

COLEÇÃO

Investigação e Proteção na Era Digital

VOLUME 05

Investigação de crimes na internet

Dados, registros, sigilos e medidas judiciais



05

HIGOR VINICIUS NOGUEIRA JORGE

www.higorjorge.com.br

DISTRIBUIÇÃO
GRATUITA

HIGOR VINICIUS NOGUEIRA JORGE

Investigação de crimes na internet

Dados, registros, sigilos e medidas judiciais

Critérios para identificar fontes, preservar registros, fundamentar medidas e examinar a atribuição de autoria.

Coleção Investigação e Proteção na Era Digital
Volume 05

1ª edição
Santa Fé do Sul, SP
CodexNauta
2026

© 2026 Higor Vinicius Nogueira Jorge

Material educativo de distribuição gratuita.

Coleção Investigação e Proteção na Era Digital, volume 05.

www.higorjorge.com.br

Ficha catalográfica

Jorge, Higor Vinicius Nogueira.

Investigação de crimes na internet : dados, registros, sigilos e medidas judiciais [recurso eletrônico] / Higor Vinicius Nogueira Jorge. -- 1. ed. -- Santa Fé do Sul, SP : CodexNauta, 2026.

1 recurso online (53 p.) : il. -- (Coleção Investigação e Proteção na Era Digital ; 5)

Formato: PDF.

Modo de acesso: World Wide Web: <www.higorjorge.com.br>.

Inclui referências e apêndices.

Publicação de distribuição gratuita.

1. Crimes na internet. 2. Investigação criminal. 3. Registros de conexão e de acesso a aplicações. 4. Sigilo das comunicações. 5. Prova digital. 6. Cooperação jurídica internacional. I. Título. II. Série.

Sumário

Apresentação.....	5
Objetivos e público-alvo.....	6
1 Arquitetura da internet e investigação.....	7
2 IP, portas lógicas e limites de identificação.....	10
3 Cadastros, registros e conteúdo.....	14
4 Marco Civil e proteção de direitos.....	17
5 Identificação de usuários e atribuição.....	20
6 Preservação e obtenção de registros.....	23
7 Conteúdo e reserva de jurisdição.....	27
8 Provedores estrangeiros e cooperação.....	30
9 Caso hipotético de ameaças pela internet.....	33
10 Fundamentação e controle das medidas.....	37
Considerações finais.....	40
Apêndice A. Matriz de dados e bases legais.....	41
Apêndice B. Checklist de medidas investigativas.....	44
Apêndice C. Roteiro de planejamento investigativo.....	45
Referências.....	47
Minicurrículo do autor.....	50
Para aprofundar o estudo.....	52
A coleção.....	53

Apresentação

Uma mensagem na internet pode gerar vestígios em lugares diferentes: no aparelho de quem a recebeu, no serviço utilizado e na infraestrutura de conexão. Cada fonte registra uma parte da atividade. A investigação precisa descobrir o que existe, o que significa e como pode ser obtido regularmente.

No meu livro *Investigação criminal tecnológica*, desenvolvo as diferenças entre disponibilidade técnica e possibilidade jurídica, entre preservação e acesso, e entre correlação e atribuição pessoal. Esta cartilha aplica esses fundamentos aos dados da internet, com atenção às categorias legais e ao alcance dos registros (Jorge, 2027).

O objetivo é tornar as medidas mais precisas. Antes de requisitar ou representar, o profissional deve conseguir dizer qual pergunta pretende responder, quem provavelmente detém o dado e por que aquela intervenção é necessária. Depois da resposta, deve examinar se o registro corresponde ao evento e se sustenta a conclusão proposta.

O volume reúne arquitetura básica, IP, portas lógicas, horários, registros, sigilos e cooperação internacional. O caso hipotético demonstra como uma informação incompleta pode levar à conexão errada e como o método permite corrigir o percurso. Os apêndices oferecem matriz de dados, checklist e roteiro de planejamento.

Higor Vinicius Nogueira Jorge
www.higorjorge.com.br

Objetivos e público-alvo

Este volume se dirige a Delegados de Polícia, policiais civis, profissionais da investigação, analistas, operadores do Direito e estudantes. O leitor não precisa dominar administração de redes, mas deve compreender os elementos técnicos que condicionam um pedido e a interpretação da resposta.

Ao concluir a leitura, espera-se que consiga distinguir cadastro, registro e conteúdo; separar guarda, preservação e acesso; formular medidas delimitadas; e avaliar o que os dados permitem afirmar sobre uma atividade e sobre uma pessoa.

Como utilizar o volume

Os capítulos 1 e 2 explicam a infraestrutura e os identificadores. Os capítulos 3 e 4 articulam categorias e direitos. Os capítulos 5 a 8 desenvolvem atribuição, obtenção, sigilo e cooperação. O capítulo 9 integra esses critérios em um caso fictício. O capítulo 10 organiza a fundamentação e o controle da execução.

Os apêndices são instrumentos de trabalho. A matriz aponta o regime de referência e os cuidados essenciais, sem substituir o exame do caso. O checklist deve ser preenchido com suporte documental. O roteiro ajuda a relacionar uma hipótese à diligência capaz de diferenciá-la de outras explicações.

A Investigação Criminal Tecnológica possui alcance transversal. Embora este volume trate de fatos e fontes da internet, seus critérios também interessam à apuração de delitos de outras naturezas que produzam vestígios informacionais relevantes (Jorge, 2027).

CAPÍTULO 1

Arquitetura da internet e investigação

1.1 Fontes diferentes registram eventos diferentes

A internet conecta redes e permite que dispositivos acessem serviços. O caminho entre uma pessoa e uma aplicação pode envolver rede local, operadora, infraestrutura intermediária e servidores. A investigação não deve tratar essa cadeia como se fosse um único banco de dados.

O provedor que oferece conexão participa de uma função diferente daquela exercida pelo serviço de mensagens ou pela plataforma de publicações. A mesma organização pode exercer mais de uma função, mas é necessário identificar em qual delas produziu ou guardou o registro solicitado.

Um registro da operadora pode ajudar a relacionar uma conexão ao assinante em certo período. Um registro da aplicação pode indicar um acesso de conta a partir de determinado IP. Nenhum desses eventos deve ser descrito automaticamente como envio da mensagem que constitui o objeto da apuração.

Exemplo hipotético. A vítima apresenta uma ameaça recebida em uma plataforma. A operadora da vítima conhece sua conexão; isso não significa que detenha o conteúdo da mensagem ou os registros da conta remetente. O pedido precisa alcançar a fonte adequada.

O método do livro de referência começa pela identificação da fonte e da pergunta juridicamente relevante. Essa escolha orienta a preservação e reduz pedidos inúteis ou excessivos (Jorge, 2027).

Aprendizado. Antes de perguntar quem usou um serviço, compreenda qual atividade cada sistema poderia ter observado e em que momento ela foi registrada.

1.2 Domínio e conta não são equivalentes

O sistema de nomes de domínio, conhecido como DNS, relaciona nomes a informações sobre recursos. Um nome pode remeter a endereços ou a outros

nomes, conforme o tipo de registro. Essa organização ajuda a localizar serviços, sem estabelecer a identidade civil de quem pratica uma ação (Mockapetris, 1987).

Uma página pode utilizar infraestrutura de hospedagem e distribuição mantida por terceiros. Descobrir um endereço associado ao site pode ajudar a identificar o próximo detentor de informações. Isso não demonstra que o administrador da infraestrutura criou a publicação investigada.

Também é necessário distinguir nome exibido e identificador da conta. O nome pode ser compartilhado por pessoas diferentes ou alterado ao longo do tempo. Quando o serviço possui um identificador interno estável, registre-o junto ao endereço da página e aos elementos visíveis, indicando a origem de cada informação.

Exemplo hipotético. Uma captura mostra o perfil “Avisos da Cidade”. Outro perfil adota o mesmo nome. Para localizar a fonte do primeiro contato, a equipe conserva o endereço específico e a identificação disponível do perfil, sem pesquisar apenas a expressão exibida.

A consulta atual ao DNS ou à página registra o estado observado naquele momento. Se o fato é anterior, será necessário examinar se os dados atuais correspondem ao período investigado. O histórico não deve ser reconstruído por simples projeção do presente.

Erro frequente. Confundir o proprietário de um serviço de hospedagem com o operador de cada conta que o utiliza.

1.3 O vestígio pode estar distribuído

O dispositivo pode conservar mensagens, arquivos, notificações ou dados temporários. O serviço remoto pode conservar outros registros e versões. O que aparece na tela pode depender de sincronização, configuração e disponibilidade do servidor. A ausência de um arquivo local não demonstra que ele nunca existiu.

No livro de referência, a investigação além do dispositivo exige identificar a função da nuvem e os limites de cada fonte. A apreensão de um aparelho não

resolve, por si, a obtenção de dados remotos nem autoriza expandir o exame para qualquer conta acessível a partir dele (Jorge, 2027).

A criptografia pode limitar o conteúdo disponível ao intermediário. É necessário conhecer o serviço e o tipo de dado, sem presumir que uma ordem obriga alguém a fornecer informação que tecnicamente não possui. A procura de outra fonte continua subordinada ao fundamento jurídico correspondente.

