RADAR INVESTIGATIVO

Ministério Público Militar

Edição nº 01 | Ano 2026

DOSSIÊ DA CAPA

O exército de TI da Ucrânia e a participação direta de civis nas hostilidades



SPAI

EXPEDIENTE

REVISTA DIGITAL RADAR INVESTIGATIVO

Publicação oficial da Secretaria de Pesquisa e Apoio à Investigação do Ministério Público Militar.

Clauro Roberto de Bortolli
Procurador-Geral de Justiça Militar

Maria de Lourdes Souza Gouveia
Vice-Procuradora-Geral de Justiça Militar

Alexandre José de Barros Leal Saraiva
Secretário-Geral de Pesquisa e Apoio à Investigação

Francisco Tarcísio Damasceno Filho
Chefe Divisão de Difusão do Conhecimento da SPAI

Antonio Carlos Alves Coutinho
Diretor-Geral

Hebert Vilson França
Secretário de Comunicação Institucional

Flávia de Paula de Oliveira
Coordenadoria de Capacitação e Desenvolvimento

Ministério Público Militar
Procuradoria-Geral de Justiça Militar
Setor de Embaixadas Norte
Quadra 801, lote 43, Asa Norte
70800-921 - Brasília/DF
www.mpm.mp.br
pgjm.spai@mpm.mp.br

Periodicidade: Semestral
Formato: Digital
Ano: 2026

Os artigos, entrevistas, estudos e demais conteúdos publicados são de responsabilidade exclusiva de seus autores e não refletem necessariamente o posicionamento institucional do Ministério Público Militar. É permitida a reprodução total ou parcial dos conteúdos, desde que citada a fonte.

SUMÁRIO

04 CARTA AO LEITOR

05 VOZES DA INVESTIGAÇÃO
ENTREVISTA - CLAURO ROBERTO DE BORTOLLI

13 DOSSIÊ DA CAPA
O EXÉRCITO DE TI DA UCRÂNIA E A PARTICIPAÇÃO DIRETA DE CIVIS NAS HOSTILIDADES
ALEXANDRE PERES TEIXEIRA

31 ARTIGO
TECNOLOGIA INVESTIGATIVA: DO EXTRATO BANCÁRIO ÀS RELAÇÕES QUE IMPORTAM
ASSESSORIA DE DESENVOLVIMENTO TECNOLÓGICO/SPAI

37 MÉTODO EM PRÁTICA
A ARTE DE RECEBER E INTERPRETAR DADOS SIGILOSOS
ASSESSORIA DE DESENVOLVIMENTO TECNOLÓGICO/SPAI

41 CASO EM PERSPECTIVA
2ª PROCURADORIA DE JUSTIÇA MILITAR EM BRASÍLIA/DF

46 RADAR DO SEMESTRE

50 FRONTEIRA DA INVESTIGAÇÃO

54 MEMÓRIA
ÂNGELA MONTENEGRO TAVEIRA

CARTA AO LEITOR

Ao encerrarmos mais um semestre de atividades, apresentamos aos leitores a primeira edição da Revista Digital Radar Investigativo, iniciativa concebida para fortalecer a cultura da inovação, da pesquisa aplicada e do compartilhamento do conhecimento no âmbito do Ministério Público Militar (MPM). A publicação nasce com o propósito de disseminar experiências, métodos, reflexões e boas práticas relacionadas à investigação, à inteligência, à tecnologia e à produção de conhecimento estratégico para a atuação ministerial.

O período foi marcado por importantes avanços institucionais. A Secretaria-Geral de Pesquisa e Apoio à Investigação consolidou iniciativas voltadas ao desenvolvimento de capacidades investigativas, ao aperfeiçoamento de metodologias de análise de dados, ao fortalecimento da segurança da informação e à prospecção de novas tecnologias capazes de ampliar a eficiência e a efetividade das atividades finalísticas do Ministério Público Militar. Essas ações refletem o compromisso permanente com a modernização e com o apoio técnico qualificado aos membros e servidores do MPM.

Também ampliamos os espaços de capacitação, intercâmbio de conhecimentos e produção intelectual, estimulando uma atuação cada vez mais integrada entre tecnologia, inteligência, ciência de dados, cibersegurança e investigação. Em um cenário marcado pela rápida transformação digital e pelo surgimento constante de novos desafios, torna-se indispensável fomentar ambientes de aprendizagem contínua e de reflexão crítica sobre as ferramentas e os métodos que apoiam a atividade investigativa.

Esta edição inaugura um espaço de diálogo entre especialistas, pesquisadores, membros e servidores, reunindo conteúdos voltados à aplicação prática do conhecimento, à difusão de experiências relevantes e à análise de temas emergentes que impactam a atividade investigativa contemporânea. A revista pretende ser uma fonte permanente de consulta, atualização e inspiração para todos aqueles que atuam na construção de soluções inovadoras para os desafios institucionais.

Por fim, registramos nosso agradecimento a todos os colaboradores que contribuíram para a concretização deste projeto editorial e aos profissionais que, diariamente, dedicam seus esforços ao fortalecimento da investigação, da inteligência e da produção de conhecimento no MPM. Convidamos os leitores a participar desta iniciativa, compartilhando experiências, pesquisas e reflexões que possam enriquecer as próximas edições da Radar Investigativo.

Boa leitura!

ALEXANDRE JOSÉ DE BARROS LEAL SARAIVA
Procurador de Justiça Militar
Secretário-Geral de Pesquisa e Apoio à Investigação

VOZES
da Investigação

RADAR
INVESTIGATIVO
MINISTÉRIO PÚBLICO MILITAR

ENTREVISTA

Clauro Roberto de Bortolli

Procurador-Geral de Justiça Militar



Na Entrevista desta primeira edição da Revista Radar Investigativo, o procurador-geral de Justiça Militar, Clauro Roberto de Bortoli, aborda os principais desafios e perspectivas para a modernização da investigação criminal no âmbito do Ministério Público Militar. Em pauta, temas como inteligência artificial, transformação digital, segurança da informação, combate às fraudes eletrônicas, cooperação internacional e aperfeiçoamento da Polícia Judiciária Militar.

Ao longo da conversa, são apresentados projetos inovadores em desenvolvimento no MPM, iniciativas voltadas à incorporação de novas tecnologias e reflexões sobre a necessidade de atualização legislativa e fortalecimento institucional da Justiça Militar. A entrevista também destaca o papel estratégico da investigação na preservação da hierarquia e da disciplina das Forças Armadas, pilares essenciais à defesa do Estado Democrático de Direito.

Uma leitura que oferece uma visão abrangente sobre os caminhos da inovação, da investigação e da justiça militar em um cenário marcado pela rápida evolução tecnológica e pelas novas formas de criminalidade.

De que forma o MPM tem integrado uso de inteligência artificial e análise de dados para otimizar as investigações de crimes militares?

Clauro Bortolli - No início desta gestão, criamos uma secretaria específica voltada à prospecção e à inovação tecnológica: a Sprint, liderada pelo promotor de Justiça Militar Luiz Felipe Carvalho Silva.

Mesmo diante de um cenário orçamentário desafiador, temos investido continuamente em novas ferramentas de inteligência artificial e na capacitação de membros e servidores. A inteligência artificial não é mais uma perspectiva para o futuro; ela já faz parte da nossa realidade e tem contribuído para o desenvolvimento de projetos relevantes para a atuação do Ministério Público Militar.

Um exemplo é o Projeto K9, que aplica recursos de inteligência artificial à análise de casos relacionados ao artigo 290 do Código Penal Militar, especialmente aqueles envolvendo posse, uso e tráfico de entorpecentes em áreas sob administração militar. Também estamos implementando ferramentas capazes de converter áudios em texto, uma funcionalidade fundamental para conferir maior agilidade e eficiência aos procedimentos realizados no processo eletrônico.

Outro projeto de destaque é o Protege, desenvolvido por meio de parceria entre o Ministério Público Militar e a Fundação de Apoio à Pesquisa do Distrito Federal. A iniciativa é voltada ao combate às fraudes digitais e reforça a necessidade de respostas tecnológicas cada vez mais rápidas e eficazes diante dos desafios impostos pela criminalidade contemporânea.

A Secretaria de Pesquisa e Apoio à Investigação (SPAI) já vem incorporando ferramentas de inteligência artificial às suas atividades. Os resultados têm se traduzido em ganhos significativos de tempo e produtividade. É importante ressaltar, contudo, que essas soluções operam sempre sob o controle e a supervisão do agente humano.

Não se trata de transferir responsabilidades às ferramentas tecnológicas. Continuaremos investindo em inteligência artificial, na medida de nossas possibilidades orçamentárias, mas sempre com a compreensão de que a responsabilidade pelas decisões e pelos atos praticados permanece integralmente com os membros e servidores que os conduzem. Afinal, a tecnologia é um instrumento de apoio à atividade institucional, e não um substituto da análise, do discernimento e da responsabilidade humana.

Quais são os principais desafios técnicos e operacionais para a transição completa da investigação militar para o ambiente digital?

Clauro Bortolli - Acredito que o primeiro grande desafio seja a segurança da informação. Recentemente, acompanhamos ataques cibernéticos que afetaram instituições importantes, como o sistema do Superior Tribunal Militar, que permaneceu mais de uma semana indisponível, além de ocorrências registradas em estruturas do Exército Brasileiro. Nesse contexto, a proteção de dados, sistemas e ativos digitais tornou-se uma prioridade permanente.

O segundo desafio está relacionado à necessidade contínua de capacitação. A transformação tecnológica ocorre em ritmo acelerado e exige atualização constante de membros, servidores e demais profissionais que utilizam essas ferramentas no exercício de suas atividades.

Um terceiro aspecto relevante é a interoperabilidade entre os diversos sistemas. Temos avançado nessa direção, mas ainda há muito a fazer. Recentemente, no âmbito do Conselho Nacional do Ministério Público, por meio do Programa de Destreza Digital, foi alcançada a marca de mais de 200 soluções tecnológicas desenvolvidas no Ministério Público brasileiro. Embora esse número demonstre capacidade de inovação, também revela um desafio: muitas dessas soluções desempenham funções semelhantes e, em diversos casos, não se comunicam entre si. Precisamos evoluir para um ambiente em que os sistemas sejam integrados, complementares e capazes de compartilhar informações de forma segura e eficiente.

A área tecnológica evolui com enorme rapidez e demanda investimentos significativos. Por isso, não basta apenas investir; é preciso investir de maneira estratégica. Afinal, aquilo que hoje é considerado moderno pode tornar-se obsoleto em pouco tempo. Por essa razão, considero fundamentais três eixos de atuação: a interoperabilidade dos sistemas, a segurança da informação e a capacitação permanente das pessoas.

Isso envolve não apenas a atualização do parque tecnológico institucional, mas também a formação contínua de membros, servidores, militares das Forças Armadas e de todos aqueles que utilizam essas ferramentas. Em um cenário orçamentário restritivo, é indispensável realizar escolhas criteriosas para garantir que os recursos sejam aplicados da forma mais eficiente possível.

São desafios relevantes, mas dos quais não podemos nos afastar. Essa transformação não pertence ao futuro; ela já está em curso e influencia diretamente a forma como trabalhamos e prestamos nossos serviços à sociedade. Por isso, acredito que continuaremos avançando de maneira consistente nessa área, mesmo diante de um cenário complexo e desafiador.

Como o MPM avalia o impacto da cibercriminalidade e das fraudes digitais dentro das Forças Armadas?

Clauro Bortolli - Essa é a nova realidade com a qual precisamos conviver e para a qual devemos estar preparados. Vivemos um processo de inclusão digital praticamente obrigatória, em que a tecnologia passou a fazer parte de todos os aspectos da vida cotidiana.

Quando observamos as Forças Armadas, percebemos que elas refletem, em grande medida, a própria diversidade da sociedade brasileira. Temos, por exemplo, jovens que ingressam no serviço militar obrigatório em busca de sua primeira oportunidade profissional. Ao mesmo tempo, convivemos com desafios cada vez mais presentes no ambiente digital, como os crimes praticados contra mulheres por meio de plataformas e redes virtuais. Esse tema ganha ainda mais relevância diante do aumento significativo da participação feminina nas Forças Armadas, especialmente após a implantação do serviço militar inicial voluntário feminino.

Outro grupo que merece atenção especial é o dos idosos, que frequentemente figuram entre as principais vítimas de fraudes digitais. Nesse contexto, também estão inseridas as pensionistas militares, que podem ser diretamente afetadas por esse tipo de crime.

Por isso, a crescente migração da atividade criminosa para o ambiente cibernético nos impacta de forma direta. Os crimes digitais deixaram de ser uma possibilidade futura e passaram a integrar a realidade cotidiana das instituições. Fraudes eletrônicas, golpes virtuais e outras modalidades de delitos cibernéticos são ocorrências cada vez mais frequentes, exigindo das organizações capacidade permanente de prevenção, investigação e resposta.

Diante desse cenário, precisamos contar com ferramentas tecnológicas adequadas e com equipes preparadas para enfrentar essas ameaças. A investigação criminal mudou e continua mudando em ritmo acelerado. Hoje, ela exige novos conhecimentos, instrumentos especializados e maior rapidez na obtenção e análise de informações.

Esse contexto demanda um esforço contínuo de aprimoramento da capacidade investigativa, com investimentos em tecnologia, inovação e capacitação. Exige também a preparação permanente dos integrantes do Ministério Público Militar e da Polícia Judiciária Militar, para que possam atuar de forma eficiente diante dos desafios impostos pela criminalidade no ambiente digital.

Quais mudanças considera prioritárias no Código de Processo Penal Militar para modernizar a investigação criminal?

Clauro Bortolli - Na realidade, precisamos promover uma ampla atualização da legislação penal militar e da legislação processual penal militar, de modo a acompanhar a evolução ocorrida na legislação penal comum ao longo dos últimos anos.

Muitas vezes nos vemos obrigados a suprir lacunas normativas em razão de decisões proferidas pelo STF, justamente porque determinadas atualizações não foram incorporadas à legislação específica da Justiça Militar. Esse cenário evidencia a necessidade de modernização do nosso arcabouço normativo.

É fundamental que essa legislação seja atualizada, preservando, evidentemente, as peculiaridades e a autonomia da Justiça Militar da União. Não se trata de eliminar suas características próprias, mas de assegurar que ela evolua em sintonia com as transformações do sistema jurídico brasileiro.

Tivemos um avanço importante com a edição da Lei nº 13.491/2017, que trouxe o crime extravagante para a Justiça Militar. Essa mudança representou um marco significativo para a atuação da Justiça Militar. Contudo, a modernização da legislação processual penal militar não acompanhou, na mesma velocidade, essa evolução legislativa.

Por isso, é essencial que as inovações legislativas e processuais implementadas na Justiça Criminal Comum também sejam analisadas e, quando compatíveis, incorporadas à Justiça Militar.

O objetivo é assegurar que a Justiça Militar permaneça alinhada às melhores práticas processuais e aos avanços do ordenamento jurídico nacional, atuando em condições equivalentes às da Justiça Criminal Comum.

É favorável à ampliação da competência da Justiça Militar para questões cíveis e administrativas?

Clauro Bortolli - Sou, há muito tempo, amplamente favorável à ampliação da competência da Justiça Militar.

Perdemos uma oportunidade histórica com a Emenda Constitucional nº 45, que ampliou a competência das Justiças Militares estaduais, mas, infelizmente, essa ampliação não foi estendida à Justiça Militar da União.

Assim, além da competência disciplinar, que considero fundamental, especialmente para a apreciação judicial dos atos administrativos disciplinares, também entendo necessária a ampliação da competência em matérias administrativas, sem deixar de fortalecer a atuação penal da Justiça Militar da União.

Destaco a questão administrativa porque, muitas vezes, discussões que se arrastam por anos na Justiça Federal, como controvérsias sobre transferências contestadas ou resistências ao cumprimento de sanções disciplinares por parte de militares, produzem impactos muito mais significativos sobre a hierarquia e a disciplina no cotidiano da caserna do que determinados crimes militares em tramitação.

