V. 20
2024

ISSN 2317-6172

Revista DIREITO GV

FGV DIREITO SP

Recebido: 17.11.2022
Aprovado: 11.12.2023
https://doi.org/10.1590/2317-6172202415

Editora responsável
Catarina Helena Cortada Barbieri
(*Editora-chefe*)

1 Escola de Comando e Estado-Maior do Exército, Programa de Pós-Graduação em Ciências Militares, Rio de Janeiro, Rio de Janeiro, Brasil
https://orcid.org/0000-0001-9330-6399

O sigilo nas Forças Armadas brasileiras: normas e procedimentos para classificar informações com base na segurança do Estado e da sociedade

SECRECY IN THE BRAZILIAN ARMED FORCES: RULES AND PROCEDURES FOR CLASSIFYING INFORMATION BASED ON THE SECURITY OF THE STATE AND SOCIETY

CONFIDENCIALIDAD EN LAS FUERZAS ARMADAS BRASILEÑAS: NORMAS Y PROCEDIMIENTOS PARA CLASIFICAR INFORMACIÓN BASADA EN LA SEGURIDAD DEL ESTADO Y LA SOCIEDAD

Karina Furtado Rodrigues[1]

Resumo
Por meio da análise da normativa vigente, de entrevistas e pedidos de informação via Lei n. 12.527/2011, este artigo propõe-se a compreender, dentro das Forças Armadas (FA) brasileiras, a regulação e a gestão da classificação em relação ao sigilo de informações com base na segurança do Estado e da sociedade. Para isso, analisam-se a habilitação das instituições classificadoras; a atribuição, manutenção, reavaliação e desclassificação do sigilo; as formas de controle externo; e as possibilidades de eliminação desses documentos quando desclassificados. Conclui-se que a complexidade do processo de classificação quanto ao sigilo nas FA impõe desafios à sua avaliação e governança, permanecendo duas questões em aberto: a ampla discricionariedade no momento de interpretar e atribuir os graus de sigilo; e o limbo regulatório quanto à publicização desses documentos após desclassificados, visto que as restrições supracitadas somam-se a outras hipóteses de salvaguarda. Logo, o sistema de classificação de informações em graus de sigilo brasileiro serve ao propósito de restringir a informação à necessidade de conhecer de agentes públicos, mas não é ferramenta suficiente, se utilizada isoladamente, para prover transparência pública.

Palavras-chave
Informações sigilosas; acesso à informação; transparência pública; classificação de documentos; Forças Armadas.

Abstract
Through the analysis of legal and infra-legal norms, interviews, and requests for information via Law n. 12,527 (2011), this article proposes to understand, within the Brazilian Armed Forces, the regulation and management of the classification regarding the secrecy of information based on the security of the state and society. For this, it analyzes the qualification of the classification institutions; the attribution, maintenance, reassessment, and declassification of secrecy; forms of external control; and the possibilities of eliminating such documents when already disqualified. It is concluded that the complexity of the classification process regarding confidentiality in the armed forces poses challenges to its evaluation and governance, with two questions remaining open: one is the broad discretion when interpreting and assigning degrees of secrecy; another is the regulatory limbo regarding the publication of these documents after being declassified since other hypotheses for safeguarding information coexist. Therefore, the Brazilian information classification system serves the purpose of restricting information to public agents' need to know, but it is not in itself a public transparency tool.

Como citar este artigo
RODRIGUES, Karina Furtado. O sigilo nas Forças Armadas Brasileiras: normas e procedimentos para classificar informações com base na segurança do Estado e da sociedade. *Revista Direito GV*, São Paulo, v. 20, e2415, 2024. https://doi.org/10.1590/2317-6172202415

Keywords
Confidential information; access to information; public transparency; classification of documents; armed forces.

Resumen
A través del análisis de normas legales e infralegales, entrevistas y solicitudes de información según la Ley 12,527 (2011), este artículo propone comprender, dentro de las Fuerzas Armadas Brasileñas, la regulación y gestión de la clasificación en relación con el secreto de la información basado en la seguridad del Estado y la sociedad. Para ello, se analiza la calificación de las instituciones de clasificación, la atribución, el mantenimiento, la reevaluación y la desclasificación del secreto; formas de control externo; y las posibilidades de eliminar tales documentos una vez descalificados. Se concluye que la complejidad del proceso de clasificación en relación con la confidencialidad en las fuerzas armadas plantea desafíos para su evaluación y gobernanza, dejando dos cuestiones abiertas: la amplia discreción al interpretar y asignar grados de secreto; y el limbo regulatorio con respecto a la publicación de estos documentos después de ser desclasificados, ya que coexisten otras hipótesis para salvaguardar información. Por lo tanto, el sistema de clasificación de información brasileño sirve al propósito de restringir la información a la necesidad de conocer de los agentes públicos, pero no es herramienta suficiente para proveer transparencia pública.

Palabras clave
Información confidencial; acceso a la información; transparencia pública; clasificación de documentos; fuerzas armadas.

Introdução[1]

O art. 23 da Lei n. 12.527/2011 (Lei de Acesso à Informação [LAI]) estipula a possibilidade de classificação quanto ao sigilo de informações "imprescindíveis à segurança do Estado e da sociedade" (Brasil, 2011a). Ainda, estabelece diferentes graus de restrição para documentos, a depender de sua sensibilidade: a classificação ultrassecreta (25 anos), a secreta (15 anos) e a reservada (5 anos). Entre as motivações para a atribuição de sigilo previstas na legislação estão: aquelas em que sua divulgação pode pôr em risco a defesa e a soberania nacionais ou a integridade do território nacional; colocar em risco a vida, a segurança ou a saúde da população; prejudicar ou causar risco a planos ou operações estratégicos das Forças Armadas (FA); comprometer atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas à prevenção ou à repressão de infrações, entre outras.

As perguntas a que este artigo pretende responder são: como esse tipo de classificação é regulado e gerido nas FA brasileiras? Como isso ocorre tendo em vista a integralidade do processo, desde a habilitação das instituições classificadoras, passando pela atribuição, manutenção, reavaliação e desclassificação do sigilo, pelas formas de controle externo, até as possibilidades de eliminação de documentos já desclassificados?

Devido à sua missão precípua de defesa da pátria, instituições militares precisam gerar e gerir sigilos, dado que a doutrina militar envolve mobilização e emprego de tropas, estratégias para dissuasão, bem como exercícios na carta e de terreno para treinamento de pessoal via ações simuladas de combate; ou seja, geram informações sensíveis que não podem ser automaticamente tornadas públicas. Classificar uma informação como sigilosa é resguardar informações que, se expostas, prejudicariam a condução da política pública em questão e, no limite, comprometeriam a segurança daqueles que se pretende proteger (Colaresi, 2014; Rodrigues, 2020a).

Depreende-se disso que a classificação quanto ao sigilo realizada pelas FA, além de exceção ao princípio da transparência pública, é também um serviço prestado pelo Estado à sociedade.

1 Esta pesquisa é uma extensão da tese de doutorado da autora, a qual teve financiamento do programa Pró-Estratégia da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (Capes). É também fruto de dados coletados pela autora para a consultoria realizada em 2015 para a organização National Security Archive/Open Society Justice Initiative sobre o acesso civil a documentos militares no Brasil. Contou também com financiamento da bolsa Jovem Cientista do Nosso Estado 2021, da Fundação de Amparo à Pesquisa do Estado do Rio de Janeiro (Faperj). A autora agradece aos pareceristas pelos comentários e aos entrevistados pela contribuição. Agradecimentos especiais também àqueles que revisaram as diversas versões deste artigo, a saber: Temístocles Murilo de Oliveira Jr. (Programa de Pós-graduação em Ciências Militares/Escola de Comando e Estado-Maior do Exército [PPGCM/ECEME]), Mariana Montez Carpes (Programa de Pós-Graduação em Ciências Militares/Escola de Comando e Estado-Maior do Exército [PPGCM/ECEME]) e Felipe Azedo Soares.

Como tal, deveria buscar efetividade e eficiência, evitando tanto a "sobreclassificação", que pode esconder ilegalidades, más decisões, bem como aumentar o ônus burocrático de se gerir tais informações, quanto a "subclassificação", que pode expor indevidamente tais informações sensíveis.

Boa parte do debate sobre as informações sigilosas na literatura brasileira teve como foco o acesso à informação como meio para um fim específico, relacionado ao direito à verdade e a uma possível revisão da Lei da Anistia (De Angelo, 2012; Fico, 2012; Lopes; Konrad, 2013; Cunha Filho, 2015; Souza, 2017). O tópico ganhou novo fôlego a partir do governo Bolsonaro, à medida que, ao designar militares da ativa e da reserva a postos-chave do Executivo federal, colocou as FA sob holofotes. Com isso, para além dos trabalhos de Hott (2005), Del Negri (2016), Rodrigues (2017a) e Cruz (2018), recentemente a área também tem debatido o tema sob uma perspectiva distinta, a da transparência da gestão do sigilo na atualidade, com vistas ao aumento de participação e à maior efetividade e controle da ação pública por parte dos cidadãos (Antunes, 2021; Cunha Filho, 2019; Cunha Filho; Antunes, 2021; Rodrigues, 2020a).

Observa-se que as instituições militares resistiram à aprovação da LAI em 2011, que regula o sigilo. A principal resistência girava em torno da continuidade da renovação ilimitada de classificações de sigilo, em especial no nível ultrassecreto; a qual foi vencida com um *lobby* forte da própria presidência, de organizações civis e de veículos jornalísticos (Rodrigues, 2020b). Sabe-se também que a classificação quanto ao sigilo é apenas uma das modalidades de um "regime de exceções de acesso" contido nas LAIs de diversos países (Article 19, 2016; OSJI, 2013; OEA, 2008). Há as exceções relativas a informações pessoais, informações de inteligência, informações sobre projetos de desenvolvimento tecnológico, sigilo judicial, entre outras, que em muitos casos se sobrepõem, nem sempre de forma clara.

Fato é que tais instituições fazem uso intenso do sigilo: de acordo com apuração feita em 2019, "entre junho de 2017 e maio de 2018, 73.281 documentos foram classificados" (Fiquem Sabendo, 2019a). Entre os 12 órgãos federais que mais classificam documentos como sigilosos estão o Comando da Marinha, em primeiro lugar, com mais de 77 mil documentos, e o Comando da Aeronáutica, em segundo lugar, com mais de 14 mil classificações (Cunha Filho; Antunes, 2021).