Exemplo hipotético. Um serviço informa que não dispõe do conteúdo pretendido, mas conserva certos registros de acesso. A equipe avalia o alcance desses registros e outra fonte potencial, como os dados apresentados pelo destinatário. Não transforma a resposta técnica em prova de apagamento doloso.

Aprendizado. Mapear fontes significa registrar possibilidades e limitações. Uma fonte pode corroborar outra, revelar uma lacuna ou exigir nova diligência. A estratégia deve permitir esses retornos, com documentação e controle de escopo.

CAPÍTULO 2

IP, portas lógicas e limites de identificação

2.1 O endereço precisa de contexto

Um endereço IP participa do endereçamento na rede. No IPv6, os identificadores têm 128 bits e são atribuídos a interfaces ou conjuntos de interfaces, conforme o tipo. Um equipamento pode possuir mais de um endereço. A arquitetura não estabelece uma identidade civil permanente entre endereço e pessoa (Hinden; Deering, 2006).

Na apuração, registre a versão, o valor integral e o contexto da informação. Um IP pode aparecer como origem, destino ou endereço de um intermediário. A pergunta “a quem pertence este IP?” precisa indicar qual relação se busca: administração do bloco, atribuição de conexão ou uso efetivo em certo evento.

A informação atual sobre quem administra um bloco de endereços não substitui a identificação do assinante no momento do fato. A atribuição pode mudar. O tempo é parte da consulta, e não um detalhe a acrescentar depois.

Exemplo hipotético. Um relatório informa que um bloco é administrado por uma operadora. Esse dado orienta o destinatário de uma medida. Ainda será preciso examinar os registros do período e as condições técnicas necessárias à correlação.

Erro frequente. Escrever que o endereço “é do investigado” antes de identificar o sentido dessa relação. O relatório deve dizer se há atribuição a uma conexão, vínculo contratual, registro de conta ou outro elemento, com sua fonte e seus limites.

2.2 CGNAT e a função da porta de origem

A tradução de endereços em escala de operadora, chamada CGN ou CGNAT, permite compartilhar um endereço IPv4 entre assinantes. A tradução relaciona endereços e portas de comunicações. O registro externo precisa ser compatível com os dados que permitem desfazer essa relação no período examinado (Perreault et al., 2013).

A porta lógica é um identificador numérico associado à comunicação em protocolos de transporte. Deve-se distinguir a porta de origem da porta de destino. Informar apenas a porta de destino do serviço não resolve, em regra, a diferenciação entre assinantes que compartilham o mesmo endereço externo.

A RFC 6302 recomenda registrar porta de origem e horário preciso, preferencialmente em UTC, junto ao IP de entrada. Protocolo e porta de destino também importam nas situações indicadas no documento. Trata-se de recomendação técnica, cuja função deve ser diferenciada da base jurídica brasileira (Durand et al., 2011).

O art. 15-A do Decreto nº 8.771/2016 prevê a guarda da porta lógica de origem associada quando necessária à identificação do terminal de origem ou do próximo enlace. O dever independe de requisição prévia; o fornecimento segue o regime legal de acesso. O dispositivo foi incluído pelo Decreto nº 12.975/2026 (Brasil, 2016; Brasil, 2026).

Aprendizado. A porta auxilia uma correspondência técnica em certo contexto. Seu número não identifica sozinho a pessoa e não deve ser separado do IP, do tempo e do significado do registro.

2.3 Comparar instantes sem apagar a origem

Um horário só pode ser correlacionado corretamente quando se conhece sua referência. Preserve data, hora, segundos, fração disponível e fuso ou deslocamento informado. UTC significa Tempo Universal Coordenado. Na representação da RFC 3339, o sufixo Z indica deslocamento zero em relação a UTC (Klyne; Newman, 2002).

Exemplo hipotético. Os registros 2026-09-15T18:14:35-03:00 e 2026-09-15T21:14:35Z representam o mesmo instante. O primeiro expressa um deslocamento de três horas a menos que UTC. A conversão exige somar essas três horas. Em horários próximos da meia-noite, a data também pode mudar.

Não substitua o valor original por uma coluna convertida sem conservar a fonte e a regra aplicada. Quando o fuso não foi informado, registre a lacuna e procure esclarecimento. A localização presumida do servidor não é fundamento suficiente para escolher um fuso.

Precisão e exatidão são questões distintas. Um sistema pode mostrar milissegundos e manter o relógio incorreto. Na análise, considere sincronização, significado do evento e possíveis atrasos de registro. Esses aspectos devem ser esclarecidos quando puderem alterar a conclusão.

Erro frequente. Procurar uma assinatura com o horário local da vítima em um registro entregue em UTC. A diferença pode selecionar outra conexão ou produzir uma resposta negativa que parece descartar a hipótese.

2.4 O que muda quando falta um campo

Considere o exemplo fictício abaixo. O endereço 203.0.113.27 pertence a bloco reservado para documentação. Os campos representam registros didáticos, não uma consulta real a operadoras (Arkko; Cotton; Vegoda, 2010).

Registro	Instante em UTC	Porta externa de origem	Vínculo técnico fictício
A	15 set. 2026, 21:14:35	51020	Conexão C-01
B	15 set. 2026, 21:14:35	51021	Conexão C-02

Os dois registros utilizam o mesmo IP e, no exercício, o mesmo protocolo e destino. A diferença da porta separa as correspondências apresentadas. Se a aplicação informa apenas IP e horário, a resposta pode ser insuficiente para selecionar uma delas. É necessário esclarecer a informação faltante pela via adequada.

Outras redes podem utilizar regras de alocação diferentes, inclusive blocos de portas. Por isso, a equipe deve verificar como o provedor realizou a correspondência e quais campos efetivamente utilizou. A tabela ilustra uma possibilidade, sem impor uma arquitetura universal.

Limite. Mesmo quando C-01 é corretamente identificada, ainda não se sabe qual pessoa utilizou a conexão. A rede pode servir a diversos usuários. A correlação técnica precisa ser seguida da análise de contexto e de outras fontes.

Aprendizado. Um campo ausente não pode ser preenchido por escolha intuitiva. A insuficiência precisa aparecer no relatório e orientar uma diligência de esclarecimento.

CAPÍTULO 3

Cadastros, registros e conteúdo

3.1 A classificação começa pelo que se pede

O regime de acesso depende da natureza da informação, de quem a detém e da medida pretendida. O nome utilizado em um formulário não resolve essa classificação. Um pacote chamado “dados básicos” pode conter histórico de acesso, contatos e outras informações que exigem análise própria.

O Marco Civil distingue conexão, registros de conexão e registros de acesso a aplicações. O registro de conexão reúne informações de início, término, duração e IP. O registro de acesso a aplicação se refere ao uso da aplicação, em determinada data e hora, a partir de um IP (Brasil, 2014, art. 5º).

O primeiro ajuda a reconstruir a ligação com a rede. O segundo ajuda a compreender o acesso ao serviço. Nenhuma definição autoriza tratar como parte do cadastro todo dado que o provedor considera útil para identificar uma conta.

Exemplo hipotético. Um pedido pergunta quem cadastrou uma conta e também solicita todos os seus IPs de acesso. São objetos diferentes. A segunda parte não se torna cadastral por acompanhar a primeira na mesma requisição.

No livro de referência, a distinção entre categorias integra a legalidade da obtenção. A equipe deve descrever o campo procurado em linguagem compreensível e escolher a via correspondente, em vez de depender de um rótulo abrangente (Jorge, 2027).

Aprendizado. Classificar antes de pedir permite fundamentar, delimitar e conferir a resposta recebida.

3.2 Requisição exige competência e motivação

O art. 10, § 3º, do Marco Civil trata do acesso a dados cadastrais de qualificação pessoal, filiação e endereço por autoridades com competência legal. O art. 11 do Decreto nº 8.771/2016 exige fundamento de competência expressa, motivação,

especificação dos indivíduos e das informações. Pedidos coletivos genéricos ou inespecíficos são vedados (Brasil, 2014; Brasil, 2016).

Na investigação policial, a Lei nº 12.830/2013 prevê a requisição dos elementos pertinentes pelo Delegado de Polícia. Essa atribuição deve ser articulada ao regime específico de proteção, sem converter a requisição em autorização para alcançar registros ou conteúdo submetidos a reserva de jurisdição (Brasil, 2013).

O provedor pode não ter coletado determinado campo. A resposta deve ser examinada como informação sobre disponibilidade, sem exigir que produza retrospectivamente uma identidade que não possui. Um dado cadastral existente também pode ser falso, desatualizado ou usado indevidamente.

Exemplo hipotético. O cadastro apresenta nome de terceiro. Antes de atribuir-lhe a conta, é preciso examinar como esse nome foi inserido, quais mecanismos de verificação existiam e quem exercia o controle do serviço.

Erro frequente. Incluir localização, histórico de dispositivos ou conteúdo de mensagens sob a expressão “cadastro completo”. Cada campo adicional exige identificação de sua natureza e do fundamento para o acesso.

3.3 O registro precisa dizer o que aconteceu

Metadados descrevem aspectos de um dado ou de uma atividade, como data, formato e origem registrada. A expressão não designa uma categoria jurídica única. Certos metadados podem revelar relações, deslocamentos e padrões de comunicação, exigindo proteção compatível com sua natureza e contexto.

