o Parlamento Europeu e o Conselho da União Europeia, em vista da necessidade ou não de extensão da notificação para os dados aparentemente menos sensíveis. A relatora da proposta no Parlamento Europeu defendeu uma posição mais abrangente, na qual a notificação seria geral, mas sofreu resistência dos Estados-Membros e dos conservadores do Parlamento Europeu[526], tendo sido, por fim, dispensada em casos menos sensíveis.

A consequência dessa versão adotada no pacote de provas digitais é que o regulamento escalona o grau de proteção à privacidade em razão do tipo de dado a que se busca acesso, oferecendo mais garantias para o acesso a dados mais sensíveis. Nessa lógica, dados cadastrais e de tráfego – utilizados somente para identificação de pessoas – detêm o menor grau de proteção, em oposição aos dados de tráfego e conteúdo. Esta escolha vai de encontro posição da Corte Europeia de Direitos Humanos, que interpreta que a hierarquização do grau de proteção pelo tipo de dado coloca em risco a privacidade dos usuários[527]. Ademais, essa categorização de nomenclatura está em linha com a Convenção de Budapeste e os ordenamentos dos Estados-Membros[528].

Em relação aos limites estabelecidos, destaca-se que as ordens não podem ser utilizadas para a produção de informações financeiras dos investigados[529]. Na mesma linha, há vedação à utilização da OEP e da OEC para obtenção de dados que sejam tratados com a finalidade de exercício de funções públicas de outro Estado-Membro[530], isto é, estabelece-se um limite prévio com o intuito de impedir a violação aos interesses essenciais dos outros Estados. Os privilégios e as imunidades também receberam regulação específica – diplomacia e jornalismo –, nesses casos, o Estado de Emissão só poderá emitir uma ordem possível no ordenamento interno[531].

Os sigilos profissionais, como o da relação entre cliente e advogado, também impõem

---

[525] EU regulation on production and preservation orders – do the new instruments remove the barriers for effective access to cross-border e-evidence? (BLAŽIČ; KLOBUČAR, 2020, p. 76-80.)
[526] SIPPEL Birgit, Guest Editorial *in* Electronic Evidence Eurocrim, 2023.
[527] STEFAN; FUSTER, 2018, p. 41.
[528] UNIÃO EUROPEIA. Regulamento (UE) 2023/1543, Cons. 31.
[529] Art. 3º, n. 3. A definição de serviço financeiro está em conformidade com o art. 2º, n. 2, alínea "b", da Diretiva 2006/123/CE do Parlamento Europeu e do Conselho.
[530] UNIÃO EUROPEIA. Regulamento (UE) 2023/1543, Cons. 44.
[531] UNIÃO EUROPEIA. Regulamento (UE) 2023/1543, Cons. 47.

restrições à emissão de OEPs, permitindo-a somente nos casos em que o profissional resida no Estado de Emissão[532]. Esta limitação deve ser lida em conjunto com a obrigação de que o emissor se certifique sobre o local de residência da pessoa visada para obtenção de dados de conteúdo e de tráfego[533]. Entretanto, a presunção de que o provedor de comunicação conhece a nacionalidade e o local de residência do usuário esbarra em questões técnicas, mas esse desafio é consequência inafastável da escolha política da não territorialidade dos dados.

Sobre a proteção de dados, a legislação da União Europeia prevê a necessidade de implementação de vias de recurso adequadas para as pessoas que tiverem dados tratados em razão do regulamento, abrangendo os visados pelas investigações e os terceiros interessados[534]. Especificamente sobre os investigados, o regulamento determina que o Estado de Emissão deve permitir o direito de defesa dos visados no processo penal interno perante cortes judiciais[535]. Dessa forma, o regulamento transfere à autoridade que tem o interesse na persecução a obrigação de possibilitar a discussão dos limites penais da cooperação *a posteriori*.

Após a exposição das alterações substanciais de modelo, abrangendo a origem e os princípios que regem as OEP e as OEC, sumarizam-se, a seguir, os procedimentos processuais relativos à emissão dessas ordens, com destaque para os limites penais, os critérios de urgência, os prazos e as regras de notificação.

6.2.1. Procedimentos processuais para obtenção da prova

A tabela abaixo apresenta os detalhes para a emissão de decisões de produção de prova, com base no tipo de dados, na gravidade do crime e nas autoridades competentes. A informação foi obtida dos artigos 4º, 5º e 8º do Regulamento 1443/2023:

Tabela 6 - Normas aplicáveis à emissão de DEP

Tipo de dados	Limite penal	Autoridade de Emissão	Notificação
Dados de	Qualquer infração penal	Autoridade judicial ou	Isenta

[532] UNIÃO EUROPEIA. Regulamento (UE) 2023/1543, Cons. 45.
[533] UNIÃO EUROPEIA. Regulamento (UE) 2023/1543, Cons. 53.
[534] UNIÃO EUROPEIA. Regulamento (UE) 2023/1543, art. 18, nº 1.
[535] UNIÃO EUROPEIA. Regulamento (UE) 2023/1543, art. 18, nº 2.

assinante		procurador	
Dados de acesso	Qualquer infração penal	Autoridade judicial ou procurador	Isenta
Dados de tráfego	Infrações puníveis com pena máxima de prisão de 3 anos ou mais (ou infrações catalogadas[536])	Autoridade judicial	Obrigatória
Dados de conteúdo	Infrações puníveis com pena máxima de prisão de 3 anos ou mais (ou infrações catalogadas)	Autoridade judicial	Obrigatória

Fonte: elaborada pelo autor

Como se pode notar, quanto mais sensíveis forem os dados, maior o grau de proteção estabelecido para a possível emissão de uma decisão de produção. Assim, para obter acesso a dados mais sensíveis relativos à privacidade – conteúdo e tráfego –, será necessária uma decisão judicial no Estado de Emissão, mesmo que o sistema jurídico interno estabeleça a competência de autoridades judiciárias para ordenar a divulgação deste tipo de prova. Além disso, o limite estabelecido para a pena de prisão é baixo para a amplitude da precaução.

O prazo para cumprir a OEP é de 10 dias após a sua recepção, sendo a empresa destinatária responsável por fornecer os dados. No entanto, se for necessária a notificação formal, a empresa destinatária deve aguardar uma manifestação de não oposição do Estado de Execução ou o decurso do prazo[537]. Excepcionalmente, para casos urgentes, o prazo do destinatário pode ser reduzido para oito horas para a produção de prova e, se a comunicação for obrigatória, a Autoridade de Execução tem 96 horas para apresentar uma oposição. Além disso, se a transmissão ocorrer antes da oposição, pode ser exigida a eliminação dos dados ou a restrição da sua utilização[538].

O prazo para notificação serve para que a Autoridade de Execução se oponha à OEP, enquanto os motivos que regulam a possibilidade de recusa estão contidos no artigo 12º do Regulamento. Também podem ser alegados como fundamento de recusa os princípios

[536] O Artigo 4º, alíneas b) e c), prevê os crimes mencionados: (i) crimes definidos nos Artigos 3º a 8º da Diretiva (UE) 2019/713 do Parlamento Europeu e do Conselho; (ii) crimes definidos nos Artigos 3º a 7º da Diretiva 2011/93/UE; (iii) crimes definidos nos Artigos 3º a 8º da Diretiva 20 13/40/UE; e (c) para crimes penais definidos nos Artigos 3º a 12 e 14 da Diretiva (UE) 2017/541.
[537] UNIÃO EUROPEIA. Regulamento (UE) 2023/1543, cit., art. 10, n. 2 e 3.
[538] UNIÃO EUROPEIA. Regulamento (UE) 2023/1543, cit., art. 10, n. 4.

convencionais da União Europeia, as imunidades ou garantias de limites penais do Estado de Execução, bem como a violação do princípio *ne bis in idem* ou o fato de a conduta não ser classificada como infração penal no local de produção da prova (ou a pena máxima ser inferior a 3 anos de prisão)[539].

Caso a Autoridade de Execução invocar algum desses motivos, deve comunicá-lo à empresa de destino e à Autoridade de Emissão, levando à suspensão da produção da prova pretendida. A oposição também pode ser parcial, o que autoriza a divulgação dos dados sujeitos excepcionados pela Autoridade de Execução.

Por uma questão de paralelismo, os mesmos critérios para a emissão de uma OEC foram sistematizados, de acordo com os artigos 5º e 6º do Regulamento. Neste caso, o principal critério para a emissão da OEC é que a conduta seja classificada como infração penal no local de ocorrência, ou seja, no Estado de Emissão[540]. Isto acontece porque a conservação de dados pode ser seguida por outros pedidos de cooperação jurídica internacional, especificamente o auxílio judiciário mútuo e a DEI (Decisão Europeia de Investigação)[541].

Tabela 7 - Normas aplicáveis à emissão de OEC

Tipo de dados	Limite penal	Autoridade de Emissão	Notificação
Dados de assinante	Qualquer infração penal	Autoridade judicial ou procurador	Não aplicável
Dados de acesso	Qualquer infração penal	Autoridade judicial ou procurador	Não aplicável
Dados de tráfego	Qualquer infração penal	Autoridade judicial ou procurador	Não aplicável
Dados de conteúdo	Qualquer infração penal	Autoridade judicial ou procurador	Não aplicável

Fonte: elaborada pelo autor

[539] UNIÃO EUROPEIA. Regulamento (UE) 2023/1543, cit., art. 12, n. 1, alíneas “a”, “b”, “c” e “d”.
[540] UNIÃO EUROPEIA. Regulamento (UE) 2023/1543, cit., art. 6º, n. 3.
[541] UNIÃO EUROPEIA. Regulamento (UE) 2023/1543, cit., art. 6º, n. 2.

A OEC dispensa a necessidade de comunicação, de modo que a ordem de conservação de dados deve ser cumprida imediatamente. O prazo para a conservação é de 60 dias, que pode ser prorrogado a pedido da Autoridade de Emissão por mais 30 dias. Durante este período, se houver qualquer comunicação de emissão ou envio de qualquer pedido de cooperação na produção e entrega da prova, o destinatário será obrigado a conservá-la pelo tempo necessário. Se a conservação deixar de ser necessária, o destinatário deve ser notificado pela Autoridade de Emissão[542].

A ordem de conservação, ou uma medida cautelar semelhante para a conservação de dados, tem potencial teórico e prático para ser utilizada em contextos mais amplos, uma vez que o congelamento de informações digitais por um prestador de serviços de internet pode ser seguido por uma ordem judicial de cooperação entre Estados. Esta utilização evitaria que a volatilidade da prova digital se tornasse um problema jurídico, ao mesmo tempo em que os Estados poderiam discutir a aplicação de possíveis limites à cooperação em casos concretos, alcançando maior proteção dos direitos humanos do que no caso da cooperação direta *per se*[543].

Por fim, foram delineados neste subtópico os critérios processuais para os mecanismos de OEP e OEC, relativos à aplicação de limites penais e aos prazos relativos a cada um, com ênfase nos motivos de recusa e na notificação obrigatória. Na perspectiva comparada, deve-se ressaltar o fato de que os privilégios, as imunidades e os dados públicos têm procedimento específico para serem sustentados, e são motivo de recusa de ordens de produção, para o qual o sistema de notificação foi a principal inovação realizada pela União Europeia no pacote para as provas digitais.

---

[542] UNIÃO EUROPEIA. Regulamento (UE) 2023/1543, cit., art. 11, n. 1 a 3.

[543] Essa opinião foi defendida pelo Conselho das Ordens dos Advogados e Sociedades de Advogados da Europa: "O CCBE afirma que a proposta deveria ser limitada, em seu escopo, às Ordens Europeias de Preservação e que os objetivos perseguidos pela Comissão poderiam ser igualmente alcançados pela utilização, em combinação com a criação de uma Ordem Europeia de Preservação, dos procedimentos previstos na EIO e nos MLATs, os quais, consequentemente, também poderiam necessitar de aprimoramento" (COUNCIL OF BARS AND LAW SOCIETIES OF EUROPE. CCBE position on the Commission proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters. [S.l.]: CCBE, 19 out. 2018.)

7. SUPERAÇÃO DA DOGMÁTICA TRADICIONAL: A FINALIDADE COMO CRITÉRIO LIMITADOR DE ATOS INVESTIGATIVOS

Os capítulos anteriores contêm uma abordagem tradicional do ponto de vista processual penal, que é descrever de que forma os atos de investigação ou atos de provas antecipadas adquirem elementos de informação para a investigação e para a futura ação penal. Dessa forma, o texto seguiu a tendência da dogmática tradicional, que usa categorias estáticas probatórias para avaliar os referidos atos. Entretanto, tal como demonstrado no Capítulo 2, esse racional encontra limitação na era da informação, especificamente nas características da *big data.*

O fato histórico é a possibilidade de fazer uso automatizado de informações, com computadores que ganham capacidade de processamento em nível exponencial e com a apresentação de resultados mais sofisticados. Nesse cenário, cresce a utilização de ferramentas atuarias, algorítmicas, de aprendizado de máquina e de inteligência artificial para a realização de funções avaliativas humanas[544]. Tal aumento vem sendo estudado criticamente pelo direito, justamente para entender o novo padrão de racionalidade que é aplicado às funções automatizadas.

O estudo dos algoritmos aplicados a funções no direito é uma das possíveis linhas de investigação desse fenômeno. Especificamente sobre o processo penal, Garcia se destaca com perguntas pertinentes, tais como "é possível compreender um algoritmo?", "é possível acessar um algoritmo?"[545] ou "o que é um algoritmo"[546]. Também é possível pesquisar essa nova realidade a partir dos resultados ilícitos de uso de dados, que se expressam em pesquisas que demonstram vieses e resultados que atingem direitos[547] e os vieses de aplicação das tecnologias por seus usuários.

Por opção de método, este capítulo não aprofunda o estudo das tecnologias em espécie, na

---

[544] MCKAY, Carolyn. Previsão de risco no processo penal: ferramentas atuariais, algoritmos, IA e tomada de decisão judicial. Current Issues in Criminal Justice, [s.l.], p. 1-25, 29 set. 2019, p. 4.

[545] GARCIA, Rafael de Deus. Processo penal e algoritmos: o direito à privacidade aplicável ao uso de algoritmos no policiamento. 2022. Tese (Doutorado em Direito) – Programa de Pós-Graduação em Direito, Universidade de Brasília, Brasília, 2022, p. 155-169.

[546] DEUS GARCIA , Rafael; PIZA DUARTE, Evandro. Compreendendo algoritmos aplicados ao sistema de justiça criminal – Ilegibilidade, acesso, compreensão, verdade e computabilidade no 'eu' identificado por algoritmos, 2025, p.10-12.

[547] Por exemplo, Pedreschi e Turini investigaram os vieses discriminatórios escondidos em algoritmos de mineração de palavras, tendo sido possível diferencias em discriminação direta e indireta. PEDRESHI, D.; RUGGIERI, S.; TURINI, F. Discrimination-aware data mining. Proceeding of the 14th ACM SIGKDD international conference on Knowledge discovery and data mining - KDD 08, 2008.

medida em que os usos delas podem ser intercambiáveis; por exemplo, o cálculo atuarial de um risco inaceitável de reincidência pode ser determinado tecnicamente por um algoritmo. Na mesma linha, o que se denomina inteligência artificial pode ser compreendido como formas avançadas de instrumentalizar tarefas, em um modelo estatístico multivariado que permite, inclusive, a alteração do algoritmo autonomamente (aprendizado), que é a função exercida por algoritmos. Portanto, o que interessa ao recorte realizado é que se escrutine para qual uso essas ferramentas são implementadas concretamente, como ponto de partida para o debate sobre a legalidade.

A compreensão do algoritmo é conceitualmente possível. Entretanto, a opacidade e a escala do processamento impedem a antecipação exaustiva dos resultados obtidos, já que eles executam instruções sobre múltiplas variáveis em um nível além das capacidades do cérebro humano. Talvez essa seja precisamente a razão para desenvolvê-los: funcionar como "um conjunto de instruções (...) [que realizam] uma tarefa, produzindo o resultado final a partir de um ponto de partida"[548].

No campo penal, o resultado dessas instruções é uma ação útil processualmente, como a progressão de regime, a estimativa de fiança, a valoração probatória na sentença[549] e, para o recorte da tese, a busca do elemento de informação na investigação preliminar.

Quando se tenta ver um algoritmo, a imagem disponível é uma equação matemática, um fluxograma ou uma sequência lógica de passos, cuja possibilidade de compreensão vai depender da complexidade e da escala da tarefa executada por ele. Diante disso, é necessário reconhecer que os algoritmos não são naturais nem são dados encontrados na natureza. Foram desenvolvidos por humanos para cumprimento de funções pré-determinadas, cuja utilidade é medida por humanos: traduzir um texto, realizar um cálculo de juros, reconhecer alguém em uma foto etc.

Nesse sentido, se as funções, a utilidade e a informação são dadas pelos humanos, nada mais natural que estudar a conduta dos agentes que utilizam algoritmos para funções processuais penais como o foco do regramento jurídico. Essa é a justificativa para o recorte metodológico realizado no capítulo, o foco da análise jurídica é o que e como as técnicas de tecnologia da informação podem ser usadas para o uso e reúso automatizado de dados pelos investigadores – os agentes de tratamento. Tal entendimento significa focar na pessoa que faz o tratamento de dados e, a partir disso, abstrair como os atos de investigação com uso e reúso de dados devem ocorrer.

---

[548] DONEDA, D.; ALMEIDA, V. A. F. O que é governança por algoritmos? In: BRUNO, F. et al. (org.). Tecnopolíticas da vigilância: perspectivas da margem. 1. ed. São Paulo. Boitempo, 2018, p. 141.
[549] CHRISTIN, Angèle; ROSENBLAT, Alex; BOYD, Danah. Courts and Predictive Algorithms. New York: Data & Society Research Institute, 2015, p. 3-5.

