ESTUDOS DE
SEGURANÇA INSTITUCIONAL
E CONTRAINTELIGÊNCIA NO ÂMBITO DO MINISTÉRIO PÚBLICO BRASILEIRO

CNMP
Conselho Nacional do Ministério Público

CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO
Comissão de Preservação da Autonomia do Ministério Público

ESTUDOS DE SEGURANÇA INSTITUCIONAL E CONTRAINTELIGÊNCIA NO ÂMBITO DO MINISTÉRIO PÚBLICO BRASILEIRO

Brasília
2019

Brasil. Conselho Nacional do Ministério Público.
Estudos de segurança institucional e contrainteligência no âmbito do Ministério Público brasileiro / Conselho Nacional do Ministério Público. – Brasília: CNMP, 2019.
162 p.

1. Segurança institucional. 2. Resolução CNMP nº 156/2017 3. Contrainteligência. 4. Ministério Público – atuação. I. Título. II. Comissão de Prevenção da Autonomia do Ministério Público – CPAMP.

CDD – 341.413

Ficha catalográfica elaborada pela Biblioteca do CNMP

COMPOSIÇÃO DO CNMP
Antônio Augusto Brandão de Aras (Presidente)
Rinaldo Reis Lima (Corregedor Nacional)
Valter Shuenquener de Araújo
Luciano Nunes Maia Freire
Marcelo Weitzel Rabello de Souza
Sebastião Vieira Caixeta
Silvio Roberto Oliveira de Amorim Junior
Luiz Fernando Bandeira de Mello Filho
Otavio Luiz Rodrigues Jr.
Oswaldo D'Albuquerque Lima Neto
Sandra Krieger Gonçalves
Fernanda Marinela de Sousa Santos

SECRETARIA-GERAL DO CNMP
Maurício Andreioulo Rodrigues

ORGANIZAÇÃO E REVISÃO
João Santa Terra Júnior
Luciana Marinho Serra Negra

PROJETO GRÁFICO, REVISÃO E SUPERVISÃO EDITORIAL
Secretaria de Comunicação do CNMP

DIAGRAMAÇÃO
Gráfica Movimento

SUMÁRIO

APRESENTAÇÃO

A segurança institucional corresponde à mais nova área de gestão do Ministério Público brasileiro, centralizada no patamar mais alto da administração da Instituição em decorrência do trato de informações sensíveis e da amplitude de abrangência das suas ações.

Seu norte regulador é a Resolução CNMP nº 156, de 13 de dezembro de 2016, responsável por instituir a Política e o Sistema Nacional de Segurança Institucional do Ministério Público brasileiro.

Em linhas rasas, afirma-se que a segurança institucional se dedica à proteção do ramo do Ministério Público em sua integralidade, por meio da antevisão de riscos de ações adversas, bem como do manejo de medidas neutralizadoras ou restauradoras dos danos ocasionados por tais ações aos ativos da Instituição. Consideram-se ativos o elemento humano (pessoas), as áreas e as instalações, os materiais, as informações e a imagem do Ministério Público.

O gerenciamento das políticas nacionais de segurança institucional desenvolve-se de maneira integrada, harmônica e em regime de corresponsabilidade entre cada ramo do Ministério Público e o Conselho Nacional do Ministério Público. Materializa-se por meio das ações da Comissão de Preservação da Autonomia do Ministério Público (CPAMP), da Secretaria Executiva de Segurança Institucional (SESI – órgão de apoio da CPAMP integrado por representantes dos ramos do Ministério Público), e do Comitê de Políticas de Segurança Institucional (CPSI), composto por membros de todos os ramos do Ministério Público brasileiro responsáveis pela segurança institucional em suas localidades.

Após dois anos de vigência da referida Resolução, o panorama da segurança institucional potencializou-se e incrementou-se, com estruturação de órgãos internos com essa específica destinação em cada ramo, bem como por meio da efetiva concretização, no âmbito nacional, de medidas destinadas à proteção dos ativos. Ademais, empreendeu-se mapeamento das realidades de cada unidade do Ministério Público brasileiro objetivando o conhecimento macro e específico das vulnerabilidades locais e nacionais, e foram empreendidas medidas para a disseminação da cultura da segurança institucional e em prol da padronização de conceitos, terminologias e procedimentos.

Contudo, por ser área recente de gestão de conhecimento, e em face da constatação de que o Ministério Público é Instituição impactada diretamente no gerenciamento dos seus ativos pelas árduas e específicas funções outorgadas pela Constituição de 1988, entendeu-se pela necessidade de desenvolvimento de doutrina própria de segurança institucional. Deve-se, ainda, considerar que a cultura de proteção exige ser moldada tendo por premissa as peculiaridades de cada objeto de tutela, não sendo possível a simples transposição para a realidade ministerial de conceitos, técnicas, medidas e doutrinas específicas já consolidadas em outras Instituições que sedimentaram essa cultura protetiva de longa data.

Nesse contexto, imprescindível que o Ministério Público produza material doutrinário para refletir, discutir e lançar bases iniciais para ser consolidada a doutrina da segurança institucional no âmbito nacional. Esse, portanto, é o objeto desta obra, que se pautou por uma abordagem livre, porém, com temáticas que se complementaram, seja pelo aspecto histórico,

com a apresentação dos meandros do surgimento da Resolução CNMP nº 156/2016, pela abordagem conceitual acadêmica, com a apresentação da segurança institucional no contexto da inteligência e da contrainteligência, pela correlação da Lei Geral de Proteção de Dados com a atividade ministerial, bem como por específicos temas de segurança orgânica e segurança ativa.

A escrita dos artigos incumbiu a profissionais diretamente vinculados à segurança institucional: Dr. Sidney Eloy Dalabrida, ex-coordenador do CPSI e atual Desembargador do Tribunal de Justiça do Estado de Santa Catarina, Dr. João Santa Terra Júnior, Promotor de Justiça membro colaborador da CPAMP, ex-vice coordenador do CPSI, ex-coordenador de segurança institucional do MPSP e organizador desta obra, Dra. Jerusa Capistrano Pinto Bandeira, Promotora de Justiça vice-coordenadora do CPSI e coordenadora de segurança institucional do MP/MA, Dr. Rui Carlos Kolb Schiefler, Promotor de Justiça coordenador de segurança institucional do MP/SC, Maria Fernanda Tonini Blazius de Oliveira, Assessora jurídica na Coordenadoria de Inteligência e Segurança Institucional do MP/SC, Vani Antônio Bueno, Procurador de Justiça coordenador de segurança institucional do MP/PR, Ricardo Caron, Capitão da Polícia Militar do Estado do Paraná, Coordenador do Núcleo de Inteligência Policial Militar do Ministério Público do Estado do Paraná, Cleverson Lautert Cruz, Gerente de Segurança Institucional do Ministério Público do Trabalho, Policial Rodoviário Federal, Marcelo Neival Hillesheim de Assumpção, Oficial de Infantaria do Exército Brasileiro, Gustavo Monteiro Muniz Costa, Oficial de Cavalaria do Exército Brasileiro, e Roberto Ferreira dos Santos, Oficial de inteligência da Agência Brasileira de Inteligência – ABIN.

A CPAMP, portanto, almeja, com a apresentação dessa obra, a solidificação do alicerce necessário para que o Ministério Público brasileiro lance olhares atentos à segurança institucional e que efetivamente desenvolva medidas protetivas aos seus ativos mais caros, as quais, em última análise, corresponderão à criação do porto seguro para que os órgãos de execução concretizem suas tarefas constitucionalmente outorgadas de defesa da sociedade.

Brasília, 24 de setembro de 2019.

Conselheiro Marcelo Weitzel Rabello de Souza

Presidente da Comissão de Preservação da Autonomia do Ministério Público

Elisa Fraga de Rego Monteiro

Coordenadora do Comitê de Políticas de Segurança Institucional (CPSI)

Nelson Lacava Filho

Promotor de Justiça Militar Membro Auxiliar da CPAMP

João Santa Terra Júnior

Promotor de Justiça Membro Colaborador da CPAMP.

RESOLUÇÃO Nº 156, DE 13 DE DEZEMBRO DE 2016: O PROCESSO DE SURGIMENTO DA NORMATIZAÇÃO SOBRE SEGURANÇA INSTITUCIONAL DO MINISTÉRIO PÚBLICO BRASILEIRO

Sidney Eloy Dalabrida[1]

SUMÁRIO: 1. Introdução. 2. Segurança Institucional: aspectos introdutórios e tratamento do tema no âmbito do Ministério Público. 2.1. Parâmetros conceituais. 2.2. O Ministério Público e a Segurança Institucional. 2.2.1. Contextualização sobre a problemática da segurança envolvendo os Ministérios Públicos e seus integrantes. 2.2.2. Necessidade de estruturação de órgãos de Segurança Institucional nos MPs. 2.3. A publicação da Resolução nº 156, de 13 de dezembro de 2016, do Conselho Nacional do Ministério Público. 2.3.1. Histórico da resolução. 2.3.2. Estudos realizados junto aos MPs brasileiros. 2.3.3. Publicação da Resolução nº 156, de 13 de dezembro de 2016. 3. Conclusão. 4. Referências.

RESUMO: O presente artigo procede a uma abordagem do processo que culminou com a Resolução nº 156, de 13 de dezembro de 2016, do Conselho Nacional do Ministério Público, publicada no Diário Eletrônico do CNMP de 14 de fevereiro de 2017. Trata-se de categoria que, até a edição do referido instrumento normativo, não dispunha de tratamento adequado no âmbito do Ministério Público, instituição completamente órfã de uma regulamentação padronizada acerca da Segurança Institucional. Foi justamente esse vazio normativo que motivou o Conselho Nacional do Ministério Público, por intermédio da Comissão de Preservação da Autonomia do Ministério Público, a criar o Comitê de Políticas de Segurança Institucional. Uma vez fixadas as premissas da atividade, por meio de uma exposição direta, o texto busca retratar sinteticamente o caminho percorrido pelos integrantes daquele Colegiado para se alcançar a aprovação da norma que romperia um período marcado pela improvisação, com vistas a conferir à Segurança Institucional um tratamento especializado e totalmente voltado à profissionalização da atividade.

1 Desembargador do TJSC. Procurador de Justiça. Procuradoria Criminal (2016). Estágio em nível de pós-doutorado Federal Judicial Center, Washington D.C., EUA (2018-2019). Doutorado em Direito (2007/2010) pela Universidade de Navarra (UNAV), Espanha. Mestrado em Ciência Jurídica (2002/2004), Universidade do Vale do Itajaí (UNIVALI). Curso de Preparação e Aperfeiçoamento do Ministério Público (1991), Escola Superior do Ministério Público (EPAMPSC).

PALAVRAS-CHAVE: Ministério Público. Conselho Nacional do Ministério Público. Comissão de Preservação da Autonomia do Ministério Público. Comitê de Políticas de Segurança Institucional. Segurança Institucional. Resolução.

1. INTRODUÇÃO

Em razão da missão constitucional que lhe é atribuída, substancialmente relacionada à defesa da sociedade, a atuação do Ministério Público, não raras vezes, repercute de maneira negativa entre aqueles que, para a manutenção de suas práticas ilícitas, empreendem ações hostis contra a Instituição ou seus membros, razão pela qual se revelou imprescindível prover em favor do MP e de seus integrantes a segurança necessária para o exercício livre e independente das suas funções institucionais.

Certo é – e a experiência assim comprovou – que somente empregando metodologia específica, com adoção de técnicas modernas, subsidiada sempre por conhecimento de inteligência, seria possível alcançar níveis de maturidade no que se refere à Segurança Institucional capazes de reduzirem as vulnerabilidades. Durante muito tempo, porém, essa atividade foi desenvolvida improvisadamente, de forma empírica, por profissionais que não tiveram preparação específica e continuada, precisamente porque as administrações superiores não reconheciam a Segurança Institucional enquanto matéria que merecesse figurar como prioritária na pauta de gestão.

O presente artigo se propõe, então, a abordar em que consiste a Segurança Institucional no âmbito do Ministério Público, quais seus elementos estruturantes, bem como expor, de modo objetivo e sem pretensão de completude, o *iter* percorrido até se alcançar, com a Resolução nº 156, de 13 de dezembro de 2016, um estágio mais avançado de proteção em favor da Instituição, dos membros e dos servidores.

2. SEGURANÇA INSTITUCIONAL: ASPECTOS INTRODUTÓRIOS E TRATAMENTO DO TEMA NO ÂMBITO DO MINISTÉRIO PÚBLICO

2.1. PARÂMETROS CONCEITUAIS

A categoria Segurança Institucional compreende diversas acepções que, embora distintas, se complementam na formação do conceito ideal. Todas elas possuem aspectos indissociáveis, evidenciados na medida em que são descritas como o conjunto de medidas voltadas à proteção de uma instituição e de seus recursos humanos.

Extrai-se disso, portanto, que o conceito de Segurança Institucional transpassa as medidas que comumente se veem empregadas nas instituições, a exemplo daquelas destinadas ao controle de acesso e à vigilância patrimonial, uma vez que pressupõe uma visão holística, abrangendo conceitos não limitados à segurança física de instalações.

Segurança Institucional é, em verdade, um bloco de medidas que visam a prevenir, detectar e neutralizar ações de qualquer natureza que constituam ameaça à instituição e a seus integrantes, inclusive no que concerne à imagem e reputação.

O conceito abarca, dentre outras regras, as de segurança ativa e as de segurança orgânica. As primeiras referem-se a medidas positivas destinadas à identificação e neutralização de ações adversas por meio da adoção da contraespionagem, contrassabotagem, contrapropaganda, contraterrorismo e contra crime organizado, que são medidas estabelecidas com base na análise das ameaças e riscos a que a instituição possa ser submetida. Já as segundas, as regras de segurança ativa, constituem-se em ações preventivas integradas destinadas à segurança dos recursos humanos, dos materiais, das áreas e instalações e da segurança da informação, que inclui a segurança nos meios da tecnologia da informação e documentação.

No que concerne à segurança orgânica, é importante discorrer sobre cada pilar que a compõe, porque, como já citado, refere-se a medidas preventivas, vocacionadas ao controle das vulnerabilidades, a fim de evitar danos de qualquer natureza que possam ser impostos à instituição, sobretudo em razão de ameaças ou de ações hostis.

Nessa perspectiva, tem-se, como primeiro pilar, a segurança de recursos humanos, que é o conjunto de normas e procedimentos destinados à proteção das pessoas, assegurando-lhes a integridade física e moral. Objetivam garantir o exercício independente das atividades institucionais e podem, em casos excepcionais, ser estendidas a familiares de pessoas diretamente ligadas à instituição, eventualmente atingidas em razão da função exercida por estes.

O segundo pilar, a segurança da documentação e do material, consiste em um aglomerado de normatizações e instruções procedimentais voltadas à proteção dos documentos e dos materiais, visando a assegurar o pleno funcionamento da instituição. Quanto aos documentos, essas medidas cuidam de todo o processo que os envolve, desde a sua produção, difusão e manuseio, até o arquivamento e destruição.

Em complemento, com vistas também à proteção dos conhecimentos e materiais sensíveis armazenados na instituição, tem-se o terceiro pilar, a segurança de áreas e instalações, representado pelas demarcações de áreas e implantação de barreiras destinadas a controlar o acesso de pessoas indesejadas em determinados locais, garantindo, assim, que as informações que se pretende resguardar não sejam expostas àqueles que objetivam sua obtenção para uso em detrimento da instituição.

Por fim, o quarto pilar da segurança orgânica é a segurança da informação, bem definida pelo Gabinete de Segurança Institucional como "ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações" (2008). Destina-se, em verdade, à proteção de todas as informações que tramitam dentro da instituição, para que não sejam acessadas por pessoas que não possuam interesse institucional no conteúdo de que tratam e, especialmente, para que não sejam obtidas por terceiros. Isso porque, atualmente, a informação

constitui-se um dos ativos mais valiosos da instituição, o que exige que ele seja mantido seguro e confiável, não comprometendo, assim, a credibilidade da instituição.

É neste ponto que se insere a segurança nos meios de tecnologia da informação. Nesse sentido, mister destacar que, atualmente, o campo mais favorável à disseminação de ataques à segurança da informação é a internet, ambiente em que se identifica o maior número de ameaças, cujo grau de sofisticação é crescente. Avulta-se, por esse motivo, a imprescindibilidade de destinar ao tema especial atenção, exigindo-se que as instituições empreguem uma gestão de segurança da informação que permita alinhamento entre as necessidades organizacionais da segurança e o gerenciamento dos sistemas de informação, não se limitando, contudo, à implantação de tecnologias, mas propondo a utilização de ferramentas eficientes, capazes de minimizar possíveis vulnerabilidades.

Importa destacar que, embora adotadas todas as medidas preventivas ressalvadas pela segurança orgânica, não se pode desconsiderar a possibilidade de ocorrências de eventuais contingências, motivo por que os responsáveis pela Segurança Institucional devem estar preparados para agir, também, reativamente. Nesse sentido, faz-se importante o desenvolvimento de protocolos de atuação reativos e planejamentos de contingências, voltados a nortear a atuação em eventual situação de anormalidade, não permitindo que a instituição fique à mercê da ação de forças antagônicas desconhecidas.

Observa-se, pelo exposto, a relevância das medidas preventivas representadas pela segurança orgânica no que tange à realização efetiva da atividade de Segurança Institucional. Entretanto, além da segurança ativa e orgânica, a atividade de inteligência figura como essencial para a integralidade da Segurança Institucional.

Define-se inteligência, segundo Joanisval Brito Gonçalves, como "um conhecimento processado (a partir de matéria bruta, com metodologia própria), obtido em fontes com algum caráter de sigilo e com o objetivo de assessorar o processo decisório" (GONÇALVES, 2016, p. 27). Trata-se, portanto, do processo de obtenção de dados que, após tratados por especialistas de inteligência, denominados analistas, mediante metodologia específica, resultarão na produção de conhecimento que se destina ao assessoramento do poder decisório em diferentes níveis e atividades.

Frisa-se que, atualmente, a atividade de inteligência, embora muitas vezes questionada em razão do secretismo que lhe é atribuído, constitui-se importante fator para o desenvolvimento das instituições. É por meio dela que se desenvolvem conhecimentos que, conforme já mencionado, subsidiam o tomador de decisões.

No que se refere à Segurança Institucional, é inegável a contribuição da inteligência para que a atividade possa ser desenvolvida em atendimento ao que preceituam as doutrinas que a estabelecem. É o conhecimento produzido pela inteligência que alimenta as análises de risco e os estudos de cenários, de alvos e de ameaças, amparando o emprego das equipes operacionais que atuam na proteção da instituição e seus integrantes.

Tem-se, assim, que a Segurança Institucional se constitui em um grande grupo de atividades que se complementam e que, por isso, são intercambiáveis. Abrange medidas preventivas, reativas e de inteligência, todas dirigidas à salvaguarda da instituição e de seus integrantes, pressupondo sempre uma atuação técnica e profissional.

2.2. O MINISTÉRIO PÚBLICO E A SEGURANÇA INSTITUCIONAL

2.2.1. Contextualização sobre a problemática de segurança envolvendo os Ministérios Públicos e seus integrantes

O cumprimento da missão constitucional reservada ao Ministério Público naturalmente atinge agentes e organizações que, visando à preservação de seus interesses ilícitos, se valem da prática de atentados e de ameaças contra membros da Instituição para desencorajá-los do exercício de suas funções institucionais. Ações desse tipo naturalmente atentam contra a ordem jurídica, desafiam o Estado Democrático de Direito e ameaçam a independência do Ministério Público brasileiro.

A história registra inúmeros casos de atentados contra membros do Ministério Público em razão da sua firme atuação funcional. Merece registro o assassinato do Procurador da República Pedro Jorge Melo e Silva, ocorrido em Pernambuco, no dia 3 de março de 1982. O crime, que representou uma forma de intimidação à Instituição ministerial, ocorreu em decorrência da atuação do Procurador da República em um dos maiores casos de corrupção da década de 80, conhecido como "Escândalo da Mandioca", praticado no sertão de Pernambuco, na cidade de Floresta, em meio à ditadura militar. Apurou-se, posteriormente, que o mentor intelectual do fato delituoso foi um dos beneficiários do esquema de corrupção. Trata-se, pois, de caso emblemático, visto que, na época do ocorrido, fatos dessa natureza raramente eram registrados, porquanto a vigência, na década de 80, do chamado "temor reverencial".

Alguns se tornaram um marco na discussão sobre a necessidade de a Instituição voltar sua atenção à própria proteção. Dentre eles, destaque-se o assassinato do Promotor de Justiça do Ministério Público de Minas Gerais Francisco José Lins do Rêgo, ocorrido no dia 25 de janeiro de 2002. Chico Lins foi assassinado, com sete disparos de arma de fogo, quando se dirigia ao trabalho. Novamente, trata-se de fato motivado pelas funções institucionais desenvolvidas pelo Promotor de Justiça, uma vez que o mandante do crime foi um empresário que era investigado em ação que apurava a "Máfia dos Combustíveis", caso de competência do Promotor. O fato tomou grandes proporções e evidenciou uma nova realidade, caracterizada pelo destemor à figura dos órgãos essenciais à Justiça. Tamanha foi a repercussão que o assassinato do Promotor de Justiça Francisco Lins desencadeou a criação dos Grupos de Atuação Especial no Combate ao Crime Organizado (GAECO), que representam hoje um importante instrumento de combate à criminalidade organizada.

Noutra angulação, não se pode olvidar que, impulsionadas pela globalização, ao aderir às novas tecnologias para poder garantir à sociedade

a prestação de um serviço público eficiente e de qualidade, as instituições ministeriais se expõem a um universo de ameaças que, com impressionante dinamismo, pululam o cyberespaço, comprometendo a segurança da integridade, disponibilidade e confidencialidade das informações e sistemas sob a guarda dos Ministérios Públicos.

Todo esse cenário de risco a que se encontram expostos os Ministérios Públicos e seus membros, por óbvio, exige a implantação de uma política de salvaguarda institucional que seja capaz de garantir o exercício pleno e livre das atividades desenvolvidas pelos seus integrantes, bem como o controle das vulnerabilidades em torno da informação e de seus sistemas.

Portanto, é imprescindível ao Ministério Público brasileiro a criação de mecanismos que, em todos os eixos de atuação por meio dos quais se manifesta (recursos humanos, áreas e instalações, materiais, informação e seus sistemas), sejam capazes de assegurar a preservação da identidade, imagem e reputação das instituições ministeriais, bem como a atuação livre e independente de seus integrantes, evitando, assim, a ocorrência de novos fatos similares aos apresentados anteriormente.

Ocorre que o alicerce central para a implementação desse modelo de Segurança Institucional é a construção e constante fomento de uma cultura de Segurança Institucional, com a conscientização e permanente sensibilização de cada membro das instituições sobre a sua responsabilidade pela proteção pessoal e da instituição a que pertencem. A ausência de uma normatização que regulamentasse a Segurança Institucional no âmbito das unidades ministeriais revelou-se fator fundamental para a falta de adesão a qualquer projeto que, no âmbito de determinado Órgão do Ministério Público, fosse implementado.

Todo esse panorama reclamava urgência na mudança de abordagem da Segurança Institucional, a fim de conferir-lhe importância tal, a ponto de figurar como prioridade institucional.

2.2.2. Necessidade de estruturação de órgãos de Segurança Institucional nos MPs

Tratar a Segurança Institucional de maneira adequada significa, em linhas gerais, a adoção de todas as medidas necessárias à gestão de segurança de forma proativa, profissional e eficiente. Não se trata tão somente de destinação de recursos à aquisição de equipamentos e tecnologias, nem mesmo de recrutamento humano ou de mudança comportamental; necessita-se de integração entre todos os segmentos que compõem o conceito de Segurança Institucional, a fim de que ela seja aplicada em sua integralidade. Para tanto, imprescindível que o Ministério Público se preocupe com a criação de organismos internos voltados especificamente à gestão estratégica de Segurança Institucional, empregando todas as ferramentas e meios disponíveis para a efetivação da atividade.

Não se pode conceber que o Ministério Público fique à mercê da criminalidade e se torne campo fértil à atuação de atores hostis. É inegável

que o histórico de atentados contra o Ministério Público não pode servir apenas de estatística, e sim de impulso para a idealização de projetos voltados à sensibilização da Administração Superior de cada instituição quanto à importância que o tema requer, convencendo-a quanto à improrrogável necessidade de criação de setor especialmente incumbido da matéria.

Trata-se de medida substancial à regularidade das atividades ministeriais, cuja omissão pode acarretar prejuízos inestimáveis à Instituição. Daí porque não se admitir que o tema seja delegado a outros órgãos ou realizado com inobservância a preceitos mínimos estabelecidos doutrinariamente. Somente órgãos estruturados para esse fim são capazes de atuar em consonância com os mandamentos sobre Segurança Institucional e revestir o Ministério Público e seus integrantes da segurança necessária ao cumprimento da missão que lhes foi constitucionalmente outorgada.

2.3. A PUBLICAÇÃO DA RESOLUÇÃO Nº 156, DE 13 DE DEZEMBRO DE 2016, DO CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO

2.3.1. Histórico da Resolução

Ao traçar o caminho percorrido até a aprovação e publicação da Resolução nº 156 do Conselho Nacional do Ministério Público, é imprescindível, de partida, fazer referência ao Comitê de Políticas de Segurança Institucional (CPSI).

Cuida-se de órgão colegiado, de natureza consultiva, deliberativa e propositiva, instituído pela Portaria CNMP-PRESI nº 150, de 31 de agosto de 2011, que tem por atribuição primordial propor os objetivos e as diretrizes gerais de Segurança Institucional no âmbito do Ministério Público, bem como buscar a uniformização, padronização e integração dos diversos planos de Segurança Institucional. Atualmente vinculado à Comissão de Preservação da Autonomia do Ministério Público (CPAMP), o Comitê é composto por representantes de todos os ramos do Ministério Público da União e dos Ministérios Públicos Estaduais, competindo sua coordenação e vice-coordenação a integrantes do colegiado designados pelo presidente da CPAMP.

Dentre outras competências que lhes foram conferidas por meio da norma que o instituiu ou pela Portaria CNMP-PRESI nº 70, de 27 de março de 2014, que ao dispor sobre a organização dos Comitês pormenorizou um rol de atribuições ao CPSI, está a de apresentar ao CNMP, por intermédio da CPAMP, sugestões para a elaboração de atos normativos na área da Segurança Institucional.

Por esse motivo, no ano de 2013 foi apresentado ao Conselho Nacional do Ministério Público o primeiro projeto de Resolução a respeito da Política de Segurança Institucional e do Sistema de Segurança Institucional. Em momentos subsequentes foram apresentados alguns substitutivos, porém nenhum deles se consolidou.

Em meados de 2016, já na gestão do Conselheiro Fábio Stica como Presidente da Comissão de Preservação da Autonomia do Ministério Público, recebemos a incumbência de coordenar o Comitê de Políticas de Segurança Institucional. Após algumas discussões, deliberou-se pela necessidade de retomar os estudos e, seguindo os trâmites internos, apresentar um novo projeto voltado à concretização de uma norma que viesse a regulamentar, nacionalmente, a Segurança Institucional no Ministério Público brasileiro. Foi essa provocação que balizou estudos e discussões que, conforme se verificará a seguir, resultaram na edição da Resolução nº 156, de 13 de dezembro de 2016.

2.3.2. Estudos realizados junto aos MPs brasileiros

Como dito alhures, com a nova atribuição delegada ao CPSI, verificou-se a necessidade de promover estudos para retomada dos projetos anteriormente apresentados e, por meio de atualizações e alterações, editar novo documento que seria, futuramente, submetido à apreciação do CNMP.

Dessa forma, constatou-se que, para chegar à edição de uma norma que pudesse atender à realidade de todos os Ministérios Públicos brasileiros, era preciso, primeiramente, obter consciência situacional, conhecendo a realidade de cada órgão do Ministério Público.

Isso desencadeou, então, a elaboração de um questionário de Segurança Institucional, cujas respostas serviriam de base para a criação de uma norma que melhor atendesse às demandas institucionais. Tratava-se de documento com 148 questionamentos, divididos em nove blocos, quais sejam: a) normatização e gestão; b) composição da unidade de Segurança Institucional; c) estrutura das unidades responsáveis pela Segurança Institucional; d) atividades da unidade de Segurança Institucional; e) capacitação e treinamento dos integrantes da Segurança Institucional; f) capacitação e treinamento dos integrantes do Ministério Público; g) cultura de segurança; h) equipamentos de segurança e controle nas áreas e instalações do Ministério Público; i) dados institucionais.

O questionário foi, então, disponibilizado aos representantes de cada Ministério Público que compunham o CPSI, estabelecendo-se prazo para seu preenchimento. Findo o período para resposta, passou-se à fase de análise e tabulação de dados, constatando-se que, dentre todos os MPs, somente três furtaram-se a respondê-lo. Por sua vez, quanto aos demais, o panorama identificado, no que tange à Segurança Institucional nos Ministérios Públicos, lamentavelmente caracterizava-se pela improvisação, amadorismo e falta de planejamento mínimo.

Observou-se que, à época, passados sete anos da Recomendação nº 13, de 16 de junho 2009, do CNMP, que orientava a implantação de Plano de Segurança Institucional, ainda havia Ministérios Públicos sem aquele regramento e que sequer dispunham de um órgão encarregado da Segurança Institucional ou, se possuíam, não era coordenado por membro do MP, havendo, ainda, instituições que delegavam às Assessorias Militares tal incumbência.

A falta de profissionalização da atividade também se evidenciou na ausência de critérios de seleção e investigação social no ingresso de pessoal nas instituições, na carência de orientações de Segurança Institucional nos cursos de ingresso na carreira do Ministério Público e, quanto ao acesso às instalações ministeriais, pela escassez de recursos ou procedimentos de controle. Não obstante, constatou-se a omissão quanto à gestão de riscos, não havendo protocolos para o enfrentamento de crises, mas tão somente medidas adotadas de maneira intuitiva e de modo segmentando, sem qualquer orientação racional.

O cenário tornou-se, então, assunto de debates nas reuniões ordinárias e extraordinárias do CPSI que sucederam a aplicação do questionário. Foi rediscutida a matéria no colegiado, colheram-se sugestões e, com isso, surgiu um novo projeto que, aprovado, tomou corpo por meio da Resolução nº 156, de 13 de dezembro de 2016.

2.3.3. Publicação da Resolução nº 156, de 13 de dezembro de 2016

Impulsionada pelo número de membros do Ministério Público ameaçados e pelo cenário de risco cada vez mais crescente, bem como pela edição de resolução, no âmbito do CNJ, tratando da matéria, e da decisão prolatada em processo de controle administrativo em que o membro do MP alegava direito a aposentadoria especial sob o argumento de que a atividade desenvolvida era de risco, em que, embora rechaçado o pleito, reconheceu o CNMP como de risco a atividade desenvolvida pelos membros do MP, qualquer que seja sua área de atuação; a aprovação do projeto apresentado culminou na Resolução nº 156/2017, que, finalmente, sanou o vácuo normativo acerca da política de salvaguarda institucional no Ministério Público – tema cuja regulamentação era premente.

Assim, com amparo na relevância da Segurança Institucional para o livre e independente exercício das funções constitucionais do Ministério Público e na necessidade de instituir um sistema nacional e uma política uniforme de Segurança Institucional que norteasse o tratamento da matéria, a Resolução nº 156/2017 chegou como um marco, estabelecendo conceitos e diretrizes regulamentadores da atividade.

Em primeiro momento, importa destacar que a Resolução criou a Política de Segurança Institucional do Ministério Público (PSI/MP) e o Sistema Nacional de Segurança Institucional do Ministério Público (SNS/MP). Quanto a este, cabe uma observação referente à proposta original apresentada à CPSI, cujo documento apresentava a seguinte estrutura: Comitê de Políticas de Segurança Institucional e Departamento de Segurança Institucional do Ministério Público. Tratava-se, portanto, de um modelo centralizado de gestão de Segurança Institucional, que se contrapunha à estrutura organizacional recomendável à segurança. Esta se fundamenta na visão sistêmica e integradora e reclama linhas hierárquicas horizontais de comando. A estrutura à época proposta se inclinava a tornar o processo de implementação da Política de Segurança Institucional mais lento e complexo. A simples necessidade de alocação de significativos recursos para viabilizar a instituição do Comitê e do Departamento em momento de escassez já

demonstrava a dificuldade na implantação. Ademais, os órgãos seriam vinculados à Presidência do CNMP, portanto sob a direção do Ministério Público Federal, cujo universo diverge das demais instituições ministeriais.

Assim, de modo distinto, a proposta apresentada no projeto que se tornou, posteriormente, a Resolução nº 156/2017, atribuiu à Comissão de Preservação da Autonomia do Ministério Público (CPAMP) a gestão e coordenação estratégica do Sistema Nacional de Segurança Institucional, criando, ainda, a Secretaria Executiva de Segurança Institucional (SESI) como órgão executivo e reafirmando o Comitê de Políticas de Segurança Institucional (CPSI) como órgão consultivo, deliberativo e propositivo.

Entretanto, o documento não se limitou à instituição da Política de Segurança Institucional do Ministério Público (PSI/MP) e do Sistema Nacional de Segurança Institucional do Ministério Público (SNS/MP), mas preocupou-se em conceituar Segurança Institucional e dispor sobre os princípios que devem regê-la, destacando-se a profissionalização e o caráter perene da atividade.

Nesse sentido, registrou-se que a atividade de Segurança Institucional deve ser tratada de modo profissional, o que implica o controle pela própria instituição, não sendo possível que sua gestão seja delegada a outros órgãos. Importante destacar, aqui, a dissonância entre órgão de Segurança Institucional e gabinetes militares com atribuições de segurança. A estes se pode reservar a realização de atividades operacionais e até mesmo táticas, mas é inconcebível que lhes sejam atribuídas funções estratégicas e de gestão. A segurança deve ser coordenada, fiscalizada e controlada por membro do Ministério Público especialmente designado para tal encargo, propósito que foi contemplado no artigo 29 da Resolução.

Preocupou-se a norma, também, com o tratamento eremítico dispensado por cada setor administrativo à Segurança Institucional. Isso porque os órgãos tratavam-na como uma questão periférica em relação ao todo e, dentro de uma concepção sistêmica e de salvaguarda institucional, é imprescindível interlocução constante entre os diversos setores da Instituição, a fim de que haja um tratamento integrado e multidisciplinar da segurança. A ausência dessa integração resulta na abordagem da segurança como atividade estanque, destinada somente a resolver problemas pontuais e episódicos. Para tanto, a formação de comitês que reúnam representantes dos setores estratégicos da instituição para tratarem, conjuntamente, da Segurança Institucional mostra-se como um facilitador no processo de integração, o que proporciona melhor internalização das normas de segurança.

De outro norte, com vistas à eficácia da atividade, determinou o instrumento normativo que

> os ramos do MP deverão proporcionar ao órgão de Segurança Institucional o acesso aos bancos de dados e sistemas da instituição, ou de acesso da instituição, para subsidiar as respectivas atividades de Segurança Institucional, inteligência, Contrainteligência, observados os procedimentos de segurança e controle (art. 7, §4º).

Justifica-se a disposição na natureza das atividades desenvolvidas pelo órgão de Segurança Institucional, que por vezes depende de acesso rápido a banco de dados, não se mostrando razoável que se coloquem entraves burocráticos dificultadores da obtenção de informações.

A propósito, a Resolução é clara ao estabelecer que nenhum setor está blindado em relação a checagens de segurança, ainda que se trate do setor de tecnologia da informação (TI), tendo-se estabelecido que a segurança da informação nos meios de TI envolve medidas de checagem mediante cruzamento para verificação e com segregação de funções por estrutura não subordinada à área de tecnologia da informação. Buscou-se, com essa medida, uma mudança conceitual pela qual a unidade específica da Segurança Institucional proceda ao gerenciamento de risco na área da tecnologia da informação, não ficando refém do setor informático.

Ainda no que concerne à segurança da informação, sabe-se que uma das maiores vulnerabilidades reside na prestação de serviços por terceiros, que, em virtude do vínculo efêmero que possuem, demonstram pouco compromisso com o resguardo do sigilo. Denota-se, diante do risco permanente à instituição, a importância da implementação de controles do ingresso de agentes hostis e o monitoramento de suas ações. É a vertente da segurança da informação que trata de pessoas – que é o elo mais sensível de todo processo. Por esse motivo, a resolução foi enfática ao impor medidas preventivas que devem ser observadas, especialmente quanto à subscrição de termo de compromisso de manutenção de sigilo (TCMS) por aqueles que, durante o desenvolvimento de suas funções laborais dentro da instituição, possam ter tido acesso a informações sensíveis ou sigilosas (art. 9º, IV, §1º).

Outro importante tema abordado pela Resolução diz respeito à gestão de riscos, ao qual foi destinada seção específica (seção III, art. 16). Ocorre que, anteriormente à publicação da resolução, como já observado, não havia, nas Instituições, processos claros no âmbito da Segurança Institucional, representando o trato não profissional do tema e demonstrando a urgência da uniformidade na execução da atividade, imprimindo-lhe eficiência.

É cediço que não se consegue uma operação segura quando a atividade é desenvolvida de modo intuitivo, sem qualquer orientação racional. Precisa-se padronizar as ações, por meio de protocolos de segurança, para que seja aumentada a previsibilidade dos resultados e minimizadas as possibilidades de crises. Nesse passo, qualquer operação de segurança da Instituição deve ser objeto de planejamento técnico e subsidiada por conhecimento de inteligência. Insere-se, neste ponto, a gestão de riscos como imprescindível, pois estes devem ser identificados e tratados de modo profissional e proativo, o que permitirá a efetividade nos resultados.

Paralelamente, destinou-se a resolução a tratar do aperfeiçoamento e capacitação continuada daqueles que integram as equipes de segurança do Ministério Público. Isso porque segurança não se faz tão somente com o recrutamento de policiais. É necessário que estes sejam submetidos a treinamentos constantes e direcionados à atividade desenvolvida dentro da

instituição. Como se sabe, a Segurança Institucional, embora indissociável da segurança pública, diverge desta, inclusive no que se refere a técnicas e doutrinas que a regem. Por isso a importância de que as unidades ministeriais invistam na capacitação de suas equipes de segurança. É preciso, para bem atender aos integrantes da Instituição e prover-lhes a segurança para o exercício de suas competências funcionais, que os profissionais a quem incumbe essa responsabilidade estejam preparados e tecnicamente capacitados para o desenvolvimento da atividade de proteção.

Rumando ao desfecho dessa análise, dentre os pontos da norma que merecem destaque, está a cultura de segurança. Por mais simples que possa parecer, o alicerce principal de toda arquitetura consiste na formação de uma cultura de Segurança Institucional. Uma postura de prevenção reduz vulnerabilidades, diminui riscos e dificulta ameaças, e consequentemente aumenta a segurança.

Teorias criminológicas aplicáveis ao contexto da segurança deixam à mostra a relação entre os contextos situacionais e os atentados. Se para o atentado se faz necessária uma vítima vulnerável e um ambiente propício, podem-se reduzir riscos com cuidados básicos. Há aqui um vasto campo para adoção de medidas proativas voltadas à minimização de riscos e ameaças, destacando-se a criação da cultura de segurança por meio de campanhas educativas, palestras, eventos e ações.

No universo da segurança da informação, é fácil identificar a procedência desse raciocínio. Tem-se a internet como campo fértil à proliferação de ameaças à segurança da informação, porém não é a tecnologia a ferramenta mais eficaz para garantir a proteção contra códigos maliciosos, uma vez que a maior vulnerabilidade deriva do comportamento do integrante da Instituição. Vê-se, assim, que o fator humano é o elo mais fraco da cadeia de segurança, o que explica a ênfase da Resolução à necessidade do desenvolvimento da cultura de segurança entre os integrantes da Instituição.

Convém sublinhar que, nesse quadrante, não foram abordados aspectos conceituais que constam do texto da Resolução, uma vez que já foram detalhados no tópico introdutório. Embora não se tenha esgotado toda a temática abrangida pela Resolução nº 156/2017, priorizou-se, aqui, as disposições que constituem os pontos cruciais para o exercício integral e profissional da Segurança Institucional, cuja observância obrigatória pelos MPs tende a impactar positivamente nos índices de segurança da Instituição e daqueles que exercem as funções conferidas ao Ministério Público.

3. CONCLUSÃO

Com a publicação da Resolução nº 156/2017, finalmente se estabeleceu, no Ministério Público brasileiro, uma política de salvaguarda institucional.

Como se pode verificar, nela se encontram as diretrizes gerais que servem para orientar as tomadas de decisões e a elaboração de normas,

processos, práticas, procedimentos e técnicas de segurança. Trata-se, em verdade, de documento de fundo principiológico, motivo por que se encontra em nível de gestão, e não tático ou operacional. Portanto, não traz em seu corpo o detalhamento dos mecanismos necessários para o atingimento dos objetivos estabelecidos, uma vez que não é função da Política de Segurança Institucional, já que esta se destina especificamente ao estabelecimento das normas regulamentadoras da atividade, prestando-se ao amparo aos Ministérios Públicos quanto à organização interna da Segurança Institucional.

É possível concluir, de todo o exposto, que a publicação da Resolução nº 156/2017 consiste em um grande passo em direção a uma maior maturidade em termos de Segurança Institucional. Por meio dela deixou-se de lado o tratamento empírico do tema, passando-se a abordá-lo de forma profissional e com observância a critérios e a princípios que devem nortear uma gestão estratégica de segurança.

O desafio passou a ser, então, sensibilizar os gestores acerca da importância da implementação da Política de Segurança Institucional, não permitindo que a resolução seja apenas mais um documento desprovido de concretude. É preciso, portanto, que sejam envidados todos os esforços na busca pela criação de uma cultura de Segurança Institucional que permita, por meio da integração de todos os setores da Instituição, cada qual na medida de suas atribuições, que as disposições da Resolução sejam fielmente aplicadas, garantindo, assim, que aquilo que antes parecia utópico e distante, torne-se cotidiano na realidade do Ministério Público brasileiro.

Por fim, avulta pontuar que a Resolução nº 156/2017 foi fruto do esforço conjunto de todos os membros do Comitê de Políticas de Segurança Institucional e que, embora naturalmente sujeito a mudanças ditadas pelo dinamismo inerente à atividade, representa um avanço significativo em termos de profissionalização da Segurança Institucional no âmbito do Ministério Público brasileiro.

4. REFERÊNCIAS

BRASIL, GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA. **Instrução Normativa GSI nº 1, de 13 de junho de 2008**: Disciplina a gestão de segurança da informação e comunicações na administração pública federal, direta e indireta, e dá outras providências. Brasília, junho 2008. Publicada no DOU nº 115, de 18 de junho de 2008 – Seção 1. Disponível em: <file:///C:/Users/User/Downloads/14_IN_01_gsidsic.pdf>. Acesso em: 17 abr. 2019.

CASTRO, C. A.; FILHO, E. B, R. **Inteligência de Segurança Pública:** um xeque-mate na criminalidade. Curitiba: Editora Jaruá, 2012.

CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO. **Resolução nº 156, de 13 de dezembro de 2016**. Institui a Política de Segurança Institucional e o Sistema Nacional de Segurança Institucional do Ministério Público e dá outras providências. Publicada no Diário Eletrônico do CNMP, Caderno Processual,

p. 1-11, de 14 de fevereiro de 2017. Disponível em: <http://www.cnmp.mp.br/portal/images/Resolucoes/Resolu%C3%A7%C3%A3o-156.pdf>. Acesso em: 9 abr. 2019.

CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO. **Portaria CNMP – PRESI nº 70, de 24 de março de 2014**. Dispõe sobre a organização e o funcionamento dos Comitês, Fóruns, Representações, Grupos de Trabalho e congêneres no âmbito do Conselho Nacional do Ministério Público e dá outras providências. Publicada no DOU, Seção 1, de 31 de março de 2014. Disponível em: <http://www.cnmp.mp.br/portal/images/Portarias_Presidencia_nova_versao/2014/2014.Portaria-CNMP-PRESI-0701.pdf>. Acesso em: 9 abr. 2019.

_____. **Portaria CNMP – PRESI nº 150, de 31 de agosto de 2011.** Institui o Comitê de Políticas de Segurança Institucional do Ministério Público. Publicada no Boletim de Serviço nº 16, 2ª quinzena, edição de 15 de agosto de 2011. Disponível em: <http://www.cnmp.mp.br/portal/images/Portarias_Presidencia_nova_versao/2011/2011.Portaria-CNMP-PRESI-150.pdf>. Acesso em: 17 abr. 2019.

_____. **Recomendação nº 13, de 16 de junho de 2009.** Dispõe sobre a implantação de Plano de Segurança Institucional nas áreas da segurança da informação, segurança de recursos humanos, segurança de materiais, segurança de áreas e instalações. Publicada no Diário da Justiça, seção única, de 2 de julho de 2009. Disponível em: <http://www.cnmp.mp.br/portal/images/Recomendacoes/Recomenda%C3%A7%C3%A3o-013.pdf>. Acesso em: 10 abr. 2019.

FARAH, Camel A. de G. Segmentos de Segurança Institucional – Curso de Gestão Estratégica de Segurança Institucional. **Apostila da fase EAD**. Logos – Inteligência e Planejamento Estratégico. Florianópolis, 2019.

FILHO, Diógenes Dantas. **Segurança Pessoal**. Rio de Janeiro: Editora Ciência Moderna Ltda., 2002.

GONÇALVES, Joanisval Brito. **Atividade de Inteligência e legislação correlata**. 4ª Ed. Niterói: Impetus, 2016.

MANDARINI, Marcos. **Segurança Cooporativa Estratégica**: fundamentos. Barueri: Manole, 2005.

SCHETTINI, M.; LOPES, L.; CARDOZO, H. **Segurança Institucional no serviço público:** aspectos técnicos e administrativos aplicáveis à segurança dos órgãos públicos brasileiros. São Paulo: Fontenelle publicações, 2018.

PREMISSAS PARA A SEDIMENTAÇÃO DA SEGURANÇA INSTITUCIONAL DO MINISTÉRIO PÚBLICO

João Santa Terra Júnior[1]

SUMÁRIO: 1. Introdução. 2. Segurança como direito humano fundamental. 3. A dificuldade de conceituação da segurança e as diversas percepções da insegurança. 4. A Segurança Institucional do Ministério Público: segurança orgânica, segurança ativa, Contrainteligência e inteligência. 5. Conclusão. 6. Referências.

RESUMO: O Ministério Público, no exercício de suas atividades destinadas à efetividade dos seus amplos deveres funcionais constitucionalmente sedimentados concernentes à proteção da ordem jurídica, do regime democrático e dos direitos fundamentais do ser humano, sofreu, após 1988, exponencial incremento de ataques engendrados por agentes de plúrimas fontes. Nesse contexto, ações hostis são direcionadas a cada dia para o alcance de dano ou para a geração de concreto perigo de dano aos ativos que guarnecem e asseguram a permanência da Instituição: as pessoas, as informações internas, os materiais, as instalações e a imagem institucional. Considerando que o abalo a tais ativos, por uma análise consequencial, ocasiona máculas à efetivação daquelas funções constitucionalmente estabelecidas, é inequívoco que a sociedade, que é a destinatária do trabalho do Ministério Público, será igualmente lesada. É imprescindível, assim, que o Ministério Público brasileiro crie mecanismos internos de aferição das suas vulnerabilidades, de análise dos seus riscos e de contenção dos danos perpetrados por ações hostis contra seus ativos. Para tanto, o Conselho Nacional do Ministério Público editou, no final do ano de 2016, a Resolução nº 156, responsável por instituir a Política e o Sistema Nacional de Segurança Institucional do Ministério Público. Esse escrito abordará as premissas que se entende de imprescindível compreensão para a sedimentação dessa nova área inerente à gestão do Ministério Público brasileiro.

PALAVRAS-CHAVE: Ministério Público. Vulnerabilidades. Contrainteligência. Segurança orgânica. Segurança Institucional.

1 Promotor de Justiça do Ministério Público do Estado de São Paulo. Membro colaborador do CNMP vinculado à CPAMP na área de Segurança Institucional. Doutorando na Universidade de Salamanca, Espanha, com pesquisa a respeito do uso da inteligência para o enfrentamento das organizações criminosas. Mestre em Direito Penal pela Universidade de São Paulo – Largo São Francisco. Professor em graduações e da Escola Superior do Ministério Público do Estado de São Paulo.

1. INTRODUÇÃO

A segurança é, em nossa realidade pós-moderna, uma das principais pautas de discussão tanto em contextos de preservação de direitos individuais quanto difusos, como no âmbito de geral proteção de entes inanimados públicos ou privados.

Se pensarmos que os seres, humanos ou fictícios, são compostos de inúmeros valores e possuidores de bens que podem ser vulnerados, lesados ou destruídos em razão de ações de terceiros ou de ocorrências naturais, encontraremos justificativa para a pulverização da preocupação com a segurança.

No entanto, a mensuração dessa preocupação e das suas consequências para o modo de vida atual merece especial atenção em decorrência do seu impacto direto nas medidas adotadas para a prevenção ou a neutralização daquelas ações e daqueles fatores capazes de vulnerar os ativos mais importantes para o homem e para as instituições.

Nesse âmbito desenvolve-se a mais nova área de gestão do Ministério Público brasileiro: a Segurança Institucional. Parte-se de uma ótica macro do Ministério Público, aceitando-o como instituição que possui ativos de diversas espécies que reclamam cada vez mais proteção em razão do incremento constante dos ataques perpetrados, bem como do surgimento de novos riscos e novas ameaças.

Antes, porém, de adentrar ao específico estudo da segurança no seio dessa Instituição, deve-se solidificar a concepção da segurança como um direito fundamental do indivíduo e delimitar a sua conceituação, bem como compreender as percepções da sua ausência, que impactam diretamente a construção de políticas e tomadas de decisões nessa seara.

2. SEGURANÇA COMO DIREITO HUMANO FUNDAMENTAL[2]

O dever estatal de proteção aos interesses essenciais à manutenção da vida social digna, representada pelo concreto exercício de direitos inerentes ao ser humano como a vida, a liberdade e a igualdade, é essencial à concepção atual de Estado e, no caso da República Federativa do Brasil, sedimentada nos alicerces da Democracia e do Direito, encontra-se assegurado por todo ordenamento jurídico, em especial no plano constitucional.

Tal conclusão decorre exatamente da letra do texto da Lei Maior, uma vez que seria inócuo, desarrazoado e irracional, sem a consagração de garantias, proteções e segurança, estabelecer, como fundamentos de constituição estatais, a soberania, a cidadania, a dignidade da pessoa humana, o pluralismo político, os valores sociais do trabalho e da livre

2 Este item foi extraído de estudo realizado no programa de mestrado da Faculdade de Direito do Largo São Francisco, da Universidade de São Paulo, finalizado em 2017: SANTA TERRA JUNIOR, João. **A organização criminosa Primeiro Comando da Capital:** análise das consequências penais da existência do PCC. Dissertação (Mestrado – Programa de Pós-Graduação em Direito Penal, Medicina Forense e Criminologia) – Faculdade de Direito, Universidade de São Paulo, 2017, p. 165/169.

iniciativa; como seus objetivos, a construção de uma sociedade livre, justa e solidária, a garantia do desenvolvimento nacional, a erradicação da pobreza e da marginalização, a redução das desigualdades sociais e regionais, a promoção do bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação; como bases para as relações internacionais, os princípios da independência nacional, da prevalência dos direitos humanos, da autodeterminação dos povos, da não intervenção, da igualdade entre os Estados, da defesa da paz, da solução pacífica dos conflitos, do repúdio ao terrorismo e ao racismo, da cooperação entre os povos para o progresso da humanidade e da concessão de asilo político; e, como pilar dos direitos fundamentais do ser humano, a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade.

Nesse contexto, Bismael B. Moraes correlaciona a existência do Estado Democrático de Direito da República Federativa do Brasil com a preservação da garantia da liberdade e dos direitos à vida e à segurança, asseverando que, para o reconhecimento de um Estado com tais características, não se pode constatar o afastamento dos princípios jurídicos, das garantias fundamentais dos indivíduos e da coletividade (em especial a liberdade) ou dos direitos inerentes à pessoa humana, entre os quais sobressai, além da vida, a segurança, que corresponde a um dever do Estado, externado por todas as suas pessoas jurídico-políticas (União, Estados, Municípios e Distrito Federal).[3]

A aposição da segurança[4] no patamar de direito humano[5] e a sua alocação como objetivo existencial de um Estado já vêm instrumentalizadas desde a Declaração da Virgínia, de 1776 (artigo 3º), da Declaração dos Direitos do Homem e do Cidadão, de 1789 (artigo 2º), e da Constituição Francesa pós-revolução, de 1793, que, em seu artigo 8º, estabeleceu que "a segurança consiste na proteção que a sociedade concede a cada um de seus membros para a conservação de sua pessoa, direitos e propriedades". A Declaração Universal dos Direitos Humanos, adotada e proclamada pela resolução 217 A (III) da Assembleia-Geral das Nações Unidas, em 10 de dezembro de 1948, também qualificava a segurança como um direito inerente ao ser humano (artigo 3º).

Disposições normativas expressas encontram-se em nossa Constituição revelando a correção do raciocínio acima empregado. Tamanha foi a preocupação do constituinte originário de 1988 com a outorga da base

3 MORAES, Bismael B. **Estado e segurança diante do direito.** São Paulo: Revista dos Tribunais, 2008, p. 20.

4 "A origem etimológica da palavra 'segurança', do latim *securus*, aponta para um estado ou situação livre de perigo, sendo corrente entender-se segurança como sinónimo de ausência de perigo" (CAIADO, Ricardo Alexandre Rodrigues. **O sentimento de insegurança e a sua integração com a criminalidade.** 2013. 232 f. Dissertação (Mestrado) – Faculdade de Ciências Jurídico-Políticas, Universidade Autónoma de Lisboa. Lisboa: 2013, p.31).

5 Luciano Oliveira, em estudo pautado em resultados de pesquisas de campo, afirma ser a segurança um direito humano "meio esquecido" ou "no mínimo, pouco citado": "Na verdade, tão raramente nos lembramos disso que seria o caso até de perguntar se algum dia 'soubemos' de tal coisa – isto é, que a segurança, a segurança pessoal, é um dos direitos humanos mais importantes e elementares" (OLIVEIRA, Luciano. Segurança: um direito humano para ser levado a sério. **Anuário dos Cursos de Pós-Graduação em Direito**, Recife: Universidade Federal de Pernambuco – Centro de Ciências Jurídicas – Faculdade de Direito do Recife –, nº 11, p. 241/254, 2000, p. 244).

normativa imprescindível à proteção dos bens e fundamentos reveladores do Estado Democrático de Direito que, repetindo a sistemática dos textos anteriores[6], erigiu a segurança à categoria de direito e garantia fundamental, no *caput* do artigo 5º.[7] Nesse âmbito, Cláudio Pereira de Souza Neto afirma que a segurança foi elevada à condição de direito fundamental pelo artigo 5º da Constituição Federal, em seu *caput*, e que, "como os demais, tal direito deve ser universalizado de maneira igual: não pode deixar de ser prestado à parcela mais pobre da população, ou prestado de modo seletivo".[8]

Explica José Afonso da Silva que "na teoria jurídica a palavra 'segurança' assume o sentido geral de garantia, proteção, estabilidade de situação ou pessoa em vários campos, dependente do adjetivo que a qualifica".[9] Nesse contexto, nossa atual Constituição utiliza, de modo expresso, o termo "segurança" em inúmeras oportunidades, objetivando resguardo dos mais diversos interesses públicos e individuais ("segurança" é empregada, além do artigo 5º, *caput*, 25 vezes, e em outra reservada ao termo "insegurança"): como objetivo do Estado Democrático instituído pela Lei Maior (preâmbulo); para preservação de sigilo das informações públicas necessárias à proteção da sociedade e do Estado (artigo 5º, XXXIII); como instrumento de proteção de direitos líquidos e certos (artigo 5º, LXIX e LXX; artigo 102, I, "d", e II, "a"; artigo 105, I, "b", e II, "b"; artigo 108, I, "c"; artigo 109, VIII; artigo 114, IV; artigo 121, § 3º, e § 4º, V); para proteção dos direitos sociais (artigo 6º, *caput*, e artigo 7º, XXII); para proteção do trânsito (artigo 23, XII); objetivando a proteção do território e do país (artigo 85, IV; artigo 91, § 1º, III; artigo 173; e artigos 35, § 1º, II, e 49, § 3º, do ato das disposições finais e transitórias); para proteção das relações jurídicas em face da divergência de interpretação de normas por órgãos judiciários e da administração pública (artigo 103-A, § 1º); e para preservação da ordem pública e da incolumidade das pessoas e do patrimônio (título do capítulo III; artigo 144, *caput*, § 7º e § 10º).

