

MARINHA DO BRASIL
ESCOLA DE GUERRA NAVAL
PROGRAMA DE PÓS-GRADUAÇÃO EM ESTUDOS MARÍTIMOS

ALAN CARVALHO DE OLIVEIRA

**INTERCEPTAÇÃO DE DADOS EM CABOS SUBMARINOS NAS
ÁGUAS JURISDICIONAIS BRASILEIRAS:
Desafios à Soberania e à Jurisdição do Estado Brasileiro**

Rio de Janeiro

2026

ALAN CARVALHO DE OLIVEIRA

**INTERCEPTAÇÃO DE DADOS EM CABOS SUBMARINOS NAS
ÁGUAS JURISDICIONAIS BRASILEIRAS:
Desafios à Soberania e à Jurisdição do Estado Brasileiro**

Dissertação apresentada à Escola de Guerra Naval, como requisito parcial para a obtenção do grau de Mestre em Estudos Marítimos.

Orientador: Prof. Dr. André Panno Beirão

Rio de Janeiro
Escola de Guerra Naval
2026

O48i Oliveira, Alan Carvalho de

Interceptação de dados em cabos submarinos nas águas jurisdicionais brasileiras: desafios à soberania e à jurisdição do Estado brasileiro / Alan Carvalho de Oliveira. – Rio de Janeiro, 2026.

171f.: il.

Dissertação (mestrado) - Escola de Guerra Naval, Programa de Pós Graduação em Estudos Marítimos (PPGEM), 2026.

Orientador (a): André Panno Beirão.

Bibliografia: f. 155-171.

1. Cabos submarinos. 2. Interceptação de dados. 3. Soberania. 4. Jurisdição marítima. I. Escola de Guerra Naval (BRASIL). II. Título.

CDD: 341.448

DECLARAÇÃO DA NÃO EXISTÊNCIA DE APROPRIAÇÃO INTELECTUAL IRREGULAR

Declaro que este trabalho acadêmico: a) corresponde ao resultado de investigação por mim desenvolvida, enquanto discente da Escola de Guerra Naval (EGN); b) é um trabalho original, ou seja, que não foi por mim anteriormente utilizado para fins acadêmicos ou quaisquer outros; c) é inédito, isto é, não foi ainda objeto de publicação; e d) é de minha exclusiva e integral autoria.

Declaro também que tenho ciência de que a utilização de ideias ou palavras de autoria de outrem, sem a devida identificação da fonte, e o uso de inteligência artificial no processo de escrita constituem grave falta ética, moral, legal e disciplinar. Ademais, assumo o compromisso de que este trabalho possua, a qualquer tempo, ser analisado para a verificação de sua originalidade e ineditismo, por meio de ferramentas de detecção de similaridades ou por profissionais qualificados.

Os direitos morais e patrimoniais deste trabalho acadêmico, nos termos da Lei nº 9.610/1998, pertencem ao seu Autor, sendo vedado o uso comercial sem prévia autorização. É permitida a transcrição parcial de textos do trabalho, ou mencioná-los, para comentários e citações, desde que seja feita a referência bibliográfica completa.

Os conceitos e ideias expressas neste trabalho acadêmico são de responsabilidade do Autor e não retratam qualquer orientação institucional da EGN ou da Marinha do Brasil.

ALAN CARVALHO DE OLIVEIRA

**INTERCEPTAÇÃO DE DADOS EM CABOS SUBMARINOS NAS
ÁGUAS JURISDICIONAIS BRASILEIRAS:
Desafios à Soberania e à Jurisdição do Estado Brasileiro**

Dissertação apresentada ao Programa de Pós-Graduação em Estudos Marítimos da Escola de Guerra Naval, como requisito parcial para a obtenção do grau de Mestre em Estudos Marítimos.

Área de concentração: Segurança, Defesa e Estratégia Marítima.

Aprovada em 31 de março de 2026.

Banca Examinadora:

Prof. Dr. Luís Manuel Brás Bernardino, Universidade Autônoma de Lisboa
Doutor pelo Instituto Superior de Ciências Sociais e Políticas da Universidade de Lisboa
Membro Externo

Prof. Dr. Tiago Vinícius Zanella, Escola de Guerra Naval
Doutor pela Faculdade de Direito da Universidade de Lisboa
Professor do PPGEM - EGN

Prof. Dr. André Panno Beirão, Escola de Guerra Naval
Doutor pela Universidade do Estado do Rio de Janeiro
Professor do PPGEM - EGN
Orientador

DEDICATÓRIA

A Deus, porque é o princípio e o fim de todas as coisas

A Tayanne, Miguel e Bia, porque são a luz da minha vida e o motivo de tudo

A minha mãe, porque me ensinou o valor do estudo

Ao meu pai, porque me ensinou o valor da perseverança

AGRADECIMENTOS

Agradeço à minha esposa e aos meus filhos pela paciência e compreensão nos muitos momentos em que estive ausente dedicado à elaboração deste trabalho, bem como pelo amor habitual, combustível nos instantes de cansaço.

Ao meu orientador, Prof. Dr. André Panno Beirão, por ter despertado em mim o interesse por tão fascinante e importante tema naquela manhã de julho de 2024, assim como pelos inestimáveis conhecimentos transmitidos ao longo de todo o curso.

Ao CMG (RM1) Anthony Steve de Lima Barros Pereira, estimado amigo e companheiro em mais essa jornada, a quem devo a iniciação nos estudos marítimos.

À CMG (T) Angélica Karina de Azevedo Caúla e Silva, pelo incentivo e pela intercessão junto à Direção da minha Organização Militar, fundamental para que eu conseguisse a autorização exigida aos militares da ativa para a participação no processo seletivo do curso.

Ao Desembargador do Tribunal Marítimo Marcelo David Gonçalves, pelo encorajamento constante ao aperfeiçoamento intelectual.

A todos os professores, amigos e colegas do PPGEM com os quais convivi nesses dois intensos anos, pela troca de conhecimentos e experiências multidisciplinares, essenciais ao processo de aprendizado típico dos estudos marítimos.

A todos aqueles que contribuíram direta e indiretamente para a consecução desse objetivo.

À Marinha do Brasil, que me proporcionou a possibilidade de conciliar as atividades acadêmicas e profissionais.

Deus ao mar o perigo e o abismo deu
Mas nele é que espelhou o céu.

Fernando Pessoa

RESUMO

Este trabalho tem o objetivo de analisar o arcabouço jurídico internacional e nacional de incidência sobre os cabos submarinos, com a finalidade de identificar se as suas disposições são adequadas para garantir a proteção jurídica dessa infraestrutura contra a interceptação de seus dados nas Águas Jurisdicionais Brasileiras. Os cabos submarinos de telecomunicações representam a principal infraestrutura de suporte à circulação mundial de dados, incluindo tráfegos governamentais, financeiros, militares e privados. Apesar disso, tais cabos apresentam elevada vulnerabilidade estrutural, especialmente em função da sua disposição ao longo do leito marinho, frequentemente em áreas não submetidas à soberania estatal e sujeitas a regimes jurídicos distintos. Parte-se da premissa de que, embora seja reconhecida a sua relevância para a comunicação global e soberania dos Estados, a disciplina jurídica dos cabos submarinos concentra-se predominantemente na tutela da sua dimensão física, existindo lacunas significativas quanto à regulação da interceptação dos dados que por eles trafegam. Para tanto, serão utilizados na pesquisa o método hipotético-dedutivo e qualitativo, de natureza jurídico-dogmática, confrontando-se a possibilidade de interceptação em cabos submarinos com o regramento jurídico-normativo atual para se chegar a um diagnóstico sobre a sua suficiência. O Tallinn Manual 2.0 é utilizado como referencial teórico interpretativo, haja vista se tratar de obra desenvolvida por grupos de especialistas na aplicação do Direito Internacional às operações cibernéticas conduzidas por Estados. Inicialmente, o trabalho examina as características da infraestrutura de cabos submarinos, a sua interceptação como risco estratégico e qual o tratamento conferido pelo Direito Internacional, abordando aspectos que envolvem soberania e direitos humanos. Em seguida, analisa-se o regime jurídico internacional aplicável aos cabos submarinos, chegando-se a um diagnóstico crítico sobre a fragmentação e a insuficiência do regime vigente. Na sequência, o estudo analisa os cenários normativos para a regulação internacional da interceptação de dados, discutindo as consequências da sua ausência, as propostas doutrinárias e institucionais existentes, as modalidades possíveis e o conteúdo desejável de um eventual instrumento internacional. Por fim, a dissertação examina os desafios e as competências do Estado brasileiro, analisando os limites da jurisdição nacional, os instrumentos jurídicos internos aplicáveis e a atuação da Marinha do Brasil, tanto na condição de Autoridade Marítima, como na de expressão do Poder Naval. Ao final, conclui-se que o arcabouço jurídico atualmente vigente, tanto no plano internacional quanto no nacional, mostra-se inadequado para enfrentar de forma satisfatória os desafios associados à interceptação de dados em cabos submarinos, evidenciando a

necessidade de desenvolvimento normativo compatível com a importância dessa infraestrutura.

Palavras-chave: Cabos submarinos. Interceptação de dados. Espionagem. Águas Jurisdicionais Brasileiras. Direito do Mar.

ABSTRACT

This paper aims to analyze the international and domestic framework applicable to submarine cables, with the purpose of identifying whether its provisions are adequate to ensure the legal protection of this infrastructure against the interception of their data within Brazilian Jurisdictional Waters. Submarine telecommunications cables constitute the primary infrastructure supporting the global circulations of data, including governmental, financial, military, and private traffic. Despite their importance, such cables exhibit high structural vulnerability, especially due to their placement along the seabed, often in areas not subject to state sovereignty and governed by different legal regimes. The study is based on the premise that, although the relevance of submarine cables to global communications and state sovereignty is widely recognized, the legal regulation of submarine cables is predominantly focused on the protection of their physical dimension, with significant gaps regarding the regulation of the interception of the data transmitted through them. To this end, the research employs the hypothetical-deductive and qualitative methods, of a legal-dogmatic nature, confronting of interception of submarine cables with the current legal-normative framework in order to arrive at a diagnosis of its sufficiency. The Tallinn Manual 2.0 is used as an interpretative theoretical reference, as it is a work developed by groups of experts on the application of International Law to cyber operations conducted by States. Initially, the paper examines the characteristics of submarine cables infrastructure, data interception as a strategic risk, and the treatment afforded by International Law, addressing aspects related to sovereignty and human rights. Subsequently, it analyses the international legal regime applicable to submarine cables, reaching a critical diagnosis of the fragmentation and insufficiency of the existing regime. Thereafter, the study examines normative scenarios for the international regulation of data interception, discussing the consequences of this absence, existing doctrinal and institutional proposals, possible regulatory modalities, and the desirable content of a potential international instrument. Finally, the dissertation examines the challenges and competencies of the Brazilian State, analyzing the limits of national jurisdiction, applicable domestic legal instruments, and the role of the Brazilian Navy, both in its capacity as the Maritime Authority and as an expression of Naval Power. In conclusion, the study finds that the current legal framework, at both the international and national levels, is inadequate to satisfactorily address the challenges associated with data interception in submarine cables, highlighting the need for normative development compatible with the importance of this infrastructure.

Keywords: Submarine cables. Data Interception. Espionage. Brazilian Jurisdictional Waters.
Law of the Sea.

LISTA DE FIGURAS

FIGURA 1 - Taxa de Usuários de Internet por Região.....	29
FIGURA 2 - Representação dos Cabos Submarinos no Mundo.....	30
FIGURA 3 - All-Red Line.....	39

LISTA DE QUADROS

QUADRO 1 - Resumo Comparativo dos Casos de Intercepção mais Notáveis.....	42
QUADRO 2 - Citações a cabos submarinos na CNUDM.....	81
QUADRO 3 - Regime Internacional dos Cabos Submarinos: panorama, escopo e lacunas.....	91
QUADRO 4 - A Atuação da Autoridade Marítima Brasileira.....	136

LISTA DE ABREVIATURAS E SIGLAS

AED	- Ação Estratégica de Defesa
AJB	- Águas Jurisdicionais Brasileiras
AMB	- Autoridade Marítima Brasileira
ANATEL	- Agência Nacional de Telecomunicações
ARPA	- Agência de Projetos de Pesquisa Avançada dos EUA (<i>Advanced Research Projects Agency</i>)
BID	- Banco Interamericano de Desenvolvimento
CCDCOE	- Centro de Excelência em Defesa Cibernética Cooperativa da OTAN (<i>Cooperative Cyber Defence Centre of Excellence</i>)
CIA	- Agência Central de Inteligência dos EUA (<i>Central Intelligence Agency</i>)
CIJ	- Corte Internacional de Justiça
CNUDM	- Convenção das Nações Unidas sobre o Direito do Mar
CP	- Código Penal
CREDN	- Comissão de Relações Exteriores e de Defesa Nacional
CRFB	- Constituição da República Federativa do Brasil de 1988
CSM	- Consciência Situacional Marítima
DECEA	- Departamento de Controle do Espaço Aéreo
DHN	- Diretoria de Hidrografia e Navegação
DICA	- Direito Internacional dos Conflitos Armados
DPI	- Inspeção Profunda de Pacotes (<i>Deep Packet Inspection</i>)
DPC	- Diretoria de Portos e Costas
EMA	- Estado-Maior da Armada
END	- Estratégia Nacional de Defesa
ENISA	- Agência da União Europeia para Cibersegurança (<i>European Union Agency for Cybersecurity</i>)
ENSIC	- Estratégia Nacional de Segurança de Infraestruturas Críticas
EU	- União Europeia (<i>European Union</i>)
EUA	- Estados Unidos da América
FDM	- Fundamentos Doutrinários da Marinha
GCHQ	- Quartel-General de Comunicações do Governo do Reino Unido (<i>Government Communications Headquarters</i>)

GGE	- Grupo de Peritos Governamentais (<i>Group of Governments Experts</i>)
GSI-PR	- Gabinete de Segurança Institucional da Presidência da República
HUMINT	- Inteligência Humana (<i>Human Intelligence</i>)
IBGE	- Instituto Brasileiro de Geografia e Estatística
ICPC	- Comitê Internacional de Proteção de Cabos (<i>International Cable Protection Committee</i>)
ICPM	- Infraestruturas Críticas do Poder Marítimo
IP	- Protocolo da Internet (<i>Internet Protocol</i>)
ISA	- Autoridade Internacional dos Fundos Marinhos (<i>International Seabed Authority</i>)
ITU	- União Internacional de Telecomunicações (<i>International Telecommunications Union</i>)
ITLOS	- Tribunal Internacional do Direito do Mar (<i>Internacional Tribunal for the Law of the Sea</i>)
LBDN	- Livro Branco de Defesa Nacional
LC	- Lei Complementar
LGPD	- Lei Geral de Proteção de Dados
MERCOSUL	- Mercado Comum do Sul
MB	- Marinha do Brasil
MN	- Milhas Náuticas
NORMAM	- Normas da Autoridade Marítima
NSA	- Agência Nacional de Segurança dos EUA (<i>National Security Agency</i>)
OBE	- Objetivos Estratégicos da Marinha
OCDE	- Organização para a Cooperação e Desenvolvimento Econômico
ODN	- Objetivo de Defesa Nacional
OEWG	- Grupo de Trabalho Aberto (<i>Open-Ended Working Group</i>)
ONU	- Organização das Nações Unidas
OTAN	- Organização do Tratado do Atlântico Norte
PC	- Plataforma Continental
PF	- Polícia Federal
PL	- Projeto de Lei Ordinária
Plansic	- Plano Nacional de Segurança de Infraestruturas Críticas
PND	- Política Nacional de Defesa
PNICS	- Política Nacional de Infraestruturas de Cabos Subaquáticos

PNSIC	- Política Nacional de Segurança de Infraestruturas Críticas
RAM	- Memória de Acesso Aleatório (<i>Random Access Memory</i>)
RIPEAM	- Regulamento Internacional para Evitar Abalroamentos no Mar
ROV	- Veículo Operado Remotamente (<i>Remotely Operated Vehicle</i>)
SIGINT	- Inteligência de Sinais (<i>Signals Intelligence</i>)
SisGAAz	- Sistema de Gerenciamento da Amazônia Azul
SOLAS	- Convenção sobre a Salvaguarda da Vida Humana no Mar (<i>Safety of Life at Sea</i>)
TI	- Tecnologia da Informação
TIC	- Tecnologias da Informação e Comunicação
TPI	- Tribunal Penal Internacional
UNCLOS	- Convenção das Nações Unidas sobre o Direito do Mar (<i>United Nations Convention on Law of the Sea</i>)
UVV	- Veículo Subaquático Não Tripulado (<i>Unmanned Underwater Vehicle</i>)
ZEE	- Zona Econômica Exclusiva

SUMÁRIO

1	INTRODUÇÃO.....	20
2	INFRAESTRUTURA SUBMARINA DE CABOS E A INTERCEPTAÇÃO COMO RISCO ESTRATÉGICO.....	28
2.1	PANORAMA.....	28
2.2	NATUREZA DAS AMEAÇAS CONTEMPORÂNEAS.....	32
2.3	INTERCEPTAÇÃO DE DADOS.....	34
2.3.1	Tipos de interceptação.....	36
2.3.2	Alguns casos conhecidos de interceptação.....	37
2.3.2.1	1902-1903 - “All-Red Line”.....	37
2.3.2.2	1917 - telegrama Zimmermann.....	39
2.3.2.3	Década de 1970 - Operação Ivy Bells.....	39
2.3.2.4	2003-2006 – room 641a (AT&T).....	40
2.3.2.5	2013 - caso Edward Snowden.....	41
2.3.3	Resumo comparativo.....	42
2.4	INTRODUÇÃO AO DESAFIO JURÍDICO.....	43
3	A INTERCEPTAÇÃO DE DADOS NO DIREITO INTERNACIONAL.....	47
3.1	CONSIDERAÇÕES INICIAIS.....	47
3.2	INTERFACES COM O TALLINN MANUAL 2.0 E O DIREITO INTERNACIONAL CIBERNÉTICO.....	48
3.3	A INTERCEPTAÇÃO COMO PRÁTICA DE ESPIONAGEM TÉCNICA.....	49
3.3.1	Contexto histórico da espionagem.....	49
3.3.2	Espionagem digital.....	50
3.4	AUSÊNCIA DE PROIBIÇÃO EXPRESSA NO DIREITO INTERNACIONAL.....	53
3.5	PRINCÍPIO DA SOBERANIA E SUA APLICAÇÃO À INTERCEPTAÇÃO.....	55
3.6	PRINCÍPIO DA NÃO INTERVENÇÃO.....	57
3.7	DIREITOS HUMANOS E PROTEÇÃO DA PRIVACIDADE.....	59
3.7.1	A privacidade como direito humano fundamental.....	59
3.7.2	Tensão entre privacidade e soberania.....	61
3.8	A INADEQUAÇÃO AOS CONCEITOS DE INVESTIGAÇÃO CIENTÍFICA MARINHA E OUTROS USOS DO MAR INTERNACIONALMENTE LÍCITOS..	62

3.8.1	Atividades de investigação científica marinha.....	63
3.8.2	Outros usos do mar internacionalmente lícitos.....	63
3.9	CONSIDERAÇÕES PARCIAIS.....	64
4	REGIME JURÍDICO INTERNACIONAL APLICÁVEL AOS CABOS SUBMARINOS.....	67
4.1	CONSIDERAÇÕES INICIAIS.....	69
4.2	A CNUDM E OS CABOS SUBMARINOS.....	69
4.2.1	Disposições sobre cabos submarinos na CNUDM.....	69
4.2.1.1	<i>Mar territorial</i>	70
4.2.1.2	<i>Estados arquipélagos</i>	72
4.2.1.3	<i>Zona Econômica Exclusiva (ZEE)</i>	72
4.2.1.4	<i>Plataforma Continental (PC)</i>	73
4.2.1.5	<i>Alto-mar</i>	74
4.2.1.6	<i>Solução de controvérsias</i>	78
4.2.1.7	<i>Quadro analítico das disposições da CNUDM</i>	79
4.3	OUTRAS NORMAS E INSTRUMENTOS RELEVANTES.....	82
4.3.1	Convenção para a proteção de cabos telegráficos submarinos de 1884.....	82
4.3.2	Outros instrumentos conexos.....	85
4.3.2.1	<i>Regulamento Internacional para Evitar Abalroamentos no Mar (RIPEAM)</i>	85
4.3.2.2	<i>Convenção de Londres de 1972 e seu Protocolo, de 1996</i>	86
4.3.2.3	<i>Direito da Guerra</i>	86
4.3.2.4	<i>Convenções contra-terrorismo</i>	88
4.3.2.5	<i>Recomendações e diretrizes do ICPC</i>	89
4.4	CONSIDERAÇÕES PARCIAIS - DIAGNÓSTICO E LACUNAS DO REGIME JURÍDICO INTERNACIONAL.....	90
5	CENÁRIOS NORMATIVOS E CAMINHOS PARA A REGULAÇÃO INTERNACIONAL.....	94
5.1	CONSIDERAÇÕES INICIAIS.....	94
5.2	CONSEQUÊNCIAS DA AUSÊNCIA DE REGULAÇÃO.....	94
5.3	PRINCIPAIS PROPOSTAS DOUTRINÁRIAS E INSTITUCIONAIS.....	96
5.3.1	Organização das Nações Unidas.....	97
5.3.1.1	<i>Grupos de trabalho e fóruns de discussão</i>	97

5.3.1.2	<i>União Internacional de Telecomunicações (ITU)</i>	99
5.3.2	Propostas de organizações regionais e setoriais.....	99
5.3.2.1	<i>International Cable Protection Committee (ICPC)</i>	100
5.3.2.2	<i>European Union Agency for Cybersecurity (ENISA)</i>	100
5.3.3	Propostas doutrinárias.....	101
5.4	MODALIDADES DE REGULAÇÃO INTERNACIONAL POSSÍVEIS.....	103
5.4.1	Soft law.....	103
5.4.2	Tratados regionais.....	104
5.4.3	Tratado multilateral global.....	105
5.5	CONTEÚDO DESEJÁVEL DE UM REGIME NORMATIVO INTERNACIONAL SOBRE INTERCEPTAÇÃO DE DADOS.....	106
5.5.1	Proibição de interceptação em tempo de paz.....	106
5.5.2	Diretrizes para cooperação.....	107
5.5.3	Criminalização e exercício de jurisdição.....	107
5.5.4	Responsabilização estatal e mecanismos de reparação.....	108
5.5.5	Disposição expressa da violação de Direitos Humanos.....	110
5.6	CONSIDERAÇÕES PARCIAIS.....	110
6	DESAFIOS E COMPETÊNCIAS DO ESTADO BRASILEIRO	113
6.1	CONSIDERAÇÕES INICIAIS.....	113
6.2	ÁGUAS JURISDICIONAIS BRASILEIRAS.....	114
6.3	O EXERCÍCIO DA JURISDIÇÃO NOS DIVERSOS ESPAÇOS MARÍTIMOS.....	116
6.3.1	No mar territorial.....	117
6.3.1.1	<i>Passagem inocente</i>	118
6.3.1.2	<i>Jurisdição do Estado da bandeira</i>	121
6.3.2	Na Zona Econômica Exclusiva e na Plataforma Continental.....	122
6.4	INSTRUMENTOS JURÍDICOS BRASILEIROS APLICÁVEIS À SEGURANÇA DOS CABOS SUBMARINOS.....	124
6.4.1	Documentos de defesa nacional.....	125
6.4.2	Documentos sobre a segurança das infraestruturas críticas no Brasil.....	126
6.4.3	O Projeto de Lei nº 270/2025 e a proposta de um marco regulatório nacional.....	128
6.4.3.1	<i>A correlação do projeto com a temática da interceptação de dados</i>	129
6.4.3.2	<i>A criminalização de condutas</i>	129
6.4.4	Status do Brasil quanto à segurança das infraestruturas críticas.....	132

6.5	O PAPEL DA MARINHA DO BRASIL NAS EXPRESSÕES DO PODER NAVAL E DA AUTORIDADE MARÍTIMA.....	133
6.5.1	O papel da Autoridade Marítima.....	135
6.5.2	O papel do Poder Naval.....	137
6.6	CONSIDERAÇÕES PARCIAIS.....	140
7	CONCLUSÃO.....	142
	REFERÊNCIAS.....	153

1 INTRODUÇÃO

A segurança dos cabos submarinos é um tema quem vem ganhando relevância mundial, tendo em vista a função que essa infraestrutura desempenha na comunicação global. Responsável pela quase totalidade do fluxo de dados internacionais, a rede de cabos submarinos constitui a principal infraestrutura em termos de volume de tráfego de dados internacionais, estando neles inseridas as transmissões de internet, telefonia e, inclusive, dados confidenciais militares (ENISA, 2023, p. 4).

Conforme dados de 2024 da TeleGeography¹, o somatório dos sistemas de cabos submarinos em operação no mundo representa um total de 1,4 milhão de quilômetros de cabos lançados nos mares, o que poderia dar a volta no planeta 35 vezes (Anatel, 2025, p. 4).

Considerando que essa malha de cabos encontra-se fisicamente disposta em ambiente marinho, consequentemente permanece suscetível a uma série de ameaças que colocam em risco a sua integridade e o seu perfeito funcionamento, refletindo a crescente preocupação mundial com a sua segurança. De acordo com dados apurados entre 1959 e 2021, a maioria das falhas foram atribuídas a atividades humanas não intencionais. Embora menos frequentes, condições naturais como tsunamis e terremotos também representam um risco a esses ativos, conforme apontado no relatório do Serviço de Pesquisa do Congresso dos Estados Unidos (Gallagher, 2022, p. 9).

Por outro lado, além das ameaças não intencionais acima relatadas, o atual cenário internacional revela preocupações com ameaças intencionais provenientes de atores estatais e não estatais, que podem ter como objetivo sabotar ou interceptar comunicações através dos cabos. Embora não haja definido um percentual exato dessas ameaças intencionais, elas vem representando uma camada a mais de vulnerabilidade que precisa ser enfrentada e considerada em estratégias de proteção (Gallagher, 2022, p. 10).

¹ A TeleGeography é uma empresa de pesquisa e consultoria especializada em telecomunicações, reconhecida por fornecer dados, análises, e visualizações independentes sobre redes globais, dentre elas, a rede de cabos submarinos. Mais informações disponíveis em: <https://www2.telegeography.com/about-us>. Acesso em: 09 fev. 2026.

Ao passo da consolidação da infraestrutura de cabos submarinos como espinha dorsal da conectividade global, observa-se a intensificação de práticas estatais destinadas à obtenção do controle e à exploração de dados, em um cenário marcado pela ampliação das capacidades técnicas de monitoramento e pela centralidade da informação como ativo de poder (Senado Federal, 2014a, p. 3).

Nossa história recente registrou um episódio de instauração de uma Comissão Parlamentar de Inquérito (CPI)²⁻³ cuja finalidade foi investigar a denúncia de existência de um sistema de espionagem estruturado pelo governo dos Estados Unidos da América (EUA), com o objetivo de monitorar e captar diversas formas de comunicação (inclusive dados digitais) de conteúdo privilegiado ou protegido constitucionalmente, em ofensa ao princípio da soberania e a outros princípios democráticos básicos do povo brasileiro (Senado Federal, 2014b, p. 6).

Sob uma perspectiva histórica, a preocupação com a proteção dos cabos submarinos não é recente, dado que a Convenção para a Proteção de Cabos Telegráficos Submarinos de 1884, diploma ainda vigente, já tinha disposições voltadas a salvaguardar os cabos telegráficos, meio de comunicação em expansão àquela altura. Todavia, mesmo já sendo reconhecido de longa data que interrupções significativas nas comunicações podem resultar impactos severos a qualquer país, algumas questões de segurança ainda parecem irresolutas, o que pode ser explicado, em parte, pelas peculiaridades do ambiente marinho onde os cabos estão dispostos, principalmente pelo seu regime jurídico, que o torna um cenário propício ao cometimento de delitos, cuja repressão se mostra de difícil implementação (Raha; Raju, 2021. p. 8-11).

Apesar da existência de um regime jurídico internacional consolidado para a proteção dos cabos submarinos, em especial no âmbito do Direito do Mar, verifica-se uma lacuna significativa quanto a interceptação de dados que por eles trafegam, levantando questionamentos acerca da suficiência do arcabouço regulatório vigente para responder as transformações tecnológicas e aos desafios estratégicos contemporâneos (Davenport, 2015, p. 97).

² As CPIs são instrumentos do Poder Legislativo previstos na Constituição Federal, com poderes de investigação próprios das autoridades judiciais, cuja finalidade é permitir aos parlamentares o exercício das suas atribuições de fiscalização da administração pública. Mais informações disponíveis em: <https://www12.senado.leg.br/assessoria-de-imprensa/releases/comissao-parlamentar-de-inquerito-o-que-e-e-como-funciona>. Acesso em: 08 fev. 2026.

³ A CPI da Espionagem, como ficou conhecida, foi instalada em 03/09/2023 em 09/04/2014.

A falta de clareza das normas do sistema internacional a respeito da (i)legalidade da espionagem em tempos de paz é fator gerador de uma ambiguidade jurídica que favorece a ocorrência de violações indiretas a normas e princípios consolidados pelo Direito Internacional, desafiando a atribuição de responsabilidades e causando dificuldades práticas para os Estados lidarem com esse problema, contribuindo para um ambiente de insegurança jurídica (Schmitt, 2017, p. 170)

Nesse ambiente, a interceptação de dados em cabos submarinos desponta como fenômeno particularmente sensível, desafiando os marcos jurídicos tradicionais, concebidos em um momento tecnológico diverso, e que tensiona os limites entre atividades toleradas internacionalmente e condutas potencialmente ilícitas.

A justificativa para a pesquisa situa-se nesse contexto, partindo do entendimento de que a segurança dos cabos submarinos, considerados como componentes de relevante infraestrutura crítica é essencial para o Brasil. O atual nível de dependência digital, a preocupação atual com o aumento de ameaças intencionais aos sistemas de cabos, a consolidação da prática de espionagem, a ambiguidade do Direito Internacional sobre o tema e as peculiaridades dos espaços marítimos são questões que justificam a necessidade do desenvolvimento de pesquisa nessa área, em razão do valor que possui a extensa malha de cabos submarinos existentes.

Em que pese a relevância dessa infraestrutura, ela teve início e se desenvolveu sem uma regulamentação específica, abrangente e eficaz que pudesse garantir o seu funcionamento. Some-se a isso, ainda, os fatos de que na maioria das vezes a sua propriedade é privada e que faz a interligação entre continentes através de regiões em que não há soberania de qualquer Estado, fatores estes que são dificultadores da manutenção da sua integridade.

Para isso, é importante identificar os principais desafios e ameaças que podem colocar em risco o bom funcionamento das comunicações pelos cabos submarinos, para, a partir de então, buscar soluções que possam contribuir com a preservação da soberania digital brasileira. Logo, este paradoxo, revelado por um lado pela extrema importância que a infraestrutura de cabos submarinos representa para o Brasil e, por outro, pela falta de uma

regulamentação adequada ao seu perfeito funcionamento é o nascedouro do interesse no desenvolvimento de pesquisa nesta área.

Ao investigar o arcabouço normativo afeto à proteção dos cabos submarinos, o trabalho poderá contribuir para o desenvolvimento de políticas públicas que manifestem a vontade estatal sobre uma atividade que também se desenvolve no mar e que com ele tem relação direta, favorecendo o fortalecimento da mentalidade de segurança e o desenvolvimento de normativas, procedimentos de monitoramento e protocolos de resposta a incidentes que poderão ser úteis não somente para reduzir riscos, mas também para criar um ambiente propício ao melhor aproveitamento de oportunidades econômicas que alavanquem o interesse estratégico e contribuam para o desenvolvimento nacional, assim como se dá com as demais atividades desenvolvidas no mar (Beirão, 2022, p. 320).

A pesquisa se depara, portanto, com o seguinte problema, que deriva do embate entre a importância estratégica da infraestrutura de cabos submarinos com as ameaças que podem comprometer o seu perfeito funcionamento, sobretudo as ameaças contemporâneas: o arcabouço jurídico atualmente vigente, no plano internacional e nacional, é adequado para garantir a proteção jurídica da infraestrutura de cabos submarinos contra a interceptação de dados nas Águas Jurisdicionais Brasileiras (AJB)?

Como possibilidade provisória de resposta ao problema apresentado é considerada a hipótese de que o ordenamento jurídico tanto no plano internacional quanto no doméstico não dispõe de meios suficientes que possam garantir a proteção jurídica contra eventuais ações de interceptação de dados nos cabos submarinos, tendo em vista a existência de ambiguidades e lacunas afetas ao tema.

O objetivo geral do trabalho, portanto, é a análise das disposições normativas do Direito Internacional, bem como da legislação nacional, de incidência sobre os cabos submarinos, com vistas a identificar as possibilidades e limitações da atuação brasileira contra ações de interceptação dos seus dados nas AJB.

Com o intuito de alcançar o objetivo geral proposto, a pesquisa foi estruturada a partir de cinco objetivos específicos, os quais orientam de maneira progressiva e complementar o desenvolvimento do trabalho. Cada objetivo específico corresponde a um

capítulo próprio, permitindo o desenvolvimento sistematizado dos aspectos jurídicos relacionados de forma autônoma, mas integrada à compreensão lógica do problema, o que permitirá a consolidação das conclusões apresentadas ao final.

O primeiro capítulo abordará a infraestrutura de cabos submarinos e a interceptação dos seus dados como um risco estratégico, contextualizando a sua representatividade para a sociedade atual. Serão discutidas questões como a natureza das ameaças contemporâneas, nelas inseridas a interceptação, seus tipos e alguns casos históricos de relevância que tiveram impacto para a compreensão atual da questão, permitindo delinear a questão jurídica que desafiou a consecução do presente trabalho.

O capítulo dois será dedicado à análise do tratamento jurídico conferido à interceptação pelo Direito Internacional, buscando estabelecer os fundamentos jurídicos gerais que norteiam a sua compreensão no plano internacional. Inicialmente, o capítulo examina a interface do tema com o Manual Tallinn 2.0, utilizando-o como parâmetro interpretativo relevante para a aplicação de normas do Direito Internacional à operações cibernéticas, ainda que sua natureza seja de norma não vinculante. Em seguida, discute-se a caracterização da interceptação como forma de espionagem técnica, situando-a no contexto histórico e contemporâneo das atividades de inteligência estatais, bem como a ausência de disposição expressa proibitiva em tempo de paz no Direito Internacional. O capítulo avança na análise da incidência dos princípios da soberania e da não intervenção, assim como na aplicação dos direitos humanos, com especial atenção ao princípio da privacidade, como elementos normativos voltados à avaliação da licitude da prática. Ao final do capítulo, é analisada a inadequação da interceptação ao conceito de investigação científica marinha, distinguindo-as das atividades caracterizadas como usos legítimos do mar.

O capítulo três desenvolve o objetivo parcial de analisar de forma sistemática o regime internacional aplicável aos cabos submarinos, identificando seus fundamentos normativos, lacunas e limitações diante dos desafios contemporâneos. A análise parte da Convenção das Nações Unidas sobre o Direito do Mar (CNUDM) como marco central, examinando os distintos regimes jurídicos estabelecidos para cada espaço marítimo e suas implicações para a proteção dos cabos submarinos. São também analisados outros instrumentos internacionais relevantes, como a Convenção para a Proteção dos Cabos Submarinos de 1884, o Regulamento Internacional para Evitar Abalroamentos no Mar

(RIPEAM), a Convenção de Londres de 1972 sobre a prevenção da poluição marinha por alijamento de resíduos e outras matérias, as normas do Direito Internacional aplicável aos conflitos armados, as convenções internacionais de combate ao terrorismo e as normas elaboradas pelo International Cable Protection Committee (ICPC). A partir desse conjunto normativo heterogêneo, é desenvolvido um diagnóstico sobre o regime jurídico internacional vigente.

O capítulo quatro será dedicado a analisar os cenários normativos futuros para a regulação internacional, partindo das insuficiências identificadas no regime jurídico vigente. Serão apresentadas algumas das principais consequências da ausência de regulação específica sobre a interceptação. Em seguida serão examinadas as principais propostas doutrinárias e institucionais voltadas ao aprimoramento da disciplina normativa do tema, considerando as contribuições dos organismos internacionais, fóruns especializados e literatura acadêmica. O capítulo segue na avaliação das modalidades de regulação internacional possíveis, analisando alternativas como instrumentos de *soft law*, acordos regionais e a eventual adoção de um tratado multilateral de alcance global. Uma proposta sobre o conteúdo material desejável de um instrumento internacional de regência é apresentado ao final do capítulo, sistematizando a opinião de especialistas com o fim de estabelecer balizas para respostas ao fenômeno estudado.

O quinto e último capítulo volta-se à análise dos desafios e das competências do Estado brasileiro no que se refere à interceptação de dados em cabos submarinos localizados nas AJB, relacionando o debate internacional com a realidade normativa e institucional nacional. Preliminarmente, o capítulo apresenta o conceito de AJB, destacando suas especificidades e as controvérsias existentes entre a concepção adotada pelo Brasil e a delimitada pelo Direito Internacional do Mar. Em seguida, é examinado o exercício da jurisdição brasileira nos diversos espaços marítimos, avaliando os limites e as possibilidades de atuação. O capítulo também se dedica a análise dos instrumentos jurídicos domésticos aplicáveis à segurança dos cabos submarinos, incluindo normas constitucionais, legais e infralegais estratégicos voltados à proteção das infraestruturas críticas. Por fim, aborda-se o papel da Marinha do Brasil tanto na condição de Autoridade Marítima, responsável pela regulação e fiscalização das atividades no ambiente marítimo, quanto como expressão do Poder Naval, incumbida da defesa dos interesses nacionais frente às ameaças intencionais oriundas do mar.

Após os capítulos de desenvolvimento do trabalho, será apresentada uma conclusão de modo a sintetizar e sistematizar os resultados obtidos durante a pesquisa, com o propósito de responder o problema de pesquisa no que se refere à aptidão do ordenamento jurídico vigente para a proteção jurídica face a atividades de interceptação de cabos submarinos nas AJB.

Passando a tratar sobre aspectos metodológicos, inicialmente é oportuno deixar claro que não é ignorado que os conceitos de segurança e proteção possuem escopos distintos quando considerados no âmbito do Direito do Mar e que em razão de uma particularidade da Língua Portuguesa, que não possui termos distintos para a noção semântica do vocábulo “segurança”, sua utilização ocorre por vezes com imprecisão (Beirão, 2014, p. 136). Todavia, apesar desse fato importar na compreensão correta do alcance dos termos *maritime safety* e *maritime security*, conforme será detalhado no capítulo 5 deste trabalho, ambos os termos (segurança e proteção) são adequados ao exame das ameaças contra os cabos submarinos, podendo ser compreendidos como espécies de um gênero maior de tutela desses ativos, razão pela qual serão tratados como intercambiáveis e representativos de uma ideia geral de “segurança”, assim como faz o idioma português.

O referencial teórico utilizado preponderantemente foi o Tallinn Manual 2.0 que, apesar de não constituir documento com caráter vinculativo, representa obra acadêmica altamente influente que oferece a interpretação de especialistas sobre o estado do Direito Internacional aplicável às operações cibernéticas em tempo de paz, decorrendo a sua autoridade do fato de ter sido elaborado por um grupo independente de especialistas de diversas nacionalidades, sob coordenação da OTAN,⁴ sistematizando de forma rigorosa a interpretação de normas convencionais e consuetudinárias do Direito Internacional, motivo pelo qual se mostra de relevante aplicação na análise jurídica da interceptação de dados em cabos submarinos.

O método de abordagem utilizado foi o hipotético-dedutivo, partindo de uma hipótese que surge com a premissa da necessidade de segurança dos cabos submarinos contra ações de interceptação de dados, passando pela análise das ameaças contemporâneas e o seu

⁴ A Organização do Tratado do Atlântico Norte (OTAN ou NATO, seu acrônimo em Inglês) é uma aliança militar intergovernamental que une países na Europa e da América do Norte para garantir a segurança coletiva e de seus membros, baseando-se no princípio de que o ataque a um membro é um ataque a todos. Informações disponíveis em: <https://www.nato.int/en/what-we-do/introduction-to-nato/natos-purpose>. Acesso em: 08 fev. 2026.

confronto com as disposições que compõem o arcabouço jurídico e normativo, internacional e nacional, de incidência sobre o tema, permitindo-se chegar a um diagnóstico sobre a sua adequação.

A pesquisa também apresenta uma abordagem qualitativa de natureza jurídico-dogmática, adequada ao conhecimento de elementos que integram um sistema jurídico-normativos específico - como é o caso do Direito Internacional - com ênfase na interpretação sistemática e teleológica nas normas internacionais e nacionais aplicáveis aos cabos submarinos e à interceptação de seus dados. Esse método permitiu analisar criticamente o arcabouço vigente, bem como as possibilidades de ações estatais com os seus parâmetros.

Complementarmente, a pesquisa utilizou a hermenêutica, especialmente no exame de instrumentos como a CNUDM, o Tallinn Manual 2.0 e outros documentos internacionais relevantes, de modo a compreender o alcance e a aplicação de conceitos como soberania, não intervenção e direitos humanos.

Quanto às fontes utilizadas, a pesquisa foi desenvolvida predominantemente com base em fontes bibliográficas e documentais, incluindo tratados internacionais, leis, relatórios, normas administrativas, recomendações de entidades técnicas e literatura científica especializada.

A seleção desses dados foi realizada intencionalmente em um universo de fontes abertas e informações públicas, assegurando a verificabilidade das informações e a coerência com o objeto de estudo. No que se refere ao plano internacional, o âmbito da pesquisa abrangeu tratados e convenções multilaterais com relevância direta ou indireta para os cabos submarinos, com ênfase na CNUDM pela abrangência das suas disposições e ampla adesão global. No plano interno, foram analisados diversos tipos de documentos, com preponderância para os decretos de regulamentação das infraestruturas críticas brasileiras e para o Projeto de Lei nº 270/2025, que objetiva instituir uma política específica afeta à infraestrutura de cabos subaquáticos. No âmbito doutrinário, a pesquisa limitou-se à literatura científica especializada, composta por artigos, relatórios técnicos e livros disponíveis em bases de dados institucionais e acadêmicas, priorizando as abertas, sendo evitadas fontes de cunho não científico.