O segundo recorte deriva da premissa de que o conhecimento a partir do dado é relacional ao entorno. Por exemplo, o dado cadastral pode revelar dados sensíveis sobre religião, a depender dos conhecimentos correlacionais que se tenha disponíveis. Logo, se não é conhecido o entorno, toda a discussão se dá estaticamente, de modo que os exemplos são ilustrativos e não exaustivos das situações possíveis, o que é uma característica muito presente em textos sobre tecnologia e direito, a exposição de inúmeros exemplos para explicar o argumento sem, contudo, formular abstrações generalizantes que possibilitem disciplinar juridicamente o tema.

Por essas razões, o capítulo recolhe as práticas investigativas que são objeto de debate internacionalmente, denominadas de técnicas especiais de investigação (TEI)[550], e identifica como a racionalidade jurídica-processual brasileira as interpreta em casos práticos, utilizando-se das hipóteses julgadas pelo STJ e pelo STF. Em todos os exemplos, é possível projetar a hipótese de pesquisa: a finalidade no uso e reúso de dados não é identificada como um limite jurídico, mantendo-se um padrão decisional binário: acesso ou não acesso.

A pesquisa encontrou três técnicas especiais de investigação, para as quais há grande divergência jurídica: o mandado de busca reverso (*geofencing*), a localização por varredura de torres e a quebra de sigilo coletivo de buscadores de palavras-chave. O debate jurídico sobre essas técnicas ocorreu de forma aprofundada nas investigações do assassinato da vereadora Marielle Franco, no Rio de Janeiro[551], por duas razões: a grande repercussão do caso e os interesses do *Google* no tema, que foi alvo de diversas ordens. Pode-se dizer que os julgamentos desse caso são um ponto de inflexão para a uniformização da jurisprudência nos tribunais superiores[552].

As técnicas especiais de investigação se baseiam no tratamento de dados pessoais para obter resultados probatórios úteis, que geralmente estão conectados à identificação de pessoas a partir dos dados coletados coletivamente de forma prévia, ou em tempo real, pela arquitetura informacional de empresas e de Estados. Assim, é o rastro digital que serve para identificar suspeitos no mundo real, e não o contrário[553]. Essa contestação é o objeto de controvérsia, que se

---

[550] ARAS, 2014, p. 596.

[551] O assassinato de Marielle Franco ocorre em 26 de agosto 2020, no Rio de Janeiro, motivado por razões políticas, especificamente por se opor a organizações criminosas que dominam territórios naquela cidade. O caso é nacional e internacionalmente referido com um assassinato político, cuja apuração contou com os esforços consideráveis das agências de persecução. Registra-se que a discordância jurídica sobre os meios de obtenção de prova não significa condescendência com esse tipo de ato odioso.

[552] A evidência da afirmação é o reconhecimento da repercussão geral no STF, que dará origem ao 1148.

[553] ARAS, 2014, p. 601.

expressa na necessidade ou não de individualizar a medida, utilizando-se o racional das medidas cautelares penais, que pressupõe a suspeita sobre a autoria[554].

Avançando especificamente sobre os métodos, o cerco digital é uma técnica que delimita áreas geográficas a partir de infraestruturas informacionais, com delimitação temporal, e que permite identificar pessoas que conectaram dispositivos eletrônicos a redes de internet, fizeram login em aplicativos e receberam sinais daquele local[555]. Dentre as traduções para *geofencing*, uma das opções encontradas é a quebra de sigilo locacional[556], que é a que mais dialoga com o histórico da discussão brasileira e permite a visualização da finalidade do uso imediatamente.

Os primeiros usos dessa técnica ocorreram nos Estados Unidos a partir de 2016 e, nos dois anos subsequentes, o *Google* passou a receber frequentemente tais ordens, tendo relatado a recepção de 180 mandados de quebra de sigilo locacional em uma única semana[557]. Nesse contexto, a discussão se coloca na causa provável para buscar coletivamente os dados, o que poderia estar em desacordo com a 4ª Emenda da Constituição dos Estados Unidos. Contudo, o que mais importa da prática americana para a tese, é o procedimento usado para o cumprimento das ordens judiciais.

A empresa criou um sistema em três passos para o cumprimento das decisões judiciais, diante da ausência de padronização das decisões: i) compilação anonimizada de dados a partir do critério temporal e geográfico, com identificação de latitude/longitude, registro de data e hora e o modo como o histórico foi gerado; ii) delimitação, pela agência de investigação, dos usuários de interesse, o que pode abranger buscas relacionadas a mais de um dispositivo e; iii) entrega, pela empresa, da identificação dos alvos de interesse da investigação, permitindo a sua identificação[558].

A primeira questão que deve chamar a atenção no protocolo do *Google* é que os funcionários da empresa realizam atos próprios de investigação, em alguns casos com

---

[554] LOPES JUNIOR, 2020, p. 906-908.

[555] SCHEMBRI, Thomas J. The rise of technology and its effect on search and seizure analysis: the constitutionality of geofencing warrants under the supreme court's fourth amendment jurisprudence. South Carolina Law Review, Columbia, SC, v. 75, n. 1, 2023, p. 131.

[556] Aras traduziu da seguinte forma: "Palavra composta de "geo" (terra) e "fence" (cerca). Nesta última está também embutidaa ideia de "georrefenciamento" (georeferecing). Pode ser traduzida como "busca por coordenadas geográficas" ou como "cerco digital" ou ainda como "quebra de sigilo locacional". (ARAS, Vladimir. Cerco digital ("geofence") e varredura terminológica: balizas constitucionais e legais. In: SALGADO, Daniel de Resende; BECHARA, Fábio Ramazzini; GRANDIS, Rodrigo de (coord.). 10 anos da Lei das Organizações Criminosas: aspectos criminológicos, penais e processuais penais. São Paulo: Almedina, 2023. p. 617.

[557] Disponível em https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking police.html. Acessado em 21/02/2023.

[558] BENGART, Aaron A. Always a Suspect: Law Enforcement's Violative Use of Geofence Warrants and Geolocation Data in Criminal Investigations and Proceedings. *Cardozo International & Comparative Law Review*, [S. l.], v. 7, n. 639, 2024, p. 655-657.

requerimentos de mais informações às agências estatais para restringirem o alcance das medidas, ou seja, a análise da proporcionalidade da ordem de entrega. Em segundo lugar, a clarividência da falta de procedimento processual penal é a observação, e o aceite judicial, de que a empresa se figure responsável por desanonimizar após exigir ações de minimização da polícia. Não há, contudo, fontes seguras para saber se o método é aplicado no Brasil.

Já a varredura de torres se caracteriza pela aquisição de dados de conexão a terminais móveis de telefonia, popularmente identificados como *pings*, com delimitação temporal. A técnica quando aplicada coletivamente permite a identificação de todas as conexões em uma janela de tempo. O uso dessa técnica tem um histórico mais consolidado no Brasil, tendo em vista que a localização de pessoas individualizadas está positivada em leis especiais, que foram descritas no capítulo a respeito das requisições, com destaque para a Lei das Organizações Criminosas, em que se fala das Estações Rádio Base (ERB).

O mandado de busca reverso e a varredura de torres para localização encontram-se na mesma situação jurídica: o reúso de dados para identificar deslocamentos geográficos de usuários de dispositivos eletrônicos, em tempo real ou no passado, num contexto coletivo, em que a técnica é utilizada para identificar possíveis autores, coautores e partícipes. É importante que as técnicas sejam definidas pela finalidade porque a origem dos dados para atingi-la pode ser diversa. Por exemplo, os metadados de serviços financeiros – cartões de crédito, acessos ao Pix, dentro outros – podem permitir o rastreamento de um suspeito em fuga[559].

Ademais, a quebra de sigilo de buscadores por parâmetros de pesquisa almeja acesso aos dados de tráfego de usuários, coletivamente, para identificação da autoria penal, retrospectivamente. Assim, não se deve limitar a discussão ao *Google*, na medida em que a técnica poderia ser aplicada para qualquer buscador ou aplicação, a exemplo dos dados de tráfego de usuários de LLM (*large language model*), como conversas com o *ChatGPT*. Essa técnica usa o parâmetro de buscas para identificação de suspeitos e tem alto potencial de aplicabilidade para impedir a realização de riscos coletivos inaceitáveis, tais como o terrorismo.

Após a explicação dos recortes aplicáveis e das tecnologias identificadas, a racionalidade processual penal brasileira, tanto doutrinária quanto jurisprudencial, é debatida em tópico específico para cada situação jurídica, com o intuito de identificar o padrão argumentativo utilizado

[559] ARAS, 2023, p. 612.

e orientar a resposta à pergunta de pesquisa.

7.1. Rastreamento geográfico por varredura de torres e cerco digital

A pesquisa identificou que o STJ passou a receber impugnações sobre a quebra de sigilo locacional pelo menos a partir de 2017, isto é, em data muito próxima aos primeiros usos internacionais identificados em 2016. Nesse contexto, cabe uma observação interessante: os recursos e remédios constitucionais que dão origem às decisões da Corte partem das próprias empresas destinatárias das ordens, e não dos investigados ou réus submetidos a investigações ou ações penais. De certa forma, essa circunstância é coerente com o propósito da medida, que visa a precisamente identificar autores desconhecidos de infrações penais a partir de dados pessoais.

O primeiro caso identificado foi a TP 292/SP[560], de 2017, ajuizada pelo *Google*, que questionava decisão judicial autorizando a quebra de sigilo locacional de número indeterminado de pessoas com base no local e horário da prática de infrações penais. No STJ, a relatoria concedeu tutela provisória, suspendendo a ordem de entrega de dados deferida na Justiça estadual de São Paulo, posteriormente mantida parcialmente em mandado de segurança pelo TJSP. Em termos de fundamentação, a decisão limitou-se a afirmar a probabilidade do direito da empresa para suspender a eficácia da ordem, sem especificá-la, mencionando o risco à privacidade dos usuários.

Meses depois, a Corte recebeu o RMS 59.716/RS[561], no qual discutia-se o deferimento da quebra de sigilo locacional do histórico de conexões de dados 3G, mensagens de texto, IMEIs e dados cadastrais, num raio de 500 metros, no intervalo de duas horas e meia. A investigação apurava uma hipótese de furto com arrombamento, cuja pena varia de quatro a oito anos, que no primeiro olhar é um limite penal baixo para a autorização de medida tão ampla. Inicialmente, a relatoria suspendeu a decisão do TJRS por violação ao sigilo do fluxo de comunicações, com fundamento no Marco Civil da Internet e na Lei de Interceptação Telefônica.

Posteriormente, a decisão de mérito inadmitiu o recurso, entendimento que foi mantido pela Turma, aplicando-se a orientação superveniente do RMS 61.302/RJ[562], no sentido de que a "requisição de dados de geolocalização, nos termos dos artigos 22 e 23 do Marco Civil da Internet,

---

[560] BRASIL. Superior Tribunal de Justiça. Tutela Provisória 292/SP, 2017.
[561] BRASIL. Superior Tribunal de Justiça. RMS 59.716/RS, 2017.
[562] BRASIL. Superior Tribunal de Justiça. RMS 61.302/RJ, 2019.

não havendo falar em ilegalidade"[563]. Antes do julgamento da 3ª Seção sobre precedente carioca, que unificou o entendimento do STJ sobre o tema, o RMS 61.419/SE[564] teve o pedido liminar indeferido, cuja fundamentação é central para o objeto da discussão da tese.

O primeiro argumento a ser destacado diz respeito à proteção mais branda da privacidade e da intimidade aos dados pessoais, em comparação ao conteúdo comunicacional[565]:

> [...] Por serem de muito menor relevo para a proteção da intimidade e da privacidade, os dados pessoais – aí incluídos os registros de conexão e de acesso a aplicações de internet – são protegidos, mas por um regime jurídico bem mais brando do que aquele aplicável ao conteúdo das comunicações. A legislação não dispõe sobre inviolabilidade, mas em "não fornecimento a terceiros" dos dados pessoais, "salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei".

O trecho evidencia uma intepretação estática baseada no tipo de dado, com objetivo de hierarquizar a proteção jurídica, isto é, "x" é menos sensível que "y", logo merece menos proteção, cuja comprovação é virtualmente impossível. Num segundo momento, a decisão afirma que há hipótese legal autorizadora para a medida em questão[566]:

> [...] O Marco Civil da Internet não menciona individualização do alvo da quebra de sigilo. Na forma do art. 22, parágrafo único, exige-se a demonstração de indícios de ilícito (I), da adequação da medida, consistente na utilidade da prova buscada (II), e a identificação precisa do dado buscado (III). Portanto, para fins do Marco Civil da Internet, não é necessário que os potenciais alvos da quebra estejam identificados: basta que os dados requisitados sejam identificáveis. (...) Não estou convencido de que as requisições aos provedores de aplicações de internet mereçam tratamento diverso daquelas direcionadas a empresas telefônicas.

Como se observa, o artigo 22 do MCI é apontado como fundamento legal, defendendo-se que não há exigência de individualização do investigado. A decisão foi mantida pela Turma e, atualmente, o processo encontra-se sobrestado em razão do reconhecimento da repercussão geral do tema no STF, ao qual já se fez referência anteriormente. Vale dizer que essa argumentação foi acolhida nos julgamentos dos *leading case* no STJ, que se passa a analisar.

Em razão do caso Marielle, o STJ recebeu duas impugnações a respeito do uso da técnica

---

[563] *Op. Cit.,* p. 10-1, RMS 59.716/RS.
[564] BRASIL. Superior Tribunal de Justiça. RMS 61.302/RJ, 2019.
[565] Decisão que indeferiu a liminar no RMS 61.419/SE no STJ, p. 4.
[566] *Op. Cit.*, RMS 61.419/SE, p. 4-5.

de cercamento digital, especificamente os RMSs 62.143/RJ e o 61.302/RJ, nos quais o recorrente é o *Google*. Nos dois casos, as autoridades de persecução fluminense delimitaram coordenadas geográficas e janela temporal para descobrir os possíveis autores do homicídio. Por exemplo, em um dos casos, determinou-se a construção de um polígono com a utilização "como parâmetro a via pedagiada TransOlímpica (...) e a data de 02/12/2018" num período de 15 minutos, com intuito de identificar smartphones conectados a aplicativos como *Google Maps* e *Waze.*

Ambos os recursos foram desprovidos no STJ, que foram julgados na mesma turma em razão da prevenção do caso. Naturalmente, a fundamentação da decisão importa para traçar o perfil argumentativo, da perspectiva jurisprudencial, sobre o tema.

O voto-vencedor ressalva a importância convencional da privacidade, com citações diretas da Declaração Universal dos Direitos do Homem, da Convenção Europeia para a Proteção dos Direitos Humanos e das Liberdades Fundamentais, da Carta de Direitos Fundamentais da União Europeia[567]. Em sequência, retoma a garantia fundamental à privacidade no Brasil e afirma que não há direitos absolutos, que podem ser afastados por "decisão proferida por autoridade judicial competente, suficientemente fundamentada, na qual se justifique a necessidade da medida para fins de investigação criminal ou persecução criminal"[568].

A primeira consideração de mérito diferenciou dados armazenados e estáticos, afastando a incidência da lei de interceptação telefônica, e citou Badaró para sustentar que metadados telefônicos não estão protegidos pelo sigilo das comunicações, que é o entendimento majoritário a respeito do tema no STF[569]. Em seguida, a decisão apresenta o fundamento principal: os artigos 22 e 23 do Marco Civil da Internet permitem a requisição desses dados, com a afastamento da necessidade individualização[570]:

> [...] Não há como pretender dar interpretação extensiva aos referidos dispositivos, de modo a abranger a requisição feita em primeiro grau, porque a ordem é dirigida a um provedor de serviço de conexão ou aplicações de internet, cuja relação é devidamente prevista no Marco Civil da Internet, o qual não prevê, entre os requisitos que estabelece para a quebra do sigilo, que a ordem judicial especifique previamente as pessoas objeto da investigação ou que a prova da infração (ou da autoria) possa ser realizada por outros meios. (...) Como se observa, os referidos dispositivos, que tratam especificamente do procedimento de que cuidam os autos, não exigem a indicação ou qualquer elemento de individualização pessoal na decisão judicial. Tal exigência, por certo, revelar-se-ia verdadeiro contrassenso,

[567] RMS 61.302/RJ, p. 12-13.
[568] RMS 61.302/RJ, p. 15.
[569] A decisão cita como precedente do STF o HC 91.867/PA.
[570] BRASIL, RMS/STJ 61.302, 2020. p. 18. 18-19.

na medida em que o objetivo da lei é possibilitar essa identificação.

Argumentação citada é imprecisa. Primeiramente, o artigo 22 versa sobre processos cíveis e criminais, permitindo que "parte interessada" requeira acesso a "registros de conexão ou de registros de acesso a aplicações de internet", tanto é assim que o inciso I, do parágrafo único, exige a fundada suspeita de ocorrência de "ilícito", sem especificar de se cível ou criminal. Assim, se a argumentação dada ao referido artigo estiver correta, partes em processo civil podem requerer, com base em um ilícito dessa natureza, conhecendo somente o local do acontecimento, o acesso aos registros de pessoas indeterminadas para identificar a autoria.

