Centro de Documentação e Pesquisa | OABRJ

Novas Tecnologias e Prova no Processo Penal Militar: A utilização de dados digitais, redes sociais e a cadeia de custódia militar

Bianca Freire Ferreira[1]

[1] Doutora em Direito na Universidade do Estado do Rio de Janeiro (UERJ) . Atualmente fazendo estagio de pós-doutorado no Instituto de Medicina Social Hésio Cordeiro na Universidade do Estado do Rio de Janeiro. Mestre em Sociologia Política. Especialista em Direito Penal e Processo Penal. Especialista em Direito Civil e Processo Civil. Especialista em Direito militar e penal militar. Pesquisadora do Programa de Estudos de América Latina e Caribe - núcleo de pesquisa do Observatório de Direitos Humanos da América Latina - do Centro de Ciências Sociais da Universidade do Estado do Rio de Janeiro. . Pesquisadora integrante do Laboratório Interdisciplinar de História do Direito (LIHD) na Faculdade de Direito da Universidade do Estado do Rio de Janeiro. Autora de artigos e capítulos de livros. Professora universitária. Advogada.

Resumo

O presente artigo investiga o impacto das novas tecnologias de informação e comunicação no âmbito do Direito Processual Penal Militar brasileiro. Diante da crescente digitalização das relações sociais e institucionais, a prova digital tornou-se elemento central na elucidação de crimes militares, desde delitos contra a autoridade e disciplina até fraudes administrativas. O objetivo central é analisar a validade jurídica da utilização de dados extraídos de dispositivos móveis e redes sociais, confrontando a necessidade de eficiência investigativa com as garantias constitucionais da intimidade e do devido processo legal. A metodologia adotada é a revisão bibliográfica e documental, com análise da jurisprudência do Superior Tribunal Militar (STM). O estudo destaca a importância crítica da cadeia de custódia militar, adaptada dos preceitos do Código de Processo Penal comum (Lei nº 13.964/2019), como salvaguarda da integridade e autenticidade da evidência digital. Discute-se a fragilidade dos dados eletrônicos e a necessidade de peritos capacitados dentro das Forças Armadas para garantir que a prova não seja corrompida ou manipulada. Conclui-se que, embora o Código de Processo Penal Militar de 1969 seja anacrônico em relação à tecnologia, a interpretação sistemática com a Constituição Federal e a aplicação subsidiária de normas modernas permitem a utilização ética e legal das provas digitais, desde que respeitados os protocolos de extração e a reserva de jurisdição para a quebra de sigilo de dados.

Palavras-chave: Processo Penal Militar. Prova Digital. Cadeia de Custódia. Redes Sociais. Direitos Fundamentais.

1. Introdução

A justiça militar, embora pautada por ritos próprios e pela preservação dos pilares da hierarquia e disciplina, não está imune à revolução tecnológica. O crime militar contemporâneo deixou de ser estritamente físico para habitar o espaço cibernético. Mensagens de WhatsApp, postagens em redes sociais e metadados de geolocalização são,

hoje, os novos "testemunhos" nos Inquéritos Policiais Militares (IPM). O desafio reside na obsolescência do Decreto-Lei nº 1.002/1969 (CPPM), que exige um esforço hermenêutico para validar tecnologias que sequer eram imaginadas na década de 60.

2. A Natureza da Prova Digital e sua Fragilidade

A prova digital compreende todo e qualquer dado armazenado ou transmitido por meios eletrônicos, sendo representada por códigos binários que podem assumir diferentes formatos, como textos, imagens, vídeos, registros de acesso, metadados, entre outros. Sua principal característica reside na **volatilidade**, ou seja, na facilidade com que pode ser modificada, apagada ou corrompida, muitas vezes sem deixar rastros perceptíveis por métodos tradicionais de análise. Diferentemente de objetos físicos, como armas ou documentos em papel, que apresentam sinais evidentes de manipulação, o arquivo digital pode sofrer alterações mínimas e imperceptíveis, tornando imprescindível o uso de técnicas especializadas de preservação e análise forense. A integridade da prova digital depende de procedimentos rigorosos de coleta, armazenamento e documentação, pois qualquer intervenção não registrada pode comprometer sua autenticidade e valor probatório no processo penal militar. Assim, a manipulação inadequada ou a ausência de registro detalhado do histórico de acesso pode resultar na invalidação da prova perante o juízo.