Ao receber um registro, pergunte se ele descreve criação de conta, autenticação, renovação de sessão, envio de conteúdo ou outra operação. Um acesso de sessão próximo ao horário da mensagem pode ser relevante, mas não comprova sozinho que aquela sessão produziu o conteúdo.

Exemplo hipotético. A aplicação fornece um evento de login às 21h10 e a vítima apresenta mensagem de 21h14. A equipe precisa verificar a relação entre os eventos. Não deve renomear o login como “envio da ameaça” para tornar a narrativa mais direta.

Peça esclarecimento sobre os campos que influenciam a interpretação. A designação de um identificador de aparelho, por exemplo, pode corresponder a valor atribuído pelo serviço e sujeito a alteração, sem representar uma identificação física universal do equipamento.

Aprendizado. A categoria legal organiza o acesso; o significado técnico organiza a inferência. A boa análise conserva ambas. O livro de referência exige que a passagem do registro à conclusão permaneça verificável, com origem e limitações declaradas (Jorge, 2027).

CAPÍTULO 4

Marco Civil e proteção de direitos

4.1 A intervenção começa na finalidade

A Constituição protege intimidade, vida privada, sigilo e dados pessoais. A investigação deve delimitar o fato e justificar a relação entre a medida e o conhecimento pretendido. O exercício de uma competência não afasta a necessidade de adequação e proporcionalidade (Brasil, 1988, art. 5º).

O Marco Civil articula esses direitos à guarda e ao fornecimento de informações. Para registros protegidos e conteúdo privado mantidos pelo provedor, o pedido precisa observar o regime legal e a reserva de jurisdição. A existência de uma apuração não permite acesso indiscriminado a toda a vida digital do investigado (Brasil, 2014).

Uma boa finalidade é formulada como pergunta verificável. “Identificar o acesso associado à conta no intervalo das mensagens” permite discutir necessidade e alcance. “Conhecer tudo sobre o usuário” não delimita um objeto investigativo suficiente.

Exemplo hipotético. A equipe pretende confirmar a origem de duas publicações em dias determinados. Um histórico de vários anos exige justificativa adicional. A ampliação não decorre apenas da facilidade de gerar um arquivo maior.

No livro de referência, o limite jurídico integra o método desde a identificação. A motivação deve anteceder a coleta e orientar os retornos a novas fontes, sem ser produzida apenas para justificar dados já obtidos (Jorge, 2027).

Aprendizado. A pergunta define o que é relevante e permite explicar por que a restrição proposta é necessária.

4.2 Delimitar pessoas, campos e tempo

A delimitação deve alcançar a pessoa ou conta, os campos, o período e o evento procurado. Se um identificador ainda é desconhecido, explique a lacuna e os

elementos que permitem localizar a fonte. A falta de um nome civil não autoriza uma consulta sem limites.

A necessidade deve ser avaliada diante das alternativas disponíveis e de sua utilidade concreta. Uma fonte menos intrusiva pode responder à pergunta com menor exposição. Se for insuficiente, descreva o que falta e por que a medida seguinte acrescenta informação relevante.

Exemplo hipotético. A vítima possui a mensagem recebida, mas o remetente é desconhecido. O acesso ao conteúdo de todas as conversas da conta não é consequência automática dessa dúvida. Registros delimitados podem ser uma etapa útil para identificar conexões, conforme os fundamentos e autorizações exigidos.

A análise precisa considerar terceiros. Uma conta pode reunir comunicações profissionais, familiares e assuntos sem relação com o fato. O pedido e a execução devem prever tratamento restrito, segregação e apresentação contextualizada do material pertinente.

O livro de referência destaca que a agregação pode revelar mais que cada dado isolado. Ao reunir acessos, contatos e deslocamentos, a equipe deve reavaliar a intensidade da intervenção e o suporte jurídico do conjunto (Jorge, 2027).

Erro frequente. Defender uma coleta ampla apenas porque o sistema permite filtrá-la depois. A disponibilidade de um filtro não substitui a justificativa para obter o material.

4.3 O acesso autorizado também exige proteção

O art. 4º, III e § 1º, da LGPD diferencia o tratamento para investigação e repressão penal e conserva exigências de proporcionalidade, devido processo e direitos. A exclusão do regime geral não cria liberdade para circulação irrestrita de informações (Brasil, 2018).

A equipe precisa definir onde os dados serão recebidos, quem poderá acessá-los e como o tratamento será registrado. Informações de terceiros devem ser limitadas ao necessário e protegidas na apresentação. A guarda institucional e a

destinação posterior seguem o regime aplicável, inclusive determinações judiciais.

Uma ordem judicial constitui fundamento para a medida que efetivamente autorizou. Ela não resolve automaticamente falhas de execução, excesso de escopo ou problemas de integridade. A conferência continua depois do deferimento e deve identificar o que foi entregue e utilizado.

Exemplo hipotético. O provedor encaminha dados de período maior que o autorizado. A equipe documenta o excesso, restringe o tratamento e submete a situação à autoridade competente, sem explorar o material como se a entrega tivesse ampliado a decisão.

A documentação deve permitir o controle pelos sujeitos processuais nos limites legais. Sigilo da diligência e direito de acesso não são questões resolvidas por uma classificação genérica de toda a investigação como secreta.

Aprendizado. Legalidade da obtenção, rastreabilidade e proteção são deveres complementares. O volume recebido só se torna útil quando seu alcance pode ser compreendido e examinado criticamente.

CAPÍTULO 5

Identificação de usuários e atribuição

5.1 A cadeia de relações precisa ser demonstrada

A investigação pode percorrer relações entre publicação, conta, sessão, conexão, contrato e pessoa. Cada passagem depende de informação própria. A existência de uma dessas relações não autoriza preencher automaticamente as demais.

A conta pode estar cadastrada em nome de alguém que não controla seu uso. A conexão pode atender a uma residência, organização ou rede compartilhada. O aparelho pode ser utilizado por mais de uma pessoa. Essas possibilidades precisam ser avaliadas conforme o caso, sem presumir que toda explicação alternativa será verdadeira.

Exemplo hipotético. Uma conta usa uma conexão contratada por uma empresa. O contrato identifica a organização; não demonstra qual empregado operou a conta. A pesquisa deve verificar o acesso pertinente e suas condições, com diligências necessárias e legalmente autorizadas.

No método do livro de referência, a correlação organiza elementos e a interpretação testa seu significado. O Controle de Viés Investigativo exige explicação alternativa plausível, apoio potencial e diligência capaz de diferenciá-la da hipótese principal (Jorge, 2027).

A conclusão deve individualizar ações. “A conexão foi atribuída ao contrato C-01” é uma afirmação técnica. “A pessoa enviou a mensagem” exige suporte sobre o uso e a conduta. O relatório deve apresentar as fontes que permitem passar de uma afirmação à outra.

Aprendizado. Identificar o primeiro vínculo útil inicia uma etapa de verificação, sem encerrar a apuração da autoria.

5.2 Atribuir uma ação exige considerar o momento

O controle de uma conta pode mudar ao longo do tempo. Recuperações de acesso, compartilhamento de credenciais e sessões persistentes afetam o significado dos registros. Um cadastro atual ou um acesso posterior pode não representar a situação existente no instante investigado.

Ao analisar, separe os eventos anteriores, contemporâneos e posteriores ao fato. Pergunte que informação permite relacionar uma pessoa à ação específica e qual apenas demonstra vínculo geral com o serviço. A proximidade temporal deve ser explicada, sem receber valor causal automático.

Exemplo hipotético. O titular relata que perdeu o acesso antes das mensagens. A equipe busca elementos sobre recuperação e sessões no intervalo pertinente. A alegação é uma versão a verificar; o cadastro não a descarta e a simples afirmação também não a confirma.

Recursos de intermediação, como redes privadas virtuais e serviços de retransmissão, podem fazer com que o IP observado corresponda a um intermediário. Isso exige compreender a fonte e os dados disponíveis. Não se deve concluir que o uso de um intermediário prova intenção criminosa.

A investigação precisa registrar as limitações do percurso. Se uma etapa não pode ser esclarecida, outras fontes podem sustentar ou enfraquecer hipóteses, mas o elo ausente não deve desaparecer da apresentação.

Erro frequente. Utilizar a mesma palavra “usuário” para designar sucessivamente conta, assinante e pessoa física. A redação deve indicar qual desses sentidos está efetivamente demonstrado.

5.3 Verificar se as fontes acrescentam informação

A corroboração deve considerar a origem dos elementos. Uma captura, sua transcrição e um relatório que reproduz a transcrição podem derivar do mesmo registro. A quantidade de documentos não os transforma em três confirmações independentes.

É útil organizar uma matriz com a afirmação, a fonte original, o alcance e a explicação alternativa. Dados de conta e de conexão podem ser combinados

com informações documentais e testemunhais regularmente obtidas. Cada relação deve permanecer compreensível e sujeita a revisão.

Exemplo hipotético. Uma testemunha diz reconhecer o estilo de escrita do remetente. A impressão pode orientar uma pergunta, mas precisa ser confrontada com outras informações. A repetição dessa avaliação em dois depoimentos não substitui o exame da base de cada reconhecimento.

O mesmo vale para ferramentas que apresentam localização aproximada ou classificação de um endereço. A saída deve ser tratada conforme a fonte e a precisão demonstráveis. Um ponto exibido em um mapa não posiciona automaticamente o aparelho no imóvel ali representado.

