ESCOLA DE COMANDO E ESTADO-MAIOR DA AERONÁUTICA
COORDENADORIA ACADÊMICA
CURSO DE POLÍTICA E ESTRATÉGIA AEROESPACIAIS

GUSTAVO DO AMARAL GAMA, Cel Inf

A fragilidade da segurança da informação nos planos estratégicos das Forças Armadas frente à Lei de Acesso à Informação

Rio de Janeiro
2025

ESCOLA DE COMANDO E ESTADO-MAIOR DA AERONÁUTICA
COORDENADORIA ACADÊMICA
CURSO DE POLÍTICA E ESTRATÉGIA AEROESPACIAIS

GUSTAVO DO AMARAL GAMA, Cel Inf

A fragilidade da segurança da informação nos planos estratégicos das Forças Armadas frente à Lei de Acesso à Informação

Trabalho de conclusão de curso apresentado à Escola de Comando e Estado-Maior da Aeronáutica como requisito parcial para aprovação no Curso de Política e Estratégia Aeroespaciais.

Orientador: Alessandro Da Costa Borges

Rio de Janeiro

2025

1 INTRODUÇÃO

"Quem confiou os seus segredos a outra pessoa, fez-se escravo dela."
Baltasar Gracián y Morales.

Em 18 de novembro de 2011, a então Presidente do Brasil, Dilma Rousseff sancionou a Lei n º 12.527 que ficou conhecida como a Lei de Acesso à Informação (LAI).

A promulgação da LAI representou um avanço na transparência do governo brasileiro, permitindo que cidadãos tivessem maior acesso aos documentos e informações oficiais, tendo em vista que "A Lei de Acesso à Informação prevê que a transparência das informações se torne a regra e o sigilo, a exceção" (Brasil, 2011), conforme descrito no Art. 3º, inc. I da Lei 12.527/2011. Segundo o Professor Celso Antônio Bandeira de Mello, "esta lei sobre o direito à Informação Pública, certamente provocaria no Brasil uma importante transformação nos costumes políticos e administrativos" (Valim; Malheiros; Bacariça, 2015).

Contudo, apesar dos avanços democráticos com os quais a LAI presenteou a sociedade brasileira, ela também trouxe, a reboque, diversas ameaças que assolam veladamente às autoridades do alto escalão das Forças Armadas do Brasil, na medida que, a aplicação dessa lei nos documentos relacionados aos Planos Estratégicos de Emprego Conjunto das Forças Armadas (PEECFA) pode gerar uma vulnerabilidade significativa à segurança nacional.

O compartilhamento de detalhes operacionais, táticos e estratégicos por meio de solicitações de acesso às informações, previstos na LAI, coloca em risco o sigilo de planos críticos para a defesa nacional, expondo dados que deveriam ser mantidos sob total sigilo. Tais informações poderiam ser usadas por adversários para antecipar movimentos militares, comprometendo a eficácia das operações e a segurança nacional.

Mesmo com exceções de sigilo previstas pela própria LAI, a constante pressão por maior transparência pode levar à redução da capacidade de proteger planos militares essenciais.

Ademais, a LAI trouxe consigo vários desafios na gestão de segurança cibernética e proteção de dados militares pois, com a ampliação do acesso a documentos públicos, inclusive os relacionados a temas militares, as Forças Armadas precisaram redobrar seus esforços para proteger dados sensíveis contra ameaças cibernéticas. Isso inclui o desafio de garantir que as plataformas e os sistemas que armazenam e divulgam tais informações sejam altamente seguros, tal como a necessidade de que a tramitação dos documentos seja feita por meio de canal que contenha proteção por criptografia de Estado, a qual atualmente não existe. No entanto, a constante necessidade de disponibilizar documentos sob o escopo da LAI aumenta

o risco de exposição de dados. A própria natureza dos documentos militares, que muitas vezes envolvem informações interligadas entre diferentes níveis de comando e de segurança, torna o gerenciamento da segurança cibernética mais complexo, exigindo investimentos constantes em tecnologia, treinamento e protocolos de proteção que, nem sempre, acompanham as necessidades emergentes. A vulnerabilidade dessas informações no ambiente digital pode ser explorada por atores hostis, comprometendo a integridade das operações militares e da segurança do Estado.