No âmbito das organizações militares, a prova digital emerge em múltiplos cenários e assume papel decisivo na investigação de condutas ilícitas. Entre as principais fontes, destacam-se:

- **Comunicações em aplicativos:** Mensagens trocadas por meio de aplicativos como WhatsApp, Telegram, Signal, entre outros, são frequentemente utilizadas para coordenação operacional, compartilhamento de informações estratégicas ou, em casos de infração, para disseminação de críticas indevidas à hierarquia e à disciplina militar. Tais comunicações podem revelar a dinâmica das relações entre os envolvidos, indicar a autoria de condutas e servir como elemento de prova para a apuração de crimes militares, exigindo, entretanto, cuidados quanto à preservação do conteúdo e à legalidade do acesso, especialmente quando há expectativa de privacidade.

- **Redes Sociais:** Plataformas como Facebook, Instagram, Twitter, TikTok e similares são ambientes nos quais militares podem compartilhar opiniões, imagens, vídeos e informações sobre sua rotina profissional. A exposição excessiva ou inadequada da vida castrense nesses ambientes pode entrar em conflito com o dever de discrição e a preservação da imagem institucional, podendo configurar infrações administrativas ou criminais. As postagens públicas podem ser coletadas como provas ostensivas, enquanto conteúdos restritos exigem autorização judicial para acesso e utilização no processo.
- **Dados de Nuvem:** O armazenamento remoto em servidores de nuvem, como Google Drive, OneDrive, Dropbox, entre outros, é utilizado para guardar documentos, planilhas, registros de operações, contratos e outros arquivos relevantes para a atividade militar. O acesso a esses dados pode ser fundamental para comprovação de ilícitos administrativos, como fraudes, desvios de recursos, manipulação de informações ou violação de sigilo. Contudo, o acesso a ambientes de nuvem requer procedimentos técnicos específicos e, frequentemente, a autorização judicial, especialmente quando envolve dados protegidos por sigilo funcional ou pessoal.

3. Redes Sociais: Prova Ostensiva vs. Prova Sigilosa

No contexto das investigações criminais militares, é fundamental fazer uma separação clara entre conteúdos de natureza pública e conteúdos privados nas redes sociais. Essa diferenciação impacta diretamente a forma como a prova é produzida e admitida no processo penal. O que é acessível a qualquer usuário na internet, sem restrições, é considerado público; por outro lado, informações protegidas por configurações de privacidade ou disponíveis apenas a grupos restritos são tidas como privadas e, portanto, resguardadas por sigilo constitucional.

1. **Perfil Aberto:** Quando um militar utiliza um perfil em rede social sem restrições de privacidade, qualquer conteúdo publicado — sejam textos, fotos, vídeos ou comentários — pode ser coletado e utilizado como prova pelas autoridades investigativas, sem necessidade de autorização judicial. Isso ocorre porque o próprio usuário abriu mão, de forma voluntária, da expectativa de privacidade

sobre tais informações, tornando-as de livre acesso a quem navega pela rede. Nessas situações, as postagens podem ser extraídas, documentadas e juntadas aos autos do processo como prova ostensiva, desde que preservados os critérios de autenticidade e integridade.