Para compreender a regulação e a gestão desse tipo de sigilo nas FA, o artigo utiliza análise documental da norma vigente, pedidos de informação por meio da LAI e análise de entrevistas. Dialoga com a regulamentação do sigilo em nível federal (leis, decretos, disposições do Gabinete de Segurança Institucional e do Ministério da Defesa [MD] que tenham incidência sobre as instituições militares) e com os documentos e processos dentro das instituições militares.

O artigo organiza-se da seguinte forma: para além desta introdução, a próxima seção apresenta um breve debate teórico sobre informações sigilosas no contexto das democracias; a segunda delineia os procedimentos metodológicos e de coleta de dados; a terceira traz o

contexto de emergência da legislação vigente; a quarta destrincha a legislação e o processo de gestão das informações sigilosas; e, por último, são apresentadas as conclusões.

1. Democracia, informações sigilosas e classificação de documentos

Em um contexto democrático em que a transparência é regra e o sigilo é exceção (Mendel, 2003), instituições que geram muitos segredos tendem a ser cada vez mais questionadas: "When transparency is prevalent, acts of secrecy are themselves suspicious" (Lord, 2006, p. 9). Como lidar com a necessidade de sigilo de forma consonante com a democracia, em especial, em um subsistema de política pública que a tem como componente estratégico, que é a Defesa Nacional?

Um mecanismo de controle dos segredos de Estado é a classificação de documentos em graus de sigilo. Sua lógica: o valor de uma informação pode ser perdido se esta tornar-se pública em momento inadequado. Contudo, o dano causado pela divulgação da informação tende a decrescer com o tempo, o que permite atribuir níveis de classificação de sigilo, com tempos distintos de restrição. Pressupõe-se que, após esse período, a informação pode se tornar pública sem prejuízos (Thompson, 1999; Rodrigues, 2017b). Diretrizes e *rankings* internacionais sugerem que nenhuma informação seria sensível o suficiente para ser eternamente sigilosa. O *Right to Information Rating,* por exemplo, sugere uma restrição máxima de 20 anos como parâmetro (Rti Rating, [*s.d.*]; OSJI, 2013).

Há, ainda, pesquisadores que argumentam que os segredos de Estado contêm, necessariamente, um potencial antidemocrático e antirrepublicano, já que essas informações "são não apenas desconhecidas, mas também desconhecíveis, ou seja, as pessoas nem ao menos sabem da existência de informações que desconhecem" (Cunha Filho; Antunes, 2020, p. 139), o que se denomina segredo profundo. Isso possibilitaria que, a despeito de uma regulação do sigilo, informações importantes continuassem a ser inacessíveis, sem que fosse possível verificar sua legitimidade democrática.

Essa constatação leva Sagar (2013) a afirmar que talvez o único mecanismo efetivo de controle de segredos de Estado seria o fortalecimento da legislação de proteção a denunciantes em caso de vazamento de dados. Apesar dessa visão, é comum a responsabilização de indivíduos pelos prejuízos causados por vazamentos. Nos Estados Unidos, por exemplo, já houve condenação de alguns jornalistas por isso (Schoenfeld, 2010). Em contraposição aos segredos profundos figurariam os segredos rasos, dos quais se sabe ao menos da existência (Cunha Filho, 2019).

Com isso, a próxima seção delineia os procedimentos metodológicos utilizados para compreender como a normativa brasileira desenha a gestão da classificação de informações sigilosas no Brasil e nas FA.

2. Procedimentos metodológicos

O presente artigo vale-se de análise documental da norma vigente, bem como da análise de cinco pedidos de informação e sete entrevistas. Na coleta de dados, buscou-se a identificação da normativa pertinente; a compreensão da própria normativa; e a percepção dos entrevistados em relação à letra e à prática da normativa. O Quadro 1 mostra a lista de entrevistados.

QUADRO 1 – **Lista de entrevistados**

IDENTIFICADOR	ANO	INSTITUIÇÃO	NOME/CARGO
ENTREVISTA 1	2015	ARQUIVO HISTÓRICO DO EXÉRCITO (AHEX)	MAJ. F. J. DA DIVISÃO DE HISTÓRIA E ACESSO À INFORMAÇÃO (DHAI)
ENTREVISTA 2	2015	DIRETORIA DO PATRIMÔNIO HISTÓRICO E DOCUMENTAÇÃO DA MARINHA (DPHDM)	TENENTE V. ENTÃO ARQUIVISTA RESPONSÁVEL PELO SETOR DE CONSULTAS
ENTREVISTA 3	2015	COMISSÃO MISTA DAS ATIVIDADES DE INTELIGÊNCIA (CCAI)	M. M. ENTÃO SECRETÁRIO DA CCAI
ENTREVISTA 4	2015	CENTRO DE COMUNICAÇÃO SOCIAL DO EXÉRCITO (CCOMSEX) – SERVIÇO DE INFORMAÇÃO AO CIDADÃO (SIC)	CORONEL R1 A. ENTÃO CHEFE DO SERVIÇO DE ACESSO À INFORMAÇÃO (SIC-EB)
ENTREVISTA 5	2015	MINISTÉRIO DA DEFESA (MD) – SERVIÇO DE INFORMAÇÃO AO CIDADÃO (SIC)	M. A. ENTÃO SECRETÁRIA DO COORDENADOR DO SIC
ENTREVISTA 6	2015	ARQUIVO NACIONAL – SEDE NO RIO DE JANEIRO	VITOR FONSECA, ESPECIALISTA EM GERENCIAMENTO DOS ARQUIVOS MILITARES ALOCADOS AO ARQUIVO NACIONAL; SILVIA ESTEVÃO, ARQUIVISTA, RESPONSÁVEL PELO SIC
ENTREVISTA 7	2022	MARINHA BRASILEIRA	OFICIAL SUPERIOR DA MARINHA BRASILEIRA QUE OPTOU POR NÃO SER IDENTIFICADO

Fonte: Elaboração própria.

Os entrevistados foram burocratas implicados no processo de classificação de informações sensíveis e imprescindíveis para a segurança do Estado e da sociedade, dentro das FA e

em instituições que estivessem implicadas na implementação e na formulação da legislação analisada. O Quadro 2 apresenta a relação de pedidos de informação via LAI realizados.

QUADRO 2 – **PEDIDOS DE INFORMAÇÃO REALIZADOS**

IDENTIFICADOR	ANO	CÓDIGO DO PEDIDO	INSTITUIÇÃO	RESUMO DO PEDIDO
PEDIDO 1	2015	08850.000271/ 2015-51	ARQUIVO NACIONAL	PERGUNTOU-SE SE O ARQUIVO NACIONAL TEM COMPETÊNCIA PARA INSPECIONAR ARQUIVOS MILITARES, AVALIAR A DESTRUIÇÃO DE DOCUMENTOS E DEMANDAR A TRANSFERÊNCIA DE ARQUIVOS MILITARES PARA O ARQUIVO NACIONAL.
PEDIDO 2	2015	00077.000098/ 2015-04	GABINETE DE SEGURANÇA INSTITUCIONAL	PERGUNTOU-SE SE O GABINETE DE SEGURANÇA INSTITUCIONAL POSSUI ALGUMA INGERÊNCIA SOBRE A CLASSIFICAÇÃO E DESCLASSIFICAÇÃO DE DOCUMENTOS NAS FORÇAS ARMADAS.
PEDIDO 3	2015	00077.000099/ 2015-41	GABINETE DE SEGURANÇA INSTITUCIONAL	PERGUNTOU-SE SOBRE AS ATIVIDADES DO NÚCLEO DE SEGURANÇA E CREDENCIAMENTO A RESPEITO DAS FORÇAS ARMADAS.
PEDIDO 4	2020	00137.015948/ 2020-76	GABINETE DE SEGURANÇA INSTITUCIONAL	SOLICITOU-SE A LISTA DE ÓRGÃOS PÚBLICOS QUE POSSUEM ACREDITAÇÃO PARA CLASSIFICAR DOCUMENTOS NOS NÍVEIS 1 E 2.
PEDIDO 5	2020	60141.000661/ 2021-95	COMANDO DA AERONÁUTICA	SOLICITOU-SE A ÚLTIMA VERSÃO DA INSTRUÇÃO NORMATIVA RELATIVA À SALVAGUARDA DE DOCUMENTOS SIGILOSOS.

Fonte: Elaboração própria.

Parte das entrevistas e dos pedidos de informação foi realizada em 2015, para pesquisa de consultoria não publicada, a qual foi atualizada por meio de análise adicional. Buscou-se realizar entrevistas adicionais, no ano de 2022, o que foi feito com a Marinha. Não se encontrou militares do Exército ou da Aeronáutica dispostos a conceder entrevistas.

3. Antecedentes da atual legislação sobre informações sigilosas no Brasil

O caso brasileiro ilustra a tensão entre instituições militares e leis de transparência. Tanto Rodrigues (2020b) quanto Cunha Filho (2019) identificam o envolvimento de instituições ligadas à Defesa Nacional na resistência ao projeto de lei que se tornou, posteriormente, a LAI. O debate sobre a regulação de informações sigilosas tornou-se vórtice de atenções de ambos os lados a partir de 2002, quando o então presidente Fernando Henrique Cardoso (1995-2002) assinou um decreto que autorizava a reclassificação de documentos por um número indefinido de vezes (Hott, 2005; Rodrigues, 2020b). Antes desse decreto, conhecido como "decreto do sigilo eterno", vigorava o chamado "decreto de acesso" (Decreto n. 2.134/1997 [Brasil, 1997]), cujo conteúdo inaugurou alguns (mas ainda insuficientes) procedimentos de acesso a informações produzidas pelo Estado.

No governo de Luís Inácio Lula da Silva (2003-2011), diante de reações da base governista, o presidente outorgou medida provisória que se tornaria a Lei n. 11.111/2005 (Brasil, 2005), que persistia na renovação ilimitada de classificações de sigilo. Somente em 2009 Lula apresentou à Câmara dos Deputados uma proposta de lei mais progressista; tal proposta deu origem à Lei n. 12.527/2011 (Brasil, 2011a), chamada de LAI, aprovada no governo de Dilma Rousseff (2011-2016) (Angélico, 2012; Rodrigues, 2020b).