Não podemos permitir, ou pelo menos não deveríamos permitir, que questões que afetam diretamente a hierarquia, a disciplina e a funcionalidade das Forças Armadas permaneçam anos aguardando solução em uma justiça que não é especializada. Sou amplamente favorável a essa ampliação de competência. Evidentemente, ela produziria impactos institucionais, mas, acima de tudo, fortaleceria a Justiça Militar.

Mais do que isso, fortaleceria os próprios princípios da hierarquia e da disciplina, bem como a operacionalidade e a funcionalidade das Forças Armadas. Costumo dizer que o foro do militar, por sua própria natureza, deveria ser a Justiça Militar.

Compreendemos quando o Supremo Tribunal Federal adota uma interpretação mais restritiva em relação aos crimes militares praticados por civis. Nesse ponto, concordamos que a submissão do civil à jurisdição militar deve ocorrer apenas em situações específicas e devidamente justificadas.

Entretanto, em relação ao militar, a lógica deveria ser inversa. O foro militar deveria ser o foro adequado e natural, o foro por excelência para a apreciação das questões que envolvem a atividade militar. Se, por um lado, entendemos a necessidade de uma interpretação restritiva quanto à submissão do civil à Justiça Militar, por outro, deveríamos adotar uma visão mais ampla em relação ao militar, para quem o foro militar deveria ser o foro de referência por definição.

Por isso, entendo que essa mudança já tarda há muito tempo. Trata-se de uma medida necessária e urgente, que produziria ganhos não apenas para a própria Justiça Militar, mas também para as Forças Armadas como um todo.

E a aplicação do Acordo de Não Persecução Penal (ANPP) na Justiça Militar e suas limitações atuais?

Clauro Bortolli - Vejo o Acordo de Não Persecução Penal como um caminho sem volta na Justiça Militar, tanto dos estados quanto da União. Embora ainda exista alguma resistência por parte do Superior Tribunal Militar em relação ao tema, o Ministério Público Militar já vem defendendo sua aplicação há bastante tempo.

Inclusive, fui coordenador de um Colégio de Procuradores realizado em 2021, já há cinco anos, ocasião em que dois enunciados trataram especificamente do ANPP, reconhecendo a tendência de sua aplicabilidade na Justiça Militar da União.

Não vejo qualquer incompatibilidade entre a aplicação do acordo e os princípios da hierarquia e da disciplina militar. Ao contrário, entendo que ambos podem coexistir de forma plenamente harmônica. Tenho defendido, por exemplo, que, nos acordos envolvendo militares, seja prevista como cláusula a preservação do poder disciplinar do comandante.

Da mesma forma, não há razão para que o civil processado na Justiça Militar deixe de ter acesso a um benefício que lhe seria assegurado caso estivesse sendo processado na Justiça Comum.

Entendo, inclusive, que um dos fundamentos da própria existência da Justiça Militar é garantir ao jurisdicionado os mesmos direitos e garantias assegurados em outros ramos do Judiciário, sempre com a devida observância dos princípios da hierarquia e da disciplina, que constituem a base de sua existência.

Por isso, vejo a aplicação do ANPP como uma evolução natural e irreversível do sistema, um caminho que, a meu ver, não tem volta.

Quais são as prioridades estratégicas da sua gestão para consolidar o MPM como um órgão de vanguarda na investigação criminal?

Clauro Bortolli - Primeiro, é importante compreender que o Ministério Público Militar realiza investigação direta apenas em situações específicas. Sua principal atribuição, nesse contexto, é exercer o controle externo da atividade da Polícia Judiciária Militar, que é a instituição responsável pela condução das investigações.

Nesse cenário, vejo duas questões centrais que precisam ser enfrentadas. A primeira é a tecnológica. No âmbito do Ministério Público Militar, ainda enfrentamos algumas defasagens nessa área e precisamos avançar de forma consistente.

Temos exemplos bem-sucedidos, como a SPAI, Secretaria de Pesquisa e Apoio à Investigação, que efetivamente se consolidou como um caso de sucesso. Entretanto, parte das atividades desenvolvidas pela SPAI deveria fazer parte da estrutura e das capacidades próprias da Polícia Judiciária Militar.

Por isso, há outro ponto que considero importante destacar. Dentro da estrutura dos órgãos que atuam na Justiça Militar e no enfrentamento do crime militar, a investigação ainda representa um elo que precisa ser fortalecido. A capacidade investigativa da Polícia Judiciária Militar demanda aperfeiçoamento e atualização constantes.

Nesse sentido, durante a gestão do procurador-geral de Justiça Militar Jaime de Cassio Miranda, o Ministério Público Militar publicou uma obra bastante

relevante: o Manual de Polícia Judiciária Militar. Atualmente, já tenho em meu gabinete a portaria para assinatura que viabilizará o lançamento de uma nova edição atualizada desse manual.

O trabalho foi desenvolvido por membros do Ministério Público Militar, representantes indicados pelo Ministério da Defesa e integrantes das três Forças Armadas: Marinha, Exército e Aeronáutica. O objetivo é incorporar ao manual as transformações observadas na criminalidade nos últimos anos.

Hoje, lidamos com temas como cadeia de custódia da prova, prova digital, macrocriminalidade, crimes licitatórios e crimes ambientais. A criminalidade mudou, e nós precisamos nos organizar para enfrentá-la adequadamente.

Por isso, precisamos aprimorar a investigação. Vejo dois pontos estratégicos e fundamentais nesse processo: o primeiro é incorporar às investigações todas as possibilidades oferecidas pela tecnologia; o segundo é fortalecer a capacidade investigativa da Polícia Judiciária Militar. Esses são dois focos prioritários para o Ministério Público Militar.

Diante dessa realidade, criamos, durante esta gestão, a Secretaria de Cooperação Jurídica e Relações Internacionais, atualmente dirigida pelo ex-procurador-geral de Justiça Militar Antônio Pereira Duarte, justamente para fortalecer esse diálogo e essa aproximação institucional. Temos uma extensa faixa de fronteira, especialmente na região amazônica, que apresenta desafios significativos de fiscalização, enquanto o crime organizado não reconhece limites territoriais. Por isso, é fundamental mantermos uma interlocução permanente com as estruturas de persecução penal dos países vizinhos.

Além disso, a Constituição e a legislação brasileira preveem a extraterritorialidade para determinados crimes militares. Isso significa que, em algumas situações, nossa atuação ultrapassa as fronteiras nacionais. E não há como desempenhar essa missão de forma eficiente sem uma cooperação estreita e bem estruturada com os órgãos responsáveis pela persecução criminal em outros países.

Essa cooperação é especialmente importante com os países da América Latina e, em particular, com aqueles que compartilham fronteiras com o Brasil na vasta região amazônica.

Como a cooperação internacional com Ministérios Públicos de outros países tem moldado o combate a crimes transnacionais que envolvem militares?

Clauro Bortolli - A criminalidade mudou. Mudou em todas as dimensões, e a criminalidade que hoje chega à Justiça Militar também é muito diferente daquela que observávamos há alguns anos.

Qual mensagem o senhor deixa para a sociedade civil sobre a relevância de uma Justiça Militar forte e modernizada na defesa do Estado Democrático de Direito?

Clauro Bortolli - Eu costumo dizer que a Justiça Militar possui uma missão muito específica: preservar a hierarquia e a disciplina, que são os pilares constitucionais das Forças Armadas. A manutenção

desses fundamentos, sem os quais as Forças Armadas não poderiam cumprir sua missão institucional, é a razão de ser da Justiça Militar da União e a atribuição do Ministério Público Militar.

Também costumo lembrar que, muitas vezes, não percebemos que hierarquia e disciplina não são valores que interessam apenas aos militares. São conceitos que interessam a toda a sociedade. Forças Armadas sem hierarquia e sem disciplina podem se transformar em qualquer coisa armada, menos em Forças Armadas.

A Constituição e a legislação conferem às Forças Armadas o monopólio legítimo do uso da força em determinadas situações. Por isso, o enfraquecimento desses pilares teria consequências graves não apenas para a instituição militar, mas também para os direitos e garantias dos cidadãos, para a soberania nacional, para os Poderes constituídos e para a própria democracia.

Assim, quando a Justiça Militar e o Ministério Público Militar atuam na proteção da hierarquia e da disciplina, estão, na verdade, protegendo todos os demais direitos e garantias que dependem da existência de Forças Armadas disciplinadas, hierarquizadas e comprometidas com a ordem constitucional.

Como o senhor imagina o MPM e a Justiça Militar daqui a cinco, dez anos?

Eu imagino um futuro com ampliação significativa da competência da Justiça Militar e das atribuições do Ministério Público Militar, para que possamos, dentro da missão que nos foi conferida pelo constituinte, prestar um serviço cada vez melhor à sociedade brasileira.

Nesse contexto, são urgentes as reformas dos nossos textos legislativos, especialmente da Constituição, para promover a ampliação da competência da Justiça Militar e, consequentemente, das atribuições do Ministério Público Militar.

Vejo essa necessidade como imperativa. Ainda assim, sou bastante otimista em relação ao futuro. Acredito que conseguiremos ampliar a compreensão sobre o papel essencial desempenhado pela Justiça Militar e pelo Ministério Público Militar na proteção da hierarquia e da disciplina no âmbito das Forças Armadas e, como consequência, na preservação de todos os demais direitos e garantias que delas decorrem.

É nesse propósito que reside a relevância dessas instituições para a Nação e para a sociedade brasileira.

RADAR INVESTIGATIVO
MINISTÉRIO PÚBLICO MILITAR

RADAR
INVESTIGATIVO
MINISTÉRIO PÚBLICO MILITAR

O EXÉRCITO DE TI DA UCRÂNIA E A PARTICIPAÇÃO DIRETA DE CIVIS NAS HOSTILIDADES



ALEXANDRE PERES TEIXEIRA

Doutor em Direito pelo CEUB. Mestre em Ciências Navais, pela Escola de Guerra Naval. Especialista em Direito Internacional Humanitário, pela Universidade de Brasília, e em Direito Internacional Cibernético, pelo Processo de Haia.

Introdução

O conflito armado deflagrado entre a Rússia e a Ucrânia a partir de 2022 tem redefinido os contornos tradicionais da guerra moderna, inserindo o ciberespaço e a tecnologia digital no centro das estratégias de confronto e da segurança internacional. Nesse cenário de hostilidades prolongadas, a mobilização de atores não estatais e, de maneira destacada, de cidadãos comuns emergiu como um fenômeno sem precedentes na dinâmica dos conflitos contemporâneos. A criação do Exército de TI da Ucrânia, formalizada nos primeiros dias da invasão por iniciativa de lideranças do setor tecnológico e endossada pelo Ministério da Transformação Digital liderado por Mykhailo Fedorov, institucionalizou a atuação de cibervoluntários nacionais e internacionais em operações de negação de serviço distribuído (DDoS), espionagem digital e guerra cognitiva.

Essa reconfiguração tática, contudo, transcende a mera inovação tecnológica, esbarrando diretamente em complexos dilemas jurídicos, éticos e humanitários. A literatura especializada e os relatórios recentes apontam que a participação ativa da sociedade civil — seja por meio de ataques cibernéticos a infraestruturas civis russas, da propagação de contra panfletos e narrativas em redes sociais por grupos como a Organização dos Companheiros do Atlântico Norte (NAFO), ou do fornecimento de inteligência tática baseada em fontes abertas e aplicativos móveis de denúncia (como o eVorog) — coloca em xeque os pilares do Direito Internacional Humanitário (DIH).

A problematização central que orienta este estudo reside na fragilização da distinção clássica entre combatentes e não combatentes. Ao incentivarem civis a atuarem como sensores de inteligência, realizarem varreduras de reconhecimento facial em soldados mortos para fins de guerra psicológica e participarem de manobras cibernéticas ofensivas, as autoridades ucranianas expõem essa população a graves riscos de retaliação e à perda da proteção jurídica conferida pelo DIH aos civis que não tomam parte direta nas hostilidades. Ademais, observa-se uma ambiguidade na postura de governos ocidentais e de organismos internacionais, que por vezes flexibilizam interpretações normativas consolidadas na última década para legitimar politicamente a resistência ucraniana, estabelecendo precedentes perigosos para conflitos futuros.

Apesar do crescente acervo jornalístico e de relatórios técnicos sobre o papel das tecnologias emergentes na guerra russo-ucraniana, ainda carece na academia de uma análise aprofundada que articule criticamente a participação civil nas hostilidades cibernéticas e informacionais sob a ótica da legalidade internacional e das repercussões humanitárias.



Diante disso, este artigo tem como objetivo analisar a estrutura, a evolução e o impacto da atuação do Exército de TI da Ucrânia e de redes civis de voluntariado digital, examinando as implicações jurídicas decorrentes da erosão do status de proteção dos civis no ciberespaço e na guerra cognitiva. Justifica-se o presente estudo pela urgência de debater os limites da participação civil em conflitos tecnológicos contemporâneos, contribuindo para o debate acadêmico sobre a adaptação do Direito Internacional Humanitário às novas fronteiras da guerra cibernética e informacional.

A Gênese e a Institucionalização do Exército de TI da Ucrânia

A ideia de criação do Exército de TI da Ucrânia começou com Yegor Aushev, um conhecido empresário de TI ucraniano e cofundador de três empresas, as quais se tornaram relevantes, em meio à guerra de oito anos com a Rússia (Cyber Unit Tech, Cyber School e Hacken.io). Segundo Janofsky[1], em algum momento entre os dias 24 de fevereiro (dia da invasão russa) e 26 de fevereiro, Aushev apresentou sua ideia de criação de um exército de "cibervoluntários" a Mykhailo Federov, ao jovem ministro da Transformação Digital da Ucrânia, de 31 anos.

Segundo Schectman e Bing[2], na mesma época, Aushev também assumiu a tarefa de reunir um grupo 1.000 homens, voluntários, para atuar na segurança cibernética da Ucrânia, a pedido de um alto funcionário do Ministério da Defesa ucraniano. Cluley[3] ressalta que Aushev facilitou a formação deste grupo no Twitter e em vários outros fóruns de hackers, ao postar um formulário de inscrição do Google Docs, com a finalidade de avaliar o nível de habilidade e a área de especialização dos prováveis candidatos.

Soesanto[4] afirma que, de acordo com Aushev, esse grupo de "voluntários ucranianos de segurança cibernética seria dividido em dois outros grupos: um ofensivo e outro defensivo". Em entrevista com a Reuters, em 24 de fevereiro, Aushev afirmou que o grupo defensivo seria empregado para proteger a infraestrutura crítica, tais como usinas de energia e sistemas de água, e o grupo ofensivo ajudaria "os militares da Ucrânia a conduzir operações de espionagem digital contra forças russas invasoras". Como disse Aushev, "temos um exército dentro de nosso país. [...] Precisamos saber o que eles estão fazendo"[5]. Ato contínuo, inspirado pela ideia de Aushev, da criação de um exército de cibervoluntários, Federov foi ao Facebook, em 26 de fevereiro e postou a seguinte mensagem em ucraniano:

> Temos muitos ucranianos talentosos na esfera digital: desenvolvedores, ciberespecialistas, designers, redatores, profissionais de marketing, targetologistas, etc. Estamos criando um exército de TI. Todas as tarefas operacionais serão apresentadas no canal do telegram: t.me/itarmyofurraine. Haverá tarefas para todos[6].

Segundo Soesanto[7], Federov postou a mesma mensagem em ucraniano em seu forte canal, de 170.000 assinantes, no Telegram. Logo depois, na sua conta certificada do Twitter, escreveu em inglês: “estamos criando um exército de TI. Precisamos de talentos digitais. Todas as tarefas operacionais serão dadas aqui: t.me/itarmyofurraine”. Segundo Simonite e Volpicelli[8], a cobertura da mídia ocidental, sobre o surgimento do Exército de TI, concentrou-se quase exclusivamente na postagem feita por Federov no Twitter – porque foi escrita em inglês – e ignorou as postagens do Facebook e do Telegram[9].

Ainda conforme Soesanto[10], existem diferenças curiosas entre essas três postagens. Primeiro, o público-alvo de Federov, no Twitter, era claramente internacional, enquanto, no Facebook e no Telegram, tinha como alvo, principalmente, a sociedade ucraniana. Em segundo lugar, em suas postagens, no Facebook e no Telegram, Federov foi muito preciso sobre o tipo exato de talento que o Exército de TI buscava.E terceiro, em todas as três mensagens, Federov escreveu errado “Ucrânia” – mas apenas sua postagem no Telegram foi corrigida posteriormente. Curiosamente, por causa desse contratempo, há apenas uma postagem no canal “itarmyofurraine” que redireciona os usuários para o canal oficial e correto “itarmyukraine2022”[11].