Diante desse panorama instigante, a proposta deste ensaio é comprovar a tese de que a promulgação da Lei nº12.527 de 18 de novembro de 2011 (Lei de Acesso à Informação) no Brasil expôs vulnerabilidades na segurança da informação dos Planos Estratégicos de Emprego Conjunto das Forças Armadas, ao facilitar o acesso público a documentos sigilosos e ao aumentar o risco de vazamentos de informações estratégicas.

2 A LAI E OS SEUS DECRETOS

2.1 A REGULAMENTAÇÃO

De acordo com o Decreto-Lei nº 4.657, de 4 de setembro de 1942, Lei de Introdução às normas do Direito Brasileiro: "Art. 1º Salvo disposição contrária, a lei começa a vigorar em todo o país quarenta e cinco dias depois de oficialmente publicada" (BRASIL,1942), todavia, a lei pode ser regulamentada por decreto do Poder Executivo, que detalha e estabelece as normas para sua aplicação. No caso da LAI dois decretos foram promulgados para a regulamentação de procedimentos nela contidos. O Decreto nº 7.845, de 14 de novembro de 2012 e o Decreto nº 7.724, de 14 de maio de 2012. O primeiro 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 (Brasil, 2012). O segundo, regulamenta, no âmbito do Poder Executivo federal, os procedimentos para a garantia do acesso à informação e para a classificação de informações sob restrição de acesso, observados grau e prazo de sigilo (Brasil, 2012).

2.1.1 O Problema Estratégico

Anteriormente a LAI, o acesso aos documentos sigilosos tais quais os Planos Estratégicos de Emprego Conjunto das Forças Armadas (PEECFA) era regulamentado pelo Decreto nº 4.553, de 27 de dezembro de 2002 que em seu Art. 1º diz:

> São considerados originariamente sigilosos, e serão como tal classificados, dados ou informações cujo conhecimento irrestrito ou divulgação possa acarretar qualquer risco à segurança da sociedade e do Estado, bem como aqueles necessários ao resguardo da inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas (Brasil, 2002).

Conforme está previsto na Sistemática de Planejamento Estratégico Militar (MD51-M-01), os PEECFA norteiam a elaboração dos planos dos comandos operacionais ativados em conformidade com a Estrutura Militar de Defesa (EttaMiD) e orientam o preparo das Forças (Brasil, 2018, p.18). Por se tratar de "documentos estratégicos que contém informações referentes a planos e operações militares, cujo conhecimento não-autorizado pode, em tese, acarretar dano excepcionalmente grave à segurança da sociedade e do Estado" (Brasil, 2002), os PEECFA são classificados com o grau de sigilo ultrassecreto. No passado, tal classificação estava regulamentada pelo Decreto nº 4.553, de 2002 o qual protegia o conteúdo dos Planos contra o acesso de pessoas ou entidades que por sua natureza não possuíam as credenciais de segurança necessárias ou a "necessidade de conhecer" o seu conteúdo, por um período de 50 (cinquenta) anos, podendo "ser renovado indefinidamente, de acordo com o interesse da segurança da sociedade e do Estado." (Brasil, 2002). Consequentemente, por se tratar de um documento sigiloso com classificação ultrassecreta, os PEECFA, seriam considerados Documentos Sigilosos Controlados (DSC), o que lhes garantia medidas adicionais de controle as quais estavam previstas no Art.18 e 19 do Decreto nº 4.553, de 2002.

Em maio de 2005, o então presidente Luiz Inácio Lula da Silva, sancionou a Lei nº 11.111 a qual dizia em seu Art. 3º que "Os documentos públicos que contenham informações cujo sigilo seja imprescindível à segurança da sociedade e do Estado poderão ser classificados no mais alto grau de sigilo" (Brasil, 2005), ou seja, o grau ultrassecreto. A mesma lei, em seu artigo 6º remetia à restrição de acesso aos documentos ultrassecretos ao previsto no § 2º do art. 23 da Lei nº 8.159, de 8 de janeiro de 1991, de autoria do presidente Fernado Collor de Mello. Neste artigo ficou estabelecido que: "O acesso aos documentos sigilosos referentes à segurança da sociedade e do Estado será restrito por um prazo máximo de 30 (trinta) anos, a contar da data de sua produção, podendo esse prazo ser prorrogado, por uma única vez, por igual período." (Brasil, 1991), evidenciando a preocupação com a manutenção do sigilo das informações ultrassecretas desde aquela época.