O livro de referência recomenda testar alternativas e distinguir padrão, indício e conclusão. A análise precisa considerar elementos exculpatórios com o mesmo cuidado dedicado aos que reforçam a suspeita (Jorge, 2027).

Aprendizado. Corroborar significa acrescentar suporte pertinente. O relatório deve mostrar como as informações se relacionam e quais questões continuam sem resposta, em vez de apenas acumular referências.

CAPÍTULO 6

Preservação e obtenção de registros

6.1 Guarda obrigatória e disponibilidade real

O art. 13 do Marco Civil prevê guarda de registros de conexão por um ano. O art. 15 prevê seis meses para registros de acesso a aplicações nas condições de organização, profissionalidade e finalidade econômica ali indicadas. As obrigações têm objetos e destinatários próprios. Para outros provedores, o art. 15, § 1º, prevê determinação judicial de guarda sobre fatos específicos e período determinado (Brasil, 2014).

Esses prazos não instituem um arquivo universal do conteúdo da internet. Não significam que toda mensagem, imagem, contato ou localização será guardada pelo mesmo período. Também não autorizam obter os registros sem observar a via jurídica pertinente.

O art. 15-A do Decreto nº 8.771/2016 integra ao dever de guarda a porta lógica de origem quando necessária à identificação técnica indicada no dispositivo. É preciso conferir a implementação, a abrangência temporal e os campos disponíveis no caso, sem presumir que a obrigação recria dados que não foram conservados (Brasil, 2016).

Exemplo hipotético. Uma aplicação responde com registro sem porta de origem. A equipe precisa esclarecer se o dado foi omitido da entrega, se existe em outro campo ou se não está disponível. A ausência na planilha não demonstra, sozinha, qual dessas situações ocorreu.

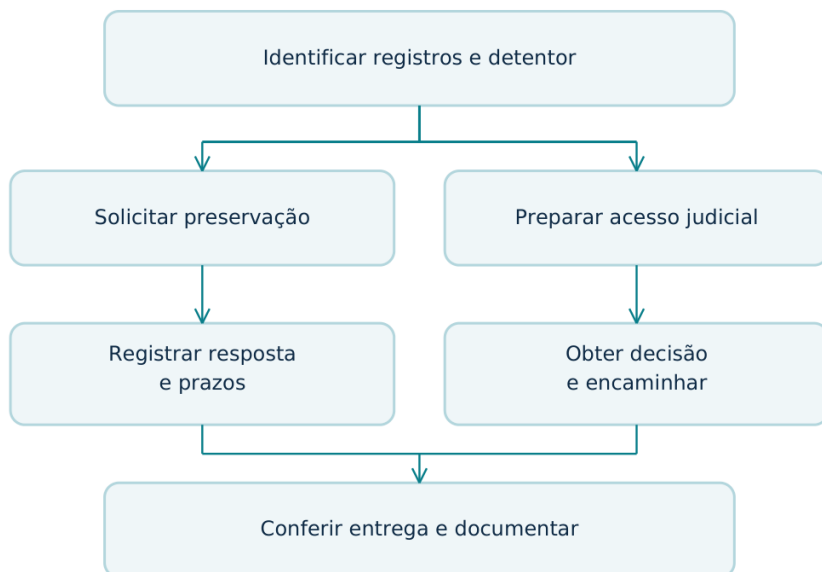
Erro frequente. Aguardar o final do prazo de guarda para pedir preservação. O planejamento deve considerar risco de perda, identificação correta e controle do acesso formal. A preservação não recupera automaticamente o que já deixou de existir.

6.2 Providências diferentes podem caminhar juntas

Preservar é buscar a conservação do dado para uma obtenção posterior. A solicitação precisa identificar os registros, o detentor, o intervalo e a relação

com o fato. O pedido de acesso deve ser preparado em paralelo, sem depender de uma espera desnecessária pela confirmação da preservação.

Figura 1. Preservação de registros e preparação do acesso



Fonte: elaboração própria. A figura trata de registros cujo fornecimento depende de autorização judicial. A resposta de preservação não entrega os dados, não amplia o escopo e não substitui a decisão de acesso.

Os arts. 13 e 15 do Marco Civil disciplinam o requerimento cautelar e a autorização para disponibilizar registros. A equipe deve registrar datas, resposta, alcance e providência judicial correspondente (Brasil, 2014).

6.3 Controlar a preservação de forma verificável

No regime do art. 13, § 3º, do Marco Civil, a autoridade requerente tem sessenta dias, contados do requerimento, para ingressar com o pedido de autorização judicial de acesso. Os arts. 13, § 4º, e 15, § 2º, disciplinam os efeitos e a aplicação desse controle aos registros pertinentes. A referência do prazo deve acompanhar o ato praticado (Brasil, 2014).

Não confunda esse marco com a data em que o servidor respondeu nem com um prazo informado em portal privado. Um controle interno deve registrar fundamento, início, vencimento, responsável e comprovante do pedido judicial. Eventuais regimes distintos precisam ser identificados, sem misturar regras nacionais e internacionais.

Delimite o intervalo segundo os eventos conhecidos e justifique uma margem quando tecnicamente necessária. A incerteza de horário pode justificar esclarecimento ou uma extensão motivada. Não autoriza escolher um período amplo sem explicar sua utilidade.

Exemplo hipotético. A captura mostra apenas o minuto do contato. O pedido registra essa limitação e justifica o intervalo para localizar o evento no serviço. A resposta será examinada antes de associar cada acesso à mensagem.

Aprendizado. O protocolo de preservação integra a rastreabilidade da diligência. Se a confirmação não chegou, registre a pendência e as ações realizadas. Silêncio do detentor não pode ser descrito como conservação comprovada.

6.4 Receber dados também é uma etapa de controle

Ao receber a resposta, confira remetente, referência do pedido, conta, período e descrição dos campos. Preserve os arquivos entregues e documente o recebimento. Trabalhe sobre cópias adequadas, com registro das transformações e das ferramentas utilizadas.

Verifique se a tabela contém registros completos, filtros aplicados ou anexos ausentes. Antes de converter horários ou relacionar identificadores, compreenda o significado de cada coluna. Solicite esclarecimento quando a interpretação puder alterar uma conclusão.

Exemplo hipotético. Um campo chamado “porta” aparece no arquivo, sem dizer se corresponde à origem ou ao destino. A equipe conserva a resposta e pede a definição. Não utiliza o valor como porta de origem apenas porque essa era a informação desejada.

Uma resposta negativa pode significar ausência do evento, erro no identificador, intervalo inadequado, indisponibilidade do dado ou outra circunstância. O relatório deve reproduzir o alcance real da resposta. “Nada foi encontrado” não equivale necessariamente a “o fato não ocorreu”.

A documentação da cadeia de custódia prevista no CPP e o método do livro de referência orientam a conservação da origem e das movimentações do material. Um hash pode apoiar o controle de integridade de arquivos, sem comprovar a verdade do conteúdo nem a identidade do usuário (Brasil, 1941; Jorge, 2027).

Aprendizado. O resultado só deve ser incorporado à análise depois de conferido no objeto e no contexto em que foi produzido.

CAPÍTULO 7

Conteúdo e reserva de jurisdição

7.1 Conteúdo armazenado exige objeto próprio

O Marco Civil protege as comunicações privadas armazenadas e disciplina seu fornecimento pelo provedor mediante ordem judicial. O pedido precisa identificar a conta, o período e o conteúdo pertinente, com fundamento na necessidade do acesso. A existência de registros de login não autoriza obter, por extensão, o histórico de conversas (Brasil, 2014, arts. 7º e 10).

O conteúdo já armazenado corresponde a um objeto diferente da captação de comunicações em curso. A distinção deve aparecer na descrição da medida. Expressões genéricas, como “quebra do sigilo telemático”, podem esconder objetos de alcance muito diferente.

Exemplo hipotético. A equipe procura uma mensagem produzida em data anterior e conservada em serviço remoto. Deve formular o pedido de acesso ao material armazenado. Não deve descrevê-lo como interceptação futura nem utilizar uma autorização limitada a registros como fundamento suficiente.

A delimitação inclui o que não é necessário. Se a conta é utilizada para diversos fins, justifique os critérios que relacionam o conteúdo ao fato. O tratamento de material excedente exige registro e controle, inclusive quando não for possível uma filtragem prévia completa.

Aprendizado. A medida deve ser identificada pelo que alcança e pela forma de obtenção. A adoção de um nome comum não supre o exame do regime jurídico.

7.2 Interceptação depende de requisitos específicos

A Lei nº 9.296/1996 alcança a interceptação de comunicações telefônicas e do fluxo em sistemas de informática e telemática. Exige ordem judicial e os pressupostos legais, incluindo indícios razoáveis de autoria ou participação, necessidade diante de outros meios disponíveis e compatibilidade com a natureza da infração investigada (Brasil, 1996).

A lei veda a interceptação para fato que constitua infração punida, no máximo, com detenção. A forma do caput do art. 147 do Código Penal é exemplo dessa limitação. O uso de aplicativo não altera automaticamente a pena nem cria os pressupostos de uma medida mais intrusiva (Brasil, 1940; Brasil, 1996).