A partir da LAI lançaram-se os Decretos n. 7.724/2012 (Brasil, 2012a) e n. 7.845/2012 (Brasil, 2012b). O primeiro traz a regulamentação direta da LAI, cuja última atualização realizou-se em 2023; o segundo versa especificamente sobre o credenciamento e a gestão de documentos classificados como sigilosos ou de acesso restrito. Com base nessa regulamentação, as FA puderam gerar ou atualizar suas portarias internas com determinações sobre o tema, como as instruções gerais da Marinha ((EMA-414/2013 [Brasil, 2013a]), do Exército (IGSAS/2014 [Brasil, 2014a]) e da Aeronáutica (ICA 205-47/2015 [Brasil, 2015a]). O Quadro 3 traz a legislação considerada neste artigo.

QUADRO 3 – **Legislação vigente em 2023 sobre a classificação de documentos na esfera federal e nas FA brasileiras**

NORMATIVA E DATA	NOME OU DESCRIÇÃO	ABRANGÊNCIA
LEI N. 12.527 (2011)	LEI DE ACESSO À INFORMAÇÃO (LAI)	OS TRÊS PODERES, ESFERAS FEDERAL, ESTADUAL E MUNICIPAL
DECRETO N. 7.724 (2012), ATUALIZADO EM 2023	DECRETO REGULAMENTADOR DA LAI	PODER EXECUTIVO FEDERAL

(continua)

NORMATIVA E DATA	NOME OU DESCRIÇÃO	ABRANGÊNCIA
DECRETO N. 7.845 (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	PODER EXECUTIVO FEDERAL
LEI N. 8.159 (1991)	LEI DE ARQUIVOS PÚBLICOS E PRIVADOS	OS TRÊS PODERES, ESFERAS FEDERAL, ESTADUAL E MUNICIPAL
RESOLUÇÃO N. 40 (2014)	DISPÕE SOBRE OS PROCEDIMENTOS PARA A ELIMINAÇÃO DE DOCUMENTOS NO ÂMBITO DOS ÓRGÃOS E DAS ENTIDADES INTEGRANTES DO SISTEMA NACIONAL DE ARQUIVOS (SINAR)	OS TRÊS PODERES, ESFERAS FEDERAL, ESTADUAL E MUNICIPAL
PORTARIA N. 154 DO MINISTÉRIO DA DEFESA (2013)	CÓDIGO DE CLASSIFICAÇÃO E TABELA DE TEMPORALIDADE E DESTINAÇÃO DE DOCUMENTOS DE ARQUIVOS RELATIVOS ÀS ATIVIDADES-FIM DO MINISTÉRIO DA DEFESA	MINISTÉRIO DA DEFESA, COMANDO DO EXÉRCITO, COMANDO DA AERONÁUTICA, COMANDO DA MARINHA
PORTARIA DO COMANDANTE DO EXÉRCITO N. 1.067 (2014)	INSTRUÇÃO GERAL PARA SALVAGUARDA DE ASSUNTOS SIGILOSOS (IGSAS) (EB10-IG-01.012)	COMANDO DO EXÉRCITO
PORTARIA DO COMANDO DO EXÉRCITO N. 1.702 (2019)	INSTRUÇÕES GERAIS PARA AVALIAÇÃO DE DOCUMENTOS DO EXÉRCITO (EB10-IG-01.012), 3ª EDIÇÃO	COMANDO DO EXÉRCITO
PORTARIA DO COMANDO DO EXÉRCITO N. 012 (2015)	INSTRUÇÕES GERAIS PARA AVALIAÇÃO E CONTROLE DE DOCUMENTOS CLASSIFICADOS (IGACDC) (EB10-IG-01.015)	COMANDO DO EXÉRCITO
SEM INDICAÇÃO DE PORTARIA. PUBLICADO EM 2013	EMA-414 – NORMAS PARA A SALVAGUARDA DE MATERIAIS CONTROLADOS, INFORMAÇÕES, DOCUMENTOS E MATERIAIS SIGILOSOS NA MARINHA (1ª REVISÃO)	COMANDO DA MARINHA
SEM INDICAÇÃO DE PORTARIA. PUBLICADO EM 2018	NORMAS SOBRE DOCUMENTAÇÃO ADMINISTRATIVA E ARQUIVAMENTO NA MARINHA (NODAM) (SGM-105/2018) (5ª REVISÃO)	COMANDO DA MARINHA
PORTARIA DO COMANDANTE DA AERONÁUTICA N. 1869/GC3 (2015)	INSTRUÇÃO PARA SALVAGUARDA DE ASSUNTOS SIGILOSOS (ISAS)	COMANDO DA AERONÁUTICA
PORTARIA DO COMANDANTE DA AERONÁUTICA N. 1.180/GC3 (2013)	ICA 200-12 – AVALIAÇÃO DE DOCUMENTOS CLASSIFICADOS NO COMANDO DA AERONÁUTICA	COMANDO DA AERONÁUTICA
PORTARIA COMGEP N. 188/ALE (2021)	NSCA 214-1/2021 – GESTÃO DE DOCUMENTOS DE ARQUIVO NO ÂMBITO DO COMAER	COMANDO DA AERONÁUTICA
PORTARIA COMGEP N. 1.024/ CPADAER (2011)	ICA 214-3 – AVALIAÇÃO DE DOCUMENTOS DE ARQUIVO	COMANDO DA AERONÁUTICA

Fonte: Elaboração própria.

A LAI não tem precedência sobre outras legislações que regulam sigilo. De acordo com o Entrevistado 5 do MD, em 2015, a LAI está "ao lado" de outras legislações, não necessariamente em consonância com todos os aspectos. De fato, o art. 22 da LAI (Brasil, 2011) estipula que a lei não regula restrições como as de confidencialidade fiscal, segredo industrial, entre outras. Alguns tipos particulares de restrição também têm sido o foco de diversos questionamentos por parte da mídia e de organizações da sociedade civil, uma vez que não são claramente regulados, como é o caso das informações pessoais e das informações de inteligência. As informações sigilosas, por sua vez, têm como legislação principal a LAI e os decretos de 2012, que estipulam tempos-limite de retenção de documentos e os procedimentos para contestação e revisão de classificação – mesmo mantendo diversas ambiguidades. A próxima seção traz um retrato esmiuçado desse processo.

4. Regulamentação e gestão de informações classificadas como sigilosas no Brasil

Esta seção tem como objetivo analisar a legislação vigente que permeia a classificação de documentos como sigilosos pelo Estado, sob a justificativa de serem imprescindíveis para a segurança do Estado e da sociedade, no âmbito das instituições militares do país. A análise dialoga com a regulamentação dos segredos de Estado em nível federal (leis, decretos, disposições do Gabinete de Segurança Institucional [GSI] e do MD, desde que tenham incidência sobre as instituições militares) e com a regulamentação específica das FA.

Analisa-se todo o ciclo de classificação quanto ao sigilo: (1) habilitação de instituições; (2) regras básicas: níveis, autoridades e motivos; (3) processo de classificação e gestão interna; (4) transparência e controle de documentos classificados; (5) reavaliação, reclassificação e desclassificação de documentos; e (6) eliminação, arquivamento e publicização de documentos desclassificados.

4.1. Habilitação de instituições

A LAI e o Decreto n. 7.845/2012 (Brasil, 2012b) estabelecem a criação de um Núcleo de Segurança e Credenciamento (NSC) dentro do GSI, responsável por acreditar instituições com necessidade de lidar com documentos restritos. Para que um servidor ou cidadão em exercício de cargo público possa atribuir grau de sigilo a uma instituição, esta deve ser habilitada pelo NSC. Há dois níveis de acreditação de instituições, o nível um e o nível dois. São seis os órgãos do governo federal habilitados no nível um: GSI; MD; Ministério das Relações Exteriores (MRE); Casa Civil da Presidência da República (CC-PR); Ministério da Justiça e Segurança Pública (MJSP); e Controladoria-Geral da União (CGU) (pedidos de informação 3 e 5). De acordo com o Decreto n. 7.845/2012, art. 3º, V e VI (Brasil, 2012b), o NSC tem poder de monitorar e inspecionar quaisquer atividades das instituições acreditadas – dispositivo que não é, de fato, utilizado, de acordo com os Entrevistados 1 e 2.

A habilitação de nível dois é concedida pelo órgão habilitado no nível um, não tendo o GSI controle sobre a subsequente concessão dessas habilitações. Cada Força obtém habilitação para classificar por meio da habilitação do MD e, em cada uma delas, há normas específicas para regular o processo de classificação. O documento que as estabelece no Exército é a Instrução Geral para Salvaguarda de Assuntos Sigilosos (IGSAS), aprovada pela Portaria do Comandante do Exército n. 1.067, de 2014 (Brasil, 2014a) (Entrevista 4); na Marinha, é o EMA-414 – publicado em 2005 e revisto em 2013 (Brasil, 2013); e na Força Aérea é a Instrução para a Salvaguarda de Assuntos Sigilosos da Aeronáutica (ISAS), aprovada pela Portaria n. 1869/GC3, de 2015 (Brasil, 2015a). Quem tem o poder de atualizar portarias e instruções normativas relacionadas à classificação e desclassificação de documentos é apenas o comandante de cada uma das Forças.

4.2. Regras básicas: níveis, autoridades e motivos

A principal legislação que determina regras para a classificação de documentos quanto ao nível de sigilo no Brasil é a LAI. Antes dela, o Brasil contava com quatro níveis distintos: restrito (5 anos), confidencial (10 anos), secreto (15 anos) e ultrassecreto (25 anos) (Lei n. 11.111/2005 [Brasil, 2005]). A decisão pela extinção do nível confidencial teve o intuito de reduzir o número de documentos classificados, obrigando as burocracias a "reclassificarem para baixo" (Entrevistado 1), ou seja, de 10 para 5 anos.