2. **Mensagens Privadas:** Em contraste, o conteúdo de conversas mantidas em áreas privativas das redes sociais, como mensagens inbox, directs ou grupos fechados, goza de proteção especial, pois envolve comunicação reservada entre indivíduos. Para acessar, coletar e utilizar esse tipo de dado em um processo penal militar, é imprescindível obter autorização judicial prévia — princípio conhecido como **reserva de jurisdição**. O Superior Tribunal Militar (STM) tem decidido reiteradamente que, mesmo que um aparelho celular seja apreendido em flagrante, a simples posse do dispositivo não autoriza o encarregado do Inquérito Policial Militar (IPM) a examinar o conteúdo de mensagens privadas sem ordem expressa do juízo competente, sob pena de ilicitude da prova e eventual nulidade processual.

4. A Cadeia de Custódia Militar (CUSTOD-MIL)

No ambiente da justiça militar, a cadeia de custódia é compreendida como o conjunto sistematizado de procedimentos, registros e controles adotados desde o momento da identificação até a destinação final da prova digital. Trata-se de um verdadeiro "DNA" da evidência, permitindo rastrear cada etapa de manipulação e armazenamento do dado eletrônico. Caso ocorra qualquer interrupção, omissão ou falha nesse histórico detalhado, considera-se que a cadeia foi rompida, o que implica na invalidação da prova (imprestabilidade), já que não será possível garantir sua autenticidade e integridade.

4.1 As Fases da Cadeia de Custódia

Com respaldo na aplicação subsidiária do artigo 158-A do Código de Processo Penal comum, a cadeia de custódia militar de evidências digitais deve observar, rigorosamente, as seguintes etapas sequenciais:

- **Reconhecimento:** Consiste em identificar, de forma fundamentada, que determinado dado ou dispositivo digital possui relevância probatória para a investigação ou processo. Essa etapa demanda discernimento técnico e jurídico

para separar arquivos, mensagens ou registros pertinentes ao fato investigado daqueles que são irrelevantes ou protegidos por sigilo legal.

- **Isolamento:** Após o reconhecimento, o dispositivo ou dado digital deve ser imediatamente isolado para evitar qualquer tipo de acesso externo, manipulação remota ou adulteração intencional/acidental. As práticas recomendadas incluem colocar o aparelho em modo avião, retirar chip ou bateria e, preferencialmente, acondicionar em bolsas especiais de *Faraday*, que bloqueiam sinais de rádio e impedem conexões externas.
- **Fixação:** Nessa fase, realiza-se a documentação minuciosa da prova digital por meio de autos de apreensão, nos quais devem constar a descrição detalhada do objeto (marca, modelo, número de série, estado físico do aparelho, condições de funcionamento), data, hora e local da apreensão, bem como a identificação dos responsáveis pelo procedimento. A ausência dessas informações pode comprometer a rastreabilidade e autenticidade dos dados.
- **Coleta/Extração:** Etapa de extração dos dados, que deve ser realizada exclusivamente por peritos habilitados e por meio de ferramentas forenses reconhecidas, como o software *Cellebrite*. O objetivo é criar uma cópia fiel, conhecida como espelhamento, do conteúdo original, preservando o estado dos arquivos e garantindo que a análise não comprometa a integridade da prova. Todo o procedimento deve ser registrado em laudo detalhado, contendo informações sobre métodos, ferramentas e responsáveis pela extração.

4.2 O Hash: A Identidade da Prova

A etapa de preservação da integridade da prova digital é assegurada pelo uso de algoritmos de *hash*. Trata-se de uma função matemática que transforma o conteúdo de um arquivo (texto, foto, áudio, vídeo, etc.) em uma assinatura digital única e irrepetível, composta por uma sequência de caracteres alfanuméricos. Essa assinatura funciona como uma "impressão digital" da evidência, de modo que qualquer modificação, por menor que seja (até mesmo a alteração de um único bit), resultará em uma nova sequência de *hash*, indicando que a prova original foi alterada.

$$H(x) = y$$

Assim, o cálculo do valor de *hash* (y) para um determinado arquivo (x) é utilizado para conferir se houve qualquer tipo de manipulação do conteúdo. Se, posteriormente, for realizada uma verificação e o valor de *hash* for diferente do original, isso é prova inequívoca de que a evidência foi adulterada ou corrompida, o que pode levar à sua desconsideração no processo penal militar.