O pedido deve explicar a situação, o objeto e os meios pretendidos. A impossibilidade de qualificar previamente uma pessoa precisa ser justificada. O art. 5º da lei exige decisão fundamentada e disciplina duração e renovação, com demonstração de indispensabilidade. Esses controles devem acompanhar a execução, sem tratar a prorrogação como automática (Brasil, 1996).

Exemplo hipotético. Uma equipe possui mensagens já recebidas e pretende identificar seu remetente. Deve examinar as fontes existentes e os registros disponíveis antes de propor captação futura. A conveniência de acompanhar comunicações não demonstra necessidade jurídica.

Erro frequente. Agravar artificialmente a classificação do fato para viabilizar a técnica. O enquadramento decorre dos elementos apurados, e os requisitos da medida precisam ser demonstrados no caso concreto.

7.3 A origem do material modifica a análise

A entrega de uma mensagem recebida por seu destinatário difere de uma requisição ao provedor para fornecer comunicações privadas. É preciso registrar quem apresentou o material, como o obteve e em quais condições foi conservado. A apresentação não dispensa exame de autenticidade, contexto e pertinência.

Essa entrega também não deve ser interpretada como autorização irrestrita para pesquisar o aparelho ou as contas da pessoa. O objeto de qualquer exame adicional precisa ser definido, com seu fundamento e com a via jurídica adequada. Em situações de dúvida relevante sobre o alcance, o controle judicial deve ser buscado antes da intervenção.

O livro de referência distingue apreensão física e acesso ao conteúdo. A posse do equipamento pela equipe não substitui a autorização para uma medida que penetre dados protegidos ou fontes remotas (Jorge, 2027).

Exemplo hipotético. A vítima apresenta a conversa em que recebeu a ameaça. O recebimento desse material não autoriza explorar todas as suas contas, nem acessar a conta do remetente mediante uma sessão disponível no aparelho.

Aprendizado. Documente a fonte efetivamente utilizada. Um arquivo fornecido por interlocutor, uma aquisição pericial e uma resposta de provedor conservam trajetórias diferentes. A apresentação deve permitir examinar cada percurso e seus limites, sem tornar equivalentes procedimentos juridicamente distintos.

7.4 A decisão não cria disponibilidade técnica

A criptografia de ponta a ponta pode impedir que o intermediário disponha do conteúdo em formato acessível. A situação depende do serviço, da configuração e do tipo de informação. Não se deve presumir que todos os dados estão no servidor nem que a ausência de conteúdo torna inúteis os demais vestígios (Jorge, 2027).

A resposta técnica deve ser examinada no objeto exato. A indisponibilidade de uma mensagem pode coexistir com registros de acesso disponíveis. Cópias ou dados em outros locais exigem identificação da fonte e fundamento próprio, sem expansão automática da autorização inicial.

Urgência também precisa de enquadramento. Uma política privada de atendimento emergencial não é uma autorização jurídica geral. Da mesma forma, hipóteses legais especiais de localização, como a do art. 13-B do CPP, têm pressupostos e alcance próprios; não podem ser transportadas para qualquer investigação na internet (Brasil, 1941).

Exemplo hipotético. Há risco atual relatado pela vítima e necessidade de proteção. A equipe organiza as providências urgentes cabíveis, documenta o risco e aciona os canais competentes. Não confunde esse atendimento com permissão automática para obter conteúdo protegido.

Aprendizado. A necessidade de resposta rápida exige coordenação e fundamento identificável. A estratégia deve buscar o que é tecnicamente disponível pela via legal pertinente e declarar quando uma fonte não consegue responder à pergunta.

CAPÍTULO 8

Provedores estrangeiros e cooperação

8.1 Sede, armazenamento e serviço são relações distintas

O art. 11 do Marco Civil estabelece critérios de aplicação da legislação brasileira, inclusive para pessoa jurídica sediada no exterior nas condições do dispositivo. A localização estrangeira de um servidor não exclui automaticamente esse regime, assim como a existência de representante no Brasil não resolve toda dificuldade de obtenção (Brasil, 2014).

Identifique qual entidade presta o serviço, quem detém os dados e qual canal recebe medidas da autoridade. A resposta pode indicar custódia em outra entidade ou exigência jurídica adicional. Essas informações precisam ser verificadas e incorporadas ao planejamento.

O livro de referência trata a nuvem e a cooperação como dimensões do método. A investigação deve antecipar a preservação e preparar o acesso formal, considerando os limites do detentor e o ordenamento pertinente (Jorge, 2027).

Exemplo hipotético. Um serviço com atuação no Brasil recebe ordem delimitada e informa que parte dos dados depende de processamento por entidade estrangeira. A equipe documenta a resposta, avalia o cumprimento e consulta a via de cooperação cabível, sem presumir que um portal privado substitui a análise jurídica.

Erro frequente. Confundir política empresarial e norma de competência. A documentação do serviço ajuda a encaminhar o pedido e compreender os campos. Ela não amplia os poderes da autoridade nem afasta as exigências legais de sigilo e controle.

8.2 Preservação internacional e obtenção formal

A Convenção sobre o Crime Cibernético, promulgada pelo Decreto nº 11.491/2023, disciplina mecanismos de cooperação. Os arts. 29 e 31 distinguem conservação expedita e assistência para acesso aos dados armazenados. O art.

35 prevê contato disponível continuamente para a assistência ali descrita (Brasil, 2023).

Na formulação, identifique autoridade, fato, dados, relação com o crime, provável detentor e necessidade da conservação. A providência urgente deve estar articulada ao procedimento de obtenção. Confirmação de conservação não deve ser registrada como entrega ou autorização para examinar o conteúdo.

A autoridade central e a via competente devem ser confirmadas no instrumento aplicável. O DRCI, no âmbito do MJSP, atua na tramitação de pedidos de cooperação penal. A análise considera legislação, acordos e requisitos do Estado requerido, sem substituir as decisões jurisdicionais necessárias (Brasil. Ministério da Justiça e Segurança Pública, 2026).

Exemplo hipotético. Há risco de perda de registros em outro país. A autoridade aciona a conservação pela via cabível e prepara o pedido formal com identificação, período e finalidade. O acompanhamento registra o marco de cada procedimento, sem aplicar automaticamente a todos o prazo do Marco Civil.

Aprendizado. A cooperação precisa ser planejada como uma sequência de atos documentados. Rapidez na conservação e precisão na obtenção se complementam, respeitados os regimes de cada via.

8.3 O acesso remoto conserva limites territoriais

A Convenção de Budapeste contempla, no art. 32, acesso a dados publicamente disponíveis e uma hipótese de acesso ou recebimento com consentimento legítimo e voluntário de pessoa com autoridade legal para revelar os dados. O dispositivo não autoriza exploração geral de contas ou sistemas estrangeiros (Brasil, 2023).

A existência de uma senha ou sessão aberta não demonstra, por si, autoridade legal para revelar todos os dados acessíveis. É preciso examinar quem consente, qual o objeto e quais direitos estão envolvidos. Quando a medida exige cooperação ou autorização específica, a facilidade técnica não dispensa essa via.

Exemplo hipotético. Uma pessoa pode apresentar arquivos de que dispõe, mas não possui poder para permitir o exame de todas as contas de uma organização. A equipe registra a origem do material e delimita o alcance de qualquer diligência adicional.

O pedido formal deve utilizar linguagem compreensível ao destinatário estrangeiro, explicar a relação dos dados com o fato e indicar as condições de tratamento. Tradução, autenticação e requisitos de tramitação devem seguir o instrumento e as orientações da autoridade central competente.

Aprendizado. A localização dos dados exige coordenação jurídica, sem alterar a obrigação de demonstrar pertinência e limitar a intervenção. A apresentação final deve conservar o percurso internacional, os documentos de encaminhamento e as condições comunicadas para a utilização do material.

CAPÍTULO 9

Caso hipotético de ameaças pela internet

9.1 Notícia do fato e fontes iniciais

Este caso é inteiramente fictício. Pessoas, contas, contratos, mensagens e respostas foram criados para fins didáticos. O IP utilizado pertence a bloco de documentação. Nenhum pedido foi enviado a provedores reais.

Bruno apresenta duas mensagens que anunciam a prática de mal injusto e grave contra ele. No exercício, foram recebidas em 15 de setembro de 2026, às 18h14min35s e 18h18min10s, com deslocamento informado de -03:00. O perfil remetente possui o identificador fictício F-17. As mensagens são designadas M-81 e M-82.

A equipe registra o relato R-01, conserva o material apresentado D-01 e identifica a forma de apresentação dos horários. Bruno formaliza sua representação quanto à ameaça descrita. A autoridade aprecia as condições legais e as medidas de proteção cabíveis. O enquadramento inicial do exercício é o art. 147, caput, sem elementos adicionais que indiquem outro delito (Brasil, 1940).

A primeira pergunta é se os dados permitem relacionar as mensagens à conta e aos acessos pertinentes. A hipótese inicial é controle da conta por quem executou os envios. A alternativa é uso da conta por terceiro. Nenhuma delas está demonstrada pelo nome exibido.

Decisão inicial. Identificar a fonte e preservar os registros pertinentes, com delimitação do período, enquanto se prepara o acesso pela via judicial cabível. A autoria pessoal permanece como questão a investigar.

9.2 Vincular cada dado a uma pergunta

O plano separa cadastro, registros de acesso e conteúdo já apresentado. A existência de D-01 não torna necessário pedir todas as conversas do perfil. O requerimento de registros identifica F-17, as mensagens e o intervalo motivado para localizar os eventos, com horário original e conversão documentada.