O art. 23 da LAI delineia as motivações pelas quais se pode classificar documentos. Os tópicos são:

> Art. 23. São consideradas imprescindíveis à segurança da sociedade ou do Estado e, portanto, passíveis de classificação as informações cuja divulgação ou acesso irrestrito possam:
> **I – pôr em risco a defesa e a soberania nacionais ou a integridade do território nacional**;
> II – prejudicar ou pôr em risco a condução de negociações ou as relações internacionais do País, **ou as que tenham sido fornecidas em caráter sigiloso por outros Estados e organismos internacionais**;
> III – pôr em risco a vida, a segurança ou a saúde da população;
> IV – oferecer elevado risco à estabilidade financeira, econômica ou monetária do País;
> **V – prejudicar ou causar risco a planos ou operações estratégicos das Forças Armadas**;
> **VI – prejudicar ou causar risco a projetos de pesquisa e desenvolvimento científico ou tecnológico, assim como a sistemas, bens, instalações ou áreas de interesse estratégico nacional**;
> VII – pôr em risco a segurança de instituições ou de altas autoridades nacionais ou estrangeiras e seus familiares; ou
> **VIII – comprometer atividades de inteligência, bem como de investigação**

> **ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações** (Brasil, 2011, grifo nosso).

Nos documentos analisados não há tipos de informação que devam ser classificados *a priori* – o que é um ponto positivo em comparação a leis que classificam automaticamente determinados tipos de documentos ou informações (Mendel, 2008).

De acordo com os Entrevistados 1, 2 e 7, a classificação depende em muito da discricionariedade da autoridade classificadora. O Entrevistado 7 afirma que a decisão é discricionária porque não só critérios técnicos são levados em consideração, mas também os políticos: há o cuidado de não disponibilizar informações que possam "macular a imagem" da instituição ou da Defesa Nacional. O Entrevistado 1 afirmou que antes da LAI era mais fácil classificar documentos, visto que as regras para se conceder credenciais de classificação eram mais flexíveis. A LAI criou novos processos burocráticos, gerando acúmulo de trabalho para os chefes de Organizações Militares (OMs). Como resultado, há mais documentos classificados no nível mais baixo de sigilo (nível reservado).

As instruções normativas das FA são mais específicas em relação à LAI quanto aos tipos de informação a serem classificados em cada um dos níveis de sigilo. A redação da IGSAS/2014 (Exército), EMA-414/2013 (Marinha) e ICA 205-47/2015 (Aeronáutica) é similar. De acordo com esses documentos, os *tipos de informação* que devem ser classificados como *ultrassecretos* são: informações que possam pôr em risco a soberania e a integridade territorial nacionais; os planos e as operações militares; as relações do país com outros países; os projetos de pesquisa e desenvolvimento científico e tecnológico de interesse da defesa nacional; e os programas e os planos econômicos.

No nível *secreto* de classificação, entram os seguintes tópicos: sistemas, instalações, programas, projetos, planos ou operações de interesse da Defesa Nacional; questões relacionadas à diplomacia e à inteligência, planos e seus detalhes, bem como programas e instalações estratégicas. Já no nível *reservado*, figuram: objetivos de interesse do Poder Executivo, objetivos e atividades da Força ou do comandante da Força, que possam comprometer atividades de inteligência, de investigação ou de fiscalização de infrações, bem como informações que possam colocar em risco a segurança do presidente, vice-presidente e respectivos filhos e cônjuges.

Há informações que não são passíveis de classificação, mas podem ter seu acesso restrito de outras maneiras (art. 22 da LAI [Brasil, 2011]). A LAI também estipula que quaisquer documentos que comprovem violação de direitos humanos não podem ser mantidos sob sigilo em hipótese alguma (art. 21, parágrafo único [Brasil, 2011]) – apesar de não estabelecer mecanismos claros de averiguação.

A classificação geralmente é feita na ocasião da criação do documento. Contudo, e conforme os resultados de pesquisa de Cunha Filho e Antunes (2020), há casos de recursos de pedidos de informação que, ao chegarem à CGU, tiveram os documentos em questão classificados

tardiamente, visto que somente por meio da provocação é que a entidade classificadora percebeu o documento como sensível. Isso é evidência de uma subclassificação de documentos.

Ao atribuir o grau de sigilo, gera-se um Termo de Classificação de Informação (TCI), documento que explica o motivo da classificação. Antes, o TCI ganhava o mesmo nível de sigilo da informação classificada, impossibilitando conhecer a motivação da classificação durante sua vigência. Contudo, o Decreto n. 11.527/2023 (Brasil, 2023b) inovou ao estipular mudanças na redação do Decreto n. 7.724/2012, adicionando a necessidade de se registrar no TCI "a descrição de elementos mínimos que permitam a identificação do tema de que se trata a classificação" (Brasil, 2012a), restringindo os chamados "segredos profundos".

A classificação *ultrassecreta* pode ser atribuída pelo presidente, pelo vice-presidente, pelos ministros de Estado e pelas autoridades com as mesmas prerrogativas, por comandantes da Marinha, da Aeronáutica e do Exército, e por diretores de missões diplomáticas no exterior. Essas classificações devem ser informadas dentro de 30 dias ao MD, à Comissão Mista de Reavaliação de Informações (CMRI) e à CGU.

A classificação *secreta* pode ser concedida a documentos pelas autoridades mencionadas para a classificação ultrassecreta e por diretores de autarquias do Estado, fundações, empresas públicas e corporações semipúblicas, conforme estipulado pela própria LAI.

Já a classificação de nível *reservado* pode ser determinada pelas autoridades mencionadas nos níveis ultrassecreto e secreto e por servidores que exercem atividades de direção, comando de chefias ou hierarquia equivalente. É obrigatório que o classificador dê ciência da classificação ao comandante da Força em um prazo de 90 dias e é vedada a subdelegação da capacidade de classificar na Marinha e na Aeronáutica.

Quanto à delegação da autoridade para classificar, isso é possível na LAI para os níveis ultrassecreto e secreto, que "poderá ser delegada pela autoridade responsável a agente público, inclusive em missão no exterior" (art. 27, § 1º [Brasil, 2011]). Entretanto, o Decreto n. 7.724/2012 é categórico na vedação dessa delegação em seu art. 30, § 1º, para os graus de sigilo ultrassecreto e secreto. A interpretação das instruções normativas das FA seguiu o estipulado pelo decreto, sem menção à disposição do art. 27 da LAI (Brasil, 2011). As classificações ultrassecretas e secretas são competência de um número reduzido de oficiais (Entrevistado 7), o que gera morosidade no processo devido a um acúmulo de funções nesses postos.

A LAI é silente sobre a delegação de autoridade de classificação no nível reservado, mas o Decreto n. 7.724/2012 autoriza a delegação (art. 30, § 2º [Brasil, 2012a]), fazendo-a possível ao dirigente máximo da instituição a "agente público que exerça função de direção, comando ou chefia". Exército e Aeronáutica, apesar do estipulado no decreto regulamentador da LAI, vedam a delegação nesse nível. Na Marinha, é facultada àqueles com credenciais para classificar no nível reservado a delegação para ocupantes de cargos de assessoramento superior e assistência imediata ao comandante da Marinha, bem como oficiais e servidores civis em função de chefia, comando ou direção. Em todos os casos é vedada a subdelegação.

4.3. Gestão interna do documento classificado com grau de sigilo

Como mencionado anteriormente, no ato da classificação é gerado o TCI, que contém as seguintes informações (art. 31 do Decreto n. 7.724/2012 [Brasil, 2012a], atualizado em 2023): código de indexação de documento; grau de sigilo; categoria na qual se enquadra a informação; tipo de documento; data da produção do documento; indicação de dispositivo legal que fundamenta a classificação; razões da classificação; assunto a que se refere a classificação (escrito de forma a ser publicizado), indicação do prazo de sigilo, contado em anos, meses ou dias, ou do evento que defina o seu termo final; data da classificação; e identificação da autoridade que classificou a informação. O autor da classificação pode ser rastreado via TCI.

Quando um documento é classificado como sigiloso, gera-se uma lista de pessoas e instituições com *necessidade de conhecer* o documento, o que é feito por meio do sistema interno de gestão de documentos de cada uma das Forças (Entrevistado 7; ENAP, 2018). Nas instruções normativas das FA, a necessidade de conhecer é definida como "condição pessoal, inerente ao efetivo exercício de cargo, da função, do emprego ou da atividade, indispensável para que uma pessoa tenha acesso à informação classificada ou sob restrição de acesso" (Brasil, 2014a, art. 2º, XI).

A necessidade de conhecer é critério fundamental para se ter acesso a um documento classificado, ou seja, um oficial pode ter credenciais de segurança que o habilitam a ter acesso a documentos classificados como secretos e ultrassecretos, mas tal habilitação não dá acesso automático a todos os documentos classificados nesses níveis – ambas as condições devem ser preenchidas. No caso de necessidade de acesso a documentos classificados por parte de órgãos de controle externo, como o Tribunal de Contas da União (TCU), registram-se os nomes dos auditores que terão acesso aos documentos, para controle e possível responsabilização por uso indevido das informações (Entrevistado 7).

Para o compartilhamento de dados sigilosos, a rede utilizada é a Rede Mercúrio – a mesma para as três Forças. Para os demais documentos, cada uma das FA tem seu próprio sistema: o da Marinha é o Sistema de Gerência de Documentos Eletrônicos da Marinha (SiGDEM); o do Exército é o Sistema de Protocolo Eletrônico de Documentos (SPED); e o da Aeronáutica é o Sistema Informatizado de Gestão Arquivística de Documentos da Aeronáutica (SIGADAER) (Martins, 2020). As FA não usam o Sistema Eletrônico de Informações (SEI) do governo federal (Entrevistado 7), visando à segurança informacional nos casos de potencial subclassificação de documentos.

A cada órgão ou entidade é facultada a criação de uma Comissão Permanente de Avaliação de Documentos Sigilosos (CPADS) (art. 34 do Decreto n. 7.724/2012 [Brasil, 2012a]). É permitido que essas comissões criem subcomissões e para a sua formação deverá haver designação formal do presidente da comissão, de membros e suplentes, estipulando responsabilidades, atuação e periodicidade de reuniões. As CPADSs não classificam informações, mas assessoram as autoridades classificadoras quanto à desclassificação, reclassificação ou classificação de documentos em todos os graus de sigilo. Ainda, preocupam-se com o resguardo

arquivístico dos documentos, que devem seguir a Tabela de Temporalidade do MD. As CPADSs devem atuar em consonância com a comissão responsável pelos arquivos, a chamada Comissão Permanente de Avaliação de Documentos (CPAD), instituída pelo Decreto n. 4.073/2002 (Brasil, 2002) (ENAP, 2018).