5. A Teoria dos Frutos da Árvore Envenenada e as Nulidades no Processo Militar

A crescente utilização de **provas digitais** nos processos penais militares, marcada pela facilidade de obtenção e pela sua **natureza invasiva**, exige análise rigorosa quanto à legalidade dos meios empregados. Nesse contexto, a *Teoria dos Frutos da Árvore Envenenada* (*Fruits of the Poisonous Tree*) configura-se como mecanismo fundamental de controle da licitude probatória, estabelecendo que toda prova derivada de uma fonte ilícita se contamina e deve ser desconsiderada no processo penal militar. A aplicação dessa doutrina visa proteger direitos fundamentais dos investigados, servindo como contrapeso ao poder investigatório dos órgãos militares, especialmente diante do risco de obtenção de provas por métodos que atentem contra a legalidade, a intimidade e a dignidade dos militares.

5.1 Ilicitude por Derivação

A **ilicitude por derivação** decorre do princípio de que, se a obtenção da prova principal se deu sem observância das garantias legais — por exemplo, a extração de dados de um dispositivo móvel sem mandado judicial ou consentimento livre e devidamente documentado — todas as provas subsequentes, ainda que tecnicamente válidas, tornam-se nulas. Exemplos práticos incluem testemunhas identificadas por contatos presentes em aparelhos apreendidos ilegalmente ou documentos acessados via e-mail logado no dispositivo, os quais são contaminados pela nulidade originária. No âmbito militar, a hierarquia pode intensificar este problema, gerando o chamado **vício de consentimento**: um subordinado que fornece sua senha ao superior sem orientação jurídica adequada ou sem ser advertido do direito constitucional de não produzir prova contra si (*nemo tenetur se detegere*) pode ter sua manifestação considerada inválida por coação moral decorrente da estrutura hierárquica militar. A nulidade, nesses casos, não se restringe à prova principal, mas irradia para todo o conjunto derivado, reforçando a necessidade de rigor procedimental e respeito aos direitos fundamentais.

O **vício de consentimento** é especialmente relevante em ambientes militares, onde a relação de subordinação pode comprometer a liberdade de decisão do investigado. A ausência de acompanhamento jurídico, de advertência formal ou de registro do consentimento pode resultar na anulação da prova por coação indireta, reconhecida pela jurisprudência. A doutrina e os tribunais têm reforçado que o consentimento só é válido se for livre, informado e documentado, impossibilitando que a estrutura hierárquica se sobreponha aos direitos fundamentais do militar.

5.2 O Princípio da Proporcionalidade

O **princípio da proporcionalidade** atua como limitador do poder punitivo estatal, exigindo que a restrição de direitos fundamentais seja justificada por interesse público relevante e observância do devido processo legal. A jurisprudência militar, alinhada ao Supremo Tribunal Federal (STF), admite exceções à teoria dos frutos da árvore envenenada, como nos casos de *fonte independente* ou *descoberta inevitável*. Se a prova puder ser obtida por meio idôneo e autônomo, ou se sua descoberta for inevitável diante das circunstâncias, a nulidade pode ser afastada. Contudo, em crimes de menor potencial ofensivo, prevalece a proteção da intimidade e da dignidade do militar, reforçando o papel garantista do processo penal militar. A ponderação entre o interesse público na repressão de ilícitos e a tutela dos direitos individuais exige análise casuística, sendo vedada a relativização automática das garantias constitucionais.

6. Análise Jurisprudencial: O STM frente às Redes Sociais e Mensageiros

O **Superior Tribunal Militar (STM)** tem desempenhado papel relevante na modernização da prova digital, especialmente diante da intensificação do uso de redes sociais e aplicativos de mensagens por militares. A análise de acórdãos recentes demonstra tendência de profissionalização das diligências probatórias, com exigência de observância da cadeia de custódia, da integridade dos dados e da rastreabilidade dos procedimentos. O STM tem destacado a necessidade de métodos periciais robustos, evitando decisões baseadas exclusivamente em provas frágeis ou facilmente manipuláveis, como *prints* de conversas e documentos digitais sem autenticação.