6 A Constituição de 1824, no seu artigo 179, trazia a "segurança individual" como um dos pilares de garantia dos direitos civis e políticos dos cidadãos brasileiros, mesma expressão empregada no artigo 72 da Constituição de 1891 (na sua Seção II, "Declaração dos Direitos"), no artigo 113 da Constituição de 1934 (no Capítulo II, "Dos Direitos e das Garantias Individuais"), no artigo 122 da Constituição de 1937 (no capítulo "Dos Direitos e Garantias Individuais") e no artigo 141 da Constituição de 1946 (no Capítulo II, "Dos Direitos e das Garantias individuais"), até que, no texto constitucional de 1967, no artigo 150, do Capítulo IV, "Dos Direitos e Garantias Individuais" (e, após a Emenda Constitucional nº 1, de 17 de outubro de 1969, no artigo 153, do capítulo de mesma numeração), passou a adotar somente a palavra "segurança".

7 Luciano de Araujo Migliavacca e Raquel Tomé Soveral, em estudo a respeito da efetividade do Direito por meio da tutela jurisdicional como mecanismo de consagração da segurança jurídica, afirmam que "a Constituição brasileira contemporânea contempla a segurança enquanto um direito fundamental (BRASIL, 1988). Notório que não menciona explicitamente segurança jurídica, mas, apenas segurança, fazendo com que a leitura seja mais ampla, denotando a existência de direitos fundamentais relacionados à segurança – pública, jurídica e social, por exemplo" (Segurança jurídica, jurisdição e efetividade do Direito. **Revista de Processo, Jurisdição e Efetividade da Justiça**, Curitiba, v. 2, nº 2, p. 190-205, jul./dez. 2016, p. 197). Nesse contexto, concluem que, para a efetividade do Direito, não basta a outorga de direitos fundamentais formais, havendo a necessidade de sua concretização, momento em que a prestação da tutela jurisdicional assume papel de relevância para a sedimentação da segurança jurídica vinculada à própria compreensão do Estado contemporâneo. Essa linha de raciocínio, da efetiva aplicação das normas jurídicas por meio da prestação da tutela jurisdicional como fonte de segurança ao usufruto dos direitos fundamentais, é plenamente aplicável às hipóteses de ofensas a bens jurídicos penalmente guarnecidos, seja em razão da maior sedimentação do monopólio estatal jurisdicional nessa espécie de lide, seja em face da maior relevância dos interesses passíveis de proteção (conforme abaixo será demonstrado).

8 SOUZA NETO, Cláudio Pereira de. A segurança pública na Constituição Federal de 1988: conceituação constitucionalmente adequada, competências federativas e órgãos de execução das políticas. **Revista de Direito do Estado**, ano 2, nº 8, p. 19-73, out./dez. 2007, p. 27.

9 SILVA, José Afonso da. **Curso de direito constitucional positivo**. 20. ed. São Paulo: Malheiros, 2002, p. 753.

Contudo, repisa-se a obrigação de ação estatal de concessão de proteção em face de condutas de terceiros, ou de contenção das suas próprias atividades para não lesão aos direitos fundamentais, não é constatada somente nos dispositivos constitucionais em que há o emprego do termo "segurança", sendo uma decorrência de toda a sistemática de outorga dos direitos e das garantias individuais e coletivas. Nesse sentido, Francisco Sannini Neto explica que o direito à segurança se projeta como uma garantia ou até mesmo uma forma de coação contra atos ilegais, que assegura o convívio em sociedade e a concretização dos demais direitos fundamentais, tratando-se de um dever do Estado voltado aos seus tutelados.[10]

A segurança deve ser vista, portanto, com base em uma visão macronormativa, como o conjunto de medidas a serem empreendidas para a proteção do "organismo estatal" (segurança orgânico-institucional), focadas no resguardo dos elementos essenciais à sua existência, ou seja, do seu povo, do seu território e da sua soberania, bem como dos seus princípios fundamentais e dos seus objetivos constitutivos. Nessa órbita, distintas fontes de ameaças e lesões podem ser identificadas, correlacionadas a variáveis objetos de proteção, concretizadas por diversas formas de execução e que, assim, demandam tutelas e atuações estatais específicas como meios de outorga de maior efetividade assecuratória. Nesse contexto é que se fala na identificação de modalidades de segurança, como a segurança jurídica, a segurança social, a segurança do trabalho, a segurança da intimidade, a segurança do domicílio, a segurança nacional e do território, a segurança pública, entre outras vertentes.[11]

Dessa ótica macro, de proteção integral de um "organismo estatal", é que se pretende sedimentar a compreensão da Segurança Institucional do Ministério Público.

3. A DIFICULDADE DE CONCEITUAÇÃO DA SEGURANÇA E AS DIVERSAS PERCEPÇÕES DA INSEGURANÇA

Segurança é termo de difícil conceituação. Assim como se constata no estudo da dignidade (um dos fundamentos de sustentação da República Federativa do Brasil – artigo 1º, III, da Constituição), a concretude da definição de segurança ocorre pelo seu aspecto negativo, ou seja, pelas hipóteses em que se constata a sua falta para o ser humano e para as instituições.

Superficialmente, segurança pode ser compreendida como a ausência de riscos ou de danos aos bens e valores inerentes aos titulares de direitos, os quais denominaremos de "ativos".

10 SANNINI NETO, Francisco. Diferenças entre a polícia investigativa e a polícia judiciária. **Consultor Jurídico**, 1º de março de 2017. Disponível em: <http://www.conjur.com.br/2017-mar-01/francisco-sannini-diferencas-entre-policia-investigativa-judiciaria>. Acesso em: 10 maio 2017.

11 Nesse sentido, Altamiro J. dos Santos, entendendo que segurança jurídica é gênero, enquanto o direito à segurança pública é espécie, afirma: "Examina-se a segurança jurídica individual, social, negocial, política e outras, com o objetivo de apontar princípios para o convívio pacífico; prevenir atrocidade, violência, criminalidade, terrorismo e corrupção contra a vida, integridade psicofísica humana e nas relações, não só em sociedade, mas também entre as pessoas naturais e jurídicas" (**Direito de segurança pública e legítima defesa social**. São Paulo: LTR Editora, 2006, p. 92).

A conceituação de segurança, portanto, está umbilicalmente cindida à sua percepção, pelo titular de direitos, a respeito das hipóteses em que estes podem ser colocados em riscos ou lesados. Por outras palavras: é perceptível, pela sua face negativa (a insegurança), quando ela (segurança) falta, em razão do dano concreto ou da mera sensação de risco de lesão; de outro lado, não ocorrendo ataques ou não sendo notados fatores hostis aos ativos protegidos, ela (segurança) torna-se de difícil percepção, conceituação ou, até mesmo, valorização.

A falta da segurança, ou seja, a insegurança, melhor se qualifica como uma sensação, que é gerada por elementos objetivos e subjetivos.

No plano objetivo, o sentimento de insegurança é ocasionado pela proximidade da ameaça ou do dano ao direito, pelo momento em que a lesão é presenciada, pelo instante em que a pessoa se torna vítima da conduta ilícita ou de um agente da natureza. Corresponde à percepção visual, tátil, auditiva ou captada por outro sentido humano, a respeito da materialização do dano ou do risco de lesão. Trata-se de percepção concreta da iminente e real possibilidade de ocorrer a lesão a um valor de relevância.

No plano subjetivo, ela decorre de pensamentos motivados pela probabilidade de as ameaças e as lesões serem efetivamente concretizadas ao indivíduo, à coletividade ou às instituições. Decorre dos pensamentos humanos, daquilo que se imagina quando se recebe a notícia da ocorrência de dano a terceiro ou da existência de risco de lesão. Não há concreta e iminente possibilidade de sofrer lesão.

Nesse contexto subjetivo, podem ser identificadas diversas fontes produtoras de tais pensamentos, destacando-se a ausência de atuação do Estado para outorga da segurança em casos pretéritos, seja pela não evitação do dano ao direito protegido ("se ocorreu antes e não foi evitado, é possível que ocorra novamente, e, agora, comigo"), seja pela não responsabilização do seu autor (a falta de percepção da punição estatal gera a sensação de falta de controle ao ato lesivo e, em consequência, ocasiona a íntima certeza de que tal danosidade não encontra freios e pode ser repetida a qualquer momento).[12]

O acesso às informações é outra inequívoca fonte produtora de pensamentos de insegurança. Esse acesso é gerado pela circulação de informações originadas do jornalismo (mídia) e da própria coletividade.

É certo que a real sensação de insegurança pressupõe a prévia constatação da sua face objetiva, ou seja, a ocorrência do dano (tomando por base a insegurança pública), porém, o livre acesso às informações pelo uso das novas tecnologias de comunicação, em especial as redes sociais, visualizadas a todo instante pela facilidade dos aparelhos celulares, potencializou essa sensação em níveis nunca constatados.

A maximização da insegurança pelo uso das redes sociais ainda decorre de outra característica da sociedade moderna: cada um entende

12 No tocante às dimensões objetivas e subjetivas da segurança, Ricardo Alexandre Rodrigues Caiado afirma: "A segurança afigura-se como sendo um estado ou condição, podendo igualmente ser considerada um fenômeno psicológico, isto é, a segurança tem uma dimensão objetiva – que é a ausência de riscos –, e uma dimensão subjetiva – que é julgar que esses riscos não existem" (*op. cit.*, p. 32).

a si como fonte produtora de informação, porém, em geral, sem prévio exercício mental a respeito dela; recebe-se uma informação na rede social, e ela é repassada sem o mínimo de preocupação com a checagem da sua credibilidade. Assim, alastram-se, com uma velocidade vertiginosa, boatos e falsas notícias, que acabam por comprometer a sensação de segurança e fomentam a massificação de uma "cultura do medo".

Ademais, o fenômeno da globalização[13], principalmente dos meios de comunicação, ocasionador da vertiginosa rapidez na circulação das informações, amplificou essa "sensação de medo coletivo", em especial com o acompanhamento midiático de desastres naturais, das questões criminais e do intenso multiculturalismo[14]. A respeito da propagação da ideia de *insegurança cognitiva* pela velocidade da comunicação social, Manuel Monteiro Guedes Valente explica

> Esta pluridifusão do crime transforma a vivência de um facto criminoso individual e localizado em comunitário (e societário) e globalizado. Um homicídio ocorrido numa aldeia recôndita de Portugal é, hoje, sentido, vivido e esgrimido (ética, política e juridicamente) em todos os lares e sofre da síndrome de multiplicação pela massificação noticiosa. Esse crime deixa de ser um e passa ao processo da multiplicação pela difusão célere e desgastante. Esta *hipervelocidade* do conhecimento de um crime pode conduzir-nos ao discurso fácil da insegurança e do <<reino da violência>>.[15]

Retornando à já anunciada premissa adotada para a compreensão da Segurança Institucional, qual seja, a compreensão do Ministério Público como um ente que reclama proteção de seus ativos em face das rotineiras ameaças existentes, é inequívoco que não se pode aceitar que a percepção subjetiva de insegurança norteie as ações dos seus gestores. Isso porque:

> Um dos problemas cruciais do enfrentamento do medo ou da sensação subjetiva de insegurança é que as reações defensivas ou agressivas resultantes, destinadas a mitigar o medo, podem assim ser dirigidas para longe dos perigos realmente responsáveis pela suspeita de insegurança.[16]

---

13 "A abertura da sociedade a partir da globalização acentuou esse processo: tragédias, desastres, crimes, ainda que possam ter efeito sob mais de um país, são experiências absorvidas em tempo real em todo o mundo e, naturalmente, vividas com a evidente perda de referência de tempo e espaço" (MORAES, Alexandre Rocha Almeida de. **Direito Penal Racional:** propostas para a construção de uma teoria da legislação e para uma atuação criminal preventiva. Curitiba: Jurua, 2016, p. 117).

14 "Em todo caso, à vista do que vem acontecendo nos últimos anos, é incontestável a correlação estabelecida entre a sensação social de insegurança diante do delito e a atuação dos *meios de comunicação*. Estes, por um lado, da posição privilegiada que ostentam no seio da "sociedade da informação" e no seio de uma concepção do mundo como *aldeia global*, transmitem uma imagem da realidade na qual o que está distante e o que está próximo têm uma presença quase idêntica na forma como o receptor recebe a mensagem. Isso dá lugar, algumas vezes, diretamente a percepções inexatas; e, em outras, pelo menos a uma sensação de impotência. Com mais razão, por outro lado, a reiteração e a própria atitude (dramatização, morbidez) com a qual se examinam determinadas notícias atam como um multiplicador dos ilícitos e catástrofes, gerando uma insegurança subjetiva que não se corresponde com o nível de risco objetivo." (SILVA SÁNCHEZ, Jesús-María. **A expansão do direito penal:** aspectos da política criminal nas sociedades pós-industriais. Tradução de Luiz Otávio de Oliveira Rocha. 3 ed. rev. e atual., São Paulo: Editora Revista dos Tribunais, 2013, p. 47/48).

15 VALENTE, Manuel Monteiro Guedes. **Segurança: bem jurídico supranacional.** JANUS.NET e-journal of International Relations. v. 3, nº 2, outono 2012. Disponível em http://observare.ual.pt/janus.net/pt/n%C3%BAmeros-anteriores/66-portugues-pt/v-3-n-2-2012-outono/artigos/191-pt-pt_vol3_n2_art4, acesso em 18.05.2017.p. 77-78.

16 MORAES, Alexandre Rocha Almeida de. Op. Cit., p. 116.

Como, portanto, realizar o diagnóstico exato dos riscos e das fontes de ataques aos ativos dessa Instituição?

Para o alcance da resposta, algumas premissas devem ser postas: a) o medo, diante da ocorrência das ameaças, dos riscos de lesões e de danos efetivos aos ativos de uma pessoa ou de uma Instituição, é uma consequência natural para o ser humano; b) o medo atrapalha a percepção da segurança, e as decisões do gestor da Instituição dele devem ser afastadas, razão pela qual deve se escorar em assessoramento profissional e blindado a tal mácula; c) o medo, decorrente da face objetiva da (in)segurança, é fundado; d) ao contrário, o medo, resultado da face subjetiva, é infundado.

O essencial, portanto, para a adoção de medidas capazes de prevenir ou neutralizar os danos, é o empreendimento de uma análise de vulnerabilidades objetiva, pautada por uma diversidade de fontes de informações a respeito dos elementos motivadores da possível ação hostil, realizada por órgão isento e previamente capacitado.

Nesse sentido, de acordo com José Luis Gonzáles Cussac e Fernando Flores Giménez, o diagnóstico de uma situação é importante para determinar o comportamento a seguir para fazer frente a ela, e, no âmbito da segurança, é imprescindível afinar o nível de concreção à ideia de ameaça e a suas possibilidades certas de realização. Por outras palavras, compreender do que se trata, quem são seus atores, seu contexto e suas causas, os indicadores que ajudam a determinar sua força, os bens e interesses estratégicos que colocam em risco e os danos que pode provocar.[17] E complementam:

> *Por lo demás, una identificación y caracterización correcta de la amenaza y su grado de riesgo exige también un análisis de sus actores, de su contexto y âmbito geográfico, de sus causas, de sus vectores y potenciadores, así como de los medios utilizados para llevarla a efecto; esa caracterizacion será imprescindible para configurar las respuestas adecuadas.*[18]

E foi, sobre essas premissas, que se escorou a Resolução nº 156, de 13 de dezembro de 2016, do Conselho Nacional do Ministério Público, responsável pela instituição da Política de Segurança Institucional e do Sistema Nacional de Segurança Institucional do Ministério Público, além de outras providências,[19] conforme abaixo indicado.

---

17 GONZÁLES CUSSAC, José Luis; FLORES GIMÉNEZ, Fernando. Seguridad global y derechos fundamentales. Una propuesta metodológica. In: _____; _____ (Coord.). **Seguridad y derechos:** análisis de las amenazas, evaluación de las respuestas y valoración del impacto en los derechos fundamentales. Valência: Tirant lo Blanch, 2018, p. 25/98, p. 51.

18 "De resto, uma identificação e caracterização correta da ameaça e seu grau de risco também requerem uma análise de seus atores, seu contexto e escopo geográfico, suas causas, seus vetores e fomentadores, bem como os meios utilizados para concretiza-la; essa caracterização será essencial para configurar as respostas apropriadas." (tradução livre). *Idem*, p. 54/55.

19 CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO. **Resolução 156, de 13 de dezembro de 2016** – Institui a Política de Segurança Institucional e o Sistema Nacional de Segurança Institucional do Ministério Público, e dá outras providências. Publicada no Diário Eletrônico do CNMP, Caderno Processual, p. 1-11, de 14 de fevereiro de 2017. Disponível em: <http://www.cnmp.mp.br/portal/images/Normas/Resolucoes/RESOLUO_156.pdf>. Acesso em: 24 set. 2019. Verdadeiro antecedente normativo que surgiu de fundamento para o surgimento da Resolução nº 156/CNMP foi a Lei nº 12.694, de 24 de julho de 2012, que, entre outras providências, disciplinou medidas de proteção pessoal de magistrados e promotores de Justiça que atuam no enfrentamento da criminalidade organizada, entre elas a (i) tentativa de despersonalização das decisões judiciais com a criação de órgãos jurisdicionais colegiados de primeira instância para dirimir questões processuais dessa seara; (ii) a autorização para os Tribunais, no âmbito de suas competências, adotarem

4. A SEGURANÇA INSTITUCIONAL DO MINISTÉRIO PÚBLICO: SEGURANÇA ORGÂNICA, SEGURANÇA ATIVA, CONTRAINTELIGÊNCIA E INTELIGÊNCIA.

Concebendo-se o Ministério Público como um ente, uma pessoa (jurídica), um sujeito de direitos, há a necessidade de proteção de seus bens e da sua estrutura integral em prol da consecução das finalidades e funções constitucionalmente determinadas.

Sendo incumbência da Instituição a defesa da ordem jurídica, do regime democrático e dos interesses sociais e individuais indisponíveis (artigo 127, *caput*, da Constituição), é possível concluir que, finalística e funcionalmente observada, a Segurança Institucional do Ministério Público atua para resguardar a hígida e tranquila atuação da Instituição em prol da consecução do direito humano fundamental de segurança para o exercício dos demais direitos fundamentais.

Para tanto, o Ministério Público deve ser compreendido como uma Instituição possuidora de diversos ativos que reclamam proteção, expostos a inúmeras vulnerabilidades decorrentes de deficiências de segurança e de ações adversas provenientes de variadas fontes produtoras, bem como de fatores naturais vulnerantes.

Desse contexto, portanto, emana a terminologia Segurança Institucional, ou seja, de proteção integral a todos os ativos da Instituição Ministério Público: pessoas, instalações, materiais, informações e imagem. Essa proteção, conforme dispõe o artigo 3º da Resolução nº 156, de 13 de dezembro de 2016, do Conselho Nacional do Ministério Público, "compreende o conjunto de medidas voltadas a prevenir, detectar, obstruir e neutralizar ações de qualquer natureza que constituam ameaça à salvaguarda da Instituição e de seus integrantes, inclusive à imagem e reputação".

Como acima ressaltado, o gestor do Ministério Público, diante do conhecimento de possíveis ameaças aos ativos da instituição, deve se afastar das percepções subjetivas de insegurança. Para tanto, deve aparelhar a Instituição com um órgão previamente capacitado para a realização de análises objetivas de vulnerabilidades, responsável pelo gerenciamento da segurança dos diversos ativos, fomentando a união e agregando esforços das diversas áreas da administração da Instituição e dos diversos órgãos de execução que a integram.

Nesse sentido, a referida Resolução nº 156 do Conselho Nacional do Ministério Público, em seu artigo 22, estabelece às Procuradorias-Gerais dos Ministérios Públicos diversas atribuições em prol de uma gestão estratégica da Segurança Institucional, em especial: a instituição daquele mencionado órgão de Segurança Institucional, incumbido da criação de mecanismos para garantir as atividades de gerência, fiscalização, auditoria e validação

medidas para reforçar a segurança dos prédios da Justiça; (iv) regramentos a respeito da proteção pessoal de autoridades e de seus familiares, decorrente de situação de risco em razão do exercício da função pública, que deve ser comunicada ao Conselho Nacional de Justiça ou ao Conselho Nacional do Ministério Público; (v) a possibilidade de criação de órgãos de segurança institucionais do Judiciário e do Ministério Público; (vi) a possibilidade de troca de placas de veículos de magistrados e membros do Ministério Público.

de processos sensíveis (as Assessorias ou Coordenadorias de Segurança Institucional), tendo como responsável um membro da Instituição; a criação de um comitê vinculado ao Procurador-Geral para gestão da Segurança Institucional e articulação sistêmica de medidas para a concretização de ações dessa área (os Comitês de Segurança Institucional); a edição de política e de plano de Segurança Institucional, bem como de planos de segurança orgânica e normas e procedimentos necessários à execução de tais planos.

O órgão de Segurança Institucional, assim, (i) atuará como um elemento fomentador de providências e medidas de todas as áreas da Instituição em prol do estabelecimento de barreiras às ações adversas e da contenção dos danos já ocasionados aos ativos, (ii) deverá ser responsável pela análise dos riscos e das vulnerabilidades do Ministério Público, gerando conhecimento e empregando ações para evitar que técnicas de inteligência tenham êxito contra a Instituição, ou para neutralizá-las, (iii) bem como zelará pela difusão e sedimentação da cultura da segurança.

Essa divisão das funções do órgão de Segurança Institucional decorre do principal regramento da área, a Resolução nº 156/2016 do Conselho Nacional do Ministério Público. Porém, deve-se ressaltar que o desenvolvimento de medidas para proteção de um organismo estatal é matéria atinente ao grande estudo da inteligência e, de acordo com as peculiaridades de cada órgão, constata-se o emprego de terminologias diversas e de bases finalístico-doutrinárias distintas.

Nesse sentido, por exemplo, André Haydt Castello Branco, Fred Harry Schauffert e Luiz Otávio Botelho Lento explicam que as funções acima indicadas compõem a Contrainteligência, que teria, assim, como seus seguimentos: "Segurança Ativa (SEGAT), Segurança de Assuntos Internos (SAI) e Segurança Orgânica (SEGOR)".[20]

Já Miguel A. Esteban Navarro explica que tais funções também compõem a Contrainteligência, seccionadas em duas vertentes: a segurança defensiva, consistente em resguardar as instalações para evitar a intrusão de elementos estranhos, em proteger as pessoas contra possíveis ameaças, em defender o desenvolvimento das operações em curso e em preservar as informações sensíveis;[21] e a contraespionagem, que se refere à identificação de adversários concretos e específicos e produção de conhecimento detalhado a respeito das operações que estão planejando ou desenvolvendo para impedir e desativar sua execução.[22]

20 BRANCO, André Haydt Castello; SCHAUFFERT, Fred Harry; LENTO, Luiz Otávio Botelho. **Inteligência e segurança pública:** livro didático. Palhoça: Unisul Virtual, 2014, p.87.

21 "La seguridad defensiva consiste en resguardar las instalaciones para evitar la intrusión de elementos ajenos, proteger el personal contra la acción de posibles amenazas, defender el desarrollo de las operaciones en curso y preservar información sensible" (ESTEBAN NAVARRO, Miguel A. Contrainteligencia y operaciones encubiertas. In: GONZÁLEZ CUSSAC, José Luis (Coord.). **Inteligencia.** Valência: Tirant lo blanch, 2012, p. 173).

22 "El contraespionaje consiste en identificar adversarios concretos y específicos y produzir conocimiento detallado acerca de las operaciones que están planificando o desarrollando para impedir y desactivar su ejecución" (idem, p. 176). Ressalta-se, contudo, que a concepção de Contrainteligência decorre originalmente do âmbito de atuação das forças militares para a proteção do Estado contra as ações de forças externas inimigas, conforme bem explicado por Carolina Andrade Quevedo (Contrainteligencia. In: DÍAZ FERNÁNDEZ, Antonio M. **Conceptos fundamentales de inteligencia.** Valência: Tirant lo blanc, 2016, p. 65/72), sendo, portanto, no âmbito da Segurança Institucional, os seus fundamentos adaptados à proteção dos organismos internos que compõem o Estado.

Contudo, essa não foi a disposição das funções da Segurança Institucional na referida Resolução.

Ainda que a Resolução CNMP nº 156/2016 não tenha se dedicado ao fornecimento da exata definição, o desempenho da primeira função acima indicada corresponderia à denominada segurança orgânica, ou seja, ao desenvolvimento, pelo Ministério Público, de ações e medidas, em todas as áreas da Instituição, para a aposição de barreiras às ações adversas e para a proteção dos seus ativos. De acordo com o seu artigo 2º, § 2º, a segurança orgânica é composta pelos seguintes grupos de medidas: I – segurança de pessoas; II – segurança do material; III – segurança das áreas e instalações; IV – segurança da informação. Nesse âmbito, exemplificativamente, podem ser elencadas a adoção de sistemas de vigilância predial (vigilância humana e tecnológica e barreiras físicas), a delimitação de áreas de acesso, a instalação de *softwares* protetivos dos sistemas tecnológicos de informação contra invasões externas, o uso de tecnologia para proteger a transmissão das informações da Instituição, a análise dos processos seletivos do material humano permanente e transitório, o emprego de operações de segurança de pessoas, a adoção de termo de compromisso de manutenção de sigilo (TCMS), a classificação de documentos sensíveis, o treinamento de servidores e membros para a detecção de fontes de ameaças, entre tantas outras medidas destinadas à proteção dos ativos da Instituição: pessoas, materiais, áreas, instalações, dados e informações (artigos 4º ao 11, da Resolução CNMP nº 156/2016).

No tocante à segunda função, de acordo com os artigos 3º, § 3º, e 12 a 15 da referida Resolução, corresponde à segurança ativa, que compreende ações de caráter proativo e ao conjunto de medidas voltadas à prevenção, à detecção, à obstrução e à neutralização de ações de contrassabotagem (ações intencionais contra material, áreas ou instalações da Instituição que possam causar interrupção de suas atividades e/ou impacto físico direto e psicológico indireto sobre seus integrantes), contraespionagem (ações adversas e dissimuladas de busca de informações sensíveis ou sigilosas), contra crime organizado (ações adversas oriundas de organizações criminosas) e contrapropaganda (ações representativas de risco de abusos, desinformações e publicidade enganosa de qualquer natureza contra a Instituição).

Existe, portanto, similaridade de todo esse conjunto de medidas, ações, providências, produção e gestão de conhecimento com aquilo que foi desenvolvido dentro dos setores de inteligência de Estado sob a denominação de Contrainteligência.

De acordo com Joanisval Brito Gonçalves, a Contrainteligência é função indissociável da inteligência e deve ser entendida, "em sentido amplo, como as atividades e procedimentos que têm por objetivo neutralizar a Inteligência adversa e salvaguardar o conhecimento produzido" (p. 89), tendo por objetivo, portanto, "tornar tão difícil quanto possível as ações adversas, tomando medidas de segurança que impeçam o acesso a tudo que se deseja manter sob sigilo e protegendo pessoas e instalações" (p. 91).[23]

23 GONÇALVES, Joanisval Brito. **Atividade de inteligência e legislação correlata**. 5ª ed. Niterói: Impetus, 2017, p. 89 e 91.

Para o exercício, portanto, da atividade de Segurança Institucional em sua completude, é imprescindível que se compreendam os órgãos ministeriais responsáveis pela sua tutela, antes de tudo, como agências de inteligência. Por essa razão o artigo 7º, § 4º, da Resolução CNMP nº 156/2016, determina que:

> os ramos do Ministério Público deverão proporcionar ao órgão de Segurança Institucional o acesso aos bancos de dados e sistemas da Instituição, ou de acesso da Instituição, para subsidiar as respectivas atividades de Segurança Institucional, inteligência e Contrainteligência, observados os procedimentos de segurança e controle.

De fato, para o efetivo, exato e completo diagnóstico objetivo das vulnerabilidades da Instituição, bem como dos riscos de ameaças de dano a que está exposta, é imprescindível a formação de conhecimento segundo dados plúrimos, decorrentes de diversas fontes, sobre os quais se deve aplicar técnicas de aferição de credibilidade e confiabilidade para processamento final da informação que será destinada à formação do gestor do Ministério Público para a adoção de medidas de segurança orgânica ou o emprego de ações de segurança ativa em prol da proteção dos ativos da Instituição.

Trata-se de emprego do "ciclo de inteligência" na atividade de Segurança Institucional. Andrés de Castro García explica que "o ciclo de inteligência é um processo composto por diferentes etapas ou fases, que serve como referência teórica para ilustrar a produção de inteligência".[24] Tais fases seriam:[25] 1ª) planejamento e direção, na qual se determinam quais são as necessidades de inteligência que devem ser priorizadas, ou seja, com base no diagnóstico dos exatos objetivos da produção do conhecimento, com o recebimento do requerimento de sua produção, passa-se à análise das necessidades do destinatário, as quais devem estar expressadas de maneira mais clara possível para não afetar o bom desenvolvimento das fases seguintes; 2ª) obtenção de dados, por meio de distintos tipos de fontes que terão cada uma suas particularidades, sendo recomendável o acesso à maior quantidade de dados para possibilitar contrastá-los e manter um alto nível de confiabilidade; 3ª) processamento dos dados, consistente na análise técnica, armazenamento ordenado, controle e posterior conservação de maneira segura; 4ª) produção de inteligência, na qual os dados convertem-se em informação de inteligência por meio de uma séria de sub etapas: 4.a) avaliação, consistente em saber qual parte do dado recebido deve ser rechaçado por incompleto ou por ser pouco confiável, observando-se a qualidade da fonte e da qualidade do dado dela decorrente; 4.b) integração, na qual são reunidos todos os dados disponíveis procedentes das distintas fontes para comparação, a fim de alcançar o grau de confiabilidade; 4.c) análise, concretizada por um exame sistemático dos dados reunidos que permite compreender a complexidade do fenômeno analisado e apresentá-lo de maneira contextualizada, oferecendo assim resposta à necessidade

24 *"El ciclo de inteligencia es un proceso compuesto por diferentes etapas o fases, que sirve como referencia teórica para ilustrar la producción de inteligencia"* (CASTRO GARCÍA, Andrés. Ciclo de inteligencia. In: DÍAZ FERNÁNDEZ, Antonio M. **Conceptos fundamentales de inteligencia.** Valência: *Tirant lo blanc*, 2016, p. 53).

25 Idem, p. 53-55.

de interpretação pela qual o analista coloca suas capacidades a serviço da contextualização dos dados recebidos e consegue outorgar-lhes mais valor como resultado de sua especialização; 5ª) difusão, momento em que o destinatário recebe o produto de inteligência que resultou do ciclo descrito, devendo ser verificado, nessa fase, quanto ao produto, a sua a pertinência (produto atende ao fim desejado), a sua confiabilidade, a sua oportunidade (difusão no tempo adequado para a tomada de decisão), bem como que ele seja transmitido com segurança ao destinatário, para que pessoas ou instituições alheias tenham acesso.[26]

Por fim, compete ao órgão de Segurança Institucional do Ministério Público a disseminação da cultura da segurança dos seus ativos. É imprescindível, à proteção integral da Instituição, que todos os seus componentes humanos recebam constantes informações a respeito das vulnerabilidades e dos possíveis danos, bem como de medidas preventivas e reativas a tais ameaças. Ademais, o treinamento e a capacitação de servidores e membros são tarefas a serem implementadas constantemente pelo órgão de Segurança Institucional.

5. CONCLUSÃO

O presente trabalho almejou, inicialmente, a apresentação de embasamento doutrinário a respeito da fundamentação constitucional e normativa para a estruturação da Segurança Institucional no Ministério Público brasileiro. Na sequência, pretendeu-se delinear os contornos funcionais dessa nova área inerente à gestão da Instituição, pautando-se pelas disposições do principal regramento atual, a Resolução CNMP nº 156/2016, bem como pela demonstração dessa atividade com as bases da Contrainteligência de Estado.

Contudo, considerando a exata temática eleita, objetivando a ampla abordagem das premissas que se entendem imprescindíveis para a sedimentação da Segurança Institucional no Ministério Público, terminamos este escrito com a mutação da abordagem teórica para a apresentação de aspectos práticos entendidos como imprescindíveis nesse contexto. Por outras palavras, para que a Segurança Institucional efetivamente seja implantada e a política de gestão dela decorrente seja respeitada (nos exatos termos delineados pela Resolução CNMP nº 156/2016), não basta que o ramo do Ministério Público crie, por ato normativo interno, uma assessoria ou uma coordenadoria de Segurança Institucional:

– deve o maior gestor da Instituição ter a exata percepção não apenas da importância da segurança para a manutenção das funções do Ministério Público, mas, também, das atividades inerentes a tal área, da sua relevância estratégica e da imprescindibilidade de proteção do conhecimento produzido para tal gestor; sem prejuízo, as Procuradorias-Gerais devem compreender que sem aparato humano, material e tecnológico hábil é

26 Andrés de Castro García explica que essas fases são aquelas consideradas clássicas, existindo autores que contemplam um passo adicional, correspondente à avaliação ou retroalimentação, consistente na indicação, pelo destinatário, qual parte e em que grau o produto de inteligência foi mais útil para a tomada de decisão (idem, p. 55).

impossível a estruturação desse setor para o desenvolvimento de todas as suas amplas tarefas;

– o órgão de Segurança Institucional, como já afirmado pela Resolução CNMP nº 156/2016, deve ter amplo e irrestrito acesso a todos os dados da Instituição, bem como a maior diversidade possível de fontes abertas e fechadas, principalmente bancos de dados de outros órgãos públicos;

– o coordenador de Segurança Institucional deve compreender que não é possível, por um único setor da Instituição, alcançar a proteção integral dos ativos; deve, assim, ser um integrador de ações a serem desenvolvidas pelas mais diversas áreas da gestão do Ministério Público, cada uma vinculada a um ativo a ser protegido, por exemplo: a assessoria de comunicação deve ser integrada nas ações de proteção da imagem institucional; a diretoria de patrimônio deve ser ativamente instada para a consecução de medidas de proteção de materiais, áreas e instalações; o órgão policial parceiro (nos Ministérios Públicos dotados de assessorias policiais ou Casas Militares) deve ser inserido no sistema de proteção pessoal de membros e servidores; o setor de tecnologia da informação deve ser incumbido da execução de medidas de proteção dos dados armazenados em bancos da dados da Instituição, bem como daqueles que circulam em razão da concretização das funções administrativas e de execução;

– deve-se, com urgência, ocorrer a estruturação normativa da Contrainteligência e da inteligência no Ministério Público brasileiro, com a compreensão da segurança como princípio máximo legitimador de tais atividades, objetivando respaldar o ciclo de produção do conhecimento, em especial o acesso aos dados necessários para a concretização das análises objetivas de vulnerabilidades e dos diagnósticos de ameaças aos ativos (ainda que as doutrinas específicas de outras Instituições sejam de elevada valia e apurada técnica, o Ministério Público é instituição peculiar e possui demandas próprias que devem ser consideradas no momento de avaliar as técnicas de produção do conhecimento, a manutenção do sigilo do seu produto e, principalmente, a transmissão da informação para os destinatários);

- por fim, devem os ramos do Ministério Público regulamentarem, no seu âmbito interno, a sua específica política de Segurança Institucional, por meio de atos normativos, protocolos de segurança e portarias específicas, capazes de materializar as diretrizes da segurança orgânica e da segurança ativa, de estruturar o trâmite seguro de documentos e informações com o gestor e com os órgãos de execução, bem como de preservar o sigilo e o segredo inerentes ao exercício da atividade de Segurança Institucional.

Essas, portanto, são as premissas doutrinárias e práticas que se entende mínimas para a estruturação da atividade da Segurança Institucional no Ministério Público Brasileiro, área de gestão que, como ressaltado no início deste texto, apresenta-se atualmente imprescindível para que tal Instituição exerça, com regularidade, suas funções constitucionais, e, assim, continue atuando em prol da proteção do destinatário único do seu labor, a sociedade.

6. REFERÊNCIAS

ANDRADE QUEVEDO, Carolina. Contrainteligencia. In: DÍAZ FERNÁNDEZ, Antonio M. **Conceptos fundamentales de inteligencia**. Valência: Tirant lo blanc, 2016.

BRANCO, André Haydt Castello; SCHAUFFERT, Fred Harry; LENTO, Luiz Otávio Botelho. **Inteligência e segurança pública:** livro didático. Palhoça: Unisul Virtual, 2014.

CAIADO, Ricardo Alexandre Rodrigues. **O sentimento de insegurança e a sua integração com a criminalidade**. 2013. 232 f. Dissertação (Mestrado) – Faculdade de Ciências Jurídico-Políticas, Universidade Autónoma de Lisboa. Lisboa: 2013.

CASTRO GARCÍA, Andrés. Ciclo de inteligencia. In: DÍAZ FERNÁNDEZ, Antonio M. **Conceptos fundamentales de inteligencia**. Valência: Tirant lo blanc, 2016.

CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO. **Resolução 156, de 13 de dezembro de 2016 –** Institui a Política de Segurança Institucional e o Sistema Nacional de Segurança Institucional do Ministério Público, e dá outras providências. Publicada no Diário Eletrônico do CNMP, Caderno Processual, p. 1-11, de 14 de fevereiro de 2017. Disponível em: <http://www.cnmp.mp.br/portal/images/Normas/Resolucoes/RESOLUO_156.pdf>. Acesso em: 24 set. 2019.

ESTEBAN NAVARRO, Miguel A. Contrainteligencia y operaciones encubiertas. In: GONZÁLEZ CUSSAC, José Luis (Coord.). **Inteligencia**. Valência: Tirant lo blanch, 2012.

GONÇALVES, Joanisval Brito. **Atividade de inteligência e legislação correlata**. 5. ed. Niterói: Impetus, 2017.

GONZÁLES CUSSAC, José Luis; FLORES GIMÉNEZ, Fernando. Seguridad global y derechos fundamentales. Una propuesta metodológica. In: _____; _____ (Coord.). **Seguridad y derechos:** análisis de las amenazas, evaluación de las respuestas y valoración del impacto en los derechos fundamentales. Valência: Tirant lo Blanch, 2018.

MIGLIAVACCA, Luciano de Araújo; SOVERAL, Raquel Tomé. Segurança jurídica, jurisdição e efetividade do Direito. **Revista de Processo, Jurisdição e Efetividade da Justiça**, Curitiba, v. 2, nº 2, jul/dez 2016.

MORAES, Alexandre Rocha Almeida de. **Direito Penal Racional:** propostas para a construção de uma teoria da legislação e para uma atuação criminal preventiva. Curitiba: Juruá, 2016.

MORAES, Bismael B. **Estado e segurança diante do direito**. São Paulo: Revista dos Tribunais, 2008.

OLIVEIRA, Luciano. Segurança: um direito humano para ser levado a sério. **Anuário dos Cursos de Pós-Graduação em Direito**, Recife: Universidade Federal de Pernambuco (Centro de Ciências Jurídicas – Faculdade de Direito do Recife), nº 11, 2000.

SANNINI NETO, Francisco. Diferenças entre a polícia investigativa e a polícia judiciária. **Consultor Jurídico**, 1º de março de 2017. Disponível em: <http://www.conjur.com.br/2017-mar-01/francisco-sannini-diferencas-entre-policia-investigativa-judiciaria>. Acesso em: 10 maio 2017.

SANTA TERRA JÚNIOR, João. **A organização criminosa Primeiro Comando da Capital:** análise das consequências penais da existência do PCC. Dissertação (Mestrado – Programa de Pós-Graduação em Direito Penal, Medicina Forense e Criminologia) – Faculdade de Direito, Universidade de São Paulo, 2017.

_____. Breve análise das atuais modificações legislativas relativas ao combate à criminalidade organizada decorrentes da lei 12.694, de 24 de julho de 2012. **Revista Jurídica O Saber Completamente**, v. 1, nº 3, maio/2013.

SANTOS, Altamiro J. dos. **Direito de segurança pública e legítima defesa social**. São Paulo: LTR Editora, 2006.

SILVA, José Afonso da. **Curso de direito constitucional positivo**. 20. ed. São Paulo: Malheiros, 2002.

SILVA SÁNCHEZ, Jesús-María. **A expansão do direito penal:** aspectos da política criminal nas sociedades pós-industriais. Tradução de Luiz Otávio de Oliveira Rocha. 3 ed. rev. e atual., São Paulo: Editora Revista dos Tribunais, 2013.

SOUZA NETO, Cláudio Pereira de. A segurança pública na Constituição Federal de 1988: conceituação constitucionalmente adequada, competências federativas e órgãos de execução das políticas. **Revista de Direito do Estado**, ano 2, nº 8, p. 19-73, out./dez. 2007.

VALENTE, Manuel Monteiro Guedes. **Segurança:** bem jurídico supranacional. JANUS.NET *e-journal of International Relations*. v. 3, nº 2, outono 2012. Disponível em: <http://observare.ual.pt/janus.net/pt/n%C3%BAmeros-anteriores/66-portugues-pt/v-3-n-2-2012-outono/artigos/191-pt-pt_vol3_n2_art4>. Acesso em: 18 maio 2017.

A CONTRAINTELIGÊNCIA NO MINISTÉRIO PÚBLICO BREVES CONSIDERAÇÕES

Jerusa Capistrano Pinto Bandeira[1]

SUMÁRIO: 1. Introdução. 2. Contrainteligência: conceito. 2.1 Segurança Orgânica. 2.2 Segurança Ativa 3. A Importância da Estruturação da Contrainteligência no Ministério Público. 4. Conclusão. 5. Referências.

RESUMO: O Ministério Público é instituição permanente à qual incumbe a defesa da ordem jurídica, do regime democrático e dos interesses sociais e individuais indisponíveis, para além da compreensão do relevante trabalho realizado diuturnamente por membros e servidores, o que o coloca como protagonista no cenário nacional por sua atuação em questões relevantes para o País, tendo, inclusive, sido reconhecida como atividade de risco. Necessário despertar para a importância de desenvolver no âmbito da Instituição a atividade de Inteligência, compreendendo a vantagem estratégica que o assessoramento pode fornecer ao decisor. Sob esse aspecto e considerando a importância de todos os ativos que formam a instituição, urge despertar o Ministério Público para a importância da estruturação normativa, técnica e operacional de um órgão de Contrainteligência dentro da Instituição, realizando a tarefa com profissionalismo e capacitação adequada, respeitando a metodologia e as técnicas próprias desenvolvidas na atividade de inteligência. A Contrainteligência é uma proteção, um escudo que mitiga riscos, diminui vulnerabilidades e pode antecipar ameaças, permitindo à instituição deter uma vantagem estratégica contra agentes hostis. Esse texto abordará as diretrizes básicas para a estruturação de um órgão de Contrainteligência no Ministério Público.

PALAVRAS-CHAVE: Ministério Público. Atividade de Inteligência. Contrantrainteligência. Segurança orgânica. Segurança ativa. Estruturação: diretrizes básicas.

1 Promotora de Justiça do Ministério Público do Estado do Maranhão. Coordenadora de Assuntos Estratégicos e Inteligência do MPMA. Membro Colaboradora da Comissão de Preservação da Autonomia do Ministério Público (CPAMP), do Conselho Nacional do Ministério Público na área de Segurança Institucional. Membro integrante da Secretaria Executiva de Segurança Institucional (SESI), do Sistema Nacional de Segurança Institucional do Ministério Público.

1. INTRODUÇÃO

O Ministério Público, como disposto no texto Constitucional, é instituição permanente à qual incumbe a defesa da ordem jurídica, do regime democrático e dos interesses sociais e individuais indisponíveis. O trabalho desenvolvido diariamente por membro e servidores do Ministério Público, além de relevante para sociedade, já foi reconhecido também como atividade de risco pelo Conselho Nacional do Ministério Público (CNMP), por meio do Procedimento de Controle Administrativo nº 1.0029/2015-49.

Assim, dispõem os artigos 127 e 129 da Carta Magna:

> Art. 127. O Ministério Público é instituição permanente, essencial à função jurisdicional do Estado, incumbindo-lhe a defesa da ordem jurídica, do regime democrático e dos interesses sociais e individuais indisponíveis.
>
> Art. 129. São funções institucionais do Ministério Público:
>
> I - promover, privativamente, a ação penal pública, na forma da lei;
>
> II - zelar pelo efetivo respeito dos poderes públicos e dos serviços de relevância pública aos direitos assegurados nesta Constituição, promovendo as medidas necessárias a sua garantia;
>
> III - promover o inquérito civil e a ação civil pública, para a proteção do patrimônio público e social, do meio ambiente e de outros interesses difusos e coletivos;
>
> IV - promover a ação de inconstitucionalidade ou representação para fins de intervenção da União e dos Estados, nos casos previstos nesta Constituição;
>
> V - defender judicialmente os direitos e interesses das populações indígenas;
>
> VI - expedir notificações nos procedimentos administrativos de sua competência, requisitando informações e documentos para instruí-los, na forma da lei complementar respectiva;
>
> VII - exercer o controle externo da atividade policial, na forma da lei complementar mencionada no artigo anterior;
>
> VIII - requisitar diligências investigatórias e a instauração de inquérito policial, indicados os fundamentos jurídicos de suas manifestações processuais;
>
> IX - exercer outras funções que lhe forem conferidas, desde que compatíveis com sua finalidade, sendo-lhe vedada a representação judicial e a consultoria jurídica de entidades públicas.

O Ministério Público trata-se de uma Instituição independente, ao qual a Constituição incumbe relevantes atribuições, tanto na esfera cível quanto criminal, deliberando o Plenário do STF, no ano de 2015, ao julgar o Recurso Extraordinário 593727, a legitimidade do Ministério Público para promover investigações de natureza penal, de forma direta.

Nesse diapasão, necessário despertar para importância da atividade de inteligência, que também abrange a contrainteligência, como mecanismo para alcançar um conhecimento que possa ser utilizado como vantagem, especialmente em nível estratégico e tático, e para a proteção e salvaguarda dos ativos da instituição.

Sobre o tema:

> A atividade de Inteligência compreende a obtenção e o processamento de um conjunto de ativos informacionais que são de interesse de uma organização ou entidade visando a produção de determinados conhecimentos que possam vir a gerar influencias em determinados juízos, ações e comportamentos, em especial no tocante à influências para os processos decisórios voltados para as pessoas, à sociedade e ao Estado.
>
> A necessidade de contornar incertezas, reduzir riscos, perigos e ameaças obrigou as sociedades desde tempos remotos a buscar obter novos conhecimentos capazes de favorecer as vantagens principalmente nos campos territorial, diplomático, econômico, geopolítico, com posições de prevalência, bem como atuações decisivas em campos de batalhas visando o atendimento de seus objetivos nacionais.[2]

A atividade de Inteligência inicialmente restrita aos campos militares hoje é tema presente em Governos e entidades públicas e privadas, vez que atua permitindo que o decisor vislumbre oportunidades e mitigue riscos.

Necessário vencer o desafio de apresentar a atividade de inteligência voltada para o fim a que se destina, de forma imparcial e sem partidarismos, desmistificando antigas noções da atividade e reconhecendo seu uso legítimo nos regimes democráticos de direito e nas instituições que o compõem.

Ainda, importa avançar para a profissionalização da atividade no âmbito do Ministério Público brasileiro, para a estruturação de normas, procedimentos, protocolos que balizarão a atividade e a execução de operações para coleta e busca de dados.

A estruturação da atividade no Ministério Público permitirá ainda sua entrada na comunidade de inteligência de forma mais adequada, vez que canais técnicos e próprios serão criados para o trânsito de informações classificadas.

Mostra-se premente, dado o cenário atual, que se realizem os avanços e investimentos necessários para dotar o Ministério Público da capacidade de uma atuação proativa e segura, na tomada de decisões e na salvaguarda e proteção dos seus ativos.

Quando se compreende o fim a que se destina a atividade de inteligência, qual seja assessoramento estratégico de um decisor, verifica-se seu caráter de imprescindibilidade.

A atividade de inteligência no Brasil passou por diversas mudanças desde sua implementação, na década de 20, com a criação do Conselho de Defesa Nacional, até o desenvolvimento do Sistema Brasileiro de Inteligência, congregando diversas agências federais, sob a coordenação de um órgão central, a Agência Brasileira de Inteligência (ABIN).

A partir da década de 60, com a criação do Serviço Nacional de Informação (SNI), até o processo de redemocratização, na década de 80,

2 PAULA, GIOVANI DE. Atividade de Inteligência de Segurança Pública: um modelo de conhecimento aplicável aos processos decisórios para a prevenção e segurança no trânsito. Santa Catarina: Universidade Federal de Santa Catarina, 2013. p. 35.

associou-se a uma atuação estigmatizada, à época dos governos militares, tanto que houve a extinção do SNI, no ano de 1990, pelo então Chefe do Executivo Fernando Collor de Melo.

Somente em 1999, no governo de Fernando Henrique Cardoso, foi idealizado o Sistema Brasileiro de Inteligência (SISBIN) e criada a agência central de inteligência ABIN, com enfoque na integração, articulação e cooperação entre todos os órgãos de inteligência, na esfera federal.

Na estrutura de um Estado Democrático de Direito, não se concebe a atividade de inteligência atuando fora dos preceitos constitucionais e normativos legais.

A Lei nº 9883, de 7 de dezembro de 1999, em seu art. 5º estabelece que a Política Nacional de Inteligência será executada pela ABIN; contudo, por muitos anos, o País manteve-se silente quanto à elaboração, edição e publicação de uma Política Nacional de Inteligência, sendo esta finalmente publicada por meio do Decreto nº 8.793, de junho de 2016. Tal demora evidencia a forma como a atividade de inteligência é vista no País, sem que lhe seja atribuída a relevância de sua correta e alinhada execução.

Os dois grandes ramos da atividade de inteligência são: Inteligência e Contrainteligência. Enquanto a primeira visa a produzir conhecimento para assessorar o decisor estratégico, a segunda busca, também, a coleta e análise de dados, mas com o fim precípuo da salvaguarda do conhecimento produzido, da instituição, e dos ativos que a formam.

2. CONTRAINTELIGENCIA: CONCEITO

O conceito de Contrainteligência (CI) descrito no art. 3º da Lei nº 9.993/199, que institui o SISBIN e cria a ABIN tem enfoque específico na neutralização da inteligência adversa.

Já o Decreto nº 4.376/2002, que dispõe sobre a organização e funcionamento do SISBIN, em seu art. 3º amplia o conceito de CI e a define como atividade que objetiva prevenir, detectar, obstruir e neutralizar a inteligência adversa.

Notadamente o escopo da atividade é ampliado, indicando uma atuação proativa da Contrainteligência.

Nesse sentido

> O Decreto nº 4.376/02, além do verbo neutralizar, acrescenta ao objetivo da contrainteligência a função de: prevenir, detectar e obstruir a inteligência adversa. Destaca ainda este mesmo decreto que estes — verbos devem combater, além da inteligência adversa, ações de qualquer natureza que constituam ameaça à —salvaguarda de dados, informações e conhecimentos de interesse da segurança da sociedade e do Estado, bem como das áreas e dos meios que os retenham ou em que transitem (BRASIL, 2002). Observe que desta definição já se pode extrair tópicos que fundamentarão a divisão e as características do ramo da contrainteligência. Perceba que o verbo prevenir, dentro do ramo da contrainteligência, tem o significado de agir com antecedência às ações adversas; o verbo detectar pode significar identificar ou

> revelar as ações,ou agente adverso, antes de se efetivar o ataque; o verbo obstruir tem como função parar a ação adversa em andamento; e por fim, o verbo neutralizar, dá o entendimento de anular uma ação adversa que já afetou a segurança dos dados, informações, conhecimentos, áreas ou meios da inteligência a serem protegidos. Segundo a doutrina clássica a contrainteligência é dividida em dois seguimentos: a segurança orgânica e a segurança ativa.[3]

O Conselho Nacional do Ministério Público, pela Resolução nº 156/17, que instituiu a Política de Segurança Institucional do Ministério Público, dispôs no art. 3º:

> Art. 3º A segurança institucional compreende o conjunto de medidas voltadas a prevenir, detectar, obstruir e neutralizar ações de qualquer natureza que constituam ameaça à salvaguarda da Instituição e de seus integrantes, inclusive à imagem e reputação.
>
> §1 As medidas a que se reporta o caput compreendem a segurança orgânica e a segurança ativa

Nota-se a semelhança dos conceitos com a utilização, inclusive, dos mesmos verbos aqui voltados não para a inteligência adversa, mas para ações de qualquer natureza que atentem contra o Ministério Público e seus ativos.

Sem aprofundar, apenas para pontuar, necessário esclarecer que contrainteligência e segurança institucional possuem matizes semelhantes, o diferencial é a possibilidade naquela da busca do dado negado, de acordo com doutrina e técnicas operacionais próprias, e o método utilizado para produção do conhecimento, processo que necessita da observância rigorosa de determinadas etapas até que se formalize um documento de inteligência. O ciclo de produção do conhecimento (CPC) se divide em três grandes momentos: orientação, produção e utilização.

De forma simples, pode-se inferir que a orientação se baseia na necessidade do decisor ou da agência, com base em suas diretrizes. A produção é a aplicação do método próprio e específico para que, ao final, seja produzido um documento de inteligência. A utilização se traduz na entrega ou difusão do conhecimento ao decisor, sendo o ciclo realimentado constantemente.

A contrainteligência estrutura-se sob dois grandes grupos: segurança orgânica e segurança ativa.

2.1. SEGURANÇA ORGÂNICA

Segurança orgânica abrange a segurança de pessoas, áreas e instalações, material e informação. Sob este aspecto, são estabelecidos protocolos, procedimentos e normas de caráter eminentemente defensivo. Sob esse prisma, busca-se mitigar vulnerabilidades, adotando procedimentos, estabelecendo níveis de acesso, adquirindo equipamentos e capacitando os agentes.

Segurança de Pessoas: conjunto de medidas que objetivam proteger a integridade não só física, mas também moral dos integrantes da Instituição.

3 NOBRE, George Karlo Dantas. **A atividade de inteligência no âmbito do Ministério Público:** um comparativo entre inteligência ministerial e investigação ministerial criminal. Natal: UNISUL, 2014. p. 71.