Sabe-se que alguém também decidiu abrir um canal no Telegram, no mesmo dia, chamado “itarmyofuraine” (um “r”, falta o “k”). Tal canal conta, atualmente, com cerca de 11.500 inscritos e repassa parte do conteúdo do canal oficial para os hackers voluntários. Provavelmente, os meios de comunicação ocidentais perderam uma postagem do canal oficial Telegram, do Ministério da Transformação Digital, realizada em 26 de fevereiro, às 18h48 (horário local da Ucrânia).

Seu conteúdo era quase idêntico à mensagem de recrutamento de Federov, exceto que na postagem do Ministério foi acrescentada uma frase crucial: “exortamos você a usar qualquer vetor de ataques cibernéticos e DDoS, contra os recursos russos”[12].Essa chamada às armas deu vazão à primeira postagem, no canal oficial do Telegram, do Exército de TI, que proclamou duas horas antes: “tarefa nº 1: Encorajamos você a usar quaisquer dos vetores de ataques cibernéticos e DDoS, nesta empreitada”[13]. A postagem “listou como alvos 31 bancos, empresas e sites governamentais russos”[14].

Um relatório público afirmou que o número de membros do Exército de TI já estaria em cerca de 300.000, no início das ações. Este montante seria derivado do número de assinantes do canal oficial do Telegram, e do Exército de TI[151617]. De acordo com a TGStat, uma plataforma que fornece análises para canais e chats do Telegram, o canal de Telegram do Exército de TI atingiu sua maior contagem de assinantes em 26 de março, com o total de 307.165 membros[18]. A partir desta data, os números diminuíram continuamente, levando a uma perda acumulada de 47.940 assinantes, nas oito semanas seguintes (15,6%).

Em 10 de junho de 2022, a contagem de assinantes do Exército de TI era de 259.225.25[19]. Embora não se saiba, ao certo as razões para a perda de tantos seguidores tão rapidamente, para Soesanto[20], a explicação mais provável está relacionada a uma combinação de alguns fatores, tais

como “(1) a perda de novidades ao longo do tempo, (2) tédio devido a tarefas repetitivas e (3) a própria guerra cinética em andamento, que permanece praticamente inalterada pelas atividades DDoS do Exército de TI, devido ao foco em se atingir a infraestrutura civil russa”[21].

A partir de um determinado momento, não se pode afirmar o porquê, ocorreu uma mudança interna na orientação das ações, que passaram a reunir desenvolvedores, designers e redatores para o foco, quase exclusivo do Exército de TI, também na realização de ataques DDoS. Uma explicação provável pode estar relacionada com o fato dos voluntários possuidores de talento específico, aos quais Federov havia destacado em seu post de convocação, terem sido canalizados para um grupo chamado “StandForUkraine”[22].

Bajak[23] afirma que o grupo “StandForUkraine” foi apoiado por Roman Zakharov, um executivo de TI ucraniano, de 37 anos. Tal grupo atualmente consiste em cerca de 1.300 “engenheiros de software, gerentes de marketing, designers gráficos e compradores de anúncios online”[24], que estão lutando na frente de guerra de informação da Ucrânia. O grupo está tentando mobilizar a comunidade internacional contra a invasão russa e está espalhando propaganda de guerra nos meios de comunicação ocidentais e plataformas de mídia social.

O grupo também expulsou, com sucesso, as empresas ocidentais da Rússia[25]. O grupo “StandForUkraine” tem seu próprio site, mas, ao contrário do Exército de TI, para se comunicar e se organizar está usando bate-papos privados apenas para convidados, no aplicativo de mensagens “Signal”[26].

Em relação às ações do Exército de TI, cabe ressaltar que Federov, apesar de muito ativo no Telegram, postou no Twitter apenas 500 vezes, ou um pouco mais, desde novembro de 2020. No entanto, mesmo no Telegram, Federov raramente fala sobre o Exército de TI. Entre 26 de fevereiro e 20 de abril de 2022, ele encaminhou apenas 18 mensagens, do canal oficial de TI do Exército.

Segundo Soensanto (2022, p. 7 – tradução nossa), para um Ministro que criou esse exército de voluntários digitais, Federov parece bastante desinteressado. Ao invés disto, a maioria de suas postagens no Telegram gira em torno de seus esforços para expulsar empresas ocidentais da Rússia, “arrecadar fundos para projetos humanitários e para as forças armadas ucranianas e informar os cidadãos sobre o trabalho mais recente de seu ministério”.

Inicialmente acreditava-se que o site do Ministério da Transformação Digital exibiria, de forma proeminente, a sua conexão com o Exército de TI da Ucrânia e cobriria suas atividades, em andamento, de alguma forma, entretanto, nada disto ocorreu[27].Até o momento, não há uma única notícia, no site do Ministério, que fale sobre o Exército de TI. Da mesma forma, o canal oficial do Telegram, do Ministério mencionou o Exército de TI apenas dez vezes e encaminhou apenas quatro postagens do canal oficial do Exército de TI, entre 26 de fevereiro e 20 de abril[28].

Possivelmente, estimulado pela falta de cobertura consistente, o canal Telegram do Ministério anunciou, em 18 de abril de 2022, que, daquela data em diante, falaria todas as segundas-feiras sobre as vitórias do Exército de TI[29]. Notavelmente, em 23 de maio, o Ministério resumiu que "desde a invasão russa da Ucrânia, o exército de TI atacou cerca de 2.000 recursos russos"[30]. O Ministério mencionou o Exército de TI, em seu canal no Telegram, em duas notícias no "kmu.gov.ua" – o portal oficial do governo ucraniano. Isto só foi ocorrer mais de duas semanas após a chamada de recrutamento de Federov.

Uma notícia, em 10 de março, reconheceu brevemente a existência do Exército de TI, enquanto o post de 12 de março tinha o título de destaque: "o Ministério da Transformação Digital criou 3 serviços para combater os ocupantes na frente digital": O Exército de TI, as Forças da Internet da Ucrânia, e o aplicativo e-Enemy[31].

Para Soesanto[32], a cobertura desigual e bastante irregular, pelo Ministério da Transformação Digital, sobre as atividades do Exército de TI, nos primeiros dois meses após a invasão, "pode ter sido decorrente da estrutura organizacional difusa e ainda em evolução do próprio Exército de TI".

Quando iniciou suas ações, o Exército de TI consistia apenas de dois grupos distintos: um chamado "global contínuo", que concentrava os hackers, de qualquer lugar do planeta, dispostos a participar de ataques coordenados DDoS, contra alvos escolhidos da infraestrutura russa – este grupo era composto, principalmente, por voluntários civis; e a "equipe interna", provavelmente composta por pessoal ucraniano da área de defesa e do setor de inteligência.

A equipe interna era encarregada pela condução de operações cibernéticas cada vez mais complexas, contra alvos russos específicos. Ambos os grupos, do Exército de TI, se ainda estiverem ativos, são de natureza puramente ofensiva e servem para reunir civis voluntários amadores, dispostos a participar das operações cibernéticas contra a Rússia, com servidores do governo (civis, militares, e da inteligência), organizados em uma estrutura hierárquica[33].

No entanto, à medida que a estrutura do Exército de TI se consolida e passa a integrar atores governamentais e especialistas, o ecossistema de resistência ucraniano expande-se para além das operações estritamente cibernéticas e de negação de serviço. Esse desdobramento dá margem a uma frente multifacetada de combate que mobiliza cidadãos comuns em campanhas de desinformação, inteligência de fontes abertas e contra narrativas psicológicas, transformando o tecido social civil em um elemento ativo da engrenagem de defesa nacional.

Guerra Cognitiva, Inteligência de Fontes Abertas (OSINT) e o Papel dos Civis

Além disso, o Exército de TI também deu origem a um ecossistema que inclui empresas de TI, de propriedade ucraniana, e indivíduos localizados fora da Ucrânia, bem como ucranianos que vivem

na Ucrânia e trabalham para empresas ocidentais. Este ecossistema tem continuamente criado novas ferramentas, gerado know-how; identificado novos alvos e cumprido outras funções de suporte de inteligência, para sustentar os esforços ofensivos da Ucrânia, no ciberespaço[34].

Para Romandash[35], um dos principais ganhos do Exército de TI foi combater, com sucesso, a guerra psicológica empreendida pela Rússia, contra a Ucrânia, desde 2014. Desta forma, a autora acredita que em 2022, a Ucrânia mudou a visão internacional sobre a invasão russa.Neste sentindo, os esforços da Ucrânia contribuíram, significativamente, para o isolamento digital da Rússia e integraram as contranarrativas da Ucrânia, com a ajuda de dados de fontes abertas, aliados digitais e campanhas de comunicação bem-sucedidas[36].

As capacidades russas para a guerra cognitiva dependem da tecnologia ocidental, bem como de recursos financeiros para financiar inúmeras fábricas de trolls, hackers e "idiotas úteis[37]". Redes de "lobistas" russas tentam "espalhar as narrativas da Rússia em países ao redor do mundo"[38]. Além disso, a Ucrânia fez parceria com empresas de tecnologia como Clearview e Palantir, que fornecem soluções baseadas em IA, às questões de identificação, com biometria facial e também com a tomada de decisões táticas, na linha na frente de combate[39].

Por meio dessa parceria, as Forças Armadas da Ucrânia agora podem acessar dados que identificam melhor os soldados da Rússia, e usar essas informações para sua própria guerra de informação com a finalidade de resistir à Rússia. O software combina a imagem real de soldados russos, cometendo crimes de guerra, e mostrando on time as suas identidades. Com certeza uma tecnologia que será extremamente útil para futuros tribunais de guerra[40].

À medida que aumenta o número de mortos na guerra entre a Rússia e a Ucrânia, a questão de como tratar adequadamente os restos mortais de soldados mortos tornou-se um tema recorrente. Alguns relatos da mídia afirmam, por exemplo, que as forças ucranianas estão publicando fotos de soldados russos mortos nas redes sociais para que os familiares possam "determinar se as imagens apresentam um ente querido desaparecido"[41]. Segundo Brewster[42], a orientação do governo ucraniano, em relação a esta questão é a seguinte:

> Encontre uma foto de um soldado russo morto, nas redes sociais. Carregue-o no software de reconhecimento facial. Obtenha uma correspondência de identidade de um banco de dados de bilhões de imagens de mídia social. Identifique a família e os amigos do falecido. Mostre a eles o que aconteceu com a vítima da guerra de Putin contra a Ucrânia[43].

Autoridades[44] ucranianas realizaram mais de 8.600 buscas de reconhecimento facial em soldados russos mortos ou capturados, nos 50 dias, desde o início da invasão, usando as varreduras de IA para identificar corpos e contatar centenas de famílias, no que pode ser uma das aplicações mais

orríveis da tecnologia, no curso de um conflito armado.O Exército de TI do país e outros ativistas voluntários, que seguem a direção do governo ucraniano, dizem que usaram essas identificações para informar as famílias sobre a morte de 582 russos, inclusive enviando-lhes fotos dos cadáveres abandonados, que são postadas em redes sociais [45].

Os ucranianos defendem o uso do software de escaneamento facial da empresa de tecnologia norte-americana Clearview AI, como uma forma brutal, mas eficaz, de provocar dissidência dentro da Rússia, desencorajar outros combatentes e apressar o fim de uma guerra devastadora. Mas alguns analistas militares e de tecnologia temem que a estratégia possa sair pela culatra, inflamando a raiva na sociedade russa por uma campanha de choque e pavor, dirigida a mães e esposas, que podem estar a milhares de quilômetros dos verdadeiros decisores da máquina de guerra do Kremlin[46].

A solidariedade do Ocidente com a Ucrânia torna tentador o apoio a um ato tão radical e bizarro, que contraria o DIH, e se destina a, desumanamente, capitalizar o luto familiar e causar sofrimento desnecessário a civis que não tomam parte nas hostilidades. O fato de contatar os familiares dos soldados mortos se perfaz em uma sinistra ação de “guerra psicológica clássica” e pode estabelecer um novo padrão perigoso para conflitos do futuro[47].

A estratégia das autoridades ucranianas, de informar as famílias sobre a morte de seus entes queridos, levantou preocupações de que isso pudesse irritar os mesmos russos que eles esperavam persuadir. Um especialista em segurança nacional disse que outras ações ucranianas – realizar coletivas de imprensa com soldados russos capturados e postar nas redes sociais fotos e vídeos mostrando prisioneiros de guerra – foram vistas dentro da Rússia, não como uma exposição bem-vinda da verdade, mas como uma humilhação[48] desnecessária e ilegal do inimigo[49].

Esta tem sido uma das estratégias de guerra psicológica da Ucrânia para tentar informar os russos, aos quais, supostamente, o acesso à mídia é controlado pelo governo. Segundo o governo da Ucrânia, as informações sobre a morte que tem sido causada pela insana invasão autorizada pelo Presidente Putin, não podem ser controladas pela Federação russa.

Brewster[50] afirma que o Vice-Primeiro-Ministro, que também é o chefe do Ministério da Transformação Digital, na Ucrânia, Mykhailo Fedorov, confirmou, em seu perfil no Telegram, que a tecnologia de vigilância estavasendo usada dessa maneira, semanas depois que a Clearview AI, empresa provedora de reconhecimento facial, com sede em Nova York, passou a oferecer seus serviços à Ucrânia para os mesmos fins[51]. A Clearview AI estaria fornecendo seu software, gratuitamente, ao governo ucraniano.

Em entrevista à Reuters, o CEO da Clearview, Hoan Ton-That, disse que a empresa tinha um estoque de 10 bilhões de rostos de usuários, extraídos de mídias sociais, incluindo 2 bilhões do

Facebook russo, que é chamado de “Vkontakte”. Fedorov escreveu em um post no Telegram que o objetivo final era “dissipar o mito russo de uma ‘operação especial’ cirúrgica, na qual ‘não há recrutas’ e ‘ninguém morre’”[52].

A intensa mobilização de civis em operações de inteligência e o emprego de táticas de forte impacto psicológico, contudo, não ocorrem em um vácuo regulatório. Ao transpor as fronteiras tradicionais do confronto militar para o ciberespaço e para a esfera da informação, essas ações exigem um escrutínio rigoroso acerca da responsabilidade estatal, levantando debates profundos sobre a atribuição de condutas a governos e o papel da comunidade internacional na validação dessas estratégias.

Os Limites da Atribuição e a Flexibilização Normativa Ocidental

O DIH, incluindo as Convenções de Genebra de 1949, o Protocolo Adicional I a esses instrumentos, bem como o direito internacional consuetudinário, regem as atividades beligerantes entre Rússia e Ucrânia. Nesse sentido, segundo Biggerstaff[53], alguns observadores condenaram as alegadas práticas ucranianas e sugeriram que a publicação de fotos de soldados mortos viola o Artigo 13º da Convenção Relativa ao Tratamento de Prisioneiros de Guerra, de 1949 (GC III), bem como o direito internacional consuetudinário ou ambos.

A divulgação de fotos para familiares também levanta a questão separada de saber se isso viola o processo de notificação de parentes próximos, delineado na primeira Convenção de 1949, para “Melhorar a Condição dos Feridos e Doentes das Forças Armadas no Campo”[54].

Ao lado das ações de DDoS, a conduta do Exército de TI compartilha uma ampla gama de sobreposições estratégicas, como ocorreu com a campanha DDoS contra a Estônia, em maio de 2007. A mencionada campanha foi organizada por hacktivistas nacionalistas russos por meio de fóruns/sites em língua russa e durou 22 dias. Até hoje, nenhuma evidência clara de envolvimento do governo russo surgiu e, como tal, a campanha nunca foi oficialmente atribuída ao Governo russo.

Como resultado, as críticas estonianas e ocidentais apontaram que Moscou não havia tomado medidas significativas para mitigar a campanha DDoS (uma violação de sua obrigação de devida diligência), bem como que a falta de cooperação com a investigação estoniana foi destacada como prova de que o governo russo estava protegendo os perpetradores – e, portanto, apoiando-os implicitamente[55].