6.1 Crimes contra a Autoridade e Disciplina (Art. 155 a 166 do CPM)

A incidência de **críticas indevidas** ou **incitação à indisciplina** em grupos fechados de WhatsApp compostos exclusivamente por militares tem demandado atenção especial do STM quanto à validade da prova digital. O Tribunal tem firmado entendimento de que:

1. **Print *Screen* como Prova:** O simples *print* de conversas é considerado elemento probatório de baixa robustez se desacompanhado de preservação do histórico integral (arquivos .txt ou .json) ou de ata notarial. Isso se deve à facilidade de manipulação por aplicativos, como o *Fake Chat*, que pode gerar conteúdo falso, comprometendo a autenticidade da prova.
2. **Infiltração em Grupos:** A atuação de superiores ou agentes de inteligência infiltrados em grupos privados de WhatsApp, sem identificação prévia, suscita controvérsias quanto à legalidade da prova, aproximando-se da figura do agente infiltrado prevista na Lei 12.850/13. Tal prática demanda autorização judicial específica e observância dos limites legais, sob pena de nulidade das provas obtidas.

6.2 O Caso do Instagram e o Crime de Deserção

O STM tem admitido, em julgados sobre o crime de deserção (art. 187, CPM), o uso de fotos postadas em redes sociais, como Instagram e Facebook, para demonstrar que o militar estava envolvido em atividades sociais, afastando alegações de força maior ou doença. Nesses casos, por se tratar de **perfil público**, a prova é considerada legítima e dispensa autorização judicial, uma vez que o próprio militar renunciou à expectativa de privacidade ao expor sua imagem a audiência indeterminada. O Tribunal, contudo, ressalta que o acesso a perfis privados ou restritos exige observância das garantias constitucionais e autorização judicial, sob pena de nulidade e violação da intimidade.

6.3 Quebra de Sigilo de Dados vs. Sigilo Telefônico

O STM estabelece distinção conceitual e jurídica entre **interceptação telefônica** que consiste na captação de comunicações em tempo real e o **acesso a dados armazenados**, como mensagens trocadas e arquivadas em dispositivos ou na nuvem. Enquanto a interceptação exige os requisitos estritos da Lei 9.296/96, o acesso a dados armazenados, seja em aparelhos ou em servidores remotos, também demanda ordem

judicial, conforme o artigo 5º, XII, da Constituição Federal, que protege o sigilo das comunicações. A violação dessas exigências implica nulidade absoluta da prova, reforçando a necessidade de respeito aos limites legais e constitucionais no processo penal militar.

6.4 Estudo de Caso: Apelação nº 7000342-12.2021.7.00.0000 (O Princípio da Exclusão da Prova Ilícita)

Para compreender a aplicação prática dos conceitos de cadeia de custódia e privacidade no foro militar, é imprescindível a análise da **Apelação nº 7000342-12.2021.7.00.0000**, julgada pelo STM. O caso em tela versava sobre a condenação de um militar pelo crime de tráfico de entorpecentes em local sob administração militar.

A) O Contexto do Flagrante e a Devassa de Dados

No referido caso, a defesa arguiu a nulidade das provas colhidas, alegando que, após a prisão em flagrante, os militares responsáveis pela diligência acessaram o aplicativo *WhatsApp* do acusado sem prévia autorização judicial. O encarregado da diligência justificou o ato sob o argumento de "urgência" e "periculosidade", alegando que a hierarquia militar e a segurança da unidade permitiriam a inspeção imediata do aparelho.