Segurança de Material: conjunto de medidas que tem como objetivo a proteção do patrimônio físico da instituição, seus bens móveis e imóveis.

Segurança de áreas e instalações: conjunto de medidas que visa a proteger o espaço físico de responsabilidade da instituição, também o espaço físico onde são realizadas atividades de interesse da instituição e seus perímetros. Nesse escopo há previsão para tratamento diferenciado para áreas consideradas mais sensíveis dentro da instituição, com possibilidade de restrição de acesso.

Segurança da informação: conjunto de medidas para a proteção de dados e informações sigilosas ou classificadas, que se difundidas irão acarretar prejuízos de qualquer natureza à instituição ou possibilitar vantagens a um ator adverso, por acesso à informação não autorizada.

A importância da segurança da informação é de tal monta, ainda mais na era da informação e conectividade em que vivemos, que se subdivide nos seguintes subgrupos: segurança da informação nos meios de tecnologia da informação, segurança da informação de pessoas, segurança da informação na documentação, segurança da informação nas áreas e instalações.

2.2. SEGURANÇA ATIVA

A segurança ativa, por sua vez, será formada por um conjunto de medidas que tem por fim detectar, identificar, avaliar, analisar e neutralizar ações adversas de qualquer natureza, que atentem contra a Instituição. O aspecto observado na segurança ativa é o da ameaça à Instituição e seus ativos; importa, assim, que seja proativa, antecipando-se a ocorrência do dano.

No caso do Ministério Público, essas medidas podem ser executadas por meio de Contraespionagem, Contrassabotagem, Contra Crime Organizado e Contrapropaganda, seguindo-se o que estabelece a Resolução nº 156 do CNMP, que, de forma inovadora e atenta à realidade institucional, adiciona às medidas de segurança ativa o enfoque sobre o crime organizado.

Contrassabotagem: medidas voltadas para prevenir, detectar, obstruir e neutralizar ações que visem a atingir setores ou materiais da instituição.

Contraespionagem: medidas voltadas para prevenir, detectar, obstruir e neutralizar ações que busquem informações classificadas, sensíveis ou sigilosas.

Contra crime organizado: medidas voltadas para prevenir, detectar, obstruir e neutralizar ações de organizações criminosas, que visem a atingir pessoas ou instalações da instituição.

Contrapropaganda: medidas voltadas para prevenir, detectar, obstruir e neutralizar ações que gerem desinformação, abusos ou propaganda enganosa contra a instituição.

Destacam-se

> As atividades de Contrainteligência possuem caráter eminentemente preventivo e proativo, antecipando-se às ações hostis dos mais

variados atores. Deve orientar a sua atuação para a proteção da imagem e reputação da organização a que pertence o sistema de Inteligência em que atua. Para desempenhar as suas atribuições, a Contrainteligência orienta-se por ameaças reais ou potenciais à sua organização. Estas ameaças podem se caracterizar por ações de atores hostis que possuem intenção deliberada de causar dano ou por ações consubstanciadas por atitudes de negligência dos integrantes da organização, às quais podem redundar em um prejuízo. O manual de campanha do exército norte americano relativo à Contrainteligência, FM 34-60 (1995), diz que a missão da Ainda que sejam grandes os desafios para uma estruturação da Contrainteligência é detectar, identificar, avaliar, obstruir, neutralizar ou explorar os esforços das ameaças de coleta de Inteligência. Prosseguindo, o texto acrescenta que a tarefa da Contrainteligência é dar o suporte para preservar o sigilo e proteger a força (ou a organização), direta e indiretamente.[4]

E do manual de campanha do exército norte americano relativo à Contrainteligência, FM34-60 (1995), no Capítulo Um, que trata da missão e estrutura da CI, extrai-se:

> *While not as flashy, routine security procedures provide crucial force protection. These procedures include but are not limited to—*
>
> *Personnel security, to include background investigations, will ensure all personnel who have access to sensitive or classified information will fully protect it.*
>
> *Information security, particularly in regard to handling classified and compartmented information, will be a challenging field in the future considering the ease with which information can be copied and transmitted in an increasingly automated Army.*
>
> *Physical security, which ensures physical measures are taken to safeguard personnel, prevents unauthorized access to equipment, installations, materiel, and documents to safeguard them against espionage, sabotage, damage, and theft.*
>
> *Operations security (OPSEC), which ensures that all essential elements of friendly information (EEFI), are reasonably concealed from enemy collection assets.*[5]

3. IMPORTÂNCIA DA ESTRUTURAÇÃO DA CONTRAINTELIGÊNCIA NO MINISTÉRIO PÚBLICO

Ainda que se apresente como um desafio a estruturação de órgão de Contrainteligência dentro do Ministério Público, inegável sua importância, e

4 FARAH, Camel André de Godoy. **Logística, ações e operações de inteligência:** livro digital / 1. ed. rev. e atual. Palhoça: UNISUL Virtual, 2015. p. 75.

5 Apesar de não ser tão chamativo, os procedimentos de segurança de rotina fornecem proteção da força crucial. Estes procedimentos incluem, mas não estão limitados a

- Pessoal de segurança, para incluir investigações de fundo, vai garantir todo o pessoal que tem acesso a informações sensíveis ou classificados será totalmente protegê-la.
- Segurança da informação, particularmente no que diz respeito ao tratamento de informação classificada e compartimentada, será um campo desafiador no futuro, considerando a facilidade com que as informações podem ser copiadas e transmitidas em um exército cada vez mais automatizados.
- Segurança física, o que garante que medidas físicas são tomadas para proteger o pessoal, impede o acesso não autorizado aos equipamentos, instalações, material e documentos para protegê-los contra a espionagem, sabotagem, dano e furto.
- Operações de segurança (OPSEC), que garante que todos os elementos essenciais da informação convivial (EEFI) são razoavelmente escondidos de ativos coleção inimigo. (tradução livre)

mais, a premente necessidade de se antecipar às ameaças e aos ataques a que a Instituição e seus ativos estão expostos.

Destaca-se a definição de ativos do Manual de Contrainteligência do Reino Unido 92001), que em seu capítulo um assim dispõe:

> *Assets are defined as "anything of value, either tangible or intangible that is owned or used by an organization or business". They can be documents and information; material such as buildings, equipment, valuables or cash; operating systems or personnel.*[6]

Não são estranhos à história situações de ameaças e exploração de vulnerabilidades por agentes adversos externos e internos, que atingiram fortemente o Ministério Público. Citam-se como exemplos casos de Promotores de Justiça no MPBA[7], MPSP[8], MPMG[9], MPPE[10], MPRN[11].

Como referido, esses são alguns exemplos facilmente encontrados em fontes abertas; no entanto, tantos outros casos são da rotina das coordenadorias de segurança institucional em cada um dos Ministérios Públicos, sem contar os inúmeros ataques à imagem, reputação de promotores, promotoras de Justiça, procuradores que acontecem hodiernamente.

A falta de uma cultura sobre a atividade de inteligência, uma compreensão desconforme de sua atuação e a falta de uma doutrina própria sobre a atividade são desafios que dificultam a implementação de forma ordenada e sistemática de um órgão de inteligência, com atribuições que lhe são próprias, na estrutura dos Ministérios Públicos do Brasil.

Necessário, assim, despertar o Ministério Público para a importância da estruturação normativa, técnica e operacional de um órgão de Contrainteligência dentro da Instituição, realizando a tarefa com profissionalismo e capacitação adequada, vez que todo o trabalho desenvolvido na atividade de inteligência possui metodologia e técnicas próprias.

A contrainteligência é uma proteção, um escudo que mitiga riscos, diminui vulnerabilidades e pode antecipar ameaças, permitindo à instituição deter uma vantagem estratégica contra agentes hostis.

Um órgão de inteligência precisa necessariamente, para criação e fortalecimento de sua identidade, de um ato que forneça os contornos de

6 Ativos são definidos como qualquer coisa de valor, tangível ou intangível, pertencente ou usado por uma organização ou empresa. Eles podem ser documentos e informações; materiais como edifícios, equipamentos, objetos de valor ou dinheiro; sistemas operacionais ou pessoal. (tradução livre)

7 Disponível em: <https://veja.abril.com.br/blog/bahia/ameacado-promotor-na-bahia-se-afasta-de-caso-de-pms-acusados-de-matar-12/>.

8 Disponível em: <https://oglobo.globo.com/brasil/ameacado-pelo-pcc-promotor-nao-sabe-mais-que-privacidade-23309151> e <http://g1.globo.com/sp/campinas-regiao/noticia/2013/09/carta-com-ameaca-de-morte-e-fotos-e-enviada-promotor-do-caso-denarc.html>.

9 Disponível em: <https://noticias.r7.com/minas-gerais/apos-ameaca-procurador-geral-cria-grupo-para-investigar-vereador-13082019>.

10 Disponível em: <https://g1.globo.com/pe/pernambuco/noticia/2019/07/29/condenado-por-morte-do-promotor-thiago-faria-e-capturado-apos-cinco-meses-de-fuga-de-penitenciaria.ghtml>.

11 Disponível em: <http://g1.globo.com/rn/rio-grande-do-norte/noticia/2017/03/servidor-que-atirou-em-procurador-e-promotor-no-rn-se-entrega.html>.

sua atribuição, balizando e legitimando a ação de todos os que nele estão envolvidos e ainda indicando os objetivos que pretende alcançar; precisa assim, conhecer "o que fazer" para então buscar o "como fazer", como alcançar os objetivos traçados.

Para trazer à realidade e tornar factível o que se pretende alcançar, necessária a realização de ações, por meio de iniciativas estratégicas, que podem estar esquematicamente divididas em ações estratégicas, projetos e programas.

> A capacitação profissional é requisito indispensável na atividade de Inteligência. Pela própria natureza da atividade, que é essencialmente velada e cujos métodos não são indiscriminadamente disseminados, é fundamental que agentes sejam devidamente capacitados. Independentemente do ramo da Inteligência, trata-se de uma atividade eminentemente técnica e, portanto, demanda aprendizado específico e direcionado.[12]

Complementando:

> Toda operação de Inteligência requer a aplicação de elementos gerencias para a sua execução, em face da complexidade das ações envolvidas na atividade operacional. Planejamento, coordenação e controle são essenciais para o desenvolvimento de uma operação, assim como o adequado concerto dos componentes que constituem uma operação de Inteligência, pois permitem a sua realização com efetividade, obtendo resultados que atendem a necessidade de dados e informações.[13]

As ações estratégicas não exigem complexidade para sua efetivação, mas principalmente um ato de vontade de quem tem a capacidade para deliberar sobre um assunto.

Os projetos e programas, estes sim, demandam maior complexidade e organização com divisão de tarefas, prazo para sua conclusão e indicação de quem será o responsável por seu gerenciamento.

Na área de inteligência são diversas suas aplicações, sendo necessário para sua efetividade que estejam alinhadas com os objetivos estratégicos identificados na política de inteligência da organização. Tal projeto necessariamente trataria de questões de integração entre órgãos e também de interoperabilidade de sistemas, o que envolveria diversas variáveis, inclusive as relativas às questões de segurança desse projeto, vez que uma grande quantidade de dados e informações estaria sendo trabalhada.

Alguns tópicos podem ser elencados brevemente, dentre outros, para um projeto de Contrainteligência dentro do Ministério Público:

a. Normatizar a atividade, com elaboração de uma Política de Inteligência do Ministério Público e de um Plano de Inteligência e demais atos que estabelecem protocolos e procedimentos a serem observados;

12 LUZ, Alessandro Roberto. **O Emprego da Técnica de Avaliação de Dados (TAD) na Produção do Conhecimento de Inteligência.** Palhoça:UNISUL, 2019. p. 53.

13 FARAH, Camel André de Godoy. **Logística, ações e operações de inteligência:** livro digital / 1. ed. rev. e atual. Palhoça: UNISUL Virtual, 2015. p. 25.

b. Definir credenciais de acesso – A definição de credenciais implica a compartimentação das informações, preservando-se o princípio da necessidade de conhecer;

c. Designar um encarregado pela Contrainteligência – necessário que dentro de um órgão de inteligência haja uma seção ou um setor responsável pela Contrainteligência, com competências e habilidades para esse fim, sendo de responsabilidade do setor ou de uma pessoa designada a elaboração do plano de segurança, seu monitoramento, plano de gestão de risco e de incidentes de segurança, dentre outras atribuições;

d. Possuir um Planejamento de Contingência – necessária a antecipação, quando da hipótese de falha na segurança da informação, com estabelecimento de um roteiro prévio, que deve ser observado em tais situações, permitindo assim a continuidade do projeto e a correção das falhas detectadas;

e. Capacitar os que atuam na área de operação e análise para adequada conformidade dos métodos e técnicas da atividade de inteligência.

4. CONCLUSÃO

Nenhuma organização pode subsistir e se desenvolver se não tiver diretrizes que indiquem o caminho necessário para alcançar os desideratos pretendidos.

Os balizamentos normativos dão legitimidade ao órgão e às ações desempenhadas por seus atores.

Indiscutível a importância dos ativos que formam o Ministério Público. O cenário da segurança se modificou com o tempo. A violência adquire formas mais estruturadas, utilizando, inclusive, de infiltração de agentes e recrutamentos para obtenção de dados e estudos de vulnerabilidades.

Necessária uma mudança de paradigma deixando-se de agir somente de forma reativa, para que seja possível produzir um conhecimento de qualidade que subsidie decisões que evitem ou neutralizem ameaças. Atenta-se aos princípios que norteiam a atividade, quais sejam: objetividade, segurança, oportunidade, controle, clareza, dentre outros e aos princípios constitucionais que devem ser preservados.

Pontua Paula (2011, p. 61): "Cabe à CI realizar as ações necessárias para regular o acesso aos dados e conhecimentos e prevenir e evitar os comprometimentos e os vazamentos".

A estruturação da atividade de inteligência no Ministério Público é assim uma importante ferramenta estratégica, para que todos os que realizam sua atividade o façam de forma livre e desembaraçada, sem medo ou intimidação.

5. REFERÊNCIAS

ALMEIDA NETO,Wilson Rocha de. **Inteligência e Contrainteligência no Ministério Público.** Dictum, 2009

BRASIL. **Decreto nº 3.695, de 21 de dezembro de 2000**. Cria o Subsistema de Inteligência de Segurança Pública, no âmbito do Sistema Brasileiro de Inteligência, e dá outras providências. Brasília/DF, 2000. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/d3695.htm>. Acesso em: 29 jul. 2019.

_____. **Decreto nº 4.376, de 13 de setembro de 2002.** Dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência, instituído pela Lei nº 9.883, de 7 de dezembro de 1999, e dá outras providencias. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/2002/D4376.htm>. Acesso em: 25 ago. 2019.

_____. **Resolução nº 156, de 13 de dezembro de 2016**. Institui a Política de Segurança Institucional e Cria o Sistema Nacional de Segurança Institucional do Ministério Público e Dá Outras Providências. Disponível em: <http://www.cnmp.mp.br/portal/images/Normas/Resolucoes/RESOLUO_156.pdf>. Acesso em: 29 jul. 2019.

BRASIL. **Decreto 8793, de 29 de junho de 2016**. Fixa a Política Nacional de Inteligência. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8793.htm>. Acesso em: 29 jul. 2019.

FARAH, Camel André de Godoy. **Logística, ações e operações de inteligência:** livro digital / 1. ed. rev. e atual. Palhoça: UNISUL Virtual, 2015.

HAMADA, Hélio Hiroshi; MOREIRA, Renato Pires. **Inteligência de segurança pública e cenários prospectivos da criminalidade.** Série inteligência, estratégia e defesa nacional. Belo Horizonte: Editora D'Plácido, 2016.

LUZ, Alessandro Roberto. **O Emprego da Técnica de Avaliação de Dados (TAD) na Produção do Conhecimento de Inteligência**. Palhoça: UNISUL, 2019.

KRIEGER, C.A *et al*. **Inteligência – Estratégia de Segurança.** Palhoça: UNISUL Virtual, 2011.

NOBRE, George Karlo Dantas. **A atividade de inteligência no âmbito do Ministério Público**: Um comparativo entre inteligência ministerial e investigação ministerial criminal. Natal: UNISUL, 2014

NUNES DE GOES, João Mario. **Plano Estadual de Segurança Público:** Relevância para o desempenho da atividade de inteligência. Palhoça: UNISUL, 2017.

PAULA, GIOVANI DE. **Atividade de Inteligência de Segurança Pública:** um modelo de conhecimento aplicável aos processos decisórios para a prevenção e segurança no trânsito. Santa Catarina: Universidade Federal de Santa Catarina. 2013.

UNITED KIGDON. **The Defence Manual of Security.** Volumes 1, 2 and 3 Issue 2, 2001.

UNITED STATE OF AMERICA. **FM 34-60-counterintelligence**. Headquarters, department of the Army.1990

A SEGURANÇA INSTITUCIONAL DO MINISTÉRIO PÚBLICO BRASILEIRO E A LEI GERAL DE PROTEÇÃO DE DADOS (LEI Nº 13.709/2018) - IMPRESSÕES INICIAIS

Rui Carlos Kolb Schiefler[1]

Maria Fernanda Tonini Blazius de Oliveira[2]

SUMÁRIO: 1. Introdução. 2. A Segurança Institucional do Ministério Público. 3. A Lei Geral de Proteção de Dados – aspectos destacados. 4. A Segurança Institucional do Ministério Público e a Lei Geral de Proteção de Dados. 5. Conclusões. 6. Referências.

RESUMO: O presente estudo visa a analisar a implicação/aplicação da Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, nas atividades de segurança institucional (Inteligência e Contrainteligência) do Ministério Público brasileiro. O quadro teórico mobilizado abrange os seguintes temas: a Segurança Institucional do Ministério Público e a discussão acerca da LGPD no quadro da segurança institucional. No âmbito dos aspectos metodológicos recorreu-se a uma pesquisa bibliográfica e documental. Os resultados deste estudo demonstram que a lei, embora tenha aspectos (aparentemente) conflituosos quanto aos casos que excepciona de sua aplicação, não promoverá dificuldades no desenvolvimento das atividades de Inteligência e Contrainteligência do Ministério Público. Trata-se de nova regulação positiva e necessária para a proteção das garantias individuais.

PALAVRAS-CHAVE: Lei Geral de Proteção de Dados (LGPD). Lei nº 13.709/2018. *General Data Protection Regulation* (GDPR). Regulamento Geral de Proteção de Dados Pessoais Europeu nº 2016/679. Conselho Nacional do Ministério Público (CNMP). Política de Segurança Institucional do Ministério Público (PSI/MP). Sistema Nacional de Segurança Institucional do Ministério Público (SNS/MP).

1 Graduado em Direito pela UFPR. Especialista em Direito pela UFSC/Fundação José Boiteux. Coordenador da Coordenadoria de Inteligência e Segurança Institucional do MPSC. Ex-Secretário-Geral do MPSC. Presidente da Associação Catarinense do Ministério Público (ACMP) e ex-Secretário-Geral da Associação Nacional dos Membros do Ministério Público (CONAMP).

2 Graduada em Direito pela Universidade do Vale do Itajaí (UNIVALI). Pós-graduanda em Direito Processo Civil pela Universidade Estácio de Sá/CERS. Mediadora judicial. Assessora jurídica na Coordenadoria de Inteligência e Segurança Institucional do MPSC.

1. INTRODUÇÃO

Em um mundo no qual a coleta de dados pessoais é total, generalizada e silenciosa[3], ainda sem regras bem definidas, e inclusive, não raras vezes, até sem respeito à ética, observa-se um emaranhado de informações e a sensação de perda do controle sobre as próprias vidas. O avanço e o uso da tecnologia da informação e da internet ampliaram em demasiado o acesso e a obtenção de dados, permitindo maior transparência entre governos, sociedade e mercado. Todavia, reconhece-se a necessidade de que o livre acesso à informação e à transparência deve ser seguido da preservação da privacidade, garantido pela Constituição da República Federativa do Brasil de 1988. Para fazer frente a este dilema, são necessárias soluções inovadoras, as quais já vêm sendo percebidas no ordenamento jurídico brasileiro, em especial com a promulgação da Lei nº 13.709, de 14 de agosto de 2018, conhecida como a Lei Geral de Proteção de Dados ou apenas pela sigla LGPD, que entrará em vigor em agosto de 2020. A nova lei surge num cenário mundial de intensa preocupação com os dados pessoais, para preservar, dentre outros, a privacidade dos indivíduos e o seu direito à autodeterminação informativa.

A extensa *vacatio* da LGPD é proposital, ao permitir discussões, críticas e interpretações multidisciplinares, visto que tal lei provocará uma verdadeira revolução não só jurídica, como tecnológica e de gestão, no tratamento de dados pessoais. Essa revolução ocorre no trato da proteção dos direitos fundamentais da liberdade e da privacidade das pessoas naturais, além do livre desenvolvimento da sua personalidade – fundada, principalmente, na transparência e boa-fé. A nova lei também exigirá de todos, frise-se, um conhecimento razoável acerca de princípios e regras gerais – e até específicas – de outras disciplinas, notadamente de gestão, negócios, informática, relacionamento humano e social, administração, *compliance* e, também, de segurança (institucional).

Com efeito, a responsabilidade pelas adaptações à nova Lei Geral não se limita às áreas de informática e Direito. As instituições públicas e privadas, em todos os seus setores (recursos humanos, *marketing*, planejamento, comunicação social etc.) terão de investir em capacitação para o aumento do seu nível de maturidade no tema. Diante disso, faz-se necessário que o Ministério Público brasileiro também acompanhe essas inovações, sob pena de comprometimento (até) das suas funções institucionais.

O presente estudo tem o propósito, assim, de analisar a implicação/aplicação da LGPD nas atividades de Segurança Institucional (Inteligência e Contrainteligência) do Ministério Público brasileiro, buscando avaliar se essa lei se aplica ou não a essas atividades, à luz do disposto em seu artigo 4°, inciso III e §1°.

Não há pretensão (nem seria possível neste momento) de exaurimento do tema, notadamente porque a LGPD – em vigor de forma parcial desde a

3 VALENTINO-DEVRIES, Jennifer. Polícia usa dados de localização do Google em investigações nos EUA. **Folha de São Paulo**, 2019. Disponível em: <https://www1.folha.uol.com.br/mundo/2019/04/policia-usa-dados-de-localizacao-do-google-em-investigacoes-nos-eua.shtml>. Acesso em: 22 abr. 2019.

edição da Medida Provisória nº 869, de 27 de dezembro de 2018[4], convertida na Lei nº 13.853, em 8 de julho de 2019 – apresenta-se como marcante e próxima disrupção[5] legislativa.

Nessa simbiose[6] entre os mundos real e virtual (estão aí a comprovar internet das coisas – *Internet of Things* (IoT), inteligência artificial – *artificial intelligence* (AI), *big data* e *analytics*[7], realidade virtual, edição de genomas, algoritmos, robôs virtuais, eletrocêutica – *electroceuticals*[8], criptomoedas, *deep* e *dark web*, dentre tantos fenômenos digitais), o trato da matéria aqui posta, na perspectiva da proteção da Instituição Ministério Público, seus integrantes e seu patrimônio (inclusive imaterial), indiretamente representa, também, a proteção do bem maior, que é a sociedade como um todo.

O presente artigo está estruturado em uma introdução que apresenta as linhas gerais do tema e o objetivo do estudo. A segunda seção versa sobre a atividade de Segurança Institucional e seus principais pilares, as atividades de Inteligência e Contrainteligência. A terceira seção é dedicada à LGPD, sua origem, objeto, alcance – especial atenção, aqui, no que diz respeito ao Poder Público. A quarta seção destina-se à análise da ingerência da Lei Geral de Proteção de Dados na Atividade de Segurança Institucional, especificamente nas atividades de Inteligência e Contrainteligência. Por fim, as conclusões apresentam as principais contribuições do estudo e (inevitavelmente) as dúvidas e preocupações sobre este novo marco legal e regulatório da proteção de dados pessoais no país.

2. A SEGURANÇA INSTITUCIONAL DO MINISTÉRIO PÚBLICO BRASILEIRO

Com o advento da Constituição Democrática de 1988[9], que consagrou a unidade, indivisibilidade e independência funcional e administrativa do Ministério Público, houve um agigantamento das suas funções institucionais.

Esse importante avanço, porém, passou a exigir um olhar mais atento à atividade de Segurança Institucional, voltada a salvaguardar o livre e desembaraçado exercício do múnus pelos seus membros e servidores. A Instituição Ministério Público fortaleceu-se com base na Carta Magna,

4 Vigência em 28 de dezembro de 2018, para os artigos que (re)criam a autoridade de fiscalização, e vigência em 24 meses, a contar da publicação da LGPD, para os demais artigos. Estas disposições foram mantidas na Lei nº 13.853/2019.

5 "Ato de romper, de interromper o curso natural de; ruptura, rompimento, fratura: disrupção de um processo". (Disrupção. In: DICIONÁRIO ONLINE DE PORTUGUÊS. Disponível em: <https://www.dicio.com.br/disrupcao/>. Acesso em: 22 abr. 2019).

6 Muito próxima ou, até, já estabelecida.

7 "*Analytics* refere-se à possibilidade de se utilizar dados, análises e raciocínio sistemático para seguir em um processo de tomada de decisão muito mais eficiente" (COELHO, Lucas. Analytics: o que é, conceito e definição. **Cetax**. Disponível em: <https://www.cetax.com.br/blog/o-que-e-analytics/>. Acesso em: 1º fev. 2019).

8 10 principais tecnologias emergentes de 2018, segundo o WEF. **CIO**, 2019. Disponível em: <https://cio.com.br/10-principais-tecnologias-emergentes-de-2018-segundo-o-wef/>. Acesso em: 22 abr. 2019.

9 Os artigos 127 a 130-A da CRFB/88, inaugurais do Capítulo IV, que trata das funções essenciais à Justiça, dispõem sobre o Ministério Público (Seção I).

implicando essa valoração na necessidade de uma maior e mais eficaz autoproteção.

A Resolução nº 156/2017 do Conselho Nacional do Ministério Público (CNMP) é o atual marco regulatório da atividade de Segurança Institucional no âmbito do Ministério Público brasileiro. Tal qual a LGPD, igualmente representou um positivo e necessário arcabouço protetivo de direitos e garantias.

De fato, a referida Resolução instituiu a Política de Segurança Institucional (PSI/MP) e o Sistema Nacional de Segurança Institucional do Ministério Público (SNS/MP), aplicando-se a todos os ramos ministeriais, tanto estaduais como da União. Está estratificada em quatro capítulos, sendo um deles dedicado exclusivamente à atividade de Segurança Institucional.

Nesse sentido, nos termos do seu artigo 2º, a atividade de Segurança Institucional deve ser permeada pelos princípios da proteção aos direitos fundamentais e do respeito aos princípios constitucionais da atividade administrativa, além de orientada pela ética profissional e pelos valores fundamentais do Estado Democrático de Direito. Atuação preventiva e proativa, com o fim de antecipar ameaças e outras ações hostis e sua neutralização, bem como a profissionalização e caráter perene da atividade, inclusive com conexão com outras áreas internas para proteção integral da Instituição e de seus integrantes, também é o que dela se espera, assim como a integração do Ministério Público com outros órgãos essenciais à atividade de segurança institucional; orientação da atividade às ameaças reais ou potenciais à Instituição e a seus integrantes, inclusive no que tange aos efeitos de acidentes naturais; e a salvaguarda da imagem da Instituição, evitando sua exposição e exploração negativas.

A atividade de Segurança Institucional congrega um conjunto de medidas que visam a proteger a Instituição e seus integrantes, inclusive quanto à imagem e reputação, nas quais estão inseridas as medidas de segurança orgânica e de segurança ativa (art. 3°, *caput* e §1º). As medidas de segurança orgânica subdividem-se em segurança de pessoas (ativo humano), do material (ativo físico móvel), das áreas e instalações (ativo físico predial) e da informação, enquanto as medidas de segurança ativa englobam as ações de contrassabotagem, contraespionagem, contra crime organizado e contrapropaganda (art. 3°, §2° e §3°).

A mencionada Resolução, ainda, traz em seu bojo expressas regras a respeito das Atividades de Inteligência e Contrainteligência, voltadas à proteção institucional e como subsídio de conhecimento (art. 4º §1º), por exemplo. Quando trata da segurança da informação, determina um conjunto de medidas dirigidas à proteção de dados e informações sensíveis ou sigilosas, visando a garantir a integridade, o sigilo, a autenticidade, a disponibilidade, o não repúdio e a atualidade do dado, informação ou conhecimento, vinculando-as à segurança da informação nos meios de tecnologia da informação, de pessoas, na documentação e nas áreas e instalações (art. 7º). Estimula o desenvolvimento interno de tal atividade, assim como a parceria e capacitação com outros órgãos de inteligência, nacionais e até internacionais (arts. 23, III, e 31).

Para bem desenvolver todas essas incumbências, o Ministério Público brasileiro desenvolve, em alto grau de confiabilidade e cientificidade, atividades de Inteligência, voltadas especialmente à busca de informações e conhecimento, a subsidiar a tomada de decisões e/ou para auxiliar nas suas investigações.

A própria Política de Segurança Institucional (PSI) do Ministério Público brasileiro prevê a urgente difusão da cultura de segurança, Inteligência e Contrainteligência em todos os ramos institucionais do país.

Sabe-se que Segurança e Inteligência são irmãs gêmeas, que precisam, como tal, ser cultuadas e desenvolvidas na mesma toada, com igual grau de responsabilidade institucional. Uma depende da outra, pois se completam. Numa instituição pública e essencial à administração da Justiça, como é o Ministério Público, são temas ainda mais relevantes, que não podem ser ignorados.

Inteligência, então, em outras palavras, significa a própria sobrevivência das instituições e, indiretamente, do Estado, enquanto ente que congrega todos os anseios sociais. Está imbricada nas atividades de segurança pública e de estado. Há praticamente um século o Brasil desenvolve o seu serviço de inteligência, algumas vezes envolto, é verdade, em certo clima de mistério.

A atividade de Inteligência tem por característica a identificação de fatos e situações – pela coleta e processamento de dados, bem como pelo estudo de informações –, que se apresentem como obstáculos ou oportunidades aos interesses nacionais, com o fim de auxiliar os tomadores de decisão a ultrapassarem eventuais obstáculos ou aproveitarem as oportunidades (ABIN, 2019).

Empresas privadas, Exército Brasileiro e demais Forças, Polícias em geral, órgãos do sistema penitenciário, órgãos financeiros e ambientais, dentre outros, usufruem do sistema de inteligência brasileiro para que as suas decisões não sejam tomadas por "achismo", empirismo, experiência administrativa do agente de plantão ou por simples tino político. Por certo, o Ministério Público brasileiro não corre o mesmo risco ou realiza uma prática errada assim.

Historicamente, no Ministério Público brasileiro, com a criação do Grupo Nacional de Combate às Organizações Criminosas "Promotor de Justiça Francisco José Lins do Rêgo Santos"[10] (GNCOC), em 22 de fevereiro de 2002, pelo Conselho Nacional de Procuradores-Gerais dos Ministérios Públicos dos Estados e da União (CNPG), houve um incremento às atividades administrativas e investigativas da Instituição por todos os seus ramos, que, dois anos depois (2004), culminou na criação do Grupo de Inteligência dos Ministério Públicos, pelo GNCOC, diante da (aferida) necessidade de os Ministérios Públicos terem um sistema de inteligência próprio (PACHECO, 2013).

10 Homenagem ao Promotor de Justiça Francisco José Lins do Rêgo Santos, combatente membro do Ministério Público do Estado de Minas Gerais, brutalmente assassinado no curso da investigação da "máfia dos combustíveis", em 25 de janeiro de 2002, na zona sul de Belo Horizonte/MG.

E foi por essas iniciativas do grupo nacional que muitas ações articuladas, exitosas e importantes, passaram a ser desenvolvidas pela Instituição, exigindo a rápida, eficiente e segura troca de informações e dados.

A próxima seção é dedicada à LGPD, sua origem, objeto, alcance – especificamente, aqui, no que diz respeito ao Poder Público.

3. A LEI GERAL DE PROTEÇÃO DE DADOS (LEI Nº 13.709/2018) – ASPECTOS DESTACADOS

A Lei nº 13.709, de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados ou apenas pela sigla LGPD,

> dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (art. 1°).

A edição da LGPD, no Brasil, seguiu tendência mundial na busca da efetiva proteção dos dados pessoais, inclusive (e, entende-se, precipuamente) no meio digital[11], especialmente empós a aprovação do Regulamento Geral de Proteção de Dados Pessoais Europeu nº 2016/679 (*General Data Protection Regulation* – GDPR), ocorrida em 27 de abril de 2016[12], cuja validade jurídica ultrapassa os limites territoriais europeus[13].

Dentre os muitos fatores que contribuíram para a aceleração desse movimento[14] pró-titular de dados pessoais, está o caso de violação da privacidade no ambiente virtual, envolvendo a assessoria britânica *Cambridge Analytica*. Segundo noticiado pela imprensa brasileira e internacional, essa assessoria obteve, ilicitamente, informações privadas de milhões de usuários do *Facebook* e teria utilizado esses dados, mediante publicidade tendenciosa e dirigida a favor do então candidato Donald Trump, na campanha para presidência dos Estados Unidos da América do ano de 2016[15].

Da experiência já vivenciada no continente europeu, a partir da entrada em vigor do assemelhado regramento (GDPR), tem-se que a nova lei atinge também empresas de todos os setores econômicos, de instituições financeiras a companhias aéreas, incluindo, por exemplo, hotéis, restaurantes, lojas de roupas, farmácias etc., e, principalmente, prestadoras

11 Nesse sentido, Artese (2019, p. 500): "Leis de proteção de dados pessoais, como a LGPD, nada mais são que respostas regulatórias aos riscos associados ao processamento massivo de dados pessoais. Não houvesse computador, não haveria LGPD".

12 Este regulamento entrou em vigor em 25 de maio de 2018.

13 "[...] No artigo 3º do GDPR é definido que tal resolução é aplicável ao processamento de dados de pessoas naturais que estejam no território da UE, independente da localização da entidade/empresa que realiza tal atividade, quando esta é relacionada à oferta de produtos e serviços e/ou ao monitoramento de comportamento dessas pessoas" (MOREIRA, 2019, n.p.).

14 De imposição geral, linear e global.

15 Entenda o escândalo do uso de dados do Facebook pela *Cambridge Analytica*. **Estadão**, 2019. Disponível em: <https://link.estadao.com.br/galerias/geral,entenda-o-escandalo-do-uso-de-dados-do-facebook-pela-cambridge-analytica,36615>. Acesso em: 16 abr. 2019.

de serviços. Nesse contexto, as empresas que exploram o ambiente digital devem se impactar sobremaneira, "sobretudo no caso daquelas que usam as informações colhidas dos seus clientes (ou "usuários") como modelo de negócio, caso da maioria das redes sociais ativas e de gigantes como o Google" (RONCOLATO, 2019, n.p.). Dentre as empresas norte-americanas designadas pelo acrônimo GAFAM[16], a *Google* foi a que recebeu a primeira expressiva multa por infração ao GDPR[17].

A preocupação com a proteção de dados pessoais tem origem no fim dos anos de 1960, coincidente com a difusão do uso de computadores e das tecnologias da comunicação e informação em grande escala (ARTESE, 2019).

Os primeiros passos na busca por tal proteção, tendo por fundamentos principais o conhecimento e o consentimento, pelo titular, da utilização de seus dados pessoais, passam pela obra intitulada *Privacy and Freedom* (1967), por meio da qual o autor americano Alan Westin defendeu que a preservação dos direitos do indivíduo, aí incluída a privacidade, está diretamente relacionada com o controle que ele exerce sobre as informações que trafegam ao seu respeito (ARTESE, 2019).

A Convenção nº 108, firmada pelos Estados-membros do Conselho da Europa, em 28 de janeiro de 1981, em Estrasburgo, na França, também se referiu ao tema. Considerada "o primeiro instrumento internacional juridicamente vinculativo adotado no domínio da proteção de dados" (MILT, 2019, p. 2), ela teve o intuito de ampliar a proteção de direitos fundamentais, especialmente o direito à privacidade, diante do aumento do fluxo de dados pessoais sujeitos a tratamento automatizado, sem deixar de considerar o direito à livre circulação de informação entre povos[18].

Outro momento relevante foi a decisão prolatada no ano de 1983, pelo Tribunal Constitucional alemão, no julgamento a respeito da Lei do Censo germânica[19], em que foi reconhecido o direito à autodeterminação informativa (ARTESE, 2019).

Bioni (2018, p. 101), a respeito, sustenta que o

> [...] julgado destaca-se por sua *ratio decidendi* sob dois aspectos: a) proteção dos dados pessoais como um direito da personalidade autônomo e a compreensão do termo autodeterminação informacional para além do consentimento; b) a função e os limites do consentimento do titular dos dados. [...] na primeira parte do julgado, estabelece-se a

16 "GAFAM é o acrônimo de gigantes da *Web, Google, Apple, Facebook, Amazon e Microsoft*, que são cinco grandes empresas dos EUA, nascidas nos últimos anos do século XX ou início do século XXI (exceto a Microsoft, fundada em 1975, e a Apple, em 1976), que dominam o mercado digital." (Disponível em: <https://pt.wikipedia.org/wiki/GAFAM>. Acesso em: 1º maio 2019).

17 França multa Google em 50 milhões de euros por violação de lei de privacidade na UE. **G1 Globo**, 2019. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2019/01/21/franca-multa-google-em-50-milhoes-de-euros-por-violacao-de-lei-de-privacidade-na-ue.ghtml>. Acesso em: 1º maio 2019.

18 COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS. **Convenção para a protecção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal.** Disponível em: <https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm>. Acesso em: 18 abr. 2019.

19 De acordo com Martins *apud* Bioni (2018, p. 101) esta lei "[...] determinou que os cidadãos fornecessem uma série de dados pessoais para mensurar estatisticamente a distribuição espacial e geográfica da população", e, além disso previa "a possibilidade de que os dados coletados fossem cruzados com outros registros públicos para finalidade genérica de execução de "atividades administrativas".

> importante construção de que o cidadão deve ter o controle sobre os seus dados pessoais, a fim de que ele possa autodeterminar as suas informações pessoais. Cunha-se, então, a expressão autodeterminação informacional ou autodeterminação informativa.

Nos anos 90, foi editada a Diretiva 95/46/CE, que disciplinava o tema na União Europeia até o advento do GDPR, que a revogou[20]. Nela orientava-se a adoção de leis de proteção de dados próprias por cada Estado-Membro da organização internacional, ao contrário do GDPR, que é geral e impositivo a todos esses Estados-Membros, embora lhes confira a possibilidade de firmarem disposições específicas, com o fim de melhor se adequarem a aplicação da regulação geral (FERREIRA *et al*, 2019, n.p.).

No cenário pátrio[21], a LGPD surge como novo marco regulatório de proteção de dados pessoais, sobrevindo e alterando[22] a Lei nº 12.965/2014 (Marco Civil da internet). Esta, a propósito, timidamente trata da proteção de dados pessoais, ao estabelecer princípios, garantias, direitos e deveres para o uso da internet no Brasil. Parentoni (2018) sustenta que essas duas leis, embora projetadas para se complementarem, possuem antinomias, as quais ensejarão casos concretos a serem enfrentados pela doutrina jurídica e jurisprudência em alguns anos[23].

Sobre a LGPD, Pinheiro (2018) assevera que a lei visa a salvaguardar direitos fundamentais de liberdade e privacidade, além do livre desenvolvimento da personalidade da pessoa natural, devendo ser observada a boa-fé em todo e qualquer tratamento de dados pessoais. Tal perpassa, simultaneamente, pelo atendimento de princípios e itens de controles técnicos de governança da informação, na fase de uso da informação que determine ou possa determinar uma pessoa, mesmo que indiretamente.

No mesmo sentido, Artese (2019, p. 499) alerta que

> [...] embora o ponto de partida dos direitos fundamentais seja vital para qualquer consideração de natureza jurídica a respeito, a discussão restrita a nível superior deixa de considerar elemento central da proteção de dados pessoais: o pressuposto de que o tratamento de dados pessoais é, em si, atividade de risco. Colocado de outra forma, o controlador dos dados pessoais, ao tratá-los, assume o risco de causar danos ao titular, e deve responsabilizar-se por isso.

A LGPD conta com dez capítulos – com as alterações e acréscimos operados pela Lei nº 13.853/2019, resultante da conversação da Medida Provisória nº 869, de 28 de dezembro de 2018, que trouxe importantes

20 Regulamento Geral sobre a Proteção de Dados aplicável em todos os países da UE a partir de 25 de maio de 2018. **EUR-Lex**, 2019. Disponível em: <https://eur-lex.europa.eu/content/news/general-data-protection-regulation-GDPR-applies-from-25-May-2018.html?locale=pt>. Acesso em: 1º maio 2019.

21 No Brasil, outras 40 normas já se referiam ao tema, de modo direto ou indireto. E, com a edição da Lei Geral, o país passou a figurar dentre os mais de 100 países que se preocupam com o adequado tratamento de dados pessoais (MONTEIRO, 2018, n.p.).

22 Art. 60 da Lei nº 13.709/2018.

23 E não é só. Tais antinomias também se percebem entre a LGPD e a Lei nº 12.527/2011 (Lei de Acesso à Informação – LAI), e entre a LGPD e a Lei nº 12.414/2011 e suas as alterações promovidas pela Lei Complementar nº 166/2019.

modificações ao texto original – mantidas pela Lei nº 13.853/2019[24] –, dentre as quais se destacam o elastecimento do prazo de *vacatio legis* (art. 65, II; dos iniciais 18 meses para 24 meses)[25], e a (tão aguardada) criação da Autoridade Nacional de Proteção de Dados e do Conselho Nacional, matéria objeto de veto presidencial no texto primeiro da LGPD (arts. 55 a 59), por identificado vício de inconstitucionalidade do processo legislativo respectivo[26].

Para a LGPD, dado pessoal corresponde a qualquer "informação relacionada a pessoa natural identificada ou identificável[27]" (art. 5°, inciso I), ao passo que dado pessoal sensível é o "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (art. 5°, inciso II). Aos dados pessoais de crianças e adolescentes a lei dispensa tratamento especial (Seção III, Capítulo II, da Lei nº 13.709/2018).

A propósito, Artese (2019, p. 501) ressalta que

> [...] dados anônimos, portanto, não são passíveis de proteção, ou o são, apenas, na medida em que puderem, por meios técnicos razoavelmente disponíveis, associar-se direta ou indiretamente a uma pessoa. A definição de dados pessoais é, portanto, elemento essencial para aplicação da lei, na medida em que apenas dados pessoais são objeto da proteção legal.

Dado pessoal, pode-se concluir, não é apenas aquele que identifica diretamente uma pessoa física, e sim, também, aquele por meio do qual se pode chegar até ela, ainda que indiretamente e/ou por meio de reversão de processos de pseudoanonimização[28]. Sua violação deve ser punida e, mais severamente, quando estiver relacionada a dados pessoais sensíveis. É preciso ter em mente que se protegem pessoas ao acautelar dados pessoais (ARTESE, 2019). Dados relacionados a pessoas jurídicas que possam levar à identificação de pessoas físicas, pelo mesmo e lógico raciocínio, igualmente carecem da proteção legal.

---

24 Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm>. Acesso em: 20 ago. 2019.

25 No tocante à Autoridade Nacional de Proteção de Dados e ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, a LGPD entrou vigor no dia 28 de dezembro de 2018 (art. 65, inciso I, da Lei nº 13.709/2018).

26 Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Msg/VEP/VEP-451.htm>. Acesso em: 8 abr. 2019.

27 Pinheiro (2018, p. 25-26) sustenta que dados pessoais são "[...] toda informação relacionada a uma pessoa identificada ou identificável, não se limitando, portanto, a nome, sobrenome, apelido, idade, endereço residencial ou eletrônico, podendo incluir dados de localização, placas de automóvel, perfis de compra, número de Internet Protocol (IP), dados acadêmicos, histórico de compras, entre outros. Sempre relacionados a pessoas natural viva".

28 Nos termos do art. 5º, inciso XI, da LGPD, anonimização é a "utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo". Dados anonimizados não serão considerados dados pessoais para os fins da Lei Geral, "salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido" (*caput* do art. 12 da Lei nº 13.709/2018). Conquanto a disposição deste artigo 12, *caput*, refira-se a dados anonimizados, o retorno ao *status quo ante* destes dados, tecnicamente, não é possível. O que se pode reverter é o processo de pseudoanomização.

Oportuna a reflexão de Bioni (2018, p. 98-99), na ideia de que outros direitos e garantias fundamentais, além da privacidade, estão ligados à proteção de dados pessoais:

> A dinâmica de proteção dos dados pessoais foge à dicotomia do público e do privado, diferenciando-se substancialmente do direito à privacidade. Propugnar que o direito à proteção de dados pessoais seria uma mera evolução do direito à privacidade é uma construção dogmática falha que dificulta a sua compreensão. É um direito que opera fora da lógica binária do público e do privado, bastando que a informação esteja atrelada a uma pessoa – conceito de dado pessoal – para deflagrá-lo.

A LGPD impõe-se às pessoas naturais ou jurídicas de direito público ou privado que realizem operações de tratamento de dados – consistente em

> toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (art. 5°, inciso X, da Lei nº 13.709/2018).

Isso se dá "independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados", desde que

> a operação de tratamento seja realizada no território nacional, a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional ou os dados pessoais objeto do tratamento tenham sido coletados no Brasil (art. 3°, *caput* e incisos I a III, da Lei nº 13.709/2018).

Vê-se, portanto, que também a LGPD tem aplicação extraterritorial.

Quando da manipulação de dados pessoais, deve-se ter em conta, obrigatória e cumulativamente, a boa-fé (objetiva) e os princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados[29], transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas, e, em regra, o consentimento – "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (art. 5°, XII, da Lei nº 13.709/2018) – do titular desses dados.

Esse consentimento é um dos pilares da LGPD, como também são os direitos do titular de dados pessoais, os (referidos) princípios e o (severo) regime sancionatório erigidos pelo normativo; a comprovação do consentimento é mais um dos inúmeros desafios àqueles a quem essa nova lei se impõe.

Há na LGPD um capítulo dedicado ao Tratamento de Dados Pessoais pelo Poder Público – inaugurado pelo art. 23, no qual há a previsão expressa de sua aplicação ao Ministério Público, já que integrante do rol do parágrafo

29 Art. 6°, incisos I a X, da Lei nº 13.709/2018.

único do art. 1° da Lei nº 12.527/2011 (Lei de Acesso à Informação ou apenas LAI)[30].

Esse tratamento de dados pessoais realizado pelo Poder Público, com o propósito de "executar as competências legais ou cumprir as atribuições legais do serviço público", tal qual as demais atividades por ele desenvolvidas, "deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público", desde que

> sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos; e seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do artigo 39 desta Lei (art. 23, incisos I e III, da Lei nº 13.709/2018).

A LGPD dedicou seu capítulo VI para tratar dos agentes de tratamento de dados pessoais: controlador, operador e encarregado, pessoas naturais ou jurídicas, de direito público ou privado (inclusive o encarregado, pós edição da MP 869/2018 – arts. 5º, incisos VI a VIII, e 37 a 41, da Lei nº 13.709/2018[31] –; alteração mantida pela Lei nº 13.853/2019).

O controlador é o tomador de decisão; a ele competem as decisões referentes ao tratamento de dados pessoais. O operador é o que realiza esse tratamento em nome do controlador. Já o encarregado é a pessoa indicada pelo primeiro para atuar como canal de comunicação entre ele, os titulares de dados pessoais e a Autoridade Nacional de Proteção de Dados, agente obrigatório, como acima enunciado, no setor público (art. 23, inc. III, da Lei nº 13.709/2018). Identificar esses atores[32], posições e perfis em cada instituição, notadamente em cada ramo do Ministério Público brasileiro, é outro dos desafios da LGPD.

Os dados pessoais submetidos a tratamento pelo Poder Público "deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral" (art. 25 da Lei nº 13.709/2018), e o compartilhamento "deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas", atendidos os princípios de proteção de dados previstos na lei (art. 26, *caput*, da Lei nº 13.709/2018).

---

30 Art. 1º. [...] Parágrafo único. Subordinam-se ao regime desta Lei:
I - os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público;
II - as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios

31 EBERLIN, Fernando B. von T. As alterações na LGPD e a criação da Autoridade Nacional de Proteção de dados. **Conjur**, 2019. Disponível em: <https://www.conjur.com.br/2019-jan-05/fernando-eberlin-lgpd-criacao-entidade-protecao-dados>. Acesso em: 7 mar. 2019.

32 Registra-se que há previsão, na LGPD, de responsabilização solidária do controlador e do operador na reparação de danos (patrimoniais ou morais, individuais ou coletivos) que provocarem em decorrência da atividade de tratamento.

Há hipóteses de transferências (a entidades privadas) de dados pessoais constantes de bases de dados a que o Poder Público tenha acesso (art. 26, §1º, incisos I, III a V, da Lei nº 13.709/2018[33]) – em regra, esse compartilhamento é vedado. Em tais casos, está dispensada a necessidade de comunicação de tais transferências à autoridade nacional (art. 27 da Lei nº 13.709/2018).

Previsão legal que também deve ser pontuada é a possibilidade de transferência internacional de dados, autorizada no artigo 33 da LGPD, destacando-se os casos em que a transferência for necessária (1) para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional ou (2) para proteção da vida ou da incolumidade física do titular ou de terceiro, quando a transferência resultar em compromisso assumido em acordo de cooperação internacional, e (3) quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do *caput* do artigo 23 da Lei. Faz-se o registro, por mais uma vez, de que, dentre as atribuições do CNMP firmadas na Resolução nº 156/2016, está a de "firmar instrumentos de cooperação técnica com o Conselho Nacional de Justiça – CNJ, com o Poder Judiciário, com órgãos de inteligência nacionais e internacionais e com outras instituições".

Às entidades e órgãos públicos, em caso de violação à LGPD, impõem-se sanções administrativas, estabelecidas em procedimento próprio – sem prejuízo do disposto nas Leis nº 8.112/1990 (Estatuto do Servidor Público Federal), nº 8.429/1992 (Lei de Improbidade Administrativa) e nº 12.527/2011 (Lei de Acesso à Informação) –, quais sejam: advertência, publicização da infração após devidamente apurada e confirmada a sua ocorrência, bloqueio dos dados pessoais a que se refere a infração até a sua regularização e eliminação dos dados pessoais a que se refere a infração. As multas, que podem atingir o patamar máximo R$ 50.000.000,00 (cinquenta milhões de reais) por infração, não se aplicam ao Poder Público (art. 52, §3°, da Lei nº 13.709/2018).

Importante anotar, por fim, que o Ministério Público tem assento no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, representado por um membro a ser indicado pelo Conselho Nacional do Ministério Público (art. 58-A, inciso V e §2º, da Lei nº 13.709/2018).

A conformidade é um desafio, conjunto e urgente. Contudo, a LGPD excepciona a sua aplicação, dentre outros, para fins exclusivos de segurança

33 Art. 26. [...]
§ 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:
I - em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação);
II - (VETADO);
III - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.
IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou (Incluído pela Lei nº 13.853, de 2019)
V - na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades. (Incluído pela Lei nº 13.853, de 2019)

pública, segurança do Estado ou atividades de investigação e repressão de infrações penais (art. 4º, inciso III, a, c e d), e é disso que trataremos a seguir.

4. A SEGURANÇA INSTITUCIONAL DO MINISTÉRIO PÚBLICO BRASILEIRO E A LGPD

A principal constatação, por meio do estudo da nova legislação, é de que para fins da atividade de segurança institucional do Ministério Público brasileiro, a LGPD, como regra geral, pode ser afastada. À semelhança do normativo europeu (GDPR), a LGPD, em seu artigo 4º, relaciona os casos de tratamento de dados pessoais que não se submetem a ela. Dentre eles estão os realizados para fins exclusivos de segurança pública, segurança do Estado e/ou atividades de investigação e repressão de infrações penais (alíneas *a*, *c* e *d*, do inciso III).

Rosso (2019) sustenta que a exceção, de um lado, é oportuna, uma vez que cumpre ao Estado, por exemplo, controlar os dados de todo o sistema penitenciário e investigar fatos que ponham em risco a segurança pública e o próprio Estado. De outro, porém, como são inúmeras as situações que demandam a intervenção estatal, a justificativa de agir em nome da segurança pública não pode legitimar a prática de abusos pelo Poder Público. Tanto é que a lei, embora excepcione sua aplicação nos casos do artigo 4º, inciso III, determina que tais casos serão disciplinados por lei própria e deverão respeitar os princípios constitucionais atinentes.

Está posto no § 1° do artigo 4º da LGPD:

> O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

Sua interpretação literal pode levar a compreensão (equivocada) de que os princípios de proteção de dados previstos na LGPD, quando da realização do tratamento de dados pessoais, nos casos do artigo 4º, inciso III, podem causar entrave no desenvolvimento da atividade de Inteligência. Afinal, por exemplo, como se poderia assegurar os princípios do livre acesso e da transparência ou o direito à anonimização de dados pessoais ou dados sensíveis na investigação de potencial ou efetivo agente hostil?

O espírito da lei é o de proteger o indivíduo de possível arbitrariedade estatal. Entretanto, não é viável defender, por exemplo, que a um investigado (titular de dados pessoais) pela prática de crime, em atenção ao princípio da transparência, sejam garantidas "informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento". E não só no âmbito criminal, como também no combate à prática de atos de improbidade administrativa, de violações aos direitos do consumidor e dos direitos humanos, ou seja, na sua atividade-fim. O atendimento de direito individual, no caso, em detrimento do interesse público, comprometeria a segurança de toda a sociedade. Aliás, o compartilhamento de informações é que potencializa

o combate (garantindo-lhe eficácia) contra a criminalidade organizada. Isso significa dizer que tratar dados é, também, compartilhar informações entre instituições. No Ministério Público catarinense, por exemplo, até o momento, há algumas dezenas de bancos de dados compartilhados com outras instituições (públicas e privadas), que garantem o cumprimento da missão institucional com maior efetividade.

Além disso, a segurança pessoal de agentes estatais, como é o caso dos membros do Ministério Público, perpassa pela prática sistemática de atividades de Inteligência e Contrainteligência, com o propósito de antever (identificar) possíveis ou reais ameaças e neutralizá-las ou, se ocorrerem, mitigá-las. Assim, evita-se o comprometimento do livre e desembaraçado exercício do múnus ministerial e se resguarda o interesse público.

Neste estudo não se tem o propósito de defender a vigilância imotivada, a arbitrária invasão à privacidade alheia desprovida de quaisquer regramentos. Tampouco se está a confundir sigilo – aquilo que não pode ser revelado, não ostensivo, característica marcante das atividades Inteligência e Contrainteligência – com privacidade, que consiste naquilo que é particular, que diz respeito à pessoa. Porém, não restam dúvidas de que tais atividades necessária e legalmente continuarão sendo desenvolvidas, mesmo com o advento da LGPD.

Resgatando a Lei nº 12.527/2011, a Lei de Acesso à Informação (LAI), reconhece-se, conforme Angelico (2015), que há limites legais do acesso à informação. Esses limites legais estão contidos nos acordos internacionais e devem estar expressamente previstos em lei.