No entanto, em contraste com o anonimato dos ataques de 2007, a conduta de ações de DDoS, do Exército de TI, é bastante clara, principalmente em relação a atribuição da ação do grupo a uma autoridade governamental no que tange às instruções, à direção e ao controle dos ataques.

É igualmente claro que o Exército de TI está atacando, de forma persistente e indiscriminada, a infraestrutura civil russa, incluindo farmácias on-line, bancos, serviços de entrega de alimentos e varejistas. Mas, embora a Rússia tenha sido justamente vilipendiada pelos ataques DDoS em 2007, o Exército de TI e seu Ministro da Transformação Digital, Mykhailo Federov, receberam dois prêmios no Fórum Europeu de Segurança Cibernética CYBERSEC 2022, em Katowice, Polônia, por sua "resistência heroica à agressão russa, e na proteção das fronteiras digitais do mundo democrático"[56].

Como mesmo disse Federov, "este prêmio é, antes de mais nada, para toda a comunidade cibernética e para os voluntários que agora estão travando a primeira guerra cibernética do mundo, conosco"[57].Soesanto[58] afirma que, embora certamente haja uma diferença entre as campanhas DDoS, conduzidas em tempos de paz e durante os tempos de conflitos armados, "parece que o Ocidente agora está jogando fora as interpretações legais e normativas que defendeu no ciberespaço na última década, para apoiar politicamente a Ucrânia".

A conduta do grupo interno do Exército de TI evoluiu rapidamente, de meras desfigurações de sites russos, durante os primeiros dias da invasão, para campanhas de espionagem sofisticadas. Evoluiu também para a primeira operação cibernética ofensiva destrutiva – que visou uma plataforma de vídeo civil - no início de maio 2022.

Atualmente, não se faz claro em que tipo de operações cibernéticas a equipe interna se concentrará no futuro. Entretanto, se a trajetória evolutiva, ao longo dos últimos 4 meses servir de métrica, os defensores russos provavelmente enfrentarão uma variedade de operações cibernéticas experimentais, que tentarão produzir impactos cada vez mais severos e efeitos mais duradouros.

Nesse sentido, Greenberg[59] afirma que um grupo de advogados de direitos humanos decidiu, recentemente, pressionar o Tribunal Penal Internacional, em Haia, a abrir o primeiro casode crime de guerra cibernética, contra o "Sandworm" – uma unidade de inteligência militar russa, que teve como alvo as concessionárias de energia elétrica, na Ucrânia e causou curtos e apagões regionais, em 2015-2016.

A maior conquista do Exército de TI ocorreu em outubro de 2016, quando conseguiram hackear e vazar o conteúdo da conta de e-mail de Vladislav Surkov, Conselheiro próximo de Putin no conflito no leste da Ucrânia. Os vazamentos revelaram os esforços de Surkov para desestabilizar a Ucrânia, minar o governo ucraniano e orquestrar a eleição de certos políticos separatistas, fornecendo evidências concretas de atividades que Moscou havia negado anteriormente[60]. Além disso, os ataques DDoS podem afetar a opinião pública na Rússia. Um fluxo constante de inconvenientes e interrupções provavelmente tem aumentado o descontentamento dos russos com a guerra.

No início de março de 2022, apenas 58% dos russos apoiavam a invasão, de acordo com uma pesquisa independente, realizada por telefone. Como Fedorov, o Vice-Primeiro-Ministro ucraniano, disse em uma entrevista recente, o objetivo desses sites retirados é "tornar a vida tão desagradável e inconveniente para os cidadãos russos que eles questionariam a guerra"[61].

Se por um lado o endosso político e a flexibilização das normas internacionais pelo Ocidente buscam legitimar a resistência estatal no ciberespaço, por outro, a institucionalização do engajamento civil irrestrito cobra um preço humano e jurídico alarmante. A diluição das fronteiras entre combatentes e não combatentes coloca em xeque a própria eficácia protetiva do Direito Internacional Humanitário, expondo a população a dilemas existenciais e a graves retaliações no teatro de operações.

Implicações Jurídio-Humanitárias: A Perda do Status de Proteção dos Civis

Um procedimento que tem gerado extrema preocupação para as organizações humanitárias é o largo emprego de civis, que não estão no contexto das operações cibernéticas maliciosas empreendidas pelos grupos do Exército de TI, mas são incentivados a se envolverem na coleta de inteligência de fontes abertas, com a finalidade de contribuir diretamente para as campanhas militares da Ucrânia, no contexto deste conflito.

Neste sentido, Melkozerova[62] afirma que os dados de fontes abertas têm sido fundamentais para desmascarar as notícias falsas da Rússia e fortalecer a narrativa da Ucrânia sobre a guerra em curso. Por exemplo, Melkozerova[63], afirma que dados de fontes abertas permitiram que jornalistas investigativos desmentissem várias declarações do Ministério da Defesa da Rússia, alegando que eles tinham destruído depósitos de munição e quartéis militares da Ucrânia, ou que mataram um número significativo de tropas ucranianas.

Segundo Romandash[64], os dados de fontes abertas foram cruciais para fornecer evidências dos crimes cometidos pelo exército russo, em Bucha, Borodyanka e outros territórios liberados da Ucrânia.A autora segue afirmando que este tipo de inteligência está sendo empregada, ativamente, enquanto a guerra continua "com a finalidade de ajudar a localizar, geograficamente, as tropas russas, confirmar declarações sobre batalhas importantes e descobrir locais de onde mísseis estão sendo lançados contra a Ucrânia"[65].

Além do seu Exército de TI, a Ucrânia agora tem seu próprio "Exército de Elfos[66]", formado por cidadãos ucranianos, de baixa capacidade tecnológica[67]. Braun[68] relata que o grupo de elfos mais proeminente é o NAFO (Organização dos Companheiros do Atlântico Norte), composto por voluntários digitais que zombam da propaganda russa online e aumentam a conscientização sobre os crimes cometidos pelos russos, na Ucrânia.

Braun[69] afirma que, embora não haja estimativa oficial do número de membros da NAFO, o total pode variar de dezenas de milhares a centenas de milhares. Voltado para o público ocidental, o movimento NAFO cria e entrega conteúdo, em inglês, para internautas nos Estados Unidos, Europa e outras partes do mundo ocidental.

A NAFO apresenta um "elemento importante da guerra cognitiva contra a Rússia ao usar memes, piadas e outros meios criativos"[70]. Por exemplo, alguns membros da NAFO geram discussões sobre temas relacionados com a Ucrânia. Alguns lutam contra o "whataboutism", que é a tentativa de propaganda da Rússia de desviar a atenção da invasão para que o papel da Rússia como agressor seja minimizado, como, por exemplo, fazendo perguntas sobre a invasão do Iraque, pelos EUA[71].

A inteligência coletada por civis foi responsável por ataques a bases russas, em território ocupado, embora a confirmação de seu uso pela Ucrânia arrisque retaliações contra civis por parte da Rússia. Já existem relatos de soldados russos atirando contra civis que estivessem fotografando ou filmando, com smartphones.

Em setembro de 2022, moradores da cidade de Kherson, então sob controle russo, usaram o eVorog para relatar a localização de um depósito, onde veículos militares russos foram armazenados. O prédio foi destruído por um forte ataque no dia seguinte. Prédios usados como quartéis, na região, também foram atingidos. Colaboradores dos russos também usaram aplicativos, disfarçados de jogos em celulares, para registrar os movimentos da artilharia ucraniana[72].

Cabe ressaltar que as pessoas que enviam informações, via eVorog, de áreas ocupadas pela Rússia, correm grandes riscos. O aplicativo aconselha aos usuários a excluir de seus telefones qualquer evidência[73] de que tenham carregado algum dado operacional. Os partidários digitais enfrentam possíveis represálias e alguns já foram mortos por conta desta atividade, que foi detectada por soldados russos. O DIH, que protegem os civis, não protegem àqueles que participam diretamente das hostilidades ativas.

O repasse de informações táticas figura como coleta de dados de inteligência e se traduz em participação de civis em hostilidades, o que faz com que o civil perca a proteção contra os ataques diretos, enquanto estiver participando do conflito[74]. O aspecto mais controverso do eVorog é que ele permite que os ucranianos denunciem colaboradores e espiões russos. Seus desenvolvedores, inicialmente, usaram como exemplo de colaboração uma mulher ucraniana que engravidou de um soldado russo, insinuando que as vítimas de estupro poderiam ser consideradas traidoras.Eles voltaram atrás e se desculparam, afirmando que o objetivo do aplicativo era o de "identificar o inimigo, não condenar as ações dos ucranianos"[75].

Joshi[76] argumenta que uma lição para ser extraída desta situação peculiar é que a conectividade se torna, cada vez mais, um recurso militar vital. Há muito tempo, o Talibã derrubou torres de telefonia móvel para impedir que aldeões afegãos enviassem denúncias às forças de segurança. Os cartéis de drogas mexicanos agora usam equipamentos de interferência de sinal. O general Nikolyuk, da Ucrânia, diz que a assistência civil foi menos disponível em Kharkiv e Donetsk, no Leste, porque a Rússia interrompeu as redes de telefonia móvel nessas áreas[77].

Tudo isso pressupõe que os exércitos estão fazendo esforços de boa-fé para discriminar entre civis e soldados – que eles se preocupam com as leis da guerra. Se os civis ucranianos, frequentemente, estão dispostos a comprometer seu status de não combatentes, tanto servindo ao Exército de TI, ou como Exército de “Elfos”, atuantes como sensores de Inteligência para as tropas ucranianas, pode ser porque o exército da Rússia tem mostrado pouca consideração por tais sutilezas.

O general Nikolyuk relembra quando as tropas russas estabeleceram um quartel-general, em uma escola em Yahidne, um vilarejo ao sul da cidade de Chernihiv. Centenas de moradores foram presos no porão naquela ocasião. Em outro momento, na cidade vizinha de Lukashivka, o General disse que soldados russos, avistando um drone ucraniano, forçaram mulheres e crianças a andar na rua como escudos humanos.

“O que você faz nesses casos? Você morde os punhos com impotência e é isso![78]. O problema central em se colocar civis despreparados dentro de tarefas táticas operacionais é saber como será a reação do inimigo, ao tomar conhecimento de tal procedimento pela parte oposta. Parece que no conflito entre Rússia e Ucrânia a reação dos Russos não tem sido a das melhores.

Em suma, a simbiose forçada entre a população civil e as engrenagens táticas de defesa da Ucrânia evidencia uma perigosa mutação nos conflitos armados contemporâneos. Ao transformar cidadãos comuns em peças ativas de uma engrenagem cibernética e de inteligência, rompe-se o delicado equilíbrio humanitário que sustenta o direito dos conflitos, deixando um legado de vulnerabilidade extrema cujos reflexos e precedentes ecoarão por gerações nos campos de batalha do futuro.



Considerações Finais

O conflito entre Rússia e Ucrânia tem se consolidado como um marco divisor na história dos conflitos armados, inaugurando uma era em que o ciberespaço, a tecnologia digital e a informação tornam-se teatros primários de hostilidades. Conforme analisado, a criação do Exército de TI da Ucrânia e a ampla mobilização de civis — seja por meio de ataques DDoS, campanhas de guerra cognitiva conduzidas pelo NAFO ou o fornecimento de inteligência tática via fontes abertas e aplicativos como o eVorog — demonstraram a eficácia de uma defesa nacional descentralizada e tecnologicamente integrada.

No entanto, essa simbiose forçada entre o aparato estatal e a sociedade civil acarreta profundos e alarmantes dilemas jurídicos e humanitários. A erosão da distinção clássica entre combatentes e não combatentes expõe cidadãos comuns a severas retaliações e à perda de sua proteção jurídica sob a égide do Direito Internacional Humanitário (DIH). Ademais, estratégias de alto impacto psicológico — como o uso de inteligência artificial para identificação de soldados mortos e o contato direto com seus familiares — e a ambiguidade na chancela de tais práticas por parte da comunidade internacional estabelecem precedentes perigosos para a estabilidade das normas globais de guerra.

Em última análise, a experiência ucraniana evidencia que a conectividade e a participação civil tornaram-se recursos militares cruciais na guerra moderna. Resta evidente, contudo, que a urgência de resistir à agressão estatal não pode anular os princípios fundamentais que buscam limitar o sofrimento humano em tempos de conflito. O futuro das operações militares e cibernéticas exigirá da comunidade acadêmica, dos Estados e dos organismos internacionais uma urgente revisão e adaptação das normativas vigentes, a fim de conter a vulnerabilidade extrema de populações civis tragicamente engajadas nas engrenagens da guerra tecnológica.



Considerações Finais

O conflito entre Rússia e Ucrânia tem se consolidado como um marco divisor na história dos conflitos armados, inaugurando uma era em que o ciberespaço, a tecnologia digital e a informação tornam-se teatros primários de hostilidades. Conforme analisado, a criação do Exército de TI da Ucrânia e a ampla mobilização de civis — seja por meio de ataques DDoS, campanhas de guerra cognitiva conduzidas pelo NAFO ou o fornecimento de inteligência tática via fontes abertas e aplicativos como o eVorog — demonstraram a eficácia de uma defesa nacional descentralizada e tecnologicamente integrada.

No entanto, essa simbiose forçada entre o aparato estatal e a sociedade civil acarreta profundos e alarmantes dilemas jurídicos e humanitários. A erosão da distinção clássica entre combatentes e não combatentes expõe cidadãos comuns a severas retaliações e à perda de sua proteção jurídica sob a égide do Direito Internacional Humanitário (DIH). Ademais, estratégias de alto impacto psicológico — como o uso de inteligência artificial para identificação de soldados mortos e o contato direto com seus familiares — e a ambiguidade na chancela de tais práticas por parte da comunidade internacional estabelecem precedentes perigosos para a estabilidade das normas globais de guerra.

Em última análise, a experiência ucraniana evidencia que a conectividade e a participação civil tornaram-se recursos militares cruciais na guerra moderna. Resta evidente, contudo, que a urgência de resistir à agressão estatal não pode anular os princípios fundamentais que buscam limitar o sofrimento humano em tempos de conflito. O futuro das operações militares e cibernéticas exigirá da comunidade acadêmica, dos Estados e dos organismos internacionais uma urgente revisão e adaptação das normativas vigentes, a fim de conter a vulnerabilidade extrema de populações civis tragicamente engajadas nas engrenagens da guerra tecnológica.



Referências

BAJAK, F. Ukraine digital army brews cyberattacks, intel and infowar. Voice of America, Ukraine, 2022. Disponível em: https://web.archive.org/web/20220608141931/https://apnews.com/article/russiaukraine-technology-europe-hacking-f2c4960e48b8022a567780f3602b54e2.Acesso em: 25 jul. 2026.

BIGGERSTAFF, W. C. Ukraine Symposium – photos of the dead. Lieber Institute- West Point, New York, 2022. Disponível em: https://lieber.westpoint.edu/photos-of-dead/ Acesso em: 25 jul. 2023.
BRAUN, S. Ukraine's info warriors battling Russian trolls. DW, Berlin, 2022. Disponível em: https://www.dw.com/en/nafo-ukraines-info-warriors-battlingrussian-trolls/a-63124443. Acesso em: 25 jul. 2026.

BREWSTER, T. Ukraine Starts Using Facial Recognition To Identify Dead Russians And Tell Their Relatives. Forbes, Jersey City, 2022. Disponível em: https://www.forbes.com/sites/thomasbrewster/2022/03/23/ukraine-starts-using-facial-recognition-to-identify-dead-russians-and-tell-their-relatives/?sh=f5b58ac28985 Acesso em: 25 jul. 2026.
CLULEY, G. Ukraine calls for volunteer hackers to protect its critical infrastructure and spy on Russian forces. Bitdefender, [S.l.], 2022. Disponível em: https://web.archive.org/web/20220608141452/https://www.bitdefender.com/blog/hotforsecurity/ukraine-calls-for-volunteer-hackers-to-protect-its-critical-infrastructure-and-spy-on-russian-forces/ . Acesso em: 25 jul. 2023.