A Aeronáutica possui documento que detalha as atividades das CPADSs – a ICA 200-12/2013 (Brasil 2013b) –, que determina os chefes de quais OMs poderão constituir as comissões. Estipula-se uma estrutura mínima para elas, com um oficial superior com posto de coronel para a presidir, dois oficiais superiores como membros e dois graduados para atuar como auxiliares, dando-se preferência na composição para o chefe do arquivo geral e o chefe do setor de inteligência da OM na qual a comissão será criada.

O documento estabelece ainda as principais competências das CPADSs, nas quais se incluem avaliações periódicas semestrais dos documentos, sempre nos meses de abril e outubro, para aqueles documentos cuja classificação se encontra próxima da expiração. A partir dessa avaliação, a comissão sugere a renovação de classificação, reclassificação ou desclassificação; supervisiona as subcomissões de organizações militares subordinadas; e elabora a lista de documentos classificados e desclassificados que comporá a transparência ativa da seção da LAI no *site* da Força Aérea. As *subcomissões* devem ser compostas também de uma estrutura mínima, que conte com um oficial superior como presidente e, quando possível, dois oficiais intermediários como membros e um graduado como auxiliar (ICA).

As CPADSs da Aeronáutica enviam seus relatórios de avaliação de documentos sigilosos para os comandantes, chefes, secretários ou diretores das organizações militares, os quais devem ser homologados por tais autoridades. Quando desclassificados, os documentos são enviados às Subcomissões Permanentes de Avaliação de Documentos da Aeronáutica (SPADAERs), que aplicam a Tabela de Temporalidade arquivística. No caso de documentos com informações pessoais, apesar da desclassificação, a instrução prevê o prosseguimento da restrição de acesso "por até 100 anos".

No Exército, as competências das CPADSs são as mesmas, mas há diferenças nos requisitos de sua composição, de acordo com as Instruções Gerais para Avaliação e Controle de Documentos Classificados (IGACDC) (EB10-IG-01.015). No documento, determina-se a localização da CPADS dentro do Centro de Inteligência do Exército (CIE), estipulando-se que essas comissões devem contar com um coronel do CIE na presidência; um coronel ou tenente-coronel do mesmo centro como primeiro membro; e um coronel ou tenente-coronel do Estado-Maior do Exército como segundo membro (art. 6º da Instrução Normativa [Brasil, 2015b]).

Diferentemente da Força Aérea, o Exército estabelece diferentes níveis hierárquicos para suas subcomissões de avaliação e controle de documentos classificados (art. 8º [Brasil, 2015b]). No nível "A", figuram as subcomissões das seguintes organizações: Estado-Maior do Exército, órgãos de assistência direta e imediata ao comandante do Exército, órgãos de direção setorial e comandos militares de área. No nível "B", figuram as divisões de Exército, regiões militares, grupamentos de engenharia e grupamentos logísticos, diretorias, centros,

estabelecimentos de ensino e institutos diretamente subordinados aos órgãos de direção setorial. Já no nível "C", incluem-se brigadas, artilharias divisionárias, comando de aviação do Exército, comando de operações especiais, comando de artilharia do Exército, base de apoio logístico do Exército, estabelecimentos de ensino não diretamente subordinados aos órgãos setoriais de direção, unidades e subunidades independentes. De acordo com o nível da subcomissão, diferentes critérios de composição são estabelecidos (art. 9º [Brasil, 2015b]), sendo vedada a participação de oficiais ou sargentos temporários.

Há, ainda, um calendário de atividades que inclui a listagem de documentos classificados nos três níveis até dia 1º de abril de cada ano; a reavaliação e a desclassificação de documentos até 1º de maio pelas subcomissões; o envio do rol de documentos reavaliados e desclassificados para o Estado-Maior do Exército até dia 15 de maio pela comissão (Anexo F do IGACDC).

Na Marinha, o detalhamento sobre a atuação das CPADSs encontra-se na EMA-414 e, tangencialmente, nas Normas sobre Documentação Administrativa e Arquivamento na Marinha (NODAM) (SGM-105/2018). O primeiro documento estipula (cap. 5) que a CPADSM deverá ser constituída por um oficial-general na presidência e por dois membros que sejam oficiais superiores do Estado-Maior. A CPADSM é responsável por responder a recursos de 1ª instância relativos a informações sigilosas. De acordo com o Entrevistado 7, a atuação das CPADSMs foi facilitada pela informatização da gestão de documentos.

As subcomissões, por sua vez, podem ser criadas

> a) pelos titulares dos Órgãos de Direção Setorial, nas suas áreas de atuação; b) pelo Vice-Chefe do Estado-Maior da Armada, no âmbito do Órgão de Direção Geral e OM subordinadas; e c) pelo Chefe de Gabinete do Comandante da Marinha, no âmbito dos órgãos de assessoramento e vinculados, dos Conselhos e Comissões do Comandante da Marinha e do Almirantado (Brasil, 2013a).

Quando uma OM possui documentos classificados como sigilosos, surge a necessidade de se criar ambientes de acesso restrito que resguardem o conteúdo dos documentos. Para sua guarda em meio eletrônico, é obrigatório o uso de recursos criptográficos e, no caso de documentos não eletrônicos, meios e equipamentos que promovam sua segurança, com pequenas variações de procedimento de acordo com o nível de classificação.

4.4. Transparência vertical e controle externo

Nesta seção cabe destacar dois aspectos importantes dos sistemas de classificação de documentos em ambientes democráticos: a transparência vertical, voltada para a sociedade como um todo; e o controle externo, que tem como pilares a transparência e a *accountability* horizontais (Hood; Heald, 2006). Quanto menor for a possibilidade de transparência vertical, maior é a necessidade de transparência horizontal para que um sistema de classificação de documentos ganhe legitimidade democrática (Rodrigues, 2020a).

No sentido da transparência vertical, art. 30, I, da LAI (Brasil, 2011) determina a publicação anual de uma lista com todos os documentos classificados e desclassificados em cada um dos órgãos federais. Essa publicização restringe-se a algumas poucas informações constantes no Código de Indexação de Documento que contém Informação Classificada (CIDIC) (arts. 50 a 52 do Decreto n. 7.845/2012 [Brasil, 2012b]).

As informações contidas no CIDIC são as seguintes: Número Único de Protocolo (NUP), que é o que resta do CIDIC quando o documento é desclassificado; indicação de grau de sigilo, sendo "U" para ultrassecreto, "S" para secreto e "R" para reservado, em vermelho; código com a categoria relativa que, para a Defesa Nacional, é a categoria 5; data da produção da informação classificada; data de desclassificação da informação; indicação de reclassificação do documento, assinalada com um "S" para positivo e "N" para negativo; e, no caso de renovação da classificação, data prevista de desclassificação.

Quanto à transparência e à *accountability* horizontais, dois atores se destacam: a CGU e a CMRI. O questionamento de classificação de documentos pela via judicial não é prática comum no Brasil, apesar de o ser nos Estados Unidos – país este em que é recorrente a decisão favorável ao sigilo pelo Judiciário (Cunha Filho; Antunes, 2020; Sagar, 2013). Ademais, mesmo sendo o GSI o responsável por fornecer credenciais de classificação a outros órgãos (conforme seção 4.1), ele não controla a classificação de documentos em cada uma das forças ou dentro do MD (pedido de informação 2).

A CMRI é criada no art. 35, § 1º, da LAI (Brasil, 2011), como órgão colegiado interministerial, com o poder de estabelecer orientações legais, criando jurisprudência para futuras decisões da comissão. Essa comissão é a última instância de recursos diante de negativas de acesso a pedidos feitos via LAI; é responsável por decidir sobre a desclassificação de sigilo de documentos; e revisa a classificação do sigilo ultrassecreto, independentemente do autor da classificação (A última palavra [...], 2020).

O art. 46 do Decreto n. 7.724/2012 (Brasil, 2012a), com alterações advindas do Decreto n. 11.489/2023 (Brasil, 2023a), determina como composição da comissão um representante de cada uma das seguintes instituições: Casa Civil (que preside a comissão), Advocacia-Geral da União, CGU, GSI, MD, Ministério dos Direitos Humanos e da Cidadania, Ministério da Fazenda, Ministério da Gestão e da Inovação em Serviços Públicos, MJSP e MRE.

A CMRI tem sido requisitada no provimento de decisões sobre a classificação de documentos e pode obter acesso integral aos documentos quando o TCI não provê informações suficientes para embasar a decisão. Contudo, para além de instância recursal, a CMRI possui prerrogativa exclusiva na determinação da renovação de um documento ultrassecreto (ENAP, 2018).

4.5. Reavaliação, reclassificação e desclassificação de sigilo

Quando se reavalia a classificação de sigilo de um documento, pode-se: (1) reclassificar o documento no mesmo nível de sigilo; (2) reclassificar o documento em um nível inferior (nunca superior) de sigilo; ou (3) desclassificar o documento.

Somente informações classificadas primariamente como ultrassecretas podem ser reclassificadas no mesmo nível de sigilo (art. 35, § 2º, da LAI [Brasil, 2011] e art. 47 do Decreto n. 7.724/2012 [Brasil, 2012a]). A CMRI possui prerrogativa exclusiva na determinação da renovação de classificação de documentos ultrassecretos. Já na reclassificação de documento em nível de sigilo inferior (Decreto n. 7.724/2012, art. 35 [Brasil, 2012a]), as classificações nos níveis secreto e reservado não podem ser renovadas no mesmo nível de sigilo, tendo a reavaliação o objetivo de diminuir o grau de sigilo ou desclassificar o documento.

A periodicidade da análise de documentos sigilosos nos níveis ultrassecreto e secreto é definida no art. 35 da LAI (§ 3º): "A revisão de ofício [...] deverá ocorrer, no máximo, a cada 4 (quatro) anos, após a reavaliação prevista no art. 39 [...]" (Brasil, 2011).