O dispositivo tem por finalidade permitir a identificação civil da pessoa por trás de um autor já conhecido no ambiente digital, por exemplo, o perfil anônimo que pratica difamação ou calúnia. Sabe-se quem é o usuário "fulano123" no *Instagram*, mas não quem ele é na vida civil. Assim, é incorreto afirmar que existe autorização legal para, a partir de um ilícito cometido no mundo real, realizar identificação com base em dados coletivos no ambiente virtual. Além disso, a alegação de que "não se exige indicação ou qualquer elemento de individualização" decorre, logicamente, do fato que se pressupõe o conhecimento do autor digital do ilícito.

Em segundo lugar, caso se considere necessário e proporcional, é óbvio que a legislação deveria prever o contrário: os limites para busca coletiva, o que começaria com o limite penal para a utilização de técnica dessa natureza, em linha com a argumentação de que os meios ocultos de investigação prescindem de tipificação específica. Dessa forma, o argumento como colocado permitiria a medida para ações penais privadas que, deveriam ser indeferidas pela desproporcionalidade, e não pelo limite penal, o que não encontra paralelo em legislações estrangeiras, a exemplo da legislação americana e da União Europeia já abordadas.

No limite, a argumentação tenta suprir a ausência de previsão legal, replicando uma racionalidade processual que se sintetiza da seguinte forma: a previsão de medida de investigação para acessos a dados permite a utilização para quaisquer finalidades sustentadas pelos órgãos de persecução, inclusive uma busca coletiva fundamentada em artigo para identificação civil na internet. A mesma defesa é realizada doutrinariamente, isto é, que previsão de acesso é igual a autorização para realizar quaisquer usos úteis, que adiciona a analogia aos acessos aos dados de

ERB, prevista na lei das organizações criminosas[571].

> [...] Podemos, assim, concluir que, embora o cerco digital (quebra de sigilo locacional ou geofence) não seja regulado pela Lei 9.296/1996 ou pela Lei 12.850/2013, a conjugação desses diplomas com os arts. 7º, 10, 22 e 23 do Marco Civil da Internet propicia a base jurídica adequada para viabilizar o deferimento de mandados de cerco digital (geofence) warrants) no Brasil. O mesmo raciocínio se aplica às buscas digitais de autoria por pesquisas terminológicas.

Ao nosso ver, a autorização legislativa para a coleta de dados não pode ser analisada em desconexão com a prática processual e as teorias cautelares vigentes na quadra histórica das alterações legais. A identificação da localização via torres de celular (ERB), por exemplo, deve ser balizada pela teoria das cautelares, que exige a identificação segura da pessoa suspeita e a demonstração de indícios de autoria e materialidade para justificar a medida[572]. A finalidade é rastrear o suspeito conhecido, e não, mais uma vez, promover uma varredura para identificá-lo.

Existe um salto hermenêutico de difícil sustentação na interpretação extensiva das leis mencionadas anteriormente. Embora se defenda que a aquisição de dados individuais está autorizada legalmente – que é o argumento do STJ sobre o marco civil da internet e de Aras sobre a Lei das Organizações Criminosas[573] – a aquisição coletiva seria implicitamente autorizada pela mesma locução que permite o acesso individual. Nessa linha, a conclusão é que não há previsão legal para coleta massificada de dados de localização, o que na visão da tese, é suficiente para afirmar a ilegalidade do ato, mas não é o entendimento do tribunal mencionado.

Antes de apresentar a sintetização da racionalidade processual analisada, deve-se notar que os precedentes não citam doutrina para sustentar a argumentação de mérito dos precedentes. Talvez isso decorra da ausência de discussão aprofundada academicamente sobre o uso das técnicas especiais de investigação. Por exemplo, a pesquisa identificou somente uma fonte publicada, em

---

[571] "Podemos, assim, concluir que, embora o cerco digital (quebra de sigilo locacional ou geofence) não seja regulado pela Lei 9.296/1996 ou pela Lei 12.850/2013, a conjugação desses diplomas com os arts. 7º, 10, 22 e 23 do Marco Civil da Internet propicia a base jurídica adequada para viabilizar o deferimento de mandados de cerco digital (geofence) warrants) no Brasil. O mesmo raciocínio se aplica às buscas digitais de autoria por pesquisas terminológicas".

[572] Lopes JUNIOR trabalha com as categorias de *fumus commissi delicti* para comprovação de autoria e indícios de materialidade para medidas cautelares penais. LOPES JUNIOR, 2020, p. 801. Naturalmente, se o meio de obtenção de provas se destina a conhecer a autoria, o racional das teorias cautelares não é aplicável a essa hipótese.

[573] ARAS, 2022, p. 610-611. "É mero rastreamento de sinais (*tracing of telecommunications*). Por esse motivo, esta medida não se regula pela Lei 9.296/1996; orienta--se pelo art. 3º, inciso II, da Lei 12.850/2013 ("sinais eletromagnéticos"), pelo art. 13-B do CPP e pelos arts. 10 e 22 do Marco Civil da Internet".

coletânea de artigos sem *peer-review*, que se refere especificamente às técnicas especiais de investigação, cujo argumento central é a equiparação de acesso à possibilidade de dar qualquer uso.

Portanto, no que se refere ao uso do cerco digital e da varredura de torres, a racionalidade processual brasileira opera com as seguintes premissas:

i) a intromissão na intimidade decorrente do processamento em massa de dados é considerada menos gravosa que o acesso a dados de conteúdo;

ii) a mera previsão legal de um meio de acesso é tomada como suficiente para suprir a ausência finalidade específica do ato investigativo;

iii) há um uso injustificado dos critérios das cautelares penais nas quais se conhece o suspeito para situações que objetivam descobrir a autoria;

Esse estado da arte é insuficiente para lidar com dados pessoais individualmente, na medida em que hierarquiza estaticamente a proteção jurídica pelo tipo de informação. Com mais razão, a busca de autoria a partir de rastros digitais, que conta com o acesso a informações de pessoas indeterminadas – ainda que determináveis – supera indevidamente a ausência de previsão legal, bem como não discute se a finalidade do uso de dados pessoais em atos investigativos. Assim, a hipótese de pesquisa se confirma nesse particular: a finalidade no uso das informações não é abordada como um critério limitador do dispositivo processual penal.

A visão desta tese é no sentido oposto ao referido estado da arte. Isso porque as técnicas invasivas de investigação, ainda que sejam consideradas meios de obtenção de provas ocultos, se assemelham ontologicamente ao tratamento de dados pessoais em massa, cujos princípios derivados da proteção de dados são mais adequados para limitá-las. Na mesma linha, a teoria das cautelares penais é inaplicável, uma vez que a individualização é impossível se o objetivo da técnica é a descoberta da autoria a partir de rastros digitais. Para infirmar essa assertiva, é preciso trabalhar com a presunção de que todas as pessoas cujos dados foram adquiridos numa TEI são suspeitas do crime, o que esbarra na demonstração de causalidade das condutas.

A aplicabilidade dos princípios da proteção de dados é colateralmente reconhecida nos precedentes em questão, na medida em que se argumenta que "[a medida] não enseja gravame às pessoas eventualmente afetadas, as quais terão seu sigilo de dados registrais publicizados, os quais, se não constatada sua conexão com o fato investigado, serão descartados"[574]. Trata-se de um

[574] RMS 61.302/RJ, p. 7

raciocínio lógico e correto, embora tal dever não seja tipificado na legislação processual. Logo, a o apagamento é uma presunção do julgador, que está respaldada no dever de apagamento como princípio da proteção de dados. Isso ocorre porque, sem a importação de conceitos desse campo, não é possível analisar o uso massificado de dados pessoais na investigação criminal.

Rompendo-se com a criticada racionalidade processual descrita acima, o modelo ideal para possibilitar varredura de torres e cercas digitais tem os seguintes elementos mínimos:

i) existência de autorização expressa para requisição de dados coletivamente, definida por critérios objetivos de limitação (tempo e espaço);
ii) o ato de investigação deve almejar finalidade autorizada legalmente (rastreamento em tempo real, retrospectivo, identificação da autoria)[575];
iii) reserva de jurisdição;
iv) limite penal para investigação de crimes graves;
v) entidades públicas e privadas obrigadas pela lei a cederem dados coletados para outros fins;

A previsão em lei decorre da constatação de que a utilização de técnicas especiais de investigação atinge o direito fundamental à autodeterminação informacional de um coletivo desconhecido de pessoas, de modo que sua relativização deve ser prevista em lei proporcional, a fim de não pôr em risco seu núcleo essencial. Nesse sentido, a finalidade probatória deve ser prevista legalmente, na medida em que a proteção jurídica aos dados pessoais não deve ocorrer de forma estática, tendo em vista que o entorno correlacional permite correlações imprevisíveis, de forma dinâmica, logo todo uso fora da hipótese investigativa deve ser proibido.

Ademais, a reserva de jurisdição deve ser respeitada em razão do sigilo legal imposto aos dados, que requer decisão judicial para ser acessado coletivamente, bem como pela relevância a direitos fundamentais envolvidos nesses atos meios ocultos de investigação. Em sequência, não se deve aceitar que medidas de intrusão informacional de grande porte sejam possíveis para criminalidade não grave – medido pela estatura do bem jurídico atingido –, como visto no visto no julgado que utilizou a técnica para furto com arrombamento, que é uma exigência do princípio da proporcionalidade. Sobre o último critério, os entes públicos e empresas, que prestam determinados

[575] A autorização para a aquisição de dados, especialmente em volume e correlacionados, não deve ser tacitamente entendida como permissão para qualquer uso. Em um modelo de estrita legalidade para técnicas especiais de investigação, a finalidade da coleta deve ser expressamente definida no instrumento autorizador, limitando o tratamento e o aproveitamento probatório dos dados obtidos.

tipos de serviços, devem ter o dever de entrega previsto na norma processual.

A premissa central desta crítica é clara: o reúso coletivo de dados, tendo em vista sua natureza intrusiva e massiva, deve estar expressamente autorizada por lei como primeiro critério de validade, por configurar monitoramento do deslocamento coletivos de pessoas. Por fim, ao nosso ver, essa argumentação é a que melhor encontra acolhida pelo princípio da legalidade estrita, em se tratando da discussão das cercas digitais e varredura de torres como técnica de investigação.

7.2. Rastreamento de autoria por parâmetros de pesquisa na internet

A discussão a respeito da possibilidade de utilizar parâmetros de pesquisa na internet como ato de investigação teve a legalidade reconhecida pelo STJ no RMS 60.698/RJ[576], que também é um *leading case* que derivou a investigação do homicídio da vereadora Marielle Franco. O referido recurso foi desprovido, sendo que o STJ argumentou em síntese: a ordem se dirigia a dados estáticos; o Marco Civil da Internet não exige individualização prévia e o interesse público e proporcionalidade da restrição a direitos fundamentais estavam adequadamente fundamentados.

A argumentação jurídica é semelhante à discutida acima. Como se sabe, o debate sobre dados estáticos e em fluxo já foi realizado no Capítulo 4, razão pela qual não será retomado. Ademais, o Tribunal defendeu a aplicabilidade dos artigos 22 e 23 do Marco Civil da Internet nos mesmos termos que foram descritos no tópico anterior, de modo que não há necessidade de repetir os fundamentos anteriormente expostos. Entretanto, a situação jurídica de fato não é idêntica, o que constitui o principal equívoco da decisão e justifica a análise separada.

As agências de persecução fluminense requereram a justiça que o *Google* fornecesse dados de tráfego de usuários que haviam realizado pesquisas por termos específicos no buscador para posterior identificação do IP e dos "device IP`s". O objetivo era identificar possíveis autores do crime, tendo em vista que os outros meios de investigação não tinham identificados suspeitos ou possíveis testemunhas, de acordo com as agências de persecução. Antes de avançar, deve-se pontuar que o objetivo é o mesmo da cerca digital e da varredura de torres, isto é, identificação de autoria com vestígios digitais, mas o tipo de informação buscada é diferente.

Para delimitar a busca, usou-se parâmetros de busca com potencial relação ao crime:

---

[576] BRASIL. Superior Tribunal de Justiça. RMS 60.698/RJ, 2019.

“Marielle Franco”, “Vereadora Marielle”, “Agenda Vereadora Marielle”, “Casa das Pretas”, “Rua dos Inválidos, 122” e “Rua dos Inválidos”. Assim, os usuários do buscador que tivessem realizado pesquisas semelhantes em datas próximas ao fato-crime teriam o IP revelado. Tal ato foi considerado, pelos juízos de origem, como uma quebra de sigilo de dados, situação em que se confunde o efeito jurídico com o ato efetivamente praticado, como vem sendo demonstrado ao longo da tese. A quebra de sigilo é uma consequência relativa ao instrumento (o sigilo), e não ao direito fundamental propriamente dito, que é o da autodeterminação informacional.

Superando-se a argumentação de que o Marco Civil da Internet possibilita a requisição judicial coletiva de metadados de comunicação, que está no centro do entendimento majoritário do STJ, o artigo 22 da referida lei delimita quais tipos de dados podem ser acessados: especificamente os “registros de conexão” e os “registros de acesso a aplicações de internet”. Vale mencionar que a referida legislação determinou o conteúdo legal desses termos:

> [...] Art. 5º Para os efeitos desta Lei, considera-se: VI - registro 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; VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.

A partir da definição legal e conforme já exposto na tese, o dispositivo em questão permite o acesso a metadados de comunicação, isto é, ao conjunto de informações que funcionam como o “envelope” necessário ao envio de dados. Não é necessária qualquer interpretação especializada para compreender que parâmetros de busca não se enquadram em informações de data, hora e duração da conexão vinculadas a dispositivos eletrônicos. Ao contrário, no caso concreto, o que se pretende é identificar, com base no conteúdo da busca, o local em que ela foi realizada.

A busca pelos parâmetros usados em buscador online é reveladora dos dados comunicacionais dos usuários da internet, ou em outra nomenclatura, dados de tráfego. Essa informação, mesmo que analisada estaticamente, deve ser protegida como dado de conteúdo, na medida em que revela dados sensíveis ou permite inferências muito seguras a respeito do usuário. Para efeito de comparação legal, como visto no Capítulo 6, o pacote de provas digitais da União

Europeia aplica os mesmos requisitos de acesso para dados de tráfego e conteúdo[577].

Ademais, constata-se, no plano normativo, que o ordenamento brasileiro não conta com previsão legal de requisição judicial de dados comunicacionais armazenados em nenhuma hipótese. Da mesma forma, remora-se que não há previsão de que requisição de dados de conteúdo[578]. Essa situação jurídica decorre da utilização de um diploma legal para finalidades distintas das quais ele foi pensado e desenvolvido, isto é, como principal fundamento para intervenções informacionais coletivas na fronteira das discussões processuais penais, enquanto foi elaborado para ser um diploma das relações civis na internet.

Portanto, no que se refere às buscas coletivas em buscadores, conclui-se que a racionalidade processual brasileira opera com premissas inaplicáveis aos casos concretos, confundindo-se até mesmo a proteção jurídica estática ser garantida em cada situação. Ao nosso ver, a evidência da argumentação é a replicação da fundamentação em acórdãos e artigos para situações jurídicas completamente diversas.

Na dimensão estática, a proteção mais branda aos dados comunicacionais, equiparando-os a metadados de registro é um erro conceitual do precedente analisado. Consequentemente, na linha do marco teórico da tese, reconhecendo-se o potencial lesivo a direitos fundamentais e a ausência de previsão legal para aquisição de dados de tráfego, essa técnica especial de investigação é ilegal.

Como dito anteriormente, a situação jurídica do *Google* se assemelha a qualquer registro do pensamento humano realizado em aplicações de internet, a exemplo de dúvidas com o LLM como o *ChatGPT*. Nessa linha, há sérias dúvidas se técnica de investigação não atingiria o núcleo essencial da autodeterminação informativa, sendo possível o acesso a registros de pensamento individual, resguardado inclusive de terceiros, isto é, aquilo que nem mesmo se ousou comunicar, tal como o acesso a um diário[579]. A situação é agravada se o acesso for determinado em massa com intuito de investigação por parâmetros de busca sem suspeita penal.

Na dimensão prática, ao contrário da limitação tempo e espaço no monitoramento geográfico, que já pressupõe o uso de dispositivos no momento da infração penal, a busca por parâmetro trabalha com a dedução do que teria sido pesquisado em determinada janela temporal.

---

[577] UNIÃO EUROPEIA. Regulamento (UE) 2023/1543, Cons. 53.
[578] CORDEIRO, 2024, p. 231.
[579] A relevância da proteção da intimidade contida em informações pessoais não comunicadas, registradas em diários, chegou a dividir o Tribunal Constitucional Alemão, resultando em empate — situação em que não se declara a inconstitucionalidade em 2008. (GRECO; GLEIZER, 2019, p. 1496)

Nesse sentido, o potencial de eficácia dessa técnica investigativa deveria ser testado previamente como critério de validade do processo legislativo que a almejasse positivá-la, tendo em vista o potencial de lesão à autodeterminação informacional, o que poderia ser previsto como obrigação para medidas dessa natureza de intrusão comunicacional em metalei.

Por essas razões, a tese não formula um modelo ideal para a aplicação desse tipo de método de investigação, na medida em que há dúvidas a respeito da constitucionalidade, reforçada pela necessidade comprovação científica da efetividade do método.

7.3. Finalidade aplicada às hipóteses analógicas com suspeita de autoria

No tópico anterior, a finalidade como critério limitador dos atos de investigação foi aplicada a situações limítrofes do cenário processual penal brasileiro. Entretanto, conforme abordado anteriormente esse princípio tem conteúdo jurídico para ser aplicado em diversas situações corriqueiras da atividade policial que não são previstas legalmente ou em que há interpretações por analogia. Retoma-se resumidamente alguns discussão já realizadas para sintetizá-las no sentido de há um modelo ideal prescritivo para positivação ou para defender a impossibilidade.