CLULEY, G. Ukraine calls for volunteer hackers to protect its critical infrastructure and spy on Russian forces. Bitdefender, [S.l.], 2022. Disponível em: https://web.archive.org/web/20220608141452/https://www.bitdefender.com/blog/hotforsecurity/ukraine-calls-for-volunteer-hackers-to-protect-its-critical-infrastructure-and-spy-on-russian-forces/ . Acesso em: 25 jul. 2026.

FAIFE, C. In Ukraine, Hacktivists fight back with Data Leaks. The Verge, [S.l.], 2022. Disponível em: https://www.theverge.com/2022/3/11/22968049/anonymous-hacks-ukraine-russia-cybercrime-danger.Acesso em: 25 jul. 2026.

GREENBERG, A. The Case for War Crimes Charges Against Russia's Sandworm Hackers. Wired, [S.l.], 2022. Disponível em: https://www.wired.com/story/cyber-warcrimes-sandworm-russia-ukraine/. Acesso em: 25 jul. 2026.

IT ARMY OF UKRAINE, Telegram channel, 26 February 2022. Disponível em: https://t.me/itarmyofukraine2022/1 ou https://archive.ph/SMt31 Acesso em: 25 jul.2026.

IT ARMY OF UKRAINE, Telegram channel, 7 May 2022. Disponível em:

Referências

BAJAK, F. Ukraine digital army brews cyberattacks, intel and infowar. Voice of America, Ukraine, 2022. Disponível em: https://web.archive.org/web/20220608141931/https://apnews.com/article/russiaukraine-technology-europe-hacking-f2c4960e48b8022a567780f3602b54e2.Acesso em: 25 jul. 2026.

BIGGERSTAFF, W. C. Ukraine Symposium – photos of the dead. Lieber Institute- West Point, New York, 2022. Disponível em: https://lieber.westpoint.edu/photos-of-dead/ Acesso em: 25 jul. 2023.

BRAUN, S. Ukraine's info warriors battling Russian trolls. DW, Berlin, 2022. Disponível em: https://www.dw.com/en/nafo-ukraines-info-warriors-battlingrussian-trolls/a-63124443. Acesso em: 25 jul. 2026.

BREWSTER, T. Ukraine Starts Using Facial Recognition To Identify Dead Russians And Tell Their Relatives. Forbes, Jersey City, 2022. Disponível em: https://www.forbes.com/sites/thomasbrewster/2022/03/23/ukraine-starts-using-facial-recognition-to-identify-dead-russians-and-tell-their-relatives/?sh=f5b58ac28985 Acesso em: 25 jul. 2026.

CLULEY, G. Ukraine calls for volunteer hackers to protect its critical infrastructure and spy on Russian forces. Bitdefender, [S.l.], 2022. Disponível em: https://web.archive.org/web/20220608141452/https://www.bitdefender.com/blog/hotforsecurity/ukraine-calls-for-volunteer-hackers-to-protect-its-critical-infrastructure-and-spy-on-russian-forces/ . Acesso em: 25 jul. 2023.

CLULEY, G. Ukraine calls for volunteer hackers to protect its critical infrastructure and spy on Russian forces. Bitdefender, [S.l.], 2022. Disponível em: https://web.archive.org/web/20220608141452/https://www.bitdefender.com/blog/hotforsecurity/ukraine-calls-for-volunteer-hackers-to-protect-its-critical-infrastructure-and-spy-on-russian-forces/ . Acesso em: 25 jul. 2026.

FAIFE, C. In Ukraine, Hacktivists fight back with Data Leaks. The Verge, [S.l.], 2022. Disponível em: https://www.theverge.com/2022/3/11/22968049/anonymous-hacks-ukraine-russia-cybercrime-danger.Acesso em: 25 jul. 2026.

GREENBERG, A. The Case for War Crimes Charges Against Russia's Sandworm Hackers. Wired, [S.l.], 2022. Disponível em: https://www.wired.com/story/cyber-warcrimes-sandworm-russia-ukraine/. Acesso em: 25 jul. 2026.

IT ARMY OF UKRAINE, Telegram channel, 26 February 2022. Disponível em: https://t.me/itarmyofukraine2022/1 ou https://archive.ph/SMt31 Acesso em: 25 jul.2026.

IT ARMY OF UKRAINE, Telegram channel, 7 May 2022. Disponível em: https://t.me/itarmyofukraine2022/331 ou https://archive.ph/ Acesso em: 25 jul. 2026.

JANOFSKY, A. This Ukrainian cyber firm is offering hackers bounties for taking down Russian sites. The Record, [S.l.], 2022. Disponível em: https://therecord.media/this-ukrainian-cyber-firm-is-offering-hackers-bounties-for-taking-down-russian-sites. Acesso em: 25 jul. 2026.

JOSHI, S. Battlefield Lessons- Special Report. The Economist, New York, 2023. Disponível em: https://www.economist.com/special-report/2023/07/03/technology-is-deepening-civilian-involvement-in-war Acesso em: 25 jul. 2026.

KMU.gov.ua. Мінцифри бореться з ворогом на цифровому фронті. KMU, San Francisco, 2022. Disponível em: https://web.archive.org/web/20220310141242/ ou https://www.kmu.gov.ua/news/mincifriboretsya-z-vorogom-na-cifrovomu-fronti Acesso em: 25 jul. 2026.

LABOTT, E. We Are the First in the World to Introduce This New Warfare: Ukraine's Digital Battle Against Russia. Politico, [S.l.], 2022. Disponível em: https://www.politico.com/news/magazine/2022/03/08/ukraine-digital-minister-crypto-cyber-social-media-00014880. Acesso em: 25 jul. 2026.

Referências

LONAS, L. Ukraine has used facial recognition tech to notify hundreds of Russian families of dead soldiers: report. The Hill, Washington, 2022. Disponível em: KMU.gov.ua. Мінцифри бореться з ворогом на цифровому фронті. KMU, San Francisco, 2022. Disponível em: https://web.archive.org/web/20220310141242/ ou https://www.kmu.gov.ua/news/mincifriboretsya-z-vorogom-na-cifrovomu-fronti Acesso em: 25 jul. 2026.. Acessso em: 25 jul. 2026.

MELKOZEROVA, V. Russian claims of revenge attack on Ukraine debunked. Politico, [S.l.], 2023. Disponível em: https://www.politico.eu/article/russian-claims-of-revengeattack-on-ukraine-kramatorsk-debunked-war/ Acesso em: 25 jul. 2026.

MINISTRY OF DIGITAL TRANSFORMATION. Telegram Channel, 26 February 2022. Disponível em: https://t.me/mintsyfra/2609 ou https://archive.ph/7UYkx . Acesso em 25 jul. 2026.

ROMANDASH, A. Ukraine's IT Army: Digital Resistance to Russian Propaganda. In: O'Brien, J. Peace Policy: Solutions to Violent Conflict, May 2023. Notre Dame: Kroc Institute for International Peace Studies, 2023. Disponível em: https://doi.org/10.7274/qr46qz24c90. Acesso em: 23 jul. 2026.

SCHECTMAN, J.; BING, C. Exclusive Ukraine calls on hacker underground to defend against Russia. Reuters, [S.l.], 2022. Disponível em: https://web.archive.org/web/20220608141232/https://www.reuters.com/world/exclusive-ukraine-calls-hacker-underground-defendagainst-russia-2022-02-24/. Acesso em: 25 jul. 2026.

SCOTT, M. How Ukraine used Russia's digital playbook against the Kremlin. Politico, [S.l.], 2022. Disponível em: https://www.politico.eu/article/ukraine-russia-digitalplaybook-war/ Acesso em: 25 jul. 2026.

SHORE, J. Don't Underestimate Ukraine's Volunteer Hackers. Foreign Policy, Washington, 2022. Disponível em: https://foreignpolicy.com/2022/04/11/russia-cyberwarfare-us-ukraine-volunteer-hackers-it-army/. Acesso em: 25 jul. 2026.

SIMONITE, T.; VOLPICELLI, G. M. Ukraine's Digital Ministry is a Formidable War Machine. Wired, [S.l.], 2022, Disponível em: KMU.gov.ua. Мінцифри бореться з ворогом на цифровому фронті. KMU, San Francisco, 2022. Disponível em: https://web.archive.org/web/20220310141242/ ou https://www.kmu.gov.ua/news/mincifriboretsya-z-vorogom-na-cifrovomu-fronti Acesso em: 25 jul. 2026..Acesso em: 25 jul. 2026.

SOESANTO, S. The IT Army of Ukraine Structure, Tasking, and Ecosystem. ETH Zürich: Cyberdefense Report Center for Security Studies (CSS), 2022. Disponível em: css.ethz.ch/en/publications/risk-and-resilience-reports.html. Acesso em: 25 jul. 2026.

TGSTAT. IT Army of Ukraine – Subscribers number growth. 2022. Disponível em: https://tgstat.com/channel/@itarmyofukraine2022/stat/subscribers Acesso em: 25 jul. 2026.

THE ECONOMIST. How a chatbot has turned Ukrainian civilians into digital resistance Fighters. The Economist, [S.l.], 2023. Disponível em: KMU.gov.ua. Мінцифри бореться з ворогом на цифровому фронті. KMU, San Francisco, 2022. Disponível em: https://web.archive.org/web/20220310141242/ ou https://www.kmu.gov.ua/news/mincifriboretsya-z-vorogom-na-cifrovomu-fronti Acesso em: 25 jul. 2026..Acesso em: 25 jul. 2026.

THE ODESSA JOURNAL. Ukraine received two awards in the field of cybersecurity at the CYBERSEC European Cybersecurity Forum. Odessa-journal, [S.l.], 2022. Disponível em: https://web.archive.org/web/20220608141159/https://odessa-journal.com/ukraine-received-two-awards-in-the-field-of-cybersecurity-at-thecybersec-european-cybersecurity-forum/. Acesso em: 25 jul. 2026.

WALKER, C. S.; MILMO, D. 'It's the right thing to do': the 300,000 volunteer hackers coming together to fight Russia. The Guardian, New York, 2022. Disponível em: https://web.archive.org/web/20220608145557/https://www.theguardian.com/world/2022/mar/15/volunteer-hackers-fight-russia Acesso em: 25 jul. 2026.

RADAR
INVESTIGATIVO
MINISTÉRIO PÚBLICO MILITAR

TECNOLOGIA INVESTIGATIVA: DO EXTRATO BANCÁRIO ÀS RELAÇÕES QUE IMPORTAM



A integração entre a Suíte Argus e o Plutão ajuda o Ministério Público a organizar informações financeiras, identificar conexões e direcionar diligências — sem transformar cada nome encontrado em um novo suspeito.

ASSESSORIA DE DESENVOLVIMENTO TECNOLÓGICO/SPAI

Um extrato com quatrocentos nomes não contém, necessariamente, quatrocentos suspeitos. Entre quem enviou ou recebeu dinheiro podem estar clientes, fornecedores, locadores e familiares. Em meio a tantas operações, quais merecem ser examinadas com maior atenção?

Essa é uma das dificuldades da investigação financeira: receber os dados não significa compreender o que eles revelam. O extrato informa quem pagou, quem recebeu, quanto e quando. Mas, isoladamente, nem sempre esclarece quem são essas pessoas, como se relacionam com os investigados ou por que movimentaram aqueles recursos.

Durante muito tempo, preencher essas lacunas exigiu uma sequência de consultas. Para cada nome, a equipe precisava procurar informações cadastrais, identificar empresas e sócios, verificar parentesco e localizar vínculos profissionais. Antes de analisar a movimentação, era necessário reunir elementos para entender quem aparecia nela.

A integração entre a Suíte Argus e o Plutão enfrenta essa etapa do trabalho. Ao aproximar informações financeiras e cadastrais, permite que o analista examine os valores ao lado das relações identificadas nas bases consultadas. Para o Promotor de Justiça, o benefício é concreto: receber informações mais organizadas para decidir o que aprofundar, o que confirmar e quais diligências solicitar.

Sistemas diferentes, uma investigação mais conectada

A Suíte Argus reúne ferramentas de apoio à investigação. O Pedido de Apoio à Investigação (PAI) organiza os pedidos de apoio; o Sistema ARGUS trabalha com extratos bancários; o Sistema Bandit, com Relatórios de Inteligência Financeira do Conselho de Controle de Atividades Financeiras, o COAF. O conjunto também inclui o Sistema SITTEL, voltado às requisições telefônicas, e módulos para informações fiscais e de licitações.

O Sistema Plutão complementa esse trabalho ao reunir informações sobre pessoas e empresas. A partir de um CPF ou CNPJ, consulta bases governamentais de acesso restrito, disponibilizadas mediante convênios e utilizadas em função do procedimento que justifica a pesquisa.

Entre as informações reunidas estão dados da Receita Federal, participação em empresas, parentesco, vínculos de trabalho, registros eleitorais, habilitação e veículos. Também podem aparecer registros de óbito, informações sobre militares, processos no Superior Tribunal Militar, registros de condenação e possíveis vínculos com organizações criminosas.

A presença de alguém em um processo, naturalmente, não significa que figure como investigado. Há duas formas de aproveitar essas informações. No PAI, elas ajudam a compor o conjunto de dados sobre o investigado que acompanha o pedido de apoio. No ARGUS e no Bandit, a integração permite relacionar informações cadastrais às pessoas e empresas presentes no material financeiro. São usos diferentes: a consulta feita no pedido não substitui o cruzamento que a equipe precisa executar na análise.

> **O resultado não é uma conclusão pronta,**
> **mas uma base mais organizada para formular perguntas.**

O que os vínculos acrescentam à leitura do dinheiro

Um valor transferido pode ganhar outro significado quando se identifica uma relação entre as pessoas envolvidas. Isso não transforma a operação em irregular, mas acrescenta contexto à investigação.

A ferramenta permite examinar, em conjunto, três aspectos: as relações cadastrais, como parentesco e participação societária; as movimentações financeiras entre as pessoas; e determinadas ocupações profissionais registradas nas bases.

Considere um exemplo hipotético: uma pessoa aparece como parente de um dos investigados e, ao mesmo tempo, movimenta recursos com outro, sem que as bases consultadas apontem relação cadastral entre eles. Esse recorte pode justificar uma pergunta sobre a razão dos pagamentos. Também pode revelar uma situação inteiramente lícita, como prestação de serviços, locação ou outra relação comercial.

O sistema oferece esse tipo de seleção para que a equipe não precise construí-la manualmente. Quando há relação cadastral e movimentação com o mesmo investigado, os valores aparecem associados ao vínculo. Em outro recorte, ficam visíveis as movimentações com investigados para os quais não foi localizada uma relação cadastral.

> **A ausência de vínculo nas bases não significa ausência de vínculo na realidade.**
> **Significa apenas que aquelas fontes não forneceram essa informação.**

A identificação de determinadas ocupações, como cargos no Ministério Público, na magistratura, na administração pública ou nas carreiras militares, também funciona como auxílio à leitura. A indicação de um cargo não é, por si só, vínculo com um investigado nem sinal de irregularidade. Antes de utilizá-la em uma manifestação, é necessário confirmar o cargo e o período de exercício, além de explicar sua pertinência para o objeto da apuração.

Quando o ponto de partida é um relatório do COAF

Nem toda análise financeira começa com extratos bancários. O Relatório de Inteligência Financeira, conhecido como RIF, reúne informações comunicadas ao COAF por instituições obrigadas a fazê-lo. Sua função é orientar a investigação: os apontamentos precisam ser aprofundados por diligências, e não tratados como comprovação automática de um ilícito. Também importa registrar se o relatório foi recebido de ofício ou produzido a partir de um intercâmbio de informações.

O Bandit recebe o material diretamente do sistema de pedidos, dispensando uma nova inclusão manual do arquivo. As informações passam a ser consultadas de forma organizada, por comunicações, instituições financeiras, agências, titulares, ocorrências e valores.
Há ainda um indicador que compara o valor total comunicado com o valor que o sistema conseguiu identificar no texto das comunicações. Embora a ferramenta use a expressão “total rastreado”, o número não significa que o destino de todo aquele dinheiro tenha sido esclarecido. Ele mostra quanto do valor comunicado foi identificado em lançamentos extraídos do texto.
Essa distinção evita que um indicador de organização dos dados seja apresentado como resultado de uma investigação já concluída.

O que precisa ser confirmado antes de entrar na peça

A utilidade da tecnologia depende de uma distinção permanente entre informação encontrada, hipótese investigativa e fato comprovado.

