Higor Vinicius Nogueira Jorge

INVESTIGAÇÃO CRIMINAL TECNOLÓGICA

Fundamentos, Método e Limites na Era dos Vestígios Informacionais

2027

EDITORA JusPODIVM

www.editorajuspodivm.com.br

Capítulo 1

A Investigação Criminal Tecnológica como Disciplina Autônoma

"A investigação criminal tecnológica não é a informatização da polícia. É a organização jurídica e metodológica de uma nova forma de conhecer fatos penalmente relevantes."

1.1. UMA CONSTATAÇÃO PRÁTICA, NÃO UMA TESE ACADÊMICA

Quando concebi a disciplina investigação criminal tecnológica, em 2015, não parti de uma intuição teórica. Parti de uma constatação que se repetia em quase todos os casos que passavam pela minha mesa: a tecnologia havia deixado de ser objeto exclusivo de um nicho de crimes para se tornar elemento presente em praticamente toda investigação. Um homicídio, um crime patrimonial, um caso de corrupção, um episódio de tráfico, uma ameaça, um desaparecimento – todos passaram a deixar vestígios informacionais. O aparelho celular, as câmeras de monitoramento, os registros de geolocalização, as movimentações financeiras digitais e as redes sociais converteram-se em fontes de prova de qualquer apuração, e não apenas das que nascem no ambiente digital.

Essa percepção muda a forma de organizar o trabalho investigativo de cima a baixo. Não basta ter, na corporação, uma unidade especializada em crimes informáticos para a qual se encaminham os casos digitais enquanto os demais seguem sem esse tratamento. É preciso que todo investigador domine os fundamentos do tratamento do vestígio tecnológico, porque ele aparecerá em sua mesa independentemente da etiqueta que o caso receba na distribuição. O delegado que apura um latrocínio precisa, hoje, saber tanto sobre a preservação de um aparelho celular quanto sobre a leitura de uma cena física. O agente de rua que chega primeiro precisa saber o que não fazer com um dispositivo eletrônico – porque o que não fazer, nesse campo, tem tanta importância quanto o que fazer. A separação entre o investigador chamado "tradicional" e o investigador chamado "digital" tornou-se artificial, e custa caro tratá-la como real.

A investigação criminal tecnológica é, portanto, o emprego metodologicamente controlado da tecnologia na persecução penal, organizado em torno da identificação, preservação, obtenção, tratamento, correlação, interpretação e apresentação de vestígios informacionais juridicamente relevantes. Sua incidência é transversal: aplica-se a investigações de qualquer natureza, do crime mais tradicional ao mais sofisticado, sempre que dados, dispositivos, sistemas, redes, plataformas ou fluxos informacionais tiverem relevância para a reconstrução do fato.

1.2. A AUTONOMIA QUE NÃO É ORNAMENTAL

A autonomia da disciplina não resulta de escolha terminológica. Ela decorre de uma alteração real no ambiente investigativo. Quando a criminalidade se projeta em dispositivos, contas, redes, bancos de dados, serviços de armazenamento remoto, registros telemáticos e padrões relacionais distribuídos em múltiplas plataformas, o problema investigativo deixa

Capítulo 2

O Método em Sete Fases: da Identificação à Apresentação

"Não existe atalho que substitua a compreensão de por que cada etapa existe. Existe a formação que transforma o procedimento em convicção – e a convicção em hábito."

2.1. POR QUE O MÉTODO IMPORTA MAIS DO QUE A FERRAMENTA

A investigação criminal tecnológica não estrutura o tratamento do vestígio em etapas porque a burocracia assim exige. Estrutura porque cada fase protege a próxima – e porque a fragilidade de qualquer elo tem o poder de comprometer todo o conjunto probatório, independentemente de quantas outras etapas tenham sido executadas com perfeição técnica. Essa arquitetura encadeada oferece duas vantagens que se reforçam mutuamente: organiza o raciocínio do investigador, prevenindo atalhos que parecem eficientes no curto prazo e se revelam custosos quando a prova é desafiada, e oferece à defesa e ao julgador um caminho auditável, no qual cada passo pode ser examinado e questionado – que é exatamente o que o contraditório requer.