A partir dessas regras, o tempo máximo de classificação permitido pela legislação brasileira é de 50 anos para informações classificadas como ultrassecretas, e renovadas no mesmo nível de classificação. Para documentos originalmente classificados como secretos, o tempo máximo é de uma renovação para o nível reservado, ou seja, 20 anos (15 anos como secreto e mais 5 anos como reservado). O Quadro 4 traz projeções de desclassificação para documentos sigilosos a partir de 1975.

QUADRO 4 – **PROJEÇÕES DE DESCLASSIFICAÇÃO PARA DOCUMENTOS CLASSIFICADOS A PARTIR DE 1975**

CLASSIFICADO INICIALMENTE COMO	ANO DE CLASSIFICAÇÃO	1975	1980	1985	1990	1995	2000	2005	2010	2015	2020
ULTRASSECRETOS	*SEM RENOV.*	2000	2005	2010	2015	2020	2025	2030	2035	2040	2045
	RECLASS. R	2005	2010	2015	2020	2025	2030	2035	2040	2045	2050
	RECLASS. S	2015	2020	2025	2030	2035	2040	2045	2050	2055	2060
	RENOV. U	2025	2030	2035	2040	2045	2050	2055	2060	2065	2070
SECRETOS	*SEM RENOV.*	1990	1995	2000	2005	2010	2015	2020	2025	2030	2035
	RECLASS. R	1995	2000	2005	2010	2015	2020	2025	2030	2035	2040
RESERVADOS	*SEM RECLASS.*	1980	1985	1990	1995	2000	2005	2010	2015	2020	2025

LEGENDA: U = ULTRASSECRETO; S = SECRETO; R = RESERVADO; RENOV. = RENOVAÇÃO DA CLASSIFICAÇÃO; EM CINZA = INFORMAÇÕES DE ACESSO AINDA RESTRITO AO PÚBLICO NOS ANOS DE CLASSIFICAÇÃO INDICADOS, CONSIDERADO O ANO DE PUBLICAÇÃO DO PRESENTE ARTIGO.

Fonte: Elaboração própria.

Há em cada uma das FA orientações adicionais acerca da desclassificação quanto ao sigilo, nos já mencionados documentos: IGSAS (Exército), EMA-414 (Marinha) e ISAS (Força Aérea). Nesses documentos, estipula-se que os originais classificados nos graus de sigilo secreto e ultrassecreto são de guarda permanente, não podendo ser eliminados; diferentemente dos documentos classificados como reservados, que podem ser eliminados caso não possuam valor para consulta posterior. O parágrafo único do art. 47 do Decreto n. 7.724/2012 (Brasil, 2012a) também determina uma desclassificação automática de documentos caso essa revisão não ocorra.

Qualquer cidadão, via provocação, e a própria CMRI, via ofício, podem pedir a revisão da classificação quanto ao sigilo de um documento (art. 29 da Lei n. 12.527/2011 e art. 36 do Decreto n. 7.724/2012). O art. 19, II, do Decreto n. 7.724 estipula que os "órgãos e entidades disponibilizarão formulário padrão para apresentação de recurso e de pedido de desclassificação" (Brasil, 2012a). O art. 17 da Lei n. 12.527/2011 (Brasil, 2011) e o art. 37 do Decreto n. 7.724/2012 (Brasil, 2012a) trazem especificidades no que tange a esse processo nas instituições militares.

No caso das FA, envia-se pedido de reavaliação de classificação primeiro à autoridade classificadora, que tem um prazo de 30 dias para responder (ICA 205-47/2015). Negado o acesso, o requerente pode encaminhar recurso, no prazo de 10 dias a contar da resposta, para o comandante da Força; persistindo a negativa, pode-se encaminhar recurso ao MD, que possui mais 30 dias para responder. Diante de outra negativa, resta apresentar recurso à CMRI em até 10 dias a partir da decisão do MD.

Esse processo não se confunde com os pedidos de informação nas plataformas da LAI. Quando um cidadão requer informações via LAI e considera a resposta insuficiente, há três instâncias recursais disponíveis: a autoridade superior do órgão, a CGU e a CMRI. Quando do prosseguimento do recurso pelo cidadão até a CGU, o órgão só dá prosseguimento à petição se "a decisão de negativa de acesso à informação total ou parcialmente classificada como sigilosa não indicar a autoridade classificadora ou a hierarquicamente superior a quem possa ser dirigido pedido de acesso ou desclassificação" (art. 16, parágrafo II da LAI [Brasil, 2011]) e quando "os procedimentos de classificação de informação sigilosa estabelecidos nesta Lei não tiverem sido observados" (art. 16, III, da LAI [Brasil, 2011]).

Se os procedimentos de classificação estiverem corretos, a CGU encerra, sem análise de mérito, o processo dentro do canal de comunicação na plataforma Fala.Br, já que o órgão não tem competência para reavaliar documentos classificados como sigilosos (art. 52 da Lei n. 9.784/1999 [Brasil, 1999],[2] subsidiariamente aplicado diante do art. 75 do Decreto n. 7.724/2012 [Brasil, 2012a]). Nesses casos, deverá ser indicado o envio dos formulários de pedido de desclassificação no processo descrito anteriormente (ENAP, 2018).

2 Regula o processo administrativo no âmbito da Administração Pública Federal.

No entanto, Cunha Filho e Antunes (2020) mostram que na tramitação regular de pedidos de informação via LAI há casos em que a CGU decide pela disponibilização de informações sigilosas. "Os dados permitem afirmar que a CGU emite decisão ordenando a divulgação de informações em aproximadamente um quarto das ocasiões em que se depara com o tema da classificação de informações" (Cunha Filho; Antunes, 2020, p. 143). A CGU age somente em casos de erros crassos, como ausência de competência para classificar ou embasamento insuficiente.

Sobre a atuação da CMRI na revisão de pedidos de revisão de classificação de sigilo, Cunha Filho e Antunes (2020, p. 142) apontam que, "das 3.416 decisões tomadas pela CMRI desde a sua instauração, em 2012, até o final do período de coleta de dados, em maio de 2020, apenas em 84 ocasiões (ou seja, em 2,5% das ocasiões) a comissão reverteu, parcial ou totalmente, decisões de órgãos do Executivo", evidência de um alinhamento com as classificações primárias dos órgãos.

Ademais, quaisquer modificações na classificação devem ser registradas no TCI (art. 31 do Decreto n. 7.724/2012 [Brasil, 2012a]) provisão também presente nas normativas das FA.

4.6. Eliminação, arquivamento e publicização de documentos desclassificados

O art. 40 do Decreto n. 7.724/2012 (Brasil, 2012a) assegura que quando um documento é desclassificado e, em adição, há a expectativa de que seja um documento permanente na Tabela de Temporalidade arquivística do órgão, esse documento deve ser enviado ao Arquivo Nacional ou a outro arquivo registrado no Sistema Nacional de Arquivos (SINAR) (pedido 1). As instruções normativas militares preveem, quando da desclassificação de um documento, um rol de regras para destruição das cópias desses documentos, com preservação apenas dos originais.

A EB10-IG-01.012 (Instruções Gerais para Avaliação de Documentos do Exército) conecta as práticas do Exército com as normativas do Conselho Nacional de Arquivos (Conarq) para documentos não classificados – o que inclui os documentos desclassificados, que passam à custódia das Comissões ou Subcomissões Permanentes de Documentos do Exército (CPADEx/SPAD) da OM quando desclassificados e incluídos na relação de documentos desclassificados da Força.

A EB10-IG-01.012 também estipula, consonante com a legislação federal, que documentos uma vez classificados como secretos e ultrassecretos, quando desclassificados, não são passíveis de eliminação. No caso de documentos anteriormente classificados como reservados, deverão ser analisados pela comissão ou subcomissão de avaliação de documentos de acordo com a Tabela de Temporalidade.

Quando da determinação pela eliminação de documentos, o órgão responsável pela criação da informação elabora uma lista de tais documentos, que deve ser submetida, anualmente, ao Conarq (Resolução n. 40/2014 do Conarq [Brasil, 2014b]). Após a elaboração da lista, ela é publicada na página do Conarq, que fica aberta a contestações durante 45 dias.

No Exército, o Arquivo Histórico do Exército (AHEx) é o órgão responsável pela elaboração de tal listagem (art. 45 do EB10-IG-01.012 [Brasil, 2019]). O art. 46 da norma explica o processo de eliminação de documentos, as fases e as interações com o Arquivo Nacional e com o TCU, no caso de documentos relativos à prestação de contas.

Quando a eliminação dos documentos é aprovada, as SPADs elaboram um Termo de Eliminação de Documento, para publicação em boletim interno da OM. O processo recursal relativo às listas de eliminação de documentos não é tão bem delineado quanto os processos recursais da LAI, por exemplo. No Exército, é o presidente da Subcomissão Permanente de Avaliação de Documentos (SCPAD) que deve avaliar a pertinência do desentranhamento.

Se, e enquanto, a destruição do documento for contestada, tal documento é retirado da listagem de eliminação. De acordo com as entrevistas 1 e 2, entre 2006 e 2015 não houve quaisquer eliminações de documentos nas FA – isso porque a Tabela de Temporalidade do MD ficou pronta somente em 2013, após aproximadamente uma década do início de elaboração. A partir de 2015, o AHEx registrou eliminações até 2019 (AHEx, 2022).

Na Aeronáutica, a ICA 214-3/2011 (Brasil, 2011b) regulamenta a eliminação de documentos de forma similar à do Exército. Na Marinha, a EMA-414 (Brasil, 2013a, p. 28) determina que "documentos ou materiais sigilosos de guarda permanente que forem objeto de desclassificação serão encaminhados à Diretoria do Patrimônio Histórico e Documentação da Marinha (DPHDM), para fins de organização, preservação e acesso".

Quanto ao processo de tornar públicos documentos desclassificados, há evidências de que ele acontece com falhas. A organização não governamental (ONG) Fiquem Sabendo, por exemplo, ao fazer à Marinha uma série de pedidos de acesso a documentos desclassificados quanto ao sigilo, deparou-se com uma lenta capacidade de publicização – 15 documentos por mês, ou seja, uma demora de 93 anos para a disponibilização de todos os documentos requeridos (Fiquem Sabendo, 2019b). Sobre esse dado, o Entrevistado 7 afirma que, se os documentos desclassificados forem documentos históricos, haveria ainda o processo de transferência de tutela dos documentos das OMs para o departamento arquivístico da Marinha, o que poderia ser uma das razões da morosidade.