Um parentesco indicado pelo sistema, por exemplo, pode resultar de cruzamentos entre cadastros, e não da consulta direta a uma certidão. A identificação da base informa onde buscar confirmação, mas não substitui o documento de origem. Quando a ferramenta apresentar uma relação como “possível”, essa ressalva deve ser preservada: o sistema não fornece um grau de certeza que autorize suprimi-la.

O mesmo cuidado vale para registros de condenação. Antes de citá-los, é preciso conhecer a fonte, a data e a situação do trânsito em julgado. O simples aparecimento de uma informação cadastral não autoriza tratá-la como condenação definitiva.

Aparecer no extrato de um investigado também não transforma alguém em alvo da apuração. As consultas sobre terceiros devem se limitar ao necessário para identificá-los e compreender sua relação com o objeto investigado, sempre vinculadas ao procedimento que as justifica.

Há limitações relevantes na leitura dos números. Em contas conjuntas, uma operação pode ser considerada no somatório de mais de um titular, exigindo conferência para evitar a superestimação dos valores. Pessoas identificadas apenas pelo nome, sem CPF ou CNPJ válido, não passam pelo mesmo cruzamento. O relatório deve informar quantas ficaram de fora; eventual identificação por nome exige outro dado de confirmação, diante do risco de homônimos.

A expressão “movimentação atípica” também exige explicação. Na consulta descrita, a seleção considera os cem maiores valores distintos, incluindo todas as operações que alcancem esse limite. Por isso, o resultado pode conter mais de cem lançamentos. Trata-se de uma regra de seleção, não de um reconhecimento automático de operações ilícitas.

Da mesma forma, a ferramenta não conclui sozinha que valores foram divididos em operações menores para disfarçar uma movimentação, nem identifica automaticamente trajetos circulares do dinheiro. Ela organiza operações e relações que podem ajudar nessa investigação. Reconhecer e demonstrar esses padrões continua sendo tarefa de análise.

Até a apresentação exige atenção: os diagramas de relações podem incluir pessoas que não aparecem no recorte de determinada tela ou planilha. Antes de comparar os resultados, é necessário verificar se representam o mesmo conjunto de informações.

A origem e o histórico da informação também importam

Para utilizar um resultado com segurança, não basta saber o que foi encontrado. É preciso conhecer a fonte, o momento da consulta e as condições em que a análise foi realizada.

O sistema mantém registros das consultas por CPF ou CNPJ, com data, horário, resultado e eventuais erros. O processamento só é marcado como concluído quando não restam documentos com erro. O acesso aos pedidos também é controlado pela distribuição formal e pelo histórico das autorizações.

Esses mecanismos ajudam a acompanhar o trabalho, mas não dispensam uma conferência no fechamento do relatório. Como a equipe pode visualizar resultados antes do término do processamento, o documento deve informar se todas as consultas foram concluídas e se ainda havia falhas naquele momento.

Há outra distinção importante: uma consulta pode ser executada corretamente e não encontrar informação. “Nada localizado” não equivale a “relação inexistente”. O resultado precisa ser descrito nos limites do que efetivamente foi pesquisado.

Mais tempo para compreender, não apenas para reunir

A integração entre a Suíte Argus e o Plutão reduz o trabalho repetitivo de consultar, identificar e reunir informações dispersas. Isso permite concentrar o esforço na etapa em que a atuação humana é indispensável: compreender as relações, verificar explicações e decidir os próximos passos.

Para a gestão, a suíte também permite acompanhar o tempo dos pedidos em cada etapa, do protocolo à distribuição, da análise à revisão, e identificar os que ultrapassam a média de sua fila. Assim, a pergunta “onde está o meu pedido?” pode ser respondida com informações sobre o andamento do trabalho.

Nenhum desses recursos substitui o discernimento do analista ou a responsabilidade do Promotor de Justiça. A ferramenta pode apontar uma relação, mas não explicar, por si só, o motivo de um pagamento. Pode organizar uma movimentação, mas não concluir automaticamente por sua ilicitude.

O avanço está em permitir que a investigação comece sua análise com mais contexto e menos trabalho manual. Ao final, aquelas quatrocentas pessoas continuam sendo quatrocentas pessoas — não quatrocentos suspeitos. A diferença é que suas movimentações podem ser examinadas ao lado das relações encontradas, com indicação da origem das informações e clareza sobre o que ainda precisa ser apurado.

RADAR
INVESTIGATIVO
MINISTÉRIO PÚBLICO MILITAR

MÉTODO EM PRÁTICA

A arte de receber e interpretar dados sigilosos

MATEUS DE FREITAS RODRIGUES

Bacharel em Direito e Contabilidade.
Chefe da Seção de Tratamento de Dados Sigilosos/SPAI

Introdução

Imagine montar um quebra-cabeça com as mãos atadas, no escuro, enquanto várias pessoas gritam instruções diferentes. Para quem trabalha com a recepção e validação de dados sigilosos (bancários, telefônicos e fiscais), essa sensação não é tão distante da realidade.

A atividade, em tese, parece direta: pedir, receber e analisar informações. Na prática, desdobra-se em cenário repleto de variáveis, atores e reguladores distintos - o Banco Central (Bacen), a Anatel e a Receita Federal, cada um com suas regras, sistemas e particularidades. O desafio central é diferenciar o que é simples do que é complexo, endereçar o que é complicado e evitar que tudo descambe para o caos.

Cenários de trabalho: simples, complicado, complexo e caótico

Para navegar nesse universo, vale recorrer à tipologia do professor Silvio Meira, que propõe enxergar os cenários em quatro categorias (MEIRA, [s.d.]): simples, complicado, complexo e caótico.

O simples é a tarefa já dominada: seguir uma receita conhecida, com resultado previsível. No dia a dia, é o preenchimento correto de um formulário eletrônico de requisição ou o envio de um ofício padronizado.

O complicado exige mais esforço, mas é resolvível com conhecimento técnico. É interpretar uma decisão judicial com requisitos específicos de afastamento de sigilo ou cruzar informações de diferentes instituições financeiras para identificar movimentações de um mesmo investigado.

O complexo deixa de ser previsível. Não existe receita pronta. Surge quando a base de dados do Bacen está desatualizada, quando os vínculos entre contas e clientes não conferem ou quando uma instituição entrega informações incompletas. A resposta vem da experiência acumulada, da especialização da equipe e da capacidade de improvisar soluções sem perder o rigor.

O caótico é o colapso. Instala-se quando há desencontro total entre os atores: pedido incompleto, decisão judicial genérica, falhas cadastrais no Bacen e instituições financeiras atrasando ou entregando dados inúteis. Não adianta seguir protocolo rígido: é preciso agir, estabilizar e reorganizar.

A maioria das atividades oscila entre o simples e o complexo. O problema começa quando se confunde um com o outro - ou quando a complicação se torna caos por falta de coordenação.

Os atores do processo: uma cadeia de responsabilidades

O sucesso na validação de dados sigilosos não depende apenas de quem analisa as planilhas no final da linha. É construção coletiva, em que cada laço influencia diretamente a qualidade e a celeridade do resultado.

Os demandantes internos

Tudo começa com quem formula o pedido. A clareza da requisição é determinante. Um pedido bem feito descreve os fatos com precisão, especifica os alvos, detalha o período de interesse, aponta a tese investigativa e anexa apenas os documentos necessários - não todos os documentos do processo. Lembre-se: quando tudo é importante, nada é importante. Sobrecarregar a análise com informações irrelevantes só atrasa o trabalho. Além disso, o pedido precisa estar em sintonia com a minuta de requerimento, documento técnico que baliza tempo, modo e objeto do afastamento de sigilo.

As autoridades judiciais e suas secretarias

Fora do Ministério Público, juízes e auxiliares da justiça têm papel fundamental. Uma decisão mal redigida (com nomes errados, CPFs incompletos ou alvos mal identificados) gera efeito cascata: o sistema do Bacen não localiza a pessoa, as instituições não sabem o que entregar e a resposta demora semanas. A observância rigorosa das orientações da minuta e o impulso processual pelo SISBAJUD são fatores que aceleram ou travam o procedimento.

Os reguladores: Bacen, Anatel e Receita Federal

Cada regulador opera como porteiro de um prédio diferente. O Bacen articula as ordens de quebra de sigilo bancário. A integração tecnológica mitigou gargalos, mas persiste problema estrutural: a base cadastral nem sempre está atualizada. Em um mundo ideal, as instituições financeiras alimentariam o cadastro tempestivamente e os vínculos seriam precisos. Na realidade, isso não ocorre. Isso nos obriga a desenvolver ferramentas próprias para detectar e corrigir inconsistências - o que chamamos de "quarentena".

A Anatel regula dados telefônicos; a Receita Federal, os fiscais. Cada ambiente tem suas regras, sistemas e prazos. Trabalhar com os três simultaneamente exige conhecimento técnico e capacidade de transitar entre lógicas diferentes.

As instituições financeiras e prestadoras de serviço

Bancos, instituições de pagamento, corretoras, distribuidoras e operadoras de telefonia entregam a matéria-prima do trabalho: os dados. O gargalo está na tempestividade (quando entregam) e na qualidade (o que entregam). Dados desorganizados, incompletos ou em formatos incompatíveis exigem esforço extra enorme para serem tratados.

A equipe da SPAI

Somos a última trincheira, mas também a primeira a sentir quando algo saiu errado lá atrás. Nossa atuação no monitoramento das entregas, na aferição da qualidade dos dados e na produção do relatório final transforma uma pilha de números em provas robustas que sustentam a tese acusatória. Investimos continuamente em ferramentas de validação, em tecnologia da informação desenvolvida internamente e na especialização das equipes.

A SINERGIA COMO FATOR CRÍTICO DE SUCESSO

Se há uma lição que décadas de trabalho ensinaram, é esta: ninguém faz esse trabalho sozinho. A qualidade do relatório final depende da qualidade do pedido inicial, da precisão da decisão judicial, da eficiência dos reguladores e da cooperação das instituições que detêm os dados.

Quando há sinergia entre todos os atores, o resultado é um relatório entregue com rapidez, sem perda de qualidade. Quando falta coordenação, o processo se arrasta, os prazos se esticam e a investigação perde fôlego.

Não existe fórmula mágica para eliminar todos os problemas. A realidade é complexa e desafia respostas prontas. O que se pode fazer é fixar uma organização mínima, atuar de forma preventiva e analítica, e apostar na experiência colhida, na especialização das equipes e na tecnologia como aliada.

Receber e interpretar dados sigilosos não é apenas tarefa técnica. É prática que exige discernimento, paciência e a certeza de que cada peça do quebra-cabeça só se encaixa quando todos que a seguram estão olhando para a mesma imagem.

REFERÊNCIAS

MEIRA, Silvio. Complexo não é complicado: como gerenciar a complexidade*. Escola de Formação e Aperfeiçoamento de Magistrados do Tribunal de Justiça do Distrito Federal e dos Territórios (TJDFT). Disponível em: https://escola.tjdft.jus.br/novo/SI267/. Acesso em: 29 ago. 2026.



CASO EM PERSPECTIVA

2ª Procuradoria de Justiça Militar em Brasília/DF
Cícero Robson Coimbra Neves - Promotor de Justiça Militar
Maria Fernanda de Melo Santos Tavares - Analista
Wesley Batista de Oliveira - Analista

O problema investigativo

Possível conluio entre empresas em pregão licitatório de Organização Militar da Guarnição de Brasília/DF, com o objetivo de fraudar o pregão a partir da simulação de uma concorrência.

A hipótese inicial

Partiu-se da hipótese de que as empresas atuaram para simular uma concorrência que, na verdade, não existiu, já que elas possuíam inúmeros elementos em comum, como mesmo quadro societário, mesmos endereços, telefones e e-mails.

O pedido de apoio formulado

O pedido de apoio à Secretaria de Pesquisa e Apoio à Investigação (SPAI) iniciou-se com o pedido de pesquisa de vínculos entre as empresas. Muito embora uma matéria jornalística tenha afirmado que as empresas possuíam mesmo quadro societário, era necessário haver uma confirmação desse fato, por isso, essa pesquisa da SPAI foi importante para definir os rumos investigatórios.

Por meio desse relatório da SPAI, foi possível confirmar que as empresas possuíam diversos dados em comum, inclusive, mesmo quadro societário, fato que levou o Ministério Público Militar (MPM) a entender que se tratava de um mesmo grupo empresarial.

Posteriormente, formulou-se ao Juízo pedido de afastamento de sigilo bancário, telefônico e fiscal dos envolvidos e, após deferido pelo Juízo, a SPAI se encarregou de analisar e confeccionar relatório sobre esses dados.



CASO EM PERSPECTIVA

As fontes utilizadas

As fontes iniciais embasaram-se em uma suposta ligação entre as empresas participantes da licitação, cuja informação se deu por meio de matéria jornalística, autuada em Notícia de Fato que procedeu a investigação preliminar de vínculos. Posteriormente, após requisição do Inquérito Policial Militar (IPM), meio mais adequado para investigação com mais acurácia, essas fontes embasaram um pedido inicial e mais detalhado sobre possíveis vinculações entre as empresas investigadas e seus sócios. A partir dessas fontes, que se mostraram positivas, enveredou-se para diligências mais aprofundadas, como afastamento de sigilos.

Como os dados foram organizados

Partindo-se do fato de que as empresas envolvidas tinham elementos de ligação entre si, os dados obtidos com os relatórios fornecidos pela SPAI foram organizados de forma a confirmar essa ligação.

Os achados relevantes

Encontrou-se dados que comprovaram que as empresas envolvidas na investigação atuaram com o propósito de simular que se tratavam de empresas diferentes, quando na verdade, se tratavam do mesmo grupo. Ademais, quando se fala na atuação dessas empresas, não nos referimos apenas à atuação no pregão, referimo-nos também a todos os atos burocráticos executados pelas empresas, anteriormente ao pregão licitatório, para simularem serem diferentes empresas. Isso envolveu, por exemplo, a apresentação de Atestados de Capacidade Técnica falsos, já que foram emitidos pelos próprios membros da empresa, inúmeras mudanças no contrato social das empresas, havendo uma rotatividade no quadro societário, a fim de se colocar sócios “laranja” como sócio principal, mudanças de endereço, de telefone, de e-mail, etc.



CASO EM PERSPECTIVA

Outrossim, os relatórios de afastamento de sigilos também permitiram constatar vínculo entre as empresas investigadas e outras empresas participantes do pregão, de modo que se pôde proceder à oitiva do representante da empresa, e trazer maiores esclarecimentos sobre os fatos.

Ademais, os relatórios de afastamento de sigilos também constataram que os investigados mantiveram vínculos financeiros com alguns militares da Organização Militar, fato que, em um primeiro momento, levantou a suspeita do MPM, o qual requisitou a instauração de IPM, fatos que foram apurados e, posteriormente arquivados.

Como ocorreu a validação humana

Os dados obtidos com o relatório de vínculos feito pela SPAI nortearam a investigação, já que tudo indicava que os investigados atuaram anteriormente ao pregão, para tornar as empresas aptas a participarem da licitação, mas com característica aparentes de empresas diferentes.

Com isso, o MPM conseguiu pautar a investigação pela possível ocorrência do crime de frustração do caráter competitivo do certame (art. 337-F do CP comum) além de enxergar a constituição de organização criminosa, nos termos da Lei n. 12.850/2013.

Com essas informações de vinculação entre os membros das empresas investigadas, requereu-se o afastamento de sigilo de dados telefônicos, telemáticos, bancários e fiscais.

Após a SPAI analisar os dados obtidos com o afastamento dos sigilos telefônico, bancário e fiscal (os dados telemáticos não são analisados pela SPAI) e emitir seus respectivos relatórios, foi possível confirmar as vinculações entre os membros das empresas investigadas.