Pergunta	Fonte e objeto pretendidos	Limite a observar
A conta corresponde ao contato?	Identificação disponível do perfil e D-01.	Nome exibido não basta.
Que eventos ocorreram no intervalo?	Registros pertinentes da aplicação.	Distinguir acesso e envio.
Que conexão corresponde ao evento?	Dados técnicos completos e resposta do provedor de conexão.	Controlar porta, protocolo e horário.
Quem efetivamente utilizou a conta?	Corroboração posterior e diligências delimitadas.	Cadastro não demonstra a conduta.

A representação expõe indícios do ilícito, utilidade dos registros e período, conforme o art. 22 do Marco Civil. Não pede captação futura: os pressupostos de interceptação não decorrem da necessidade de identificar o remetente e não estão presentes na configuração didática do fato (Brasil, 2014; Brasil, 1996).

Controle. O protocolo de preservação P-01 e o encaminhamento judicial J-01 são registrados separadamente. A equipe acompanha seus próprios marcos, a resposta e a abrangência efetivamente confirmada. Os códigos representam peças fictícias e permitem mostrar a origem de cada informação utilizada na análise.

9.3 Corrigir a correspondência antes de atribuir

No exercício, a primeira resposta da aplicação, D-02, informa login às 21h13min58sZ e IP 203.0.113.27, sem porta de origem. Esse registro não documenta diretamente M-81. A equipe pede esclarecimento dentro do objeto autorizado, sem selecionar um assinante por aproximação.

A resposta complementar D-03 informa o evento de envio de M-81 às 21h14min35sZ, com o mesmo IP, porta externa de origem 51020 e protocolo TCP. Também explica o significado dos campos. A conversão coincide com o horário de D-01, sem apagar os valores originais.

A resposta fictícia D-04 do provedor de conexão, obtida pela via cabível, associa esses campos à conexão C-01. No mesmo instante, a porta 51021 corresponderia a C-02. D-04 identifica C-01 como conexão de uma pequena empresa. Esses dados ilustram a diferença entre IP compartilhado e correspondência individualizada da conexão.

Correção metodológica. D-02 permanece conservado como primeiro resultado. D-03 acrescenta um evento mais específico e um campo necessário à distinção. Não se reescreve o login anterior como se ele já tivesse documentado o envio.

Limite. A correspondência com C-01 ainda não identifica quem utilizou a rede. A coincidência entre horário, conta e conexão reforça uma relação técnica; a participação pessoal depende de outras verificações.

9.4 O resultado técnico orienta novas diligências

No prosseguimento fictício, o responsável pela empresa informa que a rede era usada por empregados e visitantes. Essa versão é registrada em R-02, sem ser tratada como comprovação do usuário de F-17. A equipe verifica quais fontes pertinentes existem e delimita as diligências necessárias à análise do uso no momento dos envios.

O Controle de Viés Investigativo organiza duas explicações: uso por pessoa vinculada à empresa e uso por terceiro com acesso à rede ou à conta. Para distingui-las, o plano indica examinar registros institucionais pertinentes, condições de acesso e relatos com fonte de conhecimento identificada, observados os fundamentos e as autorizações exigidos.

Conclusão do exercício. D-01 documenta o material apresentado. D-03 e D-04 sustentam, no cenário construído, a correspondência entre o envio de M-81 e C-01. R-02 informa uma condição de compartilhamento ainda sujeita a verificação. O conjunto descrito não permite atribuir a mensagem a uma pessoa determinada.

O relatório registra o avanço e as pendências. Se a finalidade for subsidiar decisão posterior, deve deixar clara a diferença entre conta, conexão e conduta. Não há indiciamento automático do titular do contrato.

Aprendizado. Uma investigação pode produzir resultado técnico relevante e conservar questão de autoria em aberto. Declarar esse limite permite escolher a diligência seguinte e evita que uma hipótese passe a circular como fato estabelecido.

CAPÍTULO 10

Fundamentação e controle das medidas

10.1 Explicar a necessidade com suporte concreto

Uma medida deve começar pelo fato e pelos elementos já disponíveis. Indique o que se pretende esclarecer, qual dado pode responder à pergunta e por que o detentor escolhido provavelmente o possui. A fundamentação técnica e a jurídica precisam se referir ao mesmo objeto.

Para o pedido de registros, o art. 22 do Marco Civil exige indícios do ilícito, motivação da utilidade e período. A demonstração deve conectar esses requisitos aos documentos do caso. Copiar a descrição abstrata do artigo não explica por que determinado intervalo ou campo é necessário (Brasil, 2014).

Exemplo hipotético. A mensagem tem identificador e horário conhecidos, mas o pedido solicita todos os acessos da conta desde sua criação. A revisão precisa esclarecer que questão exige esse período. Se não houver fundamento, o pedido deve ser ajustado ao intervalo pertinente.

Quando uma etapa anterior não esclareceu o fato, descreva a resposta e a lacuna. Uma medida mais intrusiva exige demonstrar por que acrescenta informação útil e por que alternativas suficientes não estão disponíveis. A avaliação deve conservar os requisitos próprios de cada técnica.

O livro de referência orienta a formular a pergunta antes da busca e a registrar os retornos do método. A decisão deve poder ser compreendida pelo profissional que recebe os dados e pelos sujeitos que examinarão a conclusão (Jorge, 2027).

Aprendizado. A motivação vincula o dado à hipótese e limita a execução. Sua qualidade será medida pela clareza dessa relação.

10.2 Tornar o pedido executável e conferível

O objeto deve identificar conta ou referência conhecida, tipo de evento, campos, intervalo e referência temporal. Quando se procura correspondência em rede

compartilhada, explicita IP, porta de origem e os demais campos pertinentes disponíveis. Se um campo está ausente, declare a lacuna e a providência de esclarecimento.

Diferencie no pedido os registros, os dados cadastrais e o conteúdo eventualmente necessário. Indique a base de cada parte e evite fórmulas como “todos os dados disponíveis”. A individualização permite ao destinatário compreender o objeto e à equipe conferir a entrega.

Exemplo hipotético. Um arquivo é entregue em formato de tabela, com datas convertidas pelo provedor. A resposta deve explicar a referência temporal e os filtros aplicados. A equipe conserva o arquivo recebido e registra qualquer transformação adicional.

O art. 15 do Decreto nº 8.771/2016 prevê formato interoperável e estruturado para os dados abrangidos. A utilidade operacional não dispensa as diretrizes de segurança. O profissional deve definir canal institucional de recebimento e preservação do material (Brasil, 2016).

Também é preciso planejar responsáveis e prazos. Registre quem acompanha a preservação, o pedido judicial, eventual cooperação e os esclarecimentos. A representação não termina no protocolo; sua execução precisa de controle.

Erro frequente. Solicitar uma técnica que o serviço não consegue executar ou um campo sem significado definido. O diálogo técnico deve esclarecer a possibilidade sem ampliar informalmente o objeto autorizado.

10.3 Relacionar conclusão, fonte e limite

Antes de apresentar resultados, confira se cada afirmação corresponde ao registro de origem. Separe fatos documentados, versões, inferências e hipóteses. Uma tabela de acessos deve permitir recuperar a resposta de onde veio, o pedido que a fundamentou e as transformações realizadas.

O relatório precisa demonstrar a passagem entre os vínculos técnicos e a participação individual, quando houver suporte. Se essa passagem não foi esclarecida, indique a questão pendente e as diligências pertinentes. A força de uma conclusão não decorre do número de linhas processadas.

Na investigação policial, o Delegado de Polícia conduz a apuração e decide o indiciamento por ato fundamentado nos termos da Lei nº 12.830/2013. O resultado analítico ou pericial subsidia essa atividade sem substituir a decisão da autoridade (Brasil, 2013).

Exemplo hipotético. O analista relaciona um acesso ao contrato de uma pessoa. A redação final deve conservar essa descrição, a menos que outros elementos permitam sustentar que ela executou a conduta. O cargo ou a experiência de quem interpreta não substituem a fonte.

Aprendizado. O controle de qualidade pergunta se a medida foi adequada, se a execução respeitou o objeto e se a conclusão pode ser conferida. Os apêndices ajudam a registrar essas respostas, sem transformar o preenchimento de campos em certificação automática da prova.

Considerações finais

Investigar crimes na internet exige compreender o que cada registro representa e como ele pode ser obtido. Um identificador, isoladamente, costuma oferecer uma relação parcial. A utilidade investigativa aparece quando a equipe consegue situar essa informação na arquitetura do serviço, no tempo e no contexto do fato.

A classificação dos dados orienta o fundamento e a via de acesso. Cadastros, registros e conteúdo possuem diferenças que precisam aparecer nos pedidos. Preservação, fornecimento e captação futura também demandam tratamentos próprios. Essa precisão protege direitos e evita diligências que não respondem à pergunta investigativa.

A etapa seguinte é interpretar. A conexão correta pode continuar compartilhada; uma conta pode ter sido utilizada por terceiro; um evento de login pode não corresponder ao envio da mensagem. O método precisa examinar alternativas e conservar os limites na apresentação.