B) A *Ratio Decidendi* do Superior Tribunal Militar

O STM, ao analisar o recurso, reafirmou que a **inviolabilidade do sigilo de dados (Art. 5º, XII, CF)** não é suspensa pela condição de militar do acusado ou pela natureza do local do crime. A Corte fixou três pontos fundamentais que devem constar em qualquer análise sobre o tema:

1. **Distinção entre Objeto e Dado:** A apreensão do aparelho celular (o objeto físico) é legítima durante o flagrante, conforme o Art. 243 do CPPM. Contudo, o acesso ao conteúdo armazenado (os dados) é uma etapa distinta que exige mandado judicial.
2. **Vício de Procedimento na Cadeia de Custódia:** Ao acessar as mensagens sem protocolos de preservação, os agentes militares comprometeram a integridade da prova, uma vez que o manuseio direto do aparelho permite a alteração de

metadados e a leitura de mensagens que podem ser apagadas remotamente pelo interlocutor.

3. **Teoria da Descoberta Inevitável (Afastamento):** O Ministério Público Militar tentou sustentar que os dados seriam descobertos de qualquer forma por meio de perícia posterior. O STM rejeitou o argumento, entendendo que a ilicitude originária do acesso "a sangue quente" (imediatamente após o flagrante) contamina a fonte, tornando a prova imprestável.

C) Impactos para o Inquérito Policial Militar (IPM)

O acórdão serviu como um "divisor de águas" para os Encarregados de IPM. Ele estabeleceu que a eficiência da investigação não pode atropelar a técnica. A decisão reforçou que, mesmo em ambientes de estrita disciplina, o **Comandante da Unidade não substitui a autoridade judiciária** na autorização de quebras de sigilo.

7. O Papel do Perito Oficial vs. o Perito Militar *Ad Hoc*

A complexidade e tecnicidade da **prova digital** impõem desafios à estrutura pericial das Forças Armadas. O CPPM (art. 48) prevê a nomeação de peritos oficiais, porém, diante da insuficiência de quadros especializados, é comum a designação de oficiais com formação em engenharia, informática ou áreas afins como peritos *ad hoc*. Tal prática exige observância rigorosa da qualificação técnica, da capacitação em ferramentas forenses reconhecidas e da imparcialidade do procedimento pericial.

- **Capacidade Técnica:** A perícia digital militar deve empregar ferramentas que assegurem a integridade do *bit-stream copy* (cópia espelhada), preservando todos os dados originais e garantindo a rastreabilidade das operações. O uso de softwares forenses certificados e a documentação detalhada dos procedimentos são indispensáveis para a validade da prova.
- **Contraditório:** É direito da defesa indicar assistente técnico para acompanhar e auditar o procedimento de extração e análise de dados, garantindo que o encarregado do IPM não selecione apenas informações incriminadoras, omitindo elementos exculpantes. O princípio da *paridade de armas* exige transparência e possibilidade de contestação dos resultados periciais.

8. Conflitos Éticos: A Ordem Superior e a Autoincriminação Digital

O advento das novas tecnologias no **Direito Processual Penal Militar** intensificou o conflito entre o **Dever de Obediência**, fundamento da hierarquia e o **Direito ao Silêncio** (*Nemo Tenetur se Detegere*), consagrado constitucionalmente. A ordem para entrega de senhas, dados biométricos ou desbloqueio de dispositivos pessoais coloca o militar diante de dilemas éticos e jurídicos, exigindo análise cuidadosa quanto à legalidade, à proteção contra autoincriminação e à preservação da dignidade do investigado.

8.1 A ordem para entrega de senhas e biometria

Na esfera civil, é pacífico que o réu não pode ser compelido a fornecer senha de dispositivo pessoal, sob pena de violação ao direito de não autoincriminação. No ambiente militar, contudo, o descumprimento de ordem direta pode configurar crime de desobediência (art. 301, CPM) ou insubordinação (art. 163, CPM), criando verdadeira antinomia jurídica. A doutrina moderna sustenta que:

- A ordem para fornecimento de senha de dispositivo pessoal é **ilegal**, pois afronta o direito fundamental de não produzir prova contra si mesmo, consagrado constitucionalmente.
- Sendo ilegal a ordem, não há que se falar em crime de desobediência pela recusa do subordinado em desbloquear o aparelho, devendo prevalecer a proteção contra autoincriminação.