A entrega voluntária de dispositivos eletrônicos às agências de investigação é uma forma comum de testemunhas e vítimas contribuírem com a investigação, que a situação jurídica mais simples a ser resolvida. Esse ato de voluntariedade deve ter a utilidade medida a partir de hipótese investigativa. Assim, caso seja necessário aplicar técnicas automatizadas de busca por elementos informativos digitais, o uso deve ser limitado àquilo que guarde relação com a liberalidade do particular de permitir o acesso, uma vez, por outra forma, depende de autorização judicial.

A situação se complexifica ao se pensar no réu-delator, que entrega voluntariamente dispositivos eletrônicos para a realização de um acordo de delação premiada. A partir da apreensão, as agências de investigação poderiam usar o material para comprovação de hipóteses criminais distintas daquela que deu origem à aquisição da informação, com uso de tecnologias da informação? A resposta deve ser que o princípio da finalidade vincula o tratamento de dados realizados que, nesse caso, engloba também a pretensão probatória de que as alegações não são verdadeiras, já que é condicionante jurídica da validade do acordo.

Todavia, esse raciocínio não encontraria aderência na jurisprudência brasileira que, por exemplo, não vislumbra ilegalidade na realização de exame de DNA com material descartado,

involuntariamente por suspeitos, sem prévia autorização judicial[580]. Entendimentos semelhantes são encontrados em decisões estrangeiras, a exemplo da orientação jurisprudencial da Suprema Corte dos Estados Unidos que não há expectativa razoável de privacidade em relação ao lixo[581]. Esse tipo de racionalidade é orientado pela utopia da busca da verdade na atividade probatória como núcleo do processo penal.

Tal padrão de racionalidade, se aplicado às provas digitais, na medida em que custódia da informação não deve significar usos múltiplos e desconectados da razão de acesso, faz com que a entrega voluntária se torne uma questão jurídica complexa. É por isso que, a partir do marco teórico, afirma-se que o núcleo cognitivo do processo é as garantias processuais, o que justifica o esforço da tese racionalizar como dos dados pessoais ingressam no processo e como devem ser utilizados, observando-se a presunção de inocência como foco desses atos.

Avançando para situações jurídicas mais controversas, é necessário retomar a apreensão de dispositivos eletrônicos como fonte de prova. Como já exposto, essa apreensão pode ocorrer mediante autorização judicial prévia ou em decorrência de busca pessoal em situação de flagrante, bem como durante o cumprimento de mandado de busca. O que distingue essas hipóteses é o momento da intervenção judicial, partindo-se do pressuposto da imprescindibilidade da reserva de jurisdição para o acesso a provas digitais *offline*. Em ambos os cenários, contudo, a decisão judicial cumpre a mesma função no tocante à delimitação da finalidade.

Desse modo, o modelo ideal para a busca digital *offline* exige a vinculação entre a autorização judicial e a hipótese investigativa, devendo a decisão conter, como elemento indispensável, a justificativa para o rompimento das barreiras de segurança do dispositivo. Nessa perspectiva, a autorização para análises automatizadas dos dados armazenados permanece estritamente subordinada ao que foi solicitado pelas agências de persecução e deferido pelo juízo. O racional dos atos investigativos e sua necessária repetibilidade técnica funcionam, assim, como critérios de admissibilidade na ação penal, de modo a demonstrar, além da observância da cadeia de custódia, o respeito à finalidade no uso e no reúso de dados pessoais, cuja materialização deve gerar, nos casos concretos, relatórios de investigação obrigatórios legalmente.

Na mesma linha, a positivação de uma disciplina das provas digitais deve ter como um dos principais objetos as requisições de dados, na medida em que funcionam como uma relevante forma

---

[580] BRASIL. Superior Tribunal de Justiça. Habeas Corpus 354.068, 2016.
[581] ESTADOS UNIDOS. Suprema Corte. California v. Greenwood. U.S. Reports, Washington, D.C., v. 486, 1988.

de ingressos de elementos informativos digitais na investigação preliminar. As normas com essa finalidade devem identificar claramente os destinatários da norma (empresas, órgãos públicos, particulares etc.) e os limites penais autorizadores (gravidade da infração penal) e o uso lícito permitido após o acesso aos dados. Como dito anteriormente, a redação do art. 13-B do CPP é um bom exemplo de norma processual que atenderia a esses critérios.

Conforme se argumentou extensamente, a proteção jurídica não deve depender somente do tipo de dado analisado estaticamente, isso significa que, mesmo para as informações menos protegidas do ordenamento jurídico, as cadastrais, é necessário o respeito à essa finalidade. Como dito, a consolidação e uso de dados cadastrais de diversas fontes pode permitir inferências sobre dados sensíveis das pessoas investigadas, que a depender do espaço amostral, podem revelar informações tão graves quanto ou mais do que dados de conteúdo. Por outro lado, o interesse do Estado em identificar civilmente suspeitos com base nesses dados deve ser amparado.

A imposição da finalidade como critério limitador, nessa hipótese, proíbe qualquer uso distinto da identificação de informações civis básicas (nomes, parentescos e endereços). O resultado é que o rebaixamento do critério de acesso, geralmente por requisição administrativa, deve vir acompanhada da limitação para o uso óbvio dessas informações. Pode parecer alarmista o reconhecimento de riscos, mas a automatização de atividades diárias pode ser vetor de utilização de dados facilmente adquiridos para situações diversas do que verificação de informações cadastrais, de modo a ser necessária a referida limitação.

A requisição de dados de deslocamento prevista na Lei das Organizações Criminosas, apesar de se tratar de dado de conteúdo, uma vez que permite saber onde determinada pessoa esteve, deve receber proteção jurídica semelhante à que foi defendida acima. Isso evidencia que o debate sobre os limites jurídicos não deve se orientar prioritariamente pelo *nomen iuris* do tipo de dado. Entretanto, os argumentos pressupõem que o uso esteja limitado a uma hipótese com suspeito determinado, ou seja, violaria a finalidade a requisição a todas as companhias aéreas e empresas de ônibus de cidade específica pelo prazo máximo legal, caso não houvesse demonstração da necessidade num caso concreto. Nota-se que o objetivo não pode ser formar um repositório de informações que sirva para qualquer situação, mas atender a uma finalidade delimitada.

Por essa razão, não é admissível uma busca coletiva de todos os passageiros que fizeram a rota de “x” para “y” em determinado intervalo de tempo. Primeiro, a lei não autorizou que o ato investigativo fosse realizado de forma coletiva. Segundo, porque a quantidade e variedade de dados

acessados alteram a possibilidade de inferências possíveis, de modo a receber proteção jurídica mais elevada, conferida aos dados de conteúdo.

Com base nas mesmas premissas expostas acima, o uso de dados pessoais obtidos por requisição deve ser acompanhado da elaboração de relatório de investigação que detalhe as fases de tratamento, de modo a permitir a replicabilidade e a verificação da finalidade. Tomando-se como exemplo a geolocalização em caso de sequestro, já prevista em lei, o resultado seria: o relatório deve indicar quais empresas de telefonia e serviços telemáticos foram requisitadas, quais delas forneceram efetivamente dados úteis e qual foi a progressão do tratamento que permitiu identificar o local onde o suspeito ou a vítima se encontravam.

Todos os aspectos mencionados podem produzir efeitos extraterritoriais, considerando-se o local das sedes empresas que custodiam ou armazenam os dados pessoais. Nessas situações, a solução adequada é a utilização de mecanismos de cooperação jurídica internacional para acesso à elementos de informação, denominados atos próprios de cooperação, pois visam à instrução probatória. Para esses atos cooperacionais, deve-se observar, por analogia, o princípio da especialidade, que é positivado na Lei da Imigração[582]: o Estado deve utilizar os elementos informativos recebidos para comprovação das hipóteses descritas no pedido de cooperação.

Entretanto, como demonstram as legislações estrangeiras e da prática judicial brasileira, a tendência é que as empresas sejam obrigadas a cumprir ordens judiciais de para abertura de informações com base no critério do local da prestação de serviços. Contudo, como já abordado, o ordenamento brasileiro não prevê a requisição de dados de conteúdo, e qualquer prescrição legal nesse sentido enfrentaria o obstáculo do desconhecimento prévio do tipo, da variedade e da quantidade de informações que podem ser disponibilizadas pelas empresas. Basta abstrair, por exemplo, que o dado cedido pode ser proveniente de um *smart watch* ou localizador.

A discussão sobre o alcance jurisdicional para obrigar empresas a cumprir ordens em território nacional foge ao objeto da tese, mas é relevante e condiciona a efetividade do modelo proposto para a disciplina das provas digitais. Dito isso, caso se confirme a tendência de adoção da territorialização ficta dos dados, as empresas devem entregar as informações, que devem ser mais precisas quanto possível para que se evite abertura desnecessária de informações. Além disso, o

---

[582] "Art. 96. Não será efetivada a entrega do extraditando sem que o Estado requerente assuma o compromisso de: I - não submeter o extraditando a prisão ou processo por fato anterior ao pedido de extradição". BRASIL. Lei nº 13.445. Art. 96

emprego de técnicas automatizadas de investigação fica condicionado à hipótese autorizada na decisão judicial, para a qual a verificação posterior da observância finalidade dever ocorrer por meio de relatório de investigação, conforme os critérios de validade discutidos neste tópico.

Ademais, atualmente os relatórios de impacto dos pedidos provenientes de autoridades de persecução são produzidos pelas empresas privadas, por iniciativa própria, o que revela o grau de ausência normativa que incide sobre o tema desta tese. Apesar não tratar dos efeitos jurídicos da finalidade, uma lei geral de proteção de dados para o âmbito público deverá impor às agências de persecução a obrigação de elaborar relatórios anuais contendo o número requisições, pedidos atendidos, entre outras informações, como forma de controle coletivo e difuso atividade policial.

O último aspecto que merece atenção sobre o princípio da especialidade é sua aplicação na infiltração digital, que não deve ser confundida com a autorização para utilização de *malware* ou qualquer meio que permita a vigilância *online* automática, para a qual não haverá prescrições por ser inconstitucional[583]. Nesse contexto, a finalidade opera efeitos limitados, uma vez que a interação humana entre o agente infiltrado é marcada pela dinamicidade da relação digital e pela impossibilidade de antecipação dos resultados.

Em conclusão, a finalidade, como limite do dispositivo processual penal, possui conteúdo jurídico apto a evitar desvios no uso das informações obtidas na investigação preliminar. Trata-se de um critério normativo que se ajusta dinamicamente à hipótese investigativa: a utilidade das informações deve corresponder ao que as agências de persecução declararam como necessidade para obter o acesso aos suportes eletrônicos ou bases de dados. Por essa razão, a elaboração de relatórios de investigação que assegurem a repetibilidade técnica dos atos realizados com tecnologias da informação deve constituir condição de admissibilidade desses elementos na ação penal, funcionando como metaprova de validade dos atos investigativos e permitindo um controle que ultrapassa a mera classificação estática do tipo de dado.

Além disso, a vigilância automatizada e em tempo real de *malware* não foi incluída nas propostas prescritivas de modelo ideal devido à sua dificuldade inerente em ser limitada para proteger a privacidade, levantando sérias preocupações de inconstitucionalidade.

---

[583] PRADO, 2024, p. 106.

CONCLUSÃO

A racionalidade jurídico-processual brasileira é adequada para assegurar a licitude da aquisição, uso e reúso de dados pessoais no âmbito processual penal, em observância do princípio da finalidade? A resposta à pergunta de pesquisa é negativa.

Primeiramente, a análise ontológica do ordenamento processual brasileiro conduz ao entendimento que a previsão legal de normas jurídicas para lidar com os elementos de prova digital é excepcional, sendo as requisições esparsas de dados os únicos casos previstos na legislação. No primeiro caso, a inobservância na aquisição decorre do uso por analogia de procedimentos concebidos para provas analógicas, em que dispositivos eletrônicos são analisados como quaisquer objetos. Em relação às requisições, a proteção jurídica é conferida estaticamente, pelo tipo de dado, e não exige observância da finalidade no primeiro uso na investigação preliminar.

As ações de reúso de dados da segurança, isto é, aquelas primeiramente vinculadas à prevenção de perigos, também não observam o princípio da finalidade. Tal constatação decorre da unidade informacional entre os sistemas de segurança. Portanto, a dimensão institucional da autodeterminação informacional – a separação por finalidade legal – não é observada no ordenamento brasileiro. As agências de prevenção de perigos e as agências repressivas utilizam simultaneamente sistemas que permitem rastreamento individual e vigilância coletiva, tornando impossível identificar o ingresso do elemento de informação na investigação preliminar.

O reúso de informações da segurança pública na persecução criminal constitui uma intervenção informacional que não observa o princípio da finalidade, dificultando inclusive a descrição do compartilhamento em razão dos usos conjuntos.

As Técnicas Especiais de Investigação são exemplos de reúso de dados pessoais, na medida em que se concentram em informações colhidas para ações da vida cotidiana alheias à persecução penal. Neste particular, o ordenamento não contém normas que possibilitem o acesso coletivo a dados pessoais de pessoas indeterminadas para identificar a autoria de crimes graves. Este uso não se adequa ao princípio da finalidade no tratamento de dados; ao contrário, é a evidência de que o reúso de informações não é analisado como uma nova intervenção informacional.

Após oferecer uma resposta de forma mais objetiva, a tese retoma os fundamentos centrais expostos, com foco nos pontos essenciais da trajetória de pesquisa. Agora, esses elementos são apresentados em uma lógica lusófona de conclusão argumentativa, partindo dos fundamentos para

se alcançar a conclusão.

O problema de pesquisa surgiu da inquietação sobre a possibilidade de utilização de tecnologias da informação para usos automatizados de dados pessoais sem vinculação à hipótese investigativa, quando o acesso das agências de persecução ocorreu por razão diversa da implementada. A partir dela, iniciou-se uma jornada de pesquisa para compreender o problema identificado, que perpassou características das tecnologias da informação, especialmente conectadas às capacidades de processamento de alto volume de dados, os riscos envolvidos na vigilância digital e como as tradicionais categorias das ciências criminais as analisam.

Esta tese começa com a descrição de como os dispositivos de controle da sociedade disciplinar foucaultiana transcenderam os aspectos físicos a uma arquitetura informacional do Estado para segurança pública, apoiada em estratégias da sociedade do controle com o objetivo de produzir dados para predição e gestão de riscos, desconectada dos valores jurídicos[584]. Esse fenômeno deve ser analisado conjuntamente ao histórico de críticas à criminologia atuarial que, muito antes da moderna capacidade de processamento, identificou o deslumbramento dos criminólogos cientificistas com o cálculo atuarial para prevenção de riscos penais[585].

Atualmente, é crível falar em uma arquitetura, até mesmo física, construída para registros de dados pessoais, racionalizada pelos medos e riscos da sociedade moderna, em que a aparência das cidades é completamente alterada por dispositivos informáticos de registro de informações. Não surpreende, nesse contexto, que as bases para a análise das *smart cities* tenham partido de pesquisas geográficas de Melgaço, as quais verificam a racionalização de cidades pelo medo da insegurança, o que gera como resultado a legitimação prática da vigilância pelo Estado e particulares, sem o amparo em discussões de limites democráticos para tais ações[586].

A ideia de prevenção à criminalidade é usada para justificar uma sociedade de registros informacionais como dispositivos de controle; esta é a principal constatação criminológica que decorre do percurso realizado no Capítulo 1 da tese. No entanto, os debates democráticos devem ser estudados transversalmente nas organizações do Estado, o que foi apresentado no texto como um espaço de decisões de política criminal informacional, cujo ponto central é que a implementação de tecnologia na segurança pública é uma decisão, e não somente uma acomodação

---

[584] GARLAND, 2001, p. 175.
[585] FEELEY; SIMON, The New Penology, 1992, p. 449-474,
[586] MELGAÇO; VAN BRAKEL, 2021, p. 245-246.

de inovação pelo Estado ou um mal necessário da atual quadra histórica.

É nesse espaço político que a arquitetura informacional deve ser escrutinada. A primeira etapa consiste em orientar o processo legislativo com base em métodos de controle externo exercidos pela sociedade civil e pela academia, além de estar fundamentada em evidências científicas. Também deve ser prevista a obrigatoriedade de controlar a arquitetura de dados pela adequação funcional das técnicas que se pretendam implementar. No plano normativo, a decisão de política criminal deve levar em consideração os princípios de proteção de dados, tanto da experiência brasileira quanto da internacional, de modo a limitar os riscos de vigilantismo como estratégia de prevenção.

A contribuição da tese para o campo é o aprofundamento do potencial normativo do princípio da finalidade no tratamento de dados em duas dimensões de contribuição à política criminal informacional: a vinculação dos agentes de tratamento ao uso que justificou juridicamente a coleta do dado e, na dimensão institucional, permite a prescrição da separação institucional de funções estatais, especificamente entre a segurança pública e a persecução penal.

Ademais, a tese também contribui com a descrição conceitual das bases jurídicas em três tipos: as privadas, as privadas criadas por dever legal e as bases públicas, na medida em que cada uma se conecta à investigação preliminar de uma forma diversa. O aprofundamento de pesquisas com essa diferenciação pode ser útil para formalizações de teses gerais em um modelo de provas digitais, o que é raro nessa temática, em que as proposições são pontuais e fragmentadas.

A identificação de quem realiza a coleta permite identificar o uso primário. Ao se tratar das bases públicas de segurança pública, tal uso é o preventivo, com olhar para o futuro para a manutenção da ordem pública, evitando perigos a bens jurídicos tutelados, antes da existência da suspeita penal. Após o cometimento de uma infração penal, a categoria de suspeição passa a ser útil sistemicamente, de modo que os dados da segurança pública devem fluir da segurança para as agências de persecução criminal – compartilhamento de dados –, efetivando-se o reúso lícito de dados preventivos para a função repressiva.