Acontece que durante o governo Dilma Roussef, evidenciou-se a redução significativa das proteções advindas do sigilo, a partir da promulgação da LAI e de seus decretos regulamentadores. O Art. 60 do Decreto nº 7.845, de 14 de novembro de 2012 revogou o Decreto nº 4.553, de 27 de dezembro de 2002, que dispunha sobre a "salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do

Estado, no âmbito da Administração Pública Federal" (Brasil, 2002), e com a assinatura, pela Presidente Dilma Roussef, do Decreto nº 7.724, de 16 de maio de 2012, novas regras sobre o acesso a informações foram estabelecidas no Brasil. Tais regras tinham como propósito garantir o cumprimento da LAI e facilitar ao cidadão o acesso ao seu direito constitucional de solicitar e obter informações dos órgãos e entidades públicas.

É razoável afirmarmos que informações estratégicas devem ser protegidas tendo em vista que atuam diretamente: "para conhecimento dos ambientes interno e externo de uma organização e para atuação nestes ambientes"(Chaumier, 1986). No caso de informações estratégicas militares, cito os PEECFA, o dano no descuido da segurança informacional coloca em risco o próprio Estado, à medida que os dados contidos em tais documentos expõe nossas forças e vulnerabilidades no contexto de uma suposta Hipótese de Emprego (HE).

Conforme Oliveira (2024), a importância da proteção de informações militares estratégicas e o dano que o vazamento de tais informações podem causar pode ser exemplificada com o famoso caso da exposição, na rede mundial de computadores, de documentos confidenciais militares do governo do Estados Unidos pelo grupo WikiLeaks, como por exemplo aqueles denominados "Afghan War Diary", vazados do Departamento de Defesa dos EUA. Os documentos traziam com detalhes, informações sobre operações militares no Afeganistão, incluindo ataques aéreos, mortes de civis, e atividades dos insurgentes. O vazamento expôs a realidade brutal do conflito e a discrepância entre o que era comunicado oficialmente e o que realmente acontecia no campo de batalha, o que gerou um prejuízo a imagem dos EUA.

É justo dizer que a LAI trouxe benefícios ao cidadão, mas ao mesmo tempo, sua regulamentação fragilizou a segurança de informações estratégicas militares ao diminuir os prazos do sigilo dos documentos classificados conforme o Art. 28 do Decreto nº 7.724, de 2012 de 30 (trinta) para 25 (vinte e cinco) anos no caso de documentos ultrassecretos, bem como ao extinguir a figura da prorrogação da manutenção do sigilo prevista no parágrafo único do Art. 7 do Decreto nº 5.301 de 2004, bem como no Art. 23 do Decreto nº 2.134, de 24 de janeiro de 1997 "Poderá a autoridade responsável pela classificação dos documentos, considerando o interesse da segurança da sociedade e do Estado, renová-la por uma única vez, por igual período"(Brasil, 1997).

Ademais, a LAI instituiu no §1º do Art. 35 a Comissão Mista de Reavaliação de Informações, e o Decreto nº 7.724 de 2012 traz no Inciso I do seu Art. 47 uma atribuição da Comissão que se traduz em uma das principais ameaças ao sigilo das informações militares

estratégicas, qual seja: “rever, de ofício ou mediante provocação, a classificação de informação no grau ultrassecreto ou secreto ou a sua reavaliação, no máximo a cada quatro anos;” (Brasil, 2012a). O que, na prática, faz com que a classificação dos documentos secretos e ultrassecretos tenha que ser reavaliada por este colegiado, no máximo a cada quatro anos, fazendo com que o sigilo, inicialmente garantido por 20 (vinte) anos, no caso dos documentos secretos, e 25 (vinte e cinco) anos, no caso dos ultrassecretos, possa ser reduzido ou até mesmo extinto em um período menor, até mesmo daqueles documentos classificados como reservados que possuem sigilo de 5 (cinco) anos.