CASO EM PERSPECTIVA

As informações contidas nesses relatórios de afastamento de sigilo, por sua vez, foram cruzados e analisados com os dados obtidos pela perícia telemática feita pela Seção de Segurança da Informação – Organização Militar Telemática de Área da Guarnição de Brasília/DF. A perícia telemática também trouxe dados relevantes para a investigação e, juntamente com os relatórios efetuados pela SPAI, com a prova testemunhal colhida e mesmo com as declarações dos investigados, foi possível nortear o MPM para a existência do crime e posterior denúncia

O que a tecnologia não permitia concluir

Como explicado no item anterior, a tecnologia, mesmo a inteligência artificial, foi essencial no sentido de compilar dados, informações e elementos de cognição, contudo, não seria possível chegar ao panorama em que se chegou, resultando em uma denúncia criminal, sem uma análise e cruzamento de dados feito por uma consciência humana.

A inteligência humana, por meio de inferências, insights, percepção, conhecimento do modus operandi dos investigados, pôde cotejar as informações contidas nos relatórios e depoimentos e confirmar a hipótese inicial.

Resultado ou encaminhamento produzido

Resultou-se no início de uma ação penal, após oferecimento da denúncia pelo MPM - pelos mencionados delitos de frustração do caráter competitivo do certame (art. 337-F do CP comum) e de organização criminosa - contra sete pretensos autores. A denúncia foi embasada nos dados obtidos por meio dos relatórios da SPAI, das oitivas e perícia telemática, inclusive com a reprodução de tabelas extraídas dos relatórios. Esses dados foram organizados por meio da cognição humana, que pôde, por meio deles, delinear um modus operandi, como os fatos ocorreram, como se deu a atuação de cada investigado, o liame de ligação entre eles e as consequências para o erário.



CASO EM PERSPECTIVA

Lições aplicáveis a outros casos

Uma das lições apreendidas por meio dessa investigação e que pode servir como parâmetro para outras é sempre, antes de formular qualquer pedido, compreender aonde se quer chegar com a investigação, o que se está buscando e quais são as informações iniciais relevantes que se pode requerer para começar a alcançar esse fim. É claro que, inicialmente, muitas vezes tudo o que se tem são informações e dados esparsos e soltos, de modo a ser difícil traçar uma linha investigativa. Contudo, sempre há elementos mínimos aptos a nortearem o entendimento inicial,

Traçar esse caminho inicial, evita a requisição de diligências infrutíferas ou inoportunas, que atrasarão o curso da investigação e a obtenção de provas. Nesse sentido, outra lição que se apreende, refere-se justamente à questão da otimização da investigação, já que, no caso da Organização Militar, foram instaurados diversos IPMs com o objetivo de investigar fraudes licitatórias. Nesse caso, a organização administrativa feita pelos Membros e Analistas atuantes, no sentido de compreender aonde se quer chegar com cada IPM e os dados em comum entre eles otimiza a investigação, no sentido de evitar a requisição de diligências iguais ou que trarão o mesmo resultado. No que concerne à SPAI, também é importante a ingerência do setor, seja por meio de inteligência humana ou artificial, no sentido de se informar sobre diligências cujos dados resultarão em informações em comum ou semelhantes.



RADAR DO SEMESTRE

Um semestre de entregas, cooperação e novos recursos.

> **Soluções já em produção, ferramentas em homologação e projetos em desenvolvimento ampliaram o apoio tecnológico à atividade ministerial.**

O semestre registrou avanços em análise financeira, inteligência artificial, pesquisa cadastral, licitações, dados telefônicos e na disponibilidade dos próprios sistemas.

As iniciativas do semestre alcançaram diferentes etapas do apoio à investigação, da entrada do pedido até a produção do relatório técnico, passando pela pesquisa documental e pelo cruzamento de dados financeiros, cadastrais e telefônicos. Cada uma está em um estágio próprio de maturidade, mas todas caminham na mesma direção: menos tarefas repetitivas e resultados mais organizados e rastreáveis para os membros do Ministério Público, que passam a localizar com mais facilidade a informação de que precisam.

Um ponto interessa especialmente a quem lida com dados sob sigilo: toda a inteligência artificial empregada nessas ferramentas roda inteiramente dentro da infraestrutura do próprio Ministério Público, sem que documentos ou dados de investigação trafeguem para fora dela.

BANDIT ENTRA EM PRODUÇÃO

Um dos principais marcos do período foi a entrada do Bandit em produção no primeiro semestre de 2026. A plataforma aplica inteligência artificial aos grandes volumes de texto livre das Informações Adicionais dos Relatórios de Inteligência Financeira (RIF) e os converte em dados estruturados, calculados e conferíveis.

O sistema reconhece pessoas, documentos, instituições, valores, datas, operações e vínculos; agrupa e calcula; monta a linha do tempo do caso; acompanha a circulação dos recursos. Cada informação extraída permanece ligada ao trecho original de onde saiu, o que permite conferir tudo na fonte. A funcionalidade **Meus Achados** auxilia na seleção dos elementos que poderão compor o relatório de análise. A matéria **Fronteira da Investigação**, nesta edição, mostra em detalhe como essa transformação acontece.

Da integração do Bandit com o Plutão, sistema de pesquisa cadastral e de vínculos, nasceu o **Bandit Plutônico**: a funcionalidade cruza os nomes identificados nos RIFs com as relações já conhecidas entre pessoas e empresas, aproximando a pesquisa de vínculos da análise financeira sem que o analista precise alternar entre sistemas e perder o contexto do caso.

RELATÓRIO AUTOMÁTICO DE PENSÃO

Entre as novas ferramentas desenvolvidas no período está o **Relatório Automático de Pensão**, voltado aos casos de fraude em pensão. O sistema reúne os dados financeiros de importância para o caso e os entrega em um relatório pronto, eliminando a necessidade de uma fase de análise e acelerando o andamento do processo.

A novidade muda a rotina em favor do membro: ele próprio poderá gerar o relatório automático e, somente se o resultado não solucionar a questão, solicitar uma análise específica. Com essa triagem feita na origem, a fila de demandas na SPAI diminui e os analistas ficam disponíveis para os casos que exigem aprofundamento.

ASSISTÊNCIA AO USUÁRIO E DISPONIBILIDADE

O **Synapse**, assistente virtual, avançou nas etapas iniciais do projeto: levantamento de requisitos, definição dos casos de uso e organização da documentação técnica e funcional. A primeira versão deverá responder dúvidas dos usuários e orientar o uso das ferramentas; também servirá de porta de acesso ao conhecimento institucional.

Já no **Passaporte** foi concluído o desenvolvimento de um módulo para monitorar o desempenho dos servidores que hospedam as aplicações da SPAI. O recurso foi concebido para identificar falhas, lentidão e sobrecarga antes que se transformem em interrupção dos serviços.

PLUTÃO AMPLIA AS FONTES DE PESQUISA

> **O Plutão recebeu melhorias internas que tornaram mais rápidas as consultas cadastrais.**

Outra novidade veio de um acordo de cooperação com o Ministério Público de Mato Grosso do Sul (MPMS). Concluída a integração técnica entre o Plutão e o Prometheus, base de registros relacionados a facções criminosas, tornou-se possível verificar se investigados ou outras pessoas ligadas ao caso possuem registros de possível vínculo com essas organizações. Essa informação pede cautela na leitura: sozinha, não comprova pertencimento a organização criminosa e deve ser avaliada em conjunto com os demais elementos da investigação.

No **Plutão Mobile**, a consulta estará disponível a partir da versão **[PREENCHER VERSÃO]**. Para usar o recurso no aplicativo, será necessário atualizá-lo por meio do **[PREENCHER LINK]**.

INTELIGÊNCIA ARTIFICIAL APLICADA A DOCUMENTOS

O **Vertex**, em fase final de homologação (a etapa de testes que antecede a liberação para uso), nasceu para um problema que quem já trabalhou com autos volumosos conhece bem: encontrar informação em grandes conjuntos de documentos. A ferramenta extrai o conteúdo de arquivos PDF, inclusive digitalizados, e oferece pesquisa por significado, capaz de localizar trechos relacionados ao tema buscado mesmo quando as palavras não coincidem exatamente com as do texto.

Um assistente de inteligência artificial permite formular perguntas sobre o material analisado e direciona o usuário aos trechos relacionados. As respostas precisam ser conferidas nos documentos de origem, mas podem reduzir consideravelmente o tempo dedicado à localização inicial das informações.

No **Pedido de Apoio à Investigação** (PAI), porta de entrada dos pedidos de apoio à investigação, avançaram o desenvolvimento dos resumos automáticos de documentos, um novo serviço bancário voltado ao módulo de Pensão e um fluxo mais organizado para o cadastro de investigados.



PESQUISA EM LICITAÇÕES E DADOS TELEFÔNICOS

O **Pegasus**, sistema de pesquisa de licitações públicas, foi implantado em ambiente de produção e já está à disposição dos analistas, permitindo consultas integradas sobre licitações, itens e participantes. A base reúne dados relacionados às Leis nº 8.666/1993 e nº 14.133/2021, que passaram por coleta, tratamento, padronização e enriquecimento — a complementação dos registros com informações de outras fontes — e foi ampliada com os dados de empenhos das licitações. O sistema ganhou ainda uma funcionalidade de exportação de dados para análise, individual ou em lote, que padroniza os relatórios e agiliza sua entrega.

No **Sittel**, está em desenvolvimento um modelo automatizado de relatório para a análise de dados telefônicos. A ideia é padronizar a apresentação dos resultados e agilizar as respostas aos pedidos judiciais, sempre com revisão técnica antes da conclusão do trabalho.

PIX PREPARAÇÃO PARA O NOVO SIMBA

O semestre marcou ainda o início da preparação da nova geração do Simba — o chamado **Novo Simba** — para a Instrução Normativa BCB nº 636/2025, que entra em vigor em 1º de dezembro de 2026. O novo padrão ampliará o detalhamento das transações, do Pix, dos investimentos e do contexto em que as operações acontecem. As principais mudanças, e o que elas podem significar para a investigação financeira, estão na matéria Fronteira da Investigação.

No fechamento do período, ficam soluções novas em uso, ferramentas em homologação e esse prazo no calendário. O objetivo de todas as frentes permanece o mesmo: poupar o tempo de quem investiga, sem tirar das pessoas a interpretação dos fatos e a decisão fundamentada.

Fonte normativa sobre o Novo Simba: [Instrução Normativa BCB nº 636/2025] (https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?numero=636&tipo=Instru%C3%A7%C3%A3o+Normativa+BCB), do Banco Central do Brasil.



FRONTEIRA DA INVESTIGAÇÃO

DA INFORMAÇÃO DISPERSA À INTELIGÊNCIA ESTRUTURADA

O Bandit já converte os longos relatos das Informações Adicionais dos **RIFs** em dados organizados, calculados e verificáveis - com inteligência artificial executada localmente, sem que nenhuma informação saia da instituição. O **Novo Simba**, por sua vez, prepara uma ampliação sem precedentes do detalhamento bancário. São duas frentes distintas com um mesmo efeito: menos tempo copiando e tabulando, mais tempo interpretando os fatos.

Uma investigação financeira pode começar com uma pergunta aparentemente simples: para onde foi o dinheiro? Difícil é responder. A resposta costuma estar espalhada por milhares de transações, diferentes instituições, pessoas, contas e documentos — e, com frequência, o dado decisivo se esconde em um campo de texto livre que alguém precisa ler, copiar, classificar e relacionar à mão antes que qualquer padrão apareça.

Duas iniciativas começam a mudar a escala desse trabalho. O **Bandit**, que entrou em produção no primeiro semestre de 2026, transforma o texto não estruturado dos Relatórios de Inteligência Financeira (RIFs) em dados pesquisáveis e calculáveis. O **Novo Simba**, em preparação, receberá das instituições financeiras informações em maior quantidade e detalhamento do que o padrão atual prevê.

O DESAFIO DAS INFORMAÇÕES ADICIONAIS DOS RIFS

O campo de Informações Adicionais dos RIFs reúne relatos extensos sobre movimentações, pessoas, empresas, contas, instituições, datas e circunstâncias consideradas relevantes. É material valioso, mas chega, em sua maior parte, como texto corrido, sem estrutura.

Em todo o Brasil, o tratamento dessas informações ainda é, em grande medida, artesanal. O analista lê cada comunicação, identifica o que importa, copia trechos para planilhas, cria colunas e classificações, faz cálculos e tenta relacionar pessoas, valores e eventos. Em um caso com muitos RIFs e centenas de comunicados, essa preparação pode consumir boa parte do tempo que deveria estar reservado à análise propriamente dita.

O método também abre margem a falhas: uma mesma pessoa pode aparecer com grafias diferentes; um valor, estar espalhado por vários parágrafos; um mesmo fato, ser descrito em comunicações distintas; e um vínculo importante pode passar despercebido na primeira leitura. Como cada analista organiza o material à sua maneira, revisar o trabalho de um colega também se torna mais difícil.

BANDIT: INTELIGÊNCIA ARTIFICIAL COM CONFERÊNCIA NA FONTE

O **Bandit** foi construído para transformar esse texto em uma base estruturada de análise. Com **apoio de inteligência artificial, o sistema identifica pessoas, documentos, instituições financeiras, valores, datas, operações e outros elementos presentes nas Informações Adicionais. A partir daí, o material passa a ser agrupado, filtrado, comparado e utilizado em cálculos e consolidações.**

E há um aspecto que interessa diretamente a quem responde pelo sigilo dos autos: todo processamento acontece localmente, em servidores da própria instituição. O conteúdo dos RIFs não é enviado a serviços externos de inteligência artificial; os dados permanecem, do início ao fim, no ambiente protegido em que já se encontram.

O ganho vai além da velocidade. Como todos os comunicados passam pelo mesmo processo de estruturação, o conjunto pode ser examinado por ângulos que a leitura sequencial não alcança: quais pessoas aparecem juntas, quais valores se repetem, quais instituições estão envolvidas, como os fatos se distribuem no tempo.

Nada disso dispensa a conferência humana. Marcadores indicam o trecho original em que a inteligência artificial identificou cada informação; o analista pode verificar o contexto e confirmar, corrigir ou descartar resultados. O que não foi revisado fica em quarentena, fora da base definida, mecanismo pensado para evitar que uma interpretação automatizada seja tratada como dado confirmado sem a devida verificação humana.

O CASO VISTO POR INTEIRO

Estruturados os dados, há vários caminhos para explorá-los. O agrupamento inteligente aproxima comunicados relacionados entre si. A linha do tempo ordena os acontecimentos. O rastreio de valores mostra entradas, saídas e a circulação dos recursos, enquanto o painel consolidado reúne as movimentações tratadas pelo sistema e permite exportá-las para análises complementares.

Há ainda a funcionalidade **Meus Achados**, em que o profissional vai guardando, ao longo do caso, as informações que considera relevantes para o futuro relatório, sempre com a referência ao conteúdo de origem. Em vez de reconstruir o raciocínio no fim da análise, ele o registra à medida que avança.

Da integração com o **Plutão** nasceu o **Bandit Plutônico**, que acrescenta a pesquisa de vínculos cadastrais: um nome identificado em uma comunicação financeira pode ser confrontado com as relações já conhecidas entre pessoas e empresas, ampliando o contexto para a formulação de hipóteses investigativas.

Antes de chegar aos usuários, o **Bandit** foi validado em casos reais.

NOVO SIMBA: UM RETRATO FINANCEIRO MAIS DETALHADO

Se o **Bandit** atua sobre o texto dos **RIFs**, o **Novo Simba** prepara o terreno para outra transformação, a dos próprios dados bancários. A origem da mudança é a Instrução **Normativa BCB nº 636/2025, que entra em vigor em 1º de dezembro de 2026, e revoga a Carta-Circular nº 3.454/2010, padrão em uso há mais de quinze anos.**

O modelo atual se organiza em cinco conjuntos de arquivos: agências, contas, titulares, extratos e origem-destino. O novo padrão mantém esses grupos para as instituições bancárias, amplia o detalhamento dos campos e cria seis conjuntos específicos para corretoras e distribuidoras de títulos e valores mobiliários — que, em contrapartida, ficam dispensadas dos cinco conjuntos bancários.

Esses novos arquivos trarão dados cadastrais dos investidores, extratos e movimentos diários das contas de registro, posições de investimento no início e no fim do período analisado, resumos de negócios e ativos negociados. O afastamento de sigilo poderá, assim, oferecer uma visão mais abrangente das operações nos mercados à vista e a termo, derivativos, empréstimos, opções e outros ativos sob responsabilidade de corretoras e distribuidoras.