A realidade não está próxima dessa prescrição. Ao contrário, a tese identificou sistemas unificados de informações sob gestão do SUSP, tal como o Córtex, que mesclam diversas agências que cumprem funções legais distintas para usarem os dados conjuntamente. Aliás, esse é precisamente o racional de política criminal que justificou a criação do sistema único. Assim, pode-se concluir unicidade informacional é a regra, com a consequente inobservância da separação de

poderes na gestão informacional. Em síntese, esse estado de coisas justifica a afirmação de que a arquitetura informacional adota um modelo de governança fundamentado na unidade informacional, o que, em linha com o marco teórico, é inconstitucional.

Realizando-se uma comparação do modelo brasileiro com o modelo alemão, do qual se partiu no marco teórico da tese, especificamente o modelo de duas portas, pode-se dizer que o SUSP é uma porta única, na qual as agências de segurança pública e persecução utilizam os mesmos dados simultaneamente, dificultando inclusive definir o uso primário. Ademais, a legitimidade dos sistemas é bastante questionável, já que sua instrumentalização é realizada por decretos e portarias administrativas, o que incrementa o risco de desvios de finalidade e perseguição política.

Prescritivamente, o sistema brasileiro deve se adequar às exigências da separação institucional de funções com a formulação de hipóteses de reúso legítimo de informações de segurança pública na persecução penal. Tal assertiva deriva da afirmação principiológica de que todo uso no processo penal de informações de segurança pública é reúso de dados; o fluxo de informações da segurança para o processo é legítimo, ou seja, se o perigo não foi evitado, o Estado deve reprimir penalmente a infração penal consumada.

Em todas as outras hipóteses de reúso, especialmente o rastreamento de pessoas, individual e coletivamente, para fins probatórios do processo penal, deve-se exigir reserva de jurisdição, ressalvados os usos bagatelares, como a identificação civil. Isso porque a decisão judicial funciona como critério de definição da finalidade no reúso.

Por essas razões, a resposta de pesquisa é negativa sobre a observância da finalidade no compartilhamento entre agências de persecução e segurança pública.

Os capítulos 4 e 5 analisaram os atos de investigação, incluindo os meios de obtenção ocultos e a cooperação jurídica internacional, permitindo identificar o estado da arte da racionalidade processual penal brasileira a respeito das categorias dogmáticas aplicadas aos elementos probatórios digitais. O resultado desses capítulos descritivos é a constatação da ausência de sistematização de procedimentos pensados a partir dos aspectos inerentes da produção de provas digitais, que se consubstancia na utilização por analogia de conceitos e entendimentos jurisprudenciais.

Ficou demonstrado que a apreensão de dispositivos eletrônicos para obtenção de provas digitais estáticas é equiparada, para todos os efeitos legais, a itens corpóreos, com desconsideração do potencial epistêmico que pode ser extraído deles, ou seja, não são consideradas uma intervenção

informacional. Como abordado, o grau de invasividade diferencia-se ontologicamente pela escala e volume de informações encontradas, o que retira a discussão dos tradicionais sigilos a serem protegidos para a configuração de uma intervenção na autodeterminação informacional que, enquanto garantia fundamental, exige lei materialmente válida para ser flexibilizada.

Essas justificações jurídicas se aplicam a todas as situações jurídicas narradas em que as agências de persecução apreendem dispositivos eletrônicos, mas a apreensão jurídica recai sobre os dados armazenados sem prévia decisão judicial, isto é, nas apreensões decorrentes de buscas pessoais, entrega voluntária e encontro no local do crime. Nessas situações, considerando-se a dinamicidade das hipóteses de investigação, o modelo ideal proposto pode ser resumido pela seguinte equação: autorização judicial para o rompimento da barreira de segurança + uso lícito automatizado conforme a hipótese que originou a decisão judicial + produção de relatório de processamento com descrição das ferramentas e parâmetros que garantam repetibilidade, cujo resultado é a admissibilidade do resultado na ação penal. As duas primeiras parcelas da soma podem estar em uma única decisão judicial ou podem ocorrer em momentos distintos, diante da descoberta de novas informações que alterem ou aprofundem as hipóteses investigativas.

Nas hipóteses em que a apreensão é autorizada previamente por decisão judicial, ou seja, utilizada no curso da investigação como meio de obtenção de provas, soma-se ao modelo acima a autorização judicial expressa da apreensão de dispositivo eletrônico.

A análise descritiva do ordenamento também identificou em larga escala a aplicação de requisições de dados a empresas, que visam as bases privadas e as privadas criadas por dever legal. Nesse particular, há alterações legislativas esparsas no Marco Civil da Internet, na Lei das Organizações Criminosas, no Estatuto da Criança e do Adolescente e no Código de Processo Penal, que criam permissões legais não sistematizadas para requisição de informações. Diferentemente das demais situações jurídicas processuais identificadas na tese, há normas específicas que tratam do uso de dados pessoais na investigação preliminar.

O exame dos dispositivos sobre requisição de dados revela que a proteção jurídica é conferida estaticamente, isto é, pelo *nomen iuris*. Por exemplo, a regra geral é que o acesso a dados cadastrais seja realizado sem reserva de jurisdição, mas, como argumentado, essa proteção jurídica só é efetiva se a finalidade de tratamento for a identificação civil. Ainda que pareça redundante, deve-se exigir que os dados cadastrais sejam usados com a finalidade de identificação cadastral, o que significa que qualquer outro uso é ilícito. Não há dados inúteis e, a depender do entorno de

informações, um dado cadastral pode ser mais revelador que dados de conteúdo[587], logo, a vinculação do dado à finalidade garante uma proteção jurídica dinâmica.

Se as afirmações acima servem para os dados menos protegidos do ordenamento, com mais razão se aplicam a metadados que permitam rastreamento e vigilância individualizados. O exemplo inaugurado pelo artigo 13-B do Código de Processo Penal é muito positivo, uma vez que é exemplificativo de um modelo ideal, que exige a identificação pelo tipo de dado pessoal, os destinatários da norma, o limite penal e a finalidade do processamento a ser realizado pelas agências de persecução penal. Por esse motivo, ele serviu de base para se abstrair o modelo proposto para a requisição de dados pessoais, protegidos dinamicamente.

De modo mais amplo, a disciplina das provas digitais deve observar um modelo ideal que esse artigo respeita: setor de coleta (destinatário da norma) + hipótese de acesso pelos órgãos de persecução + uso lícito permitido ao investigador = elemento informativo válido. No caso do artigo da requisição para geolocalização, as parcelas da soma são: empresas de telefonia e comunicação + acesso a metadados telemáticos e telefônicos + uso para localizar suspeito ou vítima para os crimes específicos, o que culmina em atos de investigação válidos processualmente.

Em relação ao problema de pesquisa, a racionalidade processual reconhece a necessidade de que as requisições de dados sejam previstas legalmente e não está ancorada na analogia a regras para situações analógicas, afastando-se da lógica da apreensão nesse particular. Entretanto, ainda é aplicado um racional estático, o que, em casos limítrofes, pode representar riscos à autodeterminação informacional. Portanto, a resposta é negativa: o princípio da finalidade não é utilizado como limitador do uso dos dados requisitados e, de modo geral, o reúso não é visto como uma nova intervenção informacional na sistemática brasileira.

Talvez, a situação mais grave, em termos de diagnóstico, seja o padrão de utilização de dados de conteúdo, na medida em que não há autorização para essa intervenção informativa; em outras palavras, não há previsão para esse tipo de requisição[588]. Ainda que a tese tenha identificado decisões que superam a ideia de dados armazenados e em fluxo[589], que serve para justificar a inaplicabilidade da lei das interceptações telefônicas, o fato é que isso não supera a ausência de hipótese legal. Essa situação é peculiar: o legislador alterou o ordenamento para permitir a

---

[587] EILBERG, 2024, p. 29-54.
[588] CORDEIRO, 2024, p. 231.
[589] BRASIL. Supremo Tribunal Federal. 2020, HC 168.052/SP; BRASIL. Superior Tribunal de Justiça. 2016, HC 51.531/RO.

requisição de dados cadastrais, mas não há previsão para intervenção informacional mais grave.

A dogmática majoritária e o entendimento consolidado jurisprudencial são no sentido da necessidade de observância da reserva de jurisdição, o que é um acerto, tal como observado no Tema 977 do STF[590], mesmo que a hipótese seja para casos de apreensão. Consequentemente, todos os critérios que legitimam a requisição de dados de conteúdo a empresas de tecnologia são retirados de decisões judiciais que não vinculam os atos de investigação posteriores à hipótese investigativa, ou seja, não integram o princípio da finalidade ao dispositivo processual penal.

O Estado-penal não pode depender da cooperação voluntária de empresas para o exercício do poder punitivo, de modo que essa solução é inadequada: as empresas são obrigadas ou não. Se a escolha de política criminal for pela necessidade de requisitar dados de conteúdos de empresas de tecnologia, ela deve ser realizada com consciência situacional das consequências, o que passa necessariamente por discussões sobre a territorialização dos dados como estratégia processual penal. Nesse sentido, os modelos americano e da União Europeia foram abordados para que sirvam de base comparativa para a decisão política de implementar uma solução semelhante.

Reafirma-se que essa decisão política não cabe ao STF e, ainda que o fundamento do ADC 51[591], sobre a territorialização dos dados como critério de aferição jurisdicional, seja respaldado na Convenção de Budapeste, que ainda não levou às adequações necessárias do ordenamento brasileiro, ele cria hipóteses investigativas não previstas na legislação. Isso porque o artigo 18 da referida convenção internaliza o compromisso de alterar o ordenamento, mas não o altera diretamente, a ver-se pela redação da norma: "Cada Parte adotará as medidas legislativas"[592]. Mesmo que esse argumento pudesse ser superado, é inegável que o referido precedente criou uma hipótese investigativa não positivada no ordenamento: a requisição de dados de conteúdo.

Nesse contexto, no que se refere à pergunta da tese, ela somente pode ser respondida com os critérios jurisprudenciais criados, que também integram a racionalidade processual como objeto de análise. Dessa forma, os *leading cases* observados não vinculam o uso, após o acesso às informações de conteúdo, pela finalidade de tratamento, de modo que a resposta é negativa.

O último ponto é o diagnóstico da validade da utilização das técnicas especiais de investigação para identificação de autoria, especificamente a varredura de torres e o cercamento

---

[590] BRASIL. Supremo Tribunal Federal. 2025. Tema 977.
[591] BRASIL. Supremo Tribunal Federal. 2023. ADC 51.
[592] BRASIL. Decreto n.º 11.491, 2023. Art. 18.

digital. Os artigos 22 e 23 do Marco Civil da Internet não devem ser utilizados como fundamento para coleta coletiva com objetivo de identificação de autoria, na medida em que as normas se destinam teleologicamente à identificação do usuário já conhecido na rede, o "fulano123" no *Instagram.* Além disso, a afirmação dos precedentes do STJ de que a norma não exige identificação é incorreta pela razão explicada acima e pela utilização do racional das cautelares penais que presumem o conhecimento do suspeito para técnicas que objetivam identificar suspeitos com rastros digitais[593]. No atual estágio do ordenamento, não há autorização para essas técnicas.

Um modelo que autorize essas técnicas tem que observar os seguintes critérios: i) existência de autorização expressa para requisição de dados coletivamente, definida por critérios objetivos de limitação (tempo e espaço); ii) o ato de investigação deve almejar finalidade autorizada legalmente (rastreamento em tempo real, retrospectivo, identificação da autoria)[594]; iii) reserva de jurisdição; iv) limite penal para investigação de crimes graves; v) entidades públicas e privadas obrigadas pela lei a cederem dados coletados para outros fins. Naturalmente, trata-se de uma escolha de política criminal, de modo que a inércia não pode ser lida como autorização tácita.

Em relação à utilização dos parâmetros de busca do *Google,* o precedente do STJ também defendeu a aplicabilidade dos artigos 22 e 23 do Marco Civil da Internet nos mesmos termos que foram acima[595]. Contudo, a situação jurídica de fato não é idêntica, sem observar as definições do artigo 5º da mesma lei. Nesse sentido, a decisão confunde dados de tráfego com metadados de comunicação, o que permite a aplicação dos referidos artigos para situação distinta.

No plano normativo, o ordenamento brasileiro não conta com previsão legal de requisição judicial de dados comunicacionais armazenados em nenhuma hipótese e, somente por essa razão, a intervenção em questão não pode ser implementada. Em relação às prescrições, a tese não apresenta formulações para o uso desse tipo de método de investigação, na medida em que há dúvidas a respeito da constitucionalidade, reforçada pela necessidade de comprovação científica da efetividade do método, especificamente a eficácia da presunção de palavras-chave.

Por fim, a hipótese de pesquisa foi confirmada: a racionalidade processual penal brasileira

---

[593] BRASIL. Superior Tribunal de Justiça. 2019, RMS 61.302/RJ; BRASIL. Superior Tribunal de Justiça. 2019 RMS 62.143/RJ.

[594] A autorização para a aquisição de dados, especialmente em volume e correlacionados, não deve ser tacitamente entendida como permissão para qualquer uso. Em um modelo de estrita legalidade para técnicas especiais de investigação, a finalidade da coleta deve ser expressamente definida no instrumento autorizador, limitando o tratamento e o aproveitamento probatório dos dados obtidos.

[595] BRASIL. Superior Tribunal de Justiça. 2019, RMS 60.698/RJ.

não analisa a finalidade como um critério limitador para a utilização de dados pessoais para a pretensão como objeto da pretensão acusatória, em nenhuma das fases do ciclo de vida das informações digitais. Desse modo, pode-se afirmar que tal norma não engloba o dispositivo processual brasileiro para o controle do poder punitivo na era digital.

REFERÊNCIAS

ABRAHA, Halefom H. Regulating law enforcement access to electronic evidence across borders: the United States approach. **Information & Communications Technology Law**, [S. l.], v. 29, n. 3, 2020. Disponível em: https://www.tandfonline.com/doi/epdf/10.1080/13600834.2020.1794617?needAccess=true. Acesso em: 10 jun. 2024.

ABREU, Jacqueline de Souza. Comunicação de dados, não dados em si: origens e problemas do atual paradigma de proteção constitucional do sigilo de dados. **Revista de Investigações Constitucionais**, [S. l.], v. 11, n. 1, p. e256, 2024. DOI: 10.5380/rinc.v11i1.89280. Disponível em: https://revistas.ufpr.br/rinc/article/view/e+256. Acesso em: 5 out. 2025.

ABREU, Jacqueline de Souza. Guarda obrigatória de registros de telecomunicações no Brasil: sobre as origens da retenção de dados e as perspectivas para direitos fundamentais. *In*: SIMPÓSIO INTERNACIONAL LAVITS, 4., 2016, Buenos Aires. **Anais** [...]. Buenos Aires: [s.n.], 2016. Disponível em: https://lavits.org/wp-content/uploads/2017/08/P5_De_Souza_Abreu.pdf. Acesso em 12 mar. 2025.

AGUIAR, Thaís *et al*. **Rastreabilidade, metadados e direitos fundamentais: nota técnica sobre o Projeto de Lei 2630/2020**. São Paulo: Data Privacy Brasil, 2021. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2022/04/dpbr_ong_nota-tecnica_plfakenews.pdf. Acesso em: 10 dez. 2023.

ALMEIDA, Eduarda Costa. Os grandes irmãos: o uso de tecnologias de reconhecimento facial para persecução penal. **Revista Brasileira de Segurança Pública**, [S. l.], v. 16, n. 2, p. 264–283, 2022. DOI: 10.31060/rbsp.2022.v16.n2.1377. Disponível em: https://revista.forumseguranca.org.br/rbsp/article/view/1377. Acesso em: 4 jan. 2025.

ALVES, Daniel Bento. Uso de malware em investigação criminal. **Actualidad Jurídica Uría Menéndez**, Lisboa, n. 47, 2017. Disponível em: https://www.uria.com/documentos/publicaciones/5655/documento/AJUM-47-001.pdf?id=7642&forceDownload=true. Acesso em: 3 dez. 2025.

AMNISTIA INTERNACIONAL. **Ban the Scan**. Londres: Amnesty International, 2021.

ANDERSON, Terence; TWINING, William; SCHUM, David A. **Analysis of Evidence: How to Do Things with Facts**. 2. ed. New York: Cambridge University Press, 2005.

ANDRADE, Manuel da Costa. Métodos ocultos de investigação (Plädoyer para uma teoria geral). *In*: **Que futuro para o Direito Processual Penal?**: simpósio em Homenagem a Jorge de Figueiredo Dias. Coimbra: Coimbra Editora, 2009.

ANDRADE, Manuel da Costa. **Sobre as proibições de prova em processo penal.** Coimbra: Coimbra Editora, 2013.

ARAS, Vladimir. Cerco Digital (*Geofence*) e Varredura Terminológica: Balizas Constitucionais e Legais. *In*: SALGADO, Daniel de Resende; BECHARA, Fábio Ramazzini; GRANDIS, Rodrigo de (Coord.). **10 Anos da Lei das Organizações Criminosas**: Aspectos Criminológicos, Penais e Processuais Penais. São Paulo: Almedina, 2023.

AZEVEDO, Cynthia Picolo Gonzaga de *et al*. **Nota técnica**: análise comparativa entre o anteprojeto de LGPD penal e o PL 1515/2022. Belo Horizonte: Instituto de Referência em Internet e Sociedade (IRIS); Brasília: Laboratório de Políticas Públicas e Internet (LAPIN), 2022. Disponível em: https://irisbh.com.br/publicacoes/analise-comparativa-entre-o-anteprojeto-de-lgpd-penal-e-o-pl-1515-2022/. Acesso em: 07 out. 2023.