Uma ressalva antes de descrever as fases: o método não é linear de forma rígida. Há momentos em que a identificação de um novo vestígio, na etapa de correlação, obriga a retornar à preservação de uma fonte ainda não considerada. Há hipóteses em que a interpretação revelará que a coleta foi incompleta e que uma nova rodada de obtenção se faz necessária. O método funciona como uma lógica de controle, não como uma linha de montagem. O que não pode ser dispensado é a disciplina que ele impõe em cada retorno.

2.2. FASE 1 – IDENTIFICAÇÃO: A PERGUNTA ANTES DA BUSCA

A identificação é o reconhecimento das fontes informacionais relevantes para a hipótese investigativa. Antes de coletar, é preciso saber o que coletar e por quê. Esta fase impõe a primeira e mais difícil contenção metodológica: a investigação séria não começa pela coleta máxima, mas pela pergunta juridicamente relevante. O impulso de coletar tudo o que está disponível é compreensível – a informação pode ser perdida se não for coletada agora –, mas produz problemas que custam mais do que o que economizou. Coleta excessiva viola a proporcionalidade, expõe dados de terceiros que não são objeto da apuração, gera volume que ninguém consegue analisar com critério e facilita a alegação de devassa indiscriminada.

Identificar corretamente as fontes significa perguntar, desde o primeiro contato com o caso, quais sistemas, dispositivos, plataformas, registros ou bases de dados podem ter sido alcançados pelos fatos que se apuram. Essa pergunta pressupõe conhecimento prévio de como diferentes tipos de crime geram diferentes tipos de vestígios digitais, e de qual é a janela temporal em que cada vestígio está disponível antes de se perder. A identificação também impõe uma decisão de escopo com consequências jurídicas imediatas: delimitar o que está e o que não está dentro do campo de coleta autorizado pela base legal disponível. A autorização judicial para registros de conexão de um aparelho específico não autoriza, por extensão, a coleta de todos os dados de todos os aparelhos que com ele comunicaram. Ampliar o escopo além do que a autorização cobre é semear nulidade desde a primeira fase.

Capítulo 3

Os Limites Constitucionais da Investigação Tecnológica

"A investigação criminal tecnológica só se justifica quando a potência técnica do Estado permanece subordinada à Constituição."

3.1. DIREITOS FUNDAMENTAIS COMO CONDIÇÕES ESTRUTURAIS, NÃO COMO OBSTÁCULOS

A investigação criminal tecnológica opera em ambiente de possibilidades ampliadas. A tecnologia disponível hoje permite acompanhar, com precisão crescente, a localização de uma pessoa ao longo do tempo, o conteúdo de suas comunicações, seus padrões de consumo e seus vínculos sociais. Essa capacidade aumentada exige, precisamente por isso, uma definição mais clara dos limites em que pode ser exercida.

A Constituição Federal de 1988 não estabeleceu o direito à intimidade, à vida privada e ao sigilo das comunicações como obstáculos contingentes à eficiência do Estado. Estabeleceu-os como condições estruturais da legitimidade da persecução penal. Uma investigação que os viola pode até descobrir a verdade factual; mas a paga com a ilegitimidade do meio e, frequentemente, com a nulidade do resultado. É a diferença entre um Estado que persegue o crime respeitando as regras que o distinguem dos que investiga, e um Estado que, na urgência de punir, passa a operar com a mesma lógica que pretende combater.

Capítulo 4

Cadeia de Custódia da Prova Digital: o Vestígio que Não Se Vê

"O cuidado com o invisível não é exagero técnico. É a condição de que a prova exista para o processo."

4.1. O QUE TORNA O VESTÍGIO DIGITAL SINGULAR

Um vestígio físico tem materialidade evidente. A arma, o documento, a impressão papilar existem no mundo e podem ser vistos, tocados e preservados por meios que qualquer investigador compreende intuitivamente. O vestígio digital, ao contrário, existe como sequência de dados que pode ser modificada, copiada ou apagada sem deixar marcas aparentes – e, em muitos casos, sem que quem provocou a alteração soubesse que o fez. Um acesso indevido a um dispositivo é capaz de alterar metadados que documentam a última vez em que um arquivo foi aberto, registrar um novo acesso que não existia antes e comprometer justamente as informações de contexto que dariam sentido ao dado.