2.2 A SEGURANÇA CIBERNÉTICA

Dentre as atribuições prevista na LAI, coube ao Gabinete de Segurança Institucional (GSI) formular e coordenar as políticas de segurança da informação, incluindo proteção criptográfica de informações sensíveis do Estado, pois, segundo o previsto no Inciso I do Art.12 do DECRETO Nº 9.637, de 26 de dezembro de 2018, aquele Gabinete é a entidade responsável por “estabelecer norma sobre a definição dos requisitos metodológicos para a implementação da gestão de risco dos ativos da informação pelos órgãos e pelas entidades da administração pública federal” (Brasil, 2018).

De acordo com o Art. 40 do Decreto nº 7.845, de 14 de novembro de 2012, “a cifração e a decifração de informação classificada em qualquer grau de sigilo deverão utilizar recurso criptográfico baseado em algoritmo de Estado” (Brasil, 2012b).

Dito isto, existem diversos algoritmos de criptografia disponíveis no mercado, porém, a lei estabelece que, no caso específico de utilização de criptografia para tramitação dos documentos contendo informação classificada, as chaves criptográficas necessariamente devem estar baseadas em algoritmo de Estado.

Sabemos que, o Decreto nº 7.724 de 2012, prevê em seu artigo 25 que:

> São passíveis de classificação as informações consideradas imprescindíveis à segurança da sociedade ou do Estado, cuja divulgação ou acesso irrestrito possam:
> VI- prejudicar ou causar risco a planos ou operações estratégicos das Forças Armadas (Brasil, 2012a).

Ou seja, os planos estratégicos militares deverão ser obrigatoriamente classificados com algum grau de sigilo. No caso dos PEECFA, a classificação adotada foi a “ultrassecreta”, por decisão da autoridade classificadora, tendo em vista tratar-se de planos baseados em Hipóteses de Emprego (HE). Neste caso, as informações contidas nos PEECFA requerem condições especiais de segurança no seu tratamento, inclusive na tramitação e no acesso a tais documentos.

Ademais, na Instrução Normativa GSI/PR nº 3, de 06 de março de 2013 está estabelecido

que dentre os padrões mínimos para recurso criptográfico baseado em algoritmo de Estado, “o único que atende na segurança de documentos ultrassecretos é aquele que possui o algoritmo de sequência aleatória” (Brasil 2013).

Todavia, até a presente data, este tipo de algoritmo ainda não foi desenvolvido pelo órgão competente, fato este que gera transtornos na tramitação dos documentos com classificação ultrassecreta, pois caso seja necessário o acesso por outra organização que possua a necessidade de conhecer o teor do documento classificado, o dispositivo no qual estiver armazenado, deverá ser entregue pessoalmente por mensageiro, pois:

> A expedição, a condução e a entrega de documento com informação classificada em grau de sigilo ultrassecreto serão efetuadas pessoalmente, por agente público autorizado, ou transmitidas por meio eletrônico, desde que sejam usados recursos de criptografia compatíveis com o grau de classificação da informação, vedada sua postagem. (Brasil, 2012).

Tal situação se agrava ainda mais no caso do Brasil, tendo em vista as dimensões continentais do nosso país, causando diversos transtornos administrativos, dentre eles os gastos com passagens aéreas, diárias, e custos operacionais.

3 CONCLUSÃO

Ao mesmo passo que a promulgação da LAI representou um avanço na transparência do governo brasileiro, permitindo que cidadãos tivessem maior acesso aos documentos e informações oficiais, constatamos que a constante pressão por maior transparência pode levar à redução da capacidade de proteger planos militares estratégicos. As liberdades concedidas pela LAI aumentaram o risco da quebra do sigilo das informações estratégicas, como por exemplo os PEECFA, mesmo com as exceções de sigilo previstas na própria lei.

Fica claro também que o dispositivo legal trouxe consigo vários desafios na gestão de segurança cibernética dos planos militares pois, com a facilitação do acesso a documentos sigilosos, inclusive os relacionados a temas militares, as Forças Armadas precisaram redobrar seus esforços para proteger dados sensíveis contra ameaças cibernéticas, tanto no armazenamento quanto na tramitação para evitar a exploração por atores hostis. Contudo, a ausência de uma criptografia de Estado dificulta ainda mais a tarefa de manter o sigilo das informações sobre as operações militares afetando diretamente a segurança do Estado.