2 INFRAESTRUTURA SUBMARINA DE CABOS E A INTERCEPTAÇÃO COMO RISCO ESTRATÉGICO

2.1 PANORAMA

A partir da segunda metade do século XIX, com a instalação do primeiro cabo telegráfico em 1850, permitindo a transmissão de dados entre as cidades de Dover e Calais, respectivamente na Inglaterra e na França, a utilização de cabos submarinos como meio de comunicação internacional foi se tornando cada vez mais relevante, culminando com a implementação dos cabos de fibra ótica na década de 1980, elevando exponencialmente o fluxo de dados transmitidos e recebidos (Heinegg, 2013, p. 292).

O impacto da Internet na sociedade mundial atualmente é um fato incontestável. Com o seu embrião na ARPANET⁵, rede pioneira que lhe deu origem, a Internet foi projetada para múltiplas finalidades, pensada como uma infraestrutura que pudesse suportar novos usos. Até alcançar o seu estágio atual, a Internet teve o seu desenvolvimento lastreado em diversos fatores condicionantes, como por exemplo a evolução tecnológica, a gestão operacional, os aspectos sociais e a comercialização, crescendo e se desenvolvendo a partir de uma visão aberta de rede para formar a base da infraestrutura que conhecemos hoje (Leiner, 1997, p. 5).

A curva ascendente dos avanços tecnológicos que se experimenta na contemporaneidade é fruto da fluidez com que as informações tramitam pelo ciberespaço, sem a qual os modelos de atividades como comunicação, educação, segurança, comércio, serviços públicos estariam comprometidos por se encontrarem diretamente dependentes da rede mundial de computadores (Sunak, 2017, p. 9).

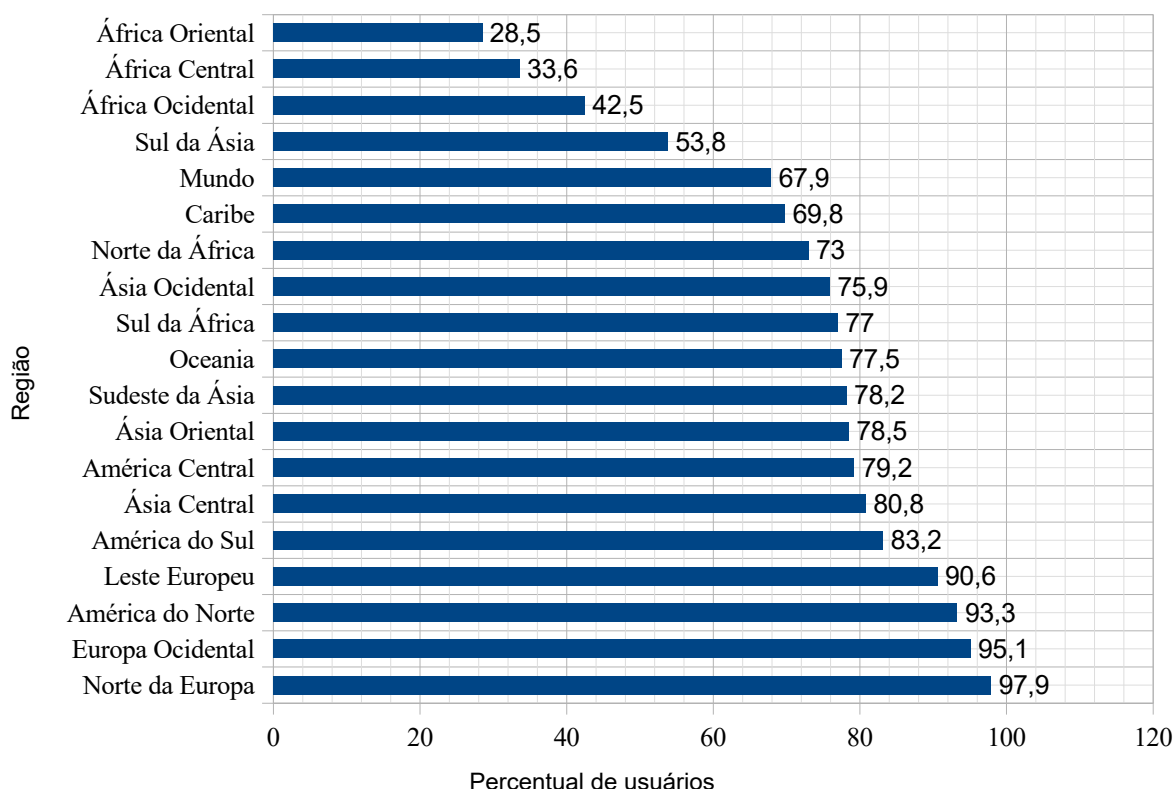
De acordo com dados de fevereiro de 2025, a população mundial conta com 8,23 bilhões de pessoas, das quais 5,65 bilhões possuem acesso à Internet, o que representa 68,7%

⁵ Rede pioneira que deu origem à Internet, desenvolvida pela Advanced Research Projects Agency (ARPA), sendo o primeiro experimento bem-sucedido de rede de comutação de pacotes, que tinha o objetivo de conectar múltiplos computadores para permitir a comunicação e o compartilhamento de recursos entre pesquisadores e instituições.

do total. O Norte Europeu ocupa a primeira posição no ranking de utilização da rede, com quase 98% das pessoas como usuárias, seguido de perto pela Europa Ocidental, com 95,1% de usuários, sendo o crescente desenvolvimento da infraestrutura de comunicações e o contínuo desenvolvimento das redes os principais responsáveis pela expansão da taxa de penetração da Internet (Statista, 2025).

A Figura 1 permite compreender melhor a dimensão global da Internet. Em que pese a disparidade entre as taxas das regiões com maior desenvolvimento quando comparadas com as de menor, revelando que a universalidade de acesso à rede ainda continua difícil de ser alcançada, é inegável o seu impacto a nível global, o que é comprovado pela taxa de uso mundial em aproximadamente 68%, conforme relatório da *International Telecommunications Union* (ITU, 2024).

Figura 1: Taxa de usuários de internet por região.

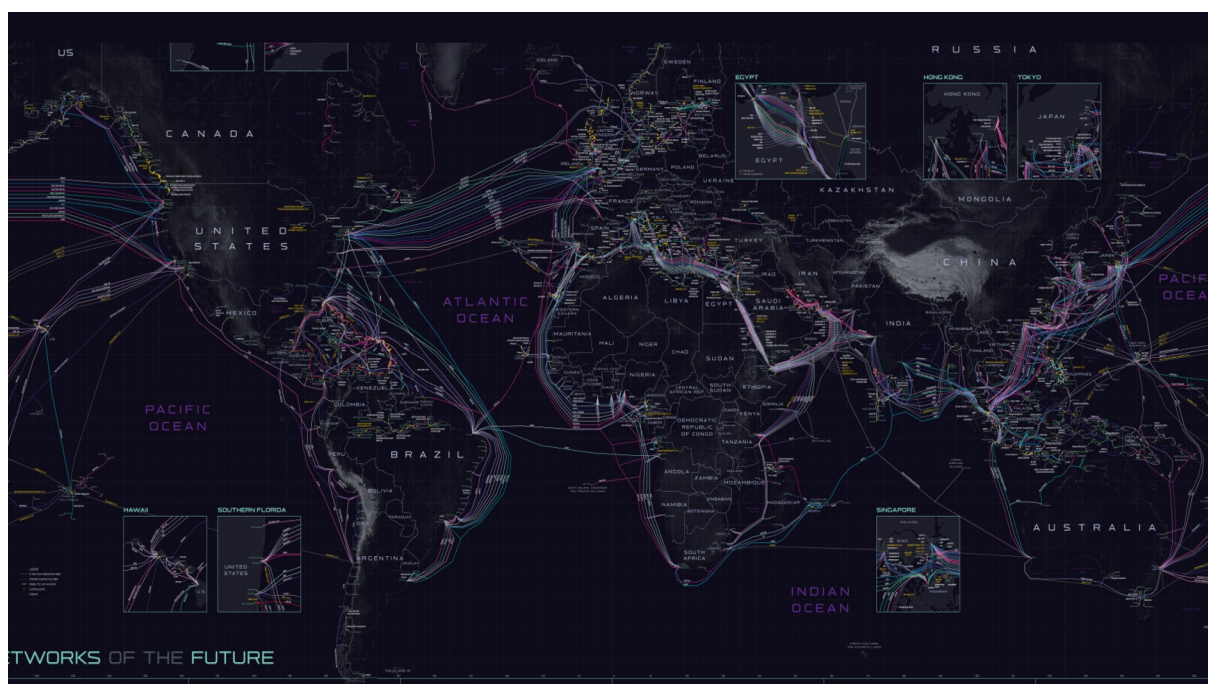


Fonte: elaborado pelo autor.

Diferentemente da percepção que permeia o senso comum, a grande maioria do fluxo de dados na internet não trafega por intermédio de satélites, mas sim através dos cabos

de fibra ótica, responsáveis por mais de 95% das informações trafegadas, distribuídos aproximadamente por 559 sistemas de cabos independentes. Tais sistemas formam uma rede de conexões estabelecida através do oceano, para além dos limites territoriais dos Estados e das respectivas jurisdições, constituindo as artérias físicas invisíveis da rede mundial de computadores (figura 1), o que evidencia a necessidade de se pensar em um regime de governança que possa garantir a integridade necessária ao perfeito funcionamento desse sistema (Davenport, 2015, p. 82).

Figura 1 – Representação dos cabos submarinos no mundo (recorte).



Fonte: TeleGeography

Disponível em: <https://submarine-cable-map-2025.telegeography.com>

Sob a ótica brasileira, refletindo a necessidade mundial de conexão e o atual estágio de dependência da Internet, a Lei nº 12.965/2014, conhecida como Marco Civil da Internet, no seu art. 2º reconhece a escala mundial da rede e associa o seu uso aos direitos humanos, da personalidade e ao exercício da cidadania, todos esses direitos muito caros a uma sociedade democrática (Brasil, 2014).

Pontieri (2022, p. 2) destaca que a lei busca assegurar o equilíbrio entre os princípios de neutralidade da rede e a liberdade de expressão na internet, objetivando garantir o seu uso de forma democrática, isonômica e livre, mas sem descuidar dos limites e responsabilidades necessários a evitar abusos e práticas ilegais que podem comprometer os aludidos direitos e princípios.

Sob essa visão, é possível afirmar que a resiliência, segurança e capacidade da infraestrutura de cabos submarinos estão relacionadas ao pleno exercício dos direitos de comunicação e liberdade de expressão, que não poderiam ser manifestados na sua perspectiva mais ampla em caso de impossibilidade de acesso à internet, de tal modo que não é exagerado falar em cidadania digital.

Ao dispor na Resolução nº 65/37, da sua Assembleia Geral, que os cabos submarinos constituem infraestrutura crítica de comunicações e fazer um apelo aos Estados para que tomem medidas voltadas à proteção dos mencionados cabos, a Organização das Nações Unidas evidenciou a preocupação dos seus signatários com o perfeito funcionamento desse sistema (ONU, 2010, p. 3). Porém, muito antes da edição dessa Resolução, levada a efeito em 2010, a ONU já defendia que a colocação de cabos submarinos (assim como dutos) em alto mar é um direito expressamente reconhecido aos Estados, conforme disposto na Convenção das Nações Unidas sobre o Direito do Mar – CNUDM, internalizada no ordenamento jurídico brasileiro pelo Decreto nº 1.530, de 22 de junho de 1995 (Brasil, 1995).

A definição de infraestruturas críticas surgiu pela primeira vez no Brasil em 2008, fruto de trabalho desenvolvido pelo Gabinete de Segurança Institucional da Presidência da República (GSI-PR), podendo ser conceituada como “[...] aquelas instalações, serviços e bens cuja interrupção ou destruição provocará sério impacto social, econômico, político, internacional ou à segurança nacional”, conforme descrito na Estratégia Nacional de Segurança de Infraestruturas Críticas (Brasil, 2020, p. 2).

À vista disso, é possível perceber a existência de uma relação direta de interdependência entre a soberania estatal e o perfeito funcionamento do sistema responsável pelo fluxo de dados no ciberespaço, de modo que a incapacidade estatal de proteger as suas infraestruturas digitais pode comprometer a estabilidade interna. Sendo assim, a necessidade de o Brasil estar atento ao tema é questão estratégica e diretamente relacionada ao pleno

exercício da sua soberania em um contexto digitalizado e globalizado (Zuccaro et al., 2025, p. 30).

A Política Nacional de Defesa – PND, documento condicionante de mais alto nível do planejamento das ações de defesa nacional, recentemente aprovada pelo Decreto nº 12.725/2025 (que aprovou também os textos da Estratégia Nacional de Defesa e do Livro Branco de Defesa Nacional), cita especificamente os cabos submarinos, prescrevendo no seu item 1.2 que a sua segurança e defesa, assim como do espaço cibernético e demais infraestruturas críticas, são essenciais para mitigar a possibilidade de uma desordem social, revelando a sua importância em matéria de defesa (Brasil, 2025).

Em âmbito mais específico, a Política Nacional de Segurança de Infraestruturas Críticas – PNSIC, aprovada pelo Decreto nº 9.573/2018, tem como um de seus princípios a salvaguarda dos interesses da defesa e da segurança nacional⁶, deixando ainda mais claro que a manutenção da operabilidade dos serviços é matéria diretamente afeta à defesa e, portanto, à segurança nacional e soberania (Brasil, 2018).

2.2 NATUREZA DAS AMEAÇAS CONTEMPORÂNEAS

Os estudos afetos à segurança marítima são delineados em função da natureza das ameaças enfrentadas, que contemporaneamente são marcadas pela complexidade, interconectividade, caráter transnacional e multissetorial, transcendendo preocupações tradicionais de *sea power*⁷ e guerra interestatal, encaixando-se a interceptação de dados em cabos submarinos na categoria de ameaças não tradicionais ou híbridas (Bueger; Edmunds, 2017, p. 4).

⁶ Art. 2º São princípios da PNSIC:

IV – A salvaguarda do interesse da defesa e da segurança nacional.

⁷ As preocupações tradicionais de *sea power* são compreendidas como aquelas que representam uma visão mais tradicional de poder marítimo, que priorizam a capacidade militar de um Estado no mar para projetar poder, defender seus interesses e competir ou manter a ordem em um cenário internacional muitas vezes anárquico ou competitivo (Bueger; Edmunds, 2017, p. 3).

No mesmo ritmo em que foi ficando cada vez mais evidente a relevância e ocorrendo a expansão dos sistemas de cabos submarinos, verificou-se também uma crescente nos índices de incidentes que acarretam danos aos cabos. Considerando que são dispostos no leito do mar, acabam ficando expostos a uma série de ameaças, que vão desde atividades humanas regulares como a pesca e a navegação, até riscos naturais, como, por exemplo, terremotos, conforme destaca Davenport (2015, p. 78).

Além disso, em função da sua localização muitas vezes pública e concentrada, a estrutura de cabos submarinos acaba sendo suscetível a ataques intencionais por parte de grupos violentos não estatais (Sunak, 2017 apud Bueger; Liebetrau, 2021, p. 395). Logo, quando se pensa nos tipos de danos que os cabos submarinos estão sujeitos, devemos ter em mente que existem os não intencionais, causados tanto pela ação humana quanto por causas naturais, e os intencionais, causados pela ação humana deliberada.

O International Cable Protection Committee (ICPC), organização de natureza privada que congrega diversos *stakeholders* de cabos submarinos, inclusive governos, criada com o propósito de liderar e orientar sobre diversas questões da área (Roach; Smith, 2012, p. 456), revela que, de acordo com as suas estatísticas, a pesca e a ancoragem de navios são responsáveis por mais de 70% dos danos globais causados aos cabos submarinos, percentual muito maior do que qualquer outra causa natural ou humana, conforme notícia publicada no site da instituição.⁸

Ainda que o foco deste trabalho seja a interceptação de dados em cabos submarinos nos espaços marinhos, é necessário contextualizar e dizer que tal atividade pode ocorrer também quando o cabo estiver em terra, como, por exemplo, nos locais de aterrissagem dos cabos. Como alerta Sunak (2017, p. 24), geralmente há um ponto de estrangulamento, com vários cabos chegando no mesmo lugar e sendo direcionados para estações (geralmente galpões ou prédios) sem a adequada segurança, o que representa uma vulnerabilidade. Uma série de discussões relacionadas à segurança dos cabos em terra pode emergir, tais como competências, responsabilidades, penalidades, regime de governança e outros, mas, como dito, o foco do presente trabalho é a “fase marinha” dos cabos, razão pela qual não adentraremos detalhadamente em abordagens afetas à interceptação durante a “fase

⁸ ICPC. Charting submarine cables is a critical for maritime safety and infrastructure protection. Disponível em: <https://www.iscpc.org/publications/icpc-viewpoints/charting-submarine-cables-is-critical-for-maritime-safety-and-infrastructure-protection/>. Acesso em 07 abr. 2025.

terrestre” das estruturas, ainda que não nos furtemos de abordar alguns aspectos relacionados a esse viés.

Apesar de representarem a minoria nas estatísticas referentes aos incidentes, os danos intencionais constituem uma significativa ameaça à infraestrutura crítica de comunicação mundial, sobretudo em tempos de tensões mundiais, conforme aponta Burnett (2021, p. 1678). Explica o autor que, em tempos de paz, os danos podem ser causados por uma variedade de atores e distintas motivações, que podem ir desde a mera obtenção de vantagem econômica a partir do furto dos cabos e a venda do material, até a intenção terrorista de desestabilizar economicamente um país por intermédio de ataques de sabotagem, da interceptação e da espionagem, apontando que, embora existam tratados internacionais que forneçam uma base de proteção, há lacunas significativas na legislação internacional.

Então, considerando que a seara do presente trabalho está nas ameaças intencionais às referidas infraestruturas, não é desnecessário mencionar que são variadas e podem ocorrer tanto em contexto de paz quanto em guerra, tendo como causadores tanto Estados como grupos maliciosos, com objetivos também variados (políticos, estratégicos ou econômicos).

Nos dias atuais o escopo das ameaças vem se tornando cada vez mais complexo, haja vista que a vulnerabilidade das infraestruturas submarinas as torna mais suscetíveis de estratégias híbridas de ataques, nas quais operações de sabotagem e espionagem podem ser empreendidas por atores estatais ou não estatais, mediante a utilização de um *modus operandi*⁹ que pode empregar métodos de guerra convencional, irregular ou de informação sem que isso importe em uma escalada convencional imediata (Pedrozo, 2025, p. 49).

É importante considerar que os ataques aos cabos podem incidir sobre a sua estrutura física, objetivando destruí-lo ou danificá-lo enquanto meio material, bem como pode incidir sobre os dados que trafegam pelo sistema. Schaller (2025, p. 175) aponta que tal distinção se revela importante na medida em que a análise jurídica acaba condicionada à natureza da ameaça, já que diferentes tipos de danos podem ter diferentes enquadramentos e,

⁹ *Modus operandi* é um termo em latim que significa "modo de operar" ou "maneira de agir", referindo-se a um método característico ou padrão de comportamento utilizado durante a realização de alguma ação.

consequentemente, distintas repercussões sob o manto do Direito Internacional, que será melhor abordado no capítulo seguinte.

No âmbito dos danos físicos, a sabotagem, apesar da falta de uma definição formal sobre o que seria o seu conceito, é caracterizada por ações intencionais cujo objetivo é causar danos físicos ou interrupções do fluxo de dados na infraestrutura de cabos. Heinegg (2013, p. 294) menciona que a sabotagem pode ocorrer de diversas formas, incluindo a utilização de cortes deliberados, arrasto de âncoras de embarcações, instalação de explosivos e qualquer outro expediente capaz de causar dano à infraestrutura.

Passando às ameaças incidentes sobre os dados, a interceptação se revela como um campo de análise complexo, na medida em que é marcada por divergências entre os estudiosos do tema acerca da sua possibilidade, como será detalhado na próxima seção.

2.3 INTERCEPTAÇÃO DE DADOS

Anteriormente ao aprofundamento das questões relacionadas a esta pesquisa, é necessário estabelecer uma definição de interceptação de dados, com o objetivo de conferir rigor dogmático e segurança metodológica ao seu desenvolvimento, evitando dúvidas acerca do seu alcance. À vista da ausência de um conceito técnico formal na legislação internacional e nacional, adotaremos um conceito a partir da conjugação da Lei nº 9.296/1996, que dispõe sobre interceptação de comunicações telefônicas e do fluxo de comunicações em sistemas de informática e telemática (Brasil, 1996, Art. 1º), com a definição deste último vocábulo. Desta feita, considerando que telemática é definida como o conjunto de serviços e técnicas que combinam recursos informáticos com os das telecomunicações (Carvalho, 2023, p. 4) e que os dados que trafegam pelos cabos submarinos estão inseridos nesta definição, neste trabalho será considerado como interceptação de dados o acesso, a captura ou o monitoramento não autorizado e clandestino de informações enquanto trafegam pela infraestrutura de cabos submarinos.

Isso posto, é necessário dizer que a interceptação de dados tornou-se uma questão altamente relevante nas discussões sobre Segurança da Informação¹⁰, uma vez que o acesso e a captação de dados proveniente das infraestruturas de comunicação envolve questões de segurança, privacidade e soberania, considerando a possibilidade de que as informações captadas podem ser confidenciais e estratégicas (Devanny; Martin; Stevens, 2021, p. 3).

Em tese, ela se dá mediante a colocação de dispositivos especiais que são capazes de realizar a coleta de dados transmitidos através dos cabos, utilizando técnicas sofisticadas sem que ocorra dano ao material e comprometimento da comunicação.

Quanto a esse ponto, inicialmente é necessário destacar a divergência de alguns estudiosos do assunto quanto a sua possibilidade de realização. O Professor Luís Manuel Brás Bernardino afirma que a possibilidade de realizar a “escuta” do cabo submarino, captando as informações que nele trafegam, é um mito que precisa ser desmistificado, pois a partir do momento em que a fibra é tocada ela se rompe, cessando de imediato o fluxo de informações e inviabilizando a interceptação de dados (Panorama, 2025, 11 min 50 s). No mesmo sentido, opina também José Sousa Barros, afirmando que a interceptação apenas pode ocorrer em terra, mas não na água (Jornal da Economia do Mar, 2025, 33 min 30 s).

Por outro lado, notícias antigas já davam conta de que a interceptação de cabos submarinos é uma prática já há muito utilizada por alguns governos. Já no ano de 2005, a Associated Press noticiou que o submarino americano USS Jimmy Carter foi preparado para transportar equipes técnicas ao fundo do mar com a finalidade de realizar a interceptação das redes de fibra ótica mediante a colocação de grampos ao longo do curso do cabo (The New York Times, 2005).

Desta feita, em que pese a divergência acerca da (im)possibilidade de interceptação física dos cabos submarinos, tal fator não compromete a relevância nem a coerência do presente trabalho, por duas razões fundamentais. A uma, porque o objeto principal da pesquisa não incide sobre aspectos técnicos de engenharia ou tecnologia dos sistemas de cabos, mas sim sobre o regime jurídico aplicável à conduta de interceptar dados, considerada como possibilidade fática e risco estratégico. Se por um lado o Direito é uma

¹⁰ Segurança da Informação - ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações (Portaria GSI/PR nº 93, de 18 de outubro de 2021 – Aprova o Glossário de Segurança da Informação).

ciência pós-fato, por outro não se pode ignorar que, em matérias relacionadas a soberania e defesa nacional, não pode haver dependência de confirmações empíricas de ameaças potenciais, sob pena de se estabelecer um regime reativo e defasado. E a duas, porque a velocidade com que ocorrem as evoluções no domínio tecnológico é típica e marcada por sucessivas rupturas de capacidade, de modo que tecnologias que hoje podem ser consideradas inviáveis, podem em um futuro breve se tornarem possíveis.

Por tais razões, mesmo que se admitia, em tese, alguma limitação técnica à capacidade de realizar ações de interceptação de dados em cabos submarinos na sua fase marinha, o presente trabalho pode contribuir, em alguma medida, com o dever Estatal de antecipação jurídico-normativa frente ao *status* estratégico que o tema está envolto.

2.3.1 Tipos de Interceptação

Apenas com a finalidade de contextualizar o debate jurídico que será o foco principal da pesquisa e demonstrar que não se trata de mera hipótese remota e abstrata, mas uma possibilidade potencial e plausível, serão apresentados alguns tipos e técnicas de interceptação de cabos submarinos. Então, a menção às técnicas possui caráter meramente contextual, sem qualquer pretensão de aprofundamento técnico, com o objetivo apenas de delimitar o fenômeno fático implícito ao problema jurídico que será analisado.

A depender da forma na qual a interceptação é realizada ela pode ser lógica (ou remota) ou física. A interceptação lógica é caracterizada pelo acesso e coleta de informações sem que haja a intervenção física direta na infraestrutura, mediante a utilização de meios digitais ou cibernéticos de maneira remota, valendo-se de métodos mais abstratos relacionados a vulnerabilidades de software ou de protocolos de comunicação, conforme Grishachev (2020, p. 682). Já quanto à interceptação física, o autor ensina que o processo de obtenção das informações se dá por meio de conexões físicas com o cabo óptico, desviando parte da radiação óptica que passa pela fibra, o que pode ser realizado por intermédio de diversas técnicas.

Heinegg (2013, p. 303) cita outros métodos específicos de interceptação física, como a colocação de uma escuta em algum ponto do cabo (*tapping*); a realização de dobra no cabo, permitindo que uma pequena quantidade de luz escape permitindo o monitoramento de dados (*bendding*); e a utilização de divisores (*splitter*), permitindo que o tráfego de dados seja desviado sem interromper a transmissão principal.

Com outro enfoque, Botua, Dewi e Siswandi (2022,p. 35) distinguem os tipos de interceptação em função do seu direcionamento, separando-as em duas categorias, quais sejam, a interceptação em massa (*bulk interception*), caracterizada pela falta de um direcionamento definido quanto ao destinatário ou conteúdo a ser interceptado, e a direcionada (*signals intelligence*), com foco específico em indivíduos ou comunicações determinadas.

2.3.2 Alguns Casos Conhecidos de Interceptação

A utilização de técnicas de interceptação de comunicações por intermédio de cabos submarinos não pode ser chamada de recente, apesar de mais atual do que nunca. Nesse sentido, serão apresentados a seguir alguns casos de interceptação que ocorreram ao longo dos anos e que tiveram destaque, demonstrando a continuidade histórica da prática da interceptação de comunicações e a atualidade do problema.

2.3.2.1 1902-1903 “All-Red Line”

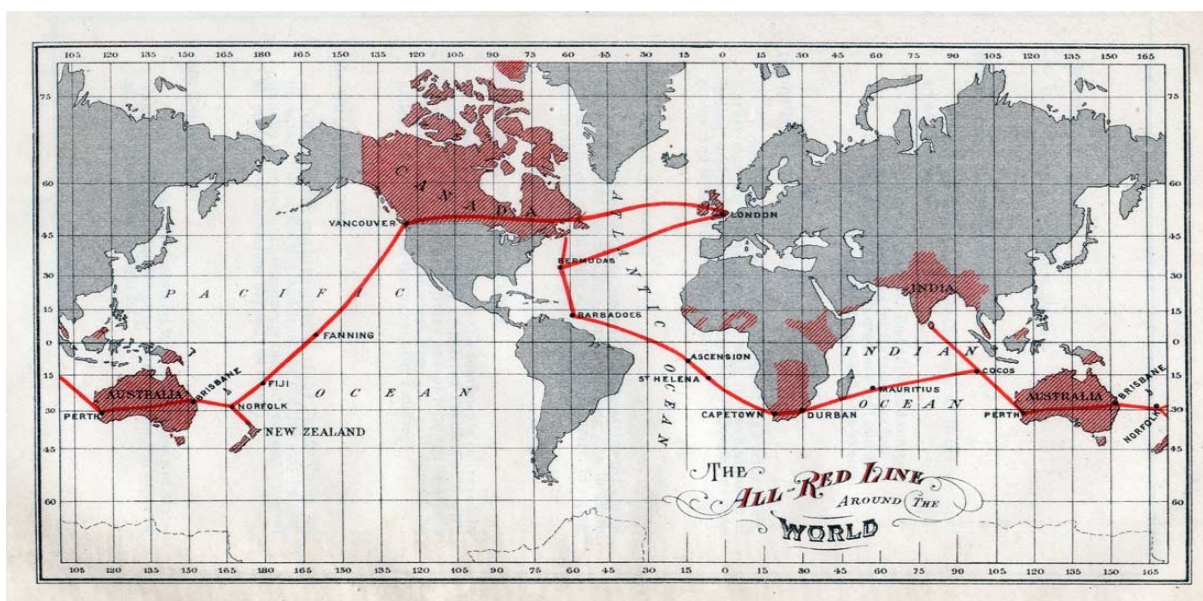
O império britânico consolidou a sua rede global de cabos telegráficos, a “All-Red Line”, que recebia esse nome em função da abrangência global e da sua representação na cor vermelha (assim como das colônias e territórios britânicos) nos mapas da época, conforme representado na figura 3.

Bufithis (2021) explica que a rede foi operada por uma mistura de empresas pública e privada com a *Eastern Telegraph Company*, permitindo que as comunicações que antes demoravam meses para serem realizadas entre o império e seus domínios pudessem ocorrer em questão de horas.

Bruthon (2017, p. 23) indica que não há relatos de que a All-Red Line tenha sido alvo de interceptação bem-sucedida, tendo em vista que foi projetada sem fazer entrada em territórios que não fossem britânicos e com segurança reforçada nos pontos em que chegava em terra, com vistas a reduzir as possibilidades de interceptação e espionagem, demonstrando a importância que o Reino Unido dava ao controle da informação e à prevenção contra os riscos que uma interceptação realizada pelo inimigo pode expor, como ocorreu no caso do Telegrama Zimmermann.

Logo, apesar de o presente caso não representar uma passagem de interceptação realizada com sucesso, foi citado como representativo da noção de que a consolidação de um sistema seguro de comunicação confere uma vantagem importante em eventuais conflitos, revelando que já no início do século XX havia preocupação com a segurança dos cabos e que a sua infraestrutura sempre foi tratada como questão sensível de poder estatal.

Figura 3 – All-Red Line



Fonte: <https://www.gregorybufithis.com>

2.3.2.2 1917 - Telegrama Zimmermann

Durante a primeira Guerra Mundial a interceptação de dados e a decodificação de informações que trafegavam por intermédio de cabos (àquela época telegráficos), era uma atividade estratégica importante. No caso que ficou conhecido como “Telegrama Zimmermann”, um telegrama do Ministério das Relações Exteriores da Alemanha para o seu embaixador no México, cujo conteúdo versava sobre uma proposta de aliança entre os dois países contra os Estados Unidos, foi transmitido por meio de cabos diplomáticos considerados neutros (possivelmente dinamarqueses e suecos), tendo em vista que os cabos alemães haviam sido cortados, sendo a transmissão interceptada quando trafegava pelo Reino Unido, provavelmente por intermédio de um relé em uma estação de retransmissão. Após ser decifrado, o conteúdo do telegrama foi transmitido aos Estados Unidos, contribuindo para a entrada dos americanos na guerra ao lado dos Aliados em 1917 (Bruton, 2017, p. 21).

Durante o conflito, a interceptação e decodificação de mensagens foi prática reiterada e desenvolvida, sendo o embrião do que mais tarde seria conhecido como inteligência de sinais (SIGINT). Este caso demonstra como um caso de interceptação de cabos submarinos tem potencial para impactar diretamente decisões geopolíticas globais, inclusive influenciando na entrada de um país em uma guerra ou até mesmo na sua deflagração. Por esse motivo, a tolerância internacional com ações de interceptação de cabos submarinos se mostra temerária, uma vez que delas podem resultar consequências para a soberania, segurança e ordem internacional, razão pela qual não podem ser tidas como atividades neutras ou inofensivas.

2.3.2.3 Década de 1970 - Operação Ivy Bells

Outro caso de grande notoriedade foi a denominada “Operação Ivy Bells”, iniciada no início dos anos 1970, que consistiu em uma operação conjunta envolvendo a Marinha dos Estados Unidos e a Agência de Segurança Nacional americana (NSA), com o

propósito de realizar interceptação das comunicações soviéticas no Mar de Okhotsky, no Pacífico.

A operação contava com a participação de submarinos dos EUA ingressando em áreas restritas com o propósito de colocar dispositivos ao redor de cabos de comunicação soviéticos altamente confidenciais, permitindo realizar a escuta e captação de informações criptografadas que seriam posteriormente decifradas. A operação foi comprometida por espionagem humana (HUMINT), quando um analista da NSA chamado Ronald Peltron revelou conhecimentos a respeito da operação a diplomatas inimigos em 1980 (Margolis, 2013, p. 56).

Um relatório da Agência Central de Inteligência dos Estados Unidos (Central Intelligence Agency - CIA), de 1986, descreve que as operações de espionagem descritas tinham a intenção de obter mais informações a respeito das capacidades dos submarinos e mísseis soviéticos, mas nega que qualquer submarino americano tenha entrado a menos de 3 milhas da costa soviética¹¹ (CIA, 1986).

A relevância deste episódio para o estudo está no fato de que representa um caso emblemático de interceptação física de cabos submarinos de comunicação, mediante atividades militares em tempo de paz e que, mesmo diante de comprovação documental da sua ocorrência, permanece a omissão do Direito Internacional e a consequente ausência de responsabilização efetiva.

2.3.2.4 2003-2006 – Room 641A (AT&T)

No ano de 2003, um técnico da empresa de telecomunicações AT&T chamado Mark Klein revelou que na sala 641A da referida empresa funcionava um aparato tecnológico utilizado pelo governo norte-americano destinado a monitorar o tráfego de internet no nível de

¹¹ Antes da entrada em vigor da Convenção de Montego Bay, vigia o conceito de liberdade dos mares, que limitava os direitos nacionais a uma faixa de 3 milhas náuticas, de acordo com a regra do “tiro de canhão”, elaborada pelo jurista holandês Cornelius van Bynkershoek.

provedor do serviço, com tecnologia que permitia, além de analisar o conteúdo das comunicações, identificar o expedidor e destinatário, de acordo com O'Day (2013, p. 240). A técnica principal utilizada nas interceptações era conhecida como Inspeção Profunda de Pacotes (Deep Packet Inspection – DPI) que permitia realizar a filtragem do tráfego de uma maneira mais eficiente. Destaca o autor que o caso teve grande notoriedade em razão de tornar público um exemplo de atividades de larga escala efetivada pelo governo com o auxílio de grandes operadoras, permitindo uma vigilância em massa e invisível aos usuários comuns, iniciando debates sobre abuso de poder e violação de direitos civis.

Este acontecimento, ocorrido em contexto diverso de operações militares em tempo de conflito armado, mostra de maneira concreta que a interceptação de comunicações pode ocorrer de maneira sistemática por intermédio da cooperação entre uma entidade estatal e operadores privados de infraestrutura crítica. Esta constatação comprova a relevância das empresas privadas que compõem o ecossistema de comunicações de cabos submarinos, a consequente complexidade jurídica no que diz respeito às responsabilidades e a necessidade de um ordenamento jurídico que disponha não somente sobre a atuação de entes estatais, mas também dos agentes privados envolvidos.

2.3.2.5 2013 - Caso Edward Snowden

As revelações de Edward Snowden, um ex-contratado da NSA que trabalhava como técnico de computação e consultor de segurança, com acesso a informações confidenciais, expuseram um grande sistema de vigilância em massa levado a efeito pelo Governo dos Estados Unidos, conforme relatado por Greenwald (2014, p. 3). Documentos detalhavam a maneira pela qual agências americanas monitoravam comunicações digitais em escala global, captando dados de servidores de grandes empresas da tecnologia, como a Google, Facebook, Yahoo e Apple, que incluía, além da análise de conexões entre suspeitos ou de indivíduos de interesse internacional, aquelas de natureza privada sem o consentimento das pessoas envolvidas.

Snowden revelou também que não era só a NSA americana que participava desse grande esquema de interceptação em massa. Conforme relatou, a agência de espionagem britânica GCHQ (*Government Communications Headquarters*) também dispõe de capacidade técnica de interceptar e armazenar um grande volume de dados extraídos de cabos de fibra óptica, de acordo com notícia publicada pelo periódico inglês *The Guardian* (2013).

A divulgação desses documentos produziu grande impacto ao tornar públicas algumas práticas que eram conhecidas apenas por pessoas ligadas ao governo, levando ao debate algumas questões afetas aos direitos civis de privacidade e segurança, bem como de transparência e dos limites do poder público na era digital. Apesar de o caso ter revelado a ocorrência contemporânea de interceptação massiva de comunicações internacionais e ter gerado debates sobre soberania, privacidade e direitos humanos, ainda assim não resultou na elaboração de qualquer instrumento internacional voltada à regulação da questão.

2.3.3 Resumo Comparativo

Com a finalidade de possibilitar uma melhor compreensão da evolução dos casos de interceptação de dados, as informações apresentadas nas subseções anteriores foram resumidas e consolidadas no Quadro 1, permitindo entender a sua evolução.

Quadro 1: resumo comparativo dos casos de interceptação mais notáveis.

Casos de interceptação	Período	Tipo de Interceptação			Objetivo
		Quanto ao meio	Quanto ao mecanismo técnico	Quanto ao destinatário	
Telegrama Zimmermann	1917	Lógica	Por meio de um relé	Direcionada	Coleta de comunicações militares
Op. Ivy Bells	Anos 1970	Física	Acoplamento de dispositivos	Direcionada	Coleta de comunicações militares
Room 641A	2003-	Lógica	Deep Packet	Em massa	Vigilância massiva e

	2006		Inspection		armazenamento de dados
Caso Snowden	2013	Física e Lógica	Variadas técnicas	Em massa	Vigilância massiva e armazenamento de dados

Fonte: elaborado pelo autor

A partir da visualização do quadro acima é possível notar que a interceptação não é uma novidade no contexto das comunicações, mostrando-se, ao contrário, prática recorrente. Ao longo do tempo, pode-se perceber que as técnicas utilizadas evoluíram, obviamente em função da tecnologia disponível em cada época, o que possibilitou também uma guinada nos objetivos das interceptações, que inicialmente tinham um escopo mais enquadrado ao aspecto militar, mas que evoluíram para sofisticadas operações de interceptação em massa em tempos de paz.

A análise dos episódios históricos de interceptação de comunicações evidencia que a apropriação clandestina de fluxos de comunicação internacionais constitui prática recorrente e estrutural na atuação dos Estados, inclusive quando apoiada em infraestruturas críticas como cabos submarinos. A ocorrência dessas práticas, sem a correspondente evolução do regime jurídico internacional aplicável, reforça o diagnóstico de lacuna normativa que fundamenta a presente investigação.

2.4 INTRODUÇÃO À QUESTÃO JURÍDICA

As discussões acerca da disciplina jurídica de regência dos cabos submarinos não é recente. Pode-se dizer que o seu embrião se deu com a Convenção para a Proteção de Cabos Telegráficos de 1884, convenção essa que ainda se encontra em vigor e o Brasil é signatário (Brasil, 1888), celebrada em Paris 34 anos após a instalação do primeiro cabo. Ocorre que apesar da remota época que marcou o início do pensamento sobre as implicações que envolvem essa infraestrutura crítica, a questão ainda não está pacificada e tem ganhado cada vez mais relevância diante do atual contexto de tensões mundiais.

Atualmente, tendo em vista a inexistência de um tratado internacional específico e abrangente que verse sobre a malha de cabos submarinos e tudo o mais que lhe seja afeto, os especialistas e estudiosos do tema fazem uso de normas destinadas a regular outras matérias, na tentativa de, de algum modo, preencher as lacunas normativas existentes. Nas palavras de Davenport (2015, p. 108) o regime jurídico aplicável ao tema é fragmentado e incompleto, caracterizando uma verdadeira “colcha de retalhos”, advogando que diversas normas e regimes internacionais podem ser aplicados ao tema, porém de maneira insuficiente para uma tutela mais integral, citando a CNUDM, o Direito Internacional dos Conflitos Armados (DICA), Convenções Contra o Terrorismo e Direito Penal Internacional, além das legislações nacionais dos Estados como normas possivelmente aplicáveis, a depender de cada situação.

Por sua vez, Raha e Raju (2021, p. 31) explicam que as previsões da CNUDM constituem a base do regime internacional de colocação e proteção dos cabos, em virtude da sua ampla adesão e da sua natureza integral em assuntos afetos ao mar, que, de fato, prescreve os princípios de regência do direito internacional do mar, neles compreendidas as prescrições incidentes sobre estes ativos.

É fato que a CNUDM expressamente estabelece direitos e obrigações aos Estados concernentes à proteção e à liberdade de colocação, reparação e manutenção dos cabos. Todavia, se por um lado a principal norma de Direito Internacional que dispõe sobre os espaços marinhos apresenta mecanismos de tutela desse sistema, por outro se verifica que essa tutela não é suficientemente adequada a resguardar todos os aspectos de segurança que envolvem a infraestrutura.

A CNUDM prevê diferentes regimes jurídicos aplicáveis a cada espaço marítimo considerado, com diferentes aspectos e peculiaridades existentes em função de cada área marítima¹². Todavia, os dispositivos que tratam do tema evidenciam uma preocupação voltada à integridade do meio físico, ou seja, do aspecto material dos cabos, não tratando, porém, da interceptação das informações em curso, revelando um vácuo legal importante atinente à comunicação digital.

¹² A Convenção traz diversas prescrições sobre cabos submarinos ao dispor sobre o mar territorial (art. 21); águas arquipelágicas (art. 51); zona econômica exclusiva (art. 58); plataforma continental (art. 79); alto mar (art. 87 e arts. 112 a 115), evidenciando a existência de diversos regimes jurídicos aplicáveis. Além das disposições atinentes aos diversos espaços marítimos, a Convenção prevê também que controvérsias relativas a sua interpretação e aplicação que envolvam cabos submarinos deverão ser submetidas à corte ou tribunal que tenha jurisdição, nos seus termos (art. 297).

Outro aspecto a ser considerado é que a Convenção de Montego Bay não confere proteção aos cabos durante conflitos armados, eis que não traz disposições relativas e esses eventos e o seu escopo é a regulamentação do uso pacífico dos mares e oceanos, conforme previsto no seu preâmbulo e em diversos outros dispositivos do seu corpo.

Em tempo de guerra, os cabos submarinos são considerados alvos militares legítimos, pois é notória a sua relevância estratégica, realidade evidenciada na prática estatal e no direito internacional (Burnett, 2021, p. 1674). Nesse sentido já previa a Convenção de Cabos de 1884, ao estabelecer a possibilidade de penalidades para danos em tempo de paz, mas permitir liberdade de ação para beligerantes em tempo de guerra¹³.