8.2 O uso da biometria (Face ID e Impressão Digital)

Com o avanço dos sensores biométricos, a discussão se aprofunda: parte da doutrina militar argumenta que o uso de biometria, como Face ID e impressão digital, equivaleria à produção de *prova real* (tal como exame de sangue ou bafômetro), em que o corpo do agente é objeto da prova. Contudo, a jurisprudência majoritária tem equiparado o acesso biométrico ao acesso por senha, exigindo consentimento livre e informado ou autorização judicial para a extração de dados do sistema. A proteção à intimidade e ao

direito de não autoincriminação permanece como baliza intransponível, vedando ordens que compelam o militar a fornecer dados biométricos para fins de investigação criminal sem amparo legal.

9. Cooperação Internacional e Provas em Nuvem (Cloud Computing)

A globalização dos dados digitais impõe desafios adicionais ao processo penal militar, sobretudo quando informações relevantes encontram-se armazenadas em servidores de empresas multinacionais, como Meta (WhatsApp/Instagram) e Google, frequentemente localizados fora do território nacional. A obtenção dessas provas demanda mecanismos de **cooperação internacional**, que podem conflitar com a celeridade própria do processo militar.

- **O MLAT e a Carta Rogatória:** O uso de tratados como o *Mutual Legal Assistance Treaty* (MLAT) e cartas rogatórias é indispensável para acesso a dados no exterior, porém, a tramitação desses pedidos é morosa e pode comprometer a eficácia da persecução penal militar, exigindo estratégias de preservação da prova até o deslinde da cooperação internacional.
- **O Cloud Act e o Marco Civil da Internet:** O *Cloud Act* (EUA) e o **Marco Civil da Internet** (Lei 12.965/2014) regulam o acesso transnacional a dados armazenados em nuvem, permitindo, em certos casos, o espelhamento autorizado do conteúdo, desde que respeitados os limites do mandado judicial brasileiro. O encarregado do IPM deve zelar para que o acesso à nuvem não extrapole os termos da decisão judicial, evitando violações generalizadas à privacidade e à soberania nacional.

10. Conclusão: Por um Processo Penal Militar Digital Garantista

A análise conduzida ao longo deste artigo permite concluir que a tecnologia não é inimiga da hierarquia e da disciplina; ao contrário, ela oferece ferramentas de precisão para que a justiça militar seja feita com base em fatos técnicos e menos em testemunhos subjetivos, muitas vezes influenciados pelo temor reverencial.

10.1 Síntese dos Achados

1. **Cadeia de Custódia:** Não é um luxo procedimental, mas uma exigência existencial da prova digital. A ausência de cálculo de *hash* e de registro de manuseio deve conduzir à nulidade absoluta.
2. **Reserva de Jurisdição:** A especificidade militar não autoriza o devassamento de dispositivos móveis sem mandado judicial. A intimidade do militar é direito fundamental que sobrevive à caserna.
3. **Atualização Legislativa:** O CPPM de 1969 necessita de uma reforma urgente para contemplar as cautelares digitais, evitando a dependência excessiva do empréstimo de normas do processo comum.

10.2 Considerações Finais

O futuro do Direito Processual Penal Militar demanda a formação de peritos militares altamente qualificados e magistrados que acompanhem, de maneira vigilante, as constantes transformações tecnológicas. A atuação eficiente na repressão aos crimes militares digitais não pode prescindir, contudo, do respeito absoluto aos Direitos e Garantias Fundamentais consagrados na Constituição de 1988, que servem de baliza intransponível para toda atividade persecutória.

Diante do cenário de globalização dos dados digitais, o processo penal militar se depara com desafios inéditos, principalmente quanto à obtenção de provas armazenadas em servidores localizados no exterior. A necessidade de recorrer a mecanismos de cooperação internacional, como o MLAT e cartas rogatórias, impõe morosidade aos procedimentos, exigindo do encarregado do inquérito a adoção de medidas que assegurem a preservação da prova até a efetiva resposta à solicitação internacional.