Desta forma, é certo que a promulgação da Lei nº12.527 de 18 de novembro de 2011 vulnerabilizou a segurança da informação dos Planos Estratégicos de Emprego Conjunto das Forças Armadas, ao facilitar o acesso público a documentos sigilosos e ao aumentar o risco de

vazamentos de informações estratégicas.

Com isso, concluo este trabalho com a certeza de que o assunto não foi esgotado, porém, certo de que existem lacunas na LAI que precisam ser preenchidas a fim de que possamos mitigar os riscos anteriormente listados a fim de preservarmos a segurança das informações sigilosas, em especial aquelas que se referem aos PEECFA, por se tratar de informações referentes à segurança nacional e a imagem do país no exterior.

REFERÊNCIAS

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. DECRETO-LEI Nº 4.657, de 4 de setembro de 1942, Lei de Introdução às normas do Direito Brasileiro. **Diário Oficial**, Brasília, p. 1, 09 set 1942. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del4657.htm. Acesso em 04 jul 2025.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. LEI Nº 8.159, de 8 de janeiro de 1991. Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. **Diário Oficial da União**, Brasília, p. 455, 09 jan 1991. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8159.htm. Acesso em 04 jul 2025.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. DECRETO Nº 2.134, de 24 de janeiro de 1997, Regulamenta o art. 23 da Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a categoria dos documentos públicos sigilosos e o acesso a eles, e dá outras providências. **Diário Oficial da União**, Brasília, p.1435, 27 jan 1997. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/d2134.htm. Acesso em 04 jul 2025.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. DECRETO Nº 4.553, de 27 de dezembro de 2002. Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências. **Diário Oficial**, Brasília, p. 6, 30 dez 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/2002/d4553.htm. Acesso em 04 jul 2025.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. DECRETO Nº 5.301 de 9 de dezembro de 2004, Regulamenta o disposto na Medida Provisória no 228, de 9 de dezembro de 2004, que dispõe sobre a ressalva prevista na parte final do disposto no inciso XXXIII do art. 5o da Constituição, e dá outras providências. **Diário Oficial da União**, Brasília, p.1, 9 dez 2004. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2004/Decreto/D5301.htm. Acesso em 04 jul 2025.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. LEI Nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. **Diário Oficial da União**, Brasília, p. 1, 18 nov 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em 09 jul 2025.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. DECRETO Nº 7.724, de 16 de maio de 2012, Regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição. **Diário Oficial da União**, Brasília, p.1, 16 mai 2012a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/d7724.htm. Acesso em 04 jul 2025.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. 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. **Diário Oficial da União**, Brasília, p.1, 16 nov 2012b. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/d7845.htm>. Acesso em 04 jul 2025.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Norma Complementar 09/IN01/DSIC/GSI/PR de 15 de julho de 2014. Orientações Específicas para o Uso de Recursos Criptográficos em Segurança da Informação e Comunicações. **Diário Oficial da União,** Brasília, p.4, 16 jul 2014. Disponível em: https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/legislacao. Acesso em 09 jul 2025.

BRASIL. Presidência da República. Secretaria Geral. Subchefia para Assuntos Jurídicos. DECRETO Nº 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. **Diário Oficial da União**, Brasília, p. 23, 27 dez 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/d9637.htm. Acesso em 09 jul 2025.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. INSTRUÇÃO NORMATIVA GSI/PR Nº 3, de 28 de maio de 2021. Dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal. **Diário Oficial da União,** Brasília, p.13, 31 mai 2021. Disponível em: https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/legislacao/copy_of_IN03_consolidada.pdf . Acesso em 10 jul 2025.

BRASIL. Comando da Aeronáutica. Universidade da Força Aérea. Manual de trabalhos acadêmicos da Universidade da Força Aérea. 8.ed. Rio de Janeiro: UNIFA, 2025.

CHAUMIER, Michel. Planejamento Estratégico: Teoria e Prática. São Paulo: Atlas, 1986.

OLIVEIRA, Danilo. Quais os principais vazamentos feitos pelo WikiLeaks? . Olhar Digital, 2024. Disponível em: https://olhardigital.com.br/2024/07/07/seguranca/quais-os-principais-vazamentos-feitos-pelo-wikileaks/ . Acesso em: 10 jul 2025.

VALIM, Rafael; MALHEIROS, Antônio Carlos; BACARIÇA, Josephina. Acesso à Informação Pública. [S.l.]: Editora Fórum, 2015.