Diante da fragmentação da legislação aplicável aos diversos aspectos que envolvem a segurança dos cabos submarinos, representada por uma série de tratados internacionais que, em tese, poderiam ser aplicados, especialistas apontam que o melhor caminho que a ser seguido passa pela edição de um tratado internacional multilateral que discipline a proteção do sistema de cabos submarinos (Beckman, 2014, p. 290).

A adoção de um tratado internacional nesse sentido poderia contribuir para o estabelecimento de uma jurisdição universal aplicável aos danos intencionais, conforme defendem Raha e Raju (2021, p. 15). Porém, os autores destacam várias dificuldades que deverão ser superadas, tais como a falta de consenso internacional, ambiguidades legais ocasionadas principalmente pela falta de definições precisas de responsabilidades na CNUDM, a necessária coordenação entre os diversos Estados e partes interessadas e a disponibilidade de recursos e capacidades por parte dos envolvidos.

A interceptação da comunicação de dados em trânsito pelos cabos submarinos pode ser utilizada como uma prática voltada à espionagem e, portanto, não regulada internacionalmente. A proibição da espionagem no Direito Internacional é uma questão ambígua e controversa, considerando que os Estados condenam a espionagem estrangeira, mas, ao mesmo tempo, legitimam suas próprias operações de inteligência, revelando uma contradição na prática internacional com a qual alguns Estados parecem estar satisfeitos (Pun, 2017, p. 361).

¹³ Art. 15, Convenção de Cabos de 1884 - Fica bem entendido que as estipulações da presente Convenção não prejudicam a liberdade de ação dos beligerantes.

A despeito dessa ausência de regulação internacional, a Corte Internacional de Justiça (CIJ) já se manifestou no sentido de que a prática de atos de espionagem caracteriza atentado à soberania nacional, violando os princípios de Direito Internacional da Soberania dos Estados e da Não Intervenção e, portanto, prática contrária ao próprio Direito Internacional (CIJ, 2014, p. 147).

Por outro lado, há quem defenda que a espionagem é um direito aferrado à própria soberania do Estado, lastreado tanto em aspectos históricos quanto no Direito Internacional contemporâneo, com sustentação no direito à legítima defesa, uma vez que a obtenção de informações é indispensável para resguardar a segurança nacional (Lubin, 2015, p. 2).

Os Direitos Humanos também constituem campo de debates sobre o assunto. A vigilância em massa levada a efeito por governos pode gerar violações à privacidade, considerado como um Direito Humano Fundamental. Conforme citam Najem e Aljahani (2025, p. 599), o aumento da coleta de dados em massa da população ameaça o direito à privacidade, tutelado no art. 17 do Pacto Internacional sobre Direitos Civis e Políticos e no art. 8º da Convenção Europeia dos Direitos Humanos, representando um grande desafio a ser enfrentado nesta vertente do Direito Internacional.

Dadas as questões já apresentadas, ainda que sumariamente, é possível perceber que o regime jurídico internacional aplicável aos cabos submarinos não é suficiente para responder a todas as questões que se apresentam, ainda que diversos diplomas do Direito Internacional lhes sejam aplicáveis. Os instrumentos jurídicos voltados à proteção dos sistemas de cabos mostram-se mais especificamente destinados ao aspecto material da infraestrutura, não contemplando a dimensão cibernética dos dados que por eles trafegam.

A ausência de salvaguardas específicas que recaiam sobre os dados transmitidos cria um espaço de insegurança jurídica, constituindo fator de vulnerabilidade dessa infraestrutura diante da ausência de um conteúdo normativo claro que possa coibir práticas maliciosas, sendo a releitura das normas existentes ou a edição de novos instrumentos internacionais possibilidades que se apresentam.

Necessária também se faz uma abordagem doméstica do tema, uma vez que o Brasil não está imune a eventuais incidentes de interceptação dos cabos que estão colocados

nas águas sob a jurisdição brasileira. Nesse sentido, discutir os poderes que o Brasil enquanto Estado costeiro dispõe sobre os seus espaços marítimos, os instrumentos jurídicos brasileiros disponíveis à repressão e os limites de atuação são tópicos que precisam ser analisados.

Os aspectos resumidamente abordados na presente seção revelam que a temática da interceptação de dados em tráfego nos cabos submarinos é permeada por uma série de desafios jurídicos que precisam ser enfrentados. Assim, as abordagens relacionadas à interceptação de dados no âmbito do Direito Internacional, a sua eventual prática em águas sob a jurisdição brasileira, os cenários normativos existentes e as possíveis vias para uma regulação internacional mais abrangente serão examinadas de forma mais aprofundada nos capítulos seguintes, por se mostrarem indispensáveis à construção de uma conclusão mais consistente sobre a matéria.

3 A INTERCEPTAÇÃO DE DADOS NO DIREITO INTERNACIONAL

3.1 CONSIDERAÇÕES INICIAIS

No âmbito do Direito Internacional, os cabos submarinos são normalmente considerados alvos militares legítimos em tempos de guerra, não sendo outro o motivo pelo qual a Convenção de Cabos de 1884 já previa que os seus termos não restringem as ações de Estados beligerantes.¹⁴ Em razão de toda a sua importância, podem ser atacados com o fim de obtenção de vantagem militar, o que envolve ações como corte ou destruição dessas estruturas, estando estas medidas, porém, submetidas a algumas balizas, como por exemplo o Direito Internacional Humanitário, ainda que em cenário de conflito (Pedrozo, 2025, p 56).

Em tempos de paz, vimos que a infraestrutura de cabos submarinos goza de certa tutela, com diplomas como a CNUDM e a Convenção de Cabos 1884 dispendo expressamente sobre a sua proteção, mas com significativas limitações à dimensão física dos cabos, não oferecendo salvaguarda explícita quanto a outros tipos de interferência que não causem a interrupção ou obstrução das comunicações. Assim, a interceptação de dados, muitas vezes utilizada por Estados como mecanismo de espionagem que se insere no campo lógico do cabo e não causa danos por si só, parece estar fora do chamado “guarda-chuva” legal de proteção desse sistema, pelo menos a uma primeira vista.

Paradoxalmente, Estados costumam adotar uma posição ambígua ao se posicionarem sobre o tema, condenado a espionagem quando estão na posição de alvo ou vítima da medida, mas a utilizando ativamente como método de espionagem em nome da segurança nacional, revelando uma contradição na prática internacional causadora de insegurança jurídica (Pun, 2017, p. 359).

Diante desse quadro, pode-se afirmar que os debates sobre esse conteúdo se situam em uma área cinzenta do Direito Internacional, merecendo uma investigação mais atenta e criteriosa. Com essa perspectiva, o objetivo do presente capítulo será analisar os princípios e regimes jurídicos mais relevantes com a finalidade de elucidar alguns aspectos e permitir uma melhor compreensão da questão.

¹⁴ Art. XV - Entende-se que as estipulações da presente Convenção não restringem de forma alguma a liberdade de ação dos beligerantes.

3.2 INTERFACES COM O TALLINN MANUAL 2.0 E O DIREITO INTERNACIONAL CIBERNÉTICO

O objeto de estudo do presente capítulo possui interseção com o escopo do Tallinn Manual 2.0 (Schmitt, 2017), publicação desenvolvida por um conjunto de especialistas em Direito Internacional sob os auspícios da OTAN, com o objetivo de apresentar uma análise abrangente alicerçada no Direito e aplicável às operações cibernéticas, razão pela qual foi adotada como referencial, considerando seu alto nível de influência, mesmo não representando um posicionamento vinculante.

Ainda que as disposições do Tallinn Manual 2.0 abordem primordialmente as operações cibernéticas, ele utiliza como fundamento das suas disposições princípios de Direito Internacional de incidência sobre a matéria, como soberania, não intervenção, uso da força e Direitos Humanos, sendo todos direta ou indiretamente aplicáveis à interceptação de dados em cabos submarinos, ainda que necessite de aprimoramentos (Zuccaro et al., 2025, p. 19).

Segundo o Centro de Excelência em Defesa Cibernética Cooperativa da OTAN, apesar de não representar um tratado vinculante, o Manual é amplamente reconhecido pela sua análise abrangente e cuidadosa sobre como o Direito Internacional se aplica às operações no domínio cibernético, de modo que a sua estrutura formada por 154 regras e comentários pode ser objeto de análise para fins de aplicação analógica às operações de interceptação de cabos submarinos, uma vez que também se tratam de operações técnicas com efeitos transfronteiriços (CCDCOE, 2025).

Desta feita, o Tallinn Manual 2.0 representa um importante parâmetro analítico do assunto, haja vista que fornece um *background* normativo, principiológico e interpretativo robusto pois, mesmo sem mencionar a possibilidade de interceptação de dados diretamente na infraestrutura crítica dos cabos submarinos, permite relacioná-la a conceitos consolidados no Direito Internacional contemporâneo. Apesar de se caracterizar como um documento não vinculante e acadêmico, reflete o consenso de dezenas de especialistas e considerou a contribuição de mais de 50 Estados, o que lhe confere autoridade como guia interpretativo para a aplicabilidade das normas existentes, inclusive para documentos complementares ou futuros instrumentos internacionais e nacionais sobre a interceptação de dados (Raidma, 2017).

3.3 A INTERCEPTAÇÃO COMO PRÁTICA DE ESPIONAGEM TÉCNICA

A interceptação, caracterizada como o ato de captar comunicações sem o conhecimento ou consentimento daqueles que são alvos da medida, é prática já há muito tempo realizada e quando é implementada por Estados com a finalidade de obter vantagens políticas, estratégicas, militares ou econômicas sobre outros Estados configura verdadeiro artifício de espionagem (Botua; Dewi; Siswandi, 2022, p. 33).

Com o passar do tempo, as atividades de inteligência continuaram a manter a sua relevância, contudo, evoluíram no que diz respeito às técnicas utilizadas, muito em função de novas tecnologias que foram sendo implementadas, avançando da era analógica para a digital, com uma profunda transformação nos meios dessa prática. Numerosos métodos de coleta de dados têm sido empregados em operações clandestinas ao redor do mundo, gerando nas organizações de inteligência uma obsessão pelo desenvolvimento de métodos tecnológicos capazes de fazer a coleta de dados de maneira mais eficiente, como a utilização de meios remotamente operados (Margolis, 2013, p. 44).

Como se verá, a espionagem sempre acompanhou a evolução dos meios técnicos disponíveis, de sorte que a interceptação de comunicações é uma prática estrutural das relações internacionais, e não um padrão recente.

3.3.1 Contexto Histórico da Espionagem

A espionagem possui uma longa história, sendo descrita por Chasterman (2006, p. 1072) como a segunda profissão mais antiga do mundo, remontando a pelo menos 500 anos a.C., haja vista os escritos do estrategista militar Sun Tzu, na obra “A Arte da Guerra”¹⁵. No mesmo sentido, Pun (2017, p. 355) destaca que espiões e práticas de espionagem são descritos desde os tempos antigos, como na Bíblia, Grécia antiga e China antiga, mas que atualmente a prática evoluiu, existindo no mundo mais de cem agências globais de inteligência operando em países de diferentes níveis de desenvolvimento militar e econômico.

¹⁵ “A Arte da Guerra” é um antigo tratado militar chinês escrito pelo general Sun Tzu, por volta de 500 a. C., sendo considerada uma das obras mais influentes de todos os tempos em razão dos seus ensinamentos sobre táticas e estratégias que, embora tenham sido elaboradas com foco no campo de batalha, podem ser empregadas em outras áreas, como empresarial e política.

Tradicionalmente, a espionagem envolve o envio de agentes para dentro do território físico de outro Estado com o fim de obter informações protegidas. Tal prática ainda é adotada, entretanto, com o avanço e desenvolvimento de novas plataformas tecnológicas, outros meios mais eficientes também passaram a ser utilizados, dando início à espionagem à distância, que passou a se valer de meios como o avião, navio, e até mesmo o espaço sideral mediante a vigilância eletrônica, conforme aponta Buchan (2016, p. 70).

Embora sua história seja muito mais longa e complexa, a espionagem humana (*Human Intelligence* ou HUMINT) foi profissionalizada apenas no século XX, com a Guerra Fria sendo o marco inicial da espionagem digital (*Signals Intelligence* ou SIGINT). Apesar das diferenças tecnológicas, muitos dos desafios estratégicos e normativos ao redor da espionagem digital se assemelham à convencional, mas, ainda assim, a espionagem digital é um tema que muitas vezes se evita debater nos fóruns multilaterais, com os Estados ainda aprendendo a lidar com as suas consequências e peculiaridades (Devanny; Martin; Stevens, 2021, p. 433).

3.3.2 Espionagem Digital

Com a transformação digital da atividade de inteligência, Zegart (2022, p. 6) destaca que a guerra cibernética e novas tecnologias se tornaram centrais na atividade de inteligência, com a internet viabilizando uma nova geração de guerra centrada na coleta de informações, citando como exemplo o roubo maciço de propriedade intelectual por parte de alguns países, incluindo dados sensíveis de programas militares relevantes¹⁶.

A utilização de interceptações como meio de espionagem não é novidade nas Relações Internacionais. Como exemplo, Moran, Burton e Christou (2023, p. 10) citam que a Agência de Segurança Nacional dos Estados Unidos (NSA) desenvolveu programas para auxiliar na transcrição e tradução de materiais estrangeiros interceptados, como as chamadas soviéticas durante a Guerra Fria, realçando o uso de interceptações como parte das atividades de espionagem.

¹⁶ Como exemplo, o autor destaca que alguns países como Cuba, Rússia e Irã possuem serviços de inteligência muito agressivos, destacando a China que, conforme afirma, teria baseado seus principais sistemas de armas em tecnologia roubada dos Estados Unidos, incluindo aqueles ligados aos programas militares das aeronaves F-35 e F-22.

A espionagem nas relações entre Estados não se resume apenas àquelas que envolvem inimigos ou adversários, tendo a história relatos de espionagem entre aliados. Passagem que confirma essa assertiva é o caso que envolve o e-mail trocado entre a *British Government Communications Headquarters* (GCHQ), agência britânica de inteligência, e a NSA, vazado por um tradutor da agência Britânica, relatando os esforços coordenados entre os Estados Unidos e o Reino Unido voltados à interceptação das comunicações dos outros treze membros do Conselho de Segurança da ONU, tanto nos escritórios quanto nas residências dos representantes dos países do Conselho, com a finalidade de obter informações a respeito das respectivas posições no debate sobre a invasão do Iraque (que àquela altura ainda não havia ocorrido), objetivando conferir aos formuladores de políticas dos Estados Unidos uma vantagem e obter resultados favoráveis (Chesterman, 2006, p. 1086).

Ocorre que, dadas a abrangência e nuances que envolvem este complexo tema, é importante que se tenha uma definição sobre o que seria a espionagem digital (ou ciberspionagem) que permita delimitar o âmbito da análise e realizar um exame mais focado. Neste ponto, entretanto, reside uma dificuldade que precisa ser superada, que é encontrar um conceito que seja preciso e completo sobre tão profundo tópico. Logo, apesar da falta de um consenso no âmbito internacional sobre uma delimitação do que seria espionagem cibernética, adotar-se-á doravante o conceito apresentado por Ziolkowski, por refletir a compreensão atual do Direito Internacional e da prática estatal a respeito de atividades cibernéticas:

Ciberspionagem é a cópia de dados que não estão disponíveis publicamente e que estão em transmissão sem fio, salvos ou temporariamente disponíveis em sistemas de TI ou redes de computadores localizados no território ou área sob jurisdição exclusiva de outro Estado por um órgão, agente estatal ou de outra forma atribuível a um Estado, conduzida secretamente, sob disfarce ou falsos pretextos, e sem o consentimento ou aprovação dos proprietários ou operadores dos sistemas de TI ou redes de computadores visados ou do Estado onde se encontram. Inclui também a cópia temporária de dados para a memória de acesso randômico ou virtual de um sistema de TI com o propósito de mera visualização ou reprodução acústica de dados (por exemplo, voz sobre IP). A cópia de dados salvos ou temporariamente disponíveis em sistemas de TI ou redes de computadores localizados no território ou área sob jurisdição exclusiva do Estado que copia é abrangida por esta definição somente se os dados forem protegidos pelo direito internacional público (Ziolkowski, 2013, p. 429, tradução própria).

Da definição acima apresentada é possível perceber que a espionagem cibernética possui seis elementos essenciais. O primeiro elemento essencial diz respeito à indisponibilidade de dados, sendo necessário para caracterizar a ciberspionagem que ocorra o acesso a dados que não estejam disponíveis publicamente.

O segundo elemento refere-se à localização dos dados, de modo que os dados podem estar em transmissão sem fio, armazenados ou temporariamente disponíveis em sistemas de Tecnologia da Informação (TI) ou redes de computadores localizados no território ou em uma área exclusiva de um outro Estado, ou seja, que não pertença ao Estado que está praticando a espionagem para configurar a espionagem.

O terceiro elemento é afeto aos agentes responsáveis, pois a ação deve ser realizada por um órgão do Estado, agente estatal ou entidade que possa ser atribuída ao Estado, não caracterizando ciberespionagem os atos realizados por agentes privados em interesse próprio ou sem ao menos que haja o concurso de interesse do Estado.

O quarto elemento essencial para a caracterização de ato de espionagem é a furtividade da ação, ou seja, necessita ser conduzida de forma secreta, disfarçada ou sob falsos pretextos, sem o consentimento (expresso ou presumido) dos proprietários ou operadores dos sistemas visados, nem do Estado onde os sistemas estão localizados.

O quinto elemento representa a temporariedade do acesso aos dados, sendo suficiente para caracterizar a ciberespionagem o ato destinado à mera visualização ou reprodução acústica dos dados, quando, por exemplo, os dados são temporariamente armazenados na memória RAM ou memória virtual, não sendo, portanto, exigível a realização de cópia definitiva dos dados, sendo suficiente o acesso a eles.

O sexto e último requisito para a configuração da ciberespionagem é a necessidade do acesso a dados de terceiros, ou seja, o acesso a dados que não estejam sob a jurisdição exclusiva do próprio Estado.

Observa-se também da definição proposta que os métodos de obtenção de informação que envolvem o uso da força não são considerados como espionagem cibernética, o que faz total sentido, haja vista que tal conceito pressupõe uma intrusão. Por esse motivo, a autora afirma que a extração de dados por meio da dobra de cabos submarinos de fibra óptica não se enquadra como espionagem cibernética, todavia caracteriza verdadeira espionagem (Ziolkowski, 2013, p. 429).

Em que pese a controvérsia desse posicionamento¹⁷, é irrelevante adentrar em debates sobre tal método caracterizar ou não espionagem cibernética, uma vez que independentemente da técnica utilizada para a obtenção dos dados provenientes de cabos submarinos, será uma modalidade do gênero espionagem.

Desta feita, considerando que a guerra cibernética representa um novo campo de desenvolvimento da espionagem que tem como uma das suas plataformas a internet, é evidente que as infraestruturas de cabos submarinos são suscetíveis de serem exploradas, representando um alvo privilegiado, tendo em vista que são responsáveis pela quase totalidade do fluxo de dados da rede e estão dispostos em áreas com vigilância restrita. Configura-se, portanto, como uma modalidade de espionagem técnica, o que permite a análise sob o prisma de institutos do Direito Internacional como soberania, não intervenção, direitos humanos, comprovando que não se trata de mera questão técnica, mas que também se insere nos campos político e jurídico, como se demonstrará.

3.4 AUSÊNCIA DE PROIBIÇÃO EXPRESSA NO DIREITO INTERNACIONAL

A espionagem realizada em tempos de guerra e em tempos de paz recebe tratamento jurídico diferenciado do Direito Internacional, tendo a espionagem em tempo de guerra disposições específicas em alguns tratados internacionais. Por exemplo, a Convenção de Haia sobre as Leis e Costumes da Guerra em Terra de 1907 (Convenção IV) apresenta um capítulo específico intitulado “espiões”, trazendo algumas disposições expressas sobre o tema¹⁸. O Protocolo Adicional I às Convenções de Genebra, de 1977, que trata da proteção de vítimas de conflitos armados internacionais, também tem disposições expressas a respeito da atuação de espiões em tempo de guerra¹⁹. Esses instrumentos abordam, de forma direta ou

¹⁷ Ousamos discordar da autora quanto a este aspecto. Considerar que o emprego de mera força física necessária para a dobra de um cabo é suficiente para descaracterizar a espionagem cibernética seria demasiadamente desproporcional. Entendemos que se trata de mera técnica com o objetivo de permitir o acesso aos dados que estão em um sistema de T.I., conforme exigido pela definição proposta. Porém, como tal discussão não resultaria em desdobramentos necessários a uma melhor compreensão do assunto, preferimos não aprofundá-la.

¹⁸ O capítulo II da Convenção IV de Haia dispõe, ainda que de maneira sucinta, sobre alguns aspectos básicos sobre a atividade de espionagem em tempo de guerra, como, por exemplo, quando uma pessoa pode e não pode ser considerada espiã (art. 29), a necessidade de julgamento prévio à aplicação de punição ao espião pego em flagrante (art. 30) e a ausência de responsabilização por espionagem pretérita, ou seja, daquele que é capturado após já ter se juntado novamente ao exército a que pertence (art. 31).

¹⁹ O art. 46 do Protocolo Adicional I às Convenções de Genebra traz disposições sobre os espiões, dentre as quais a inaplicabilidade do estatuto do prisioneiro de guerra àquele que for capturado realizando atividades de espionagem.

indireta o tratamento que deve ser conferido aos espões durante a guerra, reconhecendo a espionagem como uma realidade e estabelecendo normas relativas ao *status* e tratamento destes agentes durante os conflitos, revelando a existência de um regramento próprio dado pelo Direito Internacional em tempos de guerra.

Por outro lado, a espionagem em tempo de paz, conforme já mencionado anteriormente, está situada em um vácuo normativo no âmbito do Direito Internacional. Isso é evidenciado pela Regra nº 32 do Manual Tallinn 2.0, que estabelece que “embora a espionagem cibernética em tempos de paz por parte de Estados não viole, por si só, o direito internacional, o método pelo qual é realizada pode fazê-lo” (Schmitt, 2017, p. 168, tradução própria). Conforme prescrito na publicação, isso significa que a intrusão em sistemas de outros Estados (aqui inseridos os cabos submarinos) para coletar informações secretas não configura uma violação direta ao Direito Internacional, uma vez que a espionagem não possui um regime legal internacional próprio e que, por tal razão, até pode violar normas específicas de direito interno dos Estados envolvidos, mas por si só não configura um ato de uso ilegal da força ou intervenção coercitiva.

Em que pese ser uma medida condenada universalmente pelos Estados e frequentemente punida é, do mesmo modo, amplamente praticada entre inimigos ou mesmo entre aliados (PoKempner, 2013, p. 253). Isso revela que, embora exista uma reprovação de caráter geral à espionagem, até mesmo em termos criminais no Direito interno dos Estados, o Direito Internacional carece de um tratado claro e unificado que proíba a espionagem em si mesma fora de um contexto de conflito armado, sugerindo que a condenação seja mais de caráter político do que decorrente do descumprimento de uma obrigação jurídica vinculante.

Não faz sentido argumentar que a punição aplicada por ato de espionagem em tempo de paz tem como fundamento um costume internacional plenamente desenvolvido e de ordem proibitiva à tal prática, uma vez que o mesmo Estado que pune esta atividade, a desenvolve, constatação que corrobora a ideia de que a punição decorre de um ato político.

Logo, a ausência de uma norma clara cria um ambiente de insegurança jurídica, pois possibilita aos Estados operarem em uma “zona cinzenta” permeada por comportamentos contraditórios, enfraquecendo a previsibilidade do sistema jurídico internacional, favorecendo o aumento de tensões diplomáticas e a escalada de conflitos.

3.5 PRINCÍPIO DA SOBERANIA E SUA APLICAÇÃO À INTERCEPTAÇÃO

A soberania é um princípio fundamental do Direito Internacional que tem se consolidado como corolário do princípio da igualdade entre os homens e nações, previsto na Carta das Nações Unidas (Brasil, 1945)²⁰. É compreendida como o direito exclusivo de um Estado de exercer autoridade e controle sobre o seu território, população e assuntos internos, livre de interferências externas.

Com a Paz de Vestfália²¹, emergiu o conceito de soberania moderna, surgindo a ideia de Estados territoriais soberanos com fronteiras fixas e exclusivas, marcando o início da ordem internacional baseada em Estados-nação soberanos (Bauder; Mueller, 2021, p. 161).

Ocorre que os avanços experimentados pela sociedade desde o estabelecimento do conceito de soberania, sobretudo em tempos contemporâneos de dependência de infraestruturas críticas de comunicações, impõem novos desafios à compreensão e abrangência desse princípio. Nesse panorama, a interceptação de dados em cabos submarinos se insere em um debate central: saber até que ponto a coleta de dados de maneira clandestina em cabos submarinos viola a soberania estatal e qual deve ser a resposta do Direito Internacional, considerando a ausência de proibição expressa e a prática reiterada pelos Estados.

No contexto da segurança cibernética, o Manual Tallinn 2.0 (Schmitt, 2017, p. 11) defende que o princípio da soberania é aplicável para proteger o espaço cibernético sob o controle territorial de determinado Estado contra operações não autorizadas de outros Estados. O Manual estabelece a soberania como princípio geral de regência e ponto de partida da questão, razão pela qual reserva a Regra nº 1 para as suas disposições, tendo como pressuposto que a soberania de um Estado se estende ao seu espaço cibernético²².

²⁰ Apesar da Carta da ONU não estabelecer um conceito expresso de soberania, sua ideia está presente em diversas passagens do documento, decorrendo do princípio da igualdade de todos os Estados-membros da Organização, previsto no art. 2º, §1º.

²¹ A Paz de Vestfália foi uma série de tratados de paz assinados em 1648 nas cidades de Osnabrück e Münster, na Vestfália, sendo a precursora nas iniciativas de alcançar a paz por meio de congressos diplomáticos, inaugurando a ideia de coexistência de Estados soberanos na Europa (Bueno, 2024).

²² Considerando que o Manual Tallinn 2.0 não traz uma definição do que seria o espaço cibernético, adotamos o conceito apresentado no inciso III do art. 3º do Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações, definindo espaço cibernético como o “espaço virtual composto por um conjunto de canais de comunicação da internet e outras redes de comunicação que garantem a interconexão de dispositivos de TIC que engloba todas as formas de atividades digitais em rede, incluindo o armazenamento, processamento, e compartilhamento de conteúdo além de todas as ações, humanas ou automatizadas, conduzidas além deste ambiente” (Brasil, 2020).

Quanto a esse pressuposto, é importante notar que se trata de uma evolução do conceito tradicional de soberania, que tem como um de seus componentes o território físico como parâmetro, evoluindo para adicionar também o espaço cibernético como um dos seus elementos constituintes, desenvolvendo, assim, a ideia de território cibernético. Pirker (2013, p. 215) aduz que apesar de o espaço cibernético parecer uma dimensão “virtual” e sem fronteiras físicas claras, é, em princípio, sujeito ao conceito de territorialidade próprio do Direito Internacional. É a partir deste ponto que é possível tomar a soberania como fundamento de validade da base jurídica para impedir interferências externas não autorizadas.

Como decorrência lógica da aplicação do princípio ao espaço cibernético, tem-se que nenhum Estado pode realizar operações cibernéticas que violem a soberania de outro, tendo cada um autoridade exclusiva para governar e controlar as suas redes, infraestruturas, dados e comunicações, dentro do seu território que, como compreendido, pode ser físico ou cibernético.

O entendimento compartilhado pelos especialistas que formaram o grupo de elaboração do Manual Tallinn 2.0 é no sentido de que a soberania exercida pelo Estado no âmbito cibernético fica circunscrita àquela que pode ser exercida sobre o território físico, ou seja, o território soberano cibernético tem a mesma abrangência do território soberano físico (Walden, 2013, p. 266). Vale dizer que para que seja considerada violação da soberania, a interceptação de cabos submarinos deve ocorrer dentro das águas territoriais do Estado, seguindo as normas estabelecidas pelo Direito Internacional sobre estas estruturas, mais especificamente na CNUDM e na Convenção de Cabos de 1884.

Todavia, o Manual destaca que esse entendimento é aplicável sem prejuízo de outras disposições que vierem a ser objeto de outras normas internacionais, tais como tratados bilaterais que regulem essas circunstâncias, que poderão definir outras restrições e parâmetros além daquelas previstas no Direito Internacional geral.

A questão da violação à soberania ganha contornos mais controvertidos quando passa a ser analisada quanto à Zona Econômica Exclusiva (ZEE). Afinal, considerando que, se por um lado, a ZEE não constitui espaço soberano do Estado costeiro, mas por outro é regida por um regime jurídico próprio que assegura ao Estado direitos econômicos e de jurisdição (ainda que limitada), pergunta-se: a interceptação de dados nos cabos situados na ZEE caracteriza violação à soberania do Estado costeiro? Este aspecto está diretamente relacionado

ao regime jurídico internacional aplicável aos cabos submarinos, que será abordado de maneira mais detalhada no capítulo seguinte, mas já se adianta que o aspecto é controvertido.

Como se infere do que foi abordado anteriormente, os peritos que elaboraram o Manual Tallinn opinam no sentido de que eventual interceptação ocorrida na ZEE não constitui violação à soberania do Estado costeiro, em que pese poder configurar outro ilícito, sobretudo se ocorrer dano à estrutura física dos cabos (Heinegg, 2013, p. 316). Por outro lado, Davenport (2015, p. 108) entende que, embora a ZEE esteja sujeita às liberdades tradicionais de navegação, a interceptação ou a instalação de dispositivos nos cabos voltados à vigilância pode ser uma atividade que viola a segurança e, por conseguinte, a soberania, aumentando a tensão entre os Estados envolvidos diante da dualidade existente entre a possibilidade de ameaça à soberania do Estado costeiro e as liberdades dos demais Estados.

Assim, a compreensão de que a soberania é aplicável ao chamado “território cibernético” é de grande relevância para o estudo deste tema e, quanto a isto, não há muitas controvérsias, adotando-se essa ideia como um pressuposto para o seu desenvolvimento. Entretanto, tendo em vista que o escopo do presente trabalho é a interceptação de cabos submarinos e que estes estão dispostos ao longo de espaços marítimos distintos, há uma “área cinzenta” de incidência do referido princípio, haja vista os diferentes regimes jurídicos conferidos pelo Direito Internacional aos espaços marítimos, nos termos previstos pela CNUDM.

3.6 PRINCÍPIO DA NÃO INTERVENÇÃO

O princípio da não intervenção está intimamente ligado à noção fundamental de soberania que, como abordado, inclui o respeito à integridade territorial, independência política e inviolabilidade dos Estados. Diferentemente do que ocorre com o princípio da soberania, o princípio da não intervenção está explicitamente previsto na Carta das Nações Unidas (Brasil, 1945)²³, objetivando resguardar os Estados contra intervenções externas, ressalvadas as competências do Conselho de Segurança.

²³ Art. 2(7): Nenhum dispositivo da presente Carta autorizará as Nações Unidas a intervirem em assuntos que dependam essencialmente da jurisdição de qualquer Estado ou obrigará os Membros a submeterem tais assuntos a uma solução, nos termos da presente Carta; este princípio, porém, não prejudicará a aplicação das medidas coercitivas constantes do Capítulo VII.

Trata-se de um princípio consolidado no Direito Internacional, porém, sua amplitude quanto aos aspectos que envolvem a interceptação pode ser interpretada de diversas formas diferentes e níveis distintos de abrangência, de acordo com Gill (2013, p. 224). Explica o autor que a espionagem está situada em uma linha tênue entre o que pode ou não pode ser considerado uma intervenção ilegal sob o ponto de vista do Direito Internacional, de modo que é necessário distinguir se as ações consideradas no caso concreto caracterizam verdadeiros atos coercitivos e que, por isso, violam o princípio, ou se configuram mera interferência.

O Manual Tallinn 2.0 dispõe de uma regra específica sobre este ponto, que prevê que “um Estado não pode intervir, inclusive por meios cibernéticos, nos assuntos internos ou externos de outro Estado” (Schmitt, 2017, p. 312, tradução própria). Desta prescrição, prevista na Regra nº 66 do Manual, o grupo de especialistas que o elaborou entende que a proibição para ser considerada ilícita deve ser dotada de coercitividade, não se restringindo à força física, mas podendo decorrer da prática de qualquer ato que obrigue determinado Estado a agir (ou se abster de agir) contra a sua vontade, deixando clara a distinção entre os atos que podem ser caracterizados apenas como mera interferência daqueles que violariam o princípio em apreço.

Por sua vez, Tay (2022, p. 75) propõe uma releitura do princípio da não intervenção, tendo em vista o surgimento de novos desafios contemporâneos que não se amoldam a esse modelo que tem como ponto central a coerção, mas que possuem capacidade disruptiva à soberania de um Estado. Explica o autor que essa definição baseada na coerção foi proposta pela Corte Internacional de Justiça no caso *Nicarágua versus Estados Unidos* (CIJ, 1986), em que o primeiro acusou o segundo de realizar operações militares e paramilitares violando o Direito Internacional.

No parágrafo 205 do julgamento, a CIJ estabeleceu a necessidade de coerção para a caracterização da intervenção ilícita, sendo considerado uma referência fundamental no Direito Internacional. Entretanto, argumenta o referido autor que essa definição restrita à coerção apresenta lacunas para lidar com novas formas de intromissão externa que, embora não se caracterizem como formas de coerção direta, representam importantes riscos de desestabilização estatal (por exemplo, campanhas de desinformação voltadas a interferir no resultado de eleições), advogando a importância de uma reformulação para que o princípio em apreço permaneça relevante e eficaz.

Em síntese, o princípio da não intervenção se mostra como uma importante baliza do Direito Internacional destinada à tutela da soberania estatal contra intervenções externas prevalecendo, majoritariamente, a ideia da necessidade da coerção para a sua caracterização. Não obstante, não existe uma delimitação rígida e perfeitamente clara do que caracterizaria a coerção, uma vez que os limites a serem auferidos envolvem uma gama imensa de atos e situações considerados os desafios contemporâneos. Em outros termos, para que fique configurada a intervenção ilícita de um Estado nos assuntos de outro, não é suficiente a mera influência política, diplomática ou informacional, sendo necessária a imposição de poder ou pressão suficiente para constranger a vontade soberana do Estado afetado, suprimindo-lhe a sua liberdade de decisão. Assim sendo, pode-se entender que para que a interceptação seja classificada como violadora do princípio da não intervenção será necessário avaliá-la de maneira contextualizada, aferindo se dela decorre a prática de ato ou a omissão por Estado contra a sua vontade.

3.7 DIREITOS HUMANOS E PROTEÇÃO DA PRIVACIDADE

O tema da interceptação de dados em cabos submarinos possui relação direta com os Direitos Humanos, mais especificamente com o Direito Fundamental da Privacidade, haja vista a percepção de um conflito existente entre os interesses público e privado. Tal conflito é representado pelo interesse estatal fundamentado em uma lógica estratégica e securitária, em oposição ao interesse privado, sustentado em uma premissa de cunho individual e com preceito ético (Olmos; Favera, 2016, p. 4). É a compreensão desse conflito e das suas nuances que será objeto desta seção.

3.7.1 A Privacidade como Direito Humano Fundamental

O direito à privacidade é reconhecido como direito humano universal, vinculado à dignidade, liberdade e autonomia individual, estando disciplinado em vários instrumentos internacionais. A Declaração Universal dos Direitos Humanos (ONU, 1948) estabelece em seu art. 12 que “Ninguém será sujeito a interferências em sua vida privada, em sua família, em seu lar ou em sua correspondência [...] Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.”, representando um marco simbólico do reconhecimento desse

direito pela comunidade internacional, além de firmar o seu conteúdo programático para o desenvolvimento de diplomas posteriores.

Avançando no tratamento da privacidade como direito humano fundamental, o Pacto Internacional sobre Direitos Civis e Políticos (ONU, 1969) apresenta disposição muito semelhante²⁴, todavia, conferindo uma maior efetividade ao direito, pois, ao adotar uma formulação que estabelece uma prescrição proibitiva de ingerências arbitrárias ou ilegais na vida privada, deixa evidente que tais ingerências, ainda que tenham previsão em lei (e sejam, portanto, legais), não poderão configurar atos arbitrários, ampliando o escopo da tutela, sendo esse o entendimento firmado no Comentário Geral nº 16 do Comitê de Direitos Humanos (ONU, 1988).²⁵ Semelhantemente, há ainda disposições de tutela do direito à privacidade em outros diplomas internacionais, tais como a Convenção Americana sobre Direitos Humanos (Organização dos Estados Americanos, 1969)²⁶ e a Convenção Europeia de Direitos Humanos (Conselho da Europa, 1950)²⁷, aos quais aqui apenas se faz remissão, tendo em vista ser desnecessária a abordagem exaustiva de todos eles.

Especificamente quanto ao objeto do presente trabalho, é interessante notar que no referido Comentário nº 16 o Comitê de Direitos Humanos firma o entendimento de que quaisquer formas de vigilância, seja eletrônica ou de outra natureza (incluindo interceptações em geral) devem ser proibidas a fim de proteger a privacidade das comunicações, exigindo que a confidencialidade e a integridade das correspondências sejam asseguradas.

Trazendo a análise para o âmbito do direito doméstico, o direito à privacidade está consagrado da Constituição Federal de 1988 (Brasil, 1988) ao assegurar a inviolabilidade do

²⁴ Art. 17 – (1) Ninguém poderá ser objeto de ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais às suas honra e reputação. (2) Toda pessoa terá direito à proteção da lei contra essas ingerências ou ofensas.

²⁵ O parágrafo 4 do Comentário Geral nº 16 do Comitê de Direitos Humanos da ONU explica o conceito de interferência arbitrária, prescrevendo que “a expressão “interferência arbitrária” também pode se estender à interferência prevista em lei.” Ou seja, a proibição contra interferências arbitrárias não se limita apenas aos atos ilegais ou não previstos em lei, mas abrange também aqueles atos que mesmo autorizados legalmente estejam em desacordo com as finalidades do Pacto.

²⁶ O art. 11 da Convenção Americana sobre Direitos Humanos, ao tutelar a honra e a dignidade, prevê a proibição de ingerências arbitrárias ou abusivas na vida privada, mencionando expressamente a proteção à correspondência, podendo-se aqui incluir a correspondência digital.

²⁷ A proteção à privacidade também é alçada à categoria dos Direitos Humanos pela Convenção Europeia de Direitos Humanos, que, inclusive, estabelece condicionantes à restrição desse direito pelo Estado, ao dispor no art. 8º (2) que “Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar econômico do país, a defesa da ordem e a prevenção das infrações penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros.”

direito à privacidade e das comunicações de dados²⁸, ambos os direitos topograficamente situados no título II, que versa sobre direitos e garantias fundamentais, em conformidade com os diplomas internacionais mencionados. As práticas de interceptação afetam não apenas suspeitos específicos, mas populações inteiras, violando o princípio da proporcionalidade e o direito à vida privada, valores reconhecidos tanto na Constituição brasileira quanto em tratados internacionais de direitos humanos, deixando de representar apenas uma questão de estratégia e segurança estatal para se situar também no âmbito do núcleo essencial dos direitos fundamentais (Senado Federal, 2014, p. 15).

3.7.2 Tensão entre Privacidade e Soberania

Como visto, a interceptação como prática de espionagem está diretamente relacionada ao princípio da soberania, considerando que, sob a ótica do Estado que sofre a ação de vigilância, a espionagem representa uma afronta a esse preceito. Por tal razão, é prática comum no âmbito internacional a utilização de meios de espionagem sob a alegação de legítima defesa em face de semelhantes comportamentos externos, face a inexistência de uma vedação expressa da espionagem em tempos de paz (Davenport, 2015, p. 107). Ou seja, o argumento da soberania é suscitado tanto para reprimir a espionagem, quanto para justificá-la, a depender da posição em que o Estado se encontre, isto é, espionado ou espião.

Com vistas a legitimar as suas ações, os Estados costumam justificar programas de vigilância com base em argumentos clássicos de soberania e interesse nacional, especialmente quando situados em contextos de combate ao terrorismo e ameaças externas, funcionando como fundamento de validade para a ampliação das capacidades tecnológicas em nome de um “interesse geral” e em detrimento do “interesse individual”. Todavia, a soberania não deve operar como um poder ilimitado de atuação estatal, por outro lado, deve ser limitada por normas constitucionais internas e obrigações internacionais na seara dos direitos humanos. Essa tensão é ainda agravada quando se trata de uma ação transnacional, incidindo sobre direitos fundamentais de pessoas estrangeiras bem como sobre a soberania de Estados cujas comunicações governamentais são monitoradas, enfraquecendo a sua autonomia política (Senado Federal, 2014, p. 7).

²⁸ Art. 5º, incisos X e XII, da CRFB.

Assim, sem que haja um tratado internacional específico que regule a questão, vemos o direito à soberania e o direito à privacidade, ambos consagrados pelo Direito Internacional, em polos opostos em uma relação de direito, na qual os Estados podem lançar mão da espionagem devido à inexistência expressa de proibição nesse sentido, mesmo que possa representar violações ao direito à privacidade.

Destarte, não resta dúvidas quanto ao *status* de direito humano fundamental da privacidade. Todavia, a interceptação de dados em cabos submarinos se insere em uma complexa interseção entre o Direito Internacional Público e o Direito Internacional dos Direitos Humanos, dado que, por mais que os instrumentos internacionais e nacionais prevejam garantias ao direito à privacidade e à proteção de dados e correspondências, a característica transnacional da disposição física dos cabos desafia a efetividade dessas normas, demandando um instrumento²⁹ internacional específico que pacifique a matéria ou, no mínimo, uma releitura que confira uma maior proteção às infraestruturas submarinas enquanto isso não ocorre.

3.8 A INADEQUAÇÃO AOS CONCEITOS DE INVESTIGAÇÃO CIENTÍFICA MARINHA E OUTROS USOS DO MAR INTERNACIONALMENTE LÍCITOS

A crescente relevância estratégica dos cabos submarinos tem suscitado tentativas de enquadrar condutas marcadas por ambiguidades como manifestações legítimas de atividades estatais consolidadas e regularmente exercidas, como é o caso da pesquisa científica marinha ou mesmo o exercício de atividades militares lícitas em águas além do mar territorial (Evans; Page, 2014, p. 120). Ocorre que essa perspectiva se mostra problemática sob o ponto de vista normativo, bem como da prática internacional. Nesse raciocínio, a presente seção explicita as razões pelas quais a interceptação de dados em cabos submarinos não pode ser legitimamente enquadrada como pesquisa científica marinha por não atender aos seus requisitos e possuir especificidades que lhe impõem tratamento jurídico próprio.