Cunha Filho e Antunes (2020) também relatam órgãos públicos alegando que a classificação de sigilo inicial dada a determinados documentos foi incorreta, mais curta do que a necessária; ou afirmando que os motivos de classificação se mantiveram a despeito do fim do período de sigilo. O posicionamento da CGU é o de que as próprias organizações geradoras do sigilo precisam reavaliar informações que não foram devidamente classificadas.

A CGU estaria, portanto, abrindo a possibilidade, não prevista pela LAI, de reclassificação em grau de sigilo maior (Cunha Filho; Antunes, 2020), como a modificação da classificação reservada para a secreta. A leitura dos autores é de que a CGU atua no sentido de restringir o segredo, mas não de maneira satisfatória, prevalecendo a discricionariedade dos órgãos classificadores.

A expiração da classificação não é lida – e de fato não o é, quando analisada em conjunto com outras hipóteses de salvaguarda de informações – como condição suficiente para a

divulgação. É apenas uma das hipóteses que, apesar da extensa legislação, mostra indícios de subclassificação, sendo uma potencial fonte de fragilização da segurança do Estado.

Conclusão

A classificação quanto ao sigilo de informações é uma atividade importante para os Estados e para as instituições militares: no jogo de dissuasão que a Defesa Nacional requer, manter segredos é fundamental. Contudo, no âmbito democrático, prevalece o imperativo da transparência, o que deixa às instituições de Defesa o ônus da prova na justificativa do porquê de não tornar pública a informação. Para que esse processo tenha legitimidade democrática, desenham-se mecanismos de restrição de acesso, como o sistema de graus de sigilo, que garantiriam o que Hood e Heald (2006) chamam de "transparência em retrospecto". Mantém-se o sigilo enquanto o risco de exposição é grande, tornando pública a informação quando o tempo diminui esse risco.

Este artigo visou compreender como a legislação brasileira, junto com as normas infralegais das FA, estabelecem o processo de gestão de informações com grau de sigilo, com vistas a servir como base para estudos futuros que investiguem minuciosamente a prática de cada uma das partes desse longo e importante processo.

Conclui-se que o processo de classificação e gestão das informações sigilosas é bastante complexo. Existem claros motivos gerais pelos quais classificar (apesar da considerável elasticidade na interpretação das motivações), e há evidente disposição sobre quem pode classificar, sobre a função e a composição das comissões e subcomissões internas que lidam com informações sigilosas, bem como sobre a conexão com a legislação de acesso à informação e à legislação arquivística.

Há controle externo por meio da CMRI e da CGU, que possuem papel importante, mesmo que limitado, no controle da classificação de documentos: a CMRI serve de última instância recursal para pedidos de informação e pedidos de desclassificação de sigilo de documentos, e é responsável pela reclassificação de documentos ultrassecretos; a CGU serve como terceira instância recursal da LAI e, mesmo não podendo modificar uma classificação via de regra, pode publicizar informações incorretamente classificadas.

Apesar de uma abundância normativa, ainda paira a dúvida sobre a eficiência e o correto funcionamento de todos esses processos, que carecem de avaliações. Há evidências, por exemplo, de ineficiência por subclassificação de documentos, ou seja, documentos que só foram classificados diante da provocação de cidadãos que pediram tais informações. Ou seja, antes da provocação, tais informações eram suscetíveis a tornarem-se públicas indevidamente (Cunha Filho; Antunes, 2020).

Outra dúvida paira sobre a função da desclassificação de documentos, que não se traduz automaticamente em divulgação. Na prática, há uma miríade de outros tipos de salvaguarda, quase nada (ou absolutamente nada) debatidos pela sociedade, cuja regulação foi feita

pelas próprias burocracias que os utilizam. Questiona-se a capacidade da burocracia em dar celeridade a esse processo de averiguar, para documentos desclassificados, a incidência de outras hipóteses de salvaguarda de informações, para que se tornem públicos o quanto antes. Há também as incertezas acerca da restrição de acesso a informações pessoais, já que, decorrido o tempo de classificação de sigilo, ainda pode restringir o acesso à informação por até 100 anos. Apesar das alterações realizadas em 2023 ao Decreto n. 7.724/2012 (Brasil, 2012a), segue desconhecido o processo de avaliação sobre quanto tempo uma informação pessoal deve permanecer oculta.

Dessa forma, o sistema brasileiro de classificação em graus de sigilo serve ao propósito de restringir o acesso à *necessidade de conhecer* (Rodrigues, 2020a), não sendo suficiente, isoladamente, para prover transparência pública.

REFERÊNCIAS

ANGÉLICO, Fabiano. *Lei de Acesso à Informação Pública e seus possíveis desdobramentos à accountability democrática no Brasil*. 2012. 133 f. Dissertação (Mestrado em Administração de Empresas) – Escola de Administração de Empresas de São Paulo, Fundação Getulio Vargas, São Paulo, 2012.

ANTUNES, Luiz Fernando Toledo. *Desclassificação tarjada*: o sigilo de documentos das Forças Armadas Brasileiras no contexto da Lei de Acesso à Informação. 2021. 103 f. Dissertação (Mestrado em Administração de Empresas) – Escola de Administração de Empresas de São Paulo, Fundação Getulio Vargas, São Paulo, 2021.

ARQUIVO HISTÓRICO DO EXÉRCITO BRASILEIRO (AHEx). Divisão de Gestão Documental. *Arquivo Histórico do Exército*, 2022. Disponível em: http://www.ahex.eb.mil.br/index.php/divisao-de-gestao-e-avaliacao-de-documentos. Acesso em: 21 fev. 2022.

ARTICLE 19. *The Public's Right to Know*: Principles on Right to Information Legislation. Article 19: Londres, 2016. Disponível em: https://www.article19.org/data/files/RTI_Principles_Updated_EN.pdf. Acesso em: 16 maio 2024.

A última palavra: conheça os membros da CMRI. *Fiquem Sabendo*, São Paulo, 3 abr. 2020. Disponível em: https://fiquemsabendo.com.br/transparencia/membros-cmri. Acesso em: 14 maio 2024.

BEACH, Derek; PEDERSEN, Rasmus Brun. *Process-Tracing Methods*: Foundations and Guidelines. Ann Arbor: The University of Michigan Press, 2013.

BRASIL. *Decreto n. 11.489, de 12 de abril de 2023*. Altera o Decreto n. 7.724, de 16 de maio de 2012, para dispor sobre a composição da Comissão Mista de Reavaliação de Informações. Brasília: Presidência da República, 2023a. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11489.htm#:~:text=DECRETO%20N%C2%BA%2011.489%2C%20DE%2012,que%20lhe%20confere%20o%20art. Acesso em: 10 maio 2024.

BRASIL. *Decreto n. 11.527, de 16 de maio de 2023*. Altera o Decreto n. 7.724, de 16 de maio de 2012, que regulamenta a Lei n. 12.527, de 18 de novembro de 2011. Brasília: Presidência da República, 2023b. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11527.htm. Acesso em: 10 maio 2024.

BRASIL. *Instruções Gerais para Avaliação de Documentos do Exército (EB10-IG-01.012)*. 3 ed. Brasília, DF: Exército Brasileiro, 2019.

BRASIL. *ICA 205-47*: Instrução para a salvaguarda de assuntos sigilosos da Aeronáutica (ISAS). Brasília, DF: Comando da Aeronáutica, 2015a.

BRASIL. *Instruções Gerais para Avaliação e Controle de Documentos Classificados (EB10-IG01.015)*. 1. ed. Brasília, DF: Exército Brasileiro, 2015b.

BRASIL. *Portaria n. 1.067-Cmt Ex, de 8 de setembro de 2014*. Aprova as Instruções Gerais para a Salvaguarda de Assuntos Sigilosos (EB10-IG-01.011), 1ª Edição, 2014, e dá outras providências. 1. ed. Brasília, DF: Exército Brasileiro, 2014a. Disponível em: http://www.sgex.eb.mil.br/sg8/002_instrucoes_gerais_reguladoras/01_gerais/port_n_1067_cmdo_eb_08set2014.html. Acesso em: 16 maio 2024.

BRASIL. Ministério da Justiça. *Resolução n. 40, de 9 de dezembro de 2014*. Dispõe sobre os procedimentos para a eliminação de documentos no âmbito dos órgãos e entidades integrantes do Sistema Nacional de Arquivos – SINAR. Brasília: Conselho Nacional de Arquivos, 2014b. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq/resolucao-no-40-de-9-de-dezembro-de-2014-alterada#:~:text=Disp%C3%B5e%20sobre%20os%20procedimentos%20para,Sistema%20Nacional%20de%20Arquivos%20%2D%20SINAR. Acesso em: 10 maio 2024.

BRASIL. *EMA-414*: normas para a salvaguarda de materiais controlados, dados, informações, documentos e materiais sigilosos na Marinha (1ª rev.). Brasília, DF: Marinha do Brasil, 2013a.

BRASIL. *ICA 200-12*: Avaliação de Documentos Classificados no Comando da Aeronáutica. Brasília, DF: Comando da Aeronáutica, 2013b. Disponível em: https://www.sislaer.fab.mil.br/terminalcendoc/acervo/detalhe/3050?guid=1713225600600&returnUrl=%2Fterminalcendoc%2Fresultado%2Flistar%3

Fguid%3D1713225600600%26quantidadePaginas%3D1%26codigoRegistro%3D3050%233050&i=9. Acesso em: 16 maio 2024.

BRASIL. *Decreto n. 7.724, de 16 de maio de 2012*. Regulamenta a Lei n. 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. Brasília: Presidência da República, 2012a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/d7724.htm. Acesso em: 10 maio 2024.

BRASIL. *Decreto n. 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. Brasília: Presidência da República, 2012b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/d7845.htm. Acesso em: 10 maio 2024.

BRASIL. *Lei n. 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 n. 8.112, de 11 de dezembro de 1990; revoga a Lei n. 11.111, de 5 de maio de 2005, e dispositivos da Lei n. 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília: Presidência da República, 2011a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 10 maio 2024.