A lei específica (art. 4º, §1°, da LGPD), que ainda precisa ser editada, é fundamental para definição do alcance da norma e proteção de todos os envolvidos. Previsão expressa de que atividades de Inteligência e Contrainteligência desenvolvidas no interesse público estão fora do seu alcance seria importante, mas eventual ausência, num sistema legal integrativo, por certo não obsta que sejam desenvolvidas.

5. CONCLUSÕES

Ao tempo em que mudanças no mundo estão ocorrendo de maneira bastante acelerada, a relação entre o cidadão e o Poder Público, da mesma forma, está se aperfeiçoando. Em um caminho sem volta. Nos regimes democráticos, como no Brasil, exsurge o anseio popular cada vez mais intenso, pela transparência, qualidade e probidade das atividades e serviços estatais, nele incluído, o fim a que se destina a Instituição Ministério Público. Como diz Schiefler (2019, p. 33), "o Poder Público brasileiro deve se preparar para receber essa nova realidade e responder, de maneira eficiente, às demandas da sociedade – que busca, primordialmente, maior transparência e efetividade".

Destaca-se, nesse contexto, que o próprio setor público está se tornando cada vez mais digital (Lei nº 12.414/2011 – Cadastro Positivo – e o Documento Nacional de Identidade (DNI); IRPF; e-Social; Nota Fiscal

Eletrônica; SUS e SUSP; monitoramento eletrônico, hackaton, *blockchain* e *smart contracts*, dentre muitos outros). Essa é uma trajetória sem retrocesso e uma estratégia louvável para se aproximar dos cidadãos e facilitar o acesso à informação e à prestação dos seus serviços. No entanto, impõe-se a ele o uso de legais e boas práticas, notadamente de segurança e proteção de dados pessoais. A LGPD passa a ser mais uma ferramenta de relacionamento escorreito entre os cidadãos e as pessoas jurídicas de direito público e de direito privado, a exigir absoluto respeito no tratamento de todo e qualquer dado pessoal.

Como uma exigência mundial, a LGPD foi aprovada no Brasil para se inserir nos quadros dos acordos internacionais e garantir as relações internacionais entre setores econômicos e estatais, especialmente em relação aos países que já possuem legislação correlata. A inclusão do Poder Público no seu alcance foi acertada, assim como as respectivas hipóteses de exclusão da ingerência desse normativo.

O presente estudo buscou discutir a incidência da LGPD no Poder Público, mais especificamente o seu impacto nas atividades de Segurança Institucional (Inteligência e Contrainteligência) do Ministério Público. Dentre as preocupações relacionadas ao Ministério Público brasileiro tem-se se o atendimento (simultâneo) dos princípios gerais de proteção de dados, nas atividades de segurança pública, segurança do Estado e atividades de investigação e repressão de infrações penais e como essa regulamentação pode comprometer e privilegiar um ou mais indivíduos, em detrimento de toda a sociedade.

Observou-se que a LGPD é um avanço necessário à proteção das garantias individuais, todavia, a despeito de inexistir previsão expressa, não compromete o desenvolvimento das atividades de Inteligência e Contrainteligência, que são essenciais às atividades de diferentes instituições do Poder Público, assim como para o Ministério Público.

Muito pode ser cogitado pelas provocações lançadas neste inaugural ensaio acerca de tão importante quebra de paradigma, da verdadeira disrupção legislativa – quebra ou descontinuação, mesmo, do processo de tratamento de dados até então estabelecido –, que é o objeto deste despretensioso ensaio.

Essa é a realidade. Na perspectiva de que possuir bancos de dados pessoais constitui-se verdadeira atividade de risco, o Ministério Público brasileiro precisa estar preparado para o enfrentamento das questões que surgirão com a entrada em vigor (na íntegra) da Lei nº 13.709/2018. Isso porque, dentre os instrumentos utilizados para o bom desempenho das funções constitucionais ministeriais está o uso (devido) de bancos de dados pessoais. É imprescindível, portanto, a continuidade e ampliação das discussões acerca da Lei Geral de Proteção de Dados, notadamente sobre o seu impacto, não apenas nas ações de segurança institucional do Ministério Público, mas naquelas afetas às tarefas de gestão e à atividade-fim desta Instituição.

6. REFERÊNCIAS

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA (ABIN). Cronologia de criação dos Órgãos de Inteligência de Estado no Brasil. **ABIN**. Disponível em: <http://www.abin.gov.br/institucional/historico/>. Acesso em: 22 abr. 2019.

ANGELICO, Fabiano. **Lei de Acesso à Informação**: reforço ao controle democrático. São Paulo: Estúdio Editores.com, 2015.

ARTESE, Gustavo. *Compliance* digital: proteção de dados pessoais. In: CARVALHO, André C.; BERTOCCELLI, Rodrigo de P.; ALVIM, Tiago C.; VENTURINI, Otávio (Coord). **Manual de *compliance***. Rio de Janeiro: Forense, 2019.

BIONI, Bruno Ricardo. **Proteção de dados pessoais, a função e os limites do consentimento.** Rio de Janeiro: Forense, 2018.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 1º abr. 2019.

BRASIL. **Medida provisória nº 869, de 27 de dezembro de 2018**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Mpv/mpv869.htm>. Acesso em: 1º abr. 2019.

_____. **Mensagem nº 451, de 14 de agosto de 2018.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Msg/VEP/VEP-451.htm>. Acesso em: 8 abr. 2019.

CIO. 10 principais tecnologias emergentes de 2018, segundo o WEF. **CIO**, 2019. Disponível em: <https://cio.com.br/10-principais-tecnologias-emergentes-de-2018-segundo-o-wef/>. Acesso em: 22 abr. 2019.

COELHO, Lucas. *Analytics*: o que é, conceito e definição. **Cetax**. Disponível em: <https://www.cetax.com.br/blog/o-que-e-analytics/>. Acesso em: 1º fev. 2019.

COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS. **Convenção para a Protecção das Pessoas relativamente ao tratamento automatizado de dados de carácter pessoal**. Disponível em: <https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm>. Acesso em: 18 abr. 2019.

DICIONÁRIO ONLINE DE PORTUGUÊS. Disponível em: <https://www.dicio.com.br/disrupcao/>. Acesso em: 22 abr. 2019.

EBERLIN, Fernando B. von T. As alterações na LGPD e a criação da Autoridade Nacional de Proteção de dados. **Conjur**, 2019. Disponível em: <https://www.conjur.com.br/2019-jan-05/fernando-eberlin-lgpd-criacao-entidade-protecao-dados>. Acesso em: 7 mar. 2019.

ESTADÃO. Entenda o escândalo do uso de dados do facebook pela cambridge analytica. **Estadão**, 2019. Disponível em: <https://link.estadao.com.br/galerias/geral,entenda-o-escandalo-do-uso-de-dados-do-facebook-pela-cambridge-analytica,36615>. Acesso em: 16 abr. 2019.

EUR-LEX. Regulamento Geral sobre a Proteção de Dados aplicável em todos os países da UE a partir de 25 de maio de 2018. **EUR-Lex**, 2019. Disponível em: <https://eur-lex.europa.eu/content/news/general-data-protection-regulation-GDPR-applies-from-25-May-2018.html?locale=pt>. Acesso em: 1º maio 2019.

FERREIRA, Ricardo Barretto; BRANCHER, Paulo; TALIBERTI, Camila; CUNHA, Vitor Koketu da. Entra em vigor o Regulamento Geral de Proteção de Dados da União Europeia. **Migalhas**, 2018. Disponível em: <https://www.migalhas.com.br/dePeso/16,MI281042,81042-Entra+em+vigor+o+Regulamento+Geral+de+Protecao+de+Dados+da+Uniao>. Acesso em: 1º maio 2019.

G1.GLOBO. França multa Google em 50 milhões de euros por violação de lei de privacidade na UE. **G1.globo**, 2019. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2019/01/21/franca-multa-google-em-50-milhoes-de-euros-por-violacao-de-lei-de-privacidade-na-ue.ghtml>. Acesso em: 1º maio 2019.

MILT, Kristiina. **Proteção dos dados pessoais**. Disponível em: <http://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf>. Acesso em: 8 maio 2019.

MONTEIRO, Renato Leite. Lei Geral de Proteção de Dados do Brasil: análise contextual detalhada. **Jota**, 2018. Disponível em: <https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/lgpd-analise-detalhada-14072018>. Acesso em: 25 mar. 2019.

MOREIRA, André de Oliveira Schenini. A lei de proteção de dados pessoais da União Europeia (GDPR) e sua aplicação extraterritorial às entidades e empresas brasileiras. **Migalhas**, 2019. Disponível em: <https://www.migalhas.com.br/dePeso/16,MI267772,81042-A+lei+de+protecao+de+dados+pessoais+da+Uniao+Europeia+GDPR+e+sua>. Acesso em: 18 abr. 2019.

PACHECO, Denilson Feitosa. Atividade de Inteligência no Ministério Público. In: BRANDÃO, Priscila C.; CEPIK, Marco. (Org.). **Inteligência de Segurança Pública, Teoria e Prática no Controle da Criminalidade.** Rio de Janeiro: Impetus, 2013.

PARENTONI, Leonardo. Lei Geral de Proteção de dados v. Marco Civil da Internet: Antinomias. **DTIBR**, 2018. Disponível em: <https://www.dtibr.com/single-post/2018/09/10/LEI-GERAL-DE-PROTE%C3%87%C3%83O-DE-DADOS-v-MARCO-CIVIL-DA-INTERNET-ANTINOMIAS>. Acesso em: 19 abr. 2019.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais, comentários à Lei nº 13.709/2018 (LGPD).** São Paulo: Saraiva Jur, 2018.

RONCOLATO, Murilo. O que diz a nova lei de proteção de dados da Europa. E o efeito no Brasil. **Nexo Jornal**, 2018. Disponível em: <https://www.nexojornal.com.br/expresso/2018/05/25/O-que-diz-a-nova-lei-de-prote%C3%A7%C3%A3o-de-dados-da-Europa.-E-o-efeito-no-Brasil/>. Acesso em: 18 abr. 2019.

ROSSO, Angela Maria. LGPD e setor público: aspectos gerais e desafios. **Migalhas**, 2019. Disponível em: <https://www.migalhas.com.br/dePeso/16,MI300585,31047-LGPD+e+setor+publico+aspectos+gerais+e+desafios>. Acesso em: 18 abr. 2019.

SCHIEFLER, Eduardo André Carvalho. **Processo Administrativo Eletrônico**. Rio de Janeiro: Lumen Juris, 2019.

VALENTINO-DEVRIES, Jennifer. Polícia usa dados de localização do Google em investigações nos EUA. **Folha de São Paulo**, 2019. Disponível em: <https://www1.folha.uol.com.br/mundo/2019/04/policia-usa-dados-de-localizacao-do-google-em-investigacoes-nos-eua.shtml>. Acesso em: 22 abr. 2019.

WIKIPÉDIA, a enciclopédia livre. Disponível em: <https://pt.wikipedia.org/wiki/GAFAM>. Acesso em: 1º maio 2019.

INTELIGÊNCIA E SEGURANÇA INSTITUCIONAL: UMA ABORDAGEM SOBRE A SEGURANÇA DE ÁREAS E INSTALAÇÕES NO MINISTÉRIO PÚBLICO

Ricardo Caron[1]

Vani Antônio Bueno[2]

SUMÁRIO: 1. Introdução. 2. A atividade de inteligência no Ministério Público. 3. Salvaguarda de ativos por meio da Contrainteligência. 4. Segurança de áreas e instalações. 4.1. Delimitação de perímetros. 4.2. Demarcação de áreas e instalações. 4.3. Implantação de barreiras. 4.4. Controle de acesso. 4.5. Detecção de intrusão e monitoramento eletrônico. 4.6. Planejamento de emergência. 5. Análise de risco para segurança orgânica. 6. Cultura de segurança. 7. Considerações finais. 8. Referências.

RESUMO: Este artigo objetiva reunir conhecimentos acerca do conjunto de normas, medidas e procedimentos voltados à proteção das dependências da instituição, especialmente aquelas consideradas críticas e sigilosas. As ações preventivas visam a prevenir acessos não autorizados, danos e interferências, tendo por critério as características dos ativos a serem protegidos e as vulnerabilidades e ameaças a que estão expostos. Para tanto foi conduzido um estudo de caráter exploratório, utilizando-se de revisão bibliográfica e documental. O tema escolhido apresenta relevância no contexto da segurança institucional, uma vez que as medidas de segurança para áreas e instalações dão suporte e eficácia às demais atividades de segurança orgânica. Dentre o conjunto de normas e medidas destinadas a garantir o funcionamento da instituição, as ações para áreas e instalações são as que exigem maior integração, pois grande parte da atividade institucional se concentra nesse ambiente. As medidas de proteção mencionadas integram um Plano de Segurança Orgânica, e sua elaboração é antecedida por uma

1 Capitão da Polícia Militar do Paraná com o Curso de Aperfeiçoamento de Oficiais. Bacharel em Administração de Empresas. Especialista em Inteligência, em Administração Pública e Direito Penal e Processual Penal. Instrutor da Academia Policial Militar do Guatupê e da Diretoria de Inteligência da Secretaria Operações Integradas/ Ministério da Justiça. Coordenador do Núcleo de Inteligência Policial Militar do Ministério Público do Estado do Paraná.

2 Procurador de Justiça do Ministério Público do Estado do Paraná. Membro Colaborador da Comissão de Preservação da Autonomia do Ministério Público (CPAMP), do Conselho Nacional do Ministério Público, na área de Segurança Institucional. Membro integrante da Secretaria Executiva de Segurança Institucional-SESI, do Sistema Nacional de Segurança Institucional do Ministério Público.

Análise de Risco. A omissão dessa análise prévia poderá acarretar comprometimento de segurança por insuficiência ou inadequação. Finalmente, é inegável a necessidade do envolvimento do público interno e o desenvolvimento de uma cultura de proteção para a obtenção de níveis satisfatórios de segurança.

PALAVRAS-CHAVE: Ministério Público. Segurança Institucional. Atividade de Inteligência. Segurança Orgânica. Áreas e Instalações.

1. INTRODUÇÃO

A segurança institucional compreende um conjunto de medidas voltadas para a proteção dos ativos institucionais e para detectar e neutralizar ameaças à salvaguarda da instituição e de seus integrantes, à imagem e à reputação. Essas medidas abrangem dois segmentos de atuação, a segurança orgânica e a segurança ativa: aquela, de caráter preventivo, é composta pela segurança de pessoas, do material, das áreas e instalações e da informação; esta, com característica ofensiva e proativa, engloba as medidas de contrassabotagem, contraespionagem, contrapropaganda e contra o crime organizado.

Cumpre destacar que a segurança institucional assegura as condições necessárias para o desenvolvimento das atividades da instituição e de seus integrantes e o exercício livre e independente das funções constitucionais do Ministério Público (CNMP, 2016; FARAH, 2013).

A segurança institucional tem como princípios a abrangência, o enfoque sistêmico e a proatividade e deve ser entendida como a capacidade de prevenção, considerando atitudes, comportamentos e consciência a respeito das normas de segurança de uma instituição (FARAH, 2013).

Coadunada com as atribuições da segurança institucional, está a atividade de inteligência, com o desígnio de assessorar o processo decisório e de planejamento, por meio de conhecimentos avaliados, significativos, úteis e oportunos, em um processo de redução de incertezas, além de possibilitar previsão e antecipação de prováveis cenários futuros. Mediante o ramo da Contrainteligência, busca proteger de forma constante e ininterrupta a instituição a que pertence, neutralizando ações hostis, dentro de uma concepção preventiva e proativa.

Como parte da segurança orgânica, a segurança de áreas e de instalações compreende o conjunto de medidas voltadas à proteção das dependências da instituição, notadamente naquelas onde são elaborados, tratados, manuseados ou guardados as informações sigilosas e os materiais sensíveis. Inteligência e segurança institucional atuam em conjunto e complementarmente para a consecução desses objetivos.

A presente pesquisa qualitativa utilizou a revisão bibliográfica e documental sobre o tema com o propósito de reunir conhecimentos acerca das medidas, estratégias e sistemas de proteção para áreas e instalações.

Preliminarmente analisou-se a capacidade da atividade de inteligência e sua utilização assessorial no Ministério Público, abrangendo a segurança

institucional, as decisões estratégicas e o suporte ao processo investigativo na esfera criminal.

Na sequência o estudo explorou o ramo Contrainteligência e como suas medidas se mostram profícuas no âmbito do Ministério Público, especialmente na salvaguarda dos ativos corporativos e em apoio à segurança institucional.

A segurança de áreas e instalações é examinada a seguir, onde são descritos sistemas, estratégias e medidas de proteção, com ênfase para a delimitação de perímetros, demarcação de áreas e instalações, implantação de barreiras, controle de acesso, detecção de intrusão e monitoramento eletrônico e planejamento de emergências.

Em outro passo, estudou-se a análise de risco para segurança orgânica como um método prévio de diagnóstico que condiciona a intensidade das medidas de segurança e define requisitos, com menor subjetividade.

Por fim, buscou-se demonstrar que a obtenção de níveis adequados de segurança perpassa pelas pessoas, pelo desenvolvimento de uma cultura de segurança e uma mentalidade de proteção, estabelecendo-se atitudes favoráveis, mediante as exigências da questão.

2. A ATIVIDADE DE INTELIGÊNCIA NO MINISTÉRIO PÚBLICO

Inteligência é uma atividade, que, por meio de metodologia própria e de técnicas acessórias, produz e salvaguarda conhecimentos, visando a dar suporte às autoridades na tomada de decisões, na elaboração de planejamentos, na definição de diretrizes e objetivos (FERRO JÚNIOR, 2008).

Constitui-se em um processo de redução de incertezas, pois o conhecimento disponibilizado (produto) permite que a autoridade (cliente) compreenda as consequências de se adotar uma determinada ação (FERRO JÚNIOR; OLIVEIRA FILHO; PETRO, 2008).

Mediante uma perspectiva da utilização, revelam-se três características fundamentais da inteligência: previsão, antecipação e assessoramento (FERRO JÚNIOR; OLIVEIRA FILHO; PETRO, 2008); acentuando-se que o assessoramento é feito nos níveis político, estratégico, tático e operacional (BRASIL, 2015b).

Inteligência como atividade não se concerne a uma modalidade ou especialidade de investigação, mas a uma metodologia de caráter assessorial, que objetiva a produção de conhecimentos com conteúdo preciso, oportuno, útil e significativo, cuja finalidade precípua é auxiliar o processo decisório. Todavia, subsiste a compreensão de que a metodologia de produção de conhecimento contribui com o processo investigatório, por meio da formulação de convicção fundamentada, esta capaz de auxiliar a tomada de decisão, e, em alguns casos, antecipar-se ao cometimento de condutas. Ferro Júnior (2007) comunga desse entendimento ao afirmar que métodos de inteligência ampliam a capacidade da investigação e de solução

de crimes complexos, e, por intermédio dela, "as organizações policiais buscam obter o poder de antecipação" (p. 117).

Evidencia-se que a inteligência detém importância na atuação repressiva, mas é insigne na preventiva, antecipando-se ao cometimento de fatos, tendo grande utilidade no planejamento de estratégias de ação (GONÇALVES, 2010).

A inteligência é compreendida por Sherman Kent (1967), na clássica obra *Strategic Intelligence for American World Policy*, sobre três facetas: produto, organização e processo. Gonçalves (2010) esclarece essa acepção trina da inteligência construída por Sherman Kent:

> Inteligência como produto, conhecimento produzido: trata-se do resultado do processo de produção de conhecimento e que tem como cliente o tomador de decisão em diferentes níveis. [...] Inteligência é, portanto, conhecimento produzido.
>
> Inteligência como organização: diz respeito às estruturas funcionais que têm como missão primordial a obtenção de informações e produção de conhecimento de inteligência. Em outras palavras, são as organizações que atuam na busca do dado negado, na produção de inteligência e na salvaguarda dessas informações, os serviços secretos.
>
> Inteligência como atividade e processo: refere-se aos meios pelos quais certos tipos de informação são requeridos, reunidos (por meio de coleta ou busca), analisados e difundidos, e, ainda, os procedimentos para a obtenção de determinados dados, em especial aqueles protegidos, também chamados de "dados negados". Esse processo segue metodologia própria, a metodologia de produção de conhecimento, ensinada nas escolas de inteligência por todo globo (GONÇALVES, 2010, p. 7 e 8).

Ao referir-se essencialmente à produção de conhecimento, resta entendido como um processo formal que transforma "dados e/ou conhecimentos anteriores em conhecimentos avaliados, significativos, úteis, oportunos e seguros" (BRASIL, 2015b, p. 23), por meio de técnicas específicas e metodologia própria. Para que o produto da inteligência possa assessorar adequadamente o processo decisório, é imperativo o uso correto de metodologia, procedimentos e técnicas, excluindo a prática de ações meramente intuitivas, opiniões pessoais e procedimentos sem orientação racional (BRASIL, 2015b).

Ainda, sobre o método utilizado pela inteligência, Almeida Neto (2009, p. 50) complementa:

> Despiciendo lembrar que o método de construção do conhecimento de inteligência e, por conseguinte, o ciclo de tal atividade, foram forjados a partir de um específico critério de aceitabilidade da verdade, imbuído da primazia dos princípios da oportunidade e utilidade sobre a própria verificabilidade do conhecimento produzido (possibilidade do conhecimento ser testado).

A atividade de inteligência possui dois ramos: a Inteligência e a Contrainteligência. De forma elementar, o primeiro destina-se à produção de conhecimento, enquanto o segundo, a neutralizar as ações adversas e proteger a atividade e a instituição a que pertence. Os dois ramos estão

intrinsicamente ligados, não possuindo limites precisos, uma vez que inter-relacionam e se interdependem (BRASIL, 2015b).

Além de produzir conhecimentos em ambos os ramos, a atividade desenvolve ações especializadas para a obtenção de dados negados de difícil acesso e/ou para neutralizar ações adversas. As denominadas operações de inteligência exigem, pelas dificuldades e/ou riscos iminentes, um planejamento minucioso, um esforço concentrado, e o emprego de pessoal, técnicas e material especializados (BRASIL, 2015b).

À vista do exposto, Pacheco (2006, p. 632) ensina:

> Um órgão de inteligência se subdivide em três áreas: a) análise ou atividade de inteligência stricto sensu (produção de conhecimento, que é documentado e disseminado na forma de relatórios de inteligência, a saber - informe, apreciação, informação e estimativa); b) contrainteligência (proteção dos dados, informações e conhecimentos de uma instituição, por meio da segurança do pessoal, segurança da documentação e material, segurança das áreas e instalações, e segurança dos sistemas de informações - comunicações e informática); c) operações de inteligência (busca do dado e/ou da informação negados ou não disponibilizados).

O desígnio da atividade de inteligência concerne à obtenção e análise de dados e informações, para a produção de conhecimentos que subsidiem o processo decisório de diferentes atividades e níveis (GONÇALVES, 2008). Isto posto, "onde houver planejamento e processo decisório, a atividade de inteligência – em suas diferentes modalidades – mostra-se útil" (GONÇALVES, 2008, p. 143).

No que se refere às diferentes modalidades de inteligência, Gonçalves (2008) identifica as seguintes: inteligência militar e de defesa (defesa nacional em tempos de guerra e paz), inteligência policial (prevenção e repressão das ações criminosas), inteligência financeira (delitos financeiros, mormente a lavagem de dinheiro), inteligência fiscal (delitos contra a ordem tributária), inteligência econômica, inteligência competitiva e inteligência estratégica, a última habitualmente relacionada à inteligência de estado (interna ou externa).

Almeida Neto (2009, p. 62) classifica as modalidades mencionadas por Gonçalves (2008) em duas grandes categorias, "de acordo com o âmbito da decisão que se pretende assessorar e da natureza jurídica das funções exercidas pelos profissionais": público ou privada. Além disso, o autor subdivide a pública em clássica (ou de Estado) e de segurança pública. A clássica, com vistas ao assessoramento de assuntos relativos às questões típicas de Estado como política externa, defesa nacional e formulação de políticas públicas, pode estar em dois grupos: militar de Estado e civil de Estado. Por sua vez, a inteligência de segurança pública pode ser segmentada em policial (ostensiva e judiciária), fiscal, financeira e ministerial (ALMEIDA NETO, 2009).

O conceito da modalidade ministerial citada por Almeida Neto (2009) foi cunhado por Pacheco (2006, p. 640), nos seguintes termos:

> Podemos, assim, generalizar a noção de inteligência de Estado para a de inteligência institucional (melhor se diria: aplicarmos a inteligência

> no âmbito de outras instituições ou órgãos públicos), abrangendo-se, desse modo, órgãos públicos em geral, inclusive os Ministérios Públicos, não somente quanto à sua área criminal, mas também quanto a todas as suas áreas. Assim, é cabível dizer-se inteligência ministerial, para se referir às atividades de inteligência institucional realizadas pelo Ministério Público.

O escopo da atividade de inteligência mantém harmonia com as funções ministeriais, e sua aplicabilidade fica demonstrada nos ensinamentos de Pacheco (2013, p. 270):

> O Ministério Público, portanto, deve utilizar-se de métodos, técnicas e ferramentas adequadas para lidar com as informações necessárias ao desempenho de suas finalidades constitucionais, sejam aqueles convencionalmente denominados "atividade de inteligência", sejam, numa visão mais "gerencial", seus equivalentes dos sistemas de gestão da informação e da inteligência competitiva. Diante da crescente complexidade dos fatos com os quais lida o Ministério Público e a necessidade de sua atuação sistêmica, seja na área cível (por exemplo, ações civis para defesa de interesses difusos e coletivos), seja penal (por exemplo, programas de prevenção e repressão à criminalidade), o certo é que o Ministério Público deve utilizar algum sistema de gestão da informação, superando a fase individualista e amadorística de muitos de seus membros, e alcançando a racionalidade gerencial exigida pelo princípio constitucional da eficiência.

Para Almeida Neto (2009), a inteligência ministerial não se restringe ao assessoramento de decisões ao âmbito criminal e da segurança pública, mas envolve também todas aquelas que serão tomadas, com o objetivo de cumprir a missão institucional do Ministério Público. Nessa lógica Nobre (2014) afirma que a inteligência, nos níveis estratégico e tático, pode assessorar os decisores no campo político ou na definição dos rumos institucionais, colaborando na elaboração de planejamentos, na definição de diretrizes e objetivos (FERRO JÚNIOR, 2008), na implantação de planos e programas. No âmbito operacional, o assessoramento oportuniza suporte às investigações criminais mais complexas, viabilizando melhores meios de se produzir provas (sem que necessariamente as produza), ou ainda, quando o sigilo e a compartimentação assim exigirem (NOBRE, 2014; CASTRO; RONDON FILHO, 2012).

Dantas Filho (2013), Pacheco (2013) e Almeida Neto (2009) complementam as funções da inteligência no Ministério Público, ao destacar a utilização dos métodos de Contrainteligência no âmbito institucional, especialmente no que concerne à segurança institucional. Ao ratificar isso, o último autor assim se expressa:

> É fato que, à medida que o Ministério Público avança no cumprimento de suas funções em direção as classes mais abastadas da sociedade e aos funcionários públicos e políticos mais poderosos, as ameaças sobre a instituição aumentam e os seus membros se veem, cada dia mais, vulneráveis [...]. A própria instituição em si, não raro, torna-se vítima dessas ações, seja por intermédio de desinformações maliciosamente articuladas, seja por sabotagens, cooptações, infiltração de criminosos em seu seio (inclusive por intermédio de contratações de serviços terceirizados sem o devido acompanhamento), entre outras, que, não raro, poderiam ser devidamente evitadas (ou cujos prejuízos poderiam ser minimizados) com a realização de uma atividade responsável de

> Contrainteligência por um pessoal orgânico devidamente treinado (ALMEIDA NETO, 2009, p. 130).

Com vistas à proteção e à salvaguarda da instituição e de seus integrantes e à melhoria de processos, Dantas Filho (2013) e Almeida Neto (2009) sugerem a criação de um sistema de inteligência que integre os diferentes ramos do Ministério Público brasileiro e assegure o fluxo constante de informações. O primeiro autor desta forma se manifesta sobre isso:

> Este Sistema deve ser organizado e voltado para o ambiente interno da instituição e para o ambiente externo. Além de monitorar os pontos fortes e os pontos fracos das organizações, as ameaças e oportunidades exteriores, o Sistema deve coletar dados, informações e conhecimentos necessários à otimização do desempenho e da segurança do MP, no âmbito pessoal, material e documental (DANTAS FILHO, 2013, p. 107).

Nesse passo fica estabelecido que a inteligência ministerial se refere às atividades de inteligência institucional realizadas pelo Ministério Público (PACHECO, 2006), abrangendo o assessoramento na esfera criminal (ALMEIDA NETO, 2009), nas decisões políticas e dos rumos institucionais (NOBRE, 2014; FERRO JÚNIOR, 2008), e na segurança da instituição e de seus integrantes (DANTAS FILHO, 2013; ALMEIDA NETO, 2009).

3. SALVAGUARDA DE ATIVOS POR MEIO DA CONTRAINTELIGÊNCIA

Contrainteligência é o ramo que tem por atribuição proteger a atividade de inteligência e a instituição a que pertence, mediante a produção de conhecimento e a implementação de ações voltadas à salvaguarda de dados e conhecimentos sigilosos, bem como a identificação e neutralização das ações adversas de qualquer natureza (BRASIL, 2015b). Suas atividades são desenvolvidas de forma constante e ininterrupta, buscando-se a antecipação às potenciais ações hostis, dentro de uma concepção preventiva e proativa (BRASIL, 2015a).

Lowenthal[3] citado por Gonçalves (2008) aponta três naturezas finalísticas para a Contrainteligência: a de reunião, para a identificação da capacidade do oponente; a defensiva, com o intuito de frustrar os esforços adversos; e a ofensiva, visando a neutralizar a tentativa identificada de intrusão. Nesta acepção, Gonçalves (2008, p. 179) reconhece que a Contrainteligência objetiva "tornar tão difícil quanto possível as ações adversas, tomando medidas de segurança que impeçam o acesso a tudo que se deseja manter sob sigilo e protegendo pessoal e instalações".

Ainda, no que se refere à finalidade da Contrainteligência, Almeida Neto (2009, p. 57) leciona:

> Para cumprir, a contento, a sua finalidade, a Contrainteligência, constantemente, precisa produzir conhecimento a respeito não apenas da inteligência adversa, mas também em torno das próprias

3 LOWENTHAL, Mark. **Intelligence:** from secrets to policy. Washington, D.C.: CQ Press, 2003.

> vulnerabilidades da organização, tarefa essa que acaba implicando a necessidade de um completo conhecimento desta e uma permanente busca (em sentido lato) de conhecimentos sobre as potencialidades lesivas que vão sendo disponibilizadas no mercado diariamente.

A Contrainteligência atua por meio de três segmentos: a segurança orgânica (SEGOR), a segurança ativa (SEGAT) e a segurança de assuntos internos (SAI).

A SEGOR é um conjunto de normas, procedimentos e medidas, integradas e planejadas, de caráter eminentemente defensivo, destinadas a prevenir e a obstruir as ações adversas protagonizadas por atores hostis, com vistas a proteger os ativos institucionais e garantir o funcionamento da instituição (BRASIL, 2015b; FARAH, 2013). Ativos institucionais é tudo aquilo que tem valor para a organização (ABNT, 2013), podendo ser bens tangíveis ou intangíveis. Ativos são pessoas, instalações, materiais, documentos, conhecimentos, marca, patentes, imagem, propriedade intelectual, sistemas, entre outros (FARAH, 2013; FERREIRA, 2015).

A segurança orgânica se estrutura nas medidas de segurança: de recursos humanos, dos materiais, das áreas e instalações, das comunicações e da informação (BRASIL, 2015b; FARAH, 2013). Esclarece Farah (2013, p. 15) que as normas e procedimentos de segurança orgânica permeiam mais de um conjunto de medidas, por serem integradas e complementares:

> Há que se considerar que as normas de segurança orgânica devem ser integradas e complementares. É comum uma regra de segurança permear mais de um conjunto de medidas de segurança. Por exemplo, algumas normas de segurança de áreas e instalações contribuem para a segurança da informação e devem ser integradas.

As ações defensivas são implementadas no âmbito de cada instituição, por meio de planos, programas, normas e processos, mediante um criterioso planejamento, materializado em um Plano de Segurança Orgânica (FERREIRA, 2015).

O segmento da segurança ativa institui-se em medidas proativas, destinadas a detectar, identificar, avaliar, analisar e neutralizar as ações adversas de indivíduos ou grupos, de qualquer natureza, que atentem contra a instituição. Essas medidas são desenvolvidas por meio da: contrapropaganda, contraespionagem, contrassabotagem e contraterrorismo (BRASIL, 2015b).

A segurança de assuntos internos é o conjunto de medidas destinadas à produção de conhecimentos que visam a assessorar as ações de correição das instituições (BRASIL, 2015b). A SAI amplia a capacidade de atuação do controle interno, nas funções disciplinar e criminal, corretivo-preventivo e repressivo.

As medidas de Contrainteligência com vistas à proteção dos ativos institucionais também se mostram profícuas no âmbito do Ministério Público. Pacheco (2006, p. 643) alerta que "a era da crença ingênua na intangibilidade física dos membros do Ministério Público já passou".

A Contrainteligência, notadamente no segmento da segurança orgânica, se apropria ao ambiente do Ministério Público tanto para

salvaguardar uma imensa quantidade de informações sigilosas que advém de sua atuação forense quanto para proteger a incolumidade física de pessoas e instalações (PACHECO, 2006).

Resta evidente que as medidas de Contrainteligência asseguram a proteção dos ativos institucionais, garantindo, além disso, o exercício livre e independente de suas funções (FARAH, 2013); todavia possui um desafio ainda maior, que é o desenvolvimento de uma cultura de segurança, em todos os níveis hierárquicos, "sem que se sacrifique, além dos limites razoáveis, a eficiência e a funcionalidade da organização" (ALMEIDA NETO, 2009, p. 58).

4. SEGURANÇA DE ÁREAS E INSTALAÇÕES

Como já fora mencionado anteriormente, a segurança orgânica constitui um conjunto de medidas defensivas que se destinam a garantir o funcionamento da instituição, prevenindo e obstruindo ações adversas de qualquer natureza. Este agregado de ações integradas e planejadas visam a proteger os ativos corporativos, e entre esses múltiplos ativos estão áreas e instalações.

A segurança de áreas e instalações constitui o conjunto de normas, medidas e procedimentos voltados à proteção extensiva das dependências da instituição, notadamente naquelas em que são elaborados, tratados, manuseados ou guardados as informações sigilosas e os materiais sensíveis (BRASIL, 2009). A NBR IS0 27002 (2013) complementa que a segurança física e do ambiente visa a prevenir acesso não autorizado em áreas e instalações, danos e interferências, enfatizando que a proteção deve ser compatível com os riscos identificados.

Dessa feita, em regra, a segurança de áreas e instalações é obtida pela adoção de medidas de proteção geral, controle e fiscalização de pessoal orgânico e de visitantes, demarcação e limitação de acesso de áreas sigilosas e restritas, que deverão ser classificadas de acordo com o grau de relevância (BRASIL, 2009).

Farah (2013, p. 16) assevera que "as ações de segurança para áreas e instalações são as que exigem maior integração com as demais, pois parte considerável da atividade institucional ocorre nesse ambiente", e, segundo Brasil (2009), assegura suporte e eficácia às demais atividades de segurança orgânica.

As áreas são classificadas segundo a sua natureza, podendo ser: livres, restritas, críticas ou sigilosas. São consideradas áreas livres aquelas que tenham por finalidade o atendimento ao público em geral, como por exemplo a recepção de uma edificação. Áreas restritas são as que ultrapassam o limite da área livre, em que para o acesso se faz necessário medidas de controle, podendo citar-se as instalações internas não sujeitas ao acesso público como sala de reuniões e gabinetes. Já áreas críticas guardam infraestruturas essenciais ao funcionamento da instituição como servidores de dados, geradores e quadros de energia, salas de controle, ou

seja, aquelas que podem ser pontos de interesse para ações de sabotagem. Por fim, sigilosas são aquelas em que tratados, manuseados ou guardados documentos, materiais ou informações sensíveis e que apenas poderão ser acessadas mediante credencial de segurança.

Resta evidenciado que a proteção de áreas e instalação se materializa por uma série de medidas integradas e complementares. Assim sendo, Brasil (2009) enumera alguns desses conjuntos:

a. demarcação de áreas – visa a identificar aquelas que são sigilosas, críticas e restritas, e informar às pessoas os diferentes graus de sensibilidade delas, apresentando-se como um primeiro elemento dissuasor ao comprometimento[4];

b. implantação de barreiras – criação de obstáculos de diferentes naturezas para impedir o acesso não autorizado de pessoas em áreas sigilosas ou restritas e viabilizar um efetivo controle da circulação, daquelas que possuam autorização para isso, ou das áreas livres;

c. adoção de linhas de proteção – objetiva realizar o cercamento ou a compartimentação[5] de ambientes e definir acessos mediante credenciais de segurança. Entre diferentes linhas de proteção (concêntricas) existem sistemas de detecção que acionam antes que a ameaça atinja a linha subsequente;

d. controle de acesso – processo por meio do qual se permite ou proíbe o acesso a qualquer área. O controle baseia-se na identificação e na avaliação dos graus de autorização de acesso;

e. detecção de intrusão e monitoramento eletrônico – destinado a identificar a intrusão ou violação por meio de dispositivos de detecção, transmissão de sinal de alarme e monitoramento eletrônico; e

f. prevenção de acidentes e incêndios – tem por propósito prevenir, controlar e limitar os efeitos de acidentes e incêndios. As medidas abrangem requisitos sobre equipamentos, sinalização, iluminação de emergência, treinamentos e auditorias; estando o planejamento de emergência diretamente relacionado com os protocolos de segurança de áreas e instalações (FARAH, 2013).

A necessidade de integração das medidas de proteção de áreas e instalações, como um fator determinante de sua efetividade, também é reconhecida por Farah (2013), que categoriza três sistemas voltados a segurança:

a. sistema físico – corresponde às medidas de controle executadas pelos agentes de segurança/vigilância. Além de executar inúmeros

4 É a perda da segurança de dados ou conhecimentos, provocada por fatores humanos, naturais ou acidentais (BRASIL, 2015b)

5 Permitir acesso somente para os que tenham a necessidade de conhecer, que é condição inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para que uma pessoa possuidora de credencial de segurança tenha acesso a dados ou conhecimentos sigilosos (BRASIL, 2015b).

protocolos de segurança, tem por responsabilidade a resposta diante dos incidentes;

b. sistema eletrônico – composto por equipamentos eletrônicos e sistemas informatizados, para detecção, vigilância e monitoramento; e

c. sistema de barreiras – abrange os diversos obstáculos que controlam ou dificultam o acesso a um determinado local.

Sob uma diferente perspectiva, Ramos (2006) propõe estratégias de proteção que podem ser adaptadas para a segurança de áreas e instalações, tendo por critério as características dos ativos a serem protegidos e as vulnerabilidades e ameaças a que estão expostos:

a. privilégio mínimo *(least privilege*) – a autorização de acesso de um usuário a determinada área ou instalação deve ser condicionada ao desempenho das funções e à necessidade de conhecer (não exposição desnecessária a risco);

b. defesa em profundidade (*defense in depth*) – aplicação de diferentes medidas de proteção, complementares e redundantes;

c. elo mais fraco (*weakest link*) – o elo mais fraco de um sistema de segurança define sua resistência, sendo assim, identificar fraquezas e promover alterações constitui medida de proteção;

d. ponto de estrangulamento (*choque point*) – consiste em adotar-se medidas de proteção em um ponto de controle em que transite grande parte dos usuários;

e. segurança pela obscuridade (*security throught obscurity*) – quanto menos se souber sobre uma determinada área ou instalação, maior será a dificuldade em promover um ato lesivo; e

f. simplicidade (*simplicity*) – é preciso avaliar a complexidade do sistema a ser protegido, pois quanto mais complexo, maior será o desafio em torná-lo seguro.

Notabiliza-se que as medidas e estratégias mencionadas não são vistas isoladamente, mas como partes de um todo, que é planejado e estruturado a atuar de maneira integrada e complementar. Os diferentes métodos operando simultaneamente majoram o espectro de proteção dos ativos institucionais.

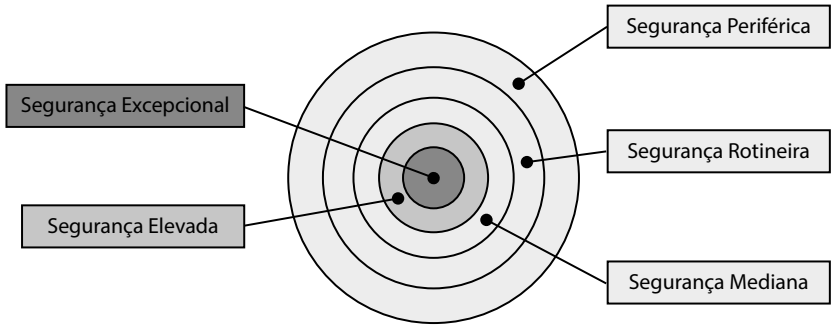
4.1. DELIMITAÇÃO DE PERÍMETROS

Na definição de Farah (2013), perímetros de segurança são áreas isoladas delimitadas por barreiras sucessivas e monitoradas pelos sistemas físico e eletrônico. O perímetro de segurança deve ser claramente definido (BRASIL, 2009), e sua localização e capacidade de resistência dependem dos requisitos dos ativos existentes em seu interior, e dos resultados da avaliação de riscos (ABNT, 2013).

No que se refere à segurança de áreas, acolhe-se a teoria de proteção dos círculos concêntricos. Segundo seus princípios, as medidas

de proteção devem ser ampliadas da periferia para o centro da instituição, onde ficariam situados os ativos mais sensíveis (ABNT, 2013). Na visão de Mandarini (2005), a criticidade do acesso ao ambiente vai do mais baixo ao mais elevado, do círculo periférico ao central, respectivamente, como demonstrado na Figura 01:

Figura 01 - Teoria do Círculos Concêntricos



Fonte: Adaptado de Mandarini (2005)

A gradação de segurança elaborada por Mandarini (2005, p. 93) estabelece características para cada círculo de proteção:

a. Excepcional: áreas de excepcional sensibilidade/periculosidade, de acesso restrito ao pessoal estritamente envolvido com as atividades-fim;

b. Elevada: áreas de elevada sensibilidade/periculosidade, de acesso ao pessoal intimamente envolvido com as atividades-fim;

c. Mediana: áreas de mediana sensibilidade/periculosidade, de acesso ao pessoal relacionado às atividades-fim;

d. Rotineira: áreas de baixa sensibilidade/periculosidade, de acesso às pessoas que precisam de trato funcional com as atividades ali desenvolvidas;

e. Periférica: áreas isentas de sensibilidade/periculosidade, que estão dentro dos limites do perímetro da instituição.

A instituição pode estabelecer protocolos para o acesso a cada uma dessas áreas circunscritas mediante credencial de segurança[6]. Comumente, as credenciais de segurança recebem uma classificação correspondente aos graus de sigilo previstos em lei (ultrassecreto, secreto, reservado), aplicando-se a mesma regra às áreas, conforme seu grau de sensibilidade, determinado pela utilização ou finalidade. O certificado autoriza o acesso na área com grau de sigilo equivalente ou inferior ao de sua credencial. Outra possibilidade é a adoção de cores para credenciais e áreas, em vez de graus de sigilo.

6 Segundo o Decreto Federal nº 7.845, de 14 de novembro de 2012, art. 2º, inciso VI, credencial de segurança é o certificado que autoriza pessoa para o tratamento de informação classificada.

Nesse passo acentua-se que, para cada perímetro concêntrico, é atribuído um diferente método de proteção, cada vez mais restritivo, de sorte que uma área mais interna é protegida concomitantemente pelos seus métodos e por aqueles aplicados aos perímetros que os circundam (NILES, 2004). Esse conceito, chamado de defesa em profundidade, e já mencionado anteriormente, assegura maior capacidade de detecção e neutralização de ameaças na proporção direta em que os ativos possuem maior sensibilidade. Ramos (2006) descreve defesa em profundidade como a aplicação de defesas distintas, de controles complementares como redundância, pois, no caso de falha ou violação de um, outro é capaz de suprir, não comprometendo todo o sistema.

A sobreposição de medidas protetivas, por circunscrição e profundida, certifica maior capacidade de resposta dos sistemas de segurança frente às ameaças.

4.2. DEMARCAÇÃO DE ÁREAS E INSTALAÇÕES

A demarcação objetiva delimitar, sinalizar e classificar áreas e instalações que possuam natureza crítica, restritiva ou sigilosa, informando o grau de sensibilidade ao público e usuários e a limitação de acesso, constituindo-se um primeiro elemento de dissuasão à intrusão (BRASIL, 2009).

A sinalização das áreas e das instalações sensíveis dinamiza o controle e a adoção de medidas protetivas e defensivas, desde que as placas indicativas estejam afixadas em locais de alta visibilidade e que possuam como características: universalidade, clareza e objetividade de códigos, linguagem e cores. A propósito, no que se refere ao último, cores distintas podem ser adotadas para identificar áreas de natureza crítica, restritiva ou sigilosa.

Compete ao titular da instituição normatizar a demarcação desses locais, tal como conceder credencial de acesso para aqueles que tenham necessidade funcional, sob a estratégia do privilégio mínimo (*least privilege).* Essa normatização é antecedida de um estudo que avaliará o ambiente e os ativos a serem protegidos, determinando o grau de sensibilidade que classificará cada área (BRASIL, 2014).

O Decreto Federal nº 7.845/12[7], que regulamenta os procedimentos para credenciamento de segurança, reconhece a necessidade de demarcação de áreas sensíveis e a restrição de acesso aos autorizados, como segue:

> Art. 42. As áreas e instalações que contenham documento com informação classificada em qualquer grau de sigilo, ou que, por sua utilização ou finalidade, demandarem proteção, terão seu acesso restrito às pessoas autorizadas pelo órgão ou entidade.

7 Decreto nº 7.845, de 14 de novembro de 2012 - Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/Decreto/D7845.htm>. Acesso em: 09 abr. 2019.

> Art. 43. Os órgãos e entidades públicas adotarão medidas para definição, demarcação, sinalização, segurança e autorização de acesso às áreas restritas sob sua responsabilidade.

No entendimento de Farah (2013), os critérios de acesso às áreas restritas são definidos com base na necessidade de conhecer que é a condição inerente ao efetivo exercício de sua função na instituição, além da credencial de segurança, que estabelece os níveis de acesso. O autor complementa que determinadas áreas restritas não necessitam ser classificadas sigilosamente, apenas possuírem o acesso controlado pela necessidade de conhecer, sugerindo que o Plano de Segurança Orgânica defina as condições de acesso, sua demarcação e a sinalização decorrente.

4.3. IMPLANTAÇÃO DE BARREIRAS

As barreiras são implementadas mediante a criação de obstáculos, de qualquer natureza, a fim de impedir o ingresso de pessoas ou bens desautorizados nas áreas restritas e permitir um efetivo controle da circulação daqueles que possuam autorização para isso (BRASIL, 2009). Tratam-se de entraves colocados entre a ameaça e aquilo que necessita ser protegido. A implementação de barreiras múltiplas converge com a estratégia de defesa em profundidade, uma vez que nesse caso a falha de uma das barreiras não significa o comprometimento imediato da segurança (ABNT, 2013).

São inúmeros os tipos de barreiras, divididas em dois grupos: naturais e artificiais. Naturais são as existentes no meio ambiente como acidentes geográficos ou rios; artificiais são as que englobam todo o tipo de proteção criado pelo homem, podendo ser estruturais (muros, cercas), eletroeletrônicas (alarmes, detectores de movimento), utilização de animais e humanas (postos de vigilância). Farah (2013) acentua que a distribuição dos postos de vigilância é parte do sistema de barreiras, contudo isso deve ser cuidadosamente planejado com vistas à integração com os sistemas físico e eletrônico.

A definição de barreiras perpassa pela consideração de alguns aspectos, conforme Brasil (2009):

a. a proteção ofertada deve ser proporcional aos riscos identificados;

b. a proteção física pode ser alcançada por intermédio da estruturação de diversas barreiras em torno da instituição e de suas instalações – cada uma delas estabelece um perímetro de segurança, contribuindo para o aumento da proteção total fornecida;

c. a localização e a resistência de cada barreira dependem dos resultados da análise de risco;

d. qualquer barreira só será efetiva se complementada por outras medidas de proteção; e

e. barreiras adicionais para controlar o acesso físico podem ser necessárias em áreas com diferentes requisitos de segurança dentro de um mesmo perímetro.

Vale mencionar que as barreiras físicas, além de prevenirem o acesso não autorizado, também contribuem para impedir a contaminação ambiental, como as causadas por fogo e inundação. Para essa finalidade as barreiras estruturais devem estender-se do piso até a laje superior (BRASIL, 2009).

Ainda no tocante ao planejamento e implantação de barreiras, é conveniente considerar o conceito da vigilância natural, que consiste na capacidade de ver e ser visto, fator psicológico importante como dissuasor de ameaças. As barreiras físicas devem permitir, como um processo natural, a observação, haja vista ser um fator de inibição para atitudes antissociais ou ilícitas (BONDARUK, 2007). Amaro (2005 apud BONDARUK, 2007) esclarece que vigilância natural abrange não apenas o espaço, mas o desenho do ambiente e as estruturas existentes, e, ao ampliar-se a visibilidade natural do lugar, reduz-se a oportunidade de uma ação adversa.

4.4. CONTROLE DE ACESSO

O controle de acesso visa a prevenir danos e interferências aos ativos institucionais. Trata-se de um processo por meio do qual se permite ou proíbe que pessoas ou bens tenham acesso a objetos ou às dependências da organização (BRASIL, 2009). Farah (2013, p. 20) esclarece que "o controle de acesso às áreas e instalações associado à demarcação de áreas sensíveis e ao estabelecimento de barreiras definem o gerenciamento de acesso", destacando ainda que a utilização de *software* de controle aprimora o processo e permite a realização de auditorias.

O monitoramento de entrada e saída, por meio de sistemas, mecanismos ou equipamentos que limitem o acesso a ambientes ou informações, garante a segurança das pessoas, do sigilo dos dados e da integridade dos bens. A normatização de procedimentos para o acesso de áreas sensíveis no âmbito institucional é obtida pela elaboração de norma de controle de acesso (BRASIL, 2014).

Mecanismos físicos ou eletrônicos efetivam o controle ao permitirem ou não o acesso. O controle físico geralmente é realizado por pessoas e composto por uma barreira física e pontos de controle com sistemas mecânicos ou eletrônicos. O controle lógico se utiliza da tecnologia, como leitura biométrica ou de íris, reconhecimento facial ou de voz, senhas ou cartões de proximidade. Neste caso, por haver prévio cadastro e autogestão, dispensa-se a utilização de pessoas *in loco*. Os autores apresentam variadas diretrizes para o controle de acesso, exemplificadas a seguir:

a. perímetros de segurança consistentes e claramente definidos, com mecanismos de controles, travas, alarmes e outros dispositivos de detecção de acesso não autorizado (BRASIL, 2009);

b. áreas de recepção com identificação e controle físico (portaria e catracas), registro de acessos, monitoramento por câmeras,

scanners de objetos, detectores de metais e vigilância física permanente (FARAH, 2013; BRASIL, 2009);

c. identificação do pessoal orgânico, fornecedores, terceiros ou visitantes por meio de crachás, estes com dispositivos de segurança para controle de acesso em locais específicos da instalação e diferenciação de cores por finalidade (ABNT, 2013; FARAH, 2013; BRASIL, 2009);

d. supervisão e condução dos visitantes mediante acesso exclusivo a áreas específicas, com propósitos autorizados e dentro dos requisitos de segurança e procedimentos de emergência, além do registro da data e hora de entrada e saída (ABNT, 2013; BRASIL, 2009);

e. postos para identificação, vistoria e controle do acesso de veículos, registro, monitoramento por câmeras, vigilância física e regulamentação de locais de estacionamento por finalidade (FARAH, 2013; BRASIL, 2009);

f. áreas de entrega e carregamento de suprimentos projetadas a não permitirem que terceiros tenham acesso às dependências da instalação, além de estarem equipadas com dispositivos para identificação e controle de pessoas e veículos e mecanismos de inspeção dos materiais entregues (ABNT, 2013);

g. protocolos e áreas específicos para identificação e controle de pessoas portadoras de necessidades especiais, cães-guia, que estejam portando armas de qualquer natureza, instrumentos que causem risco ou transportando produtos perigosos (FARAH, 2013);

h. sistema de gestão de acesso integrados às tecnologias *cloud computing*[8] e internet das coisas que permita a comunicação entre equipamentos e *software*, a fim de monitorar e registrar acessos, gerenciar diferentes níveis de segurança, controlar dispositivos e acionar alarmes. Esses sistemas ainda podem estar interligados a bancos de dados de inteligência que contenham a identificação daqueles que possam representar risco à segurança (*blacklists),* com a capacidade de emitir notificações e alertas (NILES, 2004);

i. sistema de controle de acesso às áreas sensíveis, restrito àqueles que sejam credenciadas e que tenham necessidade funcional de conhecer, mediante protocolos de autenticação por redundância, a exemplo de cartões com PIN (*personal identification number),* leitura biométrica, reconhecimento facial (ABNT, 2013; BRASIL, 2009);

j. normas e mecanismos de controle que proíbam o acesso de qualquer meio de captura de imagem e som em áreas e instalações

8 Tecnologia que permite o acesso remoto, em qualquer local ou tempo, de s*oftwares*, armazenamento de arquivos e processamento de dados pela internet. Disponível em: <https://rockcontent.com/blog/cloud-computing/>. Acesso em: 10 abr. 2019.

onde são tratados, manuseados ou guardados documentos, materiais ou informações sigilosas (BRASIL, 2014);

k. credenciais de acesso às áreas sensíveis revistas e atualizadas em intervalos regulares, e revogadas quando necessário (ABNT, 2013; BRASIL, 2009);

l. sistema de auditoria com os registros de identificação, das imagens e acessos realizados com a respectiva data e hora (BRASIL, 2009); e

m. portas contra incêndios no perímetro de segurança dotadas de sensores de alarme, vigilância eletrônica e mola para fechamento automático (BRASIL, 2009).

Após descrever algumas diretrizes para controle de acesso a áreas e instalações, pode-se inferir que esse processo perpassa pelo Protocolo AAA, oriundo no contexto da segurança da informação e aqui utilizado por analogia. Esse protocolo congrega o controle de acesso por três fundamentos: autenticação, autorização e auditoria. A autenticação trata de identificar aquele que busca o acesso. A autorização assegura que o identificado tenha somente acesso àquilo que foi consentido. Por fim, a auditoria mantém registro e possibilita a rastreabilidade dos acessos realizados (MATTOS, 2003).