²⁹ Aqui preferimos empregar o termo “instrumento” com a finalidade de conferir generalidade, em razão da possibilidade de utilização de algumas formas distintas de regulação, como será melhor tratado no capítulo 4 deste trabalho.

3.8.1 Atividades de Investigação Científica Marinha

A CNUDM disciplina a sua Parte XIII a investigação científica marinha, prevendo a possibilidade da sua realização por todos os Estados e organizações internacionais competentes, desde que tal direito não se dê em prejuízo dos direitos e deveres de outros Estados,³⁰ bem como que o seu desenvolvimento deve ser promovido e facilitado por todos, nos seus termos.³¹

Conforme pontua Zanella (2025, p. 281), a Convenção estabelece que toda atividade de pesquisa científica marinha é orientada por três princípios fundamentais, sendo eles a utilização pacífica do meio marinho, a liberdade de investigação científica e a cooperação e divulgação dos resultados. Destes princípios se extrai que a prática da pesquisa científica marinha pressupõe, portanto, um caráter público e colaborativo, que não se coaduna com operações de natureza estratégica conduzidas de forma sigilosa e de proveito restrito.

Caso a pesquisa seja desenvolvida na Zona Econômica Exclusiva ou na Plataforma Continental, prevê a CNUDM um regime claro de consentimento do Estado costeiro para a sua realização, que somente poderá ocorrer mediante pedido de autorização prévio, contendo informações sobre os objetivos, métodos e instituições envolvidas.³² Sendo assim, fica evidente que a investigação científica marinha é regida por princípios de cooperação e transparência, representando a desconfiança uma contradição prejudicial à cooperação (Belarmino, 2020, p. 31).

Diante disso, qualquer tentativa de classificar a interceptação do tráfego de dados em cabos submarinos como pesquisa científica marinha mostra-se incompatível com a lógica estruturante da CNUDM.

3.8.2 Outros Usos do Mar Internacionalmente Lícitos

No domínio marítimo consolidou-se uma prática tolerada de operações de inteligência em espaços além do mar territorial, que se baseia na controvérsia existente em

³⁰ Art. 238, CNUDM.

³¹ Art. 239, CNUDM.

³² Art. 246, CNUDM.

decorrência da ausência de uma proibição clara na CNUDM e na lógica das liberdades do alto-mar, ainda que sob frequente contestação da legalidade de atividades de coleta de informações em geral (Davenport, 2015, p. 106).

Alguns Estados, como por exemplo os Estados Unidos, defendem que as atividades de coleta de dados, incluindo o *tapping* (escuta ou interceptação física) de cabos submarinos, se enquadram nas liberdades tradicionais do alto-mar e nos outros usos lícitos do mar relacionados a essa liberdade³³, lastreando este entendimento com base no posicionamento adotado por ocasião das negociações da CNUDM, segundo o qual a ZEE não deve reservar direitos para os Estados costeiros além dos econômicos e que as tentativas de reconhecer-lhes direitos de segurança foram rejeitados (Davenport, 2015, p. 99).

Ocorre que a CNUDM afirma a utilização do alto-mar para “fins pacíficos”,³⁴ termo este que foi objeto de controvérsias acerca do seu alcance durante as negociações do texto convencional, de modo que as potências marítimas defendem uma interpretação restritiva do termo, de maneira que apenas seriam consideradas atividades não pacíficas aquelas que caracterizassem ameaça ou uso da força contra a integridade territorial ou a independência política de Estado (Zanella, 2025, p. 267). Dessa forma, ao que parece a realização de interceptação em cabos submarinos estaria fora até mesmo da interpretação mais restritiva de “fins pacíficos”, haja vista a sua realização ocorrer em prejuízo da independência política de terceiro Estado, mostrando-se incompatível com o regime jurídico da Convenção de Montego Bay, denotando a necessidade de um tratamento normativo próprio.

3.9 CONSIDERAÇÕES PARCIAIS

À vista das discussões apresentadas no decorrer deste capítulo, observa-se que a interceptação de dados em cabos submarinos representa um problema que ainda não está solucionado pelo Direito Internacional.

Apesar de gozar de certa tutela por diplomas internacionais como a Convenção de Cabos de 1884 e a CNUDM, nota-se que a proteção conferida à infraestrutura de cabos submarinos incide principalmente sobre a dimensão física da rede, mostrando-se insuficiente

³³ Art. 58(1), CNUDM.

³⁴ Art. 88, CNUDM.

a resguardar a dimensão lógica dos dados que tramitam por ela, revelando um campo amplo para a prática de interceptação, que pode ser caracterizada como ferramenta de espionagem.

Como visto, a espionagem em tempos de conflito possui regulamentação específica conferida pelo Direito Internacional, todavia, em tempos de paz, nota-se um vácuo legislativo com esse enfoque, o que possibilita um estado de contradição e ambiguidade que favorece tensões e criam um cenário de instabilidade indesejado nas Relações Internacionais.

Como forma de tentar pacificar e dar respostas ao problema, especialistas utilizam as premissas de princípios e direitos consagrados pelo Direito Internacional, como a soberania, não intervenção e privacidade. Entretanto, tais princípios e direitos são invocados pelos Estados tanto para reprimir quanto para justificar suas práticas, a depender da posição em que se encontrem. A soberania e a não intervenção são pressupostos centrais do sistema internacional, mas se mostram limitadas a solucionar o problema, diante da natureza transnacional do sistema de cabos submarinos, que extrapolam os limites territoriais de incidência. Ainda, o direito à privacidade também enfrenta dificuldades de efetivação, dada a inexistência de mecanismos de controle e responsabilização.

Ficou evidenciado que a interceptação não pode ser enquadrada no conceito de investigação científica marinha tal qual proposto pela CNUDM, eis que não atende aos seus requisitos de finalidade essencialmente científica, transparência e cooperação e que, embora haja controvérsias a respeito da possibilidade de enquadramento na definição de outros usos do mar internacionalmente lícitos, mostra-se incompatível com os fins pacíficos de regência do alto-mar.

Ante o exposto, é possível extrair da análise empreendida que, a partir de uma interpretação sistemática do Direito Internacional, a interceptação de dados em cabos submarinos em tempo de paz, apesar de não ser uma atividade ilícita em si mesma por falta de disposição expressa nesse sentido, se torna ilícita quando exercida como forma de espionagem técnica. Em especial, mostra-se incompatível com o ordenamento jurídico sempre que violar a soberania de outro Estado, Direitos Humanos ou configurar intervenção indevida em assuntos internos, principalmente se dotada de coercitividade.

Desta feita, essas constatações justificam a necessidade de se examinar mais detalhadamente o regime jurídico internacional aplicável aos cabos submarinos, que será objeto do próximo capítulo, mediante a análise de dispositivos da CNUDM e outras normas relevantes, como a Convenção de Cabos de 1884, a abordagem dos limites de jurisdição nos

espaços marinhos e as relações existentes entre os direitos e obrigações que envolvem essa infraestrutura crítica.

4 REGIME JURÍDICO INTERNACIONAL APLICÁVEL AOS CABOS SUBMARINOS

4.1 CONSIDERAÇÕES INICIAIS

Apesar das infraestruturas de cabos submarinos gozarem de *status* de recurso estratégico transnacional em razão de suportarem a vasta maioria do tráfego internacional de dados e, em que pese essa constatação já tenha sido esboçada no capítulo anterior, é indispensável destacar a inexistência no ordenamento jurídico internacional de um diploma específico que discipline de maneira suficiente e adequada tanto os aspectos que envolvem a proteção física dos cabos quanto a proteção do conteúdo informacional que por eles trafega.

A partir dessa premissa, é necessário, então, pensar de maneira sistêmica de modo a verificar quais seriam as normas de Direito Internacional aplicáveis às infraestruturas de cabos. Nesse sentido, a CNUDM³⁵ (Brasil, 1995) desempenha papel central na estruturação de uma análise das disposições aplicáveis aos cabos submarinos, na medida em que fornece um arcabouço normativo primário com disposições sobre colocação, manutenção e proteção sobre os referidos ativos, permitindo-se extrair, a partir dos seus princípios orientadores, uma ideia geral de quais seriam os limites aplicáveis para nortear também o tema da interceptação de dados³⁶.

Sob a perspectiva de Raha e Raju (2021, p. 26), a disciplina de governança dos cabos submarinos em nível global foi desenvolvida levando em conta os princípios do Direito do Mar da soberania territorial, da liberdade do mar e do patrimônio comum da humanidade, sendo constituído por tratados codificados e pelo costume internacional. Quanto ao Direito codificado, apresentam como relevantes a Convenção para a Proteção de Cabos Telegráficos Submarinos de 1884 (Brasil, 1888), as três Convenções sobre o Direito do Mar (1958, 1960 e 1982)³⁷, além do Regulamento Internacional para Evitar Abalroamentos no Mar (RIPEAM) e o Protocolo à Convenção de 1972 sobre a Prevenção da Poluição Marinha por Resíduos e

³⁵ A Convenção das Nações Unidas Sobre o Direito do Mar foi o resultado de um grande empenho por parte dos Estados para que se chegasse a um texto com aceitação universal, que somente veio a ocorrer com a Terceira Conferência das Nações Unidas Sobre o Direito do Mar, cujos trabalhos se prolongaram por anos. A Conferência foi formalmente instalada em Nova Iorque em 1972 e concluída com a assinatura da ata final em Montego Bay, Jamaica, em dezembro de 1982 (Longo, 2014, p. 74).

³⁶ A Convenção traz diversas prescrições sobre cabos submarinos ao dispor sobre o mar territorial (art. 21); águas arquipelágicas (art. 51); zona econômica exclusiva (art. 58); plataforma continental (art. 79); e alto-mar (art. 87 e arts. 112 a 115). Além das disposições atinentes aos diversos espaços marinhos, a Convenção prevê também que controvérsias relativas à sua interpretação e aplicação que envolvam cabos submarinos deverão ser submetidas à corte ou tribunal que tenha jurisdição, nos seus termos (art. 297).

outros Materiais, de 1996. Apontam os autores que as previsões da CNUDM constituem a base do regime internacional de colocação e proteção dos cabos submarinos, em virtude da sua ampla adesão e da sua natureza abrangente em assuntos afetos ao mar, que, de fato, prescreve os princípios de regência do Direito Internacional do mar, dentre eles, as prescrições incidentes sobre os cabos.

No mesmo sentido, Davenport (2015, p. 82) aponta que o arcabouço jurídico internacional sobre cabos submarinos está centrado na CNUDM, complementado por outras normas de Direito Internacional Consuetudinário³⁸, sendo ainda passível de aplicabilidade outros tratados internacionais relacionados à segurança, direitos humanos, conflitos armados³⁹, terrorismo⁴⁰ e regimes relacionados à proteção diplomática⁴¹, problematizando a capacidade do Direito Internacional em lidar com as ameaças aos cabos em razão da fragmentação do quadro jurídico existente.

Sendo assim, a exposição do presente capítulo será feita a partir da CNUDM como referência normativa para, a partir de então, identificar instrumentos complementares às suas disposições, bem como as sobreposições existentes. Desta forma, serão examinados a seguir, de forma detalhada, os dispositivos que são afetos à infraestrutura crítica de cabos submarinos dispostas na Convenção do Mar.

³⁷ Apesar de as Convenções oriundas das I e II Conferências das Nações Unidas sobre o Direito do Mar, respectivamente realizadas em 1958 e 1960, terem inegável importância para o desenvolvimento do Direito do Mar, no presente trabalho apenas serão abordadas as disposições da Convenção de 1982, tendo em vista que nela está consolidada o regime substantivo atual de regência da matéria.

³⁸ Algumas das disposições da CNUDM (art. 113 a 115) sobre a proteção dos cabos submarinos têm origem em normas consuetudinárias que foram codificadas na Convenção sobre o Alto-mar de 1958, sendo consideradas vinculantes mesmo para Estados que não são partes da CNUDM, evidenciando a sua natureza costumeira. Na mesma direção, a autora destaca o princípio consuetudinário da não-intervenção, que proíbe o uso da força contra a integridade territorial ou independência política de qualquer Estado, salvo exceções previstas, conforme amparado no Art. 2º (4) da Carta das Nações Unidas (Brasil, 1945).

³⁹ O *jus ad bellum* (conjunto de normas que regulamentam quando é apropriado ir para a guerra) e o *jus in bello* (princípios que regem como a guerra deve ser conduzida) estão dispostos em diversas fontes do Direito Internacional, dentre as quais pomos citar a Carta das Nações Unidas, Resoluções do Conselho de Segurança da ONU, as quatro Convenções de Genebra de 1949 e seus três protocolos adicionais, Convenção de Haia de 1907, o costume internacional e a jurisprudência internacional.

⁴⁰ No entendimento da autora, algumas convenções aplicadas ao terrorismo podem ser aplicadas aos casos de danos intencionais contra os cabos submarinos, como por exemplo a Convenção Internacional sobre a Supressão de Atentados Terroristas com Bombas, de 1997 (Brasil, 2002), que classifica como ato terrorista a utilização de artefatos explosivos contra instalações de infraestruturas.

⁴¹ Nomeadamente, a autora se refere a Convenção Internacional sobre Direitos Civis e Políticos (ONU, 1945) e a Convenção de Viena sobre Relações Diplomáticas (Brasil, 1965).

4.2 A CNUDM E OS CABOS SUBMARINOS

A Convenção de Montego Bay de 1982 reserva dispositivos específicos concernentes à proteção e à liberdade de colocação, reparação e manutenção dos cabos, organizando diretivas, instituindo direitos e obrigações dos Estados costeiros, além de condicionar a utilização do mar pelos demais Estados. Ao analisar estes dispositivos, é necessário ter em mente que a Convenção estabelece diferentes regimes para cada espaço marítimo considerado, e essa distinção se dá em razão das peculiaridades de cada zona, buscando-se conciliar a finalidade prática da proteção aos cabos, que é promover a livre comunicação internacional⁴², com os interesses estatais afetos à soberania (Davenport, 2015, p. 71). Isso posto, passaremos a apresentar e analisar as disposições sobre cabos submarinos presentes na CNUDM.

4.2.1 Disposições sobre Cabos Submarinos na CNUDM

Em termos numéricos, a Convenção do Direito do Mar apresenta 30 citações a cabo(s) submarino(s) no seu texto, as quais não ocorrem de forma aleatória, mas sim, variam em função de cada espaço marítimo, haja vista a existência de regimes jurídicos⁴³ próprios que foram estabelecidos levando em consideração a soberania dos Estados e a liberdade de navegação, estabelecendo as balizas de atuação dentro de cada espaço. Conforme ensina Zanella:

[...] o regime jurídico do mar se aplica de maneira diferenciada a cada zona marítima, de acordo com sua natureza, extensão e localização, e como os direitos, deveres e limitações dos Estados se ajustam a essas variações espaciais (Zanella, 2025, p. 121).

⁴² A menção aqui feita sobre a comunicação internacional se dá em razão do escopo principal do trabalho, mas não se ignora que a utilização de cabos submarinos também pode ocorrer com outras finalidades, como por exemplo a transmissão de energia.

⁴³ Conceitualmente, entende-se por regime jurídico o conjunto das normas e princípios jurídicos aplicáveis a determinado instituto ou categoria jurídica.

Sendo assim, passaremos a analisar as diretrizes estabelecidas pela Convenção para cada espaço marítimo, com o intuito de compreender a lógica regulatória posta pelo principal instrumento internacional de disciplina dos cabos submarinos.

4.2.1.1 Mar Territorial

Quanto ao Mar Territorial, a CNDM sucintamente estabelece no seu Art. 21 a possibilidade da adoção de leis e regulamentos pelo Estado costeiro com vistas a condicionar a passagem inocente voltados à proteção dos cabos submarinos. Sob os auspícios da Convenção, o Estado costeiro dispõe de autoridade para regular todas as atividades que são realizadas nas suas águas territoriais, haja vista a previsão de soberania até as 12 milhas náuticas (MN), soberania essa que deve ser exercida em conformidade com as demais disposições convencionais e regras de Direito Internacional.⁴⁴

Em que pese essa soberania no mar territorial sofrer algumas limitações como consequência do princípio da liberdade de navegação instituído pela própria Convenção, sendo a maior delas a passagem inocente,⁴⁵ ainda assim ao Estado costeiro é possível estabelecer no seu ordenamento jurídico interno condicionantes desse direito de passagem inocente a serem impostas aos outros Estado, denotando assim a relevância que a CNUDM conferiu à proteção da infraestrutura de cabos, haja vista que acaba por condicionar o exercício de um direito de raiz principiológica em seu detrimento.

Neste ponto, então, cabe uma ressalva importante. A relevância atribuída aos cabos submarinos e à passagem inocente pela CNUDM poderia levar à falsa percepção de que um navio de determinada bandeira que esteja passando por águas territoriais de outro Estado e que esteja envolvido em atividade de colocação de cabo submarino estaria em passagem inocente, quando isso não é verdade, pois qualquer coisa que vá para além de “passar” já é suficiente para descaracterizar esse instituto, de modo que para atuar dentro das águas territoriais de um país, as empresas operadoras de cabos devem se submeter às licenças e regulamentações do Estado costeiro (Raha; Raju, 2021, p. 32).

⁴⁴ Artigo 3º, CNUDM.

⁴⁵ Artigos 17 a 19, CNUDM.

Importante notar que o texto do Art. 21 da Convenção prevê que o Estado costeiro “pode” adotar leis e regulamentos em matéria de cabo submarino, extraindo-se interpretação no sentido de que se trata de mera faculdade, e não obrigação dos Estados criarem efetivamente tais regramentos, revelando verdadeiro ato de discricionariedade estatal a ser exercido mediante seus critérios de conveniência e oportunidade. Como desdobramento dessa liberalidade, Davenport (2015, p. 77) avalia que essa ausência de obrigação de certa forma contribui para a fragmentação e existência de lacunas no regime jurídico internacional, já que a proteção dessas infraestruturas depende da vontade política de cada Estado, acarretando níveis desiguais de proteção nessas áreas marítimas submetidas à soberania.

4.2.1.2 *Estados Arquipélagos*

No que se refere aos Estados Arquipélagos (ou Arquipelágicos)⁴⁶, similarmente ao que ocorre com o Mar Territorial, os Estados possuem soberania⁴⁷ em relação às águas denominadas arquipelágicas,⁴⁸ ou seja, nessas águas há o exercício de soberania, verificando-se, igualmente, o direito de passagem inocente de navios de outras nacionalidades, em razão da similaridade verificada entre os regimes jurídicos desses dois espaços marítimos.

Porém, apesar da semelhança existente entre os regimes, a Convenção estabeleceu uma distinção entre eles afeta ao tratamento da matéria ao estipular que os Estados Arquipelágicos devem respeitar os cabos submarinos que foram previamente instalados por outros Estados e que atravessam as suas águas sem tocar a terra. Trata-se do Art. 51(2), que prescreve a obrigatoriedade do Estado arquipelágico permitir a manutenção e a substituição desses cabos desde que seja previamente notificado. Todavia, é bem verdade que tal disposição parece ter pouca aplicabilidade prática nos dias atuais, tendo em vista que os cabos que já haviam sido instalados por ocasião da entrada em vigor da CNUDM provavelmente já estão fora de uso e que para a instalação de novos cabos há a necessidade de permissão do Estado arquipelágico, conforme apontam Wargo e Davenport (2014, p. 259), mas ainda assim, se trata de uma disposição que deve ser considerada.

⁴⁶ Conforme conceituação prevista no artigo 46(a) da CNUDM, “Estado arquipélago” significa em Estado constituído totalmente por um ou vários arquipélagos, podendo incluir outras ilhas.”

⁴⁷ Artigo 49(1), CNUDM.

⁴⁸ São denominadas águas arquipelágicas aquelas encerradas pelas linhas de base arquipelágicas, traçadas em conformidade com o artigo 47 da Convenção.

4.2.1.3 Zona Econômica Exclusiva (ZEE)

As duas prescrições sobre cabos submarinos afetas à ZEE encontram-se no Art. 58 da CNUDM, e podem ser analisadas sob duas óticas distintas, sendo uma do Estado Costeiro e outra do Estado usuário. O item (1) do referido dispositivo estabelece que os Estados, sejam eles com ou sem litoral, gozam na ZEE das liberdades típicas do Alto-mar elencadas no Art. 87⁴⁹, sendo uma delas a colocação de cabos submarinos. Prescreve ainda este item que os Estados dispõem também de outros usos do mar internacionalmente lícitos relacionados com tais liberdades, demonstrando um caráter instrumental da disposição, uma vez que, além de conferir o direito, confere também os instrumentos necessários ao seu exercício. Assim, o item (1) revela, sob a ótica do Estado costeiro, um ônus de suportar o exercício de certos direitos por outros Estados na sua ZEE.

Por sua vez, de modo a harmonizar o exercício de tais liberdades pelos demais Estados com os interesses e direitos do Estado costeiro, o item (2) estabelece parâmetros para a utilização desse espaço marítimo, prescrevendo que os Estados usuários deverão ter em conta os direitos e deveres do Estado costeiro e deverão respeitar as leis e regulamentos por este adotados, os quais deverão estar em consonância com a CNUDM e demais disposições do Direito Internacional.

Percebe-se, então, que os direitos e a jurisdição do Estado costeiro devem coexistir com as liberdades de outros Estados na ZEE. Especificamente, a CNUDM confere a todos os Estados o direito de instalação, manutenção e operação de cabos submarinos, desde que essas atividades sejam compatíveis com as suas disposições e respeitem os direitos do Estado costeiro, que possuem os chamados “direitos de soberania”⁵⁰ sobre os recursos naturais da sua ZEE.

⁴⁹ Artigo 87(1), alínea “c”, CNUDM.

⁵⁰ Não se deve confundir aqui os conceitos de “soberania” e “direitos de soberania”. Enquanto o primeiro tem uma conotação política e uma maior abrangência (conforme detalhado no capítulo anterior), o segundo denota um conteúdo de exclusividade no exercício de certos direitos de exploração econômica. Nesse sentido, explica Zanella, ao discorrer sobre o texto apresentado pelo grupo de trabalho que ficou responsável pelas disposições da ZEE, que a CNUDM “caracterizou a Zona Econômica Exclusiva como um espaço *sui generis*; não era Alto Mar pois os Estados possuíam direitos soberanos e também não era Mar Territorial, uma vez que esses direitos se limitavam somente à exploração dos recursos naturais” (2025, p. 230). Para um maior aprofundamento do tema, consultar BEIRÃO, André Panno. O complexo exercício da jurisdição penal no mar. *Revista de Direito e Negócios Internacionais da Maritime Law Academy - International Law and Business Review*, v. 3, n. 2, p. 104–134, 26 dez. 2023.

Portanto, tendo em conta que o regime jurídico aplicável à ZEE pode-se dizer híbrido ou *sui generis*, devendo coexistir de maneira harmoniosa os direitos soberanos do Estado costeiro sobre os recursos naturais com as liberdades universais de uso desse espaço marítimo por outros Estados, a CNUDM estabelece um regime jurídico próprio de regência dos cabos submarinos na ZEE, podendo o Estado costeiro implementar regulações razoáveis sobre esses ativos, mas sempre respeitando os direitos e liberdades dos demais Estados quanto ao exercício das suas liberdades previstas na Convenção (Zanella, 2025, p. 279).

4.2.1.4 *Plataforma Continental (PC)*

O regime estabelecido pela CNUDM aos cabos submarinos na Plataforma Continental encontra-se disciplinado no Art. 79. Segundo o item (1) do dispositivo, todos os Estados têm o direito de instalar cabos submarinos na PC de outros Estados, abrangendo também o direito a repará-los e mantê-los, conforme se depreende do item (2).

Quanto ao Estado costeiro, a CNUDM dispõe que a liberdade de colocação de cabos por outros Estados não afeta o seu direito de estabelecer condições para que tal liberdade não prejudique o aproveitamento dos seus recursos nessa extensão submersa do continente, ou o perfeito funcionamento das suas ilhas artificiais, estruturas e instalações, de acordo com o previsto no item (4). Todavia, embora os Estados costeiros tenham esse direito de estabelecer normas para condicionar a instalação de cabos na sua PC, não há a obrigação na sua adoção, nem a CNUDM estabelece os limites do seu exercício, o que pode acarretar controvérsias quanto à proteção dos cabos nessa zona, conforme apontam Raha e Raju (2021, p. 38).

A Convenção prevê também o dever dos Estados levar em consideração os cabos já instalados, não devendo dificultar a possibilidade de reparação dos cabos existentes, conforme previsão do item (5) do dispositivo em apreço, significando que as operações de instalação de cabos não devem interferir negativamente no exercício do mesmo direito por outras partes. Esse dever decorre da obrigação geral estabelecida pela CNUDM sobre o uso responsável do espaço marítimo, que busca preservar os direitos e atividades legítimas dos outros atores. Apesar do texto convencional utilizar o termo “Estado”, tal disposição é dirigida

também às empresas que operam com essas infraestruturas (Ford-Ramsden; Davenport, 2014, p. 146).

Semelhantemente ao que ocorre na ZEE, o Estado costeiro possui direitos de soberania sobre a Plataforma Continental para efeitos de exploração e aproveitamento dos seus recursos naturais,⁵¹ mas, diferentemente do que ocorre na ZEE, tais recursos compreendem aqueles vivos e não vivos que se encontrem no leito do mar e no subsolo, excluídos, portanto, aqueles encontrados na coluna d'água (Zanella, 2025, p. 297).

Verifica-se, portanto, que a jurisdição do Estado costeiro sobre a sua PC está em harmonia com a jurisdição sobre a ZEE, tendo a CNUDM integrado as disposições acerca desses espaços marítimos distintos de maneira coerente, haja vista que os regimes da Plataforma Continental e da Zona Econômica Exclusiva aplicam-se concomitantemente à mesma área geográfica em larga medida, salvo quando a Plataforma Continental se estende além das 200 milhas, quando então o regime da Plataforma Continental será o único aplicável (Davenport, 2015, p. 72).

4.2.1.5 *Alto-mar*

No tocante ao Alto-mar, inicialmente é importante pontuar que se trata de uma zona marítima regida pela liberdade, cujos princípios orientadores são a liberdade de utilização, de igualdade entre os Estados, do uso pacífico e da preservação do meio marinho, conforme ensina Zanella (2025, p. 266).

A Convenção de Montego Bay positivou uma série de liberdades próprias do Alto-mar e, especificamente no que concerne aos cabos submarinos, a primeira disposição não poderia ser outra senão a liberdade de colocá-los, remetendo aos termos da sua Parte VI, que trata da Plataforma Continental.⁵² Confirmando esse princípio de liberdade, o Art. 112 positivou expressamente o direito dos Estados de instalar cabos sobre o leito do mar além da PC, bem como o dever de não obstruir o exercício do mesmo direito pelos demais.

Os Art. 113 a 115 da CNUDM são dedicados à proteção desses ativos, os quais também são aplicados quando os cabos são instalados na ZEE, conforme disposto no Art.

⁵¹ Artigo 77, CNUDM.

⁵² Artigo 87(1), c, CNUDM.

58(2), bem como aos instalados na PC, por força da alínea “c” do seu Art. 87(1), de maneira que as regras de proteção, responsabilidade e jurisdição para os cabos submarinos estendem-se além do Alto-mar para essas zonas marítimas onde são observados direitos específicos dos Estados costeiros, revelando uma semelhança entre os regimes jurídicos cujo ponto de interseção é a liberdade (Ford-Ramsden; Davenport, 2014, p. 146).

Ocorre que essa liberdade de utilização do Alto-mar não é (e nem poderia ser) absoluta, já que o próprio Art. 87(2) da Convenção preconiza que deverá ser exercida em consonância com os seus demais termos. Portanto:

A essência da liberdade do alto-mar é que nenhum Estado pode adquirir soberania sobre suas partes. Essa é a norma geral, mas sofre a influência das doutrinas de reconhecimento, aquiescência e prescrição, segundo as quais, mediante o uso prolongado aceito por outros países, certas áreas do alto-mar que ligam águas territoriais de Estados litorâneos podem ficar sujeitos à soberania de um Estado. Isso foi sublinhado no caso Plataforma continental anglo-norueguesa (Shaw, 2010, p. 446, *apud* Pereira; Pereira, 2014, grifo próprio).

Assim sendo, o Art. 113 da Convenção estabelece que os Estados devem adotar leis e regulamentos para sancionar os danos aos cabos causados por navios que arvoem a sua bandeira ou por pessoa submetida à sua jurisdição. Em razão dos diferentes comandos contidos neste dispositivo, será ele transcrito abaixo para permitir uma melhor visualização e análise dos seus termos, *in verbis*:

ARTIGO 113

Ruptura ou danificação de cabos ou dutos submarinos

Todo Estado **deve** adotar as leis e regulamentos necessários para que constituam infrações passíveis de sanções a ruptura ou danificação, por um navio arvorando a sua bandeira ou por uma pessoa submetida à sua jurisdição, de um cabo submarino no alto mar, **causadas intencionalmente ou por negligência culposa**, de modo que possam interromper ou dificultar as comunicações telegráficas ou telefônicas, bem como a ruptura ou danificação, nas mesmas condições, de um cabo de alta tensão ou de um duto submarino. Esta disposição aplica-se também aos atos que tenham por objeto causar essas rupturas ou danificações ou que possa ter esse efeito. Contudo, esta disposição **não se aplica às rupturas ou às danificações cujos autores apenas atuaram com o propósito legítimo de proteger a própria vida ou a segurança dos seus navios, depois de terem tomado todas as precauções necessárias para evitar tal ruptura ou danificação** (grifo do autor).

É possível perceber da leitura do dispositivo supratranscrito que, diferentemente do que ocorre com os demais espaços marítimos, no Alto-mar o Estado tem a obrigação de constituir normatização tipificando infrações e estabelecendo sanções incidentes sobre os

navios que arvorem a sua bandeira, bem como sobre as pessoas submetidas à sua jurisdição, que causem dano à infraestrutura de cabos submarinos, seja por dolo ou mesmo por culpa⁵³.

Deve-se notar que para que determinada conduta danosa seja considerada uma infração (que poderá ser de natureza penal ou civil), ela deve ser praticada ou com a intenção deliberada de causar o dano (dolosamente) ou como consequência da inobservância de um dever de cuidado (culposamente). Logo, se o dano for decorrente de uma situação de emergência, quando a conduta danosa foi voltada à preservação de vidas ou a proteção do navio, mediante a adoção de todas as medidas necessárias para que fosse evitado o dano, não há que se falar em infração punível (Zanella, 2025, p. 279).

Em termos jurídicos, esse dispositivo fomenta a ampliação da jurisdição penal dos Estados, comumente limitada aos respectivos territórios, com a intenção de provocar uma atuação mais participativa dos mesmos no controle dos seus jurisdicionados, com a finalidade de manter o perfeito funcionamento do sistema nas áreas marítimas que não se encontram sob a jurisdição de qualquer Estado (Bueger, Liebetrau, Franken, 2022, p. 14).

Todavia, a CNUDM não estabelece parâmetros claros para a repressão dessas infrações, deixando a cargo de cada Estado fazê-lo, bem como restringe a jurisdição penal aos atos praticados por seus próprios nacionais ou por pessoas a bordo de navios que ostentem a sua bandeira, não prevendo mecanismos de repressão como fez com certos delitos, como a pirataria⁵⁴, o tráfico de escravos⁵⁵ e a transmissão não autorizada⁵⁶, por exemplo. Por esse motivo, Raha e Raju (2021, p. 41) apontam que essa limitação de jurisdição representa uma

⁵³ O texto, ao tratar sobre os aspectos subjetivos da conduta danosa aos cabos, utiliza as expressões “causadas intencionalmente” e “negligência culposa” para referir-se ao dolo e a culpa, respectivamente. Conforme constante no Glossário Jurídico do Supremo Tribunal Federal, o dolo pode ser definido como a intenção deliberada e consciente de praticar um ato criminoso, omissivo ou comissivo, com o intuito de produzir determinado resultado ou assumindo o risco de produzi-lo. Já a culpa é o ato voluntário, proveniente de imperícia, imprudência ou negligência, de efeito lesivo ao direito de outrem, porém, sem a intenção de provocar o dano. Disponível em: <https://portal.stf.jus.br/jurisprudencia/glossario.asp>.

⁵⁴ Para a repressão à pirataria marítima, a CNUDM confere aos Estados a possibilidade do exercício do instituto da jurisdição universal, previsto no artigo 105, que estabelece que qualquer estado pode apresar um navio que esteja cometendo atos de pirataria em alto-mar, independente da sua bandeira. Outro mecanismo previsto para a repressão à pirataria é o direito de visita, instituído no artigo 110, que confere aos navios de guerra a prerrogativa de ingresso a bordo de navios suspeitos de cometerem o delito, também independentemente da bandeira que esteja arvorando.

⁵⁵ A repressão ao tráfico de escravos também deve ser exercida por qualquer Estado. Todavia, diferentemente do que ocorre com a pirataria, o tráfico de escravos não está submetido à jurisdição universal, o que implica dizer que somente o Estado de bandeira pode julgar quem cometer este delito, conforme previsto no artigo 99 da Convenção.

⁵⁶ São consideradas transmissões não autorizadas aquelas transmissões de rádio ou televisão difundidas a partir de um navio ou instalação no alto-mar e dirigidas ao público em geral com violação dos regulamentos internacionais, exceto as de chamada de socorro, conforme artigo 109(2), CNUDM. Tais transmissões também devem ser reprimidas por todos os Estados e podem ser submetidas à jurisdição universal.

vulnerabilidade significativa na proteção das infraestruturas críticas de cabos submarinos, uma vez que não permite a responsabilização plena e a atuação efetiva dos Estados diante dessas ameaças.

Por sua vez, o Art. 114 da CNUDM dispõe sobre os eventuais danos aos cabos submarinos que já estão instalados e que sejam causados durante o procedimento de instalação ou manutenção de outros cabos ou dutos. Este dispositivo impõe a obrigação (e não mera faculdade) de os Estados adotarem a normatização necessária para que aqueles que estejam sob a sua jurisdição, que sejam proprietários de cabos ou dutos submarinos, respondam pelos custos da reparação caso causem danos a cabos ou dutos de outros proprietários durante a realização das tarefas de instalação ou manutenção (Heinegg, 2013, p. 308).

Diferentemente do que ocorre no artigo 113, o artigo 114 não intenta a caracterização de uma infração, mas apenas a responsabilização de natureza civil direcionada ao proprietário do cabo que eventualmente cause dano a outras estruturas durante a sua operação, haja vista se tratar de dano decorrente do exercício de uma atividade regular, razão pela qual a responsabilidade fica limitada ao custo dos reparos. Como afirma Kwan (2025, p. 25), trata-se na verdade de uma obrigação de cuidado imposta aos operadores de cabos, que devem exercer as suas atividades zelando pelo perfeito funcionamento do sistema.

Por último, uma outra obrigação imposta aos Estados no que concerne aos cabos dispostos no alto-mar diz respeito a necessidade de adoção de leis e regulamentos voltados à indenização por perdas ocorridas para evitar danos a tais sistemas, de acordo com o previsto no Art. 115 da Convenção.

Nota-se neste ponto a intenção dos redatores do texto da Convenção na promoção de práticas responsáveis da comunidade marítima, na medida em que o mesmo impõe aos Estados a criação de normatização interna voltada a assegurar que os proprietários de navios que comprovem ter sacrificado âncoras, redes de pesca ou qualquer outro equipamento para evitar causar danos em cabos submarinos sejam indenizados pelo seu proprietário, desde que comprove a tomada de todas as medidas razoáveis de precaução antes de tal sacrifício (Raha; Raju, 2021, p. 48).

Assim como nos dois artigos que o antecedem, o Art. 115 fomenta a atuação legislativa estatal para a proteção dos cabos submarinos, mas, da mesma forma, representa

uma lacuna na medida em que depende diretamente da implementação e execução adequada pelos Estados.

4.2.1.6 *Solução de controvérsias*

A última citação na Convenção de Montego Bay sobre os cabos submarinos está no Art. 297, topograficamente situado na Seção 3 da Parte XV, parte essa que dispõe sobre solução de controvérsias. A CNUDM apresenta um sistema abrangente de solução de controvérsias, integrando mecanismos jurídicos e diplomáticos cuja finalidade é assegurar que disputas relacionadas à interpretação ou aplicação da Convenção possam ser resolvidas por intermédio de meios pacíficos de negociação, conciliação ou por tribunais internacionais (Carvalho, 2018, p. 29).

A Seção 3 apresenta uma série de limites e exceções à aplicação da Seção 2, que por sua vez estabelece procedimentos compulsórios conducentes à decisões obrigatórias. Em linhas gerais, a Seção 2 prevê que, diante da impossibilidade de se chegar a um acordo entre as partes⁵⁷ pelas vias diplomáticas, a Convenção institui a adoção de mecanismos para se chegar a uma decisão final vinculativa aos litigantes, que poderá ser exarada pelo Tribunal Internacional do Direito do Mar (ITLOS), Corte Internacional de Justiça (CIJ), tribunal arbitral ou tribunal arbitral especial, a depender do procedimento escolhido.⁵⁸

Ocorre que a aplicação da Seção 2, ou seja, a aplicação dos mecanismos de jurisdição previstos na Convenção, é limitada por algumas circunstâncias previstas na Seção 3, tratando-se, portanto, de verdadeiras cláusulas de reserva de jurisdição, pois estabelecem que algumas matérias são subordinadas à soberania de cada Estado, não podendo ser submetidas obrigatoriamente à jurisdição de terceiros (Zanella, 2025, p. 770). O caso que interessa especificamente ao presente trabalho encontra-se na alínea “a” do Art. 297(1), *in verbis*:

⁵⁷ Ensina Zanella (2025) que, via de regra, as partes são os Estados signatários da Convenção. Entretanto, organizações internacionais também podem figurar como partes em controvérsias a serem solucionadas pelos mecanismos da CNUDM, haja vista que a Parte XV se aplica a todos os seus membros, de modo que, para exemplificar, a Autoridade Internacional dos Fundos Marinhos (ISA), com natureza jurídica de organismo internacional (artigo 157), possui legitimidade para ser parte em controvérsia a ser submetida aos referidos mecanismos, por força de disposição do artigo 285, nesse sentido.

⁵⁸ No caso de as partes não terem chegado a uma solução pela via da conciliação, podem escolher voluntariamente qual o mecanismo estabelecido pela Convenção para submeter o litígio. Caso não haja um consenso acerca do mecanismo, aplicar-se-á a arbitragem compulsoriamente, conforme determina o artigo 287(5).

SEÇÃO 3. LIMITES E EXCEÇÕES À APLICAÇÃO DA SEÇÃO 2
ARTIGO 297

Limites à aplicação da seção 2.

1. As controvérsias relativas à interpretação ou aplicação da presente Convenção, no concernente ao exercício por um Estado costeiro dos seus direitos soberanos ou de jurisdição previstos na presente Convenção, serão submetidas aos procedimentos estabelecidos na seção 2 nos seguintes casos:

a) quando se alegue que um Estado costeiro atuou em violação das disposições da presente Convenção no concernente às liberdades e direitos de navegação ou de sobrevoo ou à liberdade e ao direito de colocação de cabos e dutos submarinos e, outros usos do mar internacionalmente lícitos especificados no artigo 58; ou
(...)

Extraí-se da leitura do dispositivo acima que uma dessas matérias que devem ficar subordinadas apenas ao alvedrio do Estado costeiro é o exercício tanto dos seus direitos de soberania⁵⁹ quanto da sua jurisdição, devendo, via de regra, prevalecer a vontade estatal, desde que não viole as disposições da Convenção sobre a liberdade de colocação de cabos submarinos por outros Estados. Caso isso ocorra, ou seja, se surgir controvérsia envolvendo o o exercício de direitos soberanos ou de jurisdição do Estado costeiro de um lado, e a liberdade de colocação de cabo de outro, poderá o litígio ser submetido aos procedimentos discriminados na Seção 2.

4.2.1.7 *Quadro analítico das disposições da CNUDM*

Feitas as análises pertinentes acerca de todas as diretrizes sobre cabos submarinos apresentadas pela CNUDM, apresenta-se abaixo o Quadro 2, com o objetivo de demonstrar de maneira sintética como o legislador convencional tratou sobre o tema.

Quadro 2 – Citações a cabos submarinos na CNUDM

Parte da CNUDM	Artigos com menção a cabos (quantidade de citações)	Número de citações por parte	Conteúdo central
Parte II – Mar Territorial	Art. 21 (1)	1	Possibilidade de adoção de leis e regulamentos pelos Estados costeiros condicionando a passagem inocente, nos termos da CNUDM
Parte IV – Estado Arquipélago	Art. 51 (3)	3	Garantia a cabos existentes antes da CNUDM, bem como a sua manutenção e substituição
Parte V – Zona Econômica Exclusiva	Art. 58 (2)	2	Liberdades de colocação e manutenção de cabos por todos os Estados, respeitadas as

⁵⁹ Relativos à exclusividade da exploração econômica (vide nota 15).

Parte da CNUDM	Artigos com menção a cabos (quantidade de citações)	Número de citações por parte	Conteúdo central
			regulamentações (facultativas) do Estado costeiro de acordo com a CNUDM
Parte VI – Plataforma Continental	Art. 79 (8)	8	Liberdades de colocação e manutenção de cabos por todos os Estados, respeitadas as regulamentações (facultativas) do Estado costeiro de acordo com a CNUDM
Parte VII – Alto-mar	Art. 87 (1); 112 (3); 113 (3); 114 (5); e 115 (3)	15	Liberdade de colocação de cabos; Obrigatoriedade de adoção de leis e regulamentos destinados a sanção penal, civil e a indenização por perdas decorrentes da preservação dos cabos
Parte XV- Solução de Controvérsias	Art. 297 (1)	1	Possibilidade de utilização dos mecanismos de solução de controvérsias previstos na CNUDM

Fonte: Elaborado pelo autor.

Mediante uma detida apreciação das balizas estabelecidas pela Convenção, percebemos que elas se resumem, basicamente, em liberdades, soberania e dever de proteção. Isso posto, o cerne da discussão normativa verifica-se no conflito existente entre a liberdade de colocação dos cabos submarinos e o seu decorrente dever de proteção estipulados pela CNUDM face a uma falta de regulação do Direito Internacional, que não apresenta, explicitamente, um diploma que disponha especificamente sobre o tratamento que deve ser conferido ao conteúdo dos dados que são trafegados nesses meios.