BADARÓ, Gustavo. Editorial dossiê "Prova penal: fundamentos epistemológicos e jurídicos". **Revista Brasileira de Direito Processual Penal**, [S. l.], v. 4, n. 1, p. 43–80, 2018. DOI: 10.22197/rbdpp.v4i1.138. Disponível em: https://revista.ibraspp.com.br/RBDPP/article/view/138. Acesso em: 7 nov. 2025.

BADARÓ, Gustavo Henrique. **Ônus da prova no Processo penal**. 1. ed. São Paulo: Revista dos Tribunais, 2003.

BADARÓ, Gustavo Henrique. **Processo Penal**. 2. ed. Rio de Janeiro: Elsevier, 2013.

BADARÓ, Gustavo Henrique Righi Ivahy. O valor probatório do inquérito policial. *In*: Polícia e investigação no Brasil. Tradução. Brasília, DF: Gazeta Jurídica, 2016.

BARRETO, Alana Maria Passos; DIAS, Clara Angélica Gonçalves Cavalcanti. A EXPOSIÇÃO DA PRIVACIDADE DIANTE DA FALTA DE TRANSPARÊNCIA: UM ESTUDO SOBRE O CÓRTEX. **Interfaces Científicas - Humanas e Sociais**, *[S. l.]*, v. 10, n. 1, p. 707–719, 2023. DOI: 10.17564/2316-3801.2023v10n1p707-719. Disponível em: https://periodicos.grupotiradentes.com/humanas/article/view/11767. Acesso em: 5 nov. 2025.

BASSIOUNI, M. Cherif. **International Extradition**: United States Law and Practice. 6. ed. Oxford: Oxford University Press, 2014.

BECK, Ulrich. **Risikogesellschaft**: auf dem Weg in eine andere Moderne. Frankfurt am Main: Suhrkamp, 1986.

BENGART, Aaron A. Always a suspect: law enforcement's violative use of geofence warrants and geolocation data in criminal investigations and proceedings. **Cardozo International & Comparative Law Review**, New York, v. 7, n. 2, p. 639-674, 2024. Disponível em: https://larc.cardozo.yu.edu/ciclr-online/80/. Acesso em: 07 mar. 2025.

BENNETT, Colin J.; RAAB, Charles D. T**he Governance of Privacy**: Policy Instruments in Global Perspective. Cambridge: MIT Press, 2006.

BERENGAUT, Alexander A.; LENSDORF, Lars. The CLOUD Act at Home and Abroad. **Computer Law Review International** (CRi), [S. l.], v. 20, n. 4, 2019. Disponível

em:https://www.cov.com/-/media/files/corporate/publications/2019/08/the_cloud_act_at_home_and_abroad.pdf. Acesso em: 7 dez. 2025.

BERTI, Bianca. **Ausência de proteção de dados na contratação de tecnologias de vigilância para segurança pública**. São Paulo: Transparência Brasil, 2024. Disponível em: https://www.transparencia.org.br/downloads/publicacoes/protecaodedadostecnologiasdevigilanciaparasegurancapublica.pdf. Acesso em: 03 dez. 2024.

BILGIC, Secil. Something old, something new, and something moot: the privacy crisis under the CLOUD Act. **Harvard Journal of Law & Technology**, Cambridge, v. 32, n. 1, p. 321-348, 2018. Disponível em: https://jolt.law.harvard.edu/assets/articlePDFs/v32/32HarvJLTech321.pdf. Acesso em: 07 dez. 2025.

BLAŽIČ, Borka Jerman; KLOBUČAR, Tomaž. Removing the barriers in cross-border crime investigation by gathering evidence in an interconnected society. **Information & Communications Technology Law**, [S. l.], v. 29, n. 1, 2020. Disponível em: https://www.tandfonline.com/doi/full/10.1080/13600834.2020.1705035. Acesso em: 7 dez. 2025.

BRAMAN, Sandra. **Change of State**: Information, Policy, and Power. Cambridge, Mass.: The MIT Press, 2006.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. **Diário Oficial da União**, Rio de Janeiro, 31 dez. 1940.

BRASIL. Decreto-Lei nº 3.689, de 3 de outubro de 1941. Código de Processo Penal. **Diário Oficial da União**, Rio de Janeiro, 13 out. 1941.

BRASIL. Decreto-Lei nº 3.810, de 2 de maio de 2001. Promulga o Acordo de Assistência Judiciária em Matéria Penal entre o Governo da República Federativa do Brasil e o Governo dos Estados Unidos da América, celebrado em Brasília, em 14 de outubro de 1997. **Diário Oficial da União, Brasília**, DF, 3 maio 2001.

BRASIL. Decreto-Lei nº 4.657, de 4 de setembro de 1942. Lei de Introdução às normas do Direito brasileiro. **Diário Oficial da União**, Rio de Janeiro, 9 set. 1942.

BRASIL. Decreto-Lei nº 11.491, de 12 de abril de 2023. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. **Diário Oficial da União**, Brasília, DF, 13 abr. 2023.

BRASIL. Lei nº 4.862, de 29 de novembro de 1965. Altera a legislação do imposto de renda, adota diversas medidas de ordem fiscal e fazendária, e dá outras providências. **Diário Oficial da União**, Brasília, DF, 30 nov. 1965.

BRASIL. Lei nº 6.015, de 31 de dezembro de 1973. Dispõe sobre os registros públicos, e dá outras providências. **Diário Oficial da União**, Brasília, DF, 31 dez. 1973.

BRASIL. Lei nº 7.492, de 16 de junho de 1986. Define os crimes contra o sistema financeiro nacional, e dá outras providências. **Diário Oficial da União**, Brasília, DF, 18 jun. 1986.

BRASIL. Lei nº 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. **Diário Oficial da União**, Brasília, DF, 16 jul. 1990.

BRASIL. Lei nº 8.625, de 12 de fevereiro de 1993. Institui a Lei Orgânica Nacional do Ministério Público, dispõe sobre normas gerais para a organização do Ministério Público dos Estados e dá outras providências. **Diário Oficial da União**, Brasília, DF, 15 fev. 1993.

BRASIL. Lei nº 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. **Diário Oficial da União**, Brasília, DF, 25 jul. 1996.

BRASIL. Lei nº 9.503, de 23 de setembro de 1997. Institui o Código de Trânsito Brasileiro. **Diário Oficial da União**, Brasília, DF, 24 set. 1997.

BRASIL. Lei nº 9.613, de 3 de março de 1998. Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores [...]. **Diário Oficial da União**, Brasília, DF, 4 mar. 1998.

BRASIL. Lei nº 12.681, de 4 de julho de 2012. Institui o Sistema Nacional de Informações de Segurança Pública, Prisionais e sobre Drogas SINESP [...]. **Diário Oficial da União**, Brasília, DF, 5 jul. 2012.

BRASIL. Lei nº 12.830, de 20 de junho de 2013. Dispõe sobre a investigação criminal conduzida pelo delegado de polícia. **Diário Oficial da União**, Brasília, DF, 21 jun. 2013.

BRASIL. Lei nº 12.850, de 2 de agosto de 2013. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal [...]. **Diário Oficial da União**, Brasília, DF, 5 ago. 2013.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União**, Brasília, DF, 24 abr. 2014.

BRASIL. Lei nº 13.675, de 11 de junho de 2018. Disciplina a organização e o funcionamento dos órgãos responsáveis pela segurança pública [...]. **Diário Oficial da União**, Brasília, DF, 12 jun. 2018.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, Brasília, DF, 15 ago. 2018.

BRASIL. Lei nº 13.964, de 24 de dezembro de 2019. Aperfeiçoa a legislação penal e processual penal. **Diário Oficial da União**, Brasília, DF, 24 dez. 2019.

BRASIL. Lei nº 14.129, de 29 de março de 2021. Dispõe sobre princípios, regras e instrumentos

para o Governo Digital e para o aumento da eficiência pública. **Diário Oficial da União**, Brasília, DF, 30 mar. 2021.

BRASIL. Ministério da Justiça e Segurança Pública. Portaria nº 218, de 29 de setembro de 2021. Dispõe sobre a Plataforma Integrada de Operações e Monitoramento de Segurança Pública Córtex. **Diário Oficial da União**: seção 1, Brasília, DF, ed. 186, 30 set. 2021.

BRASIL. Superior Tribunal de Justiça. **Agravo Regimental no Recurso em Habeas Corpus n. 167.634/PA**. Relator: Min. Joel Ilan Paciornik. Quinta Turma. Julgado em 15 mai. 2023. Diário da Justiça Eletrônico, Brasília, DF, 18 mai. 2023.

BRASIL. Superior Tribunal de Justiça. **Recurso em Mandado de Segurança n. 61.302/RJ.** Relator: Min. Rogerio Schietti Cruz. Terceira Seção. Julgado em 26 ago. 2020. Diário da Justiça Eletrônico, Brasília, DF, 4 set. 2020.

BRASIL. Superior Tribunal de Justiça. **Recurso Ordinário em Habeas Corpus nº 51.531/RO.** Relator: Min. Nefi Cordeiro. Sexta Turma. Julgado em 19 abr. 2016. Diário da Justiça Eletrônico, Brasília, DF, 2016.

BRASIL. Supremo Tribunal Federal. **Ação Declaratória de Constitucionalidade n° 51/DF.** Relator: Min. Gilmar Mendes. Julgado em 21 jun. 2023. Diário da Justiça Eletrônico, Brasília, DF, 28 abr. 2023.

BRASIL. Supremo Tribunal Federal. **Habeas Corpus n. 69.912/RS**. Relator para o acórdão: Min. Carlos Veloso. Tribunal Pleno. Julgado em 30 jun. 1993. Diário da Justiça, Brasília, DF, 26 nov. 1993.

BRITO CRUZ, Francisco; SIMÃO, Bárbara (org.). **Direitos fundamentais e processo penal na era digital**: doutrina e prática em debate. v. 4. São Paulo: InternetLab, 2021. Disponível em: https://www.internetlab.org.br/pt/publicacoes/direitos-fundamentais-e-processo-penal-na-era-digital-doutrina-e-pratica-em-debate-vol-4/. Acesso em: 07 dez. 2025.

BUGIATO, Caio; TRINDADE, Thiago. O Estado nas Relações Internacionais. **Revista Oikos**, Rio de Janeiro, v. 16, n. 3, 2017. Disponível em: https://revistas.ufrj.br/index.php/oikos/article/view/51981. Acesso em: 07 dez. 2025.

CASTELLS, Manuel. **A sociedade em rede**. São Paulo: Paz e Terra, 1999.

CAVOUKIAN, Ann. **Privacy by Design**: The 7 Foundational Principles. Toronto: Information & Privacy Commissioner of Ontario, 2011.

CHIAVARIO, Mario. **Diritto processuale penale**. Nuova ediz. Torino: Giappichelli, 2024.

CHRISTIN, Angèle; ROSENBLAT, Alex; BOYD, Danah. **Courts and Predictive Algorithms.** New York: Data & Society Research Institute, 2015. Disponível em: https://www.datacivilrights.org/pubs/2015-1027/Courts_and_Predictive_Algorithms.pdf. Acesso em: 16 fev. 2023.

CLARKE, Roger. **Privacy Impact Assessment**: Its Origins and Development. Computer Law & Security Review, [S. l.], v. 25, 2009. Disponível em: https://openresearch-repository.anu.edu.au/server/api/core/bitstreams/ee4a9ce6-1a72-4981-962d-d2bb814634a8/content. Acesso em: 07 dez. 2025.

COLLETT, Clementine; NEFF, Gina; GOMES, Livia Gouvea. **Os efeitos da inteligência artificial na vida profissional das mulheres**. Brasília: UNESCO: BID: OCDE, 2023. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000384693. Acesso em: 07 dez. 2025.

CORDEIRO, Pedro Ivo Rodrigues Velloso; AGOSTI, Francisco Felippe Lebrão; CAMARGO, Pedro Luís de Almeida. Repensando o encontro fortuito de provas na era digital. **Boletim IBCCRIM**, São Paulo, v. 32, n. 384, p. 21–26, 2024. DOI: 10.5281/zenodo.13834573. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1658. Acesso em: 22 mar. 2026.

BRASIL. Conselho Nacional de Justiça. Provimento nº 88, de 1º de outubro de 2019. Dispõe sobre a política, os procedimentos e os controles a serem adotados pelos notários e registradores visando à prevenção dos crimes de lavagem de dinheiro e ao financiamento do terrorismo. **Diário da Justiça Eletrônico**, Brasília, DF, n. 187, 2 out. 2019. Disponível em: https://atos.cnj.jus.br/files/original125119201910245db19e47bcb3a.pdf. Acesso em: 07 dez. 2025.

CORDEIRO, Pedro Ivo Rodrigues Velloso. O Direito Fundamental à Proteção de Dados Pessoais e a Obtenção de Dados de Provedores de Conexão e de Provedores de Aplicações de Internet no Âmbito Processual Penal. 2024. 320 f. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2024. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2137/tde-01112024-113009/en.php. Acessado em: 06 mar. 2025.

COUNCIL OF BARS AND LAW SOCIETIES OF EUROPE. **CCBE recommendations on the establishment of international rules for cross-border access to electronic evidence**. [Brussels]: CCBE, 2019. Disponível em: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20190228_CCBE-recommendations-on-the-establishment-of-international-rules-for-cross-border-access-to-e-evidence.pdf. Acesso em: 07 dez. 2025.

COUNCIL OF BARS AND LAW SOCIETIES OF EUROPE. **CCBE position on the Commission proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters**. [S. l.]: CCBE, 19 out. 2018. Disponível em: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20181019_CCBE-position-on-Commission-proposal-Regulation-on-European-Production-and-Preservation-Orders-for-e-evidence.pdf. Acesso em: 07 dez. 2025.

COUTINHO, Jacinto Nelson de Miranda. O papel do novo juiz no processo penal. *In*: COUTINHO, Jacinto Nelson de Miranda (Coord.). **Crítica à Teoria Geral do Direito Processual Penal**. Rio de Janeiro: Renovar, 2000.

COUTINHO, Jacinto Nelson de Miranda. Verdade e fake news. **Revista Brasileira de Ciências Criminais,** São Paulo, v. 199, n. 199, p. 29–51, 2023. DOI: 10.5281/zenodo.8381453. Disponível em: https://publicacoes.ibccrim.org.br/index.php/RBCCRIM/article/view/428. Acesso em: 7 dez. 2025.

CUNHA, Murilo Bastos da; CAVALCANTI, Cordélia Robalinho de Oliveira. **Dicionário de Biblioteconomia e Arquivologia**. Brasília: Briquet de Lemos, 2008.

CUNHA, José Ricardo da. *et al*. O direito das investigações digitais no Brasil: fundamentos e marcos normativos. 3. ed. São Paulo: InternetLab, 2022.

DANIELE, Marcello. La prova digitale nel processo penale. **Rivista di Diritto Processuale**, [S. l.], v. 66, n. 2, 2011.

DASKAL, Jennifer. Microsoft Ireland, the CLOUD Act, and international lawmaking 2.0. **Stanford Law Review Online**, Stanford, v. 71, p. 9-16, maio 2018. Disponível em: https://www.stanfordlawreview.org/online/microsoft-ireland-cloud-act-international-lawmaking-2-0/. Acesso em: 10 jul. 2023.

DASKAL, Jennifer. The un-territoriality of data. **The Yale Law Journal**, New Haven, v. 125, n. 2, p. 326-398, nov. 2015. Disponível em: https://www.yalelawjournal.org/article/the-un-territoriality-of-data. Acesso em: 10 jul. 2023.

DEGRAVE, Élise. **L'Etat numérique et les droits humains**. Bruxelles: Académie Royale de Belgique, 2024.

DELEUZE, Gilles. Post-scriptum sobre as sociedades de controle (1990). *In*: DELEUZE, Gilles. **Conversações.** São Paulo: Editora 34, 1992.

DEUS GARCIA, Rafael; PIZA DUARTE, Evandro. Compreendendo algoritmos aplicados ao sistema de justiça criminal – Ilegibilidade, acesso, compreensão, verdade e computabilidade no 'eu' identificado por algoritmos. **Revista Brasileira de Ciências Criminais,** São Paulo, v. 183, n. 183, 2025. Disponível em: https://publicacoes.ibccrim.org.br/index.php/RBCCRIM/article/view/1734. Acesso em: 27 mar. 2026.

DEZAN, Sandro Lúcio. Documentos e requisição direta de dados e informações pelo delegado de polícia. *In*: PEREIRA, Eliomar da Silva; ANSELMO, Márcio Adriano (Org.). **Direito Processual da Polícia Judiciária II**: os meios de obtenção de prova. Belo Horizonte: Fórum, 2020.

DEZEM, Guilherme Madeira. A Espiritualização do Domicílio: o novo conceito de domicílio e o Marco Civil da Internet. *In*: DEL MASSO, Fabiano; ABRUSIO, Juliana; FILHO, Marco Aurélio Florêncio (Coord.). **Marco Civil da Internet**: Lei 12.965/2014. São Paulo: Revista dos Tribunais, 2014.

DIAS, Fernando Gardinali Caetano. Prova cautelar, antecipada e irrepetível e o contraditório na

investigação criminal. **Revista Fórum de Ciências Criminais** (RFCC), Belo Horizonte, v. 5, n. 10, jul./dez. 2018.