ONDE, QUANDO E POR QUAL CANAL

Para a investigação, uma das novidades mais interessantes está no contexto de cada transação. O novo leiaute permite distinguir o canal utilizado: agência física, correspondente bancário, terminal de autoatendimento, internet banking, aplicativo móvel, empresa transportadora de valores, casa lotérica ou estabelecimento comercial, caso das modalidades Pix Saque e Pix Troco.

Há também campos próprios para o município e a unidade da Federação. Nas operações digitais, eles podem indicar a localização aproximada do aparelho a partir do qual a transação foi comandada, e registros complementares podem esclarecer se o lançamento ocorreu em caixa de agência, terminal eletrônico, loja, lotérica ou banco postal. Quando disponíveis, serão informados ainda o endereço IP, a porta de conexão, a identificação do dispositivo e o horário da operação. São elementos que podem ser cotejados com locais, horários e padrões registrados em outras evidências do caso.

Convém conhecer os limites desses dados: eles não equivalem, necessariamente, a coordenadas exatas de GPS e não comprovam, isoladamente, quem realizou a operação. Seu valor nasce do confronto com documentos, depoimentos, vínculos, movimentações relacionadas e as demais evidências já reunidas nos autos.

PIX, INVESTIMENTOS E ORIGEM DOS RECURSOS

O PIX passa a receber tratamento estruturado. O novo padrão registra o tipo e o conteúdo da chave, o identificador único da transação e os comentários ou anotações que o usuário insere ao fazer a operação. O detalhamento do remetente ou beneficiário também aumenta, com ligação aos registros de origem e destino.

Os códigos de lançamento ficam mais específicos e passam a diferenciar modalidades de PIX, depósitos e saques em diferentes canais, transferências entre instituições, operações com **investimentos, estornos, recebíveis, boletos e movimentações em espécie. Quanto menos descrições genéricas, mais fácil reconstruir o percurso dos recursos e reconhecer operações relacionadas.**

Nesse terreno, o MPM oferece uma vantagem concreta: fornece hoje o Simba/Argus em SQL Server, o que dispensa a aquisição de licença Oracle — um investimento da ordem de R$ 1 milhão. A solução é utilizada pela Controladoria-Geral da União (CGU), pelo MPPB e pela Comissão de Valores Mobiliários (CVM); o MPMG e o MPGO estão em fase de transição para a implantação.

MAIS DADOS NÃO SIGNIFICAM CONCLUSÕES AUTOMÁTICAS

A responsabilidade pela conclusão investigativa, porém, não muda de lugar. A inteligência artificial pode identificar, estruturar e relacionar informações, os novos campos bancários podem fornecer contexto, e os sistemas podem calcular valores e revelar padrões — mas cada achado precisa ser examinado à luz do caso concreto.

O que essas ferramentas oferecem é tempo e campo de visão. Reduzida a preparação mecânica dos dados, o analista pode dedicar atenção à origem dos recursos, à coerência dos vínculos, às hipóteses alternativas e à qualidade das evidências.

É essa a fronteira que se desloca. O resultado que se desenha é uma investigação financeira rápida e abrangente, que preserva a rastreabilidade, a segurança e a indispensável análise humana.

RADAR
INVESTIGATIVO
MINISTÉRIO PÚBLICO MILITAR



MEMÓRIA

SECRETARIA DE PESQUISA E APOIO À INVESTIGAÇÃO SPAI

ÂNGELA MONTENEGRO TAVEIRA
Procuradora de Justiça Militar

LINHA DO TEMPO 2020 - 2025

SPAI

2020	2021	2022	2023	2024	2025
COORDENAÇÃO DO CPADSI	NASCIMENTO DA SPAI	EXPANSÃO INSTITUCIONAL	NOVAS FERRAMENTAS	CAPACITAÇÃO E AUTOMAÇÃO	ANÁLISE TELEMÁTICA E ENCCLA

MEMÓRIA

SECRETARIA DE PESQUISA E APOIO À INVESTIGAÇÃO

Memórias da Secretaria-Geral da SPAI

Passaram-se pouco mais de seis anos desde que fui convidada a assumir, em abril de 2020, a coordenação do então Centro de Pesquisa e Apoio à Investigação (CPADSI), unidade vinculada diretamente ao Procurador-Geral de Justiça Militar. Desde aquele momento, formou-se em mim uma convicção que permanece inalterada: trata-se da mais importante estrutura de apoio à atividade investigativa do Ministério Público Militar, especialmente em um cenário no qual o poder investigatório do Ministério Público foi definitivamente reconhecido e consolidado pelo Supremo Tribunal Federal.

Assumir a coordenação do CPADSI significava muito mais do que administrar uma unidade composta por especialistas voltados à elaboração de relatórios de pesquisa e análise. O propósito era contribuir para que cada Promotor de Justiça Militar dispusesse de instrumentos técnicos, conhecimento especializado e respostas céleres capazes de tornar mais eficiente a condução das investigações sob sua responsabilidade e com total independência funcional.

A missão que me foi confiada pelo então Procurador-Geral de Justiça Militar, Antônio Pereira Duarte, era clara: fortalecer a credibilidade daquele Centro de Apoio à Investigação por meio da entrega de relatórios técnicos de qualidade, produzidos com agilidade, precisão e utilidade prática para a solução de crimes cada vez mais sofisticados, para o combate à corrupção e às organizações criminosas.

EQUIPE SPAI 2025



MEMÓRIA

SECRETARIA DE PESQUISA E APOIO À INVESTIGAÇÃO

O desafio era expressivo porque em 2020 o ambiente investigativo passava por profundas transformações tecnológicas e normativas. O volume crescente de informações contidas nos dados digitais exigia novas metodologias, novas ferramentas e novos conhecimentos. Além disso, a ausência de uma polícia judiciária especializada para atuar nas peculiaridades da Justiça Militar da União impunha ao Ministério Público Militar a necessidade de desenvolver soluções próprias para enfrentar tais obstáculos.

Como se não bastasse, logo nos primeiros meses de gestão fomos surpreendidos pelos impactos da pandemia da COVID-19, que alterou rotinas de trabalho, acelerou a transformação digital e desafiou instituições em todo o mundo. Contudo, em vez de representar um fator limitador, aquele período foi considerado como uma oportunidade para reflexão, planejamento e inovação.

Foi nesse contexto que, em 2021, iniciamos o processo de transformação do CPADSI na atual Secretaria de Pesquisa e Apoio à Investigação (SPAI). Esse redesenho organizacional teve como fundamento três pilares essenciais: tecnologia, conhecimento e comunicação.

Além das divisões já existentes de Pesquisa, Análise e Combate à Corrupção, foram criadas a Divisão de Difusão do Conhecimento e o Serviço de Apoio Administrativo, estruturas voltadas à gestão de acordos de cooperação técnica, à implementação de medidas de conformidade dos processos internos e ao suporte personalizado aos membros do Ministério Público Militar na utilização de novas metodologias e ferramentas investigativas, especialmente a plataforma PAI, que foi totalmente remodelada.

A reestruturação não se limitou à alteração do organograma. Buscamos integrar competências multidisciplinares, aperfeiçoar fluxos de trabalho e incorporar técnicas modernas de inteligência investigativa. Muitas dessas metodologias já eram dominadas por servidores experientes da unidade, mas foram atualizadas e aperfeiçoadas mediante intenso programa de capacitação realizado em parceria com especialistas da Polícia Federal, fruto de uma histórica cooperação institucional.

A área de desenvolvimento tecnológico também foi fortalecida com a ampliação da equipe e a incorporação de novos talentos. Esse esforço permitiu modernizar significativamente a Suite ARGUS, migrando seu processamento para ambiente em nuvem e tornando mais ágil o atendimento das demandas.

Nesse mesmo período, a parceria firmada com a Secretaria de Perícia, Pesquisa e Análise do Ministério Público Federal possibilitou o desenvolvimento da primeira API do SIMBA 2.0, posteriormente integrado ao SISBAJUD, integração que proporcionou acesso mais rápido a bases estratégicas de informação financeira e ampliou significativamente a capacidade de resposta da SPAI.

> **Esse redesenho organizacional teve como fundamento três pilares essenciais: tecnologia, conhecimento e comunicação.**

MEMÓRIA

SECRETARIA DE PESQUISA E APOIO À INVESTIGAÇÃO



A transformação do antigo CPADSI em SPAI representou, acima de tudo, o reconhecimento institucional do trabalho realizado ao longo dos anos por outros membros do MPM que estiveram à frente daquele Centro e servidores comprometidos com a excelência. Foi uma demonstração da confiança da Alta Administração e da maturidade alcançada pela unidade como estrutura permanente de apoio à atividade investigativa.

Os anos de 2022 e 2023 marcaram um período de extraordinário crescimento. A Secretaria alcançou seus maiores índices de produtividade desde a sua criação, resultado direto da combinação entre capacitação contínua, aperfeiçoamento tecnológico e ampliação do acesso a bases de dados estratégicas.

Nesse período, consolidamos importantes ferramentas institucionais. O sistema PLUTÃO foi atualizado, ampliando sua capacidade de cruzamento de informações e identificação de vínculos entre alvos investigados. Implantamos o SITTEL, solução destinada ao tratamento de dados oriundos de quebras de sigilo telefônico e telemático.

Também disponibilizamos os portais de pesquisa RADAR e PANDORA, ampliando o acesso a informações relevantes para a atividade investigativa. Todas as ferramentas tecnológicas, acordos de cooperação e matérias relacionadas à investigação foram reunidas no PORTAL SPAI acessível pela intranet.

Nenhuma ferramenta, entretanto, possui maior valor do que as pessoas que a utilizam. Por essa razão, a capacitação contínua da equipe foi tratada como um investimento estratégico e permanente ao longo de toda a gestão. Em um ambiente investigativo cada vez mais complexo, marcado pela rápida evolução tecnológica, pelo surgimento de novas modalidades de ilícitos cibernéticos e pela crescente produção de dados digitais, tornou-se indispensável manter servidores e colaboradores constantemente atualizados. Incentivamos a participação em cursos, seminários, grupos de trabalho e treinamentos especializados, buscando não apenas aprimorar competências técnicas, mas também desenvolver uma cultura institucional voltada ao aprendizado contínuo, à inovação e à busca de soluções. Cada conhecimento adquirido refletia diretamente na

MEMÓRIA

SECRETARIA DE PESQUISA E APOIO À INVESTIGAÇÃO

qualidade das análises produzidas e na capacidade da SPAI de oferecer respostas mais rápidas, seguras e úteis aos membros do Ministério Público Militar.

> **A Ação n° 8, proposta pelo MPM e posterior adesão do CSJT, foi reconhecida como destaque do ano pelo Secretário Nacional de Justiça e resultou na elaboração do GRINPA – Guia de Rastreamento e Identificação Patrimonial.**

Atentos ao ingresso dos novos membros aprovados no 12º Concurso Público para o cargo de Promotor de Justiça Militar, buscamos ampliar ainda mais nossos serviços. Sabíamos que o crescimento da demanda com a chegada de uma turma de potenciais investigadores, entusiasmados com o novo cargo, exigiria esforço adicional de toda a equipe, mas também compreendíamos a importância de oferecer aos novos integrantes da Instituição uma estrutura de apoio investigativo moderna, eficiente e compatível com os melhores modelos existentes no Ministério Público brasileiro.

Sempre acreditamos que as limitações podem servir de estímulo à criatividade. Diante do desafio permanente de ampliar a capacidade de atendimento sem expansão proporcional do quadro de pessoal, passamos a investir intensamente em automação, integração de sistemas e modelo de inteligência artificial não pública aplicada à atividade de pesquisa e análise.

Com o início do terceiro ciclo de gestão, já sob a liderança do Procurador-Geral de Justiça Militar Clauro Roberto de Bortolli renovamos nosso compromisso com a continuidade dos projetos estratégicos que ainda aguardavam implementação.

Em 2024, implantamos o serviço de análise de Relatórios de Inteligência Financeira produzidos pelo COAF e consolidamos o módulo de quarentena do SITTEL. Avançamos também na automação de relatórios voltados à obtenção de dados cadastrais de usuários de telefonia celular e ao suporte de sistemas auxiliares de geolocalização.

Em 2025, merece destaque o projeto-piloto desenvolvido com o Ministério da Justiça e Segurança Pública, que demonstrou o elevado potencial do serviço de Análise Telemática. Os resultados obtidos evidenciaram sua capacidade de agregar profundidade às investigações, revelando conexões, relacionamentos e evidências que dificilmente seriam identificados por métodos tradicionais.

Naquele mesmo ano, coordenamos, ao lado do Conselho Superior da Justiça do Trabalho, a Ação nº 8 da ENCCLA, voltada à investigação patrimonial e à recuperação de ativos. A Ação n° 8, proposta pelo MPM e posterior adesão do CSJT, foi reconhecida como destaque do ano pelo Secretário Nacional de Justiça e resultou na elaboração do GRINPA – Guia de Rastreamento e Identificação Patrimonial, importante repositório de boas práticas, modelos e roteiros de investigação patrimonial.

Naturalmente, ao longo dessa jornada recebemos elogios, sugestões e também críticas. Todas foram importantes. As contribuições dos colegas permitiram aprimorar funcionalidades e inspiraram o desenvolvimento de soluções como a Suite ARGUS 3.0, o SITTEL, o PLUTÃO Mobile, o BANDIT e o PÉGASUS. Aprendemos que a escuta permanente e a disposição para melhorar são elementos indispensáveis para qualquer processo de evolução institucional.

MEMÓRIA

SECRETARIA DE PESQUISA E APOIO À INVESTIGAÇÃO

Muito mais poderia ser dito sobre os projetos realizados, as parcerias construídas e a participação ativa da SPAI em iniciativas nacionais desenvolvidas no âmbito do Conselho Nacional do Ministério Público, do GNCOC, da Rede LAB e da ENCCLA. Entretanto, todas essas experiências possuem um denominador comum: a busca permanente por soluções capazes de fortalecer o trabalho investigativo do Ministério Público Militar.

Nosso maior objetivo sempre foi assessorar o Procurador-Geral de Justiça Militar e auxiliar o Promotor de Justiça natural na condução das investigações, fornecendo apoio técnico seguro, fundamentado e confiável, reduzindo obstáculos operacionais, otimizando o tempo dedicado à atividade-fim e ampliando a capacidade institucional na busca das provas da materialidade, autoria e recuperação dos ativos desviados.

Ao final desse ciclo, que marcou profundamente minha trajetória profissional e pessoal, tive a satisfação de transmitir a função ao meu sucessor com o coração repleto de gratidão e orgulho.

Transformamos estruturas, aperfeiçoamos processos, desenvolvemos tecnologias, fortalecemos parcerias e consolidamos uma cultura orientada à excelência. Mais importante do que os sistemas criados ou os indicadores alcançados, é o ideal que une pessoas comprometidas com uma causa comum: servir ao Ministério Público Militar e à sociedade brasileira com profissionalismo, inovação e espírito público.

A excelência dos serviços prestados pela SPAI não foi construída apenas com tecnologia ou ferramentas de análise, mas sobretudo pela formação contínua de profissionais comprometidos em aperfeiçoar suas habilidades e ampliar suas capacidades. Investir em pessoas foi, sem dúvida, a decisão mais importante e duradoura de toda a gestão.

Seguimos, hoje, em diferentes funções e caminhos institucionais, mas unidos pelo mesmo ideal: fortalecer a Justiça, promover a defesa da ordem jurídica e contribuir para que o Ministério Público Militar continue exercendo sua missão constitucional com independência, eficiência e excelência.

Tenho a convicção de que a SPAI continuará evoluindo, inovando e oferecendo soluções cada vez mais relevantes para a atividade investigativa, porque sua maior força nunca esteve apenas na tecnologia ou nos processos, mas nas pessoas que decidiram transformar desafios em oportunidades e trabalho em legado.

Sou profundamente grata pela oportunidade que me foi concedida de servir aos colegas, às instituições parceiras e ao Ministério Público Militar. Participar dessa construção coletiva foi uma das experiências mais enriquecedoras da minha trajetória profissional e pessoal.

RADAR INVESTIGATIVO
MINISTÉRIO PÚBLICO MILITAR



RADAR
INVESTIGATIVO
Ministério Público Militar