O livro de referência propõe uma Investigação Criminal Tecnológica transversal, organizada pela identificação, preservação, obtenção, tratamento, correlação, interpretação e apresentação dos vestígios informacionais. Neste volume, esses fundamentos orientam tanto a escolha da fonte quanto o controle da conclusão (Jorge, 2027).

Os instrumentos seguintes reúnem categorias, verificações e planejamento. Sua aplicação deve conservar a pergunta concreta, a competência, a necessidade e a rastreabilidade. O objetivo é produzir conhecimento que possa ser explicado, revisado e juridicamente examinado.

APÊNDICE A

Matriz de dados e bases legais

A.1 Fontes e categorias iniciais

A matriz indica o regime de referência. A decisão depende do campo, do detentor, da finalidade e das condições do caso. Não se deve agrupar objetos diferentes em uma única autorização genérica.

Objeto	Via e base de referência	Cautela essencial
Publicação ostensivamente acessível	Consulta lícita e documentação; Constituição, art. 5º.	Registrar contexto e não contornar barreiras.
Qualificação, filiação e endereço	Requisição por autoridade com competência legal; MCI, art. 10, § 3º; Decreto nº 8.771, art. 11.	Motivar e individualizar; cadastro pode ser inexato.
Registros de conexão	Fornecimento judicial; MCI, arts. 10, 13 e 22.	Distinguir conexão, assinante e pessoa.

A atribuição de requisição prevista na Lei nº 12.830/2013 não afasta os regimes específicos de sigilo. Nos dados cadastrais, indique o fundamento de competência, as informações necessárias e os indivíduos abrangidos.

A consulta a fonte aberta também deve ter finalidade e proporção. O acesso público a um registro não autoriza explorar contas privadas nem dispensar proteção dos dados reunidos na investigação.

Fonte: síntese dos capítulos 3 e 4, Constituição, Marco Civil, Decreto nº 8.771/2016 e Lei nº 12.830/2013.

A.2 Registros e comunicações

Objeto	Via e base de referência	Cautela essencial
Registros de acesso a aplicação	Fornecimento judicial; MCI, arts. 10, 15 e 22.	Definir evento e conservar fuso e campos.
Porta lógica de origem associada	Regime dos registros; Decreto n° 8.771, art. 15-A; MCI, arts. 10 e 22.	Distinguir origem e destino e sua relação com o IP.
Conteúdo privado armazenado no provedor	Ordem judicial com objeto próprio; MCI, arts. 7°, III, e 10, § 2°.	Delimitar conta, conteúdo, período e necessidade.
Fluxo de comunicações	Ordem judicial e requisitos da Lei n° 9.296/1996.	Não confundir captação futura e acesso ao passado.

A preservação cautelar dos registros segue os arts. 13 e 15 do Marco Civil e não equivale ao fornecimento. O controle dos sessenta dias do art. 13, § 3º, deve ser vinculado ao requerimento, com registro da providência judicial.

O termo “metadados” não afasta a análise da natureza do campo. Se a informação permite conhecer relações ou atividades protegidas, seu regime deve ser examinado concretamente, sem tratá-la como cadastro por exclusão do conteúdo.

Fonte: síntese dos capítulos 3, 6 e 7 e dos dispositivos indicados.

A.3 Outras fontes e vias de obtenção

Objeto	Via e base de referência	Cautela essencial
Material apresentado por interlocutor	Recebimento documentado e exame da origem; CPP, art. 6°; método do livro de referência.	A apresentação não autoriza pesquisa irrestrita do aparelho.
Dados armazenados no exterior	Aplicação do MCI e cooperação quando cabível; art. 11; Convenção de Budapeste.	Confirmar detentor, via, autoridade e requisitos.
Conservação internacional	Instrumento e canal competentes; Convenção, arts. 29 e 35.	Controlar o prazo próprio e preparar a obtenção formal.

Para conteúdo apresentado por pessoa com acesso legítimo, documente a origem e o alcance da entrega. Para exame adicional de aparelho ou conta, identifique fundamento e autorização pertinentes antes da intervenção.

Na cooperação, confira o instrumento aplicável e a autoridade central designada. A classificação de “urgente” deve ser acompanhada de fatos e da medida necessária. Uma política privada de atendimento não substitui os requisitos jurídicos.

A cadeia de custódia, a integridade e a proteção dos dados atravessam todas as categorias. Uma fonte obtida pela via correta ainda exige conferência de identidade, objeto, completude e significado técnico antes da apresentação.

Fonte: síntese dos capítulos 7 e 8, CPP, Marco Civil, Convenção de Budapeste e Jorge (2027).

APÊNDICE B

Checklist de medidas investigativas

Marque apenas o que foi conferido e registre o suporte. Uma marcação não substitui motivação nem decisão da autoridade competente.

B.1 Antes do encaminhamento

- ☐ O fato e seus elementos de suporte estão identificados.
- ☐ A pergunta investigativa e a alternativa plausível estão claras.
- ☐ O dado foi classificado como cadastro, registro ou conteúdo.
- ☐ O detentor e o destinatário da medida foram verificados.
- ☐ Competência, base legal e via de obtenção estão indicadas.
- ☐ Conta, campos, evento e período foram delimitados.
- ☐ Horário original, fuso e conversão foram conferidos.
- ☐ A necessidade e os efeitos sobre terceiros foram avaliados.

B.2 Na execução e na análise

- ☐ Preservação e acesso possuem controles próprios de prazo.
- ☐ A resposta corresponde à conta, ao período e ao objeto.
- ☐ Há definição de IP, portas, protocolo e evento pertinentes.
- ☐ Originais, recebimento e transformações estão documentados.
- ☐ Alternativas e limites da atribuição foram considerados.
- ☐ O produto final relaciona afirmações às fontes e pendências.

Registro do revisor, data e suporte da conferência

Pendências e responsável

APÊNDICE C

Roteiro de planejamento investigativo

Modelo para adaptação ao procedimento institucional. Não substitui a representação judicial, a requisição fundamentada ou o registro de cadeia de custódia.

Procedimento, responsável e data

Fato e referências dos elementos disponíveis

Pergunta e hipótese principal

Alternativa plausível e elemento que poderia apoiá-la

Diligência capaz de distinguir as explicações

Dado, detentor, conta e período necessários

Base, competência, autorização e controle de prazo

Risco de perda e providência de preservação

C.2 Registro da resposta e dos limites

Conserve o arquivo original e a referência do pedido. Esclareça campos ambíguos antes da correlação. Não registre senhas ou códigos de autenticação neste instrumento.

Pedido, remetente, resposta e data de recebimento

Evento descrito e identificação da fonte

Campo	Valor original e referência
IP e função no registro	
Porta de origem e protocolo	
Data, hora, fração e fuso	
Conversão e regra utilizada	

Significado confirmado dos campos e esclarecimentos

Correspondência técnica e limites de atribuição pessoal

Próxima diligência, responsável e controle

A indisponibilidade de um campo deve ser registrada. A conclusão deve conservar a distinção entre dado recebido, interpretação e hipótese.

Referências

ARKKO, J.; COTTON, M.; VEGODA, L. **IPv4 address blocks reserved for documentation**. [S. l.]: RFC Editor, jan. 2010. RFC 5737. DOI: 10.17487/RFC5737. Disponível em: <https://www.rfc-editor.org/info/rfc5737/>. Acesso em: 31 jul. 2026.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília, DF: Câmara dos Deputados, 1988. Texto atualizado. Disponível em: <https://www2.camara.leg.br/legin/fed/consti/1988/constituicao-1988-5-outubro-1988-322142-normaatualizada-pl.html>. Acesso em: 5 out. 2026.

BRASIL. **Decreto nº 8.771, de 11 de maio de 2016**. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Brasília, DF: Câmara dos Deputados, 2016. Texto atualizado. Disponível em: <https://www2.camara.leg.br/legin/fed/decret/2016/decreto-8771-11-maio-2016-783094-normaatualizada-pe.pdf>. Acesso em: 26 out. 2026.

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: Câmara dos Deputados, 2023. Inclui o anexo da Convenção. Disponível em: <https://www2.camara.leg.br/legin/fed/decret/2023/decreto-11491-12-abril-2023-794051-publicacaooriginal-167576-pe.html>. Acesso em: 2 jun. 2026.

BRASIL. **Decreto nº 12.975, de 20 de maio de 2026**. Altera o Decreto nº 8.771, de 11 de maio de 2016, que regulamenta a Lei nº 12.965, de 23 de abril de 2014. Brasília, DF: Câmara dos Deputados, 2026. Disponível em: <https://www2.camara.leg.br/legin/fed/decret/2026/decreto-12975-20-maio-2026-799136-publicacaooriginal-179396-pe.html>. Acesso em: 7 ago. 2026.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Brasília, DF: Câmara dos Deputados, 1940. Texto atualizado. Disponível em: <https://www2.camara.leg.br/legin/fed/declei/1940-1949/decreto-lei-2848-7-dezembro-1940-412868-normaatualizada-pe.pdf>. Acesso em: 3 out. 2026.

BRASIL. **Decreto-Lei nº 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Brasília, DF: Câmara dos Deputados, 1941. Texto atualizado. Disponível em: <https://www2.camara.leg.br/legin/fed/declei/1940-1949/decreto-lei-3689-3-outubro-1941-322206-normaatualizada-pe.html>. Acesso em: 25 ago. 2026.