DIETER, Maurício Stegemann. **Política criminal atuarial**: a criminologia do fim da história. 2012. 309 f. Tese (Doutorado em Direito do Estado) – Universidade Federal do Paraná, Curitiba, 2012. Disponível em: https://acervodigital.ufpr.br/handle/1884/28416. Acesso em: 24 mar. 2023.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. Espaço Jurídico Journal of Law [EJJL], [S. l.], v. 12, n. 2, p. 91–108, 2011. Disponível em: https://periodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 7 dez. 2025.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: fundamentos da Lei Geral de Proteção de Dados. 2. ed. rev. e atual. São Paulo: Thomson Reuters Revista dos Tribunais, 2019.

DONEDA, Danilo; ALMEIDA, V. A. F. O que é governança por algoritmos? *In*: BRUNO, Fernanda *et al*. (Org.). **Tecnopolíticas da vigilância**: perspectivas da margem. 1. ed. São Paulo: Boitempo, 2018.

DZIMIDAS HABER, Carolina; CARDOSO AMORIM MACIEL, Natalia. As sentenças judiciais por tráfico de drogas na cidade e Região Metropolitana do Rio de Janeiro. **Cadernos de Segurança Pública**, *[S. l.]*, v. 10, n. 10, p. 1–16, 2018. Disponível em: https://www.isprevista.rj.gov.br/isprevista/article/view/108. Acesso em: 27 mar. 2026.

EILBERG, Daniela Dora. Fluxo de dados, prova e processo penal. **Revista da Faculdade Mineira de Direito**, Belo Horizonte, v. 27, n. 54, 2024. Disponível em: https://periodicos.pucminas.br/Direito/article/view/34785. Acesso em: 19 nov. 2025.

ENDELEY, Robert E. **End-to-end encryption, backdoors, and privacy**. 2019. 130 f. Tese (Doutorado em Cibersegurança) – Capitol Technology University, Laurel, MD, 2019. Disponível em: https://www.proquest.com/docview/2309795255?pq-origsite=gscholar&fromopenview=true&sourcetype=Dissertations%20&%20Theses. Acesso em: 29 abr. 2023.

ESTADOS UNIDOS. [**Constituição (1787)**]. Emenda n. 4. 1791. *In*: The Bill of Rights. Washington, D.C.: National Archives.

ESTADOS UNIDOS. **Clarifying Lawful Overseas Use of Data Act (CLOUD Act)**. Pub. L. No. 115-141, div. V, 132 Stat. 1213 (2018).

ESTADOS UNIDOS. Department of Justice. **Promoting Public Safety, Privacy, and the Rule of Law Around the World**: The Purpose and Impact of the CLOUD Act. White Paper. [S. l.]: DOJ, Apr. 2019.

ESTADOS UNIDOS. **Electronic Communications Privacy Act** (ECPA). U.S. Code, § 2510 *et seq*., 1986.

ESTADOS UNIDOS. **Federal Rules of Criminal Procedure**: Rule 16. Washington, D.C.: U.S.

Government Publishing Office, 2024.

ESTADOS UNIDOS. Supreme Court. United States, **Petitioner v. Microsoft Corporation.** No. 17-2. U.S. Reports, Washington, D.C., v. 584, 2018.

ESTADOS UNIDOS. **Stored Communications Act. U.S. Code**, Título 18, § 2703. 1986.

ESTELLITA, Heloisa. O RE 1.055.941: um pretexto para explorar alguns limites à transmissão, distribuição, comunicação, transferência e difusão de dados pessoais pelo COAF. **Direito Público**, [S. l.], v. 18, n. 100, 2022. DOI: 10.11117/rdp.v18i100.5991. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/5991. Acesso em: 7 dez. 2025.

FEELEY, Malcolm M.; SIMON, Jonathan. **The new penology: notes on the emerging strategy of corrections and its implications**. Criminology, Columbus, v. 30, n. 4, p. 449-474, nov. 1992. Disponível em: https://doi.org/10.1111/j.1745-9125.1992.tb01112.x. Acesso em: 07 dez. 2025.

FERGUSON, Andrew Guthrie. **Big Data and Predictive Reasonable Suspicion**. University of Pennsylvania Law Review, Philadelphia, v. 163, n. 2, Jan. 2015. Disponível em: https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?httpsredir=1&article=9464&context=penn_law_review. Acesso em: 07 dez. 2025.

FERNANDES, Antonio Scarance. **Teoria Geral do Procedimento**. 1. ed. São Paulo: Revista dos Tribunais, 2005.

FERRAZ JUNIOR, 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**, São Paulo, v. 88, p. 439-459, 1993. Disponível em: https://www.revistas.usp.br/rfdusp/article/view/67231. Acesso em: 07 dez. 2025.

FOUCAULT, Michel. **Microfísica do poder**. Trad. e Org. de Roberto Machado. 13. ed. Rio de Janeiro: Graal, 1998.

GARCIA, Rafael de Deus. **Processo penal e algoritmos**: o direito à privacidade aplicável ao uso de algoritmos no policiamento. 2022. 248 f. Tese (Doutorado em Direito) – Universidade de Brasília, Brasília, 2022. Disponível em: https://repositorio.unb.br/handle/10482/45140. Acesso em: 07 dez. 2025.

GARLAND, David. **The culture of control**: crime and social order in contemporary society. Chicago: The University of Chicago Press, 2001. Disponível em: https://www.antoniocasella.eu/nume/Garland_control_2001.pdf. Acesso em: 07 dez. 2025.

GERCHICK, Marissa; CAGLE, Matt. When it comes to facial recognition, there is no such thing as a magic number. **American Civil Liberties Union**, New York, 7 fev. 2024. Disponível em: https://www.aclu.org/news/privacy-technology/when-it-comes-to-facial-recognition-there-is-no-such-thing-as-a-magic-number. Acesso em: 07 dez. 2025.

GIACOMOLLI, Nereu José; CANI, Luiz Eduardo. O acesso autorizado a aparelhos smart: burla ao agente infiltrado digital? **Boletim IBCCRIM**, São Paulo, v. 30, n. 352, p. 19-21, mar. 2022. Disponível em: https://www.ibccrim.org.br/publicacoes/boletim/352. Acesso em: 07 dez. 2025.

GIACOMOLLI, Nereu José; EILBERG, Daniela Dora. Coleta e tratamento de dados na transformação tecnológica da investigação criminal. **Galileu**: Revista de Direito e Economia, Lisboa, v. 24, n. 1-2, p. 123-140, jan./dez. 2023. Disponível em: https://journals.ual.pt/galileu/wp-content/uploads/2024/12/Galileu_XXIV_1-2_Coleta.pdf. Acesso em: 07 dez. 2025.

GLEIZER, Orlandino. A dogmática dos métodos ocultos de investigação no processo penal. *In*: BRITO CRUZ, Francisco; SIMÃO, Bárbara (Ed.). **Direitos Fundamentais e Processo Penal na Era Digital**: Doutrina e Prática em Debate. São Paulo: InternetLab, 2021. v. 4.

GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo. **O direito de proteção de dados no processo penal e na segurança pública**. 1. ed. Rio de Janeiro: Marcial Pons, 2021.

GLOECKNER, Ricardo Jacobsen; KHALED JR., Prof. Dr. Salah H.; DIVAN, Gabriel. Verdade, processo penal e epistemologia: da pretensa fundamentação filosófica aos efeitos jurídicos e políticos da adoção de premissas racionalistas. **Revista Brasileira de Ciências Criminais**, São Paulo, v. 199, n. 199, p. 73–107, 2023. DOI: 10.5281/zenodo.8381441. Disponível em: https://publicacoes.ibccrim.org.br/index.php/RBCCRIM/article/view/703. Acesso em: 7 dez. 2025.

GLOECKNER, Ricardo; LOPES JR., Aury. **Investigação Preliminar no Processo Penal**. 6. ed. São Paulo: Saraiva, 2014.

GLOECKNER, Ricardo *et al*. O inviolável e o intocável no direito processual penal: Considerações introdutórias sobre o processo penal alemão [...]. *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.

GOLDSCHMIDT, James. **Prozess als Rechtslage**: Eine Kritik des Prozessualen Denkens. Berlim: Springer, 1925.

GOLDBERG, Ian. Privacy Enhancing Technologies for the Internet III: Ten Years Later. *In*: DIGITAL PRIVACY: THEORY, TECHNOLOGIES, AND PRACTICES. [S. l.]: Auerbach Publications, 2007. Disponível em: https://crysp.uwaterloo.ca/courses/pet/F07/cache/www.cypherpunks.ca/~iang/pubs/pet3.pdf. Acesso em: 13 ago. 2024.

GRAY, David. **The Fourth Amendment in an Age of Surveillance**. New York: Cambridge University Press, 2017.

GRECO, Luís. **Modernização do direito penal, bens jurídicos coletivos e crimes de perigo abstrato**. Rio de Janeiro: Lumen Juris, 2011.

GRECO, Luís. Organização e introdução. *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**. Tradução Alaor Leite, Eduardo Viana e Luis Greco. 1. ed. São Paulo: Marcial Pons, 2018.

GRINOVER, Ada Pellegrini. O regime brasileiro das interceptações telefônicas. **Revista de Direito Administrativo**, Rio de Janeiro, v. 207, p. 21-38, jan./mar. 1997. Disponível em: https://periodicos.fgv.br/rda/article/view/46935. Acesso em: 10 dez. 2023.

GUARIGLIA, Matthew. The movement to ban government use of face recognition. **Electronic Frontier Foundation**, San Francisco, 2 maio 2022. Disponível em: https://www.eff.org/deeplinks/2022/05/movement-ban-government-use-face-recognition. Acesso em: 07 dez. 2025.

HEGEL, Georg F. Wilhelm. O princípio do mundo moderno em geral é a liberdade da subjetividade. *In*: HABERMAS, Jürgen. **O Discurso filosófico da Modernidade.** Trad. Ana Maria Bernardo *et al*. Lisboa: Dom Quixote, 1991.

HEMMINGS, Justin; SRINIVASAN, Sreenidhi; SWIRE, Peter. Defining the scope of "possession, custody, or control" for privacy issues and the CLOUD Act. **Journal of National Security Law & Policy**, Washington, D.C., v. 10, n. 2, p. 665-690, 2020. Disponível em: https://ssrn.com/abstract=3469808. Acesso em: 07 dez. 2025.

INTERNETLAB. **O direito das investigações digitais no Brasil**: fundamentos e marcos normativos. 3. ed. São Paulo: InternetLab, 2022.

KERR, Orin S. Digital evidence and the new criminal procedure. **Columbia Law Review**, New York, v. 105, n. 1, p. 279-318, jan. 2005. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=665662. Acesso em: 07 dez. 2025.

KERR, Orin S. The next generation communications privacy act. **University of Pennsylvania Law Review**, Philadelphia, v. 162, n. 2, p. 373-419, jan. 2014. Disponível em: https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1546&context=penn_law_review. Acesso em: 07 dez. 2025.

KHALED JR, Salah Hassan. O PROBLEMA DA PREVALÊNCIA DO PODER NA JURISDIÇÃO PENAL: RUMO AO ESTABELECIMENTO DE UMA JURISDIÇÃO PENAL COMO PODER-DEVER E DIREITO FUNDAMENTAL. **Revista da Faculdade de Direito da UFG**, Goiânia, v. 34, n. 01, 2010. DOI: 10.5216/rfd.v34i01.9929. Disponível em: https://revistas.ufg.br/revfd/article/view/9929. Acesso em: 7 dez. 2025.

KNIJNIK, Danilo. A trilogia Olmstead-Katz-Kyllo: o art. 5º da Constituição Federal do século XXI. **Revista Escola da Magistratura do TRF da 4ª Região**, Porto Alegre, ano 2, n. 4, 2016. Disponível em: https://www.trf4.jus.br/trf4/upload/editor/2016/rlp_revista_escola_magistratura_n4_completa.pdf. Acesso em: 07 dez. 2025.

LEANDRO; DE, M.; GUILHERME, F. **Cidades inteligentes e inovação: a videovigilância na Segurança Pública de Recife, Brasil**. Cadernos Metrópole, v. 25, n. 58, p. 1095–1122, 1 dez. 2023. Disponível em: https://www.scielo.br/j/cm/a/BgjpbJwnDqq3wNzVFPsJ8Zz/?lang=pt. Acesso em: 07 dez. 2025.

LEMOS, Alessandra *et al*. **Comentários ao anteprojeto de lei de proteção de dados para a segurança pública**: tecnologia de reconhecimento facial. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio, 2021. Disponível em: https://itsrio.org/wp-content/uploads/2021/04/UK-Comentarios_LGPDPenal.pdf. Acesso em: 07 dez. 2025.

LIGUORI, Carlos. **Direito e Criptografia**. São Paulo: Saraiva Jur, 2023.

LIGUORI FILHO, Carlos Augusto; SALVADOR, João Pedro Favaretto. Crypto wars e bloqueio de aplicativos: o debate sobre regulação jurídica da criptografia nos Estados Unidos e no Brasil. **Revista da Faculdade de Direito UFPR**, [S. l.], v. 63, n. 3, p. 135–161, 2018. DOI: 10.5380/rfdufpr.v63i3.59422. Disponível em: https://revistas.ufpr.br/direito/article/view/59422. Acesso em: 7 dez. 2025.

LOPES JÚNIOR, Aury. **Direito Processual Penal.** 17. ed. São Paulo: Saraiva Jur, 2020.

LOPES JUNIOR, Aury. **A (in)existência de poder geral de cautela no processo penal**. Boletim IBCCrim, São Paulo, n. 203, out. 2009. Disponível em: https://arquivo.ibccrim.org.br/boletim_artigos/240-203-Outubro-2009. Acesso em: 7 dez. 2025.

MACHADO, André. **Investigação criminal defensiva**. 1. ed. São Paulo: Revista dos Tribunais, 2010.

MAILLART, Jean-Baptiste. **The limits of subjective territorial jurisdiction in the context of cybercrime**. ERA Forum, [S. l.], v. 19, 2019. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3249367. Acesso em: 07 dez. 2025.

MARAS, Marie-Helen; WANDT, **Adam Scott. Enabling mass surveillance: data aggregation in the age of big data and the Internet of Things**. Journal of Cyber Policy, [S. l.], v. 4, n. 2, 17 mar. 2019. Disponível em: https://ccybers.org/wp-content/uploads/2022/11/Enabling-mass-surveillance-data-aggregation-in-the-age-of-big-data-and-the-Internet-of-Things.pdf. Acesso em: 7 dez. 2025.

MASON, Stephen; SENG, Daniel. **Electronic evidence**. 4. ed. London: Institute of Advanced Legal Studies, 2017. Disponível em: https://sas-space.sas.ac.uk/6541/1/ElectronicEvidence.pdf. Acesso em: 07 dez. 2025.

MATIDA, Janaina; HERDY, Rachel. As inferências probatórias: compromissos epistêmicos, normativos e interpretativos. **Revista do Ministério Público do Estado do Rio de Janeiro**, Rio de Janeiro, n. 73, p. 133-155, jul./set. 2019. Disponível em: https://www.mprj.mp.br/documents/20184/1473819/Janaina+Matida+%26+Rachel+Herdy.pdf. Acesso em: 07 dez. 2025.

MAYER-SCHÖNBERGER, Viktor; RAMGE, Thomas. **Reinventing capitalism in the age of big data**. New York: Basic Books, 2018.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big Data: a revolution that will transform how we live, work, and think.** Boston: Houghton Mifflin Harcourt, 2013.

MCCARTHY, H. J. **Shedding Light on the "Going Dark" Problem and the Encryption Debate**. Journal of Internet Law, [S. l.], v. 20, n. 3, 2016. Disponível em https://doi.org/10.36646/mjlr.50.2.shedding. Acesso em 2 jan. 2025.

MCKAY, Carolyn. **Previsão de risco no processo penal: ferramentas atuariais, algoritmos, IA e tomada de decisão judicial**. Current Issues in Criminal Justice, [S. l.], 29 set. 2019. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3494076. Acesso em: 07 dez. 2025.
MELGAÇO, Lucas de Melo. **A cidade de poucos: condomínios fechados e a privatização do espaço público em Campinas**. Boletim Campineiro de Geografia, Campinas, v. 2, n. 1, p. 81-105, 2012. Disponível em: https://researchportal.vub.be/en/publications/a-cidade-de-poucos-condom%C3%ADnios-fechados-e-a-privatiza%C3%A7%C3%A3o-do-espa%C3%A7/. Acesso em: 10 out. 2025.

MELGAÇO, Lucas; VAN BRAKEL, Rosamunde Elise. **Smart Cities as Surveillance Theatre**. Surveillance & Society, [s.l.], v. 19, n. 2, p. 244-249, 2021. Disponível em: https://cris.vub.be/ws/files/71204211/14321_Article_Text_34329_1_10_20210625.pdf. Acesso em: 15 nov. 2025.

MELGAÇO, Lucas de Melo. Estudantes sob controle: a racionalização do espaço escolar através do uso de câmeras de vigilância. **Revista O Social em Questão**, n. 27, p. 193-212, 2012. Disponível em: https://cris.vub.be/ws/portalfiles/portal/82697184/OSocial27_Sec_a_o_Livre_Melgac_o1.pdf. Acesso em: 2 dez. 2025.

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. 218 f. Dissertação (Mestrado em Ciências Criminais) – Escola de Direito, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2018. Disponível em: http://tede2.pucrs.br/tede2/handle/tede/8537. Acesso em: 07 dez. 2025.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. 7. ed. São Paulo: Saraiva, 2012.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. 17. ed. São Paulo: Saraiva Jur, 2022.

MICROSOFT. **O que são bancos de dados?** [S. l.], [s. d.]. Disponível em: https://azure.microsoft.com/pt-br/resources/cloud-computing-dictionary/what-are-databases. Acesso em: 03 jun. 2023.