Avulta-se que o processo de autenticação pode ser obtido por meio de três categorias, cada uma com um grau de confiabilidade, e descritos por Niles (2004) e Mattos (2003) como:

a. autenticação utilizando algo que você possui: é o método mais comum e menos confiável, cuja a autenticação se dá por meio de um objeto que é portado, como um crachá, *token* ou cartão de proximidade. Apresenta como vulnerabilidade a possibilidade de ser utilizado por pessoa não autorizada, de maneira clandestina ou em decorrência de uma subtração ou extravio;

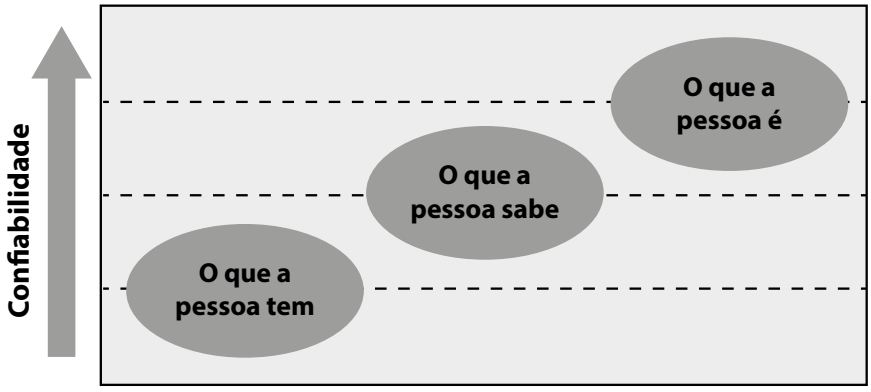
b. autenticação utilizando algo que você sabe: é um método comum, em que a autenticação ocorre por meio do fornecimento de uma informação. Possui maior confiabilidade se comparado com o anterior, mas apresenta a vulnerabilidade de poder ser compartilhado ou descoberto. Trata-se da utilização de senhas, códigos ou procedimentos combinados; e

c. autenticação utilizando algo que você é: método menos comum e mais confiável, pois baseia-se em um atributo físico exclusivo, como impressão digital, íris, voz, face do rosto e letra manuscrita.

O controle de acesso é mais efetivo se utilizado, pelo menos em conjunto, dois dos três métodos de autenticação, tendo por parâmetros a sensibilidade do ativo a ser protegido e a funcionalidade necessária (MATTOS, 2003). Sendo assim, é recomendado em locais onde são tratados, manuseados ou guardados documentos, materiais ou informações sigilosas que se tenha a combinação dos três métodos de autenticação.

A Figura 02 apresenta os métodos propostos diante do indicador confiabilidade:

Figura 02 – O que a pessoa porta, o que a pessoa sabe, identidade da pessoa.



Fonte: Adaptado de Niles (2004)

Ainda no tocante ao controle de acesso, Niles (2004) faz uma importante advertência quanto ao encobrimento voluntário ou involuntário. Tal situação representa uma vulnerabilidade do sistema e ocorre quando alguém não autorizado passa por um ponto de controle juntamente à pessoa autorizada. O encobrimento voluntário acontece quando o autorizado dá causa, por exemplo segurando uma porta; já o involuntário ocorre quando o não autorizado transpassa o controle sem ser detectado. Como solução o autor sugere a adoção de entradas compartimentadas – tipo porta rotativa, piso detector de pegadas para assegurar a passagem de uma única pessoa e atuação do pessoal de segurança. Aliás, sobre o último o autor acrescenta que, mesmo diante de tantos recursos tecnológicos, um grupo qualificado de seguranças se traduz no melhor método de proteção e controle de acesso. Isso porque possuem a capacidade de vigilância com os sentidos humanos e medidas racionais de contrarresposta diante de ameaças.

4.5. DETECÇÃO DE INTRUSÃO E MONITORAMENTO ELETRÔNICO

Além dos sistemas físico e de barreiras, a segurança de áreas e instalações engloba o sistema eletrônico (MPF, 2013), que se destina a identificar a intrusão ou a violação, por meio dos seguintes elementos:

a. dispositivos de detecção – sensores dotados de diferentes tecnologias (infravermelhos, micro-ondas, ultrassons, fotoelétrico, de proximidade, sísmico, ondas de choque) e que se destinam a identificar a presença de intrusos (BRASIL, 2009);

b. sistemas de alarme – métodos utilizados para transmitir sinais sonoros e luminosos que objetivam alertar sobre anormalidades ou ameaças iminentes, inclusive botão de pânico (BRASIL, 2009); e

c. sistema de monitoramento eletrônico – equipamentos e métodos usados para controlar e monitorar o sistema (BRASIL, 2009).

O circuito fechado de televisão (CFTV) constitui-se um eficaz meio de monitoramento eletrônico por permitir controle visual remoto sobre as instalações físicas. Todavia as câmeras que compõem o sistema devem ter alta resolução, recurso de detecção de movimento e *software* de reconhecimento ótico de caracteres (OCR). Acentua-se que o monitoramento deve acontecer em tempo real, e os dados devem ser armazenados em local seguro e de acesso restrito, com redundância e por período de tempo compatível. As configurações do sistema devem atender aos protocolos de segurança elaborados com base na análise de risco, a fim de garantir a identificação de ameaças e a rápida resposta aos incidentes (FARAH, 2013).

Os sistemas de detecção de intrusão e monitoramento eletrônico devem ser instalados por profissionais especializados e testados regularmente, abrangendo todo o perímetro da instituição (ABNT, 2013; BRASIL, 2009).

4.6. PLANEJAMENTO DE EMERGÊNCIA

O planejamento de emergência também está contido na segurança de áreas e instalações, e tem por objetivo prevenir, controlar e limitar os efeitos de acidentes e incêndios, além de ameaças externas e do meio ambiente, como enchentes, terremotos, explosões, perturbações da ordem pública e outras formas de desastres naturais ou causados pelo homem. As medidas de segurança englobam requisitos sobre instalações, equipamentos, sinalização, iluminação, treinamento e auditorias (ABNT, 2013; FARAH, 2013), planejados para prevenir perda, dano ou comprometimento dos ativos institucionais e a interrupção das atividades (BRASIL, 2009).

Para a consecução de seus objetivos, um planejamento de emergência pressupõe a elaboração de planos de prevenção e combate a incêndio, contingência e controle de danos e evacuação, os quais devem ser avaliados periodicamente (FARAH, 2013).

O plano de prevenção e combate a incêndios tem por base a legislação e as normas técnicas em vigor no que se refere a equipamentos de prevenção, além disso engloba a composição de uma brigada para combate a incêndio e a capacitação de funcionários em todos os setores das instalações, para atuar no apoio e orientação, caso ocorra alguma emergência. Fundamental ainda que sejam previstas medidas de segurança para a salvaguarda de materiais e informações sigilosas e a preservação de áreas críticas, assim como a realização rotineira de treinamentos para a adoção de comportamentos adequados frente às emergências (BRASIL, 2009). Sobre isso corrobora Bessa (2002) ao sustentar que os programas de treinamento e de sensibilização sobre a importância da segurança são partes do conjunto de medidas para proteção dos ativos corporativos e uma maneira de despertar a responsabilidade nas pessoas.

O plano de contingência reúne uma série de ações com a finalidade de reduzir o impacto advindo de um incidente de segurança[9], visando a dar continuidade às atividades e recuperar sistemas ou processos, mesmo que de forma mínima, mitigando os efeitos negativos decorrentes, sendo aplicado para atender atividades críticas da instituição ou situações de emergência (FARAH, 2013).

Bessa (2002, p. 137) esclarece a finalidade do plano de contingência, realça sua importância e a necessidade da realização de testes de aplicabilidade:

> Plano de Contingência – baseado na possibilidade de ocorrência de um desastre – natural ou provocado – explicita as providências necessárias ao pronto restabelecimento das atividades, de modo que não haja solução de continuidade. Isso implica o estabelecimento de um sistema alternativo, que deve estar em outro local, pronto para funcionar como se fosse o sistema principal. Essa providência, apesar de onerosa, pode evitar grandes prejuízos que adviriam do comprometimento ou da perda de dados ou do sistema. O grande problema dos planos de contingência é que, quando se é necessário executá-los, detectam-se falhas, uma vez que geralmente eles não são testados a priori.

O objetivo do plano de controle de danos é identificar os ativos institucionais impactados pelo incidente de segurança, a amplitude do dano causado e seu comprometimento. Também visa a mensurar o impacto pela interrupção de atividades, sistemas ou processos. Por meio dessa última avaliação, torna-se possível planejar a continuidade daquilo que foi interrompido ou ameaçado (FARAH, 2013).

A Política de Segurança Institucional do Ministério Público prevê a adoção e implementação do planejamento de contingência e controle de danos (CNMP, 2016).

Por último, o plano de evacuação se destina a delimitar os procedimentos a serem adotados para a retirada de pessoas, documentos e materiais sensíveis, encaminhando-os para um local seguro. A realização de treinamentos periódicos e a clareza de atribuições são fatores primordiais para o êxito do processo.

Por oportuno, a gestão de incidentes de segurança incorpora, além das ações previstas nos mencionados planos, outros procedimentos necessários, que são esclarecidos por Farah (2013, p. 83-84):

- Detecção – Identificação do incidente ou notificação de sua ocorrência.
- Resposta – Constitui-se nas ações desencadeadas resolver o problema. Incluem a ativação do plano de contingência, quando for o caso.
- Registro – Formalização do ocorrido para arquivo, eventual investigação ou análise de informações.

9 Segundo Sêmola (2003), incidente de segurança é um evento decorrente da exploração de uma vulnerabilidade. O incidente pode ser considerado como uma ação indesejada ou inesperada com alto potencial de comprometimento dos princípios da segurança.

- Investigação – Envolve coleta, armazenamento e utilização de evidências que podem instruir um processo administrativo, sindicância ou investigação criminal.
- Ações corretivas – São as ações implementadas para evitar a repetição de um incidente de segurança.

O mesmo autor traz à baila uma significativa recomendação sobre a estruturação de um banco de dados junto à Segurança Institucional que registre os incidentes de segurança ocorridos. Ensina Farah (2013) que a análise desses dados auxilia na compreensão do ocorrido, identificando razões, consequências e custos (financeiro, funcional e de imagem) a fim de subsidiar medidas corretivas e melhoria de processos.

5. ANÁLISE DE RISCO PARA SEGURANÇA ORGÂNICA

A segurança orgânica, como já consignado, acolhe uma série de medidas integradas e planejadas, de caráter eminentemente defensivo, destinadas a proteger os ativos tangíveis e intangíveis, além de garantir o funcionamento da instituição.

Com vistas à eficácia das ações preventivas preconiza-se que as normas e diretrizes de segurança sejam materializadas por meio da elaboração de um Plano de Segurança Orgânica (PSO), antecedido de um Estudo de Situação e de uma Análise de Risco. Sobre isso, Brasil (2015b, p. 47) alerta que "a adoção de medidas de segurança sem a necessária análise dos riscos e dos aspectos envolvidos poderá causar o comprometimento, decorrente de sua insuficiência ou inadequação".

Segundo a NBR ISO/IEC 27002[10], pela análise de riscos é possível identificar as ameaças aos ativos e às vulnerabilidades destes, além de estimar a probabilidade de ocorrência e o decorrente impacto. É o processo pelo qual se procura compreender a natureza e o grau dos riscos a que estão expostos os ativos institucionais. No que tange aos conceitos de ameaça e vulnerabilidade, oportunamente, Farah (2013) os descreve de forma esclarecedora:

> Ameaça pode ser definida como ação adversa (ou possibilidade de) expressa por vontade de um ator hostil objetivando suplantar as medidas de segurança, com consequências negativas para a instituição ou a seus integrantes. O conceito de ameaça envolve a existência de um ator hostil, com motivação para realizar uma ação adversa e que possua capacidade de realizá-la, seja técnica, logística, financeira e de mobilização de pessoal (p. 9).
>
> Quando uma ameaça explora as deficiências ou as fragilidades em segurança de uma instituição, em seus sistemas ou serviços, configura-se a vulnerabilidade, que pode ser definida como a existência de deficiências conjugadas com ameaças (p. 10).
>
> Vulnerabilidade é uma deficiência presente ou associada a pessoas, áreas e instalações, material, documentação e suportes de informação

10 ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 27002**: tecnologia da informação – técnicas de segurança - código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2013.

> que pode ser explorada por uma ameaça, podendo gerar um incidente de segurança e causar impactos negativos (p. 11).

A análise de risco é parte de um processo denominado gestão de risco, que se constitui de atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos. O propósito da gestão de risco é a criação e proteção de valor, por isso convém que seja parte integrante dos processos de gestão da instituição e da tomada de decisão (ABNT, 2018).

Laconicamente o processo de gestão de riscos compreende as seguintes etapas, previstas na NBR ISO 31000[11]:

a. identificação de riscos – reconhecer e descrever riscos que possam impedir que organização alcance seus objetivos;

b. análise de riscos – compreender a natureza dos riscos e suas características;

c. avaliação de riscos – tem por propósito apoiar decisões, ao comparar análise de risco com os critérios de risco estabelecidos; e

d. tratamento de riscos – selecionar e implementar opções para abordar riscos.

No Ministério Público a gestão de riscos deve preceder o processo de planejamento e de tomada de decisão, orientando a operacionalização de controles, o planejamento de contingência e o controle de danos. Especificamente a avaliação de riscos visa a identificar e monitorar as situações de riscos e a evolução de ameaças e, por decorrência, subsidiar a implantação de medidas de proteção (CNMP, 2016).

Evocando neste momento o objeto deste trabalho, resta comprovado que o planejamento de segurança de áreas e instalações deve ser fundamentado na análise de ameaças, reais e potenciais, e nas vulnerabilidades existentes. Essa análise condiciona a intensidade das medidas de segurança e define seus requisitos. A utilização da metodologia da gestão de risco diminui a subjetividade na definição dos requisitos de segurança (FARAH, 2013). Em complementação ao exposto, Mandarini (2005, p. 93) comenta:

> A determinação do tipo e do grau de criticidade do risco ou ameaça a que se submete cada área ou instalação, a aplicação da metodologia de avaliação e a formalização de um diagnóstico constituem a essência da Segurança de Áreas e Instalações.

Em síntese, a análise de risco em segurança orgânica antecede a elaboração do plano de segurança e pode ser entendida como um processo pelo qual se busca compreender a natureza e o grau dos riscos a que estão expostos os ativos que a instituição pretende proteger com a elaboração do aludido plano.

11 ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO 31.000**: gestão de riscos – diretrizes. Rio de Janeiro: ABNT, 2018.

6. CULTURA DE SEGURANÇA

Em algumas oportunidades no transcorrer deste trabalho, buscou-se demonstrar que um fator crítico de efetividade para a segurança de áreas e instalações é a adoção de medidas integradas e complementares. As diferentes estratégias fazem parte de um conjunto de ações planejadas e estruturadas com base na análise de risco dos ativos a serem protegidos.

Isso posto, vale ressaltar que todas as normas, medidas e procedimentos componentes desse amplo sistema de proteção estão diretamente relacionadas ao fator humano. Na visão de Kevin Mitnick (*apud* McCARTHY; CAMPBELL; BROWNSTEIN, 2003), as pessoas são para a instituição o seu melhor ativo de segurança, mas também a sua maior vulnerabilidade, o elo mais fraco da corrente. Além de erros e acidentes, as pessoas estão sujeitas à influência de uma infinidade de variáveis, que podem flexibilizar regras ou omitir procedimentos, com provável consequência desastrosa para a segurança (FARAH, 2013; NILES, 2004). Somado a isso, é necessário precaver-se ao uso de Engenharia Social, como forma de manipular ou persuadir determinadas pessoas a fim de fornecer informações sensíveis, facilitar acessos ou romper barreiras de proteção (NILES, 2004). Em vista disso, "fragilidades individuais transformam as pessoas em um ponto a ser explorado por ameaças, o que facilita a consumação de uma vulnerabilidade" (FARAH, 2013, p. 41).

Sob outro ponto de vista, as pessoas são consideradas o apoio mais forte, pois a racionalidade que permite o reconhecimento e a interpretação de fatores inesperados, aliada à mobilidade e ao excepcional uso dos sentidos humanos, mostram-se competências incomparáveis a nenhum recurso tecnológico. No que diz respeito à segurança, a presença humana é um complemento de inestimado valor para a tecnologia (NILES, 2004).

As pessoas se fazem presentes, de alguma forma, nos elementos que integram o complexo conjunto de atividades de segurança de uma instituição (FARAH, 2013). Destarte, está nas pessoas, e não no trabalho isolado de um setor, a capacidade de obtenção de níveis adequados de segurança, pela predisposição de se adotar normas e procedimentos de segurança e pelo desenvolvimento de uma mentalidade de proteção (FARAH, 2013). Coadunando com esse pensamento, Bessa (2002, p. 132) acrescenta:

> O êxito de qualquer programa de segurança é o desenvolvimento de uma sadia mentalidade de segurança entre todos os funcionários da empresa. É da máxima importância que todos os escalões hierárquicos, desde o mais alto dirigente, até o mais humilde servidor estejam suficientemente esclarecidos para a necessidade de proteção [...]

Ao se implementar a segurança institucional, deve-se incentivar o envolvimento do público interno, desenvolvendo uma cultura de segurança, com o objetivo de estabelecer atitudes favoráveis, frente às exigências de segurança (FARAH, 2013). É inegável "a necessidade de investimentos na preparação, sensibilização, conscientização e educação das pessoas para os assuntos que envolvem segurança" (p. 41).

Por último, acentua-se que o Conselho Nacional do Ministério Público acolhe de mesmo pensamento, ao considerar como fundamento

da instituição da Política de Segurança Institucional, a necessidade de desenvolver uma cultura de segurança no âmbito do Ministério Público para a proteção e salvaguarda das pessoas, dos materiais, das áreas e instalações e da informação (CNMP, 2016).

7. CONSIDERAÇÕES FINAIS

Inteligência é uma atividade de caráter assessorial que produz e salvaguarda conhecimentos com conteúdo preciso, oportuno, útil e significativo, visando a dar suporte às autoridades na tomada de decisões, na elaboração de planejamentos, na definição de diretrizes e objetivos. A metodologia de inteligência, ao formular convicções fundamentadas, com base em evidências factuais ou racionais, contribui com o processo decisório por meio da redução de incertezas, da antecipação e previsão de fatos e da prospecção de possíveis cenários futuros.

O escopo da atividade de inteligência é harmônico com as funções do Ministério Público, possibilitando o assessoramento às investigações criminais mais complexas, nas decisões do campo político, na definição dos rumos institucionais, na elaboração de planejamentos, implantação de planos e programas.

As medidas de Contrainteligência, com vistas à proteção dos ativos institucionais e em consonância com a segurança institucional, também se mostram profícuas ao identificar vulnerabilidades e potencialidades lesivas e ao salvaguardar informações sigilosas e proteger a incolumidade física de pessoas e instalações.

A segurança de áreas e instalações denota relevância no contexto da segurança institucional, haja vista que suas medidas de segurança dão suporte e eficácia às demais. A integração das medidas de proteção para áreas e instalações é fator determinante de sua efetividade, a julgar pela complexidade e abrangência e pelo fato de grande parte da atividade institucional se concentrar nesse ambiente.

O planejamento de segurança de áreas e instalações deve ser fundamentado na análise de ameaças reais e potenciais, e nas vulnerabilidades existentes. Essa análise condiciona a intensidade das medidas de segurança e define seus requisitos. A metodologia de análise de risco diminui a subjetividade nessa definição e o perigo de comprometimento do sistema de segurança, decorrente de insuficiência ou inadequação.

Vale ressaltar que, ao estabelecer normas de segurança, é necessário buscar o equilíbrio entre a proteção adotada e a funcionalidade da instituição. As medidas protetivas devem assegurar defesa, sem que se sacrifique, além do razoável, a eficiência da organização (FARAH, 2013; ALMEIDA NETO, 2009).

Em todo o conjunto de atividades de segurança de uma instituição, um elemento é comum: as pessoas. Elas podem ser o elo mais fraco da corrente, mas também o mais forte. A obtenção de níveis adequados de segurança

perpassa pelo envolvimento do público interno e pelo desenvolvimento de uma cultura de segurança, em todos os níveis.

Por fim, reafirma-se que proteger a instituição e seus ativos é garantir o livre e independente exercício de suas funções.

8. REFERÊNCIAS

ALMEIDA NETO, Wilson Rocha de. **Inteligência e contrainteligência no Ministério Público**: aspectos práticos e teóricos da atividade como instrumento de eficiência no combate ao crime organizado e na defesa dos direitos fundamentais. Belo Horizonte: Dictum, 2009.

AMARO, Marcos Antonio. **Arquitetura contra o crime:** PCAAA – prevenção do crime através da arquitetura ambiental. Rio de Janeiro, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 27002**: tecnologia da informação – técnicas de segurança – código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2013.

_____. NBR ISO 31.000: gestão de riscos – diretrizes. Rio de Janeiro: ABNT, 2018.

BESSA, Jorge Silva. **A inteligência competitiva:** as técnicas dos grandes serviços de inteligência à disposição de sua empresa. Brasília: Projecto Editorial, 2002.

BONDARUK, Roberson Luiz. **A prevenção do crime através do desenho urbano.** Curitiba: Ed. do autor, 2007.

BRASIL. **Decreto nº 7.845, de 14 de novembro de 2012**. Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/Decreto/D7845.htm>. Acesso em: 9 abr. 2019.

_____. Estado-Maior do Exército. **Manual de fundamentos**. MF 10.107: inteligência militar terrestre. 2. ed. Brasília: 2015a.

BRASIL. Ministério da Defesa, Exército Brasileiro. **Manual de campanha**. C 30-3: Contrainteligência. 2.ed. Brasília: 2009.

_____. _____. **Portaria nº 1.067, de 8 de setembro de 2014**. Aprova as instruções gerais para a salvaguarda de assuntos sigilosos. EB10-IG-01.011. IGSAS. Brasília: 2014.

_____. Ministério da Justiça, Secretaria Nacional de Segurança Pública. **Doutrina nacional de inteligência de segurança pública** – DNISP. 4. ed. rev. e atual. Brasília: Ministério da Justiça, 2015b.

CASTRO, Clarindo Alves de (Coord.); RONDON FILHO, Edson Benedito (Coord.). **Inteligência de Segurança Pública**. Curitiba: Ed. Juruá, 2012.

CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO (CNMP). **Resolução nº 156, de 13 de dezembro de 2016.** Institui a Política de Segurança Institucional e o Sistema Nacional de Segurança Institucional do Ministério Público. Brasília: 2016. Disponível em: <http://www.cnmp.mp.br/portal/images/Resolucoes/Resolu%C3%A7%C3%A3o-156.pdf>. Acesso em: 3 mar. 2019.

DANTAS FILHO, Diógenes**. Inteligência a seu alcance**. 1. ed. Rio de Janeiro: Editora Ciência Moderna Ltda., 2013.

FARAH, Camel André de Godoy. **Gestão de segurança institucional** [Recurso eletrônico] 1. ed. Florianópolis: Ed. do autor, 2013.

FERREIRA, Romeu Antônio. **Segurança orgânica**. Nota de aula 04.02.01. ESISPERJ, Rio de Janeiro, 2015.

FERRO JÚNIOR, Celso Moreira. **Inteligência organizacional, análise de vínculos e a investigação criminal**: um estudo de caso da Polícia Civil do Distrito Federal. 2007. 137f. Dissertação (Gestão do Conhecimento e Tecnologia da Informação) - Universidade Católica de Brasília, Brasília, 2007.

FERRO JÚNIOR, Celso Moreira. **A inteligência e a gestão da informação policial:** conceitos, técnicas e tecnologias definidos pela experiência profissional e acadêmica. Brasília: Fortium, 2008.

_____; OLIVEIRA FILHO, Edemundo Dias de; PRETO, Hugo Cesar Fraga. Colaboração: George Felipe de Lima Dantas. **Segurança pública inteligente:** sistematização da doutrina e das técnicas da atividade. Goiânia: Kelps, 2008.

GONÇALVES, Joanisval Brito. *SED QUIS CUSTODIET IPSO CUSTODES*? **O controle da atividade de inteligência em regimes democráticos:** os casos de Brasil e Canadá. 2008. 837p. Tese (Doutorado em Relações Internacionais) – Instituto de Relações Internacionais, Universidade de Brasília, Brasília, 2008. Disponível em: <http://repositorio.unb.br/bitstream/10482/1262/1/TESE_2008_JoanisvalBritoGoncalves.pdf>. Acesso em: 14 mar. 2019.

_____. **Atividade de inteligência e legislação correlata**. Niterói: Impetus, 2010.

KENT, Sherman. **Informações estratégicas**. Tradução: Cel. Hélio Freire. Rio de Janeiro: Biblioteca do Exército, 1967. (Coleção General Benício). Título original: *Strategic intelligence for american world policy*.

LOWENTHAL, Mark. **Intelligence:** from secrets to policy. Washington, D.C.: CQ Press, 2003.

MANDARINI, Marcos. **Segurança corporativa estratégica**. São Paulo: Manole, 2005.

MATTOS, Cristiano Lincoln de Almeida. **Sentinel**: um engenho Java para controle de acesso RBAC. 2003. 51f. Relatório (Graduação em Segurança da Informação). Recife: Universidade Federal de Pernambuco, 2003.

McCARTHY, Mary Pat; CAMPBELL, Stuart; BROWNSTEIN, Rob. **Transformação da segurança eletrônica**. São Paulo: Pearson Education do Brasil, 2003.

MINISTÉRIO PÚBLICO FEDERAL (MPF). Gabinete do Procurador-Geral da República. **Portaria nº 417, de 5 de julho de 2013**. Dispõe sobre o Plano de Segurança Institucional do Ministério Público Federal. Diário do Ministério Público Federal nº 87, de 9 jul. 2013, Caderno Administrativo.

NILES, Suzanne. **Segurança física em instalações críticas**. Relatório APC nº 82. Ver. 2. APC: 2004. Disponível em: <https://www.voltimum.com.br/sites/www.voltimum.com.br/files/fields/attachment_file/sites/www.voltimum.com.br/files/apcseguranca-_wp82.pdf>. Acesso em: 29 mar. 2019.

NOBRE, George Karlo Dantas. **A atividade de inteligência no âmbito do ministério público:** um comparativo entre inteligência ministerial e investigação ministerial criminal. 2014. 122f. Monografia (Especialização em Inteligência de Segurança) – Universidade do Sul de Santa Catarina, Natal, 2014.

PACHECO, Denilson Feitoza. **Atividades de inteligência no Ministério Público**. In: CONGRESSO NACIONAL DO MINISTÉRIO PÚBLICO – MINISTÉRIO PÚBLICO E JUSTIÇA SOCIAL, 16., 2005, Belo Horizonte. Anais...Belo Horizonte: Associação Nacional dos Membros do Ministério Público/Associação Mineira do Ministério Público, 2006..

_____. Atividade de Inteligência no Ministério Público. In: BRANDÃO, Priscila Carlos; CEPIK, Marco (Org.). **Inteligência de segurança pública:** teoria e prática no controle da criminalidade. 1. ed. Niterói: Impetus, 2013.

RAMOS, Anderson. **Security officer:** guia oficial para formação de gestores em segurança da informação. Porto Alegre: Zouk, 2006.

SÊMOLA, Marcos. **Gestão da segurança da informação:** visão executiva da segurança da informação aplicada ao *security officer*. São Paulo: Campus, 2003.

SEGURANÇA EM OPERAÇÕES DE ENFRENTAMENTO DA ESCRAVIDÃO CONTEMPORÂNEA: A APLICAÇÃO DA INTELIGÊNCIA E CONTRAINTELIGÊNCIA NO PLANEJAMENTO E EXECUÇÃO

Cleverson Lautert Cruz[1]

RESUMO: O cenário da atuação do Estado no âmbito da prevenção e repressão aos ilícitos praticados por infratores individuais ou grandes organizações ou associações criminosas, demanda a mobilização de consideráveis recursos públicos, esforços institucionais e da própria sociedade. Tais condições devem ser consideradas para que a atuação do Estado, na garantia da lei e da ordem, seja devidamente exercida, com a obtenção dos resultados pretendidos e com a manutenção das condições de segurança da ação e da própria instituição. Adotando como caso condutor a atuação do Estado contra a escravidão contemporânea, configurado como ponte entre a atividade aparentemente lícita de formação do capital aliada ao valor social do trabalho e um dos crimes mais deploráveis contra a dignidade da pessoa humana, este artigo busca provocar a reflexão sobre a reestruturação da atividade fiscalizatória e repressiva estatal. Não se pretende com o presente trabalho a mera avaliação tática de realização de operações de enfrentamento, mas a proposta de visão com um passo adiante, no desenvolvimento da atividade de segurança institucional calcada na evolução da Inteligência e Contrainteligência aplicada ao planejamento e execução de operações.

PALAVRAS-CHAVE: Inteligência. Contrainteligência. Operações. Trabalho Escravo. Direitos Humanos.

1 Gerente de Segurança Institucional do Ministério Público do Trabalho. Policial Rodoviário Federal. Comandante de Helicóptero Policial. Ex-Chefe da Divisão de Planejamento Operacional da Polícia Rodoviária Federal. Graduado em Direito e Administração. Pós-Graduado em Direito Público e em Administração Pública. Integrou a Comissão Especial do Conselho de Defesa dos Direitos da Pessoa Humana (CDDPH), constituída pela Resolução 05/2002 do CDDPH, que elaborou o Plano Nacional para a Erradicação do Trabalho Escravo no Brasil.

1. INTRODUÇÃO

O ciclo de criminalidade tem aperfeiçoado suas técnicas normalmente em descompasso com a (ainda) singela[2] atuação do Estado, resultando de ações sem o devido planejamento e coordenação no sentido de aumento da eficácia das atividades exercidas.

A estrutura estanque das instituições do aparato fiscalizador estatal frente à flexibilidade e fluidez do desenvolvimento das condutas criminosas acaba agravando as condições de manutenção da ordem. Com efeito, o caminho trilhado da conduta ilícita, normalmente permeada pela lavagem de capitais, até chegar ao lucro disponível e aparentemente lícito decorrente da infração praticada, apresenta curvas tênues de difícil identificação pelo Estado.

Um dos fatores mais representativos da zona cinzenta atravessada entre o caminho do ilícito para o lícito, configurada também como uma das condições mais degradantes da dignidade da pessoa humana, é caracterizado pela subjugação do humano coisificado pelo trabalho em condição análoga à de escravo, nas suas mais variadas vertentes e condutas periféricas.

Embora a adoção, como referencial, das particularidades do trabalho em condição análoga à de escravo, constata-se que considerável parcela das operações realizadas pelas forças públicas em condições e ambientes de risco carecem de análise e planejamento adequados.

Nesse escopo de ação estatal, a operação pode ser definida como uma atuação concreta, destinada à obtenção de algum resultado prático, seja pela repressão de algum ilícito, seja pela prevenção à sua ocorrência.

A apresentação desse ambiente frente à atuação do Estado constitui relevante complexidade na avaliação de riscos, especialmente quanto à probabilidade e criticidade de ocorrência de um fato danoso, quando da realização de operações específicas de fiscalização ou repressão. Contudo, constata-se que as operações realizadas simplesmente desconsideram fatores de extrema relevância para os resultados da ação e, principalmente, quanto à segurança dos próprios agentes públicos no exercício *propter officium*.

Nesse sentido, a produção do conhecimento, como decorrência da Atividade de Inteligência e Contrainteligência, fruto do trabalho de análise e de operações de Inteligência, aliada ao processo de planejamento adequado e à integração coordenada das ações, podem reduzir consideravelmente os riscos de exposição dos agentes públicos ao perigo, melhorar a preparação das atividades e, consequentemente, aprimorar os resultados obtidos.

---

2 Nas palavras de Sarmento: "O desafio apresentado ao Brasil é o de fazer com que a Constituição seja apropriada pelas práticas cotidianas da sociedade, sobretudo para garantir o pleno respeito aos direitos fundamentais dos excluídos. Não há dúvidas de que parte considerável da população brasileira ainda se sujeita a práticas autoritárias e opressivas. Nas favelas do Rio de Janeiro, a população é submetida à violência do tráfico de drogas ou da polícia. Na fronteira agrícola, **ainda se pratica o trabalho escravo**. Nessas partes do território, **não vigora plenamente o Estado Democrático de Direito**. Para a superação dessas disfunções da vida brasileira, certamente **os poderes constituídos devem exercer um papel central**." (grifos acrescidos). SARMENTO, Daniel; SOUZA NETO, Daniel Pereira de. **Direito Constitucional**: Teoria, história e métodos de trabalho. 2ª ed. Belo Horizonte: Fórum, 2017.

Destaca-se, de forma preambular, a corrente majoritária de entendimento da Atividade de Inteligência como um dos diversos processos integrantes do sistema de segurança institucional, decorrente do conceito de *Homeland Security*[3] norte-americano aplicado às organizações institucionalizadas.

Os limites deste artigo, no entanto, não permitem que se dê profundidade exigida a essa questão, propondo-se, desde já, o desenvolvimento do estudo e pesquisa do aperfeiçoamento e desenvolvimento da Atividade de Inteligência (entendida como a composição da Inteligência e Contrainteligência) no âmbito do Ministério Público brasileiro.

2. A INFORMAÇÃO

Embora o período recente tenha se identificado por Peter Drucker[4] como a "Era da Informação", ou a "Era do Conhecimento", especialmente quanto à influência e proliferação da informação no período pós-revolução industrial, verifica-se que a produção do conhecimento possui forte influência na atividade humana desde épocas mais remotas.

Certamente a facilidade de obtenção do conhecimento pela tecnologia tem provocado uma aceleração de todos os processos de produção do conhecimento. Tal condição assume especial relevância diante da amplitude de ações sob incumbência do Estado e, especificamente quanto à execução de operações. Como bem esclarece Castells[5], a produção do conhecimento é realizada de forma cíclica, acelerada pela tecnologia, com a respectiva aplicabilidade:

> o que caracteriza a atual revolução tecnológica não é a centralidade de conhecimentos e informações, mas a aplicação deste conhecimento e desta informação para a geração de conhecimentos e de dispositivos de processamento e comunicação da informação, em um ciclo de realimentação cumulativo entre a inovação e seu uso.

O ciclo de produção do conhecimento coincide com os ciclos de Inteligência, tanto no seu vetor estrito quanto na Contrainteligência.

Em primeiro plano, podemos identificar três objetivos bem claros de uma operação, independentemente do mérito ou da situação a ser enfrentada: a efetividade; a eficiência; a eficácia. Contudo, esses objetivos somente serão atingidos se houver a manutenção da integridade da operação, ou seja, a manutenção da sua própria segurança.

3 O Departamento de Segurança Interna dos Estados Unidos da América (USDHS), atualmente, é a terceira maior unidade organizacional do Governo estadunidense, com ligação direta ao Departamento de Defesa (USDoD) (maior Departamento do Governo dos EUA) pela Agência Nacional de Segurança (NSA). DEPARTMENT OF HOMELAND SECURITY. Disponível em: <https://www.dhs.gov/>. Acesso em: 5 de abr. 2019.

4 DRUCKER, Peter. **Administrando em tempos de grandes mudanças**. São Paulo: Thomson Pioneira, 2003.

5 CASTELLS, Manuel. A Era da Informação: economia, sociedade e cultura. v. I: A Sociedade em rede. Tradução de Klauss Brandini Gerhardt e Roneide Venâncio Majer. 2ª ed. São Paulo: Editora Paz e Terra, 2000. p. 50.

Com efeito, a segurança[6] constitui o pilar que sustenta toda a operação, que permitirá a manutenção da atuação íntegra e estável do Estado. Aqui se identifica o "ponto de toque" da reavaliação da análise de riscos das operações, pois não se limita à uma força de segurança armada e treinada ou recursos logísticos e de potencial ofensivo material, mas um elemento muito mais relevante: a informação.

Sun Wu[7], o Tzu (mestre) dos exércitos chineses no Reino de Hu Lu no século VI a.c., já advertia: "Informação é crucial. Nunca vá para a batalha sem saber o que pode estar contra você". Atualizando a recomendação do grande estrategista oriental, no escopo sob análise: "Informação é crucial. Nunca vá para a operação sem saber o que pode estar contra você". Ou seja, depois de mais de 2000 anos, a condição essencial de preparação para o enfrentamento não se alterou.

Independentemente do eufemismo utilizado para "batalha", "guerra", "combate", "enfrentamento", é certo que a atuação do Estado no sentido de manter a ordem e a aplicação da lei apresenta resistências por aqueles que eventualmente transgridam ou não cumpram suas obrigações perante o ordenamento, em que o Poder Público tem a atribuição de enfrentar essa resistência e recompor a estabilidade da paz social. Muitas vezes, de acordo com a gravidade e abrangência da infração, a resistência à atuação estatal será proporcional, demandando a melhoria de técnicas e, principalmente, do adequado planejamento para a realização de operações saneadoras.

Nesse sentido, a imprescindibilidade da Inteligência como sustentação do planejamento é enfaticamente destacado por Amorim[8]: "Não há planejamento sem Inteligência, e se ambos ocorrerem em um ambiente interagências é necessário que todos agentes tenham a mesma compreensão sobre tais processos".

De fato, assim como o enfrentamento pode ser conceituado de diversas maneiras, com as devidas ponderações, também é possível flexibilizar a definição das forças antagônicas, de restrição, ou "inimigas", como bem destaca o Manual[9] EB70-MC-10.307 do Exército Brasileiro:

> 1.2.5 O termo inimigo é utilizado nesta publicação de forma genérica, devendo ser interpretado como ameaça ou força adversa quando a operação abordada for classificada como de não guerra.

6 No mesmo sentido: "Segurança das Operações – processo de identificação de informações críticas e subsequente análise das ações amigas previstas em uma operação militar e outras atividades para: identificar as ações que podem ser observadas pelo sistema de inteligência do oponente; determinar indicadores que possam ser obtidos pela inteligência inimiga, os quais, se colocados juntos ou interpretados, possam proporcionar informações críticas sobre as nossas tropas em tempo de serem úteis ao adversário; e selecionar e executar medidas que eliminem, ou reduzam a um nível aceitável, a vulnerabilidade das ações amigas à exploração adversária." BRASIL. Exército. Estado-Maior. Manual de Campanha – Inteligência: EB20-MC-10.207. 1ª ed. Brasília: Comando do Exército, 2015.

7 TZU, Sun. A Arte da Guerra. Tradução de Sueli Barros Cassal. Porto Alegre: L&PM, 2006.

8 AMORIM, Maria Alice Barros Martins. **A Problemática da segurança pública na fronteira Brasil e Bolívia com foco no Estado do Mato Grosso**. 2012. Trabalho de Conclusão de Curso (Curso de Altos Estudos de Política e Estratégia) – Escola Superior de Guerra, Rio de Janeiro, RJ, Brasil.

9 BRASIL. Exército. Estado-Maior. **Manual de Campanha** – Planejamento e Emprego da Inteligência Militar: EB70-MC-10.307. 1ª ed. Brasília: Comando do Exército, 2016.

Assim, resta inequívoco que o sucesso e a segurança de uma operação dependem de um adequado planejamento elaborado de forma coordenada com base em levantamentos de Inteligência e técnicas de Contrainteligência.

3. PECULIARIDADES DAS OPERAÇÕES CONTRA A ESCRAVIDÃO CONTEMPORÂNEA

A Constituição[10] Democrática Republicana, vigente no Brasil desde 1988, estabelece, já nas suas primeiras disposições:

> Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos:
>
> I - a soberania;
>
> II - a cidadania;
>
> III - a dignidade da pessoa humana;
>
> IV - os valores sociais do trabalho e da livre iniciativa;
>
> V - o pluralismo político.

Para reflexão inicial, transcreve-se o Caso José Pereira, referenciado nas boas práticas da Organização Internacional do Trabalho[11]:

Caso José Pereira

> Em setembro de 1989, quando tinha somente 17 anos, José Pereira e um companheiro, com o apelido de Paraná, tentaram escapar de uma fazenda onde eles e outros 60 trabalhadores eram forçados a trabalhar sem remuneração e em condições desumanas. Eles foram surpreendidos por funcionários da fazenda e atacados com tiros de fuzil. Paraná morreu. José Pereira sobreviveu porque foi julgado morto. Ele e o corpo do companheiro foram enrolados em uma lona e abandonados na rodovia PA-150.

O trabalho em condição análoga à de escravo configura, a um só tempo, a infração a todas as diretrizes que fundamentam a estrutura da nossa sociedade atual, pois afeta a soberania, ao permitir o tráfico internacional de pessoas para escravatura com cidadãos brasileiros; a cidadania, ao suprimir os direitos fundamentais da pessoa humana; a dignidade da pessoa humana, por afronta direta às suas condições; os valores sociais do trabalho e a livre iniciativa, ao cercear os direitos sociais do trabalho e macular a livre iniciativa com a atividade ilegal; e, por fim, ataca o pluralismo político, ao permitir a prática, ainda nos dias atuais, do nefasto "coronelismo"[12].

10 BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Texto constitucional promulgado em 5 de outubro de 1988 com emendas. Brasília: Centro de Documentação e Informação (CEDI), 2019. Disponível em: <http://www2.camara.leg.br/atividade-legislativa/legislacao/Constituicoes_Brasileiras/constituicao1988.html>. Acesso em: 5 abr. 2019.

11 ORGANIZAÇÃO INTERNACIONAL DO TRABALHO. Escritório no Brasil. **As boas práticas da inspeção do trabalho no Brasil**: a erradicação do trabalho análogo ao de escravo. Brasília: OIT, 2010.

12 LEAL, Victor Nunes. **Coronelismo, enxada e voto.** São Paulo: Companhia das Letras, 2012.

Tal gravidade de afronta se irradia a inúmeros outros direitos e garantias fundamentais previstos pela Constituição da República, especialmente no vetor da liberdade – um dos valores mais sensíveis e relevantes da Dignidade da Pessoa Humana.

Não por acaso que a primeira organização internacional criada com a finalidade de defender os direitos humanos, por intermédio do Tratado de Versalhes que, em 1919, pôs fim à Primeira Guerra Mundial, foi a Organização Internacional do Trabalho (OIT).

Com efeito, tal a criticidade desse tipo de infração que levou a Corte Interamericana de Direitos Humanos (CIDH) a julgar e condenar, pela primeira vez, um país pela escravidão contemporânea e pelo tráfico de pessoas. No Caso 12.066, a CIDH[13] sentenciou, em outubro de 2016, que o Brasil violou o direito de liberdade, o direito de acesso à Justiça e às garantias judiciais, e o direito à razoável duração do processo de 85 vítimas escravizadas no ano de 2000 e de 43 trabalhadores no ano de 1997, na Fazenda Brasil Verde, no Município de Sapucaia, Estado do Pará, onde assentou:

> 303. O resumo dos fatos contidos nos parágrafos anteriores indica a evidente existência de um mecanismo de aliciamento de trabalhadores através de fraudes e enganos. Ademais, a Corte considera que, com efeito, os fatos do caso indicam a existência de uma situação de servidão por dívida, uma vez que, a partir do momento em que os trabalhadores recebiam o adiantamento em dinheiro por parte do gato, até os salários irrisórios e descontos por comida, medicamentos e outros produtos, originava-se para eles uma dívida impagável. Como agravante a esse sistema, conhecido como *truck system*, *peonaje* ou sistema de barracão em alguns países, os trabalhadores eram submetidos a jornadas exaustivas de trabalho, sob ameaças e violência, vivendo em condições degradantes. Além disso, os trabalhadores não tinham perspectiva de poder sair dessa situação em razão de: i) a presença de guardas armados; ii) a restrição de saída da Fazenda sem o pagamento da dívida adquirida; iii) a coação física e psicológica por parte de gatos e guardas de segurança e iv) o medo de represálias e de morrerem na mata em caso de fuga. As condições anteriores se potencializavam em virtude da condição de vulnerabilidade dos trabalhadores, os quais eram, em sua maioria, analfabetos, provenientes de uma região muito distante do país, não conheciam os arredores da Fazenda Brasil Verde e estavam submetidos a condições desumanas de vida.

Destacam-se ainda as condições peculiares da perda de referência sobre a organização social dos trabalhadores submetidos à escravidão contemporânea, desconectando-os dos limites de convivência e favorecendo o que Hannah Arendt[14] definiu como "banalidade do mal", representada, nesse contexto, pelo regime de agressão e violência das mais diversas formas. Tais condições determinam parâmetros ainda maiores de cautela e preparação na seara de segurança das operações, dada a gravidade do instrumento para manutenção dos trabalhadores no regime escravo.

---

13 CORTE INTERAMERICANA DE DIREITOS HUMANOS. **Caso 12.066 - Trabalhadores da Fazenda Brasil Verde vs. Brasil**. j. 20 out. 2016. publ. 15 dez. 2016. Disponível em: <http://www.corteidh.or.cr/docs/casos/articulos/seriec_318_por.pdf>. Acesso em: 5 abr. 2019.

14 ARENDT, Hannah. **Eichmann em Jerusalém – Um relato sobre a banalidade do mal**. Tradução de José Rubens Siqueira. São Paulo: Companhia das Letras, 2013.

O cenário é retratado por Costa[15] da seguinte forma:

> Quando os laços com a família e com o lugar de origem se afrouxam, o trabalhador tem sua importância social não reconhecida, o que lhe seria atribuído caso ele fosse visto como parte de uma rede de relações sociais específica. Como resultado do desenraizamento social, ele começa a morrer simbólica ou socialmente e esta morte precede à física. A partir desse processo, os trabalhadores tornam-se passíveis da "banalidade do mal", termo elaborado por Hannah Arendt que aborda uma dimensão da maldade que não se enquadra nos padrões usuais da categoria, por exemplo, patologia ou convicção ideológica do agente.

Para ilustrar o grau de degradação das condições enfrentadas, Costa[16] (*apud* FIGUEIRA, 2004), ainda traz as seguintes circunstâncias:

> Além de descrever e analisar aspectos estruturais e conjunturais do problema, o autor apresenta inúmeros relatos de trabalhadores que foram submetidos a condições análogas à escravidão, citando diferentes formas de violência que podiam afetá-los. Um exemplo marcante refere-se ao caso de um trabalhador escravizado que, após uma tentativa de fuga, foi capturado por um funcionário da fazenda em que trabalhava. Como punição, ele foi obrigado a realizar sexo oral nesse funcionário diante de todos os trabalhadores.
>
> O pagamento deve ser realizado por meio dos proventos a serem recebidos pelo trabalhador, que só poderá deixar a fazenda quando a dívida estiver quitada. O isolamento da fazenda em relação a qualquer tipo de transporte dificulta as possibilidades de fuga. Somado a isso, para que as fugas sejam evitadas, os trabalhadores podem ter seus documentos retidos, bem como são constantemente vigiados e ameaçados por funcionários armados, constituindo uma situação degradante de trabalho e cerceadora da liberdade dos trabalhadores. As condições de alimentação e moradia também são precárias. Muitos dormem fechados e trancados em barracões feitos de lona e cercados de palha e, seguidas vezes, sem acesso à comida e água potável.

Ainda no espectro da escravatura, constata-se que a liberdade do trabalho remonta ao Iluminismo, onde ressalta Sarmento[17]:

> As atividades sociais (o trabalho, por exemplo) deixam de ser atributos naturais relativos ao lugar ocupado no organismo social, e passam a decorrer da vontade livremente declarada pelos indivíduos.

Hodiernamente preocupa a retomada de procedimentos já superados pela evolução da proteção dos direitos fundamentais e da dignidade da pessoa humana, especialmente quanto às questões do trabalho. Com efeito, a configuração das condições de trabalho análogas à de escravo podem ser mascaradas pela retomada do discurso ideológico do constitucionalismo liberal-burguês, conforme esclarece Sarmento[18] que:

15 COSTA, Patrícia Trindade Maranhão. A construção da masculinidade e a banalidade do mal: outros aspectos do trabalho escravo contemporâneo. **Cad. Pagu**, Campinas, n. 31, p. 173-198, Dec. 2008. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0104-83332008000200009&lng=en&nrm=iso>. Acesso em: 17 abr. 2019.

16 Ibidem, 2006.

17 Op. Cit., 2017.

18 Ibidem, 2017.

> Se um indivíduo estivesse disposto a vender sua força de trabalho, submetendo-se a uma jornada diária de 16 horas por um salário que mal permitisse a aquisição de alimentos, e outro se dispusesse a comprá-la nesses termos, não caberia ao Estado se imiscuir no negócio privado.

Tais condições circunstanciais apresentam peculiares elementos a serem considerados no planejamento de uma operação de combate ao trabalho escravo, pois o entendimento de regularidade da situação pelo empregador que pratica condutas degradantes aos trabalhadores tende a aumentar, bem como a consequente e respectiva resistência à atuação do Estado tendem a recrudescer pela deturpação da intelecção do acobertamento de pretensa legítima defesa por parte do escravagista e de abuso de poder de polícia por parte do Estado.

O senso comum sobre o trabalho escravo determina uma ilusão fática na realidade. Não se trata mais da "casa grande" e da "senzala", da notável obra de Gilberto Freyre[19], mas a consequência dessa formação político-social-econômica, cuja marginalidade e desvios foi absorvida como instrumento da criminalidade.

A realidade recente mostra que a prática da escravatura contemporânea alcança os mais variados vetores e atinge não só os nacionais, mas vem se agravando com o número de estrangeiros oriundos de países conflagrados ou com instabilidade social, ou ainda em busca de melhores condições de vida, como venezuelanos, bolivianos, haitianos, chineses, turcos, dentre outros. No vetor inverso, de brasileiros oriundos do tráfico de pessoas e escravizados no exterior, a principal ocorrência se verifica quanto à exploração sexual, em que pode ser exemplificada pela recente "Operação Fada Madrinha"[20], deflagrada em conjunto pela Polícia Federal, Ministério Público Federal e Ministério Público do Trabalho no enfrentamento do tráfico de pessoas para exploração sexual no continente europeu. Andreucci[21] destaca essa realidade:

> A escravidão contemporânea não se resume, portanto, a aspectos de exploração sexual, sendo muito mais intensa e repugnante que ela, envolvendo primordialmente jovens, desempregados, analfabetos e estrangeiros irregulares no país, não apenas na zona rural, mas também e principalmente nas áreas urbanas, em atividades têxteis, domésticas etc.

Retomando o ambiente específico de atuação da Inteligência e Contrainteligência como pedras fundantes da atuação do Estado, verifica-se que a complexidade inerente a uma operação contra a prática de redução da pessoa à condição análoga à de escravo alcança patamares normalmente desconsiderados pelos operadores estatais, colocando em risco toda a

19 FREYRE, Gilberto. **Casa Grande & Senzala**. São Paulo: Global Editora, 2006.

20 MINISTÉRIO PÚBLICO FEDERAL. Assessoria de Comunicação. **Fada Madrinha:** MPF, PF e MPT deflagram operação contra tráfico internacional de transexuais. Disponível em: <http://www.mpf.mp.br/sp/sala-de-imprensa/noticias-sp/fada-madrinha-mpf-pf-e-mpt-deflagram-operacao-contra-esquema-de-trafico-de-pessoas-transexuais>. publ. 9 ago. 2018. Acesso em: 5 abr. 2019.

21 ANDREUCCI. Ricardo Antonio. Exploração do trabalho escravo e tráfico de seres humanos, a face desconhecida do crime organizado *In:* MESSA, Ana Flávia; CARNEIRO, José Reinaldo Guimarães (coords.) **Crime Organizado**. São Paulo: Saraiva, 2012.

atividade e obtendo resultados ineficazes. Novamente, Andreucci[22] bem retrata a permeabilidade e difusão dessa prática nefasta:

> A redução à condição análoga à de escravo é decorrência direta do tráfico de seres humanos. Isso porque, afora uns poucos casos de pessoas submetidas a essa prática por questões alheias às relações de trabalho, a quase totalidade dos casos registrados em nosso país refere-se a trabalhadores mantidos em situação de verdadeira escravidão, que o legislador convencionou denominar "situação análoga à de escravo". Vários fatores são responsáveis por essa prática, tais como a pouca oferta de emprego, o isolamento geográfico gerado em face da extensão territorial, a má distribuição de terras, a dificuldade de fiscalização e a impunidade.

O trabalho escravo tem se utilizado de um sistema de Inteligência paralelo, de manipulação, para atender às suas necessidades. Ou seja, não é só a restrição de liberdade, pela violência, que configura uma condição de escravatura, mas a subserviência da dignidade da pessoa humana em situação de trabalho degradante, sob os mais diversos prismas.

A manipulação de informações pode se dar em relação às condições pessoais do escravo (sua real situação), pela contabilidade de pagamentos pelo serviço (servidão por dívidas), pela ameaça velada (informações sobre a família, pais, filhos, etc., mesmo sem intenção de praticar a violência), pela ilusão de cooptação, pela ocultação de nocividade ou ilegalidade da atividade laboral, pelos requisitos de religiosidade, a manutenção por drogas, entre outros.

A utilização de informações ainda serve para estruturar o sistema de exploração do trabalho escravo, com o deslocamento de trabalhadores para locais ermos e de difícil acesso, sem comunicação; a qualificação dos obreiros, muitos condenados pelo "tribunal do crime" que veem no regime escravo uma forma de salvação; a fuga de retaliações sociais e familiares, como as enfrentadas por transgêneros, ou mulheres grávidas, que se subordinam à prostituição e ao tráfico de pessoas. Muitos, por vergonha e receio do julgamento e exclusão social e familiar, inserem-se em um mundo paralelo dominado pelo escravagismo e pelo tráfico.

De fato, o rompimento com a dignidade da pessoa humana proporcionado pela escravatura contemporânea passa a caracterizar o indivíduo como mercadoria e proporciona o campo fértil para atuação da criminalidade, como bem enfatiza Andreucci[23]:

> O comércio de pessoas constitui uma das atividades mais aberrantes e hediondas da atualidade, traduzindo uma face ainda pouco conhecida do crime organizado. Efetivamente, fenômenos modernos como a globalização econômica, os progressos da ciência, da medicina e da tecnologia, além de outros admiráveis frutos da inteligência humana, não conseguiram, até o presente momento, extirpar de nossa sociedade o cancro da escravidão humana e da mercancia de seres humanos.

22 Ibidem, 2012.

23 Ibidem, 2012.

Conforme descrito, a complexidade do cenário de avaliação inerente à Atividade de Inteligência e Contrainteligência na atuação contra a escravatura contemporânea, assim como o seu alcance nacional e internacional, é bem ilustrada pelo nobre membro do Ministério Público do Estado de São Paulo Andreucci[24]:

> É neste cenário deplorável que o Brasil, ao lado de diversos outros países na Ásia, América do Sul, África, Europa, tem no tráfico de seres humanos o maior exemplo de violação dos direitos humanos básicos, sendo a escravidão contemporânea, sem dúvida, um de seus aspectos mais preocupantes, uma vez que se caracteriza pela clandestinidade, autoritarismo, corrupção, segregação social e racismo.

Essa ambiência cria fatores extremamente desfavoráveis para a atuação contra o trabalho escravo, especialmente pela difusão de outros crimes de origem ou consequentes, bem como pelos instrumentos e métodos utilizados, tais como o deslocamento de trabalhadores para locais ermos, ocultos ou controlados.

Um dos maiores exemplos de demonstração do "planejamento" e "capacidade operacional" das equipes táticas de segurança pública, frequentemente expostos pela mídia[25], é representado pela "tomada de reféns". Essa demonstração é bem definida por Cirilo[26] como a "espetacularização da vida" que oculta a gama e a complexidade de crimes que permeiam nossa sociedade.

Contudo, uma ação pontual, de fácil delimitação espacial, normalmente como ato isolado, com inúmeras possibilidades de técnicas de solução diversas, não apresenta as complexas características enfrentadas na identificação do trabalho escravo contemporâneo.

Com efeito, se mesmo as ações táticas de tomada de reféns, muitas vezes, mostram resultados desastrosos[27] decorrentes de uma ação mal planejada ou mal executada, imagine-se uma operação que envolva um grau de complexidade circunstancial muito maior, com diversos outros crimes perpetrados em caráter sistêmico e estrutural.