Ao passo que a Convenção de Montego Bay consagra uma liberdade quase que ilimitada para o lançamento de cabos submarinos nos diversos espaços marítimos (à exceção do mar territorial), sendo certa, também, a obrigação dos Estados na proteção dessa infraestrutura, tamanha amplitude atualmente se revela comprometida pelo surgimento de novas ameaças, dentre elas as de cunho cibernético, não contempladas no texto convencional (Faria, 2024, p. 49).

As disposições da CNUDM foram formuladas em um tempo diferente do atual, onde os cabos de fibra ótica não eram tão amplamente utilizados e que as ameaças cibernéticas não representavam uma preocupação primária, sendo essa a causa apontada por Heinegg (2013, p. 309) para a suposta falta de adequação do regime legal atual para a proteção dos cabos, cujo escopo não contempla as novas formas de ameaça e interferência.

Divergindo do posicionamento da maioria dos especialistas, Heinegg (2013, p. 317) afasta a tese de insuficiência normativa da Convenção de Montego Bay, defendendo que suas disposições não excluem o exercício de jurisdição por outros Estados além do Estado de bandeira ou de nacionalidade do agente causador do dano, desde que essa jurisdição não seja em matéria criminal, permitindo-se a adoção de medidas protetivas. Segundo argumenta, a crítica aos Art. 113 a 115 é devida apenas na medida em que a redação não é tão clara quanto deveria, mas que o verdadeiro problema não é a falta de proteção ou jurisdição, mas a ambiguidade na linguagem da CNUDM, necessária à sua aprovação dado o contexto da época em que foi discutida.

Ainda que se pense como Heinegg e se considere que a CNUDM seja adequada à proteção dos cabos desde que suas disposições sejam devidamente complementadas pela legislação doméstica dos Estados, a comunidade internacional percebe que seus regimes são geralmente insuficientes, haja vista que grandes porções das infraestruturas estão localizados no alto-mar e, portanto, sem jurisdição de qualquer Estado, ou na ZEE, sujeitas a jurisdição muito limitada. Isso significa que mesmo que eventualmente coíbam a coleta de dados de inteligência, a aplicabilidade dos regimes domésticos ficaria muito limitada aos seus nacionais e navios que ostentem a sua bandeira ou sobre atos cometidos nas suas águas territoriais, o que as fariam parcialmente inócuas ao fim pretendido, uma vez que as atividades de coleta de dados geralmente envolvem atores estrangeiros fora das águas territoriais (Petty, 2021, p. 283).

Para Davenport (2015, p. 105) não está totalmente claro se a CNUDM pode ser aplicada à questão da vigilância em massa mediante a escuta física (*tapping*) realizada em cabos submarinos, pois tal atividade não se amolda às percepções convencionais de atividades militares ou de coleta de inteligência no mar, direcionadas a aumentar o conhecimento do ambiente marinho ou sobre as capacidades militares de outros Estados. Entretanto, reconhecendo o grau de incerteza em questão, defende a autora a aplicabilidade da Convenção a tais atividades ao propor uma abordagem partindo de uma interpretação evolutiva da CNUDM, considerando-a um “organismo vivo”, razão pela qual atenderia aos seus propósitos a sua incidência sobre estas hipóteses, mas que de toda sorte a jurisdição do Estado costeiro também estaria limitada aos seus nacionais e navios.

Evidencia-se assim a tensão existente entre a ampla liberdade de colocação de cabos submarinos prevista na CNUDM e o correlato dever de proteção imposto aos Estados

signatários, contrastada com a ausência de qualquer regime internacional que discipline o tratamento do conteúdo de dados que são transmitidos através dessa infraestrutura.

Desta feita, se por um lado a CNUDM assegura uma liberdade quase que irrestrita de instalação de cabos nos diversos espaços marítimos, bem como delimita obrigações de proteção, por outro o seu alcance revela-se insuficiente a conter novas ameaças, especialmente as de cunho cibernético, não previstas no texto convencional, conforme registrado na literatura especializada.

4.3 OUTRAS NORMAS E INSTRUMENTOS RELEVANTES

Após tratadas as disposições acerca do principal diploma de regulação da segurança e proteção dos cabos submarinos, a Convenção de Montego Bay, passaremos a apreciar outras normas e instrumentos aplicáveis, com a finalidade de compreender o alcance das disposições do Direito Internacional de trato da matéria, almejando um diagnóstico do quadro normativo de regência.

4.3.1 Convenção Para a Proteção de Cabos Telegráficos Submarinos de 1884

A Convenção para a Proteção de Cabos Telegráficos Submarinos de 1884, doravante denominada de Convenção de Cabos de 1884, é considerada como o primeiro diploma internacional dedicado ao regramento específico de cabos submarinos (Heinegg, 2013, p. 297), haja vista que antes da sua entrada em vigor não havia um arcabouço legal multilateral destinado a regulamentar essa infraestrutura, estando em vigor atualmente para 36 Estados-parte⁶⁰.

Apesar de sua criação ser motivada pela necessidade de proteção dos cabos telegráficos, suas disposições continuam sendo aplicadas aos cabos de fibra óptica modernos, uma vez que são consideradas costume internacional, ou seja, mesmo sem referência explícita

⁶⁰ A Convenção de Cabos de 1884 é um tratado antigo e a sua gestão não é centralizada por uma organização única como é o caso da ONU, o que dificulta a aferição do número exato de Estados-parte, de modo que por ocasião da elaboração do presente trabalho o quantitativo de 36 membros foi consultado no sítio eletrônico do National Oceanic and Atmospheric Administration (2025) e do Centre for International Law (2024).

aos tipos de cabos modernos, seus princípios continuam válidos e aplicáveis como prática consolidada por Estados e pela indústria (Burnett, 2011, p. 2).

A Convenção de Cabos de 1884 serviu de inspiração para os redatores da Convenção de Montego Bay, uma vez que esta incorporou algumas disposições daquela, as quais foram consideradas princípios essenciais de regência da matéria, a saber:

a) Art. 113 da CNUDM (dispõe sobre a obrigação dos Estados editarem regulamentação penalizadora para danos aos cabos submarinos) foi baseado no Art. II da Convenção de Cabos de 1884, mantendo a mesma lógica punitiva aos que causarem danos intencionais ou por negligência;

b) Art. 114 da CNUDM (dispõe sobre a responsabilidade do proprietário de cabo submarino durante as operações de instalação ou manutenção) foi inspirado diretamente no Art. IV da Convenção de 1884, reproduzindo o princípio da responsabilidade objetiva⁶¹ do proprietário de cabo que cause dano a outro cabo existente, que deverá arcar com os custos da reparação; e

c) Art. 115 da CNUDM (dispõe sobre indenização por perda de âncora, rede ou outro equipamento sacrificado para evitar dano a cabo submarino) foi baseado no Art. VII da Convenção de 1884, reproduzindo o princípio da compensação pelos sacrifícios de equipamento para proteger cabos de comunicação, como forma de incentivar os navegadores a protegerem esses ativos sem sofrerem prejuízo econômico.

Por outro lado, os preceitos constantes na Convenção de Cabos de 1884 relativos à segurança operacional dos navios engajados nas operações de colocação e manutenção de cabos não foram inseridos na CNUDM. Tais preceitos preconizam que outros navios mantenham uma distância mínima de uma milha náutica dos navios-cabo envolvidos em reparo e de um quarto de milha náutica das boias marcadoras de cabos.⁶² Conforme explicam Green e Burnett (2014, p. 228), essas omissões ocorreram durante o processo de redação dos rascunhos de artigos sobre o Direito do Mar pela Comissão de Direito Internacional que serviram de base para a CNUDM e as suas antecessoras, as Convenções de Genebra de 1958, ficando decidido que apenas os princípios gerais considerados essenciais para a codificação

⁶¹ O princípio da responsabilidade objetiva dispensa a verificação da intenção, bastando a comprovação do ato de causar o dano. Conforme ensina Carvalho Filho, “essa forma de responsabilidade dispensa a verificação do fator culpa em relação ao fato danoso. Por isso, ela incide em decorrência de fatos lícitos ou ilícitos, bastando que o interessado comprove a relação causal entre o fato e o dano” (2018, p. 669).

⁶² Artigos V e VI da Convenção de Cabos de 1884, respectivamente.

do Direito do Mar deveriam ser reproduzidos, excluindo-se, portanto, os dispositivos que fossem mais específicos.

Talvez a omissão mais relevante de todas seja a prevista no Art. X da Convenção de 1884, que confere o direito de identificar a nacionalidade de um navio supostamente envolvido em danos a cabos submarinos. Este dispositivo concedia aos navios de guerra e outros navios estatais de todos os Estados-parte o direito de parar e inspecionar navios mercantes estrangeiros suspeitos de terem causado dano a um cabo submarino, com o objetivo de identificar a nacionalidade do navio e recolher provas, representando uma exceção ao princípio da jurisdição do Estado de Bandeira,⁶³ que prevaleceu quanto a este ponto, haja vista a opção dos redatores da Comissão de Direito Internacional em não reproduzir na Convenção de Montego Bay previsão semelhante (Heinegg, 2013, p. 309).

Em síntese, pode-se afirmar que o regime jurídico da Convenção de Cabos de 1884 continua tendo alguma aplicabilidade prática, uma vez que apresenta detalhes procedimentais que a CNUDM não faz (estabelecimento de distâncias mínimas e o direito de visita), podendo complementá-la para preencher algumas de suas lacunas (Burnett, 2011, p. 12).

Contudo, ainda que tenha utilidade complementar às disposições da CNUDM, o regime jurídico da Convenção de 1884 acaba tendo a sua aplicabilidade limitada ao seu reduzido número de Estados-parte, fator que reduz a sua eficácia. Raha e Raju (2021, p. 9) destacam que as disposições da Convenção de 1884 que não foram inseridas na CNUDM não são consideradas direito consuetudinário dada a sua falta de ampla aceitação, reforçando a limitação da eficácia das suas disposições.

Sob a ótica da proteção frente as novas ameaças, o regime da Convenção de 1884 não se mostra apto para lidar com os desafios modernos, considerando que se preocupou apenas em resguardar a dimensão física de proteção dos cabos. Quanto a este ponto, Davenport (2015, p. 109) advoga a necessidade de criação de um regime especializado mais robusto, entendendo que a dependência de um tratado do século XIX é problemática por ser ineficaz a responder às ameaças atuais.

A inaptidão da Convenção de 1884 para responder às ameaças de cunho cibernético é reforçada pelo fato de que o Manual Tallin 2.0 apenas lhe faz menção ao abordar

⁶³ Direito de visita (v. nota 20).

a sua regra 54 (que dispõe sobre cabos submarinos de comunicação) para contextualizá-la como precedente histórico que fundamenta a obrigação internacional de proteção dos cabos, mencionando sua relevância somente no que diz respeito ao aspecto físico dos cabos (Schmitt, 2017, p. 257).

Assim, a Convenção de 1884 permanece como antecedente jurídico importante como instrumento complementar às disposições da CNUDM, mas insuficiente para atender as demandas contemporâneas.

4.3.2 Outros Instrumentos Conexos

Além dos diplomas específicos já apresentados, há a possibilidade de aplicação de outros instrumentos, cuja incidência dependerá do contexto fático considerado que envolva a temática dos cabos.

4.3.2.1 *Regulamento Internacional para Evitar Abalroamentos no Mar (RIPEAM)*

Como o seu título sugere, trata-se de um regulamento destinado a garantir a segurança da navegação por intermédio de uma série de regras voltadas à prevenção do choque mecânico entre embarcações, adotado por intermédio de Convenção firmada pela Organização Marítima Internacional e promulgada pelo Brasil pelo Decreto nº 80.068/1977 (Brasil, 1977). Suas diretrizes não regulam diretamente os cabos submarinos, mas estabelece uma proteção indireta ao enquadrar as embarcações dedicadas a colocar, recolher e reparar esses ativos como uma “embarcação com capacidade de manobra restrita”⁶⁴, conferindo a elas um tratamento especial de navegação.

Como consequência desse enquadramento, os navios-cabo têm prioridade de navegação em relação a outras embarcações, as quais deverão se manter afastadas da sua

⁶⁴ Regra 3(g) do RIPEAM.

rota,⁶⁵ desde que exibam as luzes e marcas de sinalização específicas,⁶⁶ representando uma proteção indireta à infraestrutura física de cabos.

4.3.2.2 *Convenção de Londres de 1972 e seu Protocolo, de 1996*

A Convenção sobre a Prevenção da Poluição Marinha por Alijamento de Resíduos e Outras Matérias é uma das primeiras Convenções com ampla aceitação global voltada à proteção do meio ambiente marinho das atividades humanas, estando em vigor desde 1975, sendo promulgada pelo Brasil por intermédio do Decreto nº 87.566/1982 (Brasil, 1982). Juntamente com o seu Protocolo de 1996, a Convenção de Londres de 1972 objetiva promover o controle efetivo de todas as fontes de poluição marinha através da regulação do descarte de resíduos no mar (IMO, 2025).

O Protocolo de 1996 estabelece que a colocação de cabos submarinos no mar, desde que não seja com o propósito de mero descarte, não é caracterizado como uma atividade de poluição marinha sujeita às proibições de alijamento, em que pese a necessidade de cumprimento de padrões ambientais em algumas jurisdições (Raha; Raju, 2021, p. 26). Ou seja, conforme previsto no referido Protocolo, o abandono de cabos submarinos que foram instalados com a finalidade de se prestarem à sua utilização não é caracterizado como alijamento,⁶⁷ representando, portanto, uma proteção voltada ao meio ambiente marinho do que propriamente à infraestrutura de cabos.

4.3.2.3 *Direito da Guerra*

Especificamente no que diz respeito aos danos intencionais causados aos cabos submarinos, a normatização internacional aplicada à guerra pode preencher algumas lacunas, conforme explica Davenport (2015, p. 87). O ramo do Direito Internacional comumente denominado de Direito da Guerra é composto por um conjunto de tratados internacionais,

⁶⁵ Regra 18 do RIPEAM.

⁶⁶ A Regra 27 do RIPEAM dispõe especificamente sobre embarcações sem governo ou com capacidade de manobra restrita, as quais deverão exibir luzes e marcações diferenciadas destinadas a identificá-las como tais tipos.

⁶⁷ Parágrafo 4.2.3 do Protocolo de 1996 à Convenção de Londres de 1972.

costumes e princípios gerais, sendo doutrinariamente bifurcado em outras duas vertentes, o *ius ad bellum*, que cuida do direito a declarar guerra e empreender hostilidades, e o *ius in bello*, que estabelece princípios, regras e limitações durante o estado de guerra (Guedes, 2007, p. 176).

Sob essa perspectiva, Davenport (2015, p. 87) defende que o artigo 2(4) da Carta das Nações Unidas, que estabelece que os Estados devem se abster da ameaça ou uso da força contra a integridade territorial ou independência política de qualquer Estado, pode ser empregado como ponto de partida e, a partir daí, levar a efeito o uso da força contra um Estado agressor.

Ocorre que para que tal medida seja efetivada, o dano intencional a cabo submarino deve ser considerado uma ameaça à paz ou segurança internacionais ou, ainda, representar um ato de agressão, hipóteses nas quais o Conselho de Segurança da ONU, após deliberar a respeito, poderá autorizar o uso da força contra o Estado agressor, na forma prevista no Art. 39 da Carta.

Sendo assim, algumas dificuldades se apresentam à efetiva aplicação dos princípios e regras estabelecidos pelo Direito da Guerra na proteção dos cabos submarinos, em razão da dificuldade prática de se demonstrar que os danos às estruturas estão no patamar de uma ameaça à paz e à segurança internacional aptos a justificar a intervenção do Conselho de Segurança ou o exercício do direito de autodefesa dos Estados. Além disso, estas disposições regulam as interações entre Estados em regime de guerra ou hostilidades, não sendo passíveis de aplicação quando o dano intencional for causado por um ator não estatal e em tempo de paz.

Em se tratando de interceptação de dados, a aplicação do Direito da Guerra poderia ser invocado, em tese, desde que fique configurado que a obtenção dos dados represente um ato de espionagem e seja de tal monta que caracterize um atentado aos princípios do Direito Internacional da Soberania e Não-intervenção, conforme já se manifestou a Corte Internacional de Justiça (CIJ, 2014), representando uma possibilidade de aplicação indireta e com certo caráter de excepcionalidade.

4.3.2.4 *Convenções contra-terrorismo*

Embora ainda não haja nenhum relato noticiado, não deve ser desconsiderada a hipótese na qual a infraestrutura de cabos submarinos pode ser alvo de ações de sabotagem executadas por grupos terroristas financiados, com o objetivo de causar interrupção e transtornos no mercado e em sistemas em geral (Vichi; Pinto; Sá, 2020, p. 334), suscitando o questionamento acerca da possibilidade de aplicação de convenções internacionais contra-terrorismo em face de ataques a danos submarinos.

Quanto a este ponto, a dificuldade surge já na falta de consenso sobre uma definição do que seria terrorismo, termo este dotado de ampla ambiguidade conceitual e diversidade de critérios nas diversas formulações existentes, o que acarreta uma série de dificuldades de ordem teórica e prática para lidar com este problema, ainda que muito debatido no contexto da geopolítica internacional (Semeraro; Nasser, 2025, p. 34).

Conforme informações colhidas no sítio eletrônico do Escritório das Nações Unidas sobre Drogas e Crime no Brasil⁶⁸, a ONU dispõe de um conjunto de 13 convenções e 6 protocolos adicionais que versam sobre o terrorismo, abordando diferentes áreas e tipos de atividades consideradas terroristas. Todavia, deste conjunto de diplomas, apenas a Convenção Internacional para a Supressão de Atos Terroristas com Bombas⁶⁹ poderia ser aplicada caso um cabo submarino fosse alvo de um ato terrorista, uma vez que é o único dos referidos tratados que protege diretamente infraestruturas críticas de comunicação, destacando-se que para a sua aplicação é necessário que o ataque seja realizado com o emprego de bombas ou artefatos explosivos (Davenport, 2015, p. 90). Porém, a aplicação dessa Convenção aos cabos submarinos tal qual encontra-se redigida hoje seria bem restrita, pois a utilização de artefatos explosivos contra cabos submarinos teria como alvo, provavelmente, instalações como pontos de ancoragem e outras estruturas localizadas em terra, razão pela qual não nos estenderemos na sua abordagem, considerando que o escopo da presente pesquisa está adstrita às águas sob jurisdição do Brasil.

⁶⁸ Disponível em: <https://www.unodc.org/cofrib/pt/sobre/convencoes-e-mandato.html>.

⁶⁹ Convenção Internacional para a Supressão de Atos Terroristas com Bombas, adotada em 15 de dezembro de 1997, com entrada em vigor em 23 de maio de 2001. Atualmente, conta com 172 Estados-parte.

4.3.2.5 *Recomendações e Diretrizes do ICPC*

O International Cable Protection Committee (ICPC), fundado em 1958, é reconhecido como a principal organização não governamental dedicada a proteção e resiliência dos cabos submarinos. Sua missão é promover a segurança dessa infraestrutura crítica frente a riscos tanto naturais quanto causados pelo homem. A composição do ICPC é ampla e diversificada, incluindo proprietário de cabos, operadores de navios especializados, empresas de levantamento de rotas, além de representantes governamentais. Atualmente, reúne mais de 235 membros distribuídos em mais de 70 países⁷⁰, funcionando como um fórum internacional para a troca de informações técnicas, bem como no desenvolvimento de pesquisa científica e na formulação de recomendações regulatórias (Azaria; Davenport, 2020).

O Comitê possui um compêndio de Recomendações elaboradas por grupos de trabalho constituídos por seus membros destinados a disseminar boas práticas a serem observadas por todos os *stakeholders* de cabos submarinos. Conforme definido pelo Comitê, uma Recomendação representa “um guia que fornece aos proprietários de cabos e outros usuários do leito marinho informações tecnicamente precisas para promover os mais altos padrões de confiabilidade e segurança no ambiente de cabos submarinos” (ICPC, 2024, ICPC Recommendations, tradução própria).

Sendo assim, o papel do ICPC no contexto da proteção dos cabos submarinos é, dentre outros, o de formulador de boas práticas de natureza não vinculante e típicas de *soft law*⁷¹ que, embora forneçam padrões úteis de atuação operacional e de complementação entre a regulação estatal e a governança privada, a falta de força vinculante das suas disposições revelam uma fragilidade.

Mencione-se, ainda, que nenhuma das publicações do ICPC aborda a questão da proteção do fluxo de dados que trafega pelos cabos submarinos, ao contrário, todos os documentos sobre proteção são voltados ao aspecto físico e à resiliência da infraestrutura contra danos acidentais e intencionais.

⁷⁰ Dados obtidos no sítio do ICPC em 22 dez. 2025. Disponível em <https://www.iscpc.org/about-the-icpc/member-list>.

⁷¹ *Soft law* refere-se a normas, diretrizes e princípios que não são juridicamente vinculativos, destinados a influenciar e orientar comportamentos, sendo mais comumente definido como fontes de obrigações exortativas, em vez de obrigações de natureza juridicamente vinculativa (Guzman; Meyer, 2010).

4.4 CONSIDERAÇÕES PARCIAIS - DIAGNÓSTICO E LACUNAS DO REGIME JURÍDICO INTERNACIONAL

Com o objetivo de sistematizar e tornar mais compreensível o arcabouço jurídico internacional aplicável aos cabos submarinos, será apresentado abaixo um quadro sintético das convenções, tratados e instrumentos examinados ao longo deste capítulo, cujo propósito é permitir identificar de maneira objetiva o âmbito material e espacial de cada diploma, o tipo de obrigação ou liberdade instituída, as convergências e sobreposições existentes, além de evidenciar a principal lacuna verificada, qual seja, a ausência de disposições específicas de tutela do conteúdo informacional que trafega pelos cabos submarinos. Vejamos o Quadro 3:

Quadro 3 – Regime internacional dos cabos submarinos: panorama, escopo e lacunas.

Diploma/Instrumento	Temática principal e abrangência	Aspectos principais regulados sobre cabos	Proteção dos dados	Principais lacunas
CNUDM	Direito do Mar, de caráter geral e adesão universal. Vinculativa.	Liberdades; obrigações; e responsabilidades nos diversos espaços marítimos	Inexistente	Foco na proteção física; jurisdição limitada aos regimes de cada zona marítima e pelo princípio do Estado da bandeira
Convenção de Cabos de 1884	Específica sobre cabos telegráficos, com pouca adesão. Vinculativa.	Liberdades; obrigações; e responsabilidades além do Mar territorial	Inexistente	Baixa adesão; foco na proteção física; disposições obsoletas
RIPEAM	Específico sobre segurança da navegação, com adesão quase universal. Vinculativo	Prioridade de navegação conferida aos navios-cabo	Inexistente	Proteção apenas indireta e operacional, não tutelando os cabos em si
Convenção de Londres (1972) e Protocolo (1996)	Específico sobre proteção ambiental marinha, com ampla adesão. Vinculativa.	Não considera como alijamento proibido a colocação de cabos submarinos	Inexistente	Foco na proteção ambiental, não tutelando os cabos em si
Direito da Guerra	Específico sobre Relações Diplomáticas, de adesão universal. Vinculativo	Autorização do uso da força	Indireta e excepcional	Aplicável apenas em casos de hostilidades entre Estados e de difícil enquadramento
Convenções contra-terrorismo	Específico sobre terrorismo, com ampla adesão. Vinculativo	Supressão de atos terroristas com bombas e explosivos	Inexistente	Aplicabilidade restrita à utilização de bombas e provavelmente em terra
ICPC – Recomendações e Diretrizes	Específico sobre cabos submarinos, com ampla adesão. Não vinculativo.	Boas práticas técnicas, resiliência e proteção física	Inexistente	Ausência de força vinculante e silêncio quanto aos dados

Fonte: Elaborado pelo autor.

A análise desenvolvida no decorrer no presente capítulo demonstra que o regime internacional de regência dos cabos submarinos apresenta-se fragmentado e alicerçado predominantemente sobre normas formuladas para tutelar objetos diversos das infraestruturas em si, tais como a utilização dos diversos espaços marítimos, segurança da navegação, meio ambiente marinho, relações diplomáticas e outros. Na sua menor parte apresentam algumas disposições de tutela dos cabos, mas essencialmente aplicáveis à dimensão física, sendo silentes quanto ao fluxo informacional.

A Convenção das Nações Unidas sobre o Direito do Mar surge como o referencial normativo central desse regime ao estruturar liberdades, deveres e responsabilidades afetos à colocação, manutenção e proteção desses ativos, buscando apaziguar interesses distintos sobre soberania estatal, liberdade nos mares e interesses da comunicação internacional. Isso se deve ao seu *status* internacional de “Constituição dos Oceanos,”⁷² o que dá às suas diretrizes aceitação universal e lhe permite colocar como marco regulatório principal.

Entretanto, em que pese a CNUDM tratar de maneira muito abrangente e detalhada uma grande gama de temáticas afetas ao oceano, ela foi elaborada em um contexto histórico no qual os cabos submarinos ainda não exerciam um papel tão significativo quanto ao que desempenha atualmente, do mesmo modo em que também não eram cogitadas as ameaças de natureza cibernética e as técnicas modernas de interceptação e espionagem conhecidas contemporaneamente. Por tal razão, ainda que o texto convencional forneça ferramentas relevantes para a proteção física dessa infraestrutura crítica, o seu alcance se mostra limitado quando confrontado com novas formas de interferência que extrapolam o mero dano físico e incidem sobre o fluxo de dados.

Para além da Convenção de Montego Bay, a regulamentação da interceptação de dados e da coleta de inteligência marítima e cibernética também não é tratada em nenhum instrumento específico do Direito Internacional, fato que acaba levando os estudiosos do tema a tentarem preencher essa lacuna com a aplicação de uma série de outras normas e regimes legais cuja incidência e aplicação não é objeto de consenso. O estudo dos demais instrumentos internacionais examinados reforçam esse diagnóstico.

A Convenção de Cabos de 1884, ainda que represente um antecedente histórico importante e contenha disposições procedimentais mais detalhadas que a CNUDM,

⁷² Apesar de tecnicamente não ser considerada uma Constituição é comumente chamada dessa forma em razão da sua grande abrangência (Zanella, 2025, p. 74).

permanece restrita à dimensão física dos cabos e padece com a baixa adesão de Estados-parte e com a inadequação das suas previsões para responder às demandas atuais.

De igual modo, instrumentos como o RIPEAM e a Convenção de Londres de 1972 oferecem apenas proteção indireta e muito reduzida, eis que são voltadas especificamente a outras áreas afetas ao mar, sem enfrentar diretamente as dificuldades afetas aos cabos submarinos enquanto condutores de fluxos informacionais estratégicos.

Por sua vez, a utilização de regimes jurídicos de aplicação excepcional, como o Direito da Guerra e Convenções contra o terrorismo, se mostram mais como uma tentativa dos estudiosos do tema em apresentar uma solução diante da ausência de um sistema adequado do que propriamente uma possibilidade viável, haja vista estar condicionada a hipóteses específicas e de difícil verificação na prática.

Nesse mesmo raciocínio, as diretrizes e recomendações expedidas pelo ICPC cumprem relevante papel na difusão de informações de caráter técnico e operacional em proveito daqueles *stakeholders* da indústria de cabos, contribuindo para a resiliência e proteção física dos cabos. Entretanto, a natureza não vinculante das suas disposições e a ausência de disposições concernentes aos dados reforçam a constatação de que o regramento internacional desses ativos permanece lacunosa.

Dessa forma, o quadro normativo delineado ao final deste capítulo revela que o regime legal atual é percebido com lacunas, destacando-se entre elas a inexistência de um regramento jurídico específico e abrangente voltado à tutela do fluxo informacional que transita pelos cabos submarinos, de modo que a regulação existente atualmente permanece concentrada na dimensão material da infraestrutura, deixando desprotegida a dimensão imaterial dos dados, justamente aquela que se mostra mais sensível sob a ótica da soberania.

Esse diagnóstico evidencia a necessidade de construção de um regime normativo internacional específico capaz de harmonizar os interesses estatais e a segurança das comunicações globais, preenchendo a lacuna legal que torna as atividades de interceptação de dados em cabos submarinos fora das águas territoriais de um Estado uma atividade altamente permissiva sob a luz do Direito Internacional clássico. É nesse contexto que se insere a análise que será desenvolvida no capítulo seguinte, voltado aos desafios a serem enfrentados pela comunidade internacional no estabelecimento de um regime jurídico abrangente e suficiente.

5 CENÁRIOS NORMATIVOS E CAMINHOS PARA A REGULAÇÃO INTERNACIONAL

5.1 CONSIDERAÇÕES INICIAIS

Como apresentado no capítulo anterior, o regime jurídico internacional de incidência sobre os cabos submarinos, centrado principalmente na CNUDM mas também marcado pontualmente por diversos outros instrumentos, é caracterizado por ser fragmentário e pela sua limitação material, tendo em vista a concentração das suas disposições predominantemente sobre a dimensão física dos cabos, ou seja, sobre o mero suporte que serve de instrumento para o fluxo de dados, este sim verdadeira razão de ser da tutela almejada e deixada à margem. A partir dessa avaliação, o presente capítulo objetiva avançar na análise dos possíveis caminhos normativos para o desenvolvimento de um regime internacional mais condizente com a realidade atual. Busca-se, portanto, apreciar as consequências da existência das lacunas verificadas no regime e associá-las a algumas propostas existentes, bem como ao que se vislumbra como possibilidades, de modo a permitir a compreensão do debate existente sobre este ponto.

5.2 CONSEQUÊNCIAS DA AUSÊNCIA DE REGULAÇÃO

Como primeira consequência relevante que pode ser apontada para a falta de um regime internacional específico sobre cabos submarinos é a insegurança jurídica, que pode afetar tanto os Estados quanto os operadores privados e, em última análise, toda a sociedade que se beneficia de um sistema de comunicação eficaz. Como visto, a fragmentação normativa e, especificamente no que toca a interceptação de dados, a falta de parâmetros delimitadores da ilicitude e de responsabilidades produzem um ambiente no qual eventuais condutas prejudiciais ao bom funcionamento do sistema não podem ser eficazmente prevenidas. Para Davenport (2015, p. 97), a falta de clareza sobre as atividades de inteligência sob os ditames da CNUDM gera um ambiente de incerteza e ambiguidade, acarretando o aumento da desconfiança dos Estados em relação a atividades de lançamento de cabos.

Outra consequência evidenciada pela falta de regulação específica é a normalização de práticas unilaterais, principalmente por parte de Estados com maior capacidade tecnológica, favorecendo o desequilíbrio do sistema internacional, conforme destacado por Petty (2021, p. 296). Aponta o especialista que as grandes potências

frequentemente se envolvem em *hacking* de cabos submarinos e, por isso, podem querer preservar essa capacidade de vigilância em detrimento de Estados sem litoral e/ou com menor potencial tecnológico, contribuindo para uma dinâmica na qual a superioridade técnica se sobrepõe à legalidade como fator determinante da conduta estatal.

A potencial violação sistemática de direitos humanos também é um outro efeito indesejado da falta de uma tutela mais específica, principalmente no que concerne à privacidade. Conforme entendimento manifestado pelo Alto Comissariado das Nações Unidas para os Direitos Humanos, os programas de vigilância em massa são incompatíveis com a Declaração Universal dos Direitos Humanos⁷³ e com o Pacto Internacional sobre Direitos Civis e Políticos⁷⁴ quando realizados sem fundamento legal. Em relatório que dispõe sobre a privacidade na era digital, a ONU reconhece que o Direito Internacional dos Direitos Humanos estabelece um quadro claro e universal para a proteção do direito à privacidade que, no entanto, não é implementado em razão de práticas e realidades estatais incompatíveis com essa tutela, apresentando como resultado a falta de responsabilização por interferências ilegais (ONU, 2014, p. 16).

Ameaças à soberania e à igualdade dos Estados também representam uma outra consequência que pode ser assinalada como decorrência da lacuna normativa, haja vista que a interceptação clandestina de comunicações afetas a questões estratégicas pode configurar ingerência indevida em assuntos internos (Gill, 2013, p. 226). Como visto no capítulo 2, embora o Direito Internacional tradicionalmente trate a espionagem com ambiguidade, isso não significa que toda a forma de coleta de informações seja neutra, ainda mais quando se tratar de uma prática sistematizada em larga escala, que pode conferir vantagens e permitir ingerências externas em assuntos internos.

Analisando sob uma ótica mais repressiva, Cate *et al* (2017, p. 73) enfatizam a escalada internacional dos ataques de natureza cibernética, destacando a sua natureza transnacional, o que sugere a necessidade de uma resposta jurídica que transcenda as fronteiras das jurisdições nacionais. A inexistência de regras internacionais impede a possibilidade de responsabilização internacional por condutas ilícitas, haja vista que deixa ao arbítrio dos Estados a edição de leis e regulamentos com esse fim e que somente poderá incidir, via de regra, sobre os seus nacionais e navios que arvoem a sua bandeira.

Esse quadro é marcado pela falta da adoção de critérios objetivos e minimamente uniformes voltados à atribuição de responsabilidades, representando um *deficit* do nível de

⁷³ Art. 12, DUDH.

⁷⁴ Art. 17, PIDCP.

segurança. Khader e França (2024, p. 9) argumentam que para que um delito seja legítimo sob a ótica democrática ele precisa estar intrinsecamente ligado à proteção de um bem jurídico real e material, e não apenas por razões arbitrárias. Nessa perspectiva, não há dúvidas que o perfeito funcionamento das comunicações representa bem jurídico de especial relevância internacional e que a interceptação em cabos submarinos atingiria não somente bens jurídicos individuais (privacidade e liberdade), mas também coletivos (como a segurança pública e ordem econômica), além daqueles de titularidade do Estado (sobretudo a soberania).

Como entende Costa (2011, p. 10), a criação de um delito é legítima apenas se for estritamente necessária (obediência ao princípio penal da intervenção mínima⁷⁵), se proteger um bem jurídico claramente definido e se a antecipação da punibilidade nos crimes de perigo⁷⁶ (como seria o caso da interceptação) for racionalmente justificada e proporcional ao perigo, estando claro que tais critérios são perfeitamente atendidos.

Por fim, o vazio legal concorre também para potenciais consequências econômicas significativas que podem se estender a níveis globais. A Organização para a Cooperação e Desenvolvimento Econômico (OCDE) já alertou que a percepção de vulnerabilidades e as incertezas que podem ser exacerbadas pela falta de ações de segurança adequadas, como a ausência de mecanismos jurídicos de proteção, podem levar ao aumento de medidas protecionistas digitais e ao enfraquecimento da cooperação internacional, minando o alcance dos objetivos econômicos e sociais (OCDE, 2015, p. 30).

Logo, a ausência de uma regulação específica dedicada à segurança dos cabos submarinos e que englobe atos de espionagem mediante o uso de interceptação não constitui mero problema jurídico abstrato, mas sim um empecilho à estabilidade sistêmica, pois transcende a esfera dogmática e projeta efeitos concretos sobre as relações internacionais e direitos estatais e individuais, revelando a necessidade de uma resposta normatizadora internacional.

5.3 PRINCIPAIS PROPOSTAS DOUTRINÁRIAS E INSTITUCIONAIS

A ausência de normas específicas sobre a regulação de cabos submarinos é apontada pela literatura especializada como um dos principais fatores de fragilidade desse

⁷⁵ Segundo Greco (2017, p. 127), “o direito penal só deve preocupar-se com a proteção dos bens mais importantes e necessários à vida em sociedade”, sendo esse o mote do princípio da intervenção mínima ou *ultima ratio*.

⁷⁶ Os crimes de perigo são aqueles nos quais a conduta do agente é punível antes que ela venha efetivamente causar dano ao bem jurídico protegido (por exemplo, do prejuízo financeiro, violação da privacidade ou interferência em assuntos internos do Estado), conforme Greco (2017, p. 252).

sistema. Especialistas como Davenport (2015, p. 106) e Pettty (2021, p. 276) sustentam que o escopo da legislação existente, voltada ao aspecto exclusivamente físico dos cabos, tal como na CNUDM, não é o bastante quando considerada a dimensão do fluxo de dados informacionais e a natureza das ameaças contemporâneas, cada vez mais sofisticadas. Para os citados especialistas, a interceptação clandestina em tempos de paz afronta diretamente princípios basilares dos Direito Internacional, como soberania e não intervenção.

Algumas iniciativas e debates voltados a desenvolver um sistema de governança mais adequado e robusto emergem no âmbito da comunidade internacional, as quais serão tratadas a seguir.

5.3.1 Organização das Nações Unidas

A inexistência de um tratado específico no âmbito da ONU poderia levar à falsa percepção de que o tema aqui tratado não recebe a devida atenção das Nações Unidas. Entretanto, os debates e trabalhos desenvolvidos por grupos de especialistas neste campo florescem já há décadas (ONU, 2025, p. 1), bem como a atuação da União Internacional de Telecomunicações (ITU, na sigla em Inglês), organismo específico direcionado ao trato das telecomunicações, evidenciam a discussão da governança das comunicações nos seus domínios, como se verá.

5.3.1.1 *Grupos de Trabalho e Fóruns de Discussão*

A ONU dispõe de dois grupos diferentes com natureza de fóruns de discussões focados no debate e estabelecimento de normas de comportamento responsável no ciberespaço e sobre segurança das Tecnologias da Informação e Comunicação (TIC), sendo eles o Grupo de Peritos Governamentais⁷⁷ (GGE, na sigla em Inglês) e Grupo de Trabalho Aberto sobre Desenvolvimentos na Área da Informação e Telecomunicações no Contexto da Segurança Internacional⁷⁸ (OEWG, na sigla em Inglês).

De uma forma geral, os relatórios elaborados pelo GGE e pelo OEWG já vêm reconhecendo que atividades cibernéticas maliciosas que atinjam infraestruturas críticas

⁷⁷ O Grupo de Peritos Governamentais (GGE) é caracterizado por ser um grupo mais restrito, formado por especialistas nomeados pelos Estados-membros da ONU para estudar e propor medidas para a segurança internacional no ciberespaço.

⁷⁸ O Grupo de Trabalho Aberto sobre Desenvolvimentos na Área da Informação e Telecomunicações no Contexto da Segurança Internacional (OEWG) representa um fórum mais inclusivo, admitindo a participação de todos os interessados.

violam o Direito Internacional (ONU, 2015 e ONU, 2021), fato que fornece base argumentativa para sustentar a ilicitude de interceptações realizadas em cabos submarinos em determinadas circunstâncias.

O GGE de 2015, que se concentrou em estudar e analisar as ameaças que surgem do uso das TIC pelos Estados e atores não estatais, estabeleceu como norma fundamental que um Estado não deve conduzir ou apoiar conscientemente atividades de TIC que danifiquem intencionalmente ou prejudiquem o uso de infraestruturas críticas de outros Estados, destacando a importância da cooperação internacional para lidar com as vulnerabilidades (ONU, 2015). O relatório elaborado pelo grupo apontou um pacote de medidas com o objetivo de mitigar as ameaças, destacando-se a sugestão da adoção de diretrizes voluntariamente estabelecidas e não vinculativas definindo os parâmetros de comportamento dos Estados, bem como a análise de como o Direito Internacional pode ser aplicável, com ênfase na aplicação da Carta das Nações Unidas e no princípio da soberania.

Avançando no debate do tema, a Assembleia Geral decidiu instituir, a partir de 2019, um Grupo de Trabalho Aberto que atua de maneira consensual no desenvolvimento de regras, normas e princípios voltados a atuação responsável dos Estados, com a participação de diversas partes interessadas estatais e não estatais. O relatório do OEWG destacou a preocupação com a evolução da sofisticação das ameaças e com o desenvolvimento de capacidades de TIC para usos militares e por atores não estatais, reafirmando a aplicabilidade do Direito Internacional, sobretudo da Carta das Nações Unidas, como essencial para a manutenção da segurança no ambiente cibernético. Merece destaque a menção ao fato de que alguns Estados manifestaram o desejo de negociação de um instrumento juridicamente vinculante nessa seara, todavia, as conclusões finais do grupo se concentraram no fortalecimento do quadro existente (normas voluntárias e Direito Internacional) e na continuação do diálogo regular sob os auspícios da ONU (ONU, 2021, p. 24).

Como seu mais recente esforço, o OEWG estabelecido para o quinquênio 2021-2025 teve como foco principal alcançar um consenso geral mediante a adoção de um Mecanismo Global, que sucederá o referido grupo, projetado para servir como uma plataforma permanente direcionada ao diálogo e à ação de membros das Nações Unidas sobre a segurança da TIC, marcado pela sua natureza consensual e não vinculativa. Quanto a infraestrutura de cabos submarinos, o Relatório final apenas faz menção à preocupação dos Estados com a necessidade de sua proteção, não fazendo outras considerações a respeito (ONU, 2025).

5.3.1.2 União Internacional de Telecomunicações (ITU)

A ITU é uma agência especializada das Nações Unidas para as tecnologias de informação e comunicações, cujo objetivo é padronizar e regular os assuntos relativos ao uso das ondas de rádio e telecomunicações internacionais.⁷⁹ No âmbito da segurança dos cabos submarinos, sua atuação tem sido marcada por reiterar a importância estratégica dessa infraestrutura e o fortalecimento de uma governança global. Nessa linha, lançou em 2024 em conjunto com o Comitê internacional de Proteção de Cabos (ICPC, na sigla em Inglês), o Órgão Consultivo Internacional para a Resiliência de Cabos Submarinos, com o objetivo de fortalecer a resiliência desse sistema.⁸⁰ Todavia, embora essa iniciativa represente um significativo esforço de coordenação multissetorial, ela também tem natureza de fórum consultivo destinado a estimular o diálogo e a cooperação entre Estados e demais atores participantes, cujas deliberações são carentes de força vinculante própria dos tratados internacionais, a exemplo da Declaração elaborada na primeira Cúpula Internacional sobre Resiliência de Cabos Submarinos realizada em 2025, na Nigéria.⁸¹

5.3.2 Propostas de Organizações Regionais e Setoriais

As iniciativas de desenvolvimento de normas e práticas regulatórias não são apenas desenvolvidas no âmbito global e de organismos de natureza governamental, mas também no plano regional e de entidades setoriais especializadas, cujo papel é relevante para a proteção da infraestrutura de cabos submarinos, haja vista a ausência de uma regulação abrangente e vinculativa em nível global. Embora tais instrumentos não possuam natureza jurídica vinculante, contribuem para a formação de um arcabouço normativo progressivo (*soft law*) e para o amadurecimento do debate, contribuindo para o preenchimento de lacunas deixadas pelo Direito Internacional (Frazier, 2021, p. 18).