BRASIL. **Lei nº 9.296, de 24 de julho de 1996**. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Brasília, DF: Câmara dos Deputados, 1996. Texto atualizado. Disponível em: <https://www2.camara.leg.br/legin/fed/lei/1996/lei-9296-24-julho-1996-349049-normaatualizada-pl.pdf>. Acesso em: 8 jun. 2026.

BRASIL. **Lei nº 12.830, de 20 de junho de 2013**. Dispõe sobre a investigação criminal conduzida pelo delegado de polícia. Brasília, DF: Câmara dos Deputados, 2013. Disponível em: <https://www2.camara.leg.br/legin/fed/lei/2013/lei-12830-20-junho-2013-776286-publicacaooriginal-140173-pl.html>. Acesso em: 12 jul. 2026.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Câmara dos Deputados, 2014. Texto atualizado. Disponível em: <https://www2.camara.leg.br/legin/fed/lei/2014/lei-12965-23-abril-2014-778630-normaatualizada-pl.html>. Acesso em: 14 ago. 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Câmara dos Deputados, 2018. Texto atualizado. Disponível em: <https://www2.camara.leg.br/legin/fed/lei/2018/lei-13709-14-agosto-2018-787077-normaatualizada-pl.html>. Acesso em: 11 jun. 2026.

BRASIL. Ministério da Justiça e Segurança Pública. **Cooperação jurídica internacional em matéria penal**. Brasília, DF: MJSP, 2026. Publicada em 1 jan. 2016; atualizada em 26 ago. 2026. Disponível em: <https://www.gov.br/mj/pt-br/assuntos/sua-protecao/cooperacao-internacional/cooperacao-juridica-internacional-em-materia-penal>. Acesso em: 15 set. 2026.

DURAND, A. et al. **Logging recommendations for Internet-facing servers**. [S. l.]: RFC Editor, jun. 2011. RFC 6302. DOI: 10.17487/RFC6302. Disponível em: <https://www.rfc-editor.org/info/rfc6302/>. Acesso em: 26 ago. 2026.

HINDEN, R.; DEERING, S. **IP version 6 addressing architecture**. [S. l.]: RFC Editor, fev. 2006. RFC 4291. DOI: 10.17487/RFC4291. Disponível em: <https://www.rfc-editor.org/info/rfc4291/>. Acesso em: 12 set. 2026.

JORGE, Higor Vinicius Nogueira. **Investigação criminal tecnológica: fundamentos, método e limites na era dos vestígios informacionais**. 1. ed. Salvador: Juspodivm, 2027. ISBN 9788544277386.

KLYNE, G.; NEWMAN, C. **Date and time on the Internet: timestamps**. [S. l.]: RFC Editor, jul. 2002. RFC 3339. DOI: 10.17487/RFC3339. Disponível em: <https://www.rfc-editor.org/info/rfc3339/>. Acesso em: 24 out. 2026.

MOCKAPETRIS, P. **Domain names: concepts and facilities**. [S. l.]: RFC Editor, nov. 1987. RFC 1034. DOI: 10.17487/RFC1034. Disponível em: <https://www.rfc-editor.org/info/rfc1034/>. Acesso em: 29 set. 2026.

PERREAULT, S. et al. **Common requirements for carrier-grade NATs (CGNs)**. [S. l.]: RFC Editor, abr. 2013. RFC 6888. DOI: 10.17487/RFC6888. Disponível em: <https://www.rfc-editor.org/info/rfc6888/>. Acesso em: 19 jun. 2026.

Minicurrículo do autor

HIGOR VINICIUS NOGUEIRA JORGE

Delegado de Polícia da Polícia Civil do Estado de São Paulo, professor, escritor e pesquisador nas áreas de Direito, tecnologia, investigação criminal e inteligência cibernética. Autor e coordenador de mais de 80 obras jurídicas publicadas, integra o Conselho de Direito Digital, Transformação e Novas Tecnologias da Editora Juspodivm.

Mestre em Educação pela Universidade Estadual de Mato Grosso do Sul (UEMS) e graduado em Direito pelo Centro Universitário Toledo de Araçatuba (UniToledo/SP), é professor concursado da Academia de Polícia Dr. Coriolano Nogueira Cobra (Acadepol/SP). Possui pós-graduações em Polícia Comunitária (Unisul), Repressão e Prevenção à Corrupção (Faculdade Estácio), VANTs e Drones: Legislação, Planejamento e Aplicações (Uniminas), Cybercrime e Cybersecurity: Prevenção e Investigação de Crimes Digitais (Uniminas) e Investigação Digital (WB Educação).

Sua atuação acadêmica compreende o ensino, a pesquisa e a produção de conhecimento nas áreas de investigação criminal tecnológica, direito digital, crimes cibernéticos, inteligência cibernética, prova digital e aplicação de novas tecnologias à segurança pública. Além de sua atividade docente na Acadepol/SP, ministra aulas de inteligência cibernética no âmbito do Ministério da Justiça e Segurança Pública (MJSP). Também atuou em cursos de pós-graduação e programas de formação especializada de instituições como a Escola Brasileira de Direito (EBRADI), o Complexo de Ensino Renato Saraiva (CERS), a Escola Superior de Advocacia da OAB-SP (ESA-OAB/SP), a Escola da Magistratura do Estado do Rio de Janeiro (EMERJ), a Escola Mineira de Direito (EMD), o Damásio Educacional, a Verbo Jurídico, o MeuCurso, a WB Educação e a Associação dos Diplomados da Escola Superior de Guerra (ADESG, Campinas).

Em 2015, desenvolveu a disciplina Investigação Criminal Tecnológica, concebida como uma proposta teórico-metodológica voltada à aplicação sistemática, juridicamente fundamentada e tecnicamente controlada de recursos tecnológicos à investigação criminal. Diferentemente da investigação

de crimes cibernéticos, cujo objeto está relacionado às infrações penais praticadas no ambiente digital ou mediante o emprego de tecnologias, a Investigação Criminal Tecnológica possui abrangência transversal, aplicando-se à apuração de delitos de qualquer natureza. Sua abordagem compreende a identificação, a preservação, a obtenção, o tratamento, a correlação, a interpretação e a apresentação de vestígios informacionais relevantes à persecução penal, com observância das garantias fundamentais, dos requisitos de validade probatória e da cadeia de custódia.

Integra a Associação Internacional de Informática Forense (ASIIF) e a Associação Internacional de Investigação de Crimes de Alta Tecnologia (HTCIA). É titular da Cadeira nº 30 da Academia de Ciências, Artes e Letras dos Delegados de Polícia do Estado de São Paulo e Diretor de Relações Institucionais da Associação dos Delegados de Polícia do Estado de São Paulo (ADPESP), na gestão 2024-2026.

Entre 2017 e 2026, recebeu, em dez edições consecutivas, reconhecimento na categoria Jurídica do levantamento Melhores Delegados de Polícia do Brasil, promovido pelo Portal Nacional dos Delegados e pela Revista da Defesa Social.

Para aprofundar o estudo

Investigação criminal tecnológica

Fundamentos, método e limites na era dos vestígios informacionais

Higor Vinicius Nogueira Jorge. Salvador: Editora Juspodivm, 1ª edição, ano editorial 2027. ISBN 9788544277386.

O livro apresenta a Investigação Criminal Tecnológica como disciplina de abrangência transversal, aplicável à apuração de crimes de qualquer natureza. Desenvolve o vestígio informacional juridicamente relevante como objeto de estudo, o método em sete fases (identificação, preservação, obtenção, tratamento, correlação, interpretação e apresentação) e o Controle de Viés Investigativo, além de examinar prova digital, fontes abertas, inteligência artificial, inteligência criminal, drones, fraudes, dados em nuvem, cooperação jurídica internacional e governança.

Esta cartilha é um material educativo gratuito, escrito para aproximar esses fundamentos da prática. O livro é uma publicação comercial da Editora Juspodivm, indicada a quem deseja aprofundar o estudo.

Conheça o livro no site da editora: editorajuspodivm.com.br

A coleção

A Coleção Investigação e Proteção na Era Digital reúne oito cartilhas gratuitas sobre investigação criminal, prova digital, uso responsável da tecnologia e proteção de pessoas e famílias no ambiente digital. Todos os volumes estão disponíveis em www.higorjorge.com.br, em formato PDF.

- Vol. 01** **Investigação Criminal Tecnológica.** Fundamentos, métodos e aplicações práticas
- Vol. 02** **Provas digitais e cadeia de custódia.** Da coleta à valoração jurídica
- Vol. 03** **Inteligência artificial na investigação criminal.** Aplicações, limites e boas práticas
- Vol. 04** **Golpes digitais e fraudes eletrônicas.** Prevenção, identificação e investigação
- Vol. 05** **Investigação de crimes na internet.** Dados, registros, sigilos e medidas judiciais (este volume)
- Vol. 06** **Raciocínio investigativo e decisão fundamentada.** Do indício ao relatório final
- Vol. 07** **Internet segura.** Guia prático para proteger você e sua família
- Vol. 08** **Crianças e adolescentes na internet.** Guia de proteção para pais e responsáveis

Canais oficiais do autor

- Site** www.higorjorge.com.br
- YouTube** youtube.com/@direitoetecnologia
- Instagram** [@higorjorge](https://www.instagram.com/higorjorge)
- Facebook** facebook.com/professorhigorjorge