O resultado desastroso é sintetizado com simplicidade e maestria por Diniz[28], ao analisar o fracasso da Força Delta da Força Aérea dos Estados

---

24 Ibidem, 2012.

25 Como, por exemplo, dentre inúmeros, os treinamentos da polícia e das Forças Armadas para os Jogos Olímpicos do Rio de Janeiro, em 2016. Disponível em: <http://g1.globo.com/rio-de-janeiro/noticia/2015/02/pm-simula-sequestro-onibus-brt-como-treino-para-olimpiadas-no-rio.html>. Acesso em: 5 abr. 2019.

26 CIRILO, Bianca Sant'Anna de Sousa. **Resgate policial de reféns:** uma forma de espetacularização da vida. Revista EPOS; Rio de Janeiro – RJ, Vol.4, nº 2, jul-dez de 2013.

27 Não são poucos os exemplos divulgados pela mídia em todo o mundo, tais como o assalto à Linha 174, no Rio de Janeiro, em 2000 (Disponível em: <https://canalcienciascriminais.com.br/onibus-174/>. Acesso em: 5 abr. 2019); a Operação *Eagle Claw*, promovida pelos Estados Unidos no Irã (Disponível em: o sequestro do voo AF 8969 – Paris/Argélia, em Marselha, em 1994 – narrativa do original em francês do L'assaut. MÔNTINS, Roland; CARADEC'H, Jean-Michel. L'assault. **Paris**: Oh! Editions, 2010); ou ainda o mais recente Caso Eloá Pimentel, em São Paulo, onde houve a responsabilização do Estado de São Paulo pelo erro de atuação (Disponível em: <https://g1.globo.com/sp/sao-paulo/noticia/2018/10/12/apos-10-anos-do-caso-eloa-justica-obriga-estado-de-sp-a-indenizar-nayara-em-r-150-mil.ghtml>. Acesso em: 5 abr. 2019).

28 DINIZ, Fernando. **25 Anos da Operação Eagle Claw**: a fracassada tentativa de resgate dos reféns americanos. Iran, 24-25 Abril 1980. publ. 27. Jul. 2005. Disponível em: <http://www.defesanet.com.br/sof/noticia/254/25-Anos-da-Operacao-Eagle-Claw/>. Acesso em: 5 abr. 2019.

Unidos da América no desenvolvimento da Operação Eagle Claw, em 1994, da seguinte forma: "Informação insuficiente e mau planejamento foram um fator essencial no fracasso da missão".

No âmbito nacional, o maior exemplo da falta de planejamento e preparo para uma operação contra a escravatura contemporânea é descrito pela "Chacina de Unaí", sintetizado por Aras[29]:

> As vítimas foram três auditores fiscais do trabalho e um motorista do Ministério do Trabalho, que fiscalizavam fazendas do noroeste das Minas Gerais para reprimir trabalho escravo ou condições degradantes de trabalho em áreas de cultivo de feijão. Foi um crime *propter officium*, que teve como alvo principal o auditor fiscal Nelson José da Silva. Este fato definiu a competência federal, com base no art. 109, inciso IV, da Constituição. Os demais servidores do MTE só foram mortos porque estavam em sua companhia no momento da emboscada, ocorrida numa estrada de terra, às margens da rodovia Unaí-Paracatu, no grande entorno do Distrito Federal.

Ou seja, a Inteligência como subsídio para o planejamento da operação, nas mais variadas vertentes, comprova-se como conjunto indissociável para o sucesso das ações.

Embora a execução da operação represente a concretização de apenas uma parcela da política pública inerente ao enfrentamento da escravatura contemporânea, constata-se que é a fase que apresenta a maior criticidade e riscos.

Nesse ponto, convém ressaltar que a Inteligência não subsidia somente o planejamento de uma operação, mas deve integrar os três níveis de atuação, como bem define o Manual[30] EB20-MC-10.207 do Exército Brasileiro: "3.1.1 O planejamento de inteligência ocorre nos níveis político, estratégico, operacional e tático dos diversos centros decisores e demandam diferentes processos e produtos, a fim de alcançar seus objetivos específicos".

Uma operação contra o trabalho escravo, dessa forma, não representa um ato isolado, mas a concretização do instrumento coator do Estado na efetivação da política pública, como bem enfatiza Andreucci[31] ao destacar o marco específico de combate à escravatura contemporânea:

> No Brasil, uma das demonstrações mais efetivas da vontade política de erradicação de todas as formas de escravidão contemporânea, foi o lançamento do Plano Nacional para a Erradicação do Trabalho Escravo, em 2002, que apresentou medidas a serem cumpridas pelos diversos órgãos dos Poderes Executivo, Legislativo e Judiciário, Ministério Público e entidades da sociedade civil brasileira.

Embora essa importante medida e mobilização adotada pelo Plano Nacional para Erradicação do Trabalho Escravo, constata-se que, após mais de 15 anos, a execução se apresenta extremamente deficitária, tanto pela dificuldade de estruturação das ações estabelecidas quanto pela ausência de

29 ARAS, Vladimir. **Se ergues da Justiça a clava forte.** Publ. 1 set. 2013. Disponível em: <https://vladimiraras.blog/2013/09/01/se-ergues-da-justica-a-clava-forte/>. Acesso em: 5 abr. 2019.

30 BRASIL. *op. cit.*, 2015.

31 ANDREUCCI, *op. cit.*, 2012.

protocolos integrados de atuação e planejamento[32]. Infelizmente a prática nos mostra a negligência desses fatores fundamentais de Inteligência e Contrainteligência para a realização das operações contra escravatura contemporânea, que, na mais das vezes, beiram a imprudência, colocando em risco a integridade de todos os participantes e o sucesso da própria empreitada fiscalizatória.

Com efeito, em que pese a operacionalidade consagrada aos Grupos Especiais de Fiscalização Móvel (GEFM), vinculados atualmente ao Ministério da Economia, as próprias "boas práticas" publicadas[33] pela Organização Internacional do Trabalho expõem a vulnerabilidade da atuação operacional já na sua gênese, pois "a atuação do grupo móvel é provocada principalmente por denúncias", que irão orientar toda a ação:

> Preparação das operações: O conjunto de denúncias a serem apuradas (geralmente por volta de 3) são encaminhadas a um dos coordenadores, respeitando o sistema de rodízio. Ao mesmo tempo, ofícios são encaminhados ao Ministério Público Federal (MPF), Advocacia-Geral da União e ao Ministério Público do Trabalho (MPT). A CONAETE/MPT subsequentemente designa um procurador para acompanhar a operação. Outro ofício é encaminhado à Polícia Federal (ao Coordenador-Geral de Defesa Institucional do Departamento de Polícia Federal ou à Polícia Rodoviária Federal para que esta designe uma equipe de policiais. O(a) coordenador(a) convida, geralmente, dependendo do porte do empreendimento a ser fiscalizado e da atividade econômica, mais quatro AFTs, ademais do(a) sub-coordenador(a).

Ou seja, não se verifica nenhum tratamento de Inteligência ou prospecção da informação, de maneira a garantir a integridade e credibilidade das "denúncias"[34], tampouco a adoção de medidas de Contrainteligência, condicionando os aspectos de segurança tão somente ao suporte policial.

Assim como diversas outras operações, muitas das condições relevantes para o planejamento da operação, que poderiam ser adequadamente consideradas em uma Atividade de Inteligência prévia, são verificadas no local e momento[35] de realização das ações, já com toda equipe exposta aos riscos encontrados.

---

32 Aliás, uma infeliz realidade presente na grande maioria das ações governamentais de enfrentamento do crime, conforme apontado por Amorim: "Os fatores de maior relevância para esse resultado incipiente são a ausência de planejamento conjunto entre os órgãos, a ausência de estruturas e de processos permanentes e institucionalizados de integração e a ausência de vínculos de confiança entre os órgãos." (AMORIM, *op. cit*., 2012).

33 ORGANIZAÇÃO INTERNACIONAL DO TRABALHO. *op. cit*., 2010.

34 Nesse sentido, os ensinamentos de Girardi: "Detectar casos de trabalho escravo sem esperar as denúncias é evidentemente um progresso, mas pode-se tentar avançar mais, pelos mesmos métodos, e dar mais um passo: identificar as regiões onde existe um risco sério de recrutamento de trabalhadores para atividades que os colocarão em situação de escravidão, criando um índice de vulnerabilidade ao aliciamento de escravos". GIRARDI, Eduardo Paulon, *et. al.* Mapeamento do trabalho escravo contemporâneo no Brasil: dinâmicas recentes. Espaço e Economia - **Revista Brasileira de Geografia Econômica**, 2014, Ano II, Número 4.

35 Como, por exemplo, ao modo de operação de segurança "padronizado" extraído das "boas práticas" da OIT: "Por motivos de segurança, o deslocamento do grupo, geralmente em caminhonetes, é feito em forma de comboio, com três policiais no primeiro e três no último carro. Quando necessário, antes da entrada do resto do grupo na fazenda, alguns policiais à paisana se dirigem ao local para confirmar a localização e as condições de segurança". (ORGANIZAÇÃO INTERNACIONAL DO TRABALHO. *op. cit*., 2010).

Em suma, as particularidades da atuação contra a escravidão contemporânea, além do planejamento, devem ser repensadas à luz dos subsídios prestados pela Inteligência, com a adoção de medidas de Contrainteligência, para se garantir um melhor resultado com redução de riscos da ação.

4. A INTELIGÊNCIA E A CONTRAINTELIGÊNCIA EM OPERAÇÕES

A consciência sobre a situação a ser enfrentada representa um dos fatores primordiais do planejamento de uma operação, somente podendo ser sustentada pela produção do conhecimento oriundo da Atividade de Inteligência.

Na Atividade de Inteligência, o ramo Inteligência proporciona oportunidades, produzindo conhecimento de Inteligência que gera vantagem competitiva à organização. Por outro lado, a Contrainteligência assinala, analisa e avalia as ameaças, fornecendo os fatores necessários de mitigação dos riscos associados a tais ameaças.

O que orientará toda a Atividade de Inteligência que sustentará a ação é o objetivo a ser atingido, que deverá estar presente em todo o ciclo de Inteligência[36] necessário ao processo de planejamento e definição da segurança da operação.

Conforme enfatizado anteriormente, a definição do cenário de atuação, com todas as suas variantes, constitui o ponto inicial de todo o planejamento da operação. Assim, a composição dos fatores de Inteligência se mostra como ação imprescindível para o desencadeamento de toda análise do cenário, conforme explica Farah[37]:

Os cenários de risco em Segurança Pública são situações de vulnerabilidade, real ou potencial, da sociedade e do Estado em relação à ordem pública. São definidos por componentes como fonte de risco, área geográfica, ativos envolvidos, faixa de tempo, probabilidade de ocorrência e impactos.

O estudo e o acompanhamento desses cenários pela Inteligência são de fundamental importância, em particular com vista a identificar ações para mitigar os riscos, estabelecer alertas antecipados e definir respostas aos incidentes. Permite o desencadeamento de ações proativas em benefício da população.

De antemão, convém trazer as delimitações doutrinárias decorrentes do Manual[38] EB70-MC-10.307 do Exército Brasileiro, como base na avaliação

36 *CENTRAL INTELLIGENCE AGENCY*. *The Intelligence Cycle*. Disponível em: <https://www.cia.gov/kids-page/6-12th-grade/who-we-are-what-we-do/the-intelligence-cycle.html>. Acesso em 5 abr. 2019.

37 FARAH, Camel André de Godoy. A atividade de Inteligência de Defesa em operações de Garantia da Lei e da Ordem (GLO) *in* Sociedade, Segurança e Cidadania: Paz social. Livro 1. Org. Giovani de Paula. Palhoça: UNISUL, 2017.

38 BRASIL. op. cit., 2016.

da Inteligência e da Contrainteligência sob o prisma dos seus resultados esperados, com a devida releitura da aplicabilidade às operações civis:

> 4.1.1 A CONTRAINTELIGÊNCIA TEM POR FINALIDADE:
>
> 4.1.1.1 Impedir que uma força inimiga, real ou potencial, adquira conhecimentos sobre nossa ordem de batalha, situação em material, pessoal, planos, vulnerabilidades e possibilidades;
>
> 4.1.1.2 Impedir ou reduzir os efeitos das atividades de espionagem, sabotagem, desinformação, propaganda adversa e terrorismo contra as nossas forças;
>
> 4.1.1.3 Proporcionar liberdade de ação para o Comando;
>
> 4.1.1.4 Contribuir para a obtenção da surpresa;
>
> 4.1.1.5 Impedir ou limitar as ações que possibilitem a força inimiga de obter a surpresa;
>
> 4.1.1.6 Impedir ou neutralizar as ações hostis que possam afetar o potencial de nossas forças; e
>
> 4.1.1.7 Induzir o centro de decisão adversário à tomada de decisões equivocadas.

Por outro lado, o mesmo Manual[39] Militar identifica os elementos essenciais da Inteligência nas operações contra forças irregulares (como o caso do crime organizado):

> 10.10.3 As Operações Contra Forças Irregulares bem sucedidas devem ter como Centro de Gravidade (CG) o apoio da população local do TO [Teatro de Operações]/A Op [Área de Operações], que também representa o foco para as F Irreg [Forças Irregulares]. Para isso, os Elementos Essenciais de Inteligência devem incluir:
>
> a) as razões político-ideológicas, étnicas, religiosas e/ou econômicas que sustentam as reivindicações da causa oponente;
>
> b) existência ou não de apoio externo oriundo de atores estatais e/ou não estatais (alinhamento ideológico e disseminação do proselitismo insurgente, apoio político e assistência financeira, dentre outros);
>
> c) campanhas conduzidas contra o poder estatal e as forças legais;
>
> d) identificação de lideranças e vínculos; e
>
> e) prováveis áreas de homizio e treinamento.

Embora a diversidade de teorias sobre Inteligência e Contrainteligência, é certo que a adoção de padrões já estabelecidos se faz necessária a uma adequada análise e comunicação de informações para subsidiar ações operacionais desenvolvidas pelo Estado.

Com efeito, a utilização de técnicas consolidadas na área de Inteligência e Contrainteligência permite a facilitação dos trabalhos e a melhoria das condições de segurança inerentes às atividades desenvolvidas, seja lá quais forem.

Sem apegos ao preciosismo técnico ou doutrinário, utilizar-se-á da doutrina adotada pelo Exército Brasileiro no desenvolvimento da linha de raciocínio para o planejamento de operações, devidamente relida com

39 Ibidem, 2016.

fundamento das circunstâncias de "tempo de paz" hoje vividas (ou, pelo menos, sem guerra "declarada").

Tal condição de utilização das bases conceituais é permitida pela própria configuração das infrações, notadamente quanto ao trabalho escravo, pois um dos mais graves crimes contra a sociedade mundial, perpetrado pelos exércitos nazistas na Segunda Guerra Mundial, consideravam a escravatura como um dos vetores de força, conforme testemunho de Rousset (apud ARENDT, 2013[40]), ex-prisioneiro de Buchenwald:

> O triunfo da SS exige que a vítima torturada permita ser levada à ratoeira sem protestar, que ela renuncie e se abandone a ponto de deixar de afirmar sua identidade. E não é por nada. Não é gratuitamente, nem por mero sadismo, que os homens da SS desejam sua derrota. Eles sabem que o sistema que consegue destruir suas vítimas antes que elas subam ao cadafalso é incomparavelmente melhor para manter todo um povo em escravidão.

Passando à configuração da Inteligência como subsídio de operação de combate ao trabalho escravo, é necessária a consciência de que os fatos da vida, ou como prefere Kelsen[41], do mundo do ser, não apresentam as barreiras estanques do mundo do dever-ser. Ou seja, as infrações que permeiam a prática da escravatura contemporânea são extremamente fluídas e com complexas inter-relações criminosas, desde a mais simples contravenção até o crime mais hediondo.

No mesmo sentido estabelece os itens 6.9 e 6.11 da Política Nacional de Inteligência (PNI), aprovada pelo Decreto[42] nº 8.793, de 29 de junho de 2016, em que são destacados o crime organizado e as ações contra o Estado Democrático de Direito (entre seus elementos, a dignidade da pessoa humana, os direitos e garantias fundamentais) como principais ameaças que sustentam a necessidade da política.

Essa condição pode ser representada pela própria manifestação e constatação das autoridades nacionais, como, por exemplo, do ex-Ministro do Meio Ambiente, Edson Duarte[43]:

> De acordo com o ministro do Meio Ambiente, Edson Duarte, "o recrudescimento do crime organizado que atua no desmatamento ilegal da Amazônia, destruindo as riquezas naturais do país e causando danos para toda sociedade, está associado a outras práticas criminosas, como tráfico de armas e animais, trabalho escravo, evasão de divisas e lavagem de dinheiro.

Como o desmatamento ilegal muitas vezes está associado a outros crimes, como lavagem de dinheiro, tráfico de armas, drogas e animais e trabalho escravo, a Polícia Federal instaurou 823 procedimentos criminais no período.

---

40 Op. cit., 2013.

41 KELSEN, Hans. **Teoria pura do Direito**. Tradução de João Baptista Machado. 7 ed. São Paulo: Martins Fontes, 2006.

42 BRASIL. **Decreto nº 8.793, de 29 de junho de 2016**. Fixa a Política Nacional de Inteligência. DOU 30 jun. 2016.

43 MINISTÉRIO DO MEIO AMBIENTE. Assessoria de Comunicação Social. **Taxa de Desmatamento na Amazônia Legal**. publ. em 28 nov. 2018. Disponível em: <http://redd.mma.gov.br/pt/component/content/article?id=1018>. Acesso em: 5 abr. 2019

Um dos vetores mais reconhecidos do trabalho em condição análoga à de escravo é o labor rural, em que o ex-Juiz Odilon de Oliveira[44] assim resume o campo fértil ao crime organizado proporcionado pela atividade agropecuária:

> O juiz Odilon de Oliveira, da vara especializada em lavagem de dinheiro, afirma que o agronegócio é um dos destinos preferenciais das remessas polpudas do crime organizado. Segundo ele, a compra de fazendas é uma das maneiras mais fáceis de lavar os lucros com atividades ilegais. A partir delas, criminosos que movimentam grandes somas de capital ilegal conseguem esconder a origem do dinheiro sujo em operações fictícias de venda de bois e grãos – estratagema que a Polícia Federal chama de vaca-papel e soja-papel.

Assim, adotadas as premissas iniciais da ambiência inerente à escravatura contemporânea, é possível iniciar o desenvolvimento do raciocínio da aplicabilidade da Inteligência e da Contrainteligência como vetor do sucesso e segurança das operações realizadas.

Aliada ao objetivo da operação, tomado como primeiro fator de planejamento, a realização da análise de risco e o seu respectivo gerenciamento devem ser adotados como o segundo ponto a ser tratado. Como bem explicita o Delegado de Polícia Federal Kel Souza[45],

> Pode-se dizer que o gerenciamento de riscos está relacionado à diminuição de incertezas. É crucial que as decisões sejam tomadas com base no máximo de informações alcançáveis, a fim de que tudo não se resuma a uma questão de sorte ou azar. Considerando que os riscos estarão lá, o que se pretende é o conhecimento das variáveis que integram a operação e que poderão nela impactar.
>
> Considerando somente seus impactos negativos, é certo que os riscos da atividade policial serão minimizados com um bom planejamento, seja a missão simples ou complexa.

Ao detalhar a direta inter-relação do uso de informações e a importância do devido planejamento, o mesmo autor[46] traz interessante exemplo que demonstra a fundamentação exposta neste trabalho, nos seguintes dizeres:

> Erwim Rommel, habilidoso general do exército alemão durante a Segunda Guerra Mundial, recebeu o comando da 7ª Divisão Panzer, mesmo sem experiência em operações com blindados.
>
> Sabedor de suas deficiências, estudou diversos livros – muitos deles de origem britânica – um dos principais oponentes dos alemães no período –, e impôs aos Aliados fragorosas derrotas utilizando a blitzkrieg ("guerra-relâmpago"). O domínio da tática e a surpresa de seus ataques levaram-no a vitórias com inferioridade numérica e sem supremacia aérea. Com uma velocidade de deslocamento pouco vista na história das guerras, a 7ª Divisão Panzer foi batizada de "Divisão Fantasma", revelando a visão e a audácia de seu comandante. Honrado,

44 REPORTER BRASIL. Org. **Agronegócio é "lavanderia" do crime organizado, diz juiz.** Disponível em: <https://reporterbrasil.org.br/2008/01/agronegocio-e-lavanderia-do-crime-organizado-diz-juiz/>. publ. em 8 abr. 2008. Acesso em: 5 abr. 2019.

45 SOUZA, Kel Lucio Nascimento de. Os riscos da atividade policial. **Revista CEJ - Centro de Estudos Jurídicos**, Ano XXI, n. 73, p. 63-66, Brasília: Conselho da Justiça Federal, set./dez. 2017.

46 Ibidem, 2017.

> acabou por se suicidar após ter consentido com uma tentativa de assassinato a Hitler (HART, 1980, p. 67-74).
>
> A história do general aponta que o estudo da missão e elaboração de uma estratégia são fundamentais à obtenção de êxito. A ressalva é importante porque a praxe vem demonstrando que a negligência dos riscos é mais comum do que se imagina. Estejam eles relacionados à integridade física do efetivo ou mesmo às repercussões jurídicas e políticas de uma operação, há a necessidade de previamente identificá-los e considerá-los à definição dos procedimentos de atuação. A escolha indevida do efetivo e seu eventual cansaço, o uso de armamento inadequado, a ignorância sobre as características geográficas do cenário e a elaboração de um plano operacional intrincado e pouco claro são alguns dos fatores que poderão pôr tudo a perder.

O uso da Atividade de Inteligência no planejamento de operações, bem como a utilização da Contrainteligência para melhorar os parâmetros de segurança e sucesso das ações, deve contemplar os limites de atuação do Estado, de forma a evitar a transgressão de outras normas do ordenamento jurídico. Nesse escopo, convém relembrar que a criminalidade não possui tais condicionantes, permitindo um maior campo de ação de resistência, normalmente com maior violência, conforme descrito por de Souza[47]:

> O uso da violência de forma exacerbada, descontrolada e inconsequente, por parte das facções criminosas, cria uma assimetria em relação aos agentes do Estado, os quais são obrigados a pautar sua conduta debaixo de um estrito conjunto de regras e limites que o colocam em franca desvantagem tática em relação aos criminosos. Infelizmente, isso coloca em risco a vida do agente público e dificulta sobremaneira o cumprimento de sua missão.

Já o Manual de Operações Especiais (EB20-MC-10.212[48]) do Exército Brasileiro bem traduz esse quadro de atuação da criminalidade no país, devidamente compatibilizado com a nomenclatura do sistema de Inteligência, descrevendo que o ambiente operacional contemporâneo se caracteriza por ser volátil, incerto, complexo e ambíguo, apresentando uma dinâmica de difícil interpretação e baixo nível de controle. Nesse cenário, as situações conflagradas se caracterizam por durar longos períodos de tempo, natureza crônica, violação sistêmica, alta criticidade, baixa intensidade e impacto difuso.

Delimitando a aplicabilidade da Inteligência à atuação operacional, especialmente quanto aos fatores de resultado e de segurança das operações, o Manual[49] EB20-MC-10.207 assim define:

> 3.4 PLANEJAMENTO DE INTELIGÊNCIA NO NÍVEL OPERACIONAL
>
> 3.4.1 Neste nível de planejamento a Inteligência centra seus esforços na busca de conhecimentos sobre o Teatro de Operações e as forças oponentes que podem atuar sobre o espaço de batalha. A Inteligência,

47 DE SOUZA, Cel Inf QEMA FABIO NEGRÃO. **O emprego do Exército Brasileiro no combate ao crime organizado**: desafios e perspectivas. Trabalho de Conclusão de Curso (Especialização em Ciências Militares) – Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2018.

48 BRASIL. Comando de Operações Especiais. Exército Brasileiro. Estado-Maior do Exército. **Manual de Operações Especiais** - EB20-MC- 10.212, 2ª ed. Brasília: Comando do Exército, 2014.

49 BRASIL, op. cit., 2015.

> assim, analisa e avalia a ameaça real ou potencial quanto à sua importância, intensidade e magnitude.
>
> 3.5.5 Uma atividade importante da Função de Combate Inteligência é a salvaguarda dos planos, ordens e conhecimentos produzidos. A Contrainteligência possui a responsabilidade de impedir a força oponente de ter acesso a esses dados e conhecimentos sensíveis. Para isso, realiza atividades de detecção, identificação e neutralização da Inteligência oponente.

Importante destacar, nesse ponto, o elo da aplicabilidade dos instrumentos de Defesa com as atuações de Garantia da Lei e da Ordem (GLO), como bem enfatizado por Farah[50] e que demonstra a estruturação de todo o sistema de Inteligência aplicada, nas suas dimensões operacional e analítica para a produção do conhecimento de Inteligência, assim como a necessária integração para a adequada identificação do cenário de atuação,

> É importante destacar que as atividades de Inteligência em um quadro de Garantia da Lei e da Ordem (GLO) exigirão a integração entre os órgãos e agências do SINDE, do SISBIN e do Subsistema de Inteligência de Segurança Pública (SISP) para perfeita identificação do cenário da área de atuação. (...) Para o acompanhamento da conjuntura, a Inteligência de Defesa emprega as duas dimensões intrínsecas ao desenvolvimento da atividade e que delineiam a sua atuação: a dimensão operacional e a dimensão analítica.
>
> A dimensão operacional refere-se à obtenção de dados e informações a respeito de um determinado assunto. É a aquisição de dados e informações solicitadas pela dimensão analítica, por meio de ações de busca ou coleta, incluindo a sua preparação. A dimensão analítica é encarregada de avaliar a conjuntura, processar e analisar informações e dados necessários a atender a produção do conhecimento sobre um determinado assunto. É esta dimensão que aciona a dimensão operacional para a obtenção de informações e dados necessários ao processo de análise.

Convém relembrar, conforme estabelece o Manual[51] EB70-MT-10.401, que "o produto da Atividade de Inteligência é materializado, essencialmente, pelos conhecimentos de Inteligência". Ou seja, segundo o mesmo Manual militar, são os conhecimentos que "buscam reduzir o grau de incerteza existente nos diversos ambientes operacionais, estabelecendo suas implicações (consequências) e reflexos" na instituição.

Especificamente no âmbito do Ministério Público, constata-se que a Atividade de Inteligência e Contrainteligência ainda é incipiente, muitas vezes permeada por procedimentos equivocados ou premissas incompatíveis com a "comunidade de inteligência". Esta situação demanda uma reavaliação da importância das atividades no desempenho das funções ministeriais e, da mesma forma, para a estruturação da segurança institucional, aliada à Contrainteligência, como bem descreve Pacheco[52]:

---

50 Op. cit, 2017.

51 BRASIL. Comando de Operações Especiais. Exército Brasileiro. Estado-Maior do Exército. **Manual Técnico:** Produção do Conhecimento de Inteligência – EB70-MT- 10.401, 1ª ed. Brasília: Comando do Exército, 2019.

52 PACHECO, Denilson Feitoza. Atividade de Inteligência no Ministério Público. In: BRANDÃO, Priscila Carlos; CEPIK, Marco (Org.). **Inteligência de segurança pública:** teoria e prática no controle da criminalidade. 1ª ed. Niterói: Impetus, 2013.

> O Ministério Público, portanto, deve utilizar-se de métodos, técnicas e ferramentas adequadas para lidar com as informações necessárias ao desempenho de suas finalidades constitucionais, sejam aqueles convencionalmente denominados — Atividade de Inteligência, sejam, numa visão mais —gerencial, seus equivalentes dos sistemas de gestão da informação e da inteligência competitiva. Diante da crescente complexidade dos fatos com os quais lida o Ministério Público e a necessidade de sua atuação sistêmica, seja na área cível (por exemplo, ações civis para defesa de interesses difusos e coletivos), seja penal (por exemplo, programas de prevenção e repressão à criminalidade), o certo é que o Ministério Público deve utilizar algum sistema de gestão da informação, superando a fase individualista e amadorística de muitos de seus membros, e alcançando a racionalidade gerencial exigida pelo princípio constitucional da eficiência.

Tal manifestação do nobre Pós-Doutor e Procurador de Justiça do Ministério Público do Estado de Minas Gerais já denota uma das mazelas correntes nas instituições e que afetam sobremaneira a própria Atividade de Inteligência e Contrainteligência. De fato, um dos pontos mais sensíveis da Atividade de Inteligência está no compartilhamento da informação, pois nessa tônica surgem incompatibilidades internas e externas que podem trazer graves prejuízos às operações e às instituições, como ressaltado por de Souza[53]:

> Para se obter esse compartilhamento, algumas dificuldades têm de ser superadas, dentre as quais as de ordem técnica, referentes à falta e/ou incompatibilidade de equipamentos ou sistemas; as de natureza cultural, relativas à predisposição, por parte de integrantes de determinadas corporações, a não compartilhar dados e informações de valor, com o propósito de se obter a primazia no desencadeamento de ações futuras; e, por fim, a própria necessidade de compartimentação em função dos riscos de vazamento ou em decorrência da falta de conhecimento e confiança mútua para o compartilhamento seguro de informações.
>
> A integração dos sistemas de inteligência é condição *sine qua non* para que planejadores e decisores obtenham uma consciência situacional mais efetiva, dando-lhes melhores condições para a tomada de decisão, o planejamento e a execução das operações.

A origem identificada dessas desconformidades também é apontada por de Lima[54]:

> A falta de compartilhamento de informações também pode ocorrer por questões de Contrainteligência interna, onde os atores envolvidos demonstram desconfiança quanto a capacidade de manutenção do sigilo de determinado dado por parte de outros órgãos ou agências envolvidas. Por último, existe também a vaidade pessoal, onde os atores envolvidos, por questões anteriores e por descompromisso com o país, colocam situações pessoais e particulares à frente dos interesses nacionais, dificultando, propositalmente ou inconscientemente, o fluxo de informações interagências.

53 DE SOUZA, op. cit., 2018.

54 DE LIMA, Cap Inf Albemar Rodrigues. **O Centro de Coordenação Tático Integrado (CCTI)**: O planejamento de operações especiais em prol da força tática nas atividades de inteligência e operações em Grandes Eventos. Trabalho de Conclusão de Curso (Especialização em Ciências Militares) – Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2017.

Com efeito, a situação denota a linha tênue do equilíbrio na atuação interagências, conforme pronunciado por Amorim[55]:

> Se relações de confiança são requisitos básicos para a interação entre diferentes agências, na comunidade de Inteligência essa necessidade é muito mais pronunciada. Isso porque se trabalha com informações sensíveis das quais a não observância do sigilo acarreta em prejuízos institucionais e em riscos às fontes e a outros ativos próprios de cada serviço de inteligência.

A mesma autora[56] apresenta um exemplo de proposta de solução para a atuação de interagências de forma coesa e coordenada com a indicação do Grupo de Atuação Especial de Combate ao Crime Organizado (GAECO), conduzido pelo Ministério Público, da seguinte forma:

> O GAECO é um exemplo de organização interagências da qual é possível obter paralelos com a realidade da Força Terrestre cuja aplicabilidade poderia gerar melhorias nos processos desenvolvidos em operações como a Ágata. De forma geral, os GAECO se organizam no âmbito estadual, tem como fim o combate a crimes de natureza específica, e são coordenados pelo Ministério Público do respectivo estado.

Contudo, constata-se que os GAECOs constituem, em múltiplas vertentes, organismos apartados da própria estrutura dos ramos do Ministério Público, não raramente desvinculados dos organismos de Inteligência e segurança institucional internos. Ou seja, a solução para o adequado e coerente sistema seria a consolidação das atividades dos GAECOs, no âmbito dos ramos do Ministério Público, em estruturas únicas de Inteligência, Contrainteligência e segurança institucional.

O próprio caso de referência adotado neste artigo, inerente à escravidão contemporânea, bem explicita a limitação da abrangência dos GAECOs e do Grupo Nacional de Combate as Organizações Criminosas (GNCOC), em que praticamente não há participação dos dois principais ramos do Ministério Público de enfrentamento do trabalho em condição análoga à de escravo: o Ministério Público do Trabalho e o Ministério Público Federal.

Em síntese, o equilíbrio entre compartimentação da informação e a necessidade de compartilhamento, assim como a manutenção do sigilo, representa os maiores desafios da Atividade de Inteligência, normalmente colocados como primados éticos[57] da própria comunidade e dos operadores de Inteligência.

5. SITUAÇÃO DE APLICABILIDADE

Embora o recorte realizado busque tão somente descrever um ponto de início para o pensamento da utilização da Inteligência e da Contrainteligência na realização de operações contra a escravidão

55 AMORIM, op. cit., 2012.

56 Ibidem, 2012.

57 CENTRAL INTELLIGENCE AGENCY. **Mission**. Disponível em: <https://www.cia.gov/about-cia/cia-vision-mission-values>. Acesso em: 5 abr. 2019.

contemporânea, convém mencionar uma possibilidade de concretização da sistemática apresentada.

Um dos primeiros pontos a serem considerados no planejamento de uma operação, seja lá qual for a ação, são as informações acerca da ambiência em que será desenvolvida. Tais condições configuram as informações essenciais de Inteligência, conforme descreve o Manual[58] EB70-MC-10.307 do Exército Brasileiro:

> 10.6.5 Os Elementos Essenciais de Inteligência devem ser detalhados, permitindo determinar a melhor forma de conduzir as operações e influenciar a população para aumentar a estabilidade local. A identificação e análise das ameaças, bem como do terreno, do clima, e das considerações civis são essenciais para o correto emprego da tropa.
>
> 10.6.6 A falta de conhecimento sobre a Força Oponente, sobre a política local, os costumes e a cultura, bem como a forma de diferenciar entre a população dos Agentes Perturbadores da Ordem Pública (APOP), muitas vezes leva a ações que podem resultar em situações não intencionais e consequências desvantajosas, tais como atacar alvos inadequados ou ofender ou causar desconfiança entre a população local. Esta falta de conhecimento pode potencialmente ameaçar o cumprimento da missão.

O segundo ponto, conforme acima descrito, é o objeto da operação (ameaça), contemplando as características do alvo ou da situação a ser enfrentada. Todos esses fatores devem compor a Atividade de Inteligência que sustentará o planejamento da operação, bem como as medidas de Contrainteligência necessárias.

A título ilustrativo, poderíamos considerar uma ação com base em denúncia anônima, em determinada área rural, onde houvesse a informação da prática de trabalho escravo para realização de algum tipo de plantação.

Como ponto mínimo, teríamos a necessidade de confirmação da denúncia que, nesse caso, foi confirmada por informações de um bar na cidade, onde o proprietário confirmou as práticas realizadas com eventuais clientes que frequentavam seu estabelecimento.

Confirmado o fato gerador de uma pretensa ação do Estado, ou seja, se há fortes indícios da prática do trabalho em condições análogas à de escravo, poderíamos considerar que há necessidade de uma rápida mobilização e atuação, deflagrando-se a respectiva operação.

Contudo, embora seja prática corrente em muitas ações desencadeadas, a ausência de planejamento coloca em risco todos participantes e o próprio sucesso da atuação.

Uma operação em determinada fazenda denunciada, por exemplo, demanda o levantamento de informações pormenorizadas da atuação, localização, práticas correntes, fontes de cruzamento, credibilidade, pontos de acesso, pontos de fuga, indicativos de segurança, dentre muitos outros.

Quando pensamos em planejamento de uma operação de combate ao trabalho escravo, normalmente os quesitos que surgem em primeiro

58 BRASIL. op. cit., 2016.

plano são relacionados à quantidade de possíveis resgatados, os meios logísticos de atendimento e acolhimento, a identificação de responsáveis e, no máximo, se há segurança armada (sob o prisma da segurança da operação).

Muitas vezes, um simples questionamento pode mudar todo o rumo e estrutura da ação, como, por exemplo, qual o tipo de plantação que é realizada mediante trabalho escravagista. De acordo com a resposta, com a produção do conhecimento a partir da indagação, poderemos ter condições extremamente adversas. Por óbvio, é claro que os requisitos serão diferenciados se a resposta for, por um lado, uma plantação de "moranguinhos", ou, por outro, uma cultura de *Erythroxylum coca*, destinada à produção de cocaína.

Da mesma forma, outras questões aparentemente irrelevantes começam a adquirir representatividade à medida que são inter-relacionadas para a produção do conhecimento que subsidiará a deflagração de uma operação adequadamente planejada. A existência de fertilizantes, agrotóxicos, combustíveis, venenos, pode indicar a possibilidade de um sistema de proteção e destruição de provas, com a utilização desses componentes como meio de fortuna (provocar a intoxicação dos agentes públicos, explosão com lesões e mortes, dentre outros fatores).

A forma de manutenção do vínculo de escravagismo também apresenta especial relevância para o planejamento de uma eventual operação repressiva.

Diversos são os instrumentos de manutenção da pessoa em situação escrava, passando desde a simples supressão de informação dos direitos e deveres decorrentes da relação de trabalho até a restrição da liberdade de locomoção pela violência.

Não raro a verificação de situações de servidão por dívida, de ameaças veladas e explícitas à pessoa escravizada e sua família, o controle da saúde, a dependência de drogas e o círculo de bebidas e prostituição são utilizados como intermediários para manutenção do controle dos trabalhadores. Da mesma forma, a cooptação e a coação de agentes públicos, seja por ameaça ou por corrupção, apresentam-se como fatores adicionais de risco a serem considerados no levantamento de Inteligência e planejamento das operações.

Destaca-se ainda que a questão da violência (leia-se como o aumento da criticidade e gravidade dos fatores de risco operacionais) no âmbito da escravatura se apresenta como fator intrínseco e inerente, tal como descrito por Girardi[59]:

> No mapeamento exploratório dos dados de libertação de trabalhadores escravizados entre 1995 e 2006, foi possível confirmar a relação entre pobreza e suscetibilidade ao aliciamento e entre a prática do trabalho escravo e a violência. Ao estabelecer correlações entre dados do trabalho escravo (condições de vida do trabalhador, suas condições sociais, tipos de atividades econômicas exercidas, violências e

59 GIRARDI, op. cit., 2014.

> assassinatos), detectou-se as principais estruturas do trabalho escravo no Brasil.

Cada um desses fatores de risco impõe aos agentes do Estado uma forma de abordagem e de realização da operação e, consequentemente, das necessidades de segurança institucional[60] a serem providenciadas.

Registre-se que a adoção da Atividade de Inteligência em operações contra a escravidão contemporânea, assim como em qualquer tipo de ação de enfrentamento, não se constitui em uma medida única, mas sim como um ciclo permanente de produção do conhecimento[61], de forma a se compatibilizar com as demandas de mutação[62] da atividade criminosa

6. CONSIDERAÇÕES FINAIS

Sem propor a exaustão da discussão, mas pelo contrário, a simples provocação e sensibilização acerca da imprescindibilidade da Atividade de Inteligência e da utilização da Contrainteligência para subsidiar as ações do Ministério Público, especialmente nas atuações operacionais desenvolvidas, este trabalho buscou apresentar um panorama do sistema de Inteligência e Contrainteligência aplicável ao enfrentamento da escravidão contemporânea, de forma a permitir a visualização de sua aplicação concreta e não meramente acadêmica.

Nesse sentido, convém trazer à conclusão a particularidade inerente ao Ministério Público no ambiente tratado, pois o sistema de poder e cultura atinge as próprias estruturas estatais de controle, como bem explicita Nepomuceno[63]:

> O sucesso dos fazendeiros que se instalaram no estado do Pará, por exemplo, dependia, em grande medida, da sua capacidade de transformar em seus aliados as polícias militar e civil. As milícias privadas dos fazendeiros são, até hoje, frequentemente formadas e mantidas com a participação de policiais. As principais vítimas das milícias são trabalhadores rurais, religiosos, ambientalistas, militantes em defesa dos direitos humanos e dirigentes sindicais do campo que procuram defender os direitos daqueles com baixas rendas e submetidos à exploração das mais diversas ordens.

60 Admite-se o ciclo de inteligência e Contrainteligência como um dos inúmeros processos inerentes à segurança institucional, conforme já reconhecido na formação do Grupo Estrutural dos GAECOs, da seguinte forma: "É composto por integrantes dos Gabinetes de Segurança Institucional (GSI) dos Ministérios Públicos estaduais, que são órgãos de inteligência dos MPs." Disponível em: <https://www.cnpg.org.br/index.php/gncoc-menu/grupo-estrutural>. Acesso em: 5 abr. 2019.

61 No mesmo sentido: "2.2.5 A função de combate Inteligência é muito mais que a simples obtenção de dados e informações. É um processo contínuo que integra a análise da informação com o desenvolvimento das operações, de maneira que se possa visualizar e entender a situação". (BRASIL, Op. cit., 2015).

62 Como registrado por Figueira: "Adicionalmente, os fenômenos mencionados parecem revelar que as estratégias de operação dos grupos móveis precisam de reorientação periódica. A submissão de trabalhadores a condições análogas à escravidão, sendo um crime, corresponde a uma realidade que se esforça por permanecer invisível. Parece importante que a política monitore e planeje ações estratégicas para identificar novos espaços e novas "formas" de trabalho escravo no país". FIGUEIRA, Ricardo Rezende. **Pisando fora da própria sombra:** a escravidão por dívida no Brasil contemporâneo. Rio de Janeiro: Civilização Brasileira, 2004.

63 NEPOMUCENO, Eric. **O massacre - Eldorado dos Carajás:** uma história de impunidade. São Paulo: Editora Planeta Brasil, 2007.

Detentores de surpreendente força política e econômica, os fazendeiros personificam o poder soberano, o que lhes garante impunidade e gera a reincidência no crime de redução de pessoas a condições análogas à escravidão. A vida e os corpos dos trabalhadores tornam-se, portanto, o local, por excelência, da sua decisão soberana. Deixá-los morrer, ordenando sua execução ou retirando-lhes as condições mínimas de sobrevivência (água, comida, alojamento, cuidados médicos) no local de trabalho, tornam-se "práticas corriqueiras" plenamente justificadas pelas atividades produtivas. Além disso, são práticas também viabilizadas pelo processo de desenraizamento dos trabalhadores que, ao desconectá-los de suas referências sociais e morais, contribui para a desvalorização das suas vidas.

Essa relação de poder configura um dos maiores desafios do Ministério Público na atuação de enfrentamento da escravidão contemporânea, como bem relata Figueira[64]:

> Fora das fazendas, a soberania dos fazendeiros é reconhecida pela força política que possuem. Muitos exercem poder e influência em diferentes instâncias da política nacional, seja de forma direta, ocupando efetivamente cargos em Prefeituras, Câmaras Legislativas Municipais, Governos Estaduais e no Congresso Nacional, ou, de forma indireta, por possuir estreitos laços com representantes dos seus interesses nos referidos cargos (OIT, no prelo). Além disso, os fazendeiros podem contar com a conivência da polícia, que pode atuar como parte dos instrumentos de repressão utilizados contra os trabalhadores. Não são poucos os casos em que autoridades locais, ao invés de registrarem denúncias de abusos sofridos por trabalhadores fugitivos, entregam os trabalhadores novamente aos "gatos" que os contrataram.

Nesse ponto, ingressa a atuação do Ministério Público com maior representatividade e força, demandando um extenso trabalho de produção do conhecimento para o processo decisório e medidas específicas de proteção, pois atinge o nó górdio de todo o sistema criminoso. Como bem explicita Neto[65], a adoção de medidas de Inteligência e Contrainteligência passa a ser fundamental para a atuação e própria sobrevivência da instituição:

> É fato que, à medida que o Ministério Público avança no cumprimento de suas funções em direção as classes mais abastadas da sociedade e aos funcionários públicos e políticos mais poderosos, as ameaças sobre a instituição aumentam e os seus membros se veem, cada dia mais, vulneráveis, dependentes de cursos isolados de segurança, de profissionais terceirizados, de órgãos policiais locais (muitas vezes afetados por investigações do próprio membro do Parquet). A própria instituição em si, não raro, torna-se vitima dessas ações, seja por intermédio de desinformações maliciosamente articuladas, seja por sabotagens, cooptações, infiltração de criminosos em seu seio (inclusive por intermédio de contratações de serviços terceirizados sem o devido acompanhamento), entre outras, que, não raro, poderiam ser devidamente evitadas (ou cujos prejuízos poderiam ser minimizados)

64 FIGUEIRA, Ricardo Rezende. **Pisando fora da própria Sombra**. A escravidão por dívida no Brasil contemporâneo. Rio de Janeiro: Civilização Brasileira, 2004.

65 NETO, Wilson Rocha de Almeida. **Inteligência e Contrainteligência no Ministério Público**: Aspectos práticos e teóricos da atividade como instrumento de eficiência no combate ao crime organizado e na defesa dos direitos fundamentais. 1. ed. Belo Horizonte: Dictum, 2009.

> com a realização de uma atividade responsável de Contrainteligência por um pessoal orgânico devidamente treinado.

Diante de tal cenário, conclui o mesmo Procurador da República[66]:

> Com a estruturação de uma unidade de Contrainteligência, o Ministério Público passará a depender cada vez menos de fatores externos para preservar a sua segurança, fazendo com que o membro, os servidores, as áreas, os materiais e as informações sensíveis que detém, não sejam presas fáceis de ações adversas de toda ordem.

Por óbvio, a estruturação de um organismo autônomo de Inteligência e Contrainteligência no Ministério Público não representa isolamento, mas, pelo contrário, deverá ser integrado à comunidade de Inteligência e Contrainteligência com a atuação interagências.

Adota-se a boa prática da formação de uma unidade de Inteligência, composta suscintamente pelas seguintes etapas: estruturação da segurança institucional básica; a formação de procedimentos e canais seguros; a mitigação de ameaças; a estruturação da Contrainteligência; a estruturação da segurança interna da rede de agentes e analistas de Inteligência; a implantação do sistema de Inteligência no âmbito interno; e, por fim, a integração à comunidade de Inteligência. Esta última possibilita a consequente operação interagências, adotando-se, por exemplo, as *Joint Intelligence Preparation of the Operational Environment*[67] da doutrina Norte Americana, com a participação em *Task Forces*[68] – plenamente compatíveis com a abordagem do planejamento de operações com subsídio na Inteligência e na Contrainteligência interagências.

Assim, partindo da configuração do enfrentamento da escravidão contemporânea, foi possível comprovar a importância[69] da Inteligência e da Contrainteligência no planejamento e execução de operações, em especial remetidas à atuação do Ministério Público, tanto na obtenção de resultados mais efetivos quanto na manutenção da segurança institucional[70], além de se identificar a irradiação por toda estrutura organizacional.

Talvez, com a completa e adequada estruturação de um sistema de Inteligência e Contrainteligência, será possível atingir o que Sun Tzu[71] definiu como o ápice de toda sua obra estrategista: "A suprema arte da guerra é derrotar o inimigo sem lutar".

---

66 Ibidem, 2009.

67 US ARMY. **Joint Publication 2-0**: Intelligence. publ. 22 oct. 2013. Disponível em: <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_0.pdf>. Acesso em: 5 abr. 2019.

68 Conceito cunhado pela Marinha Norte Americana (US Navy) e utilizado atualmente nas mais diversas ações governamentais. US NAVY - US NAVAL FORCES CENTRAL COMMAND. **Combined Maritime Forces** - U.S. 5th FLEET. Disponível em: <https://www.cusnc.navy.mil/Task-Forces/>. Acesso em: 5 abr. 2019.

69 Destaca-se a mesma constatação que orientou a mudança de paradigma e estrutura do FBI após os atentados de 11 de setembro de 2001: "*The Bureau's transformation into an intelligence-driven organization has been successful, Pepper explained, "because our leadership understood that the change was necessary and that it was simply the right thing to do to mitigate the threats the country faces.*" FBI. FEDERAL BUREAU OF INVESTIGATION. **Intelligence Analysts**. Part 1: Central to the Mission. Aug 18, 2011. Disponível em: <https://www.fbi.gov/news/stories/intelligence-analysts-central-to-the-mission>. Acesso em: 5 abr. 2019.

70 Destaca-se que a própria criação do GNCOC pelo Conselho Nacional dos Procuradores-Gerais (CNPG) foi motivada por uma questão de segurança institucional: assassinato do Promotor de Justiça de Minas Gerais Francisco José Lins do Rêgo Santos, ocorrido em 25 janeiro de 2002.

71 Op. cit., 2006.

7. REFERÊNCIAS

AMORIM, Maria Alice Barros Martins. **A Problemática da segurança pública na fronteira Brasil e Bolívia com foco no Estado do Mato Grosso**. 2012. Trabalho de Conclusão de Curso (Curso de Altos Estudos de Política e Estratégia) – Escola Superior de Guerra, Rio de Janeiro, RJ, Brasil, 2012.

ANDREUCCI. Ricardo Antonio. **Exploração do trabalho escravo e tráfico de seres humanos, a face desconhecida do crime organizado** In: MESSA, Ana Flávia; CARNEIRO, José Reinaldo Guimarães (coords.) **Crime Organizado**. São Paulo: Saraiva, 2012.

ARAS, Vladimir. **Se ergues da Justiça a clava forte**. Publ. 1 set. 2013. Disponível em: <https://vladimiraras.blog/2013/09/01/se-ergues-da-justica-a-clava-forte/>. Acesso em: 5 abr. 2019.

ARENDT, Hannah. Eichmann em Jerusalém - **Um relato sobre a banalidade do mal.** Tradução de José Rubens Siqueira. São Paulo: Companhia das Letras, 2013.

BRASIL. Comando de Operações Especiais. Exército Brasileiro. Estado-Maior do Exército. **Manual de Operações Especiais** - EB20-MC- 10.212, 2ª ed. Brasília: Comando do Exército, 2014.

_____. _____. **Manual Técnico**: Produção do Conhecimento de Inteligência – EB70-MT- 10.401, 1ª ed. Brasília: Comando do Exército, 2019.

_____. Constituição (1988). **Constituição da República Federativa do Brasil**. Texto constitucional promulgado em 5 de outubro de 1988 com emendas. Brasília: Centro de Documentação e Informação (CEDI), 2019. Disponível em: <http://www2.camara.leg.br/atividade-legislativa/legislacao/Constituicoes_Brasileiras/constituicao1988.html>. Acesso em: 5 abr. 2019.

_____. **Decreto nº 8.793, de 29 de junho de 2016**. Fixa a Política Nacional de Inteligência. Diário Oficial da União de 30 jun. 2016.

_____. Exército. Estado-Maior. **Manual de Campanha - Inteligência** – EB20-MC-10.207. 1ª ed. Brasília: Comando do Exército, 2015.

_____. _____. **Manual de Campanha – Planejamento e Emprego da Inteligência Militar**: EB70-MC-10.307. 1ª ed. Brasília: Comando do Exército, 2016.

_____. Presidência da República. **Plano Nacional para a Erradicação do Trabalho Escravo**. Disponível em <https://www.ilo.org/brasilia/publicacoes/WCMS_227535/lang--pt/index.htm>. Acesso em: 5 abr. 2019.

CASTELLS, Manuel. **A Era da Informação:** economia, sociedade e cultura. v. I: A Sociedade em rede. Tradução de Klauss Brandini Gerhardt e Roneide Venâncio Majer. 2ª ed. São Paulo: Editora Paz e Terra, 2000.

CIA. CENTRAL INTELLIGENCE AGENCY. **Mission**. Disponível em: <https://www.cia.gov/about-cia/cia-vision-mission-values>. Acesso em: 5 abr 2019.

_____. **The Intelligence Cycle.** Disponível em: <https://www.cia.gov/kids-page/6-12th-grade/who-we-are-what-we-do/the-intelligence-cycle.html>. Acesso em: 5 abr. 2019.

CIRILO, Bianca Sant'Anna de Sousa. Resgate policial de reféns: uma forma de espetacularização da vida. **Revista EPOS**. Rio de Janeiro – RJ, Vol.4, nº 2, jul-dez de 2013.

CORTE INTERAMERICANA DE DIREITOS HUMANOS. Caso 12.066 - **Trabalhadores da Fazenda Brasil Verde vs. Brasil**. j. 20 out. 2016. publ. 15 dez. 2016. Disponível em: <http://www.corteidh.or.cr/docs/casos/articulos/seriec_318_por.pdf>. Acesso em: 5 abr. 2019.

COSTA, Patrícia Trindade Maranhão. A construção da masculinidade e a banalidade do mal: outros aspectos do trabalho escravo contemporâneo. **Cad. Pagu**, Campinas, n. 31. Dec. 2008. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0104-83332008000200009&lng=en&nrm=iso>. Acesso em: 5 abr. 2019.

DE LIMA, Cap Inf Albemar Rodrigues. **O Centro de Coordenação Tático Integrado (CCTI):** O planejamento de operações especiais em prol da força tática nas atividades de inteligência e operações em Grandes Eventos. 2017. Trabalho de Conclusão de Curso (Especialização em Ciências Militares) – Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2017.

DE SOUZA, Cel Inf QEMA FABIO NEGRÃO. **O emprego do Exército Brasileiro no combate ao crime organizado: desafios e perspectivas**. 2018. Trabalho de Conclusão de Curso (Especialização em Ciências Militares) – Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2018.

DHS. DEPARTMENT OF HOMELAND SECURITY. Disponível em: <https://www.dhs.gov/>. Acesso em: 5 de abr. 2019.

DINIZ, Fernando. **25 Anos da Operação *Eagle Claw*:** a fracassada tentativa de resgate dos reféns americanos. Iran, 24-25 Abril 1980. publ. 27. Jul. 2005. Disponível em: <http://www.defesanet.com.br/sof/noticia/254/25-Anos-da-Operacao-Eagle-Claw/>. Acesso em: 5 abr. 2019.

DRUCKER, Peter. **Administrando em tempos de grandes mudanças.** São Paulo: Thomson Pioneira, 2003.

FARAH, Camel André de Godoy. A atividade de Inteligência de Defesa em operações de Garantia da Lei e da Ordem (GLO) In: DE PAULA, Giovani (Org.). **Sociedade, Segurança e Cidadania**: Paz social. Livro 1. Palhoça: UNISUL, 2017.

FBI. FEDERAL BUREAU OF INVESTIGATION. **Intelligence Analysts. Part 1:** Central to the Mission. Aug 18, 2011. Disponível em: <https://www.fbi.gov/

news/stories/intelligence-analysts-central-to-the-mission>. Acesso em: 5 abr. 2019.

FIGUEIRA, Ricardo Rezende. **Pisando fora da própria sombra:** a escravidão por dívida no Brasil contemporâneo. Rio de Janeiro: Civilização Brasileira, 2004.

FREYRE, Gilberto. **Casa Grande & Senzala**. São Paulo: Global Editora, 2006.

GIRARDI, Eduardo Paulon, *et. al*. Mapeamento do trabalho escravo contemporâneo no Brasil: dinâmicas recentes. Espaço e Economia - **Revista Brasileira de Geografia Econômica**, 2014, Ano II, Número 4.

GLOBO. G1. **PM simula sequestro a ônibus BRT como treino para as Olimpíadas no Rio**. Disponível em: <http://g1.globo.com/rio-de-janeiro/noticia/2015/02/pm-simula-sequestro-onibus-brt-como-treino-para-olimpiadas-no-rio.html>. Acesso em: 5 abr. 2019.

KELSEN, Hans. **Teoria pura do Direito**. Tradução de João Baptista Machado. 7 ed. São Paulo: Martins Fontes, 2006.