⁷⁹ Conforme glossário constante no sítio do Departamento de Controle do Espaço Aéreo (DECEA), a ITU é a organização internacional mais antiga do mundo, fundada como International Telegraph Union no dia 17 de maio de 1865, em Paris. Disponível em: <https://www.decea.mil.br/index.cfm?i=utilidades&p=glossario&single=2271>. Acesso em: 16 jan. 2026.

⁸⁰ Informações disponíveis em: <https://www.itu.int/en/mediacentre/Pages/PR-2024-11-29-advisory-body-submarine-cable-resilience.aspx>.

⁸¹ A Declaração sugere um quadro para fomentar a resiliência e incentivar esforços cooperativos. Não se trata de um documento com natureza vinculativa, mas mero protocolo de intenções. Disponível em: <https://www.itu.int/digital-resilience/submarine-cables/wp-content/uploads/sites/2/2025/02/summit-declaration-nigeria-2025.pdf>. Acesso em: 16 jan. 2026.

5.3.2.1 *International Cable Protection Committee (ICPC)*

Conforme já abordamos no capítulo anterior⁸², o ICPC é reconhecido como o principal ator setorial dedicado à proteção dos cabos submarinos, desempenhando papel significativo no setor ao elaborar e difundir recomendações direcionadas à resiliência dessa infraestrutura crítica, as quais têm natureza de diretrizes consensuais para a orientação dos proprietários, da indústria, Estados e demais usuários do leito marinho sobre ações que aumentam a segurança das redes submarinas, que, embora não sejam normas vinculantes, de certa forma acabam por condicionar e influenciar decisões regulatórias, uma vez que fornecem um padrão técnico praticado internacionalmente. Além do que já foi dito e no que diz respeito à sua importância para a formulação de novos caminhos de regulação, o ICPC promove a conscientização governamental e coopera com organismos internacionais por meio de eventos como a sua plenária anual e parcerias técnico-regulatórias (como o Órgão Consultivo Internacional para a Resiliência de Cabos Submarinos, em parceria com a ITU), apresentando orientações para a formulação de regimes legais nacionais e internacionais que versem sobre segurança da infraestrutura de cabos submarinos.

Conforme apontam Raha e Raju (2021, p. 45), o ICPC já sugeriu em 2008 um projeto de convenção no âmbito da CNUDM para a proteção e reparo dos cabos submarinos, abordando a aplicação das obrigações estabelecidas pela Convenção de Montego Bay e a negligência dos Estados quanto às mesmas, sem, no entanto, apresentar maiores inovações para além do aperfeiçoamento das disposições que já estão presentes na CNUDM.⁸³

Aspecto importante a ser mencionado é que, apesar de ser o maior *stakeholder* com atuação na segurança de cabos submarinos, o ICPC não traz em nenhuma das suas publicações qualquer recomendação atinente à interceptação dos dados em trânsito nesses ativos, o que demonstra que o cerne da preocupação do Comitê é o aspecto físico da infraestrutura.

5.3.2.2 *European Union Agency for Cybersecurity (ENISA)*

No âmbito da União Europeia (UE), a ENISA é uma agência dedicada a alcançar um elevado nível de cibersegurança na Europa e tem participado de iniciativas sobre a proteção de cabos submarinos para além do aspecto técnico. O foco da sua atuação está na

⁸² Ver subseção 3.3.2.5.

⁸³ O projeto de convenção proposto pelo ICPC está sob acesso restrito (Raha; Raju, 2021, p. 45, nota 124).

cooperação internacional e na coordenação de ações dentro da UE e com parceiros estratégicos. Nos documentos pesquisados no presente estudo não foram identificadas iniciativas voltadas à celebração de um tratado regional de incidência no continente europeu, não havendo nenhuma proposta da ENISA nesse sentido. Em vez disso, em relatório de 2023 a agência relaciona os tratados internacionais aplicáveis à segurança dos cabos submarinos, manifestando o entendimento de que eles já estabelecem normas suficientes para esse intuito. No lugar de buscar a celebração de um novo tratado, a ENISA concentra as suas recomendações em esclarecer as responsabilidades e os mandatos das autoridades nacionais, o aprimoramento da regulamentação já existente (ENISA, 2024), ou seja, suas disposições têm igualmente natureza de *soft law*.

No tocante à interceptação de dados, muito embora a entidade discuta a possibilidade da sua ocorrência, posiciona-se no sentido de que a sua realização é altamente improvável de ocorrer no fundo do mar em razão de questões técnicas (ENISA, 2023, p. 19). Como decorrência lógica desse entendimento, não há recomendações da agência voltadas à proteção e resposta contra esse tipo de ameaça.

5.3.3 Propostas Doutrinárias

A partir de uma analogia com o Direito aplicável às operações cibernéticas, vem ganhando força o entendimento de que operações de interceptação de cabos submarinos podem violar a soberania, mesmo se não chegar a ocorrer o uso da força, com supedâneo no Manual Tallin 2.0. Essa construção teórica vem ganhando notoriedade e sendo utilizada por autores para sustentar que essas práticas de espionagem representam grave violação do Direito Internacional, bem como a necessidade de elaboração de um novo instrumento normativo multilateral, seja por meio de um tratado específico, seja por meio de um protocolo adicional à CNUDM.

Raha e Raju (2021, p. 54) propõem a necessidade de um regime internacional mais especializado e robusto, embora a sua forma possa admitir variações entre uma nova convenção, um protocolo adicional, ou um aprimoramento substancial do regime existente. Embora os autores apresentem considerações sobre aspectos de segurança nacional, o fazem no contexto da integridade física e resiliência operacional dos cabos, não apresentando proposições relevantes acerca da interceptação, escuta ou vigilância dos dados que trafegam no sistema de cabos.

Davenport (2015, p. 90) é enfática ao defender a necessidade de elaboração de um tratado internacional especializado para a proteção dos cabos submarinos, sob o argumento de que o atual regime legal aplicável é um emaranhado de leis com lacunas significativas, e que apenas um regime próprio seria capaz de preencher os vazios normativos e superar as ambiguidades atuais. Sugere que o novo tratado seja suficientemente abrangente para tratar de questões como a definição e previsão da gama de ofensas que podem ser direcionadas à infraestrutura e o estabelecimento de casos especiais de ampliação da jurisdição do Estado que de alguma forma esteja ligado ao ato danoso. Por outro lado, quanto a possibilidade da interceptação ser objeto de tratado internacional, a autora se mostra cética, sob o argumento de que esta prática é envolta em mistérios, sobretudo se for utilizada para realizar vigilância em massa ou em grande escala (Davenport, 2015, p. 109).

Parte relevante da doutrina defende uma interpretação mais moderna e sistemática da CNUDM, sustentando que seus Art. 113 a 115 podem e devem ser lidos à luz das novas ameaças (o que incluiria a interceptação de dados), pois tais riscos não estavam no horizonte de possibilidades do legislador convencional de 1982. Essa interpretação considera que o dever de proteger as infraestruturas de cabos, dada a sua relevância, deve ser exercido de maneira funcionalmente ampliada e compatível com a finalidade da Convenção, sendo desnecessário, portanto, a criação de um regime legal totalmente novo (Heinegg, 2013. p. 310; Shvets, 2020, p. 280).

Seguindo também uma linha de interpretação mais ampliativa e teleológica⁸⁴ da CNUDM, há ainda o entendimento segundo o qual seria possível a adoção de medidas contra embarcações estrangeiras sem o consentimento do Estado da bandeira, caso este deixe de cumprir com as suas obrigações previstas no Art. 113, pois em assim agindo estaria se escondendo atrás do véu da jurisdição exclusiva do estado de bandeira e, portanto, abusando de seus direitos, o que legitimaria eventual atuação mais coercitiva do Estado costeiro (Pedrozo, 2025, p. 63).

Em síntese, os entendimentos doutrinários contemporâneos convergem no sentido de que o regime jurídico vigente é insuficiente para enfrentar os desafios a que estão submetidos os cabos submarinos. Entretanto, não há um consenso sobre como solucionar esse problema, com proposições que vão desde a necessidade de realização de interpretação

⁸⁴ Interpretação teleológica é um método de interpretação das normas no qual o intérprete busca alcançar o sentido e a finalidade das mesmas, com foco em compreender qual era o objetivo social, jurídico ou político do legislador ao elaborá-las, ao invés do mero sentido literal, com a finalidade de adaptar as leis às necessidades sociais atuais e garantir que ela cumpra o seu propósito.

evolutiva da CNUDM, sem a necessidade de alteração substancial do seu texto, até a edição de um tratado internacional específico com vistas a inaugurar um novo regime.

5.4 MODALIDADES DE REGULAÇÃO INTERNACIONAL POSSÍVEIS

A discussão desenvolvida nas seções anteriores evidencia que dificilmente o *deficit* normativo sobre a segurança dos cabos submarinos, em especial quanto à proibição da interceptação de dados, será resolvido por intermédio de um único caminho regulatório. Ao contrário, a possibilidade mais realista é aquela que aponta no sentido do desenvolvimento de um arcabouço progressivo e em diversos níveis, na qual diferentes tipos de regulação internacional podem coexistir e se complementar. Isso posto, três possibilidades merecem uma análise mais detida, sendo elas os mecanismos de *soft law*, tratados de caráter regional e a adoção de um tratado internacional multilateral.

5.4.1 Soft Law

Como é possível inferir da análise das seções anteriores, os mecanismos de *soft law* se apresentam como a via mais pragmática e viável no curto prazo. Diretrizes, recomendações, guias de boas práticas e declarações interpretativas representam instrumentos que já são amplamente adotados com a finalidade de estabelecer padrões desejáveis de comportamento pelos *stakeholders*. Ainda que desprovidos de força vinculante, tais iniciativas demonstram que é possível estabelecer um regramento normativo que contribua para o bom funcionamento do sistema e para a redução das ameaças, inclusive aquelas voltadas para a interceptação.

Acordos setoriais entre partes diretamente interessadas podem funcionar como laboratórios normativos, que poderiam estabelecer compromissos específicos de não interceptação (em que pese certa limitação de alcance e abrangência), com potencial para evoluir para a formação de práticas consolidadas e futuras negociações de acordos formais. Como desvantagens, tais mecanismos dependem da adoção voluntária das partes e carecem de instrumentos formais de responsabilização em caso de descumprimento dos seus termos (Oliveira; Bertoldi, 2010, p. 6278)

5.4.2 Tratados Regionais

A elaboração de tratados regionais representa uma segunda via de possibilidade relevante, sobretudo em espaços que já gozam de certa densidade normativa e institucional aptos a desenvolver temas complexos como o que aqui é abordado. A título de exemplo, na esfera da União Europeia, onde já está consolidada a preocupação com as infraestruturas críticas, cibersegurança e soberania digital, existe um ambiente que teoricamente seria mais favorável ao desenvolvimento de iniciativas para a celebração de um tratado voltado especificamente (ou ao menos que incluam) a proteção dos cabos submarinos. Enquanto entidade detentora de personalidade jurídica, a UE possui competência para concluir diretamente tratados internacionais sobre a maioria das matérias mediante um procedimento mais simplificado e ágil. Até mesmo para tratados celebrados no âmbito da política externa e segurança comum, em que há um regime legal especial e um procedimento diferente, a capacidade de celebrar tratados diretamente pela UE enquanto detentora de personalidade jurídica sem dúvidas é um ponto de grande relevância, uma vez que não é necessária a presença ou o consenso unânime de todos os seus integrantes (Ceia, 2011, p. 173).

Quanto ao Mercado Comum do Sul (MERCOSUL), é bem verdade que o seu nível de institucionalização é menor quando comparado à UE, o que importa em diferenças essenciais quanto à facilidade de celebração de tratados internacionais. Enquanto no bloco europeu existe uma ordem jurídica comunitária supranacional, no sul-americano vigora a soberania dos Estados-membros. Como resultante, há a necessidade de consenso nas tomadas de decisão e ainda na internalização por cada membro das decisões tomadas para que possam produzir efeitos nos respectivos ordenamentos jurídicos internos, o que torna o processo de conclusão de tratados mais dificultoso (Silva, 2019, p. 20). Sem ignorar esse fato, a temática da segurança dos cabos submarinos poderia ser incorporada nos debates do MERCOSUL, considerando que a via regional confere uma maior possibilidade de homogeneidade normativa e maior grau de comprometimento entre as partes.

Considerando que a referência aos blocos europeu e sul-americano tem uma função meramente ilustrativa de demonstrar a viabilidade jurídica e política da adoção de tratados regionais, entendemos ser desnecessário uma abordagem de outros blocos regionais, não objetivando a presente seção realizar um estudo comparado entre eles.

5.4.3 Tratado Multilateral Global

Sem dúvidas a proposta mais abrangente e a melhor maneira de conferir uniformidade no trato das questões afetas a segurança dos cabos submarinos seria mediante a adoção de uma convenção multilateral. Diferentemente dos mecanismos de *soft law* e dos tratados regionais, uma convenção multilateral poderia estabelecer normas claras e uniformes sobre interceptação, incluindo obrigações de cooperação, notificação de incidentes, responsabilização e outras. Como visto no capítulo anterior, o quadro jurídico existente no Direito Internacional do Mar, conforme tradicionalmente compreendido, não fornece aos Estados costeiros autoridade suficiente para combater eficazmente novas ameaças para além do seu mar territorial (Schaller, 2025, p. 182).

Autores como Davenport (2015) e Sunak (2017) sustentam que apenas uma convenção internacional clara poderia superar as deficiências existentes no regime da CNUDM no que tange a uma proteção mais abrangente dos cabos. No mesmo sentido, Petty (2021, p. 268) entende que a comunidade internacional está se aproximando de um ponto crucial ou de uma mudança significativa na forma como lidar com *hacking* de cabos submarinos, com os Estados se movendo em direção à criação de acordos formais e vinculativos.

Contudo, não se ignora que o caminho para se chegar a um tratado internacional tão abrangente quanto o desejável é muito difícil, particularmente no que se refere a eventuais disposições sobre a interceptação de dados, tradicionalmente tratada como um aspecto sensível de segurança nacional pelas grandes potências, fato que pode acabar por inviabilizar as negociações e a assunção de compromissos vinculantes que importem na aceitação de regras proibitivas sobre a espionagem (Lubin, 2015, p. 23).

De tal maneira, é mais provável que a regulação internacional sobre a interceptação em cabos submarinos evolua, como já vem ocorrendo para outros aspectos, de maneira gradativa por meio de instrumentos de *soft law* e arranjos regionais e setoriais e com o passar do tempo sejam criadas condições para a discussão de acordos multilaterais mais abrangentes.

5.5 CONTEÚDO DESEJÁVEL DE UM REGIME NORMATIVO INTERNACIONAL SOBRE INTERCEPTAÇÃO DE DADOS

A elaboração de eventual instrumento normativo com o escopo de normatizar especificamente a interceptação de dados em cabos submarinos, independentemente da forma que será utilizada (*soft law*, tratados regionais ou até mesmo um tratado de abrangência global), necessita da definição de parâmetros mínimos que sejam capazes de preencher as lacunas identificadas no regime jurídico vigente. Nesse sentido, Davenport (2015, p. 90) sustenta que a proteção dos cabos deve ultrapassar a dimensão exclusivamente física e incorporar também a dimensão informacional, argumentando que qualquer iniciativa regulatória eficaz deve articular proibições claras de condutas ilícitas em tempo de paz, mecanismos de responsabilização, dever de cooperação entre os Estados, sob pena de manter a fragmentação atualmente vigente.

5.5.1 Proibição de Interceptação em Tempo de Paz

Conforme tratado no capítulo 2, a interceptação de dados enquanto técnica de espionagem possui regulamentação suficiente no Direito Internacional para os tempos de guerra. Entretanto, a mesma tutela não é conferida para os tempos de paz, em que pese tal prática representar uma potencial violação a princípios básicos do Direito Internacional. Esse vácuo normativo, decorrente da falta de proibição expressa da interceptação no Direito Internacional, expõe Estados e indivíduos a riscos de violação da soberania e de direitos individuais, o que faz com que sejam buscadas soluções em outros diplomas esparsos e em interpretações evolutivas, o que gera certo grau de insegurança jurídica.

Princípios basilares do Direito Internacional como a soberania e a não intervenção preconizam que nenhum Estado deve interferir nos assuntos internos de outro, o que inclui práticas de espionagem mediante a interceptação de dados em cabos submarinos. Portanto, se por um lado essa ausência de um mandamento de proibição geral à espionagem em tempos de paz suscita uma possível permissibilidade, por outro estabelece uma ambiguidade indesejada no Direito Internacional (Sun, 2025, p. 239), o que, por si só, justifica a necessidade de disposição explícita da sua vedação, estabelecendo salvaguardas para a soberania estatal e direitos fundamentais das pessoas.

5.5.2 Diretrizes para Cooperação

A efetividade de um instrumento internacional sobre o tema não dependerá somente da definição de condutas proibidas, mas também da criação de mecanismos claros de cooperação entre os Estados. A título de exemplo, a Convenção das Nações Unidas contra o Crime Cibernético estabeleceu um mecanismo de cooperação judicial e técnica entre os Estados mediante a criação de um canal global de assistência mútua para enfrentar delitos transnacionais que utilizam a internet como plataforma, evidenciando que a cooperação sistemática e a troca de informações são instrumentos relevantes para lidar com ameaças transfronteiriças (ONU, 2024).

No contexto específico de atividades que eventualmente tenham a sua legitimidade questionada, como operações militares⁸⁵ ou interceptação autorizada na ZEE, diretrizes de notificação preventiva poderiam reduzir tensões e evitar a escalada de conflitos entre os Estados. A literatura de Direito Internacional aplicável ao ciberespaço, como aquela proveniente dos fóruns da ONU sobre comportamento estatal – GGE e OEWG – reforça a ideia de que a cooperação e a transparência contribuem para a previsibilidade e confiança mútua.

5.5.3 Criminalização e Exercício de Jurisdição

O modelo de tratados internacionais que versam sobre delitos transnacionais, como por exemplo as convenções contra o terrorismo, demonstra que a exigência de criminalização interna é um mecanismo consolidado com vistas a assegurar a implementação efetiva do que é pactuado (Davenport, 2015, p. 90). Sendo assim, esse padrão normativo indica que os países que aderirem a esse instrumento deverão buscar incluir as condutas nele definidas no seu ordenamento jurídico interno mediante a criação ou adaptação das suas disposições, estabelecendo penas proporcionais à gravidade do ato praticado. A ausência de tipificação penal específica no arcabouço jurídico interno é um entrave à devida persecução e

⁸⁵ Alguns Estados interpretam a CNUDM como permissiva à operação das suas marinhas na ZEE de outros Estados da mesma forma como em alto-mar. Por sua vez, alguns Estados costeiros, dentre eles o Brasil, declararam que as disposições da Convenção não autorizam outros Estados a realizarem atividades e exercícios militares na sua ZEE sem o seu consentimento, especialmente se envolver o emprego de armas e explosivos (Sun, 2025, p. 210)

punição de agentes que violem as normas do Direito Internacional, mesmo que haja tipificação na lei internacional e até mesmo previsão de jurisdição universal.⁸⁶

Além disso, o instrumento deverá prever a obrigatoriedade do exercício da jurisdição quando os infratores cometerem os delitos nele previstos, desde que, obviamente haja essa possibilidade segundo as disposições da CNUDM, ou seja, quando cometidos no mar territorial, ou por seu nacional ou por navios que arvoem a sua bandeira. Isso objetiva garantir que os perpetradores das ofensas não fiquem impunes, mesmo que os atos tenham sido cometidos em local que não esteja submetido à jurisdição exclusiva de um único Estado.

Ainda quanto ao exercício da jurisdição, é desejável que haja previsão da possibilidade de extradição, quando se tratar de cometimento do delito por estrangeiro no mar territorial de outro Estado e este optar por não julgar, desde que o Estado de nacionalidade do infrator seja parte do instrumento e se comprometa a exercer a sua jurisdição (Davenport, 2015, p. 90).

5.5.4 Responsabilização Estatal e Mecanismos de Reparação

A responsabilidade internacional de um Estado e o consequente direito à reparação de outro surgem do descumprimento de uma obrigação internacional ou da violação das suas normas, sendo necessário a presença de dois elementos: uma conduta (ação ou omissão) de um Estado e que essa conduta configure um ato internacionalmente ilícito. Diferentemente do que ocorre com muitos direitos internos, inclusive no Brasil, o dano não é considerado um elemento essencial para configurar um ato ilícito internacional nem para gerar responsabilidade, de modo que a necessidade ou não do dano para o estabelecimento da responsabilidade dependerá do conteúdo específico da norma internacional que foi violada (Andrade, 2007, p. 8). Tal questão é relevante na medida em que a efetiva ocorrência do dano em atos de interceptação de dados não seria de fácil comprovação, haja vista que recairia sobre institutos jurídicos intangíveis.⁸⁷

A constatação da responsabilidade internacional implica a obrigação de reparar os danos causados, eliminando todas as consequências do ato ilegal e restabelecer a situação que existiria caso o ato não tivesse ocorrido, incluindo também o dever de investigar, processar e

⁸⁶ Conforme ensina Zanella ao discorrer sobre o delito de pirataria, sujeito à jurisdição universal (2023, p. 94), de nada adianta efetuar a prisão se no ordenamento jurídico interno não houver previsão legal do delito.

⁸⁷ Bens jurídicos intangíveis ou imateriais ou incorpóreos são aqueles que não possuem existência física ou material, mas que possuem valor jurídico e/ou econômico, como por exemplo a privacidade, soberania, patentes, pesquisas científicas etc.

julgar os responsáveis pelas violações (Ramos, 2005, p. 54 e 57). Ocorre que restabelecer o *status quo ante*⁸⁸ decorrente de um ato ilícito de interceptação de dados ao que parece é inviável, considerando que a obtenção e o proveito de informações sensíveis acabam por exaurir essa possibilidade, de modo que a questão se resolveria apenas no campo da reparação econômica.

Na seara do Direito Internacional dos Direitos Humanos, violação a direitos instituídos como *jus cogens*⁸⁹, como por exemplo os instituídos no Pacto Internacional sobre Direitos Civis e Políticos (ONU, 1969), são passíveis de gerar responsabilização estatal com fundamento no Projeto de Artigos sobre Responsabilidade Internacional dos Estados por Ato Internacionalmente Ilícito de 2001, que ainda não está em vigor como tratado internacional, mas é amplamente aceito e utilizado como Direito Consuetudinário (Andrade, 2007, p. 7). Nessa voga, seria recomendável previsão estabelecendo que Estados que conduzam, permitam ou consintam interceptações ilegais respondam por tais atos em face de Estados, corporações ou pessoas.

A maneira pela qual a responsabilização poderá ser levada a efeito também é cláusula desejável a ser prevista no instrumento, prevendo dispositivos sobre mecanismos de solução de controvérsias, que não implicaria um regime penal típico⁹⁰, mas poderia se dar por intermédio de negociações, arbitragem ou julgamento por tribunais internacionais. Considerando a disposição dos cabos submarinos no leito marino, em que pese a possibilidade de instituição de mecanismos próprios de solução de controvérsias nesse instrumento, talvez o mais viável seja a utilização dos mecanismos de solução de controvérsias presentes no Capítulo XV da CNUDM. A Convenção de Montego Bay estabelece um sistema com uma variedade de procedimentos postos à escolha dos Estados para que possam resolver suas disputas pacificamente, incluindo a possibilidade de conciliação, a submissão de disputas ao Tribunal Internacional do Direito do Mar, à Corte Internacional de Justiça, ou à arbitragem *ad*

⁸⁸ Expressão em latim costumeiramente utilizada em Direito que significa “o estado em que as coisas se encontravam antes”.

⁸⁹ *Jus cogens* é definido pelo Art. 53 da Convenção de Viena sobre o Direito dos Tratados como “uma norma aceita e reconhecida pela comunidade Internacional dos Estados como um todo como uma norma da qual nenhuma derrogação é permitida, e que só pode ser modificada por norma ulterior de direito internacional geral da mesma natureza”.

⁹⁰ Apesar de não ser o escopo do presente trabalho, deve ser ressaltado que não se ignora neste ponto que apenas os crimes de genocídio, contra a humanidade, de guerra e de agressão são objetos de jurisdição do Tribunal Penal Internacional, conforme previsto no Estatuto de Roma, razão pela qual não se está a sugerir eventual atuação do TPI nos casos de interceptação. Na verdade, apenas não ignoramos também a controvérsia sobre a dualidade existente entre o chamado Direito Penal Internacional e o direito internacional penal. Enquanto o primeiro se ocupa do conflito espacial de leis penais, da extradição e da eficácia da sentença penal estrangeira, o segundo trata do direito penal de abrangência internacional, ou seja, da proteção penal do direito internacional, representando uma extensão do Direito Internacional Público (Zilli, 2012).

hoc, razão pela qual entendemos ser mais viável a sua adoção por ser tratar de um sistema já consolidado (Zanella, 2025, c. 41).

5.5.5 Disposição Expressa da Violação de Direitos Humanos

É desejável que o instrumento utilizado, seja ele vinculante ou não, reconheça expressamente que a interceptação ilícita de dados em cabos submarinos configuraria violação a Direitos Humanos internacionalmente protegidos, em especial o direito à privacidade, proteção de dados pessoais, liberdade de expressão e ao sigilo das comunicações. Essa qualificação não tem apenas finalidade simbólica, mas projeta a tutela pretendida para o campo de regimes jurídicos dotados de maior densidade institucional e de mecanismos mais sólidos de proteção, como ocorre no sistema internacional de proteção dos Direitos Humanos.

Este posicionamento se encontra alinhado com a jurisprudência e os documentos interpretativos dos principais sistemas de proteção dos Direitos Humanos. Para exemplificar, o Comitê de Direitos Humanos das Nações Unidas interpretou que o Art. 17 do Pacto Internacional sobre Direitos Civis e Políticos entendeu que qualquer forma de vigilância ou interceptação de comunicações deve observar critérios estritos de legalidade, necessidade e proporcionalidade, sendo incompatível com o tratado as interceptações arbitrárias ou secretas sem base legal (ONU, 1988).

A inclusão de previsão expressa nesse sentido produziria efeitos jurídicos importantes, pois não deixaria dúvidas a respeito da possibilidade do acionamento de mecanismos internacionais já existentes sempre que interceptações configurassem violações de direitos fundamentais. Além disso, serviria como fator de desestímulo a práticas ilegais de interceptação, reforçando a obrigação dos Estados em implementar no seu arcabouço interno medidas de controle nessa direção. Por conseguinte, a proteção dos cabos deixaria de ser compreendida apenas como uma questão de infraestrutura e soberania, passando a integrar também o escopo dos direitos fundamentais.

5.6 CONSIDERAÇÕES PARCIAIS

O presente capítulo buscou analisar o problema normativo identificado ao longo da dissertação, qual seja, a inexistência de um regime jurídico internacional claro, específico e abrangente sobre a segurança dos cabos submarinos, em especial sobre a interceptação de dados nesses ativos.

A partir do diagnóstico proveniente dos capítulos anteriores – o Direito Internacional tutela prioritariamente a dimensão física da infraestrutura de cabos submarinos, havendo um vácuo normativo a respeito do seu conteúdo de dados – foram examinadas as consequências desse vácuo legal, as principais propostas doutrinárias e institucionais existentes, as medidas de regulação possíveis e, por fim, apresentados alguns elementos normativos que poderiam compor um instrumento internacional que seja eficaz e que possa preencher essa lacuna.

Demonstrou-se que a ausência de regulação não espelha mera deficiência teórica, por outro lado, tem potencial para produzir efeitos concretos relevantes como insegurança jurídica, vulnerabilidade à soberania estatal, potencializa riscos à segurança das comunicações e à proteção de direitos fundamentais, especialmente à privacidade. Em razão da ausência de proibição expressa no Direito Internacional, viu-se que a interceptação em tempo de paz situa-se em zona cinzenta, que apesar de ser relativamente tolerada, representa também um problema sob a ótica jurídica internacional.

O exame das propostas doutrinárias e institucionais comprovou que já existe na literatura especializada fóruns técnicos e regulatórios, o que evidencia a percepção da necessidade de evolução normativa. Instituições como o ICPC, ENISA e setores da comunidade acadêmica nacional e internacional vêm apontando, ainda que sob óticas distintas, a insuficiência do regime atual e a necessidade de mecanismos mais claros de proteção. Entretanto, ficou também evidenciado que as iniciativas que surgem como solução para as deficiências do atual regime são da mesma forma fragmentadas e insuficientes, ocupando-se primordialmente da dimensão física dos cabos e sob a forma de *soft law*.

Os instrumentos comumente mais utilizados para regulação — *soft law*, tratado regional e tratado multilateral global — foram apresentados como possibilidades, revelando-se que cada modelo apresenta vantagens e limitações.

Os instrumentos de *soft law* oferecem flexibilidade e maior viabilidade política, mas carecem de força vinculante, dependendo da boa-fé das partes, o que pode levar a sua ineficácia.

Por sua vez, tratados regionais podem alcançar uma maior densidade normativa, porém possuem a desvantagem da limitação geográfica em se tratando de proteger ativos que são transoceânicos.

Já um tratado multilateral global teria potencial para oferecer coerência sistêmica e uniformidade de tratamento, porém enfrentaria grandes entraves diplomáticos e geopolíticos durante o seu processo de discussão e aprovação.

Esse cenário expõe que a construção de um instrumento internacional que verse sobre interceptação de dados em cabos submarinos exigirá não apenas elaboração jurídica apurada, mas também o avanço e o amadurecimento na discussão sobre espionagem em tempos de paz e sobretudo vontade política e coordenação institucional.

Não obstante o modelo normativo a ser adotado, foi apresentado que certos conteúdos materiais são essenciais para a sua efetividade, como a definição da proibição expressa da interceptação em tempo de paz, diretrizes de notificação e cooperação estatal, obrigações quanto a criminalização interna e ao exercício de jurisdição pelos Estados, mecanismos de reparação e solução de controvérsias e a incorporação explícita de parâmetros de Direitos Humanos. É de se destacar que esses elementos não representam inovação, mas apenas a sua sistematização e a aplicação normativa neste campo, eis que já presentes e amplamente consagrados no Direito Internacional.

6 INTERCEPTAÇÃO EM ÁGUAS JURISDICIONAIS BRASILEIRAS: DESAFIOS E COMPETÊNCIAS DO ESTADO BRASILEIRO

6.1 CONSIDERAÇÕES INICIAIS

O protagonismo dos cabos submarinos no perfeito funcionamento das comunicações mundiais impõe deveres e responsabilidades para os Estados costeiros signatários da CNUDM como visto no capítulo anterior. É bem verdade que a Convenção ao estabelecer tais encargos tinha em vista a dimensão física, mas também é verdadeiro que a proteção dessas infraestruturas contra atividades de interceptação é igualmente relevante.

No caso do Brasil, privilegiado com um extenso litoral⁹¹, a Zona Econômica Exclusiva e a Plataforma Continental recebem importantes rotas de cabos de fibra ótica, fato que impõe dificuldades particulares, na medida em que se faz necessário conciliar aspectos fundamentais das relações internacionais, dentre os quais podemos citar a soberania, liberdade de navegação, obrigações decorrentes do Direito do Mar e outros, tudo isso em espaços marítimos com jurisdição limitada (Vichi; Pinto; Sá, 2020, p. 338).

Tendo como baliza as lacunas jurídicas do arcabouço jurídico internacional identificadas no capítulo anterior, este capítulo será dedicado a apreciar as competências, limites e responsabilidades do Estado Brasileiro diante de eventuais práticas de interceptação de dados na Águas Jurisdicionais Brasileiras. Como apontado, a CNUDM é adotada como marco normativo principal para estudo do assunto, estabelecendo os diversos espaços marítimos e as respectivas jurisdições dos Estados, ainda que sem dispor especificamente sobre o conteúdo de dados que trafegam pelos cabos.

Para além da CNUDM, o capítulo explorará o arcabouço jurídico interno brasileiro aplicável aos cabos submarinos, incluindo normas sobre defesa nacional, políticas públicas e instrumentos normativos diversos que, embora não tenham sido concebidos especificamente com foco nesse sistema, podem ser empregados complementarmente. Desta forma, busca-se perceber até que ponto o ordenamento jurídico brasileiro é capaz de oferecer respostas às ameaças associadas à interceptação de dados nos cabos submarinos, bem como os riscos jurídicos decorrentes de uma atuação estatal excessiva ou, por outro lado, omissa.

Ao término, o capítulo pretende conferir uma perfeita compreensão do atual *status* normativo nacional afeto à proteção dessa infraestrutura crítica, proteção essa que deve estar

⁹¹ O litoral brasileiro tem 7.367 quilômetros de extensão, conforme dados do Atlas Geográfico Escolar do Ensino Fundamental (IBGE, 2015).

assentada na busca por um delicado equilíbrio entre a tutela da soberania informacional e o respeito às liberdades consagradas pelo Direito do Mar.

6.2 ÁGUAS JURISDICIONAIS BRASILEIRAS

Como aspecto inicial do presente capítulo, é necessário explicar que a delimitação geográfica desta pesquisa cingiu-se às Águas Jurisdicionais Brasileiras (AJB) pois somente nos espaços marítimos sobre os quais o Brasil exerce alguma jurisdição será possível analisar de forma consistente se o país está desempenhando (ou tem condições de desempenhar) de maneira adequada as suas competências relacionadas à segurança dos cabos submarinos e à repressão das práticas de interceptação de dados.

O conceito de AJB é estabelecido pela Instrução Normativa nº 3/MB/MD, não se tratando, portanto, de conceituação proveniente de texto de lei, mas sim de ato normativo de natureza administrativa da lavra do Comandante da Marinha, no exercício das suas atribuições de Autoridade Marítima⁹², que resolveu:

Art. 1º Estabelecer, perante a Marinha do Brasil, o seguinte conceito: as “Águas Jurisdicionais Brasileiras (AJB)” compreendem as águas interiores e os espaços marítimos, nos quais o Brasil **exerce jurisdição, em algum grau**, sobre atividades, pessoas, instalações, embarcações e recursos naturais vivos e não-vivos, encontrados na massa líquida, no leito ou no subsolo marinho, para os fins de controle e fiscalização, dentro dos limites da legislação internacional e nacional. Esses espaços marítimos compreendem a faixa de 200 milhas marítimas contadas a partir das linhas de base, **acrescida das águas sobrejacentes à extensão da Plataforma Continental além das 200 milhas marítimas**, onde ela ocorrer. (Brasil, 2022b, grifo próprio).

A Marinha do Brasil (MB) possui como atribuições subsidiárias particulares contribuir para a formulação de políticas afetas ao mar⁹³, bem como implementar e fiscalizar o cumprimento de leis e regulamentos neste espaço geográfico⁹⁴, atribuições estas diretamente relacionadas com o escopo do presente trabalho, constatando-se que a MB participa como importante ator nas questões afetas à segurança dos cabos submarinos.

Essa constatação ganha relevância quando se considera que, para a referida Força Naval, o Brasil exerce jurisdição sobre as águas sobrejacentes à extensão da Plataforma

⁹² A designação do Comandante da Marinha como Autoridade Marítima está prevista no parágrafo único do art. 17 da Lei Complementar nº 97/1999 e seu objetivo foi atribuir competência àquela autoridade militar para tratar das atribuições subsidiárias particulares conferidas à Marinha do Brasil.

⁹³ Inciso III, Art. 17, Lei Complementar nº 97/1999.

⁹⁴ Inciso IV, Art. 17, Lei Complementar nº 97/1999.

Continental além das 200 milhas marítimas, nascendo deste ponto uma controvérsia no âmbito do Direito do Mar, haja vista que o exercício de jurisdição reconhecido pela Autoridade Marítima estaria, em tese, extrapolando os limites do regime jurídico da Plataforma Continental estabelecido pela CNUDM, que confere ao Estado costeiro o exercício de direitos de soberania para fins de exploração e aproveitamento dos seus recursos naturais⁹⁵, recursos estes localizados no leito do mar e no subsolo⁹⁶, consequentemente não afetando o regime jurídico das águas sobrejacentes⁹⁷.

Para Zanella (2018, p. 2854) o conceito de AJB estabelecido por meio de norma infralegal que submete à jurisdição brasileira a coluna d'água sobrejacente à extensão da Plataforma Continental além das 200 milhas marítimas é incompatível com o Direito do Mar, pois essas águas têm natureza jurídica de alto-mar, não podendo ser submetidas à jurisdição nacional. O autor enfatiza que a CNUDM distingue claramente o regime do leito e do subsolo do regime da coluna d'água, de modo que, no seu entendimento, houve uma confusão na redação da Instrução Normativa nº 3/MB/MD em separar os regimes dos fundos marinhos da coluna d'água, uma vez que os direitos exclusivos do Estado costeiro recaem apenas sobre o primeiro regime, não incluindo o segundo, e que entender de modo diverso poderia representar tentativa de apropriação indevida do alto-mar passível de responsabilização internacional.

Por outro lado, Barretto (2024, p. 41) entende que o conceito de AJB estabelecido pela norma interna é compatível com o Direito do Mar, devendo ser interpretada conforme os limites e obrigações estabelecidos pela CNUDM como uma ferramenta operacional interna para exercer controle e fiscalização sobre espaços marítimos onde o Brasil já detém direitos ou jurisdição, e não como um meio de apropriação do alto-mar.

A despeito da relevância dessa discussão para diversos temas afetos aos Estudos do Mar, maiores considerações sobre o debate não se mostram necessários ao prosseguimento do trabalho. Isso porque, independentemente da possibilidade ou não de o Brasil exercer jurisdição sobre a coluna d'água sobrejacente à extensão da Plataforma Continental além das 200 milhas ou quaisquer outras ambiguidades conceituais, fato é que os cabos submarinos encontram-se assentados sobre o seu leito, razão pela qual estão submetidos à jurisdição funcional do Estado costeiro, nos termos do Art. 77 da CNUDM. Assim, considerando que o objeto deste trabalho é a interceptação de dados que trafegam por cabos fisicamente dispostos

⁹⁵ Art. 77 (1), CNUDM.

⁹⁶ Art. 77 (4), CNUDM.

⁹⁷ Art. 78 (1), CNUDM.

sobre o solo marinho, a análise prescinde de um exame mais aprofundado dessas controvérsias atinentes à Plataforma Continental estendida, motivo pelo qual contentamo-nos com esta breve exposição.

6.3 O EXERCÍCIO DA JURISDIÇÃO NOS DIVERSOS ESPAÇOS MARÍTIMOS

A análise da interceptação de dados em cabos submarinos nas Águas sob Jurisdição Brasileira exige, como ponto de partida, a delimitação dos poderes que o Brasil exerce sobre os diferentes espaços marítimos. Como apresentado no capítulo anterior⁹⁸, a CNUDM estabelece regimes jurídicos distintos para o mar territorial, ZEE, e Plataforma Continental, atribuindo ao Estado costeiro graus diferentes de soberania, direitos soberanos e competências funcionais, os quais condicionam diretamente a possibilidade de adoção de medidas voltadas à proteção da infraestrutura de cabos, sejam elas medidas legislativas, normativas ou administrativas.

Sem adentrar profundamente em aspectos teóricos próprios da ciência jurídica, é necessário, ainda que de maneira bem simples, conceituar o que seria, então, jurisdição. Nas palavras de Gonçalves (2012, p. 54), jurisdição é a “função do Estado, pela qual ele, no intuito de solucionar os conflitos de interesse em caráter coativo, aplica a lei geral e abstrata aos casos concretos que lhe são submetidos.” Já Bueno (2019, p. 117), sustenta que a jurisdição vai além da mera conceituação mais clássica de “dizer o direito”, refutando a figura do juiz como mera “boca da lei”, afirmando que “[...] cabe ao Estado-juiz concretizá-lo no sentido de realizá-lo concretamente [...]”. Além das funções tipicamente jurisdicionais de dizer e aplicar o direito, Moura (1991, p. 144, *apud* Martins, 2008, p. 79) expõe que jurisdição “[...] é o termo empregado algumas vezes para designar o espaço submetido à autoridade de um Estado (como por exemplo, a jurisdição sobre as águas territoriais) [...]”

Assim, de maneira bem simples, como dito acima, podemos compreender que jurisdição é a capacidade de dizer qual é o Direito aplicável e de aplicá-lo aos casos concretos em determinado espaço geográfico. Essa capacidade está intrinsecamente vinculada à ideia de soberania, estando nela circunscrita, pois jurisdição é manifestação da soberania e só existe em razão dela. Ocorre que o exercício da soberania no mar é dificultado pelas peculiaridades próprias do Direito do Mar, tendo em vista que um dos seus pilares de sustentação é a

⁹⁸ Ver Seção 3.2.

soberania do Estado de Bandeira, a quem cabe, via de regra, o exercício da jurisdição sobre os atos praticados a bordo de seus navios (Beirão, 2023, p. 131).

Isso posto, torna-se indispensável examinar, de forma sistemática, o alcance dos poderes estatais em cada espaço marítimo, especialmente no que se refere à regulação e fiscalização da atuação de outros atores nessas áreas, com vistas a compreender se é possível (e em que medida) a atuação do Brasil voltada à restrição das atividades de coleta de dados realizadas através da interceptação de cabos submarinos. Devido ao escopo do presente estudo, não serão considerados os limites da atuação estatal nas águas interiores das AJB, tendo em vista que são parte do território nacional e sobre elas não incidem as limitações à soberania próprias do Direito Internacional do Mar.

6.3.1 No Mar Territorial

Conforme estabelecido pela CNUDM, a soberania do Estado costeiro se estende além do seu território até os limites do seu mar territorial⁹⁹. Para Menezes (2015, p. 94), a Convenção “[...] reconhece a jurisdição absoluta do Estado sobre o mar territorial, mas em razão de ser um espaço dinâmico de inter-relações, cuidou de resguardar certas garantias e imunidades que são aplicadas para embarcações, pessoas e outros Estados”. Ou seja, a jurisdição do Estado costeiro, em que pese ser absoluta, é circunstancialmente condicionada por alguns princípios do Direito do Mar.

Logo, a regra geral é que o Estado costeiro pode elaborar e aplicar normas a respeito de qualquer assunto que diga respeito ao mar territorial estando, obviamente, a temática dos cabos submarinos inserida nesses assuntos. Contudo, essa liberdade de disposição de matérias no mar territorial apesar de ampla não é irrestrita, pois deve obedecer sempre às balizas estabelecidas pelo Direito Internacional (Zanella, 2023, p. 23).