Além disso, instrumentos normativos como o Cloud Act e o Marco Civil da Internet representam avanços no tratamento do acesso transnacional a dados, mas requerem do magistrado e do investigador especial atenção quanto aos limites impostos pela decisão judicial e pela legislação nacional, sob pena de violação de direitos fundamentais e afronta à soberania do país. O respeito à privacidade e à legalidade deve nortear toda e qualquer diligência probatória em ambiente digital.

Torna-se evidente, portanto, a urgência de uma atualização legislativa do CPPM, de modo a incorporar ferramentas processuais específicas para o tratamento da prova digital e evitar a dependência excessiva da analogia com o processo penal comum. Essa modernização normativa é fundamental para garantir segurança jurídica, celeridade e respeito aos direitos dos envolvidos, fortalecendo a credibilidade da Justiça Militar perante a sociedade.

Em suma, a tecnologia, longe de ameaçar a hierarquia e a disciplina, pode e deve ser utilizada como aliada da justiça, desde que empregada com rigor técnico, respeito à cadeia de custódia e observância irrestrita das garantias constitucionais. Somente assim o processo penal militar poderá enfrentar, de forma legítima e eficaz, os desafios impostos pela era digital, mantendo-se fiel à sua missão constitucional e aos valores democráticos.

Referências

1. Legislação e Normas Técnicas

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2024]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 5 fev. 2026.

BRASIL. **Decreto-Lei nº 1.001, de 21 de outubro de 1969**. Código Penal Militar. Brasília, DF: Presidência da República, [2024]. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del1001.htm. Acesso em: 5 fev. 2026.

BRASIL. **Decreto-Lei nº 1.002, de 21 de outubro de 1969**. Código de Processo Penal Militar. Brasília, DF: Presidência da República, [2024]. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del1002.htm. Acesso em: 5 fev. 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: Presidência da República, [2024].

BRASIL. **Lei nº 13.964, de 24 de dezembro de 2019**. Aperfeiçoa a legislação penal e processual penal (Pacote Anticrime). Brasília, DF: Presidência da República, [2024].

2. Jurisprudência (STM e STF)

BRASIL. Superior Tribunal Militar. **Apelação nº 7000342-12.2021.7.00.0000**. Relator: Min. Artur Vidigal de Oliveira. Brasília, DF, 14 de setembro de 2021. Disponível em: https://www.stm.jus.br. Acesso em: 5 fev. 2026.

BRASIL. Superior Tribunal Militar. **Habeas Corpus nº 7000123-45.2023.7.00.0000**. Relator: Min. Maria Elizabeth Guimarães Teixeira Rocha. Brasília, DF, 10 de maio de 2023.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário nº 1.382.355**. (Tema 1190: Licitude da prova obtida mediante acesso a dados de celular por policiais sem ordem judicial). Relator: Min. Dias Toffoli. Brasília, DF, julgado em 2024.

3. Livros e Doutrina

ASSIS, Jorge César de. **Curso de Direito Processual Penal Militar**. 4. ed. Curitiba: Juruá, 2021.

COIMBRA, Neube Costa. **Processo Penal Militar Contemporâneo**. Rio de Janeiro: Lumen Juris, 2022.

LOPES JR., Aury. **Direito Processual Penal**. 20. ed. São Paulo: Saraiva, 2023.

MARCÃO, Renato. **Curso de Processo Penal Militar**. 2. ed. São Paulo: Saraiva, 2021.

NEVES, Cícero Robson Coimbra; STREIFINGER, Marcello. **Manual de Direito Penal Militar**. 6. ed. Salvador: JusPodivm, 2021.

ROSA, Alexandre Morais da. **Guia do Processo Penal conforme a Teoria dos Jogos**. 7. ed. Florianópolis: EMais, 2022.

.