LEAL, Victor Nunes. **Coronelismo, enxada e voto**. São Paulo: Companhia das Letras, 2012.

MINISTÉRIO DO MEIO AMBIENTE. Assessoria de Comunicação Social. **Taxa de Desmatamento na Amazônia Legal**. publ. em 28 nov. 2018. Disponível em: <http://redd.mma.gov.br/pt/component/content/article?id=1018>. Acesso em: 5 abr. 2019

MINISTÉRIO PÚBLICO FEDERAL. Assessoria de Comunicação. **Fada Madrinha**: MPF, PF e MPT deflagram operação contra tráfico internacional de transexuais. Disponível em: <http://www.mpf.mp.br/sp/sala-de-imprensa/noticias-sp/fada-madrinha-mpf-pf-e-mpt-deflagram-operacao-contra-esquema-de-trafico-de-pessoas-transexuais>. publ. 9 ago. 2018. Acesso em: 5 abr. 2019.

NEPOMUCENO, Eric. **O massacre - Eldorado dos Carajás:** uma história de impunidade. São Paulo: Editora Planeta Brasil, 2007.

NETO, Wilson Rocha de Almeida. **Inteligência e contra-inteligência no Ministério Público:** Aspectos práticos e teóricos da atividade como instrumento de eficiência no combate ao crime organizado e na defesa dos direitos fundamentais. 1. ed. Belo Horizonte: Dictum, 2009.

OIT. ORGANIZAÇÃO INTERNACIONAL DO TRABALHO. Escritório no Brasil. **As boas práticas da inspeção do trabalho no Brasil:** a erradicação do trabalho análogo ao de escravo. Brasília: OIT, 2010.

PACHECO, Denilson Feitoza. Atividade de Inteligência no Ministério Público. In: BRANDÃO, Priscila Carlos; CEPIK, Marco (Org.). **Inteligência de**

segurança pública: teoria e prática no controle da criminalidade. 1ª ed. Niterói: Impetus, 2013.

REPORTER BRASIL. Org. **Agronegócio é "lavanderia" do crime organizado, diz juiz**. Disponível em: <https://reporterbrasil.org.br/2008/01/agronegocio-e-lavanderia-do-crime-organizado-diz-juiz/>. publ. em 8 abr. 2008. Acesso em: 5 abr. 2019.

SARMENTO, Daniel; SOUZA NETO, Daniel Pereira de. **Direito Constitucional:** Teoria, história e métodos de trabalho. 2ª ed. Belo Horizonte: Fórum, 2017.

SOUZA, Kel Lucio Nascimento de. Os riscos da atividade policial. **Revista CEJ** - Centro de Estudos Jurídicos, Ano XXI, n. 73. Brasília: Conselho da Justiça Federal, set./dez. 2017.

TZU, Sun. **A Arte da Guerra**. Tradução de Sueli Barros Cassal. Porto Alegre: L&PM, 2006.

US ARMY. **Joint Publication 2-0:** Intelligence. publ. 22 oct. 2013. Disponível em: <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_0.pdf>. Acesso em: 5 abr. 2019.

US NAVY - US NAVAL FORCES CENTRAL COMMAND. **Combined Maritime Forces - U.S. 5th FLEET**. Disponível em: <https://www.cusnc.navy.mil/Task-Forces/>. Acesso em: 5 abr. 2019.

OS DESAFIOS E OPORTUNIDADES PARA A ATIVIDADE DE CONTRAINTELIGÊNCIA NA ERA DO CONHECIMENTO[1]

Major Marcelo Neival Hillesheim de Assumpção[2]

Major Gustavo Monteiro Muniz Costa[3]

SUMÁRIO: 1. Introdução. 2. As Características da Era do Conhecimento. 3. Os Impactos e os Desafios que a Era do Conhecimento traz à Contrainteligência. 4. Oportunidades para a Contrainteligência na Era do Conhecimento e as Quatro Premissas Gerais e Direcionadoras. 5. Conclusão. 6. Referências.

RESUMO: O momento histórico da humanidade em que vivemos, conhecido como a Era do Conhecimento, tem trazido profundas e céleres alterações em todas as atividades desempenhadas no mundo, bem como renovado o conteúdo do saber humano em todos os campos. A velocidade na transmissão das informações; a conexão em rede de toda a humanidade por meio da internet; a proliferação das mídias sociais *onlines*, com a consequente alteração nas relações interpessoais e a crescente dependência dos meios tecnológicos para o dia a dia das pessoas são alguns dos fenômenos atuais que caracterizam a Era do Conhecimento. Dentro desse cenário, o presente trabalho realizou uma pesquisa qualitativa, exploratória e bibliográfica – quanto à abordagem, objetivos e procedimentos, respectivamente – com o objetivo de analisar os desafios e oportunidades para a atividade de Contrainteligência dentro dessa nova Era. O resultado foi a identificação de diversos óbices, os quais colocam à prova justamente a atividade que tem entre suas incumbências a proteção da informação. No entanto, o trabalho também elenca oportunidades inerentes à nova Era, bem como identificou quatro premissas gerais e direcionadoras para a Contrainteligência nos dias atuais. Entre as oportunidades, destacam-se, entre outras, as novas ferramentas para as medidas ativas de contraterrorismo, comprovando que, nesse ramo, a Era do Conhecimento agregou

1 Trabalho de Conclusão de Curso apresentado à Escola de Inteligência Militar do Exército, como requisito para a obtenção do Grau de Pós-graduação *Lato Sensu* de Especialização em Análise de Inteligência Militar. Especialização em Análise de Inteligência Militar. Orientador: TC LEANDRO MARONÊS PEÇANHA.

2 Oficial de Infantaria do Exército Brasileiro. Academia Militar das Agulhas Negras. Pós-graduado em Ciências Militares. Escola de Comando e Estado-Maior do Exército.

3 Oficial de Cavalaria do Exército Brasileiro. Academia Militar das Agulhas Negras. Pós-graduado em Ciências Militares. Escola de Comando e Estado-Maior do Exército.

mais vantagens que vicissitudes. Diante desse cenário, as premissas elencadas demonstram a necessidade de constante atualização da legislação e regulamentos, o risco das informações sem prévia análise, a dependência do controle sobre os Meios de Tecnologia da Informação (MTI) e a importância do profissional que opera esses meios. Assim, o tema elencado para o presente estudo, Os Desafios e Oportunidades para a Contrainteligência na Era do Conhecimento, reflete a importância atribuída ao desempenho de tal atividade em um mundo cada dia mais globalizado, informatizado, instável e dinâmico.

PALAVRAS-CHAVE: Inteligência. Contrainteligência. Era do Conhecimento. Mídias sociais. Desafios.

1. INTRODUÇÃO

Ocorrências significativas na História Geral delimitaram os cinco períodos nos quais a história da humanidade é dividida, a saber: Pré-História, Idade Antiga, Idade Média, Idade Moderna e Idade Contemporânea. Tais períodos, classificados para fins didáticos e por convenção, revelam panoramas da existência humana com características próprias e com foco principal na perspectiva de intelectuais europeus.

O período em que vivemos, a Idade Contemporânea, iniciou-se em 1789, ano da Revolução Francesa, e estende-se até a atualidade. Esse período, em particular, revela uma fase tão significativa de mudanças e evoluções na humanidade que já poderia ter sofrido nova divisão e categorização.

A delimitação de tais períodos é algo relativamente recente, surgida somente após a Idade Média. É possível que, face às profundas mudanças geopolíticas, sociais e comportamentais ocorridas nos últimos anos, historiadores e especialistas daqui a alguns anos estabeleçam o fim da Era Contemporânea e definam que atualmente vivemos sob a Era do Conhecimento.

O marco que separará essas Eras caberá aos futuros estudiosos, podendo definir a Queda do Muro de Berlim, o fim da União Soviética ou mesmo o ataque às Torres Gêmeas como a data limítrofe, face às profundas e irreversíveis mudanças ocorridas na geopolítica mundial devido a esses acontecimentos.

As alterações nos relacionamentos entre os entes privados e estatais no mundo, devido ao uso da rede mundial de computadores, a internet, e aos meios de tecnologia da informação (MTI), causaram uma mudança comportamental na humanidade capaz de influenciar o futuro das nações, bem como determinar o resultado de eleições, como ocorreu recentemente nos Estados Unidos da América com a eleição de Donald Trump.

O exemplo da recente eleição presidencial norte-americana demonstrou que o presidente eleito e sua adversária, Hillary Clinton, utilizaram em larga escala meios de comunicação atrelados à internet para sua campanha. No entanto, da mesma forma, foram vítimas desses.

Hillary foi acusada e investigada pelo *Federal Bureau Investigation* (FBI), a polícia federal norte-americana, por comprometer a segurança do país ao usar e-mails particulares, para enviar mensagens oficiais enquanto ocupava o cargo de Secretária de Estado de Barack Obama. Partidários de ambos postavam incessantemente em redes sociais fotos e notícias distorcidas ridicularizando, ofendendo ou mesmo manipulando informações contra os adversários. Já sobre Trump, pairam acusações de ter sido beneficiado por ações de *hackers* russos que o teriam favorecido na disputa do pleito, algo que, mesmo que se comprove ser inverídico, permanecerá desgastando a figura do presidente eleito (GUILHERME, 2016).

As vulnerabilidades surgidas com a Era do Conhecimento para a proteção aos ativos das nações ficaram muito bem evidenciadas com os milhares de documentos confidenciais norte-americanos vazados num sítio na internet. Edward Snowden, ajudado por um ex-militar, Bradley Manning, entregou milhares de documentos diplomáticos e confidenciais a Julian Assange, fundador da organização chamada Wikileaks, que os divulgou seletivamente na internet. Comprovações de grampos telefônicos contra inúmeros líderes mundiais e até, recentemente, acusações de que a *Central Intelligence Agency* (CIA) é capaz de monitorar os telefones de qualquer cidadão no mundo, demonstraram que nem mesmo a maior potência global é capaz de possuir sistemas de segurança orgânica que impeçam o vazamento de informações e comprometam os seus ativos (BATISTA, 2017).

Por outro lado, foram justamente os meios de tecnologia da informação empregados no contraterrorismo, atividade da segurança ativa da Contrainteligência, que identificaram e localizaram o terrorista mais procurado do mundo, Osama Bin Laden. Após um dos membros da Al-Qaeda ter dito breves palavras suspeitas, por poucos segundos, usando um celular descartável e num local remoto do Paquistão, é que foi possível iniciar o processo de localização daquele líder terrorista (OWEN, 2012).

O fato é que a revolução tecnológica, iniciada há algumas décadas, aliada à propagação em escala global das informações e dos "saberes" já gerou um consenso mundial em chamar o período em que vivemos de Era do Conhecimento. Como dificilmente se conseguirá, em um mundo globalizado, consenso no meio acadêmico acerca do fato histórico que marca o início desse período, é bem provável que continuemos "situados" na Idade Contemporânea por um bom tempo.

Independentemente da denominação histórica e acadêmica que se queira atribuir a este período em que vivemos, é preciso reconhecer que a atividade de Inteligência Militar, tanto no ramo da Inteligência quanto no ramo da Contrainteligência, tem passado por constantes desafios frente ao mundo da Era do Conhecimento. Desafios estes que têm colocado à prova justamente a atividade cujo fulcro é a gestão do conhecimento, além de sua proteção.

Definiu-se, como objetivo geral dessa pesquisa, analisar o que é a Era do Conhecimento, quais suas características principais e como elas afetam a atividade de Contrainteligência. Com base nisso, traçaram-se objetivos específicos que eram a identificação dos desafios, impactos, oportunidades

dessa Era e, se possível, a realização da integração dos conhecimentos obtidos, apresentando como contribuição premissas direcionadoras para esse ramo da Contrainteligência.

Dessa forma, realizou-se uma pesquisa de abordagem qualitativa, exploratória quanto aos objetivos e utilizando-se de procedimentos bibliográficos, apoiando-se em literaturas atuais, fatos recentes e análises de especialistas acerca de um tema pouco estudado e consolidado. Os conhecimentos obtidos nas diversas fontes consultadas foram então integrados às experiências profissionais dos pesquisadores do presente estudo, resultando em um trabalho que reflete a importância atribuída ao desempenho da atividade de Contrainteligência, em um mundo no qual a proteção das informações parece se tornar a cada dia mais difícil.

Diante desse cenário, o tema apresentado, **Os Desafios e Oportunidades para a Contrainteligência na Era do Conhecimento**, foi dividido em cinco capítulos, com a introdução, conclusão e mais três capítulos inerentes ao desenvolvimento. No capítulo dois, o leitor será apresentado a algumas das características principais da Era do Conhecimento. No terceiro capítulo estão identificados alguns dos impactos e desafios dessa Era. Já o capítulo quatro integra os conhecimentos apresentados anteriormente, sugerindo quatro premissas gerais e direcionadores para a Contrainteligência e elencando algumas das novas oportunidades a esse ramo da Inteligência. Por fim, a conclusão mostra as limitações desse trabalho e as necessidades de novos estudos sobre o tema.

2. AS CARACTERÍSTICAS DA ERA DO CONHECIMENTO

Dentre as 100 maiores invenções da humanidade elencadas no livro homônimo (PHILBIN, 2015), mais de 60% delas foram criadas entre o fim da segunda metade do século XIX e o início da segunda metade do século XX. O Museu de Ciência de Londres elegeu em 2009 as dez maiores invenções da humanidade, dentre as quais todas ocorreram nesse mesmo período, com exceção do telégrafo e da máquina a vapor (BBC, 2009). Antes de 1970, o homem já havia criado a televisão, o satélite, o telefone, o rádio, o avião, a bomba atômica, a energia nuclear, a penicilina, o cloro, o computador e a *Arpanet,* predecessora da internet. Daí em diante, a tecnologia aprimorou as criações já existentes, como os carros autônomos, o ônibus espacial, submarinos de propulsão nuclear, os celulares, os computadores portáteis, os smartphones e a própria internet.

A corrida armamentista ocorrida no período da Guerra Fria entre os EUA e a ex-União das Repúblicas Socialistas Soviéticas (URSS) impulsionou o desenvolvimento científico-tecnológico mundial a partir do investimento de governos e empresas por eles contratadas, com destaque para a corrida aeroespacial e o Programa Guerra nas Estrelas do governo de Ronald Reagan nos EUA (LOBO, 2015). No entanto, foi o acesso da população à tecnologia dos telefones portáteis, bem como o uso da internet por pessoas comuns para a troca de e-mails, pesquisas, transações financeiras e demais

utilidades até então limitadas pela baixa capacidade de transmissão de dados, que resultaram nas mudanças mais significativas de nossa Era.

Os principais meios de comunicação hoje são os meios de tecnologia da informação (MTI), conectados à internet e, muitas vezes, integrados em uma rede social *online*, as quais permitem que a ligação entre usuários e telespectadores ocorra sem o intermédio dos grupos de mídia. Seja por meio de aplicativos ou programas criados para interação entre usuários, como *Instagram*, *Twitter*, *WhatsApp*, *Telegram* e *Facebook,* seja por sítios da *web* disponíveis para postagens de vídeos, opiniões, artigos, imagens e qualquer outra forma de comunicação por pessoas comuns, como *YouTube*, *blogs* e *Daily Motion.* Praticamente não existe mais sociedade alheia ou que não esteja sob as influências da Era do Conhecimento.

O resultado dessa mudança foi a transformação da sociedade de um estado simples, controlável, previsível, lento, estável e baseado em instituições sólidas para um ambiente complexo, fora de controle, imprevisível, rápido, instável e pautado sobre o indivíduo, capaz de mudar rumos inteiros de nações por meio de um ato único, isolado e independente (GUIMARÃES, 2016).

Esse dinamismo e rapidez com que as informações são transmitidas entre uma fonte e milhões de destinatários possibilitaram que notícias, propagandas, difamações e quaisquer outras formas de informações possam trafegar por intermédio dos meios de comunicação sem nenhum filtro ou confirmação prévia, causando efeitos que muitas vezes não podem ser mitigados ou solucionados oportunamente.

O dicionário Oxford elegeu o termo "pós-verdade" como a palavra do ano de 2016, definindo-o como "um adjetivo que se relaciona ou denota circunstâncias nas quais fatos objetivos têm menos influência em moldar a opinião pública do que apelos à emoção e às crenças pessoais". (OXFORD, 2016).

Esse neologismo denota a importância em bem se compreender e estar preparado para os desafios da Era do Conhecimento, em que a verdade pode facilmente ser substituída por distorções e mentiras que serão capazes de moldar, alterar ou mesmo influenciar comportamentos com uma velocidade inédita, principalmente aquelas feitas sob o prisma das Operações Psicológicas.

Nas eleições presidenciais brasileiras em 2014 diversos boatos, mentiras e inverdades circularam nas redes sociais, fora do alcance da fiscalização do Tribunal Superior Eleitoral (TSE) e sempre à frente da capacidade de reação dos alvos elencados. Porém, muitas dessas "pós-verdades" não eram realizadas por pessoas comuns, mas sim por especialistas em propaganda política detentores de conhecimento e ferramentas afins àquelas utilizadas nas Operações Psicológicas.

No entanto, constatou-se que, comparando-se com as eleições presidenciais norte-americanas em 2016, o ocorrido no Brasil dois anos antes era apenas uma fase embrionária desse processo de difamação, manipulação de opiniões, disseminação do medo e controle das massas.

Ambos os principais candidatos àquela eleição, Donald Trump e Hillary Clinton, utilizaram-se largamente de um meio gratuito, incontrolável, disseminador e, muitas vezes anônimo, para atacar seu adversário: as redes sociais *online*.

Outro fato contundente da Era do Conhecimento é a ligação direta entre a notícia e o usuário, sem necessariamente haver um órgão de imprensa interligando essas duas pontas. Enquanto, há pouco tempo, era absolutamente necessário um fotógrafo, um jornalista, uma câmera ou os próprios meios de imprensa para divulgar uma notícia, como jornais impressos, locutores de rádio ou um cinegrafista, atualmente, a vítima de um bombardeio na Síria consegue transmitir em tempo real suas agruras a milhões de expectadores, uma refugiada afegã consegue prestar seu depoimento pessoal e sem censura em uma rede social virtual que será lida por pessoas nos cinco continentes.

Ao mesmo tempo, transações financeiras bilionárias ocorrem entre hemisférios sem que os envolvidos sequer se vejam. Forças Armadas em todo o mundo desenvolvem e aperfeiçoam suas defesas cibernéticas e, principalmente, suas capacidades de realizarem ataques nessa nova dimensão do combate.

Hoje, um bombardeio aéreo sobre uma usina elétrica pode ser substituído por invasões à rede que distribui a energia aos usuários, economizando meios, vidas e ainda assim atingindo os mesmos fins militares definidos pelo atacante.

Porém, um fato peculiar ao período de transição entre as Eras está ocorrendo: grande parte dos líderes e pessoas com poder de decisão, seja na esfera governamental, civil ou militar, possui mais de quarenta anos de idade. Assim, são pessoas que, em sua maioria, tiveram suas formações acadêmicas ocorridas ainda sob as características da Era Contemporânea, quando havia maior previsibilidade e controle das informações. Já os mais jovens, que estão familiarizados com as novas tecnologias desde a infância, não possuem a maturidade e experiência profissional para adequar o uso dessas novas capacidades às realidades comportamentais da humanidade.

Exemplo dessa imaturidade dos jovens é o grande número de comprometimento de informações e exposições indevidas a que eles mesmos se submetem, variando desde divulgações de conteúdo íntimo privado até o vazamento de informações sigilosas de governos. Esses atos comprometem tanto a própria honra e dignidade pessoal, com reflexos que podem perdurar a vida inteira para a família, como colocam em risco a segurança nacional, quando, movidos por idealismos temporais e sem reflexão das consequências, organizam grupos especializados em atacar governos, como o grupo *Anonymus*.

Quanto à falta de adaptação dos decisores sobre as atuais ferramentas dessa Era, por exemplo, é fato que mensagens trocadas em grupos de *WhatsApp* chegam aos chefes nos diversos escalões sem o prévio filtro e análise dos órgãos assessores. Essas informações não trabalhadas e sem uma adequada técnica de análise prévia acabam por influenciar decisões.

Durante as Olimpíadas do Rio de Janeiro em 2016, inúmeras denúncias anônimas espalhavam-se em grupos daquele aplicativo em uma progressão geométrica, anunciando mochilas suspeitas e ou outras formas de ameaças à população, todas infundadas, mas que nos primeiros dias resultaram no acionamento de equipes diversas para checar os locais *in loco*, antes mesmo da análise dos dados difundidos. Obviamente, diante da incapacidade de cobrir as inúmeras denúncias com as equipes de operações, constatou-se que as informações difundidas em grupos de rede social deveriam, antes de qualquer coisa, ser previamente analisadas antes da tomada de decisão dos chefes.

A grande maioria dos países no mundo sequer tem leis adaptadas às dificuldades e peculiaridades dessa Era. Crimes cibernéticos, ofensas trocadas por meio de redes sociais, vazamento de conteúdos pessoais, propagação de mentiras e difamações, clonagem de dados financeiros ou comprometimento de investigações policiais e processos judiciais ainda não recebem o tratamento civil e criminal específico que merecem, sendo enquadrados em tipificações penais mais genéricas, seja pela incapacidade de os órgãos investigativos atenderem à infinita e crescente demanda dessa sorte, seja pelo próprio vácuo legal existente.

Portanto, entender a Era do Conhecimento, esse "ser vivo" altamente mutável e incontrolável, buscar compreender suas características, desafios, ameaças e, ao mesmo tempo, identificar as oportunidades que ora se apresentam é uma obrigação de todos aqueles que têm a responsabilidade de liderar e conduzir suas instituições.

3. OS IMPACTOS E OS DESAFIOS QUE A ERA DO CONHECIMENTO TRAZ À CONTRAINTELIGÊNCIA

Diante do que foi abordado até este ponto no presente estudo, já é possível perceber que a Era do Conhecimento enseja desafios imensuráveis para todas as atividades humanas, em particular, para as ligadas à segurança das instituições e à proteção do conhecimento. Fica a indagação: como resguardar as instituições e proteger a informação em um contexto global em que a transparência e a instantaneidade na transmissão de dados parecem ser as palavras de ordem e encontram um ambiente virtual totalmente voltado para isso? Como tal contexto tem refletido na atividade de Contrainteligência?

Nos últimos anos, foi recorrente o caso de terroristas e combatentes de países invadidos por exércitos estrangeiros postarem vídeos em *sites*, com o fito de realizar Operações Psicológicas contra os países invasores.

Durante a campanha dos Estados Unidos da América (EUA) no Iraque (2003 a 2011), um *sniper,* que foi apelidado de Juba, deixou dezenas de soldados estadunidenses mortos ou feridos após disparos precisos que eram filmados por outro insurgente que, logo após, postava os vídeos dessas ações na internet utilizando, principalmente, o site *YouTube* (CARROLL, 2005).

Tais vídeos tiveram um alcance mundial, influenciando a opinião pública dos EUA e do mundo, em prol do fim da guerra. Além disso, abalou o moral das tropas norte-americanas de uma forma que a Contrainteligência daquele país, com suas Contra-Ações Psicológicas, não puderam evitar (CARROLL, 2005).

Da mesma forma, os vídeos postados na internet pelo grupo terrorista Estado Islâmico do Iraque e do Levante (ISIS) mostrando decapitações de soldados e de jornalistas de várias nacionalidades nos últimos anos têm causado grande comoção junto à opinião pública mundial, propagando sua causa, causando terror em seus inimigos e levando empresas como *Facebook* e *Twitter* a reverem seus procedimentos de controle sobre o conteúdo publicado em seus sites (ALMEIDA, 2015).

Para complicar ainda mais a situação, apoiadores do ISIS criaram o *Khelafabook,* mídia social com uma interface muito semelhante à do *Facebook* e disponível em vários idiomas, inclusive em português, e que tem tido um alcance global, haja vista o número de curtidas em suas publicações (ALMEIDA, 2015).

A internet vem sendo usada como o principal vetor para o recrutamento de novos terroristas para o ISIS, que tem sido bem-sucedido em angariar simpatizantes de todas as idades, nacionalidades e gêneros ao redor do mundo, com seus vídeos caracterizados por uma produção visual impactante e com grande apelo emocional, dignos de grandes produtores midiáticos.

Segundo Costa (2016, p. 2):

> Hoje, a atuação do Estado Islâmico passa por práticas como os *twitter bombs* (militantes utilizam as *hashtags* mais populares do *Twitter* nas postagens relacionadas ao EI, aumentando a visibilidade de seus conteúdos) e chega aos vídeos criados por seu braço midiático, estruturado em torno de dezenas de produtoras audiovisuais coordenadas principalmente pela *Al Hayat Media Center*, divisão de mídia responsável pela marcação da temática, estética, duração e cronograma de distribuição dessas produções.

Tais recursos tecnológicos têm colocado à disposição de grupos terroristas ferramentas de propaganda, recrutamento e Operações Psicológicas que dispensam o emprego de recursos vultosos e não expõem a grandes riscos os homens que desempenham tais tarefas, além de dificultar sobremaneira as medidas de Contraterrorismo e Contra-Ações Psicológicas.

A propaganda de guerra realizada por intermédio de panfletos jogados de aeronaves em territórios inimigos e que custaram a vida de muitos pilotos parece ter ficado em um passado longínquo na história da humanidade. A propaganda na Era do Conhecimento pode ser feita de um café na cidade de Paris ou de uma *lanhouse* na periferia de um país asiático.

Ainda com relação à propaganda terrorista por meio da internet, Woloszyn (2013, p. 118) pontua que:

> [...] a própria Al Qaeda já se manifestava, em 2003, depois da invasão do Iraque: "Recomendamos urgentemente que qualquer muçulmano

> ou outros profissionais disseminem notícias e informações sobre a Jihad por meio de listas de e-mails, grupos de discussão e em seus próprios sites na internet para difundir nossa causa e desencorajar infiéis para a luta contra nossos irmãos".

A internet tem sido utilizada também para habilitar pessoas interessadas em empreender atentados terroristas, instruindo-as na fabricação de bombas, execução de sequestros, destruição de prédios, utilização de armamentos, falsificação de documentos, entre outros ilícitos. Na atualidade, existem cerca de seis mil *sites* ligados a grupos terroristas internacionais que cumprem esse papel (WOLOSZYN, 2013).

A dimensão virtual ensejou o surgimento dos "profissionais do ciberespaço", os chamados *hackers.* Tais pessoas se valem de grande conhecimento cibernético e, na maioria dos casos, do anonimato, para realizar toda sorte de ações, algumas nefastas e ilegais, no ambiente das redes. Com relação ao ciberespaço, Filho (2014, p. 54) cita que:

> [...] é dominado por diferentes agentes (*hackers, Insiders* etc), com ou sem patrocínio estatal, possuidores de notáveis conhecimentos técnicos, e engajados em diferentes atividades, tais como: espionagem industrial, propaganda, vigilância, censura e sabotagem.

A atuação dos *hackers,* há alguns anos, deixou de ser exclusivamente empreendida com fins privados e passou a ser conduzida por nações com finalidades diversas, desde ações de espionagem e de sabotagem até ataques diretos que passaram a ser qualificados como ataques cibernéticos, a mais nova forma de agressão a ser explorada na disputa entre entes estatais (CLARKE, 2015).

Para exemplificar, podemos citar o caso Guerra do Golfo (1990 a 1991), em que os EUA empregaram um vírus com a finalidade de inutilizar a defesa antiaérea do Iraque. Outro caso foi o ataque realizado pela Rússia contra a Estônia, em 2007, com a finalidade de causar o caos no país, paralisando bancos, empresas, repartições públicas e provedores de internet (FILHO, 2014).

Nesse contexto, Woloszyn (2013, p. 111) destaca:

> Podemos afirmar que estamos diante de nova forma de guerra assimétrica, sem exércitos, tanques e aviões, mas com igual letalidade, na qual hackers e crackers, solitários ou a serviço de estados, exercem, ao mesmo tempo, a função de general e soldado e se utilizam de características especiais oportunizadas por tais tecnologias, como rapidez, instantaneidade na difusão de vírus ou informações, abrangência, invisibilidade, baixo custo, difícil detecção e falta de regulamentação na maioria dos países e organismos internacionais, incluindo a ONU.

Outro fenômeno típico de nossa Era e que desafia frontalmente os prognósticos dos analistas de Inteligência comprometendo a estabilidade das nações e suas instituições, tendo em vista a tempestividade com que ocorre e as suas dimensões, é a mobilização das massas em prol de uma causa, por intermédio das redes sociais. Um exemplo disso foi a Primavera Árabe, uma escalada de revoltas populares em países do mundo árabe que desestabilizou a região, no ano de 2011. O movimento teve início na Tunísia

e rapidamente se alastrou por outras nações, depondo os representantes da "velha ordem", ditadores que mantinham seus regimes mediante opressão, mas que de certa forma, traziam estabilidade à região e possuíam uma política externa com certo grau de previsibilidade (CANEPA, 2012).

As massas, coordenadas e motivadas pelo ambiente cibernético, superaram o medo de se manifestar, em países cuja cultura política oprime as manifestações populares, em particular, de caráter reivindicatório, e foram capazes de derrubar governos e mudar o rumo de suas nações. Castells (2013, p. 7) define:

> Da segurança do ciberespaço, pessoas de todas as idades e condições passaram a ocupar o espaço público, num encontro às cegas entre si e com o destino que desejavam forjar, ao reivindicar seu direito de fazer história – sua história –, numa manifestação da autoconsciência que sempre caracterizou os grandes movimentos sociais.

As manifestações populares mobilizadas pelas redes sociais também encontraram palco no Brasil, no ano de 2013, quando milhões de pessoas em várias cidades do país realizaram protestos, inicialmente, contra o aumento no preço das passagens e, em um segundo momento, por uma grande variedade de temas como os gastos públicos em eventos esportivos internacionais, a má qualidade dos serviços públicos e contra a corrupção política.

As dimensões dessas manifestações e o caráter violento de algumas delas pegaram autoridades, órgãos de segurança pública, analistas políticos e os serviços de Inteligência totalmente desprevenidos, impedindo a tomada das ações adequadas com a antecipação necessária.

Outro fenômeno de massas que teve origem no ambiente das redes sociais é o que ficou conhecido como "Pós-verdade", já citado no capítulo anterior. Este fenômeno certamente não é novo, entretanto, ao ocorrer no âmbito das mídias sociais, tomou uma dimensão muito maior. Ainda mais em um ambiente onde a profusão de informações em um ritmo acelerado oferece poucas condições de as pessoas exercitarem seu pensamento crítico em prol de um juízo mais apropriado acerca de algum assunto. Desta forma, qualquer informação com conteúdo negativo acerca de uma instituição macula sua imagem com enorme repercussão, ainda que não expresse a verdade e seja posteriormente rebatida.

Trazendo mais complexidade ainda ao cenário de incertezas da Era do Conhecimento, observa-se que não somente a efetividade da Segurança Ativa tem sido desafiada. As falhas na Segurança Orgânica também têm, por vezes, tomado um vulto de dimensões globais. Foi o caso das fotos postadas por soldados norte-americanos, em que os militares aparecem torturando presos iraquianos na prisão de *Abu Ghraib*, no Iraque, demonstrando uma grave falha dos Recursos Humanos estadunidenses no desempenho de suas funções. Tais imagens comprometeram seriamente a imagem do Exército dos EUA e reforçaram o discurso contra a campanha militar e sua legitimidade (HERSH, 2005).

A postagem de fotos, imagens e gravações de áudio tem sido recorrente nos últimos anos e tem servido tanto para denunciar esquemas

de fraude, crimes e corrupções como para comprometer a imagem de instituições sérias e que são alicerçadas na credibilidade depositada nelas pela sociedade como, por exemplo, as Forças Armadas. Tais fenômenos evidenciam a já citada quebra do monopólio da cobertura jornalística.

Em suma, diante do que foi apresentado até o momento, percebe-se que a Era do Conhecimento trouxe uma evolução tecnológica sem precedentes para a humanidade, proporcionando rapidez no tráfego das informações e conectando as pessoas entre si como nunca antes visto. Entretanto, a proteção do conhecimento e das instituições não acompanhou tal evolução, de tal forma que a eficiência da Contrainteligência se encontra ameaçada, o que enseja uma revisão de suas técnicas, táticas e procedimentos.

4. OPORTUNIDADES PARA A CONTRAINTELIGÊNCIA NA ERA DO CONHECIMENTO E AS QUATRO PREMISSAS GERAIS E DIRECIONADORAS

Apesar dos inúmeros desafios e impactos que essa nova Era trouxe à proteção da informação e ao trabalho da Contrainteligência, é fundamental identificar as oportunidades inerentes. O ser humano normalmente entende como uma ameaça aquilo que é novo e incompreensível. Porém, as ferramentas criadas nesse período têm sido utilizadas como as principais armas no combate ao terrorismo, uma das maiores ameaças mundiais dos dias de hoje.

Muito embora a Era do Conhecimento tenha facilitado a cooptação, recrutamento e preparação dos terroristas, esse advento facilitou as atividades-meio e intermediárias. Ou seja, enquanto um grupo criminoso especializado em roubar contas bancárias pela internet não precisa se expor pessoalmente, um terrorista não conseguirá empreender um ataque utilizando unicamente os MTI e a internet. No máximo poderá usar equipamentos adaptados como drones ou celulares para acionamentos remotos. Mas, em todos os casos, ele será obrigado a cruzar alfândegas, manipular explosivos, adquirir armas, expor-se pessoalmente diante dos alvos que elencou ou mesmo recorrer à internet para se preparar para o ato, facilitando seu monitoramento.

Existe ainda o conceito de ciberterrorismo. Recentemente, o Brasil definiu o conceito de terrorismo, conforme tipificado no artigo 2º da Lei nº 13.260, de 16 de março de 2016 (BRASIL, 2016, p. 1):

> O terrorismo consiste na prática por um ou mais indivíduos dos atos previstos neste artigo, por razões de xenofobia, discriminação ou preconceito de raça, cor, etnia e religião, quando cometidos com a finalidade de provocar terror social ou generalizado, expondo a perigo pessoa, patrimônio, a paz pública ou a incolumidade pública.

Até os dias de hoje, não foi comprovada nenhuma ação cibernética que tenha resultado no terror social ou generalizado. Todas as ações empreendidas até o presente se enquadram como cibersabotagem ou ciberativismo, neologismos que definem ações deliberadas que resultaram

em prejuízos financeiros, interrupções de serviços públicos ou simples divulgação de material propagandístico de grupos anarquistas.

Após o atentado às Torres Gêmeas em Nova Iorque, em 11 de setembro de 2001, o governo norte-americano criou a Comissão Nacional sobre Ataque aos Estados Unidos, também conhecida como Comissão do 11 de Setembro. O relatório final dessa comissão identificou falhas na Contrainteligência da CIA e do FBI, resultando numa revisão da estrutura de Inteligência e na criação do cargo de Diretor Nacional de Inteligência, que coordena e integra o trabalho de dezessete agências de Inteligência daquele país e se reporta diretamente ao presidente (WASHINGTON POST, 2010).

A sinergia do trabalho das agências norte-americanas, mas, principalmente, o uso das novas tecnologias para monitoramento, identificação e eliminação das ameaças resultaram que o país maior alvo do terrorismo mundial, com uma população de mais de trezentos milhões de habitantes e com mais de onze milhões de imigrantes ilegais, que comprova a permeabilidade de suas fronteiras, foi alvo de somente um atentado terrorista vultoso em seu solo desde o ataque às Torres Gêmeas.

Em 2013, dois jovens chechenos residentes nos EUA detonaram duas bombas na maratona de Boston, matando três pessoas e ferindo mais de duzentas. Em menos de 72 horas, um dos autores já havia sido morto, e o outro, capturado. Os demais ataques foram pontuais e não envolveram emprego de explosivos ou produtos químicos e biológicos, somente armas de fogo, semelhantes a outros crimes perpetrados por atiradores nos EUA com motivações diferentes do terrorismo.

Em 2015, um casal que jurou fidelidade ao Estado Islâmico (EI) atacou funcionários de saúde em San Bernardino, na Califórnia. No mesmo ano, um americano de ascendência afegã matou dezenas de pessoas em uma boate gay em Orlando, na Flórida. Nesse caso, a polícia não conseguiu confirmar se a motivação era terrorista ou problemas psicológicos, pois suspeitou-se que o atirador era gay e tinha medo de assumir sua condição (FOLHA, 2015).

Nesse contexto, todos os ataques terroristas cometidos nos EUA foram empreendidos por americanos ou estrangeiros residentes no país, sendo somente no da maratona de Boston onde houve o uso de explosivo improvisado, confirmando a eficiência das novas tecnologias no controle de suas fronteiras e no monitoramento dos materiais e insumos que podem ser utilizados na fabricação de explosivos e produtos químicos ou biológicos com fins terroristas.

Nesse mesmo período, o governo norte-americano destituiu o Taleban do poder no Afeganistão, desarticulou a Al Qaeda, eliminou inúmeros líderes terroristas, inclusive Osama Bin Laden, e mantém um monitoramento constante das ameaças terroristas no mundo, como se exemplifica com os ataques aéreos de mísseis contra líderes e posições do Estado Islâmico no Oriente Médio.

Já na Europa, onde está a maioria dos países mais ricos do mundo, que, consequentemente, possuem os recursos necessários à aquisição, desenvolvimento e emprego das novas tecnologias, também se verifica a vantagem das medidas contraterroristas sobre as ameaças. As vulnerabilidades europeias são imensamente maiores que as norte-americanas, graças à permeabilidade de suas fronteiras, à proximidade geográfica de "países-refúgios" de terroristas e à sua própria configuração populacional com milhões de muçulmanos, o que facilita o homizio dos radicais islâmicos. No entanto, muito embora um ataque na Europa tenha um grande impacto midiático e o fato de que esses países também se configuram como alvos dos terroristas, os números de atentados e de vítimas europeias representam menos de 1% do total mundial.

Em 2016, o continente foi palco de quatro ataques, todos com grande repercussão mundial. Eles ocorreram em Bruxelas, Berlim, Nice e Rouen, na França, com um total de 134 (cento e trinta e quatro) vítimas fatais (WIKIPEDIA, 2017). Já até maio de 2017, foram dois em Paris, um em Londres e um em Estocolmo, com um total de 11 (onze) mortos (SUNDAY EXPRESS, 2017). De setembro de 2001 a 30 de abril de 2017, a Europa e a Rússia, somadas, sofreram 293 (duzentos e noventa e três) ataques praticados por muçulmanos (THE RELIGION OF PEACE, 2017). A fonte registra que a grande maioria foram ações isoladas, inclusive contabilizando crimes comuns perpetrados por muçulmanos, enquanto houve em nível mundial mais de trinta mil ataques no mesmo período. Somente em 2016, o sítio *The Religion of Peace* contabilizou 2.479 (dois mil quatrocentos e setenta e nove) ataques praticados por islâmicos, com mais de vinte e um mil mortos no mundo.

No Brasil, a Operação Hashtag desarticulou um grupo que planejava realizar ataques terroristas durante as Olimpíadas do Rio em 2016. Alguns brasileiros, utilizando-se das novas tecnologias, juraram lealdade ao EI e iniciaram os planejamentos, para realizarem ataques pontuais e indiscriminados durante os jogos olímpicos. E foi justamente a ação dos órgãos de Inteligência brasileiros no monitoramento do uso da internet pelos suspeitos que possibilitou a prisão desses elementos antes mesmo que executassem um atentado.

Portanto, infere-se que o trabalho silente e eficaz realizado pelas agências de Contrainteligência no uso das novas tecnologias para a segurança ativa é fundamental para sobrepujar a larga escalada do terrorismo mundial.

Ainda sobre as oportunidades, a dinâmica na análise de informações e os novos sistemas de obtenção de dados potencializaram as capacidades dos profissionais encarregados das medidas de Contraespionagem e Contra-Ações do público interno. Pessoas que, há pouco tempo, poderiam roubar informações ou mesmo cometer crimes utilizando-se de seus cargos estão sob um maior risco de serem detectadas antes que causem prejuízos institucionais, graças às novas tecnologias de varredura de ambiente, bloqueadores de celulares, interferidores de gravação e toda sorte de medidas eletrônicas para proteção das informações.

No campo da segurança orgânica, a segurança das áreas a instalações ganhou um importante advento no controle e monitoramento do acesso de pessoas graças às novas tecnologias. Atualmente, programas de computadores aliados às imagens geradas por câmeras de monitoramento possuem 97% de eficácia na identificação de um rosto, ao passo que há seis anos esse índice de acerto era de 27%. Já a capacidade de monitoramento de uma pessoa frente a um monitor é reduzida a menos de 50% após 18 minutos, chegando a quase zero após uma hora olhando para as telas do sistema (VILICIC, 2017). Portanto, *softwares* modernos de monitoramento instalados em alfândegas, aeroportos, áreas de acesso restrito ou mesmo nas ruas potencializam a capacidade de detecção e neutralização das ameaças.

Assim, da análise dos inúmeros desafios e impactos apresentados no capítulo anterior e as oportunidades acima elencadas, verifica-se que as instituições que possuem ativos de interesse sempre se constituirão em alvos e devem estar perfeitamente adaptas à nova Era em que vivem.

Nesse interim, é fundamental identificar, de forma macro e sem descer ao nível tático de procedimentos pontuais, quais são as principais premissas que devem nortear as ações de Contrainteligência na Era do Conhecimento. E, como proposta deste presente trabalho, identificaram-se quatro premissas gerais e direcionadoras:

Primeira premissa: diversas medidas de Contrainteligência atuais tornar-se-ão obsoletas em pouco tempo. Isso significa que, assim como testes antidopings e sistemas antivírus de computadores estão sempre reagindo às ameaças depois que surgem, as medidas de Contrainteligência voltadas à segurança orgânica ou à segurança ativa estarão constantemente sendo alvos de técnicas e táticas que as sobreponham. Portanto, manuais, regulamentos, regras de uso, recomendações profissionais e toda sorte de procedimento interno de uma instituição deverão estar sob constante revisão, auditoria e aprimoramento.

Segunda premissa: a Contrainteligência nunca será capaz de analisar os dados na mesma velocidade com que estes são propagados. Enquanto uma simples foto pode chegar instantaneamente a milhares de pessoas, analisá-la, confirmar sua veracidade e transformar esse dado em um conhecimento sempre demandará um tempo bastante superior ao que se levou para que fosse difundida. Assim, muito embora o decisor por vezes tenha necessidade de reagir ou decidir baseado em uma informação não confirmada, os chefes devem estar cientes de que decisões baseadas em informações sem prévia análise colocam em risco a própria organização.

Terceira premissa: a segurança da informação depende diretamente do controle sobre os meios de tecnologia da informação, já que são a ferramenta indispensável ao encaminhamento de um dado. Uma vez enviado um arquivo, foto, vídeo ou qualquer outra informação, perde-se o controle sobre eles, pois não existe criptografia ou qualquer ferramenta que garanta sua perfeita inviolabilidade. Portanto, qualquer forma de controle e proteção sobre a informação deve ocorrer sobre os MTI e o seu acesso à internet. Proibição de celulares, bloqueadores de sinal telefônico,

uso de computadores fora da rede e da internet e proibição de filmagem e fotografias são apenas alguns exemplos do controle sobre a ferramenta para a proteção dos ativos.

Quarta premissa: os encarregados das medidas de Contrainteligência devem ser afeitos às novas tecnologias ou assessorados por especialistas capazes de usar esses meios com a mesma desenvoltura que aqueles que se dedicam ao seu mau uso. Relegar esta atividade apenas aos métodos empregados na Era Contemporânea seria semelhante à tentativa dos alemães de deterem com metralhadoras os blindados ingleses na Batalha de *Somme*, durante a 1ª Guerra Mundial. Portanto, o emprego de especialistas em MTI na Contrainteligência e o constante acompanhamento desses profissionais que trabalham em outras áreas são fundamentais para a segurança dos ativos de uma organização.

Portanto, da análise das diversas fontes bibliográficas, que permitiram apresentar nos capítulos anteriores as características, os desafios e os impactos da Era do Conhecimento, com as oportunidades elencadas nessa parte do trabalho, comprovaram que a metodologia empregada foi adequada aos objetivos propostos, que conduziu a uma integração de todos os conhecimentos sob as quatro premissas gerais e direcionadoras.

5. CONCLUSÃO

É inquestionável que a velocidade e a profundidade das mudanças comportamentais, sociais, econômicas e científico-tecnológicas ocorridas nos últimos vinte anos ensejarão mais mudanças de extremo significado e impacto em todas as atividades desenvolvidas pelo ser humano, além de abrirem espaço para uma mudança pelo meio acadêmico na classificação da Era em que vivemos.

Conforme apresentado, a Era do Conhecimento não se caracteriza pela invenção de novas tecnologias, mas por um aprimoramento substancial dos meios de comunicação, apoiados sobre uma capacidade de transmissão instantânea de dados e financiado principalmente pelo mercado consumidor, não mais pelos governos.

Um futuro breve nos reserva novas tecnologias ainda mais impactantes. Especialistas da área de tecnologia afirmam que em dez anos não usaremos mais *smartphones*, que óculos de realidade virtual mudarão a forma como interagimos com o mundo e que a velocidade de transmissão de dados dos domicílios saltará de megabytes por segundo para gigabytes. O ciberterrorismo e outros crimes utilizando a internet se tornarão mais comuns. Pessoas mal-intencionadas possivelmente poderão assumir o controle de trens, metrôs, carros e caminhões autônomos e toda sorte de meios que possam ser empregados para causar morte, pânico e terror.

Atualmente, a gestão e a proteção do conhecimento, o ativo mais precioso de nossa Era, se tornará o grande desafio da humanidade. O sucesso desta empreitada, em particular da Contrainteligência, será um dos

aspectos que determinará o papel de cada uma das nações neste mundo, cada dia mais conectado.

Esse presente estudo integrou conhecimentos diversos, reunindo os desafios, impactos e oportunidades para o ramo da Contrainteligência e integrou-os sob a forma de quatro premissas gerais e direcionadoras: leis, manuais e regulamentos deverão estar sob constante revisão, auditoria e aprimoramento; chefes devem estar cientes que decisões baseadas em informações não analisadas colocam em risco a própria organização; todo controle e proteção da informação deve ocorrer sobre os MTI; e a atividade de Contrainteligência não pode prescindir de especialistas em MTI, bem como esses profissionais de outras áreas devem estar sob constante acompanhamento.

A atuação da Inteligência, em seus dois ramos, dentro do ciberespaço, agora é uma imposição, tendo em vista ser este o ambiente onde a maioria das informações trafega, e o ciberespaço se tornou a quinta dimensão do combate, ao lado das dimensões: terrestre, aquática, aérea e espectral magnética. Desta forma, as Forças Armadas de todo mundo devem se adequar a esta realidade sabendo que a dimensão cibernética não pode ser encarada como paralela às demais citadas, mas como uma dimensão que permeia e condiciona todas as outras. Assim, é mister novos estudos para auxiliar em uma adequação técnica e tática das tropas militares, não apenas na atividade de Inteligência, mas em todas as funções de combate.

O presente estudo optou por utilizar somente conhecimentos disponíveis em fontes abertas, como forma de ampliar a sua possibilidade de leitura. Isso, no entanto, também se configura em uma limitação, pois não utilizou dados de conhecimento classificados ou sob restrição de acesso, o que restringe a sua abrangência metodológica quanto ao procedimento, bibliográfico. Outras limitações presentes neste trabalho dizem respeito ao nível que se decidiu focar a integração dos conhecimentos, com premissas gerais e direcionadoras, ou seja, sem pontuar ações, procedimentos e normas que devem ser estabelecidas de acordo com o cliente ou instituição objeto de análise.

Portanto, é difícil imaginar um país que pretenda desempenhar um papel de protagonista no cenário mundial e que não esteja focado em se adequar à realidade da Era do Conhecimento. Da mesma forma, é difícil imaginar Forças Armadas que pretendam ser a garantia desse mesmo país e que não estejam preparadas para fazer um bom uso das oportunidades que a Era do Conhecimento traz à gestão da informação ou que não saibam proteger adequadamente seus ativos.

6. REFERÊNCIAS

ALMEIDA, Reginaldo Rodrigues de. **Estado Islâmico:** à distância de um clique. JANUS 2015-2016-Integração regional e multilateralismo, 2016.

BATISTA, Henrique Gomes. **CIA controla celulares, PC e até smart TV.** O Globo, Rio de Janeiro, 07 de março de 2017. Caderno Mundo.

BBC NETWORK**. Um siglo de exhibir inventos**. Redacción BBC Mundo. Londres, Inglaterra. Disponível em: <http://www.bbc.com/mundo/ciencia_tecnologia/2009/06/090610 _museo_ciencias_rec.shtml>. Acesso em: 21 maio 2017.

BRASIL. **Lei nº 13.260**, de 16 de março de 2016.

CANEPA, Beatriz. **Mundo árabe em mutação.** – Atualidades – São Paulo: Abril, 1º semestre de 2012.

CARROLL, Rory. The Guardian. **Elusive sniper saps US morale in Baghdad**, 2005. Disponível em: <https://www.theguardian.com/world/2005/aug/05/iraq.usa>.

CASTELLS, Manuel. **Redes de indignação e esperança:** movimentos sociais na era da internet. Jorge Zahar Editor Ltda, 2013.

CLARKE, Richard A.; KNAKE, Robert K. **Guerra Cibernética:** a próxima ameaça à segurança e o que fazer a respeito. Rio de Janeiro, RJ, 2015.

COSTA, Ana Carolina. **Propaganda do terror:** A Relação Entre a Produção Audiovisual do Estado Islâmico e a Experiência Visual do First Person Shooter. Congresso Internacional Comunicação e Consumo. 2016

FILHO, Oscar Medeiros; NETO Walfredo Bento Ferreira; GONZALES Selma Lúcia de Moura. **Segurança e defesa cibernética:** da fronteira física aos muros virtuais. Recife: UFPE, 2014.

FOLHA DE SÃO PAULO. **Motivos de atirador para matar em boate gay nos EUA se confundem**. Jornal Folha de São Paulo, São Paulo 2016. Disponível em: <http://www1.folha.uol.com.br/mundo/2016/06/1782214-motivos-de-atirador-para-atacar-boate-gay-em-orlando-se-confundem.shtml>. Acesso em: 28 maio 2017.

GUILHERME, Paulo. **Hackers russos ajudaram Trump a ser eleito nos EUA**, **diz CIA**. Tecmundo, 2016. Disponível em: <https:/tecmundo.com.br/amp/ataque-hacker/112637-hackers-russos-ajudaram-Trump-eleito-eua.htm>. Acesso em: 7 maio 2012.

GUIMARÃES, Ricardo. **Thymus-Natura:** Contexto de Mundo. Vídeo (11min03s). YouTube, publicado em 14 de junho de 2016. Disponível em: <https://www.youtube.com/watch?v=NHqV5YIvA2A&list=>. Acesso em: 1º maio 2017.

HERSH, Seymour M.; Peter FRIEDMAN. **Chain of command.** Harmondsworth: Penguin, 2005.

LEIGH, Davis. **Wikileaks:** a Guerra de Julian Assange contra os Segredos de Estado / David Leigh, Luke Harding; tradução Ana Resende. Campinas/SP: Verus, 2011.

LESACA, Javier. **Fight against ISIS reveals power of social media.** Brookings Institution, 2015.

LÓPEZ, José Maria Álvarez-Pallete. A morte do telefone. **Revista VEJA**, São Paulo, edição 2529, ano 50, nº 19, 10 de maio de 2017.

LOBO, Carlos Eduardo Riberi. O Programa "Guerra nas Estrelas" e o Governo Reagan. **Revista de História, Política e Cultura**, São Paulo, v.1, n.1, Julho/2015.

NEVES, Eduardo Borba; DOMINGUES, Clayton Amaral. **Manual de metodologia da pesquisa científica.** Rio de janeiro,/RJ, 2007.

OWEN, Mark. **Não há dia fácil:** um líder da tropa de elite americana conta como mataram Osama Bin Laden. São Paulo: Editora Paralela, 2012.

OXFORD, Dictionaries. **The Word of the Year 2016 is...** English Oxford Living Dictionaries. Disponível em: <https://en.oxforddictionaries.com/word-of-the-year/word-of-the-year-2016>. Acesso em: 1º maio 2017.

PHILBIN, Tom. **As 100 Maiores Invenções da História. Uma classificação cronológica.** – 1 Ed – Algés, Portugal. DIFEL. 2015.

SUNDAY EXPRESS. **Terror Attack Timeline**: 2017. Londres, Inglaterra [2017]. Disponível em: <http://www.express.co.uk/news/world/693421/Terror-attacks-timeline-France-Brussels-Europe-ISIS-killings-Germany-dates-terrorism>. Acesso em: 7 maio 2017.

THE RELIGION OF PEACE. **List of Islamic Terror:** 2016. Disponível em: <https://www.thereligionofpeace.com/attacks/attacks.aspx?Yr=2016>. Acesso em: 7 maio 2017.

VILICIC, Felipe. Ela já está entre nós. **Revista VEJA**, São Paulo, edição 2520, ano 50, nº 10, 08 de março de 2017.

WOLOSZYN, André Luís. **Ameaças e desafios à segurança humana no séc. XXI:** de gangues, narcotráfico, bioterrorismo, ataques cibernéticos às armas de destruição em massa / André Luís Woloszyn. 2 Ed. Rio de Janeiro: Biblioteca do Exército; Salto (SP): Schoba, 2013.

WASHINGTON POST. **Top Secret America.** Washington, Estados Unidos da América: *Washington Post Journal*, [2010]. Disponível em: <http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/>. Acesso em: 1º maio 2017.

WIKIPEDIA. **Terrorism in Europe.** Wikipedia Group, [2017]. Disponível em: <https://en.wikipedia.org/wiki/Terrorism_in_Europe>. Acesso em: 7 maio 2017.

A LEGISLAÇÃO CONTRATERRORISTA DO BRASIL E SEUS LIMITES PARA A ATIVIDADE DE PREVENÇÃO: o papel da Atividade de Inteligência

Roberto Ferreira dos Santos[1]

SUMÁRIO: 1. Considerações iniciais. 2. O desafio da definição de terrorismo. 3. O terrorismo como crime. 4. O terrorismo como um fenômeno. 5. A estruturação da prevenção do terrorismo. 6. Os instrumentos para a prevenção do terrorismo. 7. Considerações finais. 8. Referências.

RESUMO: O Congresso Nacional aprovou, em 16 de março de 2016, a Lei nº 13.260, que regulamenta o crime de terrorismo e reformula o conceito de organização terrorista. A Lei nº 13.260/2016 não versou sobre aspectos importantes do enfrentamento do terrorismo e abordou somente uma parte do fenômeno. Utilizar-se da política criminal para prevenir o terrorismo é um passo necessário, mas é somente um passo. Existe uma abrangência do fenômeno que ultrapassa a esfera penal. O fenômeno do terrorismo envolve aspectos sociais, políticos e psicológicos. O arcabouço legal brasileiro define um sistema de Inteligência que possui um órgão central – a ABIN, que pode fazer uso de técnicas e meios sigilosos para atuar na prevenção e no combate ao terrorismo. Para contribuir com o enfrentamento do terrorismo no mundo e prevenir e combater seu desenvolvimento no Brasil, o Estado brasileiro deve fazer opções quanto à estruturação do contraterrorismo no Brasil e a criação ou regulação de instrumentos que aumentem a efetividade das ações de forma a torná-las compatíveis com a dimensão do fenômeno. Este trabalho destaca e analisa algumas características da legislação contraterrorista do Brasil e discute seus limites para as atividades de prevenção do terrorismo no Brasil.