A delimitação dos poderes e competências do Estado costeiro no mar territorial demanda o estudo de dois institutos basilares do Direito do Mar previstos na CNUDM. De um lado, o direito de passagem inocente representa uma limitação à soberania do Estado ribeirinho, privilegiando a liberdade dos mares, que é tido como o principal interesse da comunidade internacional (Mello Filho; Guedes, 2017, p. 273). De outro, a jurisdição do Estado de bandeira, que também representa uma mitigação da soberania do Estado costeiro e tem sua origem no costume e na prática internacionais, representa um instituto relevante

⁹⁹ Art. 2º (1), CNUDM.

quando se trata de condutas potencialmente ilícitas cometidas a bordo de navios estrangeiros que, via de regra, exercerão suas jurisdições sobre tais condutas, salvo em casos específicos previstos expressamente em tratados internacionais (Zanella, 2025, p. 85).

A análise combinada desses dois institutos permitirá compreender o necessário equilíbrio estabelecido pelo Direito do Mar entre as liberdades da navegação e o exercício da soberania no mar territorial pelo Estado costeiro, em especial no que concerne à segurança da infraestrutura de cabos submarinos.

6.3.1.1 *Passagem Inocente*

Especificamente quanto ao instituto da passagem inocente, Martins (2008, p. 58) aponta que a CNUDM fez previsão particular referente a possibilidade (e não obrigatoriedade) de adoção de leis e regulamentos pelo Estado costeiro¹⁰⁰, condicionando o exercício deste direito pelos navios estrangeiros que passem pelo mar territorial com a finalidade de proteção dos cabos submarinos. Sendo assim, opinamos no sentido de que a edição de normatização brasileira voltada à repressão da interceptação de dados que trafegam por estas infraestruturas estaria em consonância com o Direito do Mar, haja vista que inserta nos poderes jurisdicionais conferidos pela Convenção de Montego Bay aos Estados costeiros.

Este entendimento decorre da interpretação do próprio conceito de passagem inocente, uma vez que, para ser assim caracterizada (inocente), não pode estar relacionada com nenhuma outra atividade senão a própria passagem¹⁰¹, sendo forçoso reconhecer que eventual navio estrangeiro, seja de guerra ou não, que ao passar pelo mar territorial brasileiro se envolva com atividades de interceptação de cabo submarino estará, portanto, agindo em prejuízo à paz e/ou boa ordem e/ou segurança nacional, a depender da forma de atuação do agente interceptador¹⁰².

¹⁰⁰ Art. 21, CNUDM.

¹⁰¹ O Art. 19 (2) da CNUDM elenca um rol de atividades que são consideradas proibidas durante a passagem pelo mar territorial e que retiram o seu caráter de inocente, as quais poderiam todas ser suprimidas a exceção da última, sendo suficiente apenas a disposição contida na alínea “I” para a manutenção da tutela pretendida.

¹⁰² Os elementos essenciais da passagem inocente são a paz, boa ordem e segurança do Estado costeiro. O primeiro relaciona-se à proibição do uso da força, enquanto o segundo com a preservação das leis e regulamentos do Estado costeiro e o terceiro com a segurança em qualquer de suas vertentes, ou seja, militar, econômica, ambiental, digital ou outra. Atuando o agente em prejuízo de qualquer desses elementos, a passagem se caracteriza como prejudicial (Zanella, 2023, p. 29).

Deve ser ressaltado que tais atividades de operação cibernética no mar territorial não precisam ser necessariamente dirigidas contra o Estado costeiro, sendo consideradas ilegais mesmo se tiverem como alvo um outro Estado qualquer, pois tal fato teria potencial para prejudicar a ordem pública, descaracterizando, assim, a passagem como inocente. Nesse sentido é o entendimento da maioria dos especialistas que elaboraram o Manual Tallin 2.0 no que diz respeito às operações cibernéticas em geral:

Os especialistas também discutiram a questão da realização de operações cibernéticas direcionadas a terceiros Estados ou atores não estatais localizados em terceiros Estados, durante o trânsito pelo mar territorial. A maioria concluiu que as atividades cibernéticas realizadas durante a passagem inocente não devem prejudicar a segurança ou a ordem pública do Estado costeiro, incluindo suas relações com outros Estados e seus deveres para com esses Estados. Para ilustrar, invadir a rede de defesa de um terceiro Estado seria, para eles, incompatível com a passagem inocente e poderia comprometer a ordem pública do Estado costeiro, afetando suas relações com outros Estados (Schmitt, 2017, p. 243, tradução própria).

Em sentido contrário, o referido manual cita que a minoria dos *experts* entendeu que cada caso deve ser analisado individualmente, sob o argumento de que o propósito fundamental da passagem inocente é proteger os interesses do Estado costeiro, não de terceiros Estados, bem como que o potencial impacto nas relações diplomáticas devem ser apreciadas em cada caso. Ousamos divergir dessa minoria e por uma razão simples, qual seja, a literalidade da alínea “l” do Art. 19 (2) da CNUDM, pois qualquer outra atividade diversa da mera passagem é suficiente para descaracterizá-la como inocente.

No entanto, quando o Manual Tallin, ao apresentar as razões da sua regra 54¹⁰³, discorre especificamente sobre a possibilidade de interceptação física dos cabos para coleta dos dados, o entendimento apresentado é que tal fato constitui uma violação da soberania do Estado costeiro incompatível com o regime de passagem inocente, mas que, por outro lado, não viola a soberania de outros Estados, como por exemplo os proprietários ou operadores destes ativos.¹⁰⁴ Quanto ao aspecto da soberania, pensamos que é passível de debate se há ou não ofensa a este preceito de outro Estado, o que será apresentado mais adiante. Contudo, entendemos que a interceptação de cabos submarinos no mar territorial, independente de quem sejam seus proprietários ou os operem, viola o instituto da passagem inocente pelos mesmos motivos apresentados para a divergência anterior, razão pela qual opinamos pela sua ilegalidade frente aos ditames da CNUDM. Ademais, não vislumbramos razões plausíveis que

¹⁰³ Dispõe sobre as regras e princípios do Direito Internacional aplicáveis aos cabos submarinos.

¹⁰⁴ Como se destaca do excerto “Os especialistas observaram, no entanto, que uma operação de interceptação no mar territorial ou em águas arquipelágicas não viola a soberania de outros Estados, como aqueles que instalaram e operam o cabo” (Schmitt, 2017, p. 247, tradução própria).

justifiquem o tratamento diferenciado entre as operações cibernéticas em geral e a interceptação quanto a este ponto, considerando que ambos os casos extrapolariam os limites da mera passagem.

Uma vez caracterizada a passagem como prejudicial, é facultado ao Estado costeiro a adoção das medidas necessárias para impedi-la, conforme previsão da CNUDM,¹⁰⁵ proibindo a passagem ofensiva e utilizando os meios necessários para fazer cessar a violação do Direito do Mar. Como medida primária e proporcional a uma violação de menor importância, o Estado costeiro tem o poder de exigir a cessação da atividade ilícita e ordenar que a embarcação deixe o seu mar territorial. Poderá, ainda, suspender temporariamente a passagem inocente em áreas determinadas do mar territorial, desde que essa medida não seja discriminatória em relação a determinado(s) Estado(s) e seja devidamente divulgada e fundamentada em motivos de segurança, facultando, inclusive, a prática de exercícios militares com armas¹⁰⁶, sendo essa uma medida de uso da força autorizada pelo Direito Internacional (Menezes, 2025, p. 96).

Em se tratando de atos perpetrados por navios de guerra¹⁰⁷ ou outros navios de Estado, o descumprimento de leis e regulamentos do Estado costeiro relativos a passagem inocente pelo mar territorial fica sujeito apenas ao pedido de cumprimento e a exigência de saída imediata desse espaço marítimo¹⁰⁸, sendo passível de responsabilização no plano internacional o Estado de bandeira do navio que causar dano¹⁰⁹.

Trazendo a análise para a hipótese específica da realização de operações de interceptação de dados nos cabos submarinos no mar territorial brasileiro durante uma suposta passagem inocente, é necessário dizer que à luz do Direito Internacional consuetudinário e da própria sistemática da CNUDM, o limite de atuação do Brasil deverá, como regra, privilegiar medidas de natureza não coercitiva, atentando para os princípios da proporcionalidade e razoabilidade e evitando o uso da força, salvo nos casos que são autorizados pelo Direito Internacional¹¹⁰, o que dificilmente ocorrerá nas atividades envolvendo cabos submarinos (Roach; Smith, 2012, p. 578).

¹⁰⁵ Art. 25, CNUDM.

¹⁰⁶ Art. 25 (3), CNUDM.

¹⁰⁷ O Art. 29, CNUDM dá a definição de navio de guerra.

¹⁰⁸ Art. 30, CNUDM.

¹⁰⁹ Art. 31, CNUDM.

¹¹⁰ O Direito Internacional autoriza o uso da força em legítima defesa (em resposta a um ataque armado real ou iminente) ou mediante autorização do Conselho de Segurança da ONU (para manter ou restabelecer a paz e a segurança internacionais), conforme Artigos 42 e 51, respectivamente, da Carta das Nações Unidas.

Dada essa realidade, a maneira pela qual o Estado costeiro disporia para possibilitar a adoção de medidas coercitivas e de investigação seria a tipificação no ordenamento jurídico interno dessas condutas danosas, conforme será abordado na próxima subseção. Caso não haja previsão na lei interna de responsabilização pelas condutas que atentem contra a infraestrutura de cabos, a limitação de ordem prática das medidas disponíveis ao Estado costeiro deixariam ao alvedrio do Estado de bandeira para que faça valer a sua jurisdição e a manutenção da boa ordem no mar, o que, na prática, representaria uma transferência da competência jurisdicional do Estado costeiro para o de bandeira, ainda que seja possível ao primeiro buscar a responsabilização internacional do segundo pela omissão no dever de fiscalização do navio ao qual está vinculado.

6.3.1.2 *Jurisdição do Estado da Bandeira*

A edição de leis e regulamentos para a proteção de cabos submarinos no mar territorial é uma faculdade conferida pela CNUDM¹¹¹ e importante medida para que o Estado costeiro possa adotar medidas mais efetivas de proteção desses ativos conforme já apresentado, de modo que eventual iniciativa brasileira voltada a sancionar os responsáveis por atos atentatórios a essa infraestrutura, sejam incidentes sobre o seu suporte físico ou sobre os dados, estaria em conformidade com o Direito Internacional.

Haja vista essa possibilidade, poderia surgir a dúvida se tal medida não estaria em oposição ao princípio da jurisdição do Estado de bandeira, que representa uma regra do Direito Internacional que confere aos navios estrangeiros mercantes imunidade penal e civil, preconizando a submissão de atos cometidos a bordo dessas embarcações ao Direito interno do Estado da respectiva bandeira (Martins, 2008, p. 97).

Em se tratando de jurisdição penal, a CNUDM prevê como regra que o Estado costeiro não poderá exercê-la a bordo de navio estrangeiro que esteja em passagem pelo mar territorial¹¹², não sendo possível a detenção de pessoa ou a realização de investigação relacionada a eventual delito cometido, ressalte-se, a bordo desse navio.

Todavia, é necessário esclarecer que esse tratamento conferido pela Convenção de Montego Bay refere-se a infrações penais cometidas por pessoas dentro da embarcação (por exemplo homicídio, lesão corporal), não sendo aplicável a delitos cometidos por ato da

¹¹¹ Art. 21 (1) (c), CNUDM.

¹¹² Art. 27 (1), CNUDM.

própria embarcação. Ou seja, na hipótese de o navio ser utilizado deliberadamente como instrumento ou meio para o cometimento de atos ilícitos não há que se falar em imunidade penal por força do princípio do Estado de bandeira, como bem destaca Zanella:

Nesse sentido, a CNUDM regulamenta a jurisdição penal especificamente por crimes cometidos “a bordo” e não “pelo bordo”, ou seja, pelo navio. Nos casos de infrações por ato da própria embarcação que impliquem responsabilidade penal, não que ser utilizados outros tratados internacionais específicos. Entretanto a maioria destes possíveis crimes cometidos “pelo bordo” são de natureza ambiental e, para estes, a própria CNUDM já estipula o direito do Estado costeiro de investigar e responsabilizar criminalmente o capitão ou responsável pelos danos (Zanella, 2014, p. 17759).

Outro não poderia ser o entendimento, tendo em vista que a razão de ser da imunidade penal é não permitir embaraços à liberdade de navegação diante do cometimento de ilícitos que não tenham repercussão sobre o Estado costeiro, o que se interpreta da leitura das hipóteses de exercício excepcional da jurisdição do Estado costeiro por infração criminal ocorrida a bordo de navio estrangeiro, previstas nas alíneas do Art. 27 (1) da CNUDM.

Logo, se em hipóteses excepcionais o sistema estabelecido pela Convenção permite o afastamento da regra da imunidade de jurisdição penal e o consequente exercício jurisdicional pelo Estado costeiro diante de hipóteses que causem uma repercussão interna, com muito mais razão será possível o exercício dessa jurisdição frente a ilícitos cometidos pelo navio. Caso não fosse essa a interpretação, se estaria conferindo um salvo conduto para a utilização da embarcação para o cometimento de ilícitos, o que, certamente, não foi a intenção dos redatores do texto convencional.

Desse entendimento é possível concluir que, caso haja previsão tipificadora na lei penal brasileira, as condutas de eventual navio estrangeiro engajado em operação de interceptação ou de dano físico a cabo submarino não estaria acobertado pela imunidade penal, o que permitiria a persecução em face dos responsáveis pela prática criminosa.

6.3.2 Na Zona Econômica Exclusiva e na Plataforma Continental

Apesar da Zona Econômica Exclusiva e da Plataforma Continental apresentarem regimes jurídicos distintos estabelecidos pela CNUDM (Partes V e VI, respectivamente), suas disposições são aplicáveis em grande parte ao mesmo espaço geográfico, pelo menos até o limite das 200 milhas marítimas, compartilhando um mesmo regime normativo comum incidente sobre os cabos submarinos, marcado pela inexistência de soberania plena do Estado

costeiro, liberdade de colocação e manutenção dos cabos pelos demais Estados e jurisdição funcionalmente limitada e destinada a tutela de interesses específicos. Essa sobreposição normativa é expressamente estabelecida pela Convenção de Montego Bay, que no seu Art. 58 (2) remete às disposições da Parte VII (Alto-mar) e no Art. 79, a um regime quase espelhado para os cabos na Plataforma Continental, conforme destaca Davenport (2015, p. 72).

Quando se tratar de situações em que o Estado tiver uma Plataforma Continental que se estenda para além das 200 milhas marítimas (caso do Brasil), em que pese a diferença entre os regimes existente a partir dessa limitação geográfica, com a aplicação somente do regime da PC, não haverá distinção de tratamento quando se cuidar de proteção dos cabos submarinos, uma vez que, assim como também ocorre na ZEE, o regime da PC tutela os recursos existentes no leito marinho, sendo esse o caso dos cabos submarinos, os quais se encontram dispostos sobre esse assoalho oceânico, conforme já exposto¹¹³.

Desta feita, o alcance dos poderes brasileiros no que se refere a proteção dos cabos submarinos nesses dois espaços geográficos serão tratados conjuntamente nesta subseção, tendo em consideração a inexistência de diferenças que justifiquem os respectivos tratamentos separadamente.

A ZEE e a PC representam espaços marítimos de natureza jurídica complexa, situados entre a soberania plena (ou quase) do mar territorial e o regime de liberdade do alto-mar. Com supedâneo nos Art. 56 e 77 da CNUDM, o Estado costeiro não exerce soberania em sentido estrito na ZEE e na PC, mas possui direitos soberanos (ou de soberania) que lhe confere exclusividade no exercício de certos direitos de exploração econômica¹¹⁴ (Tanaka, 2019).

Em razão da previsão do Art. 58 (1) da Convenção, que estende à ZEE certas liberdades típicas do alto-mar, dentre as quais está a de colocação e manutenção de cabos submarinos, esses direitos soberanos dos Estados costeiros coexistem com tais liberdades asseguradas aos demais Estados, o que eventualmente pode significar a existência de uma tensão em virtude de interesses opostos. Como maneira de equilibrá-la, a CNUDM dispõe no Art. 58 (3) que os Estados usuários devem ter em devida conta os direitos e deveres do Estado costeiro, bem como cumprir as leis e regulamentos por ele adotados, desde que as mesmas não sejam incompatíveis com o próprio regime estabelecido pelo Direito Internacional do Mar (Raha; Raju, 2021, p. 12).

¹¹³ Ver seção 4.2.

¹¹⁴ Ver diferenciação entre os conceitos de soberania e direitos soberanos (ou de soberania) apresentados na subseção 3.2.1.3.

No que se refere a coleta de dados a partir de *tapping* nos cabos submarinos, a CNUDM não confere ao Estado costeiro competência para exercer a jurisdição penal sobre estrangeiros na ZEE e na PC. Como abordado na subseção 3.2.1.7, mesmo que o Estado costeiro cumpra com a obrigação imposta pela Convenção¹¹⁵ e insira na sua legislação doméstica previsão de responsabilização criminal pelo dano causado a cabos submarinos, tal medida apenas recairia sobre os seus nacionais e navios que ostentem a sua bandeira (Petty, 2021. p. 274).

No tocante à possibilidade de eventuais medidas coercitivas voltadas a impedir a interceptação de dados nesses espaços marítimos, a sistemática da CNUDM não confere a um navio de guerra a possibilidade de abordar ou apresiar um navio suspeito da prática de interceptação (Davenport, 2015, p. 106). Apesar da existência de discussão a respeito, fato é que a interceptação do fluxo de dados não se enquadra, de forma clara, no conceito de pesquisa científica marinha tal qual está definido na Parte XIII da CNUDM¹¹⁶. Sendo assim, inadmite-se a utilização do seu Art. 56 (1) (c) (ii) - que estabelece a jurisdição do Estado costeiro no que se refere a investigação científica marinha na ZEE - para fundamentar a execução de qualquer medida de natureza coercitiva ou mesmo restritiva.

À vista disso, a atuação brasileira nas suas ZEE e PC frente a eventuais operações estrangeiras de monitoramento e interceptação de dados em cabos submarinos fica limitada a restrições significativas, em razão da ausência de previsão no Direito Internacional de disposição nesse sentido, salvo se ficar comprovada uma violação concreta às suas competências previstas na CNUDM, tais como danos ambientais, interferência na exploração dos recursos econômicos ou outra decorrente do regime estabelecido pela Convenção (Raha; Raju, 2021).

6.4 INSTRUMENTOS JURÍDICOS BRASILEIROS APLICÁVEIS À SEGURANÇA DOS CABOS SUBMARINOS

O ordenamento jurídico brasileiro ainda não dispõe de um regime jurídico específico voltado exclusivamente à proteção dos cabos submarinos. Esta constatação implica dizer que o Brasil, embora seja parte e tenha internalizado a CNUDM por intermédio do Decreto nº 1.530/1995 (Brasil, 1995), incorporando ao seu ordenamento jurídico interno os direitos e deveres inerentes à condição de Estado costeiro no que tange a proteção dos cabos

¹¹⁵ Art. 113, CNUDM.

¹¹⁶ Art. 238 a 241, CNUDM.

submarinos, não levou a termo as previsões contidas nos Art. 113 a 115 da Convenção, que impõem aos Estados a obrigação de adotar leis e regulamentos voltados a sancionar danos (intencionais ou culposos) aos cabos submarinos.

A promulgação da Convenção, por si só, não supre a necessidade da adoção de regramentos internos para conferir a adequada efetividade à proteção dessa infraestrutura como almejado pelo sistema convencional, o qual necessita de complementação doméstica (Wargo; Davenport, 2014, p. 263).

Nesse contexto, vale mencionar que o Projeto de Lei nº 270/2025 encontra-se atualmente em tramitação no Congresso Nacional,¹¹⁷ objetivando criar um marco regulatório para a infraestrutura de cabos e será mais detidamente abordado em subseção própria.

6.4.1 Documentos de Defesa Nacional

O Decreto nº 12.725/2025, recentemente publicado¹¹⁸, instituiu a Política Nacional de Defesa (PND), a Estratégia Nacional de Defesa (END) e o Livro Branco de Defesa Nacional (LBDN) que juntos representam o arcabouço fundamental em matéria de defesa nacional, definindo, respectivamente, o que se deve defender, como se deve defender e o que o país possui e planeja para a sua defesa (Brasil, 2025a).

A PND, documento condicionante de mais alto nível do planejamento das ações de defesa nacional, reconhece o papel essencial das infraestruturas críticas para o desenvolvimento, integração, segurança e soberania nacionais, dispondo que os cabos submarinos são fundamentais para o funcionamento dos sistemas de informações, gerenciamento e comunicações de interesse nacional, sendo necessário o seu devido resguardo pelo aparato de Defesa Nacional¹¹⁹.

Em adição ao previsto na PND, a Estratégia Nacional de Defesa prevê a necessidade de o país deter capacidade cibernética mediante a participação sinérgica e coordenada de órgãos, entidades governamentais e entes privados a fim de assegurar a soberania, patrimônio, interesses nacionais, inviolabilidade territorial e resiliência das infraestruturas críticas.¹²⁰ No contexto dos cabos submarinos, a END estabelece como Ação Estratégica de Defesa (AED) contribuir para o aumento do nível de segurança das

¹¹⁷ O acompanhamento do PL nº 270/2025 pode ser realizado pelo sítio da Câmara dos Deputados, disponível em <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2482914>.

¹¹⁸ O Decreto nº 12.725/2025 foi publicado em 19 de novembro de 2025.

¹¹⁹ Item 1.2 da PND.

¹²⁰ Item 2.2 da END.

infraestruturas críticas¹²¹, ação esta subordinada ao primeiro Objetivo de Defesa Nacional (ODN)¹²², o que denota o reconhecimento da importância que o país vem dando à matéria.

Na mesma direção, o LBDN reconhece que os cabos submarinos fazem parte do sistema de infraestruturas críticas e são ativos estratégicos para a Defesa Nacional, necessitando de uma robusta proteção e, sobretudo, de um sistema de defesa cibernética capaz de neutralizar ameaças e garantir a continuidade das comunicações.¹²³

Dessa forma, os documentos que traçam as diretrizes sobre Defesa Nacional reconhecem a importância estratégica dos cabos submarinos enquanto infraestruturas críticas, afirmando que cabe ao Estado brasileiro a sua garantia e proteção como meio para assegurar a soberania e os interesses nacionais.

6.4.2 Documentos sobre a Segurança das Infraestruturas Críticas no Brasil

O Brasil estabeleceu um arcabouço normativo específico voltado à segurança das infraestruturas críticas por intermédio de um tripé formado por três decretos, sendo o primeiro país da América do Sul a apresentar um programa de segurança das suas Infraestruturas críticas (Badin *et al.*, 2024, p. 33).

A Política Nacional de Segurança de Infraestruturas Críticas (PNSIC), aprovada pelo Decreto nº 9.573/2018 (Brasil, 2018), estabelece como finalidade fundamental¹²⁴ desse tripé garantir a segurança e a resiliência das infraestruturas críticas, representando o documento de mais alto nível desse sistema. Além disso, especifica os princípios, objetivos e diretrizes¹²⁵ para a sua implementação e a consecução da sua finalidade, instituindo como seus instrumentos a Estratégia Nacional de Segurança de Infraestruturas Críticas, o Plano Nacional de Segurança de Infraestruturas Críticas e o Sistema Integrado de Dados de Segurança de Infraestruturas Críticas¹²⁶ (Castilho, 2023).

O Decreto nº 10.569/2020 aprovou a Estratégia Nacional de Segurança de Infraestruturas Críticas (ENSIC), seguindo o disposto na PNSIC e sendo o elemento central para a sua implementação. Em linhas gerais, a ENSIC define princípios, desafios, eixos

¹²¹ AED 02 da END.

¹²² O OND I – Garantir a soberania, o patrimônio nacional, a integridade e a inviolabilidade territorial – pelo tratamento de conteúdos sensíveis e diretamente relacionados à soberania do país, revela a importância que vem sendo dispensada ao objeto do presente trabalho pelo país.

¹²³ Capítulo 1, item SEGURANÇA E DEFESA CIBERNÉTICAS, LBDN.

¹²⁴ Art. 1º, Anexo, Decreto nº 9.573/2018.

¹²⁵ Art.2º ao 4º, Anexo, Decreto nº 9.573/2018.

¹²⁶ Art. 5º, Anexo, Decreto nº 9.573/2018.

estruturantes, objetivos e iniciativas estratégicas¹²⁷, não criando obrigações diretamente exigíveis, mas orientando a atuação dos agentes envolvidos no campo da defesa das infraestruturas críticas. Embora a ENSIC não aborde diretamente interceptação de dados, espionagem ou mesmo cite cabos submarinos no seu texto (assim como a PNSIC), indiretamente reconhece que as ameaças às infraestruturas críticas não se limitam à dimensão física ao prescrever que a sua abordagem deve ser a mais abrangente possível e levar em consideração “ameaças de toda ordem”¹²⁸, abrangendo, portanto, os riscos cibernéticos e as ações híbridas, representando um instrumento doméstico relevante de complementação da CNUDM. Assim, a ENSIC reconhece que as infraestruturas críticas devem ser protegidas não apenas contra danos físicos, mas também contra ameaças intencionais complexas, ainda que não tipifique essas condutas, permitindo enquadrar a interceptação de dados em cabos submarinos como um risco estratégico, mesmo que não expressamente previsto.

O Plano Nacional de Segurança de Infraestruturas Críticas (Plansic) foi instituído pelo Decreto nº 11.220/2022 (Brasil, 2022a) e apresenta um nível de detalhamento maior que os outros dois instrumentos anteriores, estruturando a governança, estabelecendo ações estratégicas (metas e prazos) e prevê a criação de planos complementares (setoriais e de outros entes federativos). É o único dos três instrumentos que cita diretamente os cabos submarinos ao ressaltar que tais infraestruturas extrapolam as fronteiras dos países e destacar a importância da cooperação internacional para a sua governança.¹²⁹ Apesar da simples menção, o Plansic reconhece a existência de riscos estratégicos às infraestruturas críticas, apesar de também não traduzir esse reconhecimento em normas específicas aplicáveis aos cabos submarinos. Dessa forma, é possível afirmar que o Brasil reconhece a importância da proteção às infraestruturas de cabos submarinos contra as diversas ameaças, funcionando o Plansic como um elo intermediário para uma regulação mais precisa e específica no âmbito interno.

Sintetizando brevemente as disposições desse tripé regulatório das infraestruturas críticas no Brasil, verifica-se que os seus instrumentos apresentam forte conteúdo programático, ou seja, denotam muito mais diretrizes e metas a serem buscadas do que propriamente mecanismos mais concretos de execução. Sendo dessa forma, embora forneça supedâneo político-estratégico para a proteção dos cabos, não estabelece medidas concretas

¹²⁷ Itens 2 a 5, Anexo, Decreto nº 10.569/2020.

¹²⁸ Item 2.1.1, Anexo, Decreto nº 10.569/2020.

¹²⁹ Item 4, Anexo, Decreto nº 11.200/2022.

para prevenir e reprimir ameaças aos cabos submarinos, mantendo o *deficit* normativo verificado tanto no plano internacional quanto no nacional.

Essa lacuna normativa é compatível com o contexto que motivou a elaboração do PL nº 270/2025, pois busca justamente preenchê-la e estabelecer um marco regulatório próprio para esses ativos em consonância com os decretos aqui apresentados, de acordo com o descrito no seu texto de justificativa e melhor abordado na próxima subseção.

6.4.3 O Projeto de Lei nº 270/2025 e a Proposta de um Marco Regulatório Nacional

O Projeto de Lei nº 270/2025 (Brasil, 2025b), atualmente em tramitação no Congresso Nacional¹³⁰, objetiva instituir a Política Nacional de Infraestruturas de Cabos Subaquáticos¹³¹ (PNICS), representando uma tentativa do estabelecimento de um marco regulatório específico no trato da infraestrutura de cabos em meio a um contexto normativo marcado por diretrizes programáticas, como apontamos. Como o seu próprio texto de justificativa revela, o projeto pode ser entendido como uma consequência lógica das disposições trazidas pelos decretos analisados na subseção anterior e sinaliza a tentativa de suprir as lacunas verificadas na legislação brasileira quanto ao trato do tema, buscando aperfeiçoar e adequar o arcabouço doméstico às obrigações e desafios existentes no âmbito internacional.

Sem desconsiderar a iniciativa pioneira e a relevância do projeto, merece registro o fato de que o seu texto atual, tal como proposto, ainda suscita alguns questionamentos que merecem um maior aprofundamento, de maneira que certos aspectos conceituais, delimitação de competências e medidas de repressão revelam margens de indeterminação que podem comprometer a sua efetividade. Tais observações não afastam o mérito da proposta, mas apenas indicam a conveniência do seu aprimoramento no curso do processo legislativo ainda em curso, de modo a melhor harmonizá-la aos desafios contemporâneos correlatos à segurança da infraestrutura. Considerando o escopo deste trabalho, não serão realizadas

¹³⁰ Em 4 nov. 2026, data de escrita da subseção 4.4.3, a situação do nº PL 270/2025 era a de aguardando parecer do Relator na Comissão de Relações Exteriores e de Defesa Nacional (CREDN).

¹³¹ Ao longo do presente trabalho, utiliza-se predominantemente a expressão “cabos submarinos”, consagrada no Direito Internacional do Mar e especialmente na CNUDM. O PL nº 270/2025 utiliza a expressão “cabos subaquáticos”, que revela uma abrangência maior, englobando, além daqueles dispostos no leito do oceano, os colocados nas águas interiores como rios, lagos ou até mesmo represas, conforme previsto no Art. 3º, I, do projeto. Não obstante a diferença terminológica, ambas as expressões se referem à mesma infraestrutura crítica de comunicação e serão tratadas como equivalentes.

análises de todos os aspectos do projeto, mas apenas daqueles que guardem alguma relação com a temática da interceptação de dados.

6.4.3.1 *A Correlação do Projeto com a Temática da Interceptação de Dados*

Nessa direção, a análise deve inicialmente ser considerado que a proposta parte do pressuposto que os cabos submarinos representam um vetor de segurança nacional e de soberania digital, sendo ambos os termos tratados como princípios fundamentais¹³² e mencionados em diversas passagens do seu texto.¹³³ Tal fato é relevante porque estabelece uma base principiológica permitindo inserir a interceptação de dados no campo das ameaças e considerá-la como um risco estratégico e não apenas uma questão de privacidade das comunicações, ainda que o texto assim não faça expressamente.

O Art. 16 do PL é um dispositivo que tem relevância perante o tema, pois impõe aos operadores de cabos submarinos a adoção de protocolos de segurança nas redes e serviços de telecomunicações, incluindo proteção contra acessos não autorizados e ataques cibernéticos, monitoramento contínuo da integridade dos dados e armazenamento de logs¹³⁴ em conformidade com a Lei Geral de Proteção de Dados (LGPD), reconhecendo que a segurança da infraestrutura não se limita apenas à sua dimensão material, albergando também a dimensão digital, revelando um avanço importante se comparado com o regime da CNUDM.

Ao remeter diretamente à LGPD (Brasil, 2018), que dispõe sobre o tratamento de dados pessoais e tem como fundamentos o respeito à privacidade, inviolabilidade da intimidade, privacidade, honra e imagem, o projeto estabelece um vínculo normativo entre a segurança da infraestrutura de cabos e os direitos fundamentais, reforçando a perspectiva de direitos humanos e proteção da privacidade, abordados no capítulo 2.

6.4.3.2 *A Criminalização de Condutas*

Este ponto, da maneira como proposta no PL nº 270/2025, representa um ponto sensível e juridicamente relevante do projeto, ainda mais quando considerado à luz do Direito

¹³² Conforme previsto nos Arts. 1º e 2º.

¹³³ Os termos “segurança nacional” e “soberania digital” aparecem seis vezes cada um no projeto.

¹³⁴ Os arquivos de log são registros da atividade do sistema gerados por diversos recursos computacionais e desempenham um papel importante no que diz respeito à segurança cibernética e proteção de sistemas, fornecendo registros detalhados de acessos e comportamentos de usuários que podem conter indícios de um ataque (Flinders; Smalley, 2025).

Internacional do Mar e do Direito Penal. Isso porque, em primeiro lugar, o projeto de lei estabelece a sujeição de quem descumprir à sanções civis, administrativas e penais¹³⁵, em conformidade com o que é exigido pela CNUDM (especialmente nos seus Art. 113 a 115), cumprindo a função de sinalizar, ainda que tardiamente, o atendimento da obrigação internacional assumida pelo Brasil quanto à adoção de leis e regulamentos voltados à sancionar danos causados aos cabos submarinos. Sem desconsiderar essa importância, entretanto, o caráter genérico dessa previsão evidencia que o projeto não esgota o conteúdo normativo necessário para a implementação dessa obrigação internacional de maneira plena, pois, da maneira como está redigido, dependerá de complementação por normas infralegais e, principalmente, por tipos penais claros e tecnicamente adequados estabelecidos por lei federal, para que se possa saber o seu exato alcance (Greco, 2017, p. 99).

O ponto central da proposta penalizadora encontra-se disposto no Art. 22 do projeto, o qual transcreveremos abaixo para melhor compreensão:

Art. 22. Altera-se o Decreto Lei nº 2.848 de 1940 para incluir o art. **266-B** com a presente redação:

Art. 266-B. Interromper, **perturbar**, **alterar**, sabotar:

I - cabos subaquáticos.

II - infraestrutura crítica.

II - estruturas correlatas aos cabos subaquáticos que afetem a operação.

III - II - estruturas correlatas à infraestrutura crítica que afetam a operação.

Pena - reclusão de oito a quinze anos.

§1º A pena será aumentada em 1/3 (um terço) se o crime for cometido em calamidade pública ou por profissional com o dever de operação, manutenção ou defesa da infraestrutura ou estrutura correlata afetada (Brasil, 2025b, grifo nosso)

Sob a ótica da interceptação de dados, é possível sustentar, em tese, que as práticas de *tapping* ou qualquer outra forma de interceptação de dados poderiam ser enquadradas aos verbos “perturbar” ou “alterar”, especialmente se tais condutas, no caso concreto, impactarem o perfeito funcionamento das comunicações. Todavia, essa interpretação encontra um obstáculo no princípio da legalidade penal na sua vertente estrita (*nullum crimen, nulla poena sine lege stricta*) que veda a criação ou o agravamento de normas incriminadoras por meio da analogia (Rosa, 2024, p. 60). Como é reiteradamente afirmado

¹³⁵ Art. 21, PL nº 270/2025.

pela jurisprudência da mais alta corte brasileira, a tipicidade penal deve ser certa e inequívoca, não sendo possível ampliar o alcance dos tipos penais por interpretação extensiva que, na prática, funciona como analogia (Brasil, 2021). Dessa forma, em que pese haver proximidade semântica com os núcleos dos verbos previstos no tipo penal, a interceptação deveria ser expressamente prevista como uma conduta tipicamente penal, sob pena de violação à Constituição Federal.¹³⁶

O *quantum* de pena estabelecido no preceito secundário¹³⁷ do tipo penal também merece ser apreciado. O projeto comina a pena de reclusão de 8 a 15 anos, patamar significativamente elevado quando comparado com os demais delitos inseridos no mesmo capítulo do Código Penal - CP (Brasil, 1940).¹³⁸ Por exemplo, o Art. 266 do CP, que trata da interrupção ou perturbação de serviço telegráfico, radiotelegráfico ou telefônico (que inclusive guarda certa semelhança com o delito que ora se pretende criar e aqui se está analisado) prevê pena de detenção de um a três anos, e multa, de modo que não somente a quantidade da pena abstratamente considerada é inferior, mas também a sua espécie é mais benéfico.¹³⁹ Ao que parece, o rigor pretendido pelo projeto, manifestado no *quantum* de pena abstratamente considerado, é devido ao caráter estratégico dos cabos submarinos e ao potencial impacto em larga escala decorrentes da sua danificação. Porém, tal aspecto merece uma reflexão crítica à luz do princípio da proporcionalidade, em razão de que, como destaca Greco (2017, p. 159), a pena deve ter coerência não apenas com o bem jurídico tutelado em si, mas com a estrutura do sistema penal como um todo.

À vista das considerações apresentadas, é possível que a criação de mais um outro tipo penal específico voltado a criminalizar a conduta de interceptação de dados seja mais adequado ao atendimento de uma tutela mais ampla, sugerindo-se situá-lo entre os crimes contra a soberania nacional,¹⁴⁰ principalmente se considerarmos as mudanças trazidas pela Lei nº 14.197/2021 (Brasil, 2021), que inseriu no Código Penal o delito de espionagem¹⁴¹ no rol desses delitos, cuja pena pode chegar até 15 anos de reclusão, limite também pretendido pelo

¹³⁶ O princípio da legalidade penal está previsto no inciso XXXIX, Art. 5º, CRFB/1988.

¹³⁷ As chamadas normas penais incriminadoras são constituídas por dois preceitos: primário e secundário. Enquanto o primeiro se encarrega de fazer a descrição detalhada da conduta considerada criminosa, ao segundo cabe individualizar a pena, estabelecendo a sua quantidade em abstrato (Greco, 2017, p. 97).

¹³⁸ O PL almeja inserir o Art. 266-B no Capítulo II do Título VIII, que versa sobre os crimes contra segurança dos meios de comunicação e transporte e outros serviços públicos.

¹³⁹ O Código Penal brasileiro prevê duas espécies de penas privativas de liberdade, quais sejam, a reclusão e a detenção. Sem adentrar em aspectos mais pormenorizados do tema que extrapolam o escopo do presente trabalho, é suficiente dizer que o CP prevê algumas diferenças de tratamento entre as penas de reclusão e detenção, sendo certo dizer que a primeira impõe um ônus maior ao apenado (Greco, 2017, p. 628).

¹⁴⁰ Os crimes contra a soberania nacional estão previstos no Capítulo I do Título XII do Código Penal.

¹⁴¹ Art. 359-K do Código Penal.

PL. Essa perspectiva parece estar mais alinhada com o ponto de vista de autores que defendem uma compreensão mais ampliada do conceito de soberania, incluindo nele o espectro digital (Kello, 2017, p. 229).

Entretanto, apesar de o crime de espionagem revelar que o ordenamento jurídico brasileiro já contempla um tipo penal relacionado à subtração de informações estratégicas, não é adequado estendê-lo à conduta de interceptação de dados em cabos submarinos, sob pena de violação do princípio da legalidade. Isso porque não obstante a interceptação poder ser classificada como uma prática de espionagem técnica, como apresentamos¹⁴², pressupõe a captação de comunicações sem o conhecimento ou consentimento dos interessados, enquanto o crime de espionagem, da maneira como está tipificado, pressupõe a entrega de documentos ou informações a um poder estrangeiro com o específico fim de agir de prejudicar a defesa nacional (Stoco, 2023, p. 44). Ainda, o tipo de espionagem do Art. 359-K do CP é marcado pela exigência de que o objeto material da infração constitua um documento ou informação classificado como secreto ou ultrassecreto de acordo com a lei, caracterizando este dispositivo como uma norma penal em branco¹⁴³, apesar de já estar devidamente complementada pela Lei nº 12.527/2011 (Souza, 2023).

A criação de um delito específico para a interceptação permitiria uma maior precisão na formulação do tipo penal, sendo possível utilizar termos técnicos adequados que prevejam como conduta criminosa a utilização de qualquer meio técnico ou dispositivo para captar, reproduzir, transmitir ou interferir no fluxo de dados que trafegam pela estrutura de cabos, bem como estabelecer qualquer outra peculiaridade que se faça necessária à exigência da leitura contemporânea do princípio da legalidade. Uma maior precisão na criminalização das condutas é desejável em um Estado Democrático de Direito, pois permite o conhecimento das condutas que efetivamente são proibidas, evita arbitrariedades estatais e permite a interpretação da norma pelo juiz de forma não discricionária (Góes; Santin, 2024, p. 134).

6.4.4 *Status* do Brasil Quanto à Segurança das Infraestruturas Críticas

De acordo com o Banco Interamericano de Desenvolvimento (BID), o Brasil tem feito avanços significativos na proteção de suas infraestruturas críticas. Em relatório que avalia a capacidade institucional e discorre sobre os desafios, vulnerabilidade e maturidade

¹⁴² Seção 2.3.

¹⁴³ Conforme definição constante no Glossário Jurídico do Supremo Tribunal Federal, uma norma penal em branco “é uma norma penal genérica, cujo mandamento necessita de outra norma penal específica que a complemente”. Disponível em: <https://portal.stf.jus.br/jurisprudencia/glossario.asp>. Acesso em: 6 jan. 2026.

em cibersegurança na América Latina e no Caribe, o BID aponta que o país possui uma estratégia estabelecida e em evolução para a proteção de infraestruturas críticas, com estruturas de governança e coordenação ativas e um nível de maturidade considerado estabelecido (BID, 2025, p. 66). Apesar de o relatório não mencionar especificamente as redes de cabos submarinos, discute a cibersegurança em um escopo mais amplo, o que permite considerá-lo como fonte útil.

Mediante uma análise das informações apresentadas, o relatório permite um diagnóstico no sentido de que o Brasil possui uma estrutura legal robusta, incluindo normas substantivas,¹⁴⁴ capacidades institucionais para persecução de crimes e mecanismos de cooperação internacional voltados à repressão do cibercrime, apesar da existência de algumas lacunas. Todavia, mediante uma comparação com outros países da região, o Brasil ainda precisa avançar em quesitos afetos ao seu quadro regulatório e legal, apresentando uma nota média de 3 pontos (em uma escala até 5), ficando atrás de países como a Argentina e o Chile quanto a este aspecto (BID, 2025, p. 70).

6.5 O PAPEL DA MARINHA DO BRASIL NAS EXPRESSÕES DO PODER NAVAL E DA AUTORIDADE MARÍTIMA

A Estratégia Nacional de Defesa estabelece que adicionalmente às suas atribuições primárias previstas constitucionalmente,¹⁴⁵ as Forças Armadas devem ter condições de desempenhar outras atividades com o propósito de atender aos compromissos assumidos pelo Brasil e salvaguardar os seus interesses. Especificamente quanto à Marinha do Brasil, a END prevê como sua tarefa as atividades de vigilância e patrulhamento das AJB no campo da Segurança Marítima, bem como diversas outras atividades desenvolvidas em cooperação com outros órgãos do Estado associadas ao cumprimento das suas atribuições subsidiárias previstas em lei (Brasil, 2025a, p. 17).