Três singularidades marcam a prova digital. A primeira é a volatilidade: dados podem desaparecer por ação automática do próprio sistema, por sobrescrita, por expiração de registros ou por comando remoto. A segunda é a alterabilidade sem rastro perceptível: um arquivo pode ser aberto, copiado, movido ou modificado sem qualquer sinal visível para quem o manuseia. A terceira é a dependência do contexto: o que confere força probatória ao dado digital é o conjunto que o cerca – proveniência, momento, autoria, integridade. Por isso, na prova digital, a forma de obtenção integra o próprio valor do resultado: não é possível separar o quê do como.

Capítulo 5

Fontes Abertas na Investigação: o Método por Trás da Informação Pública

"O analista experiente não é o que encontra mais. É o que confirma melhor e distingue o que orienta do que prova."

5.1. OSINT: ENTRE A POTÊNCIA E A BANALIZAÇÃO

A sigla OSINT – do inglês open source intelligence, inteligência de fontes abertas – popularizou-se a ponto de ser banalizada. Reduzida a pesquisar na internet, perde aquilo que a torna valiosa: o método. Informação de fonte aberta é toda aquela disponível publicamente, sem necessidade de meios sigilosos: registros públicos, publicações em redes sociais, notícias, documentos oficiais, dados disponibilizados por órgãos e empresas. A abundância dessas informações não as transforma automaticamente em inteligência – e muito menos em prova.

O que distingue a inteligência de fontes abertas de uma busca casual é o rigor com que a informação é coletada, verificada e interpretada. A facilidade engana: como a informação está ao alcance de qualquer pessoa, cria-se a ilusão de que o trabalho consiste apenas em encontrá-la. Encontrar é o mais simples. O difícil – e o que produz valor investigativo real – é saber o que procurar, confirmar o que se encontra, extrair sentido do conjunto e distinguir o que pode orientar uma diligência do que pode, validamente, sustentar uma conclusão processual.

Capítulo 6

Inteligência Artificial na Investigação: Entre a Eficiência e a Responsabilidade

"A máquina amplia o alcance de quem investiga. Mas é a responsabilidade humana que confere legitimidade ao resultado."

6.1. O ENTUSIASMO LEGÍTIMO QUE PRECISA DE MÉTODO

Há um entusiasmo legítimo em torno das ferramentas de inteligência artificial aplicadas à investigação criminal. Sistemas capazes de correlacionar grandes volumes de dados em segundos, reconhecer padrões que escapariam à análise humana por semanas, transcrever automaticamente horas de áudio, organizar vínculos entre investigados em estruturas visuais compreensíveis e sugerir hipóteses a partir de anomalias estatísticas representam um salto de capacidade investigativa que seria impensável há uma geração. Ignorar esse potencial seria um equívoco de proporções crescentes à medida que a criminalidade se sofistica. Incorporá-lo sem critério seria um equívoco maior: o preço se paga em prova anulada, em direito violado e em investigação desperdiçada.

Capítulo 7

Fraudes Eletrônicas: a Engenharia Social como Porta de Entrada do Crime

"Por trás da maioria das fraudes eletrônicas não há uma falha tecnológica sofisticada, mas a exploração de algo muito mais antigo: a confiança humana."

7.1. O GOLPE NÃO ESTÁ NA MÁQUINA

Na esmagadora maioria dos casos de fraude eletrônica, o golpista não burla a tecnologia. Ele convence a vítima a abrir a porta. Um falso comunicado de banco, uma mensagem de urgência, uma oferta boa demais para ser verdadeira, um suposto parente em apuros. O alvo não é o sistema; é a pessoa. Essa constatação reorganiza tanto a prevenção quanto a investigação. Se a vulnerabilidade explorada é humana, a defesa começa no comportamento – na criação do hábito de desconfiar antes de agir. E a apuração começa na reconstrução da abordagem que conduziu a vítima ao erro: o roteiro de persuasão empregado, os canais utilizados, a infraestrutura montada para dar aparência de legitimidade ao golpe.