1. CONSIDERAÇÕES INICIAIS

O fenômeno do terrorismo internacional é algo novo e estranho na cultura política do Brasil. A legislação pátria se ateve, por muito tempo, ao repúdio abstrato e à penalização por condutas periféricas. Após os atentados de 11 de setembro de 2001, houve um aumento das pressões internacionais,

1 Oficial de inteligência da Agência Brasileira de Inteligência (ABIN).

inclusive sobre o Brasil, para a adoção de medidas mais concretas para o enfrentamento do terrorismo.

O Conselho de Segurança das Nações Unidas reafirmou, por meio da Resolução 1373, de 28 de setembro de 2001, que qualquer ato de terrorismo internacional constitui uma ameaça à paz e à segurança internacional. Entre as decisões da Resolução, estão que todos os Estados devem prevenir e suprimir o financiamento de atos terroristas, devem criminalizar o financiamento do terrorismo e se abster de qualquer forma de apoio ativo ou passivo a pessoas envolvidas em atos terroristas.

O Grupo de Ação Financeira Internacional (GAFI) emite recomendações para o combate à lavagem de dinheiro e ao financiamento do terrorismo. O GAFI é um organismo intergovernamental criado em 1989, no âmbito da Organização para a Cooperação e Desenvolvimento Econômico (OCDE), e tem por objetivo conceber e promover, quer em nível nacional, quer em nível internacional, estratégias contra a lavagem de dinheiro e o financiamento do terrorismo. O não cumprimento das recomendações do GAFI poderia levar à inclusão do Brasil em uma lista que indicaria "alto risco" nas transações financeiras do país.

O aumento dos compromissos internacionais firmados pelo governo brasileiro principalmente a partir do posicionamento mais rigoroso adotado pelo Conselho de Segurança da Organização das Nações Unidas (ONU), de natureza imperativa, e das recomendações do GAFI, associado ao aumento da percepção da importância do tema pela comunidade política na proximidade com a realização dos Jogos Olímpicos Rio 2016, levou o Congresso Nacional a aprovar uma lei contraterrorista. A Lei nº 13.260, de 16 de março de 2016, regulamenta o crime de terrorismo, trata de disposições investigatórias e processuais e reformula o conceito de organização terrorista.

A Lei nº 13.260/2016 não pode ser considerada de forma isolada na legislação aplicável à prevenção do terrorismo no Brasil. Outras leis, como a nº 12.850/2013 (Lei de Organizações criminosas), a Lei nº 7.960/1989 (Prisão Temporária), a Lei nº 9.296/1996 (Lei de interceptações telefônicas), a Lei nº 9.883/1999, o Decreto nº 8.793/16 (Política Nacional de Inteligência) e outros dispositivos legais, compõem a legislação aplicável de alguma forma aos órgãos que atuam no enfrentamento do terrorismo no Brasil.

A identificação das características da legislação aplicável à atividade de prevenção do terrorismo, a sua comparação com as características do fenômeno do terrorismo internacional e a consequente necessidade de atuação dos órgãos brasileiros no enfrentamento tornam possível compreender as adequações, inadequações e reflexos da legislação para a atividade de prevenção do terrorismo.

A Lei nº 13.260/2016 não versou sobre aspectos importantes do enfrentamento do terrorismo. Os estudos sobre a Lei e a legislação correlata têm se concentrado no debate sobre o direito penal e a política criminal brasileira e destacam uma preocupação mais orientada para repressão do terrorismo. Esse trabalho problematiza a adequação da legislação brasileira para o suporte às ações de enfrentamento do terrorismo que sejam

anteriores ao crime ou que ultrapassem a esfera penal. Com isso, volta o olhar para o aspecto da prevenção do terrorismo.

O objetivo deste trabalho é analisar algumas características da legislação contraterrorista do Brasil, discutir seus limites para as atividades de prevenção e avaliar o papel da inteligência na prevenção do terrorismo no País. Para tanto, é necessário identificar e sistematizar as lacunas e limitações da lei e fundamentar conceitualmente, doutrinariamente e com evidências práticas as possibilidades de criação de novos instrumentos para operacionalizar as ações de prevenção.

Este artigo está dividido em sete partes. A primeira parte apresenta algumas considerações iniciais sobre a questão do terrorismo e das limitações da legislação sobre o tema. A segunda parte discute sobre o desafio da definição do terrorismo. Com base nesses desafios, é feita uma análise do terrorismo como um crime, na terceira parte. A quarta parte busca expandir o entendimento do terrorismo para além do tipo penal em um debate sobre o terrorismo como um fenômeno. Com uma visão mais ampla do terrorismo, a quinta parte – estruturação da prevenção do terrorismo – aborda aspectos estruturais e organizacionais do contraterrorismo no Brasil. A sexta parte discute os instrumentos para a prevenção do terrorismo, voltados para o aumento da eficácia das ações contraterroristas com base nas características do fenômeno e na atuação dos órgãos de prevenção. A sétima parte apresenta algumas considerações finais sobre a legislação contraterrorista do Brasil e a atividade de prevenção.

O resultado deste trabalho colaborará para aumentar a compreensão sobre o papel dos órgãos do Estado na prevenção do terrorismo e sobre os consequentes instrumentos que aumentam a efetividade desses órgãos no cumprimento de suas missões institucionais. Desse modo, como consequência para a aplicabilidade prática deste estudo, serão destacados pontos de debates para eventuais alterações legislativas que contribuam para maior efetividade das ações dos órgãos que atuam na prevenção do terrorismo.

2. O DESAFIO DA DEFINIÇÃO DO TERRORISMO

As tentativas de se obter consenso sobre terrorismo resultam em uma séria redução de complexidade e na convergência de questões de poder que estão presentes em qualquer definição de terrorismo (SPAAIJ, 2012). Segundo Schmid (SCHMID, p. 380), o termo terrorismo é usado inadvertidamente para um alcance muito grande de manifestações, o que nos faz questionar se ele é um conceito unitário. Terrorismo é um construto social. Não está dado no mundo real. É uma interpretação de eventos e suas causas presumidas (TUK A, 2008, p. 491).

O *National Consortium for the Study of Terrorism and Responses for Terrorism* (START), um centro de estudos financiado pelo Departamento de Segurança Interna (*Departament of Homeland Security – DHS*, em inglês) **gerencia o *Global Terrorism Database*** (GTD), um banco de dados aberto

incluindo informações sobre eventos terroristas no mundo, desde 1970. O START, desde 2007, coleta dados com a seguinte definição de terrorismo:

> [...] um ato intencional de violência ou ameaça de violência por um ator não estatal" que atenda a pelo menos dois dos três critérios:
>
> 1. O ato violento foi perpetrado com objetivo político, econômico, religioso ou social;
>
> 2. O ato violento incluiu evidências de intenção de coagir, intimidar ou enviar uma mensagem para uma audiência (ou audiências) além das vítimas imediatas; e
>
> 3. O ato violento foi realizado contra os preceitos do Direito Internacional Humanitário (DIH). (*Global Terrorism Database* [*homepage na internet*]).

O terrorismo, no cenário internacional, apresenta-se como um fenômeno amplo, com causas de cunho social, político e moral. A maneira pela qual os países tratam o fenômeno considera as suas relações internacionais, a amplitude internacional da questão e as realidades internas de cada país em termos de sociedade e de Estado. Apesar da dificuldade de se definir o fenômeno precisamente, existem pontos de convergência no repúdio aos comportamentos ligados ao terrorismo.

A Resolução nº 2253 de 2015, adotada pelo Conselho de Segurança das Nações Unidas no seu 7587º Encontro, em 17de dezembro de 2015, reafirma que o terrorismo, em todas as suas formas e manifestações, constitui uma das ameaças mais sérias à paz e à segurança e que quaisquer atos de terrorismo são criminosos e injustificáveis, independentemente das suas motivações, de quando, onde ou quem quer que tenha cometido, e reitera a condenação inequívoca do Estado Islâmico (ISIL), Al Qaeda e indivíduos associados, grupos, apoiadores e entidades pelos continuados e múltiplos atos terroristas criminosos que objetivaram causar a morte de civis inocentes e outras vítimas, destruir propriedade e ampla corrosão da estabilidade.

A Resolução A/70/L.55, contendo a proposta de resolução submetida pelo presidente da Assembleia-Geral da ONU com a revisão da Estratégia Global de Contraterrorismo das Nações Unidas, propõe a renovação do compromisso de fortalecimento da cooperação internacional para prevenir e combater o terrorismo em todas as suas formas de manifestação. O documento propõe, ainda, a reafirmação que qualquer ato de terrorismo seja crime injustificável, independentemente da sua motivação.

O Brasil acompanha o repúdio ao terrorismo de uma das maneiras mais elevadas possíveis, ao prever na Constituição Federal, no artigo 4º, que elenca os princípios pelos quais o Brasil rege-se, nas suas relações internacionais, o Repúdio ao terrorismo e ao racismo. A Constituição não somente repudia o fenômeno do terrorismo como prevê a criminalização de condutas. O artigo 5º, inc. XLIII, prevê que a lei considerará, dentre os crimes inafiançáveis e insuscetíveis de graça ou anistia, o terrorismo, por eles respondendo os mandantes, os executores e os que, podendo evitá-los, se omitirem.

3. O TERRORISMO COMO UM CRIME

Para regulamentar o disposto no inciso XLIII do artigo 5º da Constituição Federal, foi promulgada a Lei nº 13.260, de 16 de março de 2016. A lei trata do crime de terrorismo e das disposições investigatórias e processuais, e reformula o conceito de organização terrorista. A Lei, em seu artigo 2º, define em que consiste o terrorismo:

> Art. 2º O terrorismo consiste na prática por um ou mais indivíduos dos atos previstos neste artigo, por razões de xenofobia, discriminação ou preconceito de raça, cor, etnia e religião, quando cometidos com a finalidade de provocar terror social ou generalizado, expondo a perigo pessoa, patrimônio, a paz pública ou a incolumidade pública.

A lei tipifica condutas e prevê penas de restrição de liberdade para os crimes cometidos além de definir quais são os atos de terrorismo:

> § 1º São atos de terrorismo:
>
> I - usar ou ameaçar usar, transportar, guardar, portar ou trazer consigo explosivos, gases tóxicos, venenos, conteúdos biológicos, químicos, nucleares ou outros meios capazes de causar danos ou promover destruição em massa;
>
> II - (VETADO);
>
> III - (VETADO);
>
> IV - sabotar o funcionamento ou apoderar-se, com violência, grave ameaça a pessoa ou servindo-se de mecanismos cibernéticos, do controle total ou parcial, ainda que de modo temporário, de meio de comunicação ou de transporte, de portos, aeroportos, estações ferroviárias ou rodoviárias, hospitais, casas de saúde, escolas, estádios esportivos, instalações públicas ou locais onde funcionem serviços públicos essenciais, instalações de geração ou transmissão de energia, instalações militares, instalações de exploração, refino e processamento de petróleo e gás e instituições bancárias e sua rede de atendimento;
>
> V - atentar contra a vida ou a integridade física de pessoa.

A política criminal, exposta na Lei nº 13.260/2016, adotou claramente a estratégia de criminalizar algumas condutas relacionadas a um conceito escolhido de terrorismo. A lei apresenta um caráter repressivo e punitivo das condutas. Segundo a teoria relativa, finalista, utilitária ou da prevenção, a pena tem um fim prático e imediato de prevenção geral ou especial do crime (CAPEZ, 2008, p. 359). Sob o aspecto da prevenção especial, a pena impediria o criminoso de voltar a delinquir por meio da readaptação e segregação social. A prevenção geral é representada pela intimidação dirigida ao ambiente social. As pessoas não delinquem porque têm medo de receber punição.

A preocupação com a prevenção do terrorismo na Lei nº 13.260/16 se restringe ao aspecto preventivo da pena, na esperança de que a pena concretizada fortaleça o poder intimidativo estatal, representando alerta a toda a sociedade. Pela natureza do fenômeno do terrorismo, muitas vezes resultado de um processo de radicalização que passa pela ressignificação de valores morais e de remoção de limites psicológicos e sociais que coibiriam

a ação contra a integridade física das pessoas, o efeito preventivo geral da sanção penal teria impacto muito reduzido ou quase nulo.

Além disso, muitos casos de radicalização de indivíduos que resultaram em ações violentas aconteceram em ambiente prisional, uma vez que condenados recebem material de orientação espiritual com ideologia radical, por meio de doutrinadores com ideias radicais, o que comprometeria o aspecto da prevenção especial da pena.

O fenômeno do terrorismo é mais amplo do que o previsto na Lei nº 13.260/16. A Lei não engloba o fenômeno do terrorismo. Tipifica condutas, diferencia um tipo penal de outro para haver a penalização adequada e a individualização adequada das condutas. Entretanto, a extensão do fenômeno é maior do que o previsto na lei penal.

Um dos princípios do direito penal derivado da dignidade humana é o princípio da alteridade ou transcendentalidade. O fato típico pressupõe um comportamento que transcenda a esfera individual do autor e seja capaz de atingir o interesse do outro (altero) (CAPEZ, 2008, p. 13). É preciso que haja lesividade para legitimar a intervenção penal.

O fenômeno do terrorismo transcende a esfera da conduta puramente interna que merece intervenção penal somente quando afeta terceiros. O Estado necessita intervir no fenômeno muito antes da ação ser externada. O processo de deterioração das relações sociais e da corrosão das instituições políticas e da ressignificação de elementos morais para a execução de uma ação violenta necessita de monitoramento e de intervenção do Estado em fases muito anteriores à exteriorização da conduta. A intervenção penal pode ser inócua e tardia demais. Neste ponto, é possível que já haja vítimas e autores de crimes. A ação estatal no contraterrorismo deve atuar para evitar que o fenômeno chegue a esse ponto. De nada importaria apurar autoria e materialidade de um crime cujo autor, muitas vezes, se martiriza na ação.

4. O TERRORISMO COMO UM FENÔMENO

A regulamentação do inciso XLIII do artigo 5º da Constituição Federal e a tipificação do terrorismo consideram uma parte do fenômeno do terrorismo. Utilizar-se da política criminal para prevenir o terrorismo é um passo necessário, mas é somente um passo. Existe uma abrangência do fenômeno que ultrapassa a esfera penal.

O fenômeno do terrorismo envolve aspectos sociais, políticos e psicológicos. A execução de uma ação violenta, como um atentado terrorista, envolve um processo em que concretização de um atentado terrorista envolve uma combinação de vários aspectos diferentes. Os atentados terroristas são frutos de uma longa cadeia de ações racionais planejadas e interconectadas (LAMAR, 2015). A radicalização por meio do desenvolvimento ou adoção de crenças radicais que justificam a violência é um dos caminhos possíveis para o envolvimento com o terrorismo (BORUM, 2011, p.8).

Como Newman (2010) define, o extremismo pode ser usado para se referir a ideologias políticas que se opõem aos valores e princípios centrais de uma sociedade. Ideias radicais não são condicionantes da ação terrorista. A maioria das pessoas que possuem ideias radicais não se envolve com terrorismo, e muitos terroristas não são muito ideologizados e não se radicalizam, mesmo aqueles que dizem defender uma causa (BORUM, 2011, p. 8). Existem milhões de muçulmanos que são simpáticos às ideias jihadistas, mas a maioria deles não se envolve com ações violentas. Ideologia e ação estão ligadas, mas nem sempre. Entretanto, alguns indivíduos absorvem ideias radicais e avançam ao ponto de executar ações violentas contra pessoas ou construções sob a crença de que estão fazendo algo correto.

De que forma, então, esse processo de interesse, aceitação, apoio a ideias radicais e execução de atos violentos ocorreria? Segundo T. Veldhuis and J. Staun (2009), as definições de radicalização normalmente se concentram em torno de dois focos diferentes: na radicalização violenta, onde a ênfase está na busca ou aceitação do uso da violência para obter um determinado objetivo; e em um sentido mais amplo de radicalização, onde a ênfase está na busca ou aceitação de mudanças mais profundas na sociedade, que pode ou não representar um risco para a democracia, e pode ou não envolver a ameaça ou uso de violência para atacar determinados objetivos.

A internet é usada para atrair a atenção para uma causa particular e para espalhar material de propaganda baseada em interpretações religiosas que legitimam ataques terroristas (SHETRET, 2011, p.2). As mensagens de Jihad Global são frequentemente customizadas para explorar populações vulneráveis, como os jovens. Também são customizadas linguisticamente para audiências ocidentais, em particular para encorajar a aceitação ideológica (SHETRET, 2011).

A narrativa dos terroristas pode ser categorizada em quatro camadas distintas, mas não mutuamente excludentes: narrativa política, narrativa moral, narrativa religiosa e narrativa social/heroica (OSCE, 2006, p. 6). A narrativa da Jihad Global pode ser ilustrada em quarto níveis:

> 1. O Islã está sob ataque pelo ocidente cruzado liderado pelo Estado Unidos da América;
>
> 2. Jihadistas, a quem o ocidente se refere como terroristas, estão se defendendo contra esse ataque;
>
> 3. As ações que eles tomam em defesa do Islã são proporcionais, justas e santificadas religiosamente; e 4. É dever de bons muçulmanos apoiar essas ações. (LEUPRECHT et al, 2010)

Depois dos atentados de 11 de setembro de 2011 nos Estados Unidos da América, os governos começaram a se preocupar com a relação entre terrorismo e internet (STEVENS, 2010). Vídeos de ataques e declarações de terroristas serviram de inspiração para grupos de indivíduos interessados, e as plataformas como salas de bate-papo, fóruns e correios eletrônicos também são usadas por pregadores radicais (STEVENS, 2010).

O discurso dos terroristas busca alcançar, cada vez mais, populações em distintos países, independentemente de origem cultural e religiosa. Objetiva encontrar indivíduos ou grupos em localidades que apresentem realidades psicológicas, econômicas, sociais e políticas que possibilitem a propagação e a aceitação das ideias radicais.

5. ESTRUTURAÇÃO DA PREVENÇÃO DO TERRORISMO

As políticas contraterroristas adotadas pelos Estados e por organizações internacionais evoluíram ao longo dos anos. Depois de anos concentrando principalmente em medidas de segurança de característica repressiva, é possível notar uma mudança em direção a uma agenda mais preventiva (VAN GINKEL, 2011, p.26).

A agenda de prevenção do terrorismo inclui a análise de fatores que levam as pessoas a escolherem por uma ação violenta. Inclui entender e focar nas demandas e reclamações que, se ignoradas, podem levar à raiva, frustração e, eventualmente, à violência. Essa, por si só, é uma evolução positiva, pois prevenir é melhor do que curar. Mais preocupante, contudo, é o fato de que o sistema penal está mudando em direção à criminalização de atos que são considerados parte da fase de preparação do terrorismo, misturando prevenção e repressão em uma maneira possivelmente contraproducente (VAN GINKEL, 2011, p.26).

A Lei nº 13.260/2016 reflete a visão de criminalização de atos e prioriza a repressão. A prevenção do terrorismo no Brasil, expressa nos termos da Lei nº 13.260/2016, parece se restringir à política penal de criminalização de condutas consideradas terroristas. O tratamento do terrorismo como uma questão de direito penal reduz a dimensão do problema. A Lei nº 13.260/16 é limitada justamente por ser uma lei penal. Carece de instrumentos que definam competências, atribuições, prerrogativas, instrumentos e controle para a prevenção do terrorismo.

Segundo Jorge Mascarenhas Lamar:

> No Brasil, não existe uma única instituição centralizada e específica encarregada de prevenir e combater o terrorismo internacional. Em realidade, há uma verdadeira justaposição de competências parciais e difusas sobre essa matéria. Diversas agências de segurança e inteligência brasileiras atuam na prevenção e combate ao terrorismo internacional (LAMAR, 2015).

Devido à especialização de atribuições dos diversos órgãos públicos brasileiros, a existência de diversas agências de segurança e de inteligência atuando na prevenção do terrorismo é algo esperado e desejado pelo legislador, uma vez que otimiza as especialidades de cada órgão frente à questão e aumenta o controle sobre as suas ações. Contudo, as competências, atribuições, protocolos de ação e instrumentos para a execução das missões institucionais devem estar claramente definidos e atribuídos.

Lamar acrescenta que, apesar das frequentes negativas das autoridades brasileiras e da falta de foco na mídia sobre as atividades

terroristas, "há crescente evidência documental de que uma série de atividades ligadas ao apoio e facilitação ao terrorismo no estrangeiro de fato aconteceram e continuam a acontecer dentro do território brasileiro" (LAMAR, 2015).

A atividade de prevenção do terrorismo atua para evitar que os atos violentos até mesmo venham a ocorrer e não se concentrar somente na apuração da autoria e da materialidade e na punição dos culpados. Para atender aos compromissos assumidos no âmbito internacional e às obrigações do direito internacional, e evitar o desenvolvimento do fenômeno em território nacional, a prevenção do terrorismo envolve ações anteriores à persecução penal, durante a persecução penal e posteriores a ela.

A principal maneira de se prevenir o terrorismo é por meio do conhecimento das causas do fenômeno, de como ele se desenvolve e de como os indivíduos ou grupos assumem ideais radicais e preparam e executam um ato violento. Com base nesses conhecimentos, é possível antecipar as ações e permitir que se atue para reduzir as causas e desmobilizar e conter pessoas ou grupos. Para tanto, a atividade de inteligência cumpre papel central na atividade de prevenção do terrorismo.

No Brasil, a Lei nº 9.883, de 7 de dezembro de 1999, institui o Sistema Brasileiro de Inteligência e cria a Agência Brasileira de Inteligência como órgão central do Sistema. O SISBIN tem como finalidade fornecer subsídios ao Presidente da República nos assuntos de interesse nacional.

Inteligência é definida pela Lei nº 9.883/99 como:

> a atividade que objetiva a obtenção, análise e disseminação de conhecimentos dentro e fora do território nacional sobre fatos e situações de imediata ou potencial influência sobre o processo decisório e a ação governamental e sobre a salvaguarda e a segurança da sociedade e do Estado.

O Decreto nº 4.376, de 13 de setembro de 2002, e seu artigo 3º define contra-inteligência como:

> a atividade que objetiva prevenir, detectar, obstruir e neutralizar a inteligência adversa e ações de qualquer natureza que constituam ameaça à salvaguarda de dados, informações e conhecimentos de interesse da segurança da sociedade e do Estado, bem como das áreas e dos meios que os retenham ou em que transitem.

Segundo o artigo 2º, § 1º, da lei, o Sistema Brasileiro de Inteligência é responsável pelo processo de obtenção, análise e disseminação da informação necessária ao processo decisório do Poder Executivo, bem como pela salvaguarda da informação contra o acesso de pessoas ou órgãos não autorizados, por meio de seu órgão central – a ABIN. O sistema de inteligência está normativamente constituído para fornecer subsídios ao processo decisório do poder executivo federal, mais precisamente ao Presidente da República.

O artigo 3º da Lei nº 9.883/99 encarrega a ABIN de planejar, executar, coordenar, supervisionar e controlar as atividades de inteligência do País, obedecidas à política e às diretrizes superiores. Ainda na Lei nº 9.883/99, o artigo 5º estabelece que a execução da Política Nacional de Inteligência

(PNI), fixada pelo Presidente da República, será levada a efeito pela ABIN, sob a supervisão da Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo. Compete ao órgão externo de controle da atividade de Inteligência o exame da PNI antes da aprovação pelo presidente da República.

A Política Nacional de Inteligência foi fixada pelo Decreto nº 8.793, de 29 de junho de 2016. É uma política elaborada pelo Poder Executivo e examinada pelo Poder Legislativo. A Política visa a definir os parâmetros e os limites de atuação da atividade de inteligência e de seus executores no âmbito do Sistema Brasileiro de Inteligência. O item 6 da PNI define como principais ameaças aquelas que apresentam potencial capacidade de pôr em perigo a integridade da sociedade e do Estado e a segurança nacional do Brasil. Dentre elas, encontra-se o terrorismo.

A PNI considera o terrorismo como uma ameaça à paz e à segurança dos Estados. Reafirma o compromisso do Brasil de implementar as resoluções pertinentes do Conselho de Segurança da Organização das Nações Unidas. Destaca a necessidade de prevenção e combate a ações terroristas e a seu financiamento, visando a evitar que ocorram em território nacional ou que este seja utilizado para a prática daquelas ações em outros países. Reafirma também a necessidade de parceria entre os órgãos envolvidos na área de segurança e defesa.

Dentre os objetivos da Inteligência Nacional, a PNI estabelece, no item 7:

> I – acompanhar e avaliar as conjunturas interna e externa, assessorando o processo decisório nacional e a ação governamental;
>
> II – identificar fatos ou situações que possam resultar em ameaças, riscos ou oportunidades;
>
> III – neutralizar ações da Inteligência adversa;
>
> IV – proteger áreas e instalações, sistemas, tecnologias e conhecimentos sensíveis, bem como os detentores desses conhecimentos; e
>
> V – conscientizar a sociedade para o permanente aprimoramento da atividade de Inteligência.

Na identificação das ameaças e na fixação dos objetivos, a PNI avança a Lei nº 9.883/1999 no sentido de detalhar o que na lei seria fornecer subsídios para o processo decisório do Presidente da República. O Decreto nº 8.793/2016 demanda dos órgãos componentes do SISBIN e de seu órgão central mais do que assessorar o Presidente da República e fornecer subsídios para a tomada de decisão. Sobre o terrorismo, a PNI considera a temática como uma "área de especial interesse e de acompanhamento sistemático por parte da Inteligência em âmbito mundial" e espera que a Inteligência contribua para a prevenção e o combate do terrorismo dentro do território nacional e para que o País não seja usado como apoio para ações em outros países.

No sentido de considerar o terrorismo como um fenômeno mais amplo do que o abarcado pela política criminal expressa na Lei nº 13.260/2016, o Manual de Inteligência: Doutrina Nacional de Inteligência – Bases Comuns

afirma que terrorismo se caracteriza pela ameaça ou emprego da violência física ou psicológica, de forma premeditada, por indivíduos ou grupos adversos, apoiados ou não por Estados. É motivado por razões políticas, ideológicas, econômicas, ambientais, religiosas ou psicossociais, e objetiva coagir ou intimidar autoridade ou parte da população, subjugar pessoas ou alcançar determinado fim ou propósito.

A definição de terrorismo presente na Doutrina Nacional de Inteligência também considera o terrorismo como algo mais amplo. A doutrina elenca, dentre as ameaças à sociedade e ao Estado, o terrorismo e o define como:

> [...] é a ameaça ou emprego premeditado de violência física ou psicológica, perpetrada contra alvos civis ou militares não combatentes ou contra propriedades, praticada por indivíduos ou grupos adversos, apoiados ou não por Estados, visando intimidar, coagir ou subjugar pessoas, autoridades ou populações, por razões político-ideológicas ou religiosas (Doutrina Nacional da Atividade de Inteligência, 2016, p. 60/149).

O parágrafo único do artigo 4º da Lei nº 9.883/1999 estabelece que os órgãos componentes do SISBIN fornecerão à ABIN, nos termos e condições a serem aprovados mediante ato presidencial, para fins de integração, dados e conhecimentos específicos relacionados com a defesa das instituições e dos interesses nacionais.

A ABIN pode fazer uso de técnicas e meios sigilosos, com irrestrita observância dos direitos e garantias individuais, como preceitua o parágrafo único do artigo 3º da Lei nº 9.883/1999. A PNI reforça a possibilidade de uso de técnicas e meios sigilosos ao definir, no item 2.4, a atividade de Inteligência como uma atividade especializada que exige o emprego de meios sigilosos, como forma de preservar sua ação, seus métodos e processos, seus profissionais e suas fontes. Destaca, ainda, que a inteligência desenvolve ações de caráter sigiloso destinadas à obtenção de dados indispensáveis ao processo decisório, indisponíveis para coleta ordinária em razão do acesso negado por seus detentores. Executa operações de inteligência que buscam a obtenção do dado negado.

O arcabouço legal brasileiro define, então, um sistema de inteligência, que possui um órgão central, a ABIN, que pode fazer uso de técnicas e meios sigilosos, na função de assessorar o Presidente da República em assuntos de interesse nacional. No caso específico do terrorismo, o sistema de inteligência e seu órgão central devem atuar na prevenção e no combate ao terrorismo.

Para o exercício da atividade de produção de conhecimentos sobre o terrorismo, a ABIN deve acompanhar o comportamento do fenômeno do terrorismo no mundo, prevenir, detectar e obstruir, o desenvolvimento do fenômeno no Brasil; deve compreender a inserção do Brasil na prevenção do terrorismo internacional e as peculiaridades do fenômeno do terrorismo no Brasil. Para desempenhar essas funções, a inteligência deve compreender os aspectos políticos, sociais, econômicos e psicológicos que envolvem o fenômeno do terrorismo.

Por meio dessa atuação, a ABIN pode contribuir para orientar as ações de alteração legislativa relativa ao tema, a organização das ações de prevenção, de repressão e de mitigação de eventuais atentados terroristas. A atuação da ABIN, como uma agência de inteligência, deve ocorrer também por meio de proposição de ações estruturantes e do fornecimento de conhecimentos sobre o terrorismo e suas causas psicológicas, sociais e políticas.

A atividade de contraterrorismo do Brasil não possui documentos estruturantes que definam atribuições, competências, procedimentos e protocolos de ação. Dentre os documentos estruturantes do contraterrorismo, poderia ser elaborado um Plano Nacional de Contraterrorismo. Esse Plano elencaria definições, objetivos, atribuições e competências. Outros documentos estruturantes seriam os protocolos de ação contraterrorista, principalmente sob o aspecto da prevenção.

Segundo o artigo 3º da Lei nº 9.883/99, a ABIN tem a seu cargo o planejamento, a execução, a coordenação, a supervisão e o controle das atividades de inteligência do País. No tocante à prevenção do terrorismo, em decorrência da preponderância das ações de inteligência, o planejamento, a coordenação, a supervisão e o controle estão a cargo do órgão central do SISBIN, a ABIN.

Compete à ABIN elaborar estudos, apresentar propostas e promover discussões com os demais órgãos para criar instrumentos normativos que permitam organizar as atividades de prevenção do terrorismo, e as definições de competências e atribuições que irão contribuir para o aumento da efetividade do contraterrorismo no Brasil.

Como agência de inteligência e órgão central do SISBIN, a ABIN, no exercício das funções de planejar e coordenar as atividades de inteligência do país, tem o papel de coordenar os órgãos que possam contribuir para ações de prevenção do terrorismo. Como decorrência, tem a atribuição de promover o debate, reuniões técnicas e o comprometimento dos órgãos para a elaboração de documentos que organizem o contraterrorismo no Brasil.

6. OS INSTRUMENTOS PARA A PREVENÇÃO DO TERRORISMO

Além de exercer papel estruturante do contraterrorismo no exercício de suas atribuições de planejar, coordenar, supervisionar e controlar, a ABIN também tem a atribuição de executar ações contraterroristas.

Dentre as ações contraterroristas exercidas pela ABIN, está a de produzir conhecimentos sobre a realidade do terrorismo internacional e seus reflexos para o Brasil, bem como sobre características, a situação e as tendências do fenômeno no País. Além disso, caberia à ABIN propor aos decisores e legisladores o aperfeiçoamento dos instrumentos legais necessários para a sua atuação institucional em face da prevenção do terrorismo.

A Lei nº 9.883/1999, o Decreto nº 4.376/2002 e o Decreto nº 8.793/2016 criaram órgão e sistema, estabeleceram atribuições e competências, criaram instâncias e mecanismos de controle, criaram prerrogativas para o desenvolvimento das atividades, mas não criaram elementos que garantam eficácia e segurança para a ação. Uma das maneiras de criar esses elementos decorreria da regulamentação do parágrafo único do artigo 3º da Lei nº 9883/1999, que possibilita à ABIN o uso de meios e técnicas sigilosas. A especificação de um rol não exaustivo de meios e técnicas sigilosas teria dupla função: garantir segurança jurídica e consequente aumento da eficácia das ações da ABIN e especificar os mecanismos de controle da aplicação dos meios e das técnicas.

Na atividade de produção de conhecimento para assessorar decisões do presidente da República e para contribuir com a prevenção do terrorismo, a atividade de inteligência pode utilizar de técnicas e meios sigilosos. As técnicas e meios sigilosos não foram regulamentados pelo legislador. Também não foram regulamentados os meios para a obtenção de dados para a produção dos conhecimentos. No silêncio do legislador, restam duas possibilidades de reflexão: o órgão de inteligência e o sistema de inteligência podem tentar obter dados de todas as formas que não violem direitos protegidos; e buscar regulamentações e alterações legislativas que garantam maior clareza e segurança jurídica para as atividades de inteligência na prevenção do terrorismo.

A atuação dos órgãos de inteligência, em especial da ABIN, sem uma regulamentação mais expressa de seus meios, e consequentes limites, para a obtenção de dados faz com que seja gasto tempo e esforço institucional para interpretar quais seriam as possibilidades e limites de atuação. Esse esforço interpretativo pode levar a posicionamentos mais conservadores que resultariam na redução da efetividade das ações do órgão de inteligência.

Para atuar na prevenção do terrorismo, a inteligência busca obter dados e analisar o comportamento do fenômeno nos principais centros irradiadores dos conflitos, nas regiões do mundo que são atingidas por ações terroristas e identificar a expansão do fenômeno, o modo de agir dos envolvidos e os meios utilizados para recrutar pessoas e praticar atos. Uma das formas de se compreender o fenômeno é compreender as dinâmicas políticas e sociais dos países em conflito, as características sociais e políticas dos países que sofrem atentados, as correspondências com o Brasil, as movimentações financeiras e os processos de radicalização de indivíduos.

Como decorrência, uma das maneiras de se prevenir o terrorismo é acompanhar indivíduos que possam estar envolvidos em um processo de radicalização, que tenham contatos com ideologias extremistas violentas e que possam estar se envolvendo com grupos terroristas. O acompanhamento desses alvos propicia a obtenção de dados para que se possa entender as causas do fenômeno do terrorismo e suas ligações com fenômenos internacionais, e antecipar a identificação de indivíduos que estejam em um processo que possa o levar a cometer atos violentos ou incentivar pessoas a fazer.

Quanto mais a inteligência possa conhecer sobre esses indivíduos, suas motivações e as características do ambiente social e político que os cerca, mais terá possibilidades de interferir no processo. A interferência nesse processo pode se dar de forma a desmotivar os indivíduos a aderirem a ideias radicais violentas, a desconstruir o discurso radical difundido para convencer novos adeptos e a orientar ações do Estado no sentido de atuar nos aspectos sociais e políticos que possam propiciar a adesão a ideias radicais violentas.

Dois são os tipos de indivíduo a ser monitorados: aqueles que motivam pessoas para o extremismo violento ou facilitam seu acesso a doutrinadores de grupos extremistas; e aqueles que podem ser vítimas de um processo de radicalização.

A inteligência tem a atribuição de atuar no contraterrorismo de forma a prevenir o avanço de processos de radicalização, prevenir a realização de atos terroristas e interferir nos elementos que possam levar a um ato violento. A preocupação mais ampla é como o indivíduo se envolve com o terrorismo, continua envolvido e, às vezes, se afasta.

Para executar suas tarefas, a inteligência necessita ter acesso a dados e ter capacidade de análise para produzir conhecimentos úteis e oportunos. Uma das maneiras de se obter dados é ter acesso a bancos de dados de órgãos públicos ou de instituições privadas. Informações contidas em bancos de dados, de forma isolada, podem não ter relevância, mas, quando analisadas em conjunto, podem auxiliar a construir linhas analíticas que permitem a compreensão do fenômeno do terrorismo. Outra forma de obter dados é por meio da utilização de fontes humanas que possam vir a ter acesso a dados não ostensivos.

A Lei nº 12.850/13, que define organização criminosa, inclusive a terrorista, dispõe sobre a investigação criminal e, por conseguinte, sobre os meios de obtenção da prova. Os dispositivos dessa lei se aplicam também aos crimes previstos na Lei nº 13.260/16. Dentre os meios de obtenção de prova previstos no capítulo II da Lei nº 12.850/13 estão:

> II - captação ambiental de sinais eletromagnéticos, ópticos ou acústicos;
>
> IV - acesso a registros de ligações telefônicas e telemáticas, a dados cadastrais constantes de bancos de dados públicos ou privados e a informações eleitorais ou comerciais;
>
> V - interceptação de comunicações telefônicas e telemáticas, nos termos da legislação específica;
>
> VII - infiltração, por policiais, em atividade de investigação, na forma do art. 11;
>
> VIII - cooperação entre instituições e órgãos federais, distritais, estaduais e municipais na busca de provas e informações de interesse da investigação ou da instrução criminal.

A atividade de prevenção do terrorismo requer que haja a regulamentação dos meios e técnicas que a ABIN tem a prerrogativa de utilizar e os consequentes controles para seu exercício, aos moldes dos meios elencados na Lei nº 12.850/13.

Os meios apresentados na Lei nº 12.850/13 são voltados para a investigação policial e, consequentemente, para a obtenção de provas. Os crimes previstos na Lei nº 13.260/16 são praticados contra o interesse da União, e cabe à Polícia Federal a investigação criminal, em sede de inquérito policial, e à Justiça Federal o seu processamento e julgamento.

A fase de investigação tem natureza administrativa e é realizada anteriormente à provocação da jurisdição penal (PACELLI, 2009, p. 49). Trata-se de um procedimento que visa ao esclarecimento do caso penal, destinado à formação do convencimento do responsável pela acusação. A acusação poderá, no decurso do processo legal, resultar em condenação e cerceamento de direitos dos indivíduos envolvidos.

A ação da inteligência não visa à obtenção de provas e à formação do convencimento do responsável pela acusação. Busca obter dados para atuar no fenômeno do terrorismo de forma mais ampla, identificando as causas e os meio pelos quais o fenômeno de desenvolve para assessorar decisões políticas (legislativas e executivas) no sentido de se evitar que haja até mesmo a necessidade de instauração de inquérito policial. Eventualmente, parte das ações da inteligência irão resultar em apoio às ações policiais e militares.

Sobre o acesso a registros, dados cadastrais, documentos e informações, o artigo 15 da Lei nº 12.850/13 estabelece que o delegado de polícia e o Ministério Público terão acesso, independentemente de autorização judicial, apenas aos dados cadastrais do investigado que informem exclusivamente a qualificação pessoal, a filiação e o endereço mantidos pela Justiça Eleitoral, empresas telefônicas, instituições financeiras, provedores de internet e administradoras de cartão de crédito. A lei franqueou a possibilidade do acesso pelo delegado e pelo Ministério Público a dados sem a necessidade de autorização judicial.

Na atividade de prevenção do terrorismo, a inteligência não atua para definir autoria e materialidade de uma conduta, com a suspeita do cometimento de um crime. A sua ação não resulta em prejuízo a direito individual protegido. O acesso pela ABIN aos dados cadastrais dos indivíduos não constituiria violação do direito à privacidade. O direito individual existe com determinado conteúdo. Mendes destaca que na teoria interna do direito não existem os conceitos de direito individual e de restrição como categorias autônomas (MENDES, 2014, p.41). Não existiriam restrições a direitos individuais, mas o próprio direito individual traz, em seu conteúdo, um limite. Se entendermos que existe a necessidade o indivíduo na comunidade, sob a ótica da teoria interna (Alexy, Robert), entenderemos que o próprio direito individual impõe uma necessidade de harmonização com direitos coletivos. O acesso aos dados individuais ocorreria com o objetivo de prevenir o avanço do fenômeno do terrorismo e garantir a segurança da sociedade e do Estado e a segurança da coletividade.

A Lei nº 12.965, de 23 de abril de 2014, estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Em seu artigo 8º, a Lei estabelece que a garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito

de acesso à internet. Acrescenta, ainda, no parágrafo único, que são nulas de pleno direito as cláusulas contratuais que violem o disposto no caput, tais como aquelas que impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet.

A proteção à privacidade prevista na Lei nº 12.965/14 visa a proteger a privacidade do indivíduo no uso da internet. Não seria razoável que tal normativo garantisse a privacidade do indivíduo frente ao Estado em questões de tal natureza como o terrorismo. O acesso aos dados pela inteligência não causaria prejuízos à privacidade do indivíduo. Não geraria nenhum constrangimento ao indivíduo, nem causaria danos à sua imagem e à sua honra. Por outro lado, contribuiria para melhorar a prevenção do terrorismo e aumentar a segurança da coletividade.

O acesso a bancos de dados sob custódia dos órgãos públicos pela ABIN constituiria uma transferência de sigilo. A ação estatal na temática do terrorismo se fundamenta em princípios constitucionais e em valores mais caros para a coletividade. Não se trata de caçadas aos terroristas, mas de utilização de meios para prevenir que o fenômeno do terrorismo prospere no país. A ação da inteligência não resulta em restrição de direitos ou liberdades do indivíduo, consiste em enfrentar o fenômeno com algo mais amplo do que uma questão de direito penal. Significa direcionar os esforços para se evitar que seja necessária a penalização de indivíduos. Não se trata, também, de violação da privacidade do indivíduo. Trata-se de dados que já estão disponíveis ao Estado e que serão utilizados para fins de inteligência, com o objetivo de prevenir ações terroristas ou o apoio a elas. Não culminarão em judicialização e eventual condenação com restrição de direitos.

Sobre a infiltração de agentes, o artigo 10 da Lei nº 12.850/13 estabelece as regras para a infiltração de agentes de polícia em tarefas de investigação. O § 2º do artigo 10 admite a infiltração se houver indícios de infração penal de que trata o artigo 1º e se a prova não puder ser produzida por outros meios disponíveis. O legislador demonstrou a preocupação com a colocação de um agente do Estado dentro de um ambiente criminoso para tornar-se parte de um crime, para que, dessa forma, fosse possível a obtenção de provas que venham a resultar na condenação dos criminosos. Duas são as preocupações do legislador: garantir que as provas sejam obtidas de maneira lícita e preservar a integridade do agente.

A ação da inteligência para obtenção de dados sobre a difusão de ideias radicais extremistas e o processo de radicalização de indivíduos para a ação violenta envolve a identificação dessas ideias e de pessoas que possam estar incentivando o cometimento de atos violentos. A inteligência pode, dessa forma, utilizar-se de agentes próprios ou de fonte humana para se aproximar de pessoas ou de grupos que possa estar em processo de radicalização. Esses grupos ainda não estariam cometendo as condutas tipificadas na Lei nº 13.260/16. Até esse ponto, não há o que se falar da necessidade de observância das regras para garantir a legalidade das provas obtidas, pois a atividade de inteligência não busca por provas. Também não há o que se falar sobre garantia da integridade do agente, pois não há ilícito em andamento.

O problema surge a partir do momento em que a ação de inteligência observa que existem indícios de que as condutas já são abarcadas pelas Lei nº 13.260/2016 ou nº 12.850/2013. Nesse momento, surge o problema de que haverá ou um agente do órgão ou uma fonte humana dentro de um ambiente que se tornou criminoso. A permanência do agente ou do colaborador pode colocá-lo como coautor de algum crime, como o de associação criminosa. Uma opção é a retirada desse agente ou fonte. Essa retirada pode causar dois problemas: risco para a integridade física e descontinuidade da ação de inteligência; e perda de dados e da possibilidade de se entender melhor o fenômeno do terrorismo e alcançar pontos mais importantes da rede, até mesmo fora do Brasil, que poderiam colaborar mais efetivamente para a prevenção de atos violentos no país ou em outros países. Não existem instrumentos que garantam a integridade do agente da inteligência para a continuidade de sua ação a partir do momento em que se inicia a ação policial em decorrência de inquérito para apuração das condutas previstas na Lei nº 13.260/16.

No sentido de garantir os instrumentos necessários para a ação de prevenção do terrorismo, Portugal recentemente regulamentou a ação dos órgãos de inteligência para a obtenção de dados. Portugal promulgou a Lei Orgânica nº 4/2017, de 25 de agosto de 2017, que regulamenta o acesso do Serviço de Informações de Segurança (S.I.S.) e do Serviço de Informações Estratégicas de Defesa (S.I.E.D.) a dados de telecomunicações e internet. A referida lei permite que esses Serviços de Informações tenham o acesso a dados de identificação, localização e tráfego relativos aos utilizadores de serviços de comunicações eletrônicas, para finalidades de defesa nacional, de segurança interna e prevenção de atos de sabotagem, espionagem, terrorismo, proliferação de armas de destruição em maça e de criminalidade altamente organizada. O acesso está sujeito à autorização judicial e a controle judicial posterior.

A Lei Orgânica nº 4/2017 está em consonância com a jurisprudência do Tribunal de Justiça da União Europeia que, quer no Acórdão Digital *Rights Ireland* de 8 de abril de 2014, quer no Acórdão Tele2/Watson de 21 de dezembro de 2016, tem reforçado a necessidade de a ingerência nas comunicações eletrônicas estar sujeita a limites claros e condições materiais e processuais objetivas. A normatização feita pelo Estado português esclarece forma e os limites de atuação dos serviços de inteligência. Cria instrumentos para atuação mais efetiva, bem como os necessários mecanismos de controle.

7. CONSIDERAÇÕES FINAIS

O Estado brasileiro elevou o repúdio ao terrorismo ao nível de princípio que rege suas relações internacionais. Considerou o terrorismo como crime inafiançável e insuscetível de graça ou anistia. A Lei nº 13.260/16 regulamenta o artigo 5º, inc. XLIII, da Constituição Federal. Entretanto, é uma lei que tipifica condutas e define competências do inquérito e do juízo. Trata do terrorismo somente sob o aspecto penal e se demonstra insuficiente como instrumento de prevenção. A Lei nº 13.260/16 é insuficiente para ser

considerada uma lei contraterrorista. A criminalização do terrorismo reduz a dimensão do fenômeno. Transfere para a esfera do indivíduo a culpa por um fenômeno que não é individual e não enfrenta as causas do problema. Além disso, é insuficiente para prevenir atentados terroristas.

A regulamentação prevista na Lei nº 13.260/16 representa somente um dos aspectos necessários para o contraterrorismo. Os compromissos e obrigações internacionais assumidos pelo Brasil com relação ao contraterrorismo, baseados nas determinações do Conselho de Segurança da ONU, e os instrumentos normativos nacionais demonstram a compreensão de que o terrorismo é um fenômeno mais amplo, com aspectos psicológicos, sociais e políticos que ultrapassam a esfera do direito penal.

O debate em torno da estruturação do contraterrorismo e da regulação dos meios e técnicas sigilosos utilizados pela ABIN refletem a forma que o Estado brasileiro se posiciona frente ao terrorismo. Uma vez que se trata de um fenômeno internacional, repudiado no âmbito dos fóruns internacionais e pelo próprio país, existem respostas que o Brasil precisa fornecer à comunidade internacional para não se tornar um país omisso ou amigável ao terrorismo. Também necessita oferecer respostas à população brasileira no sentido de impedir o avanço do fenômeno no país.

O repúdio ao terrorismo foi elevado a um dos princípios fundamentais da República Federativa do Brasil já em 1988. Uma vez que esse repúdio é alçado ao nível de princípio que rege as relações internacionais do Brasil, não seria razoável que, no âmbito nacional, o País adotasse uma postura mais permissiva com relação ao referido fenômeno.

Mesmo que se trate de um fenômeno incipiente no âmbito nacional, o terrorismo é um fenômeno que se pode atuar o mais cedo possível para que se evite a sua escalada e uma impossibilidade de controle efetivo.

A ação de prevenção do terrorismo ocorreria em momento anterior à materialização das condutas previstas na Lei nº 13.260/16. O início do inquérito policial e da ação penal previstos na lei, com indícios de cometimento dos crimes, pode não ser suficiente para impedir a execução de um ato violento. Ademais, o processo de radicalização de um indivíduo ou de grupos pode ser rápido ao ponto de ser inútil à ação de repressão prevista na Lei nº 13.260/16.

Para evitar a execução de atos terroristas, a inteligência deve monitorar os elementos que levam à radicalização de um indivíduo ou grupo. Esse monitoramento ocorre por meio de obtenção e análise de dados. A qualidade dos dados e das análises que resultaram em conhecimento para subsidiar decisões e ações depende da qualidade e da quantidade dos acessos a dados que a inteligência possa ter e da sua capacidade de análise.

Para o desenvolvimento de uma rede de proteção preventiva, a inteligência deve desenvolver uma rede de contatos e fontes humanas que possibilite alertas privilegiados de atividades suspeitas, deve conseguir entender quais são as redes de contatos que levam à radicalização de indivíduos e identificar quem seriam os principais difusores de ideias radicais dentro e fora do país.

O terrorismo é um fenômeno político e social que envolve uma combinação de elementos ligados ao indivíduo, à sociedade e à política. A compreensão desses elementos por meio de instrumentos adequados de atuação aumenta a capacidade de ação e neutralização do processo que pode levar a atentados terroristas. Para tratar do terrorismo de forma eficaz, o Estado deve fornecer mecanismos de atuação, de proteção e de controle igualmente eficazes. Para tratar de um fenômeno dessa magnitude deve-se profissionalizar as ações, inclusive com instrumentos legais adequados.

Nesse processo de amadurecimento institucional sobre o terrorismo, compete à ABIN exercer suas funções e apresentar as iniciativas necessárias para a formulação de instrumentos que organizem o contraterrorismo no Brasil, como um Plano Nacional Contraterrorista, um Protocolo de Ação Contraterrorista e o seu próprio Plano de Contraterrorismo. Compete à ABIN, também, fazer as gestões necessárias para a sensibilização e aprovação dos instrumentos legais necessários para a sua atuação na prevenção do terrorismo.

Para contribuir com o enfrentamento do terrorismo no mundo e prevenir e combater seu desenvolvimento no Brasil, o Estado brasileiro deve fazer opções quanto à estruturação do contraterrorismo no Brasil e criar ou regulamentar instrumentos que aumentem a efetividade das ações de forma a torná-las compatíveis com a dimensão do fenômeno. Essas opções demonstram a coerência entre o discurso sobre o terrorismo e as ações efetivas para preveni-lo e combatê-lo.

8. REFERÊNCIAS

ALEXY, Robert. **Teoria dos Direitos Fundamentais**. São Paulo: Malheiros, 2017.

ATRAN, S.. **Pathways to and From Violent Extremism**: The Case for Science-Based Field Research, Statement before the Senate Armed Services Subcommittee on Emerging Threats & Capabilities, March 10, 2010.

BORUM, Randy. **Radicalization into Violent Extremism I**: A Review of Social Science Theories. Journal of Strategic Security. Vol. 4 Nº 4, 2012. Disponível em: <http://scholarcommons.usf.edu/jss/vol4/iss4/2>.

_____. Agência Brasileira de Inteligência. **Portaria nº 244, de 23 de agosto de 2016**. Doutrina Nacional da Atividade de Inteligência.

_____. Conselho Consultivo do Sisbin. **Manual de Inteligência**: Doutrina Nacional de Inteligência – Bases Comuns. Brasília: Agência Brasileira de Inteligência, 2004.

BRASIL. **Constituição da República Federativa do Brasil de 1988**.

_____. **Lei nº 7.960, de 21 de dezembro de 1989**.

_____. **Lei nº 9.296, de 24 de julho de 1996**.

_____. **Lei nº 9.883, de 7 de dezembro de 1999**.

_____. **Decreto nº 4.376, de 13 de setembro de 2002**.

_____. **Lei nº 12.850, de 2 de agosto de 2013**.

_____. **Lei nº 12.830, de 20 de junho de 2013**.

_____. **Lei nº 12.965, de 23 de abril de 2014**.

_____. **Lei nº 13.260, de 16 de março de 2016**.

_____. **Decreto nº 8.793, de 29 de junho de 2016**.

CAPEZ, Fernando. **Curso de Direito Penal**: Parte Geral. São Paulo: Saraiva, 2008.

Global Terrorism Database [homepage na internet]. Data Collection Methodology [acesso em 31 nov 2017]. Disponível em: <https://www.start.umd.edu/gtd/using-gtd/>.

LAMAR, Jorge Mascarenhas. A legislação brasileira de combate e prevenção do terrorismo quatorze anos após 11 de Setembro: limites, falhas e reflexões para o futuro. **Revista de Sociologia e Política**. vol. 23. nº 53. Curitiba Mar. 2015 Disponível em: <http://dx.doi.org/10.1590/1678-987315235304>.

LEUPRECHT, Christian; HATALEY, Todd; MOSKALENKO, Sophia; MCCAULEY, Clark. **Narrative and Counter-narratives for Global Jihad:** Opinion versus Action. In:

KESSELS, Eelco J.A.M. (Ed.). **Countering Violent Extremist Narratives**. National Coordinator for Counterterrorism, julho de 2010.

MENDES, Gilmar. **Direitos Fundamentais e Controle de Constitucionalidade**: Estudos de Direito Constitucional. 4ª Edição. São Paulo: Saraiva, 2014.

NEUMAN, P.. **Prisons and Terrorism Radicalisation and De-radicalisation in 15 Countries**. A policy report published by the International Centre for the Study of Radicalisation and Political Violence (ICSR). Londres: King's College London, 2010.

ONU. **Resolução Nº 1373, de 28 de setembro de 2001**.

ONU. **Resolução A/70/L.55**

PACELLI, Eugênio. **Curso de Processo Penal**. Rio de Janeiro: Lumen Juris, 2009.

PORTUGAL. **Lei Orgânica nº 4/2017, de 25 de agosto de 2017**.

SCHMID, A.P. **Terrorism**: The definitional problem. Case Western Reserve Journal of International Law 36:375-419. Disponível em: <http://scholarlycommons.law.case.edu/jil/vol36/iss2/8>.

SHETRET, Liat. **Use of the Internet for Counter□Terrorist Purposes**. Center on Global Counter□Terrorism Cooperation, Policy Brief, fevereiro de 2011. Disponível em: <https://www.files.ethz.ch/isn/126762/LS_ policybrief_119.pdf>.

SPAAIJ, Ramón. **Understanding Lone Wolf Terrorism**: Global Patterns, Motivations and Prevention⁰ Melbourne: Springer, School of Social Sciences, La Trobe University. Disponível em: <www.springer.com>.

STEVENS, Tim. New Media and Counter-Narrative Strategies. In: KESSELS, Eelco J.A.M. (Ed.). **Countering Violent Extremist Narratives**. National Coordinator for Counterterrorism, julho de 2010.

THE COUNCIL OF EUROPE. **Summary of the Expert Workshop on Preventing Terrorism**: Fighting Incitement and Related Terrorist Activities, Vienna, 19-20 October 2006, Organised by the Organisation of Security and Cooperation in Europe (OSCE), the Council of Europe, the Federal Republic of Germany and the Russian Federation. Disponível em: <https://rm.coe.int/16805d70fd>.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. **Acórdão Digital Rights Ireland, de 8 de abril de 2014.**

TUK, A. Sociology of terrorism. In: MATSON, Ronald R. (ed). **The spirit of sociology***:* a reader. Boston: Pearson, 2008.

VAN GINKEL, Bibi. **Incitement to Terrorism**: A Matter of Prevention or Repression. Haia: ICCT, 2011.

VELDHUIS, Tinka & STAUN, Jorgen. **Islamist Radicalisation**: A Root Cause Model. Haia: Netherlands Institute of International Relations Clingendael, 2009.

CNMP

Conselho
Nacional do
Ministério Público