MOURA, Maria Thereza Rocha de Assis. **A prova por indícios no processo penal**. Rio de Janeiro: Lumen Juris, 2009.

MOURA, Maria Thereza Rocha de Assis; BARBOSA, Daniel Marchionatti. Dados digitais: interceptação, busca e apreensão e requisição. *In*: **DIREITO, PROCESSO E TECNOLOGIA.** [S. l.: s. n.], 2021.

SRNICEK, N. **Platform capitalism**. Cambridge, UK: Polity Press, 2017.

ORLANDI, Eni. Recortar ou segmentar? *In*: **Linguística**: Questões e Controvérsias. Série Estudos. Uberaba: Faculdades Integradas de Uberaba, 1984. p. 11-25. Disponível em: https://pt.scribd.com/document/318639266/Segmentar-Ou-Recortar-Orlandi. Acesso em: 07 nov. 2025.

PEDRESCHI, Dino; RUGGIERI, Salvatore; TURINI, Franco. Discrimination-aware data mining. *In*: ACM SIGKDD INTERNATIONAL CONFERENCE ON KNOWLEDGE DISCOVERY AND DATA MINING, 14., 2008, Las Vegas. **Proceedings** [...]. New York: ACM, 2008. p. 560-568. Disponível em: https://pages.di.unipi.it/ruggieri/Papers/kdd2008.pdf. Acesso em: 04 out. 2025.

PORTUGAL. Lei n.º 109/2009, de 15 de setembro. Aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa. **Diário da República**, Lisboa, 1.ª série, n. 179, p. 6321, 15 set. 2009. Disponível em: https://diariodarepublica.pt/dr/detalhe/lei/109-2009-489693. Acesso em: 07 dez. 2025.

PRADO, Geraldo. Esboço de proposta sobre dispositivo de controle da investigação digital: o "aspecto dinâmico da prova digital". **Revista do Sistema Único de Segurança Pública**, Brasília, v. 3, n. 1, p. 240-261, jul./dez. 2024. Disponível em: https://revistasusp.mj.gov.br/susp/index.php/revistasusp/article/view/621. Acesso em: 07 dez. 2025.

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.

PRAMANIK, M. I. *et al*. Big data analytics for security and criminal investigations. **WIREs Data Mining and Knowledge Discovery**, Hoboken, v. 7, n. 4, p. e1208, jul./ago. 2017. Disponível em: https://doi.org/10.1002/widm.1208. Acesso em: 07 dez. 2025.

RAMALHO, David da Silva. **Métodos Ocultos de Investigação Criminal em Ambiente Digital**. 1. ed. Coimbra: Almedina, 2017.

REBELLATO, Luiz Fernando Bugiga. **A análise constitucional do sigilo e da privacidade nas investigações criminais**: o acesso a dados armazenados em aparelhos celulares. 2021. 305 f. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2021. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2137/tde-08072022-

114811/. Acesso em: 07 dez. 2025.

RIBEIRO, Gustavo Alves Magalhães; CORDEIRO, Pedro Ivo Rodrigues Velloso; FUMACH, Débora Moretti. O malware como meio de obtenção de prova e a sua implementação no ordenamento jurídico brasileiro. **Revista Brasileira de Direito Processual Penal**, Porto Alegre, v. 8, n. 3, p. 1463-1500, set./dez. 2022. Disponível em: https://doi.org/10.22197/rbdpp.v8i3.723. Acesso em: 07 dez. 2025.

RIBEIRO, Marcelo Stopanovski. **Características da informação na Teoria Quântica e suas possíveis interpretações para um objeto informacional na Ciência da Informação**. 2014. x, 129 f., il. Tese (Doutorado em Ciência da Informação) – Universidade de Brasília, Brasília, 2014. Disponível em: https://repositorio.unb.br/handle/10482/17773. Acesso em: 25 mar. 2026.

RODRIGUES, Benjamin Silva. **Da prova penal: Tomo II** – Bruscamente... A(s) Face(s) Oculta(s) Métodos Ocultos de Investigação Criminal. Porto: Rei dos Livros, 2010.

ROSA, Alexandre Morais da; LOPES JR., Aury. Limite Penal: quando a Cinderela do processo penal ganha novas roupas. **Consultor Jurídico**, São Paulo, 28 jul. 2017. Disponível em: https://www.conjur.com.br/secoes/colunas/limite-penal. Acesso em: 07 dez. 2025.

RUBINSTEIN, Ira S. **Regulating Privacy by Design**. Berkeley Technology Law Journal, [S. l.], v. 26, n. 3, 2011. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1837862. Acesso em: 07 dez. 2025.

SAAD, Marta. Editorial do dossiê “Reformas da investigação preliminar e a investigação defensiva no processo penal” – Investigação preliminar: desafios e perspectivas. **Revista Brasileira de Direito Processual Penal**, Porto Alegre, v. 6, n. 1, p. 29-40, jan./abr. 2020. Disponível em: https://revista.ibraspp.com.br/RBDPP/article/view/348/200. Acesso em: 07 dez. 2025.

SAAD, Marta. Direito de defesa na etapa preliminar da apuração penal: reconhecimento, novas perspectivas e desafios. **Boletim IBCCRIM**, São Paulo, v. 32, n. 381, p. 13–17, 2024. DOI: 10.5281/zenodo.12709853. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1341. Acesso em: 12 mar. 2026.

SÃO PAULO (Estado). Lei nº 15.518, de 17 de julho de 2014. Dispõe sobre a afixação de aviso com o número do Disque Denúncia da Violência contra a Mulher (Disque 180) em estabelecimentos de acesso ao público que especifica. **Diário Oficial do Estado de São Paulo**, São Paulo, v. 124, n. 132, Seção 1, p. 1, 18 jul. 2014.

SARLET, Ingo Wolfgang; SARLET, Gabrielle Bezerra Sales. **Separação informacional de poderes no direito constitucional brasileiro**. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2022. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2022/09/DataPrivacy.-Separacao-Informacional-de-Poderes.-2022.pdf. Acesso em: 08 dez. 2025.

SCHAAR, Peter. Privacy by design. **Identity in the Information Society**, Berlin, v. 3, n. 2, p. 267-274, 2010. Disponível em: https://doi.org/10.1007/s12394-010-0055-x. Acesso em: 08 dez. 2025.

SCHEMBRI, Thyler J. The rise of technology and its effect on search and seizure analysis: the constitutionality of geofencing warrants under the supreme court's fourth amendment jurisprudence. South Carolina Law Review, Columbia, SC, v. 75, n. 1, 2023. Disponível em: https://scholarcommons.sc.edu/sclr/vol75/iss1/8/. Acesso em: 07 dez. 2025.

SHANMUGAM, Divya *et al*. Learning to limit data collection via scaling laws: a computational interpretation for the legal principle of data minimization. *In*: ACM CONFERENCE ON FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY (FAccT '22), 2022, Seoul. **Proceedings** [...]. New York: ACM, 2022. p. 175-186. Disponível em: https://arxiv.org/pdf/2107.08096. Acesso em: 07 dez. 2025.

SHOSTACK, Adam; SYVERSON, Paul. What Price Privacy? (and Why Identity Theft Is About Neither Identity Nor Theft). *In*: CAMP, L. Jean; LEWIS, Stephen (Ed.). **Economics of Information Security**. Boston: Kluwer Academic Publishers, 2004. p. 129-142.

SIDI, Ricardo. A interceptação de e-mails e a apreensão física de e-mails armazenados. **Revista Fórum de Ciências Criminais** (RFCC), Belo Horizonte, ano 2, n. 4, jul./dez. 2015. Disponível: https://sidiandrade.com.br/wp-content/uploads/2024/11/ricardo-sidi-a-interceptacao-e-a-apreensao-fisica-de-emails-armazenados.pdf. Acesso em: 07 dez. 2025.

SILVA, Viviani Ghizoni da; MELO E SILVA, Philipe Benoni; MORAIS DA ROSA, Alexandre. **Fishing expedition e encontro fortuito na busca e na apreensão: um dilema oculto do processo penal.** 2. ed. Florianópolis: Emais, 2022.

SILVA, Virgílio Afonso da. A evolução dos direitos fundamentais. **Revista Latino-Americana de Estudos Constitucionais**, Belo Horizonte, n. 6, p. 541-558, jul./dez. 2005. Disponível em: https://constituicao.direito.usp.br/wp-content/uploads/2005-RLAEC06-Evolucao.pdf. Acesso em: 07 dez. 2025.

SILVA, Thales Cassiano. **Como a Petrobras foi de vítima à ré?**: Lava Jato vs. Vaza Jato: instrumentalidade processual e limites penais da assistência direta. 2021. 237 f. Dissertação (Mestrado em Ciências Criminais) – Escola de Direito, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2021. Disponível em: https://tede2.pucrs.br/tede2/handle/tede/10236. Acesso em: 07 dez. 2025.

SIPPEL, B. Guest editorial eucrim 2-2023. **Eucrim**: The European Criminal Law Associations' Forum, n. 2, 2023. DOI 10.30709/eucrim-2023-011. Disponível em: https://doi.org/10.30709/eucrim-2023-011. Acesso em: 8 dez. 2024.

SOARES, Gustavo Torres. **Investigação criminal e inovações técnicas e tecnológicas**: perspectivas e limites. 2014. 307 f. Tese (Doutorado em Direito Processual) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2014. Disponível em: https://doi.org/10.11606/T.2.2015.tde-30112015-165420. Acesso em: 11 nov. 2025.

SOLOVE, Daniel J. **The Digital Person**: Technology and Privacy in the Information Age. New York: New York University Press, 2004.

SOUSA, Pedro. **Direito penal nos tempos da inteligência artificial**: uma análise da responsabilidade dos agentes envolvidos no desenvolvimento e na operação de algoritmos de seleção e recrutamento em relação ao crime de racismo previsto no art. 4º da Lei 7.716/1989. 2022. 123 f. Dissertação (Mestrado em Direito Constitucional) – Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, Brasília, 2022. Disponível em: https://repositorio.idp.edu.br/handle/123456789/4283. Acesso em: 08 dez. 2025.

SPIEKERMANN, Sarah. The challenges of privacy by design. **Communications of the ACM**, New York, v. 55, n. 7, p. 38-40, jul. 2012. Disponível em: https://doi.org/10.1145/2209249.2209263. Acesso em: 07 dez. 2025.

STEFAN, Marco; FUSTER, Gloria González. **Cross-border Access to Electronic Data through Judicial Cooperation in Criminal Matters**: State of the art and latest developments in the EU and the US. [Brussels]: CEPS, 2018. (CEPS Paper in Liberty and Security in Europe, n. 2018-07). Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3298705. Acesso em: 07 dez. 2025.

TARUFFO, Michele. **La prova dei fatti giuridici**: nozioni generali. Milano: Giuffrè, 1992.

THALER, Richard H.; SUNSTEIN, Cass R. **Nudge**: Improving Decisions about Health, Wealth, and Happiness. New Haven: Yale University Press, 2008.

TONINI, Paolo. **Manuale di procedura penale**. 9. ed. Milano: Giuffrè Editore, 2008.

TOSZA, Stanislaw. **The e-evidence package is adopted end of a saga or beginning of a new one?** European Data Protection Law Review, [S. l.], v. 9, n. 2, 2023. Disponível em: https://orbilu.uni.lu/bitstream/10993/57666/1/edpl_2023_02-012.pdf. Acesso em: 07 dez. 2025.

TSUNODA, Denise Fukumi; CANDIDO, Ana Clara; GUIMARÃES, André José Ribeiro. Tecnologias disruptivas em segurança pública: uma análise situacional brasileira. **Revista Tecnologia e Sociedade**, Curitiba, v. 20, n. 61, 2024. Disponível em: https://periodicos.utfpr.edu.br/rts/article/view/18408. Acesso em: 07 dez. 2025.

UNIÃO EUROPEIA. Parlamento Europeu; Conselho. Diretiva 95/46/CE, de 24 de outubro de 1995. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. **Jornal Oficial das Comunidades Europeias**, Luxemburgo, n. L 281, p. 31-50, 23 nov. 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:31995L0046. Acesso em: 10 mar. 2025.

UNIÃO EUROPEIA. Parlamento Europeu; Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, Luxemburgo, n. L 119, p.

1-88, 4 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679. Acesso em: 10 mar. 2025

UNIÃO EUROPEIA. Parlamento Europeu; Conselho. Diretiva (UE) 2016/680, de 27 de abril de 2016. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. **Jornal Oficial da União Europeia**, Luxemburgo, n. L 119, p. 89-131, 4 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016L0680. Acesso em: 03 jan. 2025.

UNIÃO EUROPEIA. Parlamento Europeu; Conselho. Diretiva (UE) 2023/1544, de 12 de julho de 2023. Estabelece regras harmonizadas aplicáveis à designação de estabelecimentos designados e à nomeação de representantes legais para efeitos de recolha de prova eletrónica em processos penais. **Jornal Oficial da União Europeia**, Luxemburgo, n. L 191, p. 181-190, 28 jul. 2023. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32023L1544. Acesso em: 04 ago. 2024.

UNIÃO EUROPEIA. Parlamento Europeu; Conselho. Regulamento (UE) 2023/1543, de 12 de julho de 2023. Relativo às ordens europeias de produção e às ordens europeias de conservação para efeitos de prova eletrónica em processos penais e para efeitos de execução de penas privativas de liberdade na sequência de processos penais. **Jornal Oficial da União Europeia**, Luxemburgo, n. L 191, p. 118-180, 28 jul. 2023. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32023R1543. Acesso em: 08 dez. 2025.

UNIÃO EUROPEIA. Tribunal de Justiça (Grande Secção). Acórdão de 8 de abril de 2014. Processos apensos C-293/12 e C-594/12. Digital Rights Ireland Ltd contra Minister for Communications, Marine and Natural Resources e o. e Kärntner Landesregierung e o. **Coletânea da Jurisprudência**, Luxemburgo, ECLI:EU:C:2014:238, 8 abr. 2014. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:62012CJ0293. Acesso em: 08 dez. 2025.

UNIÃO EUROPEIA. Tribunal de Justiça (Grande Secção). Acórdão de 21 de dezembro de 2016. Processos apensos C-203/15 e C-698/15. Tele2 Sverige AB contra Post-och telestyrelsen e Secretary of State for the Home Department contra Tom Watson e o. **Coletânea da Jurisprudência**, Luxemburgo, ECLI:EU:C:2016:970, 21 dez. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:62015CJ0203. Acesso em: 08 dez. 2025.

VALENTE, Rubens; FREITAS, Caio de. Ata revela 'consultas irregulares' em sistemas de vigilância do Ministério da Justiça. **Agência Pública**, [S. l.], 21 jan. 2025. Disponível em: https://apublica.org/2025/01/ata-revela-consultas-irregulares-em-sistemas-de-vigilancia-do-ministerio-da-justica/. Acesso em: 08 set. 2025.

VASCONCELLOS, Vinicius Gomes de. Fundamento e função do processo penal: a centralidade do juízo oral e sua relação com as demais fases da persecução penal para a limitação do poder punitivo. **Revista Eletrônica de Direito Processual**, Rio de Janeiro, v. 19, n. 2, p. 229-260, maio/ago. 2018. Disponível em: https://www.e-publicacoes.uerj.br/redp/article/view/31959. Acesso em: 08 nov. 2025.

VAZ, Denise Provasi. **Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório**. 2012. Tese (Doutorado em Direito Processual) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2012. Disponível em: https://teses.usp.br/teses/disponiveis/2/2137/tde-28052013-153123/pt-br.php. Acesso em: 03 dez. 2024.

VERGNOLLE, Suzanne. Understanding the French criminal justice system as a tool for reforming international legal cooperation and cross-border data requests. In: BRÄUTIGAM, Tobias; MIETTINEN, Samuli (ed.). **Data Protection, Privacy and European Regulation in the Digital Age**. Helsinki: Unigrafia, 2016. p. 206–228. Disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2921364. Acesso em 16 fev. 2024.

WACHTER, Sandra; MITTELSTADT, Brent. **A right to reasonable inferences: re-thinking data protection law in the age of Big Data and AI**. Columbia Business Law Review, [S. l.], n. 2, p. 497, 2019. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829. Acesso em: 07 dez. 2025.

WANDERLEY, Gisela. Privacidade e Cidadania: Os Limites Jurídicos da Atividade Investigativa e a Legalidade do Acesso Policial a Aparelhos Celulares. *In*: ANTONIALLI, Dennys; FRAGOSO, Nathalie (Org.). **Direitos Fundamentais e Processo Penal na Era Digital**: Doutrina e Prática em Debate. São Paulo: InternetLab, 2019. v. 2. Disponível em: https://internetlab.org.br/wp-content/uploads/2019/08/InternetLabCongressoII_dupla.pdf. Acesso em: 07 dez. 2025.

ZARAGOZA TEJADA, Javier Ignacio. La prueba ilícita y prueba tecnológica. Reflexiones a raíz del caso Encrochat. *In*: ORTIZ PRADILLO, Juan Carlos; ABELLÁN ALBERTOS, Antonio (Dir.). **El derecho de defensa en la justicia penal digital**. Valencia: Tirant lo Blanch, 2024.

ZILLI, Marcos. A prisão em flagrante e o acesso de dados em dispositivos móveis: nem utopia, nem distopia: apenas a racionalidade. *In*: ABREU, Jacqueline de Souza; ANTONIALLI, Dennys (Ed.). **Direitos Fundamentais e Processo Penal na Era Digital**: Doutrina e Prática em Debate. São Paulo: InternetLab, 2018. v. 1.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder**. Tradução: George Schlesinger. Rio de Janeiro: Intrinseca, 2020.