BRASIL. *ICA 214-3/2011*: Avaliação de Documentos de Arquivo. Brasília, DF: Comando da Aeronáutica, 2011b. Disponível em: https://www2.fab.mil.br/cendoc/images/doc/arq_pdf/ICA214-3.pdf. Acesso em: 16 maio 2024.

BRASIL. *Lei n. 11.111, de 5 de maio de 2005*. Regulamenta a parte final do disposto no inciso XXXIII do *caput* do art. 5º da Constituição Federal e dá outras providências. Brasília: Presidência da República, 2005. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2005/lei/l11111.htm. Acesso em: 10 maio 2024.

BRASIL. *Decreto n. 4.073, de 3 de janeiro de 2002*. Regulamenta a Lei n. 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados. Brasília: Presidência da República, 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/2002/d4073.htm. Acesso em: 10 maio 2024.

BRASIL. *Lei n. 9.784, de 29 de janeiro de 1999*. Regula o processo administrativo no âmbito da Administração Pública Federal. Brasília: Presidência da República, 1999. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9784.htm. Acesso em: 10 maio 2024.

BRASIL. *Decreto n. 2.134, de 24 de janeiro de 1997*. Regulamenta o art. 23 da Lei n. 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. Brasília: Presidência da República, 1997. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/d2134.htm#:~:text=DECRETO%20N%C2%BA%202.134%2C%20DE%2024%20DE%20JANEIRO%20DE%201997.&text=Regulamenta%20o%20art.,eles%2C%20e%20d%C3%A1%20outras%20provid%C3%AAncias. Acesso em: 10 maio 2024.

COLARESI, Michael P. *Democracy Declassified*: The Secrecy Dilemma in National Security. Nova York: Oxford University Press, 2014.

CRUZ, Isabela de Paula. *Contexto, prática e obstáculos do acesso à informação*: insumos para a discussão a partir da experiência com o setor nuclear brasileiro. 2018. 146 f. Dissertação (Mestrado em História, Política e Bens Culturais) – Centro de Pesquisa e Documentação de História Contemporânea do Brasil, Fundação Getulio Vargas, Rio de Janeiro, 2018.

CUNHA FILHO, Marcio Camargo. *A construção da transparência pública no Brasil*: análise da elaboração e implementação da Lei de Acesso à Informação no Executivo Federal (2003-2019). 2019. 239 f., il. Tese (Doutorado em Direito) – Universidade de Brasília, Brasília, 2019.

CUNHA FILHO, Marcio Camargo. O desencontro entre direito à informação e direito à verdade: análise das práticas da controladoria-geral da União. *Direito, Estado e Sociedade*, Rio de Janeiro, n. 47, p. 91-107, jul./dez. 2015.

CUNHA FILHO, Marcio Camargo; ANTUNES, Luiz Fernando Toledo. Regime legal de classificação de informações no Brasil: problemas teóricos, empíricos e (in)compatibilidade com a ordem jurídica democrática. *Cadernos EBAPE.BR*, Rio de Janeiro, v. 19, n. 1, p. 138-151, 2021.

DE ANGELO, Vitor Amorim. Quem tem documentos sobre a ditadura? Uma análise da legislação e das iniciativas governamentais. *Política & Sociedade*, Florianópolis, v. 11, n. 21, p. 199-234, jul. 2012.

DEL NEGRI, André. *Segredo de Estado no Brasil*. Belo Horizonte: D'Plácido Editora, 2016.

ESCOLA NACIONAL DE ADMINISTRAÇÃO PÚBLICA (ENAP). *Módulo 3*: classificação de informações e dados abertos. Brasília: Enap, 2018. Disponível em: https://repositorio.enap.gov.br/bitstream/1/3144/1/M%C3%B3dulo%203%20-%20Classifica%C3%A7%C3%A3o%20de%20Informa%C3%A7%C3%B5es%20e%20Dados%20Abertos%20%281%29.pdf. Acesso em: 26 jan. 2022.

ESCOLA NACIONAL DE ADMINISTRAÇÃO PÚBLICA (ENAP). *Módulo 2*: negativas de acesso à informação. Brasília: Enap, 2017. Disponível em: https://repositorio.enap.gov.br/bitstream/1/3143/

1/M%C3%B3dulo%202%20-%20Negativas%20de%20acesso%20%C3%A0%20informa%C3%A7%C3%A3o.pdf. Acesso em: 10 mar. 2024.

FICO, Carlos. História do tempo presente, eventos traumáticos e documentos sensíveis: o caso brasileiro. *Varia Historia*, Belo Horizonte, v. 28, n. 47, p. 43-59, jan./jun. 2012.

FIQUEM SABENDO. Marinha é responsável por 96% das informações classificadas como sigilosas. *Fiquem Sabendo*, 25 jan. 2019a. Disponível em: https://fiquemsabendo.com.br/transparencia/marinha-informacoes-sigilosas/. Acesso em: 22 fev. 2022.

FIQUEM SABENDO. Marinha pede "só" 93 anos para entregar documentos que perderam sigilo – Don't LAI to me. *Fiquem Sabendo*, 31 mar. 2019b. Disponível em: https://fiquemsabendo.com.br/transparencia/newsletter-edicao-5/. Acesso em: 22 fev. 2022.

HOOD, Christopher; HEALD, David (eds.). *Transparency*: The Key to Better Governance? Oxford: Oxford University Press, 2006.

HOTT, Daniela Francescutti Martins. *O acesso aos documentos sigilosos*: um estudo das comissões permanentes de avaliação e de acesso nos arquivos brasileiros. 2005. 411 f. Dissertação (Mestrado em Ciência da Informação) – Faculdade de Estudos Sociais Aplicados, Universidade de Brasília, Brasília, 2005.

HOTT, Daniela Francescutti Martins; RODRIGUES, Georgete Medleg. O acesso aos arquivos sigilosos no Brasil: do acesso restrito à instância recursal. *In:* ENCONTRO NACIONAL DE PESQUISA E PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO, 18, 2017, Marília. *Anais* [...]. Marília: Unesp; Ancib, 2017.

LOPES, Janaina Vedoin; KONRAD, Glaucia Vieira Ramos. Arquivos da repressão e leis de acesso à informação: os casos brasileiro e argentino na construção do direito à memória e à verdade. *Revista Aedos*, [*s.l.*], v. 5, n. 13, p. 6-23, ago./dez. 2013.

LORD, Kristin M. *The Perils and Promise of Global Transparency*: Why the Information Revolution May Not Lead to Security, Democracy, or Peace. Nova York: State University of New York Press, 2006.

MARTINS, João Batista. O impacto da informação existente no SIGADAER na gestão do conhecimento. *AtoZ*: Novas Práticas em Informação e Conhecimento, Curitiba, v. 9, n. 2, p. 57-68, jul./dez. 2020.

MENDEL, Toby. *Freedom of Information*: A Comparative Legal Survey. 2. ed. rev. e atual. Paris: Unesco, 2008.

MENDEL, Toby. Freedom of Information as an Internationally Protected Human Right. *Comparative Media Law Journal*, [*s.l.*], v. 1, n. 1, p. 39-70, 2003.

OPEN SOCIETY JUSTICE INITIATIVE (OSJI). *Tshwane Principles*: Global Principles on National Security and the Right to Information. Nova York: Open Society Justice Initiative, 2013.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS (OEA). *Recommendations on Access to Information*. Atlanta: Organização dos Estados Americanos, 2008. Disponível em: https://www.oas.org/en/sla/dil/docs/CP-CAJP_2599-08_eng.pdf. Acesso em: 2 out. 2022.

RODRIGUES, Karina Furtado. Desvelando o conceito de transparência: seus limites, suas variedades e a criação de uma tipologia. *Cadernos EBAPE.BR*, Rio de Janeiro, v. 18, n. 2, p. 237-253, 2020a.

RODRIGUES, Karina Furtado. A política nas políticas de acesso à informação brasileiras: trajetória e coalizões. *Revista de Administração Pública*, Rio de Janeiro, v. 54, n. 1, p. 142-161, 2020b.

RODRIGUES, Karina Furtado. *Democratic Transparency Pacts on Defense*: Assessing Change in Civilian Access to Military Information in Brazil. 2017. 218 f. Tese (Doutorado em Administração) – Escola Brasileira de Administração Pública de Empresas, Fundação Getulio Vargas, Rio de Janeiro, 2017a.

RODRIGUES, Karina Furtado. Informações de defesa e segurança nacional: entre a legitimidade do segredo e o direito à informação. *In*: REIA, Jhessica *et al*. (orgs.). *Horizonte presente*: tecnologia e sociedade em debate. Rio de Janeiro: Letramento, 2017b.

RTI RATING. *Global Right to Information Rating – Rating Map*, [*s.d.*]. Disponível em: http://www.rti-rating.org/. Acesso em: 10 mar. 2024.

SAGAR, Rahul. *Secrets and Leaks*: The Dilemma of State Secrecy. Woodstock: Princeton University Press, 2013.

SCHOENFELD, Gabriel. *Necessary Secrets*: National Security, the Media, and the Rule of Law. Nova York: WW Norton & Company, 2010.

SOUZA, Rosale de Mattos. *Produção de sentido em documentos e informações de arquivos sigilosos*: comunidade de informação e contrainformação sob o olhar da Assessoria de Segurança e Informação – ASI UFF de 1971-1982. 2017. 271 f. Tese (Doutorado em Ciência da Informação) – Escola de Comunicação, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2017.

THOMPSON, Dennis F. Democratic Secrecy. *Political Science Quarterly*, [*s.l.*], v. 114, n. 2, p. 181-193, 1999.

Karina Furtado Rodrigues

Doutora em Administração pela Escola Brasileira de Administração Pública e de Empresas (Ebape) da Fundação Getulio Vargas (FGV). Professora no Programa de Pós-Graduação em Ciências Militares (PPGCM), na Escola de Comando e Estado-Maior do Exército (ECEME). Coordenadora do Laboratório de Governança, Gestão e Políticas Públicas em Defesa Nacional (Lab GGPP Defesa) do PPGCM/ECEME.

karinafrodrigues@gmail.com