A Lei Complementar nº 97/1999 atribui à MB uma série de atividades subsidiárias particulares, designando o Comandante da Marinha como “Autoridade Marítima” e estabelecendo a sua competência para o trato dessas atividades¹⁴⁶ (Brasil, 1999). Conforme

¹⁴⁴ Leis substantivas (ou materiais) são aquelas que definem direitos, deveres e relações jurídicas. Diferentemente, as normas adjetivas (ou processuais) dispõem sobre os ritos e processos para fazer valer aqueles direitos.

¹⁴⁵ A destinação constitucional das Forças Armadas está prevista no *caput* do Art. 142 da CRFB, sendo ela a defesa da pátria, a garantia dos poderes constitucionais e, por iniciativa de qualquer destes poderes, a garantia da lei e da ordem.

¹⁴⁶ Art. 17, LC nº 97/1999.

ensina Beirão (2014, p. 163), a designação do Comandante da Marinha, no caso da própria MB, como Autoridade Marítima Brasileira (AMB) representa uma particularidade brasileira que implica o exercício de atribuições relacionadas à segurança no mar compreendida em seus dois vieses: como segurança da navegação (*maritime safety*) e como segurança contra ameaças deliberadas (*maritime security*), não havendo dúvidas acerca da incumbência da MB para atuação em ambos.

Trazendo a distinção para o campo da segurança dos cabos submarinos, estar-se-á falando de *maritime safety* quando as questões versarem sobre a proteção dos cabos submarinos contra danos (físicos) não intencionais decorrentes do exercício da navegação ou das demais atividades desenvolvidas no mar, estando este viés afeto ao trato da Autoridade Marítima Brasileira. Por outro lado, será de *maritime security* quando a abordagem incidir sobre questões afetas às ameaças intencionais às infraestruturas aqui consideradas (abrangidas, logicamente, as ações de interceptação de dados), estando este viés, diversamente do caso anterior, submetido ao crivo da MB enquanto detentora do Poder Naval. A compreensão dessa distinção de competências é particularmente relevante no que diz respeito aos cabos submarinos, eis que se tratam de ativos que se encontram localizados no domínio marítimo e a sua proteção está diretamente relacionada com o cumprimento tanto das atribuições primárias, quanto das atribuições subsidiárias da MB e, por conseguinte, da sua missão tal qual encontra-se prevista na Política Naval¹⁴⁷ (Brasil, 2019).

Assim, a análise do papel da Marinha do Brasil na segurança e na proteção dos cabos submarinos exige uma distinção conceitual e funcional entre estas duas dimensões da sua atuação funcional, que são complementares entre si. Ora a MB atua como Poder Naval, integrante da expressão militar do Poder Nacional, voltada à defesa da soberania, integridade territorial e interesses estratégicos do país no mar, ora atua investida das atribuições de AMB, com competências administrativas, normativas e fiscalizatórias voltadas à segurança da navegação e à ordenação do uso dos espaços marítimos. A análise em separado dessas duas funções permite compreender, de forma mais precisa, os instrumentos jurídicos, os limites de atuação e as respostas institucionais disponíveis em cada esfera.¹⁴⁸

¹⁴⁷ Segundo a Política Naval a Missão da MB é “Preparar e empregar o Poder Naval, a fim de contribuir para a Defesa da Pátria; para a garantia dos poderes constitucionais e, por iniciativa de qualquer destes, da lei e da ordem; para o cumprimento das atribuições subsidiárias previstas em Lei; e para o apoio à Política Externa.” (Marinha do Brasil, 2019, p. 43).

¹⁴⁸ As competências da Marinha do Brasil estão dispostas no Decreto nº 5.417/2005 (Brasil, 2005).

6.5.1 O Papel da Autoridade Marítima Brasileira

Conforme estruturado pelo nosso ordenamento jurídico, a Marinha do Brasil (assim como as demais Forças Armadas) não exerce apenas funções de natureza tipicamente militar, mas desempenha também um conjunto de atribuições definidas como subsidiárias, assim compreendidas aquelas conferidas à MB por força de norma legal que não estejam relacionadas com a defesa da pátria, a garantia dos poderes constitucionais, e da lei e da ordem.¹⁴⁹ Como já apontado anteriormente, essa condição decorre da LC nº 97/1999 que atribui à MB funções específicas tais como proteger a segurança da navegação aquaviária, implementar e fiscalizar o cumprimento de leis e regulamentos no mar e cooperar com outros órgãos em matérias correlatas, ficando designado o Comandante da Marinha como AMB.

No exercício dessas funções, a Marinha, por intermédio das suas Capitânicas, Delegacias e Agências, atua de forma descentralizada em todo o território nacional, fiscalizando o tráfego aquaviário, ordenando a navegação, promovendo a salvaguarda da vida humana no mar e prevenindo a poluição hídrica. Para atingir esse fim, a AMB elabora normas técnicas em observância à legislação interna e aos tratados internacionais ratificados pelo Brasil como explicitado, por exemplo, na Missão institucional da Diretoria de Portos e Costas (DPC, 2026).

Nesse contexto e especificamente no que concerne aos cabos submarinos, as Normas da Autoridade Marítima para Obras e Atividades Afins em Águas sob Jurisdição Brasileira (NORMAM-303/DPC), cujo propósito é apresentar os princípios fundamentais para normatizar e estabelecer os procedimentos para obras e atividades correlatas nas AJB, constitui instrumento regulatório que disciplina a autorização para a instalação e remoção desses ativos, estabelecendo um regime de autorização prévia, fiscalização e controle-técnico administrativo que se aplica expressamente às atividades de colocação, manutenção e retirada dos cabos (Marinha do Brasil, 2023c). A norma estabelece uma série de procedimentos e recomendações para as empresas, focado na segurança e redundância do sistema, podendo ser citados a ampliação da diversidade geográfica dos pontos de conexão dos cabos em terra, a redundância do sistema, a instalação de sensores de monitoramento de ameaças, dentre outros. Ao trazer tais disposições na norma, a AMB está criando mecanismos de redução de riscos de danos a infraestrutura e facilitando a coordenação com outros usuários do espaço marítimo.

¹⁴⁹ Conforme previsto no sítio eletrônico da Diretoria de Portos e Costas (DPC). Disponível em: <https://www.marinha.mil.br/dpc/atribuicoes-da-dpc-sobre-meio-ambiente>. Acesso em: 8 jan. 2026.

Com o propósito de evitar danos acidentais causados pela navegação nas AJB, a AMB estabelece um conjunto de outras normas regulando atividades e fatores que de alguma forma guardem relação com os sistemas de cabos, citando-se a proibição do fundeio de embarcações dentro das zonas de proteção de cabos submarinos ou a uma distância inferior a quinhentos metros das linhas que demarcam essas zonas nas cartas náuticas,¹⁵⁰ a necessidade de sinalização especial da sua localização,¹⁵¹ a demarcação em cartas náuticas e divulgação de avisos de atividades de lançamento desses ativos,¹⁵² o seu georreferenciamento em levantamentos hidrográficos,¹⁵³ os procedimentos para apuração de eventual colisão da embarcação e/ou seus apêndices ou acessórios com os cabos,¹⁵⁴ apenas para citar algumas.

Diante da quantidade de normatização exemplificativamente citada a respeito da atuação da MB enquanto Autoridade Marítima, fica evidenciado que o viés de *maritime safety* é caracterizado por uma regulação relativamente robusta, sendo possível considerar que a infraestrutura de cabos submarinos nas AJB encontra-se disciplinada a contento, pelo menos em certa medida, conforme se pode concluir da análise do Quadro 4, a seguir.

Quadro 4 – A atuação da Autoridade Marítima Brasileira

Eixo de atuação	Atividades desenvolvidas	Relação com a proteção dos cabos submarinos
Segurança da navegação	Fiscalização do tráfego aquaviário; normatização de embarcações; controle de rotas e fundeios.	Redução do risco de danos acidentais aos cabos (ancoragem, pesca de arrasto, colisão).
Ordenamento do uso do mar	Emissão de normas e autorizações para atividades marítimas, delimitação de áreas restritas.	Possibilidade de criar corredores de segurança delimitadores do exercício de atividades.
Fiscalização e poder de polícia administrativa	Inspeção naval, aplicação de sanções; cooperação com outros órgãos.	Prevenção e repressão indireta de condutas que possam causar riscos à integridade física dos cabos.
Coordenação interinstitucional	Atuação conjunta com outras agências (GSI-PR, ANATEL, Polícias Militares e outros).	Disseminação de conhecimento e maior eficácia na proteção pela integração sinérgica das agências.

Fonte: Elaborado pelo autor.

Todavia o mesmo não se pode afirmar quanto às atribuições afetas ao Poder naval, havendo uma assimetria existente entre o nível de detalhamento e definição de competências

¹⁵⁰ Item 2.2, NORMAM-204/DPC.

¹⁵¹ Item 3.18, NORMAM-601/DHN.

¹⁵² Item 5.4.1, NORMAM-511/DHN.

¹⁵³ Item 2.6, NORMAM-501/DHN.

¹⁵⁴ Item 1.6.1, NORMAM-302/DPC.

relacionadas ao aspecto da segurança contra ameaças intencionais (*maritime security*), como será abordado a seguir.

6.5.2 O Papel do Poder Naval

Nos documentos estratégicos da Marinha do Brasil encontra-se o arcabouço conceitual e operacional que orienta a sua atuação no campo do Poder Naval, conceito previsto nos Fundamentos Doutrinários da Marinha - FDM (EMA-301) como:

O Poder Naval é um dos componentes da expressão militar do Poder Nacional e integrante do Poder Marítimo, capaz de atuar no mar, nas águas interiores e em certas áreas terrestres limitadas de interesse para as operações navais, incluindo o espaço aéreo sobrejacente, visando contribuir para a conquista e a manutenção dos Objetivos Militares e Setoriais de Defesa, decorrentes dos Objetivos Nacionais de Defesa, identificados na Política Nacional de Defesa (PND), conforme as diretrizes estabelecidas pela Estratégia Nacional de Defesa (END) (Marinha do Brasil, 2023a, p. 1-4).

Como já mencionamos, antes mesmo das atribuições exercidas pela MB na condição de AMB encontram-se aquelas decorrentes da sua finalidade primeira prevista constitucionalmente, afeta ao Poder Naval, inserindo-se neste escopo a segurança da infraestrutura de cabos em face de ameaças intencionais, como atos de sabotagem e, especificamente no ponto que interessa ao presente estudo, de interferência deliberada na interceptação de dados. Com esse enfoque, a segurança dos cabos submarinos assume o viés de *security*, encontrando-se em um âmbito mais amplo de defesa nacional e resguardo de assuntos estratégicos, haja vista a importância desses sistemas para a soberania nacional, podendo a MB no exercício do seu Poder Naval valer-se de atividades de emprego da força, desde que dentro dos limites estabelecidos pelos tratados internacionais ratificados pelo Brasil (Piñon, 2016, p. 53).

Uma outra publicação que dispõe de maneira mais direta essas competências é a Estratégia de Defesa Marítima (EMA-310), cujo propósito é estabelecer a orientação estratégica de mais alto nível na MB. Para isso, discrimina os Objetivos Estratégicos da Marinha (OBE) a serem seguidos para a consecução da sua missão, destacando-se o OBE-3, voltado a proteger as Infraestruturas Críticas do Poder Marítimo (ICPM).¹⁵⁵ Para alcançar esse

¹⁵⁵ O Centro de Desenvolvimento Doutrinário de Guerra Naval entende que as ICPM são instalações, serviços e bens, cinéticos e não cinéticos, necessários para a realização de atividades que colaborem para a navegação, exploração do mar e das águas interiores, a produção de energia, sejam quais forem as suas finalidades e objetivos, em todo o seu potencial, realizada em superfície ou submersa.

objetivo, “[...] o Poder Naval deverá adotar postura coercitiva, e ser capaz de realizar ações de reconhecimento e ações diretas, que contemplam, inclusive, o emprego de meios não tripulados e ações de contraterrorismo, retomada e resgate, destacamentos de abordagem [...]” (Marinha do Brasil, 2023b, p. 1-14).

Sob a ótica do papel operacional desempenhado pela MB, identificar o alcance da responsabilidade das Forças Armadas representa uma tarefa complexa, haja vista que muitas das atividades de proteção dos cabos submarinos são de responsabilidade dos seus proprietários. Em termos de capacidades, a atuação da MB depende em grande medida do fortalecimento da Consciência Situacional Marítima (CSM)¹⁵⁶ e, nesse contexto, o Sistema de Gerenciamento da Amazônia Azul (SisGAAz) se apresenta como um instrumento central para o monitoramento de áreas sensíveis nas AJB, nelas compreendidos os trechos de passagem de cabos e áreas de maior vulnerabilidade em águas rasas, permitindo a identificação precoce de comportamentos anômalos e a pronta resposta a incidentes (Zuccaro et al., 2025, p. 12).

A atuação da Marinha não se limita à vigilância, compreendendo também a capacidade de intervir e responder às diversas ameaças existentes, envolvendo o emprego de meios navais de superfície, submarinos, mergulhadores, aeronaves de patrulha, meios subaquáticos operados remotamente e não tripulados (ROVs e UUVs)¹⁵⁷ que podem ser empregados e se revelam muito úteis na oposição à ameaças assimétricas.

Ocorre que apesar da aparente clareza das disposições das referidas normas, nem sempre é fácil estabelecer com precisão a devida repartição das competências entre os atores envolvidos no processo de segurança. Como já abordado, em se tratando de atividades ilícitas no domínio marítimo a jurisdição é condicionada aos respectivos regimes jurídicos dos espaços marítimos, sobretudo quando se falar da interceptação, que ainda se encontra em um vácuo legislativo. Não resta dúvidas que o Poder Naval estará legitimado a adotar medidas coercitivas diante de um ataque deliberado voltado a destruir a infraestrutura de cabos, todavia essa certeza não se faz presente diante de uma suspeita de interceptação nas AJB, que por sua própria natureza furtiva e tecnicamente sofisticada (superados aqui eventuais

¹⁵⁶ A definição de Consciência Situacional Marítima (CSM) pode ser compreendida a partir do conceito de Consciência Situacional apresentado pela publicação Fundamentos Doutrinários da Marinha (FDM), entendida como a “capacidade de ter a percepção do que lhe acontece e que envolve a manutenção do nível de conhecimento nas áreas de interesse, de forma a detectar, identificar e acompanhar, por meio de informações ou da experiência, eventuais situações anômalas ou ameaças com a antecedência necessária que possibilite a tomada de decisão e resposta ou a reação adequada. Essa capacidade envolve diretamente a utilização de todos os recursos disponíveis de Inteligência e a existência de uma estrutura de alarmes, assim como de Comando e Controle adequado” (Brasil, 2023).

¹⁵⁷ ROV corresponde a *Remotely Operated Vehicle* (veículo operado remotamente) e UUV a *Unmanned Underwater Vehicle* (veículo subaquático não tripulado).

questionamentos sobre a sua efetiva possibilidade, como discutido no capítulo 1) representa um desafio particular que encontra limites jurídicos e operacionais impostos pelo Direito Internacional.

A propósito, as novas modalidades de ameaças evidenciam também um outro aspecto da atuação da MB, manifestado no relacionamento interagências pois, embora a Marinha detenha responsabilidades específicas no domínio marítimo, a segurança dos cabos exige coordenação contínua com outros atores, notadamente o Ministério das Comunicações, a ANATEL, o Gabinete de Segurança Institucional da Presidência da República (GSI-PR), além de operadores privados de telecomunicações. Tal coordenação vem sendo desenvolvida por iniciativa da Marinha, por exemplo, durante a realização de exercícios¹⁵⁸ e de eventos destinados ao treinamento de pessoal no emprego de meios disponíveis e à discussão para o aprimoramento de aspectos regulatórios (Zuccaro et al., 2025, p. 29), ainda que as atribuições de articulação e coordenação sejam do GSI-PR.¹⁵⁹

A fixação de competências dos diversos atores envolvidos representa um dos principais obstáculos a serem superados, sob pena da ocorrência da sobreposição de atribuições e da existência de lacunas, tudo em prejuízo do sistema de cabos submarinos, principalmente diante da verificação de eventos que demandem respostas rápidas e integradas. Para exemplificar, o modelo de pacto federativo¹⁶⁰ instituído pela CRFB/1988 determina que compete à União assegurar a defesa nacional (Art. 21, III) e executar os serviços de polícia marítima (Art. 21, XXII), sendo a primeira tarefa atribuição das Forças Armadas (Art. 142) e a segunda atribuição da Polícia Federal - PF (Art. 144, §1º, III). Ocorre que a PF possui competência, enquanto polícia marítima, para prevenir e reprimir crimes praticados a bordo, contra ou em relação a embarcações fundeadas no mar territorial, bem como crimes de repercussão interestadual ou internacional no âmbito marítimo.¹⁶¹ Assim sendo, na hipótese do advento de lei penal criminalizadora referente a cabos submarinos, tanto a MB quanto a PF teriam competência para prevenir e reprimir a conduta, o que não é desejável.

Enfim, a análise da atuação da Marinha do Brasil enquanto Poder Naval evidencia que, em que pese a existência de diretrizes estratégicas gerais e amparo constitucional e legal

¹⁵⁸ Informações disponíveis em <https://www.agencia.marinha.mil.br/defesa-naval/exercicio-inedito-da-marinha-garante-manutencao-de-cabos-submarinos>. Acesso em: 8 jan. 2026.

¹⁵⁹ Item 4 (I), Decreto nº 11.200/2022.

¹⁶⁰ Conforme descrito no sítio do Senado Federal, o pacto federativo é o conjunto de regras que tratam das relações entre a União, os estados, o Distrito Federal e os municípios conforme definido na Constituição, que define as competências e atribuições de cada um desses entes, que podem ser exclusivas, concorrentes e comuns. Disponível em: <https://www12.senado.leg.br/noticias/entenda-o-assunto/pacto-federativo>. Acesso em: 8 jan. 2026.

¹⁶¹ Incisos I e II, Art. 7º, Instrução Normativa nº 2/1999 (Departamento de Polícia Federal, 1999).

que permitem enquadrar a segurança de cabos submarinos no espectro da defesa nacional, desafios precisam ser superados no âmbito normativo e institucional. A ausência de disposição legal específica sobre danos intencionais e interceptação, somada às disposições do Direito Internacional, à sofisticação técnica dessas operações e a falta de clareza quanto ao estabelecimento de competências acabam por limitar a efetividade de uma resposta estatal adequada.

6.6 CONSIDERAÇÕES PARCIAIS

O presente capítulo teve como objetivo examinar os desafios que a interceptação de dados em cabos submarinos a partir de uma perspectiva interna, delimitando a análise às Águas Jurisdicionais Brasileiras e às competências atribuídas ao Estado brasileiro pelo Direito Internacional e pelo ordenamento jurídico interno. A partir dessas balizas, buscou-se demonstrar que a segurança dos cabos submarinos, embora inseridos em um contexto global, exige respostas concretas nas esferas jurídica e institucionais também no âmbito doméstico, considerando as lacunas existentes no ordenamento jurídico internacional expostas no capítulo anterior.

A análise cingiu-se às AJB uma vez que somente nos espaços onde pode ser exercido algum grau de jurisdição nacional é possível examinar se isso ocorre adequadamente, sendo abordado que a discussão existente sobre a definição de AJB adotada pelo Brasil, apesar de relevante para outras temáticas, é despicienda para o desenvolvimento deste estudo.

Quanto ao exercício da jurisdição brasileira nos diversos espaços marinhos, foi abordado que ocorre de formas substancialmente distintas, marcadas pelo exercício da soberania no mar territorial (ainda que limitada pelos institutos da passagem inocente e jurisdição do Estado de bandeira) e pela jurisdição funcional marcada pela fruição de direitos soberanos na ZEE e na PC, onde as competências são bem mais restritas. Essa diferenciação se mostrou fundamental para a percepção dos limites jurídicos à atuação estatal como resposta à atividade de interceptação.

Por último, foram apreciados os instrumentos jurídicos aplicáveis (ou ao menos potencialmente aplicáveis) à segurança da infraestrutura de cabos, evidenciando que o ordenamento interno dispõe de um conjunto relevante de normas, políticas, estratégias que podem ser manejadas para essa finalidade, mas que, assim como é verificado no plano internacional, é fragmentado. Da análise desses instrumentos, ficou constatado que a

abordagem incide sobre a dimensão física e operacional dos sistemas de cabos submarinos, não havendo abordagem direta da interceptação. Foi analisado o PL nº 270/2025 como importante iniciativa para o estabelecimento de um marco regulatório específico, sobretudo no que diz respeito à criminalização de condutas, mas que também não prevê expressamente a possibilidade de interceptação, merecendo aprimoramento diante de aspectos como os princípios da legalidade e proporcionalidade. A atuação da Marinha do Brasil nas suas duas vertentes (Autoridade Marítima e Poder Naval) também foi analisada, constatando-se que a primeira se encontra em estágio de normatização robusto e com atribuições bem delimitadas, não se podendo dizer o mesmo quanto à segunda vertente, que ainda carece de aprimoramentos em razão das peculiaridades próprias que permeiam o tema.

Em síntese, o capítulo demonstrou que o Estado brasileiro dispõe de bases jurídicas e mecanismos institucionais suficientes para atuar na proteção dos cabos submarinos nas águas sob a sua jurisdição sob a perspectiva das ameaças não intencionais (*maritime safety*), ainda que essa atuação necessite de aprimoramentos em razão da fragmentação normativa e coordenação interagências. Por outro lado, a ausência de leis e normas específicas quanto às ameaças intencionais e as limitações ao exercício da soberania nos espaços marítimos, sobretudo na ZEE e na PC, evidenciam a necessidade de melhorias no plano jurídico interno, aspecto que se lança em direção às conclusões finais do presente trabalho.

7 CONCLUSÃO

Desde a instalação do primeiro cabo submarino na Europa, ligando as cidades de Dover (Inglaterra) a Calais (França), naquela época com tecnologia telegráfica, a comunicação mundial vem experimentando um crescimento constante do fluxo de dados trafegados, em razão da necessidade cada vez maior de troca de informações, figurando a Internet como elemento fundamental para o funcionamento dos diversos modelos de atividades desenvolvidas atualmente. Ao analisar a evolução histórica dos cabos submarinos, desde os sistemas telegráficos do século XIX até as atuais redes de fibra óptica, ficou evidenciado que essas infraestruturas sempre estiveram associadas a interesses estratégicos, razão pela qual não podem ser tratadas como de menor importância e negligenciadas.

No contexto contemporâneo, a análise demonstrou que os cabos submarinos assumem uma relevância qualitativa, na medida em que concentram a quase totalidade do fluxo global de dados, inclusive comunicações governamentais, financeiras, militares e pessoais. Essa relevância importou o reconhecimento desses ativos como infraestruturas críticas, cuja proteção ultrapassa a lógica tradicional da segurança das comunicações e passa a permear questões de soberania, segurança nacional e proteção de direitos fundamentais. A dependência estrutural dos Estados em relação a essas infraestruturas amplia de maneira significativa os potenciais impactos que qualquer dano ou interferência podem causar.

A distinção entre os danos físicos aos cabos submarinos e as ameaças incidentes sobre os dados revela-se relevante, pois embora o Direito Internacional do Mar tenha desenvolvido um sistema normativo relativamente consolidado para lidar com os danos materiais aos cabos — especialmente aqueles de natureza accidental —, o mesmo não se verifica em relação às ameaças informacionais, como a interceptação clandestina de dados. Ao compreender essa dualidade normativa, foi possível verificar a existência de uma lacuna específica quanto à proteção da dimensão imaterial dos cabos submarinos, que não se confunde com a proteção física da infraestrutura, mas que apresenta relevância jurídica e estratégica.

A caracterização da interceptação de dados como uma ameaça híbrida é elemento essencial à perfeita compreensão da dimensão do problema. Demonstrou-se que a interceptação não se enquadra nas categorias tradicionais de ameaças, mas tampouco pode ser reduzida a uma prática meramente técnica ou neutra. Trata-se de uma conduta que se situa na interseção entre o domínio físico, cibernético e informacional, explorando vulnerabilidades estruturais das infraestruturas globais de comunicação em proveito de interesses estratégicos

estatais. Essa compreensão permite afastar leituras simplificadoras da questão e reforçar a necessidade de uma abordagem jurídica, capaz de dialogar com diferentes regimes normativos do Direito Internacional.

Diferenciar as técnicas possíveis de interceptação mostrou-se relevante para deixar claro que o foco da pesquisa não reside na comprovação de que operações de interceptação realizadas diretamente nos cabos submarinos no leito do mar são atualmente viáveis, mas sim nas suas implicações jurídicas, uma vez que a exposição sucinta de algumas técnicas reconhecidas por especialistas, ainda que sem maiores aprofundamentos em aspectos tecnológicos e operacionais, são suficientes para evidenciar, se não a sua comprovação, pelo menos seu potencial risco, o que já seria suficiente para justificar o estudo do tema. Nessa seara, a existência de divergências doutrinárias quanto à possibilidade de interceptação dos cabos na sua fase marinha não compromete a relevância do problema jurídico analisado, uma vez que o Direito Internacional deve ser capaz de lidar com riscos plausíveis e potenciais, sobretudo quando são considerados os constantes avanços tecnológicos.

Os ensinamentos colhidos de casos históricos e notáveis de interceptação de comunicações evidencia que não se trata de fenômeno novo, mas sim a manifestação contemporânea de uma prática historicamente consolidada nas relações internacionais. A abordagem dos episódios como o *All Red Line*, Telegrama Zimmermann, a Operação *Ivy Bells*, o caso do *Room 614A* e as revelações trazidas por Edward Snowden comprovam que a interceptação das comunicações sempre foi utilizada como instrumento de espionagem e projeção de poder, ainda que frequentemente envolta em sigilo e tolerância prática. Essa continuidade histórica reforça a premissa de que a ausência de regulamentação específica não decorre da inexistência do fenômeno, mas sim da dificuldade do Direito Internacional em disciplinar práticas estatais sensíveis.

Desse modo, concluiu-se que a interceptação de dados em cabos submarinos constitui um problema jurídico relevante e autonomamente identificável, cuja análise exige a articulação entre diferentes campos da ciência jurídica, incluindo o Direito do Mar, o Direito Internacional geral, o Direito Internacional dos Direitos Humanos, regimes emergentes de cibersegurança, o Direito da Guerra e outros. Delimitado o objeto de pesquisa e demonstrada a sua relevância jurídica, foram lançadas as bases conceituais necessárias para o desenvolvimento do tema, especialmente no que se refere à ilicitude da interceptação e como o Direito Internacional pode enfrentar o problema, justificando a necessidade de uma pesquisa aprofundada sobre os limites normativos relacionados ao fenômeno.

Foram estabelecidos os fundamentos conceituais, técnicos e jurídicos necessários à compreensão da interceptação de dados em cabos submarinos no âmbito do Direito Internacional. Ficou demonstrado que a interceptação não pode ser analisada de maneira isolada, mas deve ser compreendida como um fenômeno jurídico complexo, pois se encontra assentado na confluência entre conceitos jurídicos inter-relacionados como soberania, regimes jurídicos dos espaços marítimos, atividades de inteligência e Direitos Humanos. À vista disso, foi delimitado o que se entende conceitualmente por interceptação de dados em cabos submarinos, caracterizada pelo acesso não autorizado, sigiloso e unilateral de comunicações alheias, e que representa verdadeira espécie de espionagem, distinguindo essa prática de outras modalidades de acesso ou tratamento de informações.

Embora os meios tecnológicos evoluam, a lógica da interceptação permanece a mesma, conforme indicado pela análise das técnicas históricas e contemporâneas de interceptação, reforçando a premissa de que a discussão jurídica não depende da viabilidade técnica, mas de sua potencialidade e de seus efeitos jurídicos, sendo desnecessários debates excessivamente técnicos que poderiam obscurecer a análise normativa.

O tratamento conferido à espionagem difere se considerado em tempo de paz ou guerra, de modo que, neste último, o Direito Internacional apresenta disposições específicas, enquanto no primeiro existe um vácuo normativo. Tal fato leva à situação de ambiguidade representada pela condenação da prática dessa atividade por Estados quando, ao mesmo tempo, a executam, criando um ambiente de insegurança jurídica fomentado por comportamentos contraditórios.

A partir de uma leitura sistemática da doutrina especializada e de instrumentos como o Manual Tallin 2.0, que tem forte interseção com o escopo do presente trabalho, ficou exposto que ações de interceptação podem ser consideradas violadoras da soberania estatal e que esta não se restringe apenas ao território físico, estendendo-se também ao ambiente cibernético e, desta forma, será considerada ilícita a interceptação se ocorrer nos limites do mar territorial, resguardando-se outras disposições que vierem a definir diversamente outras restrições e parâmetros.

Com relação à interceptação eventualmente ocorrida na Zona Econômica Exclusiva, os especialistas opinam de maneira distinta, não havendo consenso quanto à violação ou não da soberania nesse espaço marítimo, havendo quem sustente posicionamentos para ambos os lados.

Ao tratar do princípio da não intervenção, ficou caracterizado que a interceptação pode violar este princípio do Direito Internacional se for dotada de coercitividade, não sendo

suficiente a mera interferência para considerá-la ilícita. Entretanto, a caracterização da coerção não se restringe à comprovação do uso da força, ficando configurada a intervenção como ilícita que importar na ação ou omissão do Estado prejudicado contra a sua vontade, que deverá ser avaliada contextualmente.

Para além dos interesses estatais, foi apresentado que as ações de interceptação são potencialmente violadoras de direitos humanos, em especial o direito à privacidade, conforme demonstrou casos históricos de interceptação em massa de maneira indiscriminada. A discussão elucidou que há um ponto de contato entre o Direito Internacional dos Direitos Humanos e os aspectos do Direito Internacional geral afetos à segurança, destacando-se que, ainda que as práticas de interceptação possam ser justificadas sob um prisma securitário, devem observar parâmetros de legalidade e proporcionalidade.

Destacou-se que a interceptação de dados não pode ser enquadrada no conceito de investigação científica marinha, eis que não atende aos seus requisitos de finalidade essencialmente científica, transparência e cooperação, previstos na CNUDM. Também, apesar da existência de controvérsias a respeito, ficou evidenciado que o seu enquadramento no bojo da definição de outros usos lícitos do mar é incompatível com os fins pacíficos de regência do alto-mar.

Desta feita, ficou consolidada a compreensão de que a interceptação, em si mesma, não é violadora do Direito Internacional, mas que poderá ser caso seja exercida em violação à soberania, configurar intervenção coercitiva estatal ou afetar Direitos Humanos, ficando estabelecidas as bases conceituais para a análise jurídica do regime internacional aplicável aos cabos submarinos.

Essa análise do regime jurídico foi realizada de forma sistêmica com a finalidade de verificar quais seriam as normas de Direito Internacional de incidência, com especial atenção às suas potencialidades e limitações, identificando-se a CNUDM como eixo central da análise em razão das suas abrangentes disposições. A Convenção desempenha um papel fundamental na regulação dos cabos submarinos ao estabelecer direitos, liberdades e obrigações relativos a sua colocação, manutenção e reparo nos diferentes espaços marítimos, refletindo um equilíbrio delicado entre a garantia da comunicação internacional e a proteção dos interesses soberanos dos Estados costeiros. Ao longo do exame dos seus dispositivos, ficou notório que a sua preocupação principal recai sobre a integridade física da infraestrutura, inexistindo previsão expressa ou implícita suficientemente clara voltada à proteção do fluxo de dados em si, nem em relação à regulação de práticas de interceptação.

Ao detalhar o tratamento conferidos aos cabos submarinos nas diferentes zonas marítimas, a análise evidenciou que o grau de jurisdição do Estado costeiro varia de acordo com o regime jurídico de cada zona. No mar territorial, a soberania do Estado costeiro permite uma ampla margem regulatória, possuindo o direito de adotar leis e regulamentos para dispor sobre a matéria, ainda que limitada pelo direito de passagem inocente, direito esse que pode ser condicionado em prol da proteção da infraestrutura de cabos.

Na ZEE, a CNUDM assegura a todos os Estados o direito de instalar cabos submarinos, desde que em respeito aos direitos de soberania do Estado costeiro sobre os recursos naturais desse espaço geográfico. Nesse sentido, confere a Convenção o direito ao Estado costeiro adotar regulamentação para resguardar a fruição desses direitos na ZEE, marcando a sua natureza híbrida de coexistência de direitos soberanos do Estado costeiro de um lado, e da liberdade dos demais Estados de outro.

A Convenção prevê para a plataforma continental o mesmo regime jurídico aplicável aos cabos submarinos na ZEE, exceto quando ultrapassar as 200 milhas marítimas, quando então somente será aplicável o regime próprio da PC, de modo que o Estado costeiro também deve suportar o direito dos demais Estados instalar cabos, bem como pode adotar regulamentação voltada à adequada fruição dos direitos próprios dessa zona.

No alto-mar prevalece a lógica da liberdade de colocação dos cabos submarinos, estipulando a Convenção a obrigação do Estado costeiro adotar leis e regulamentos sancionatórios às condutas danosas cometidas por navios que arvoem a sua bandeira ou por pessoa que esteja submetida à sua jurisdição, fomentando o exercício da jurisdição penal, mas de maneira restrita a estas duas hipóteses.

Prevê também a Convenção para o alto-mar a obrigação regulamentadora do Estado costeiro voltada à responsabilização de natureza civil do proprietário de cabo que durante a sua operação cause danos a outros cabos, preconizando a obrigatoriedade de indenizar os custos da reparação. Ainda, dispõe a CNUDM a necessidade de regulamentação destinada a indenizar os proprietários de navios que sacrificaram seus equipamentos para evitar a ocorrência de danos aos cabos submarinos, incentivando a proteção dessas infraestruturas.

Como último ponto de disposição da CNUDM, eventual controvérsia que incida sobre o exercício de direitos soberanos ou de jurisdição de uma parte e a liberdade de

colocação e operação dos cabos de outra, poderá ser submetida ao sistema de solução estabelecido na Convenção.

A síntese analítica das disposições convencionais demonstra que há uma ampla liberdade de instalação de cabos submarinos nos diversos espaços marítimos, contrastando com a imposição de obrigações de regulamentação de proteção que dependem da efetiva atuação dos Estados, o que muitas vezes não ocorre, bem como da insuficiência no que tange às medidas de cunho cibernético, não contemplado no texto convencional.

Para compreender o alcance do Direito Internacional para tutelar o tema, foram analisadas outras normas e instrumentos de incidência. O exame da Convenção de Cabos de 1884 permitiu constatar que apesar de ter sido pioneiro e ainda possua alguma aplicabilidade complementar, especialmente no que se refere a aspectos procedimentais relativos a danos físicos aos cabos, sua eficácia é diminuta em razão do reduzido número de Estados-parte, além do que as suas disposições também não abarcam a dimensão cibernética dos dados.

A análise de outros instrumentos conexos que contém alguma menção aos cabos submarinos, como o RIPEAM, a Convenção de Londres de 1972 e o seu Protocolo de 1996, as normas do Direito Internacional aplicável à guerra e as convenções sobre terrorismo revelam apenas uma proteção indireta e circunstancial, eis que são aplicáveis apenas em contextos específicos, não sendo capazes de responder de maneira direta a questão da interceptação de dados em tempos de paz. Ficou denotado que o recurso a esses regimes revela mais uma tentativa doutrinária de suprir lacunas do que uma solução jurídica satisfatória.

Da análise das recomendações de natureza técnica do ICPC, ficou abalizado que cumprem papel relevante ao difundir boas práticas entre os diversos *stakeholders* envolvidos. Entretanto, suas disposições dotadas de caráter não vinculativo, bem como a ausência de qualquer abordagem sobre a proteção do fluxo de dados ou sobre interceptação, revelam que são insuficientes para solucionar os desafios jurídicos centrais analisados neste trabalho.

O diagnóstico do regime internacional de incidência vigente é no sentido de que o quadro normativo internacional é marcado por lacunas estruturais, sendo a mais relevante delas a inexistência de disposições específicas voltadas à tutela do conteúdo informacional transmitido pelos cabos submarinos. A proteção conferida pelo Direito Internacional permanece concentrada na dimensão material dos sistemas de cabos, deixando desprotegida a dimensão imaterial dos dados, justamente aquela que assume maior relevância estratégica no

contexto das relações internacionais. Essa constatação leva à conclusão de que, à luz do Direito Internacional clássico, as atividades de interceptação de dados em cabos submarinos, sobretudo se realizadas além dos limites do mar territorial, se situam em uma zona cinzenta normativa permeada por uma maléfica permissividade jurídica, favorecendo práticas lesivas à soberania estatal, denotando a necessidade de estabelecimento de um regime normativo específico que busque preencher as lacunas verificadas.

A partir desse diagnóstico, avançou-se em direção à análise das alternativas possíveis para o estabelecimento de um regime internacional que seja adequado às ameaças contemporâneas. Mediante investigação das consequências da ausência de regulação, ficou constatado que o vazio normativo não representa um problema meramente teórico, mas que produz efeitos concretos e sistêmicos, sendo o primeiro deles a insegurança jurídica, marcada por um ambiente no qual eventuais atividades de interceptação prejudiciais ao bom funcionamento do sistema não podem ser evitadas de maneira eficaz.

A falta de regulamentação específica favorece também a normalização de práticas unilaterais por Estados dotados de maior recursos tecnológicos, o que tende a ampliar assimetrias de poder no sistema internacional, em detrimento da igualdade dos Estados. Soma-se, ainda, o risco elevado de violações de direitos humanos, ameaças à soberania estatal e à estabilidade das relações internacionais, assim como potenciais impactos econômicos globais relevantes favorecidos por um ambiente de impunidade.

O exame das principais propostas doutrinárias e institucionais revelou que, apesar da crescente conscientização internacional da importância dos cabos submarinos, as respostas normativas permanecem insuficientes. No âmbito das Nações Unidas, os trabalhos do GGE e do OEWG reafirmam a aplicabilidade do Direito Internacional ao ciberespaço e a importância das infraestruturas críticas, mas não avançam na elaboração de normas vinculantes específicas sobre a interceptação de dados. A atuação da ITU, ainda que relevante sob o ponto de vista técnico e cooperativo, limita-se a fóruns consultivos e declarações de caráter não vinculante. No plano regional e setorial, iniciativas como as do ICPC e da ENISA contribuem para o fortalecimento da resiliência física e operacional dos cabos, mas não enfrentam a questão da interceptação de dados, concentrando-se em recomendações de boas práticas. O estudo das propostas doutrinárias reforçou esse diagnóstico, convergindo os entendimentos dos especialistas no que diz respeito à insuficiência do regime atual, mas evidenciando uma

divergência acerca do melhor caminho normativo a ser seguido, variando entre interpretações evolutivas da CNUDM e a defesa de um novo tratado internacional especializado.

A averiguação das modalidades de regulação internacional possíveis permitiu demonstrar que não há solução única ou imediata para o *deficit* normativo identificado. Os mecanismos de *soft law* se apresentam como alternativa pragmática e politicamente viável no curto prazo, capazes de estabelecer padrões mínimos e fomentar a cooperação internacional, todavia, carentes de força vinculante. Os tratados regionais, por seu turno, apresentam maior densidade normativa e capacidade de comprometimento entre os Estados participantes, mas enfrentam limitações geográficas, sobretudo quando se considera a característica intercontinental típica dos cabos submarinos. Já a adoção de uma convenção multilateral global desponta como a solução mais abrangente e sistematicamente coerente, porém, a sensibilidade com qual a interceptação de dados é tratada impõe obstáculos diplomáticos de superação improvável no curto prazo, inviabilizando a assunção de compromissos que importem na sua abstenção.

Como conteúdo material mínimo de um regime normativo internacional sobre interceptação de dados em cabos submarinos, o estudo sistematizou elementos que qualquer instrumento que venha a ser proposto, seja ele vinculante ou não, deveria contemplar para ser efetivo. Nessa direção, apresenta-se como necessária a expressa proibição da interceptação clandestina em tempo de paz, superando a atual zona cinzenta do Direito Internacional. A previsão de diretrizes claras de cooperação e notificação também se mostra necessária como medida apta a reduzir tensões e prevenir a escalada de conflitos. Outra medida imperativa é a criminalização interna e o efetivo exercício da jurisdição pelos Estados, que devem se comprometer nesse sentido, como forma de coibir a prática ilícita. Igualmente necessária é a definição de mecanismos de responsabilização estatal e reparação dos danos causados, apresentando-se como viáveis os sistemas de resolução consolidados pela CNUDM. Como última medida e de maneira particularmente relevante, o reconhecimento explícito de que a interceptação ilícita de dados configura violação de direitos humanos, conferindo à proteção contra interceptação de cabos submarinos maior densidade normativa e institucional, permitindo, inclusive, o acionamento de mecanismos internacionais existentes de tutela desses direitos.

A identificação desse vazio normativo, a análise das propostas de debate, das possibilidades de modalidades regulatórias, bem como a sistematização do conteúdo desejável

de um futuro instrumento fornecem as balizas necessárias para se adentrar na parte final da pesquisa, voltada à análise dos desafios e competências do Estado brasileiro frente as ameaças de interceptação de cabos nas Águas Jurisdicionais Brasileiras.

No caso brasileiro, demonstrou-se que o debate sobre a (in)compatibilidade com o Direito do Mar do conceito interno de AJB não é relevante para a análise desenvolvida na presente pesquisa, uma vez que, independentemente da controvérsia sobre a possibilidade ou não do exercício de jurisdição sobre a coluna d'água sobrejacente à PC estendida, os cabos encontram-se pousados no leito marinho, portanto, submetidos à jurisdição do Estado costeiro na sua extensão.

Após a análise sistemática das competências jurisdicionais em cada espaço marítimo considerado, constatou-se que, sob os auspícios do Direito do Mar, o Brasil possui reduzidas possibilidades de atuação em face de eventuais casos de interceptação clandestina de cabos submarinos.

No mar territorial, apesar de a CNUDM afirmar a soberania plena do Estado costeiro, mitigada apenas pelos institutos da passagem inocente e da jurisdição do Estado de bandeira, na prática apenas poderiam ser adotadas medidas necessárias para impedir ou fazer cessar a interceptação, limitando-se a ações de menor coercitividade e sem fazer uso da força, salvo nas hipóteses autorizadas pelo ordenamento internacional. Para atos perpetrados por navios de guerra ou por outros navios de Estado, as medidas são ainda mais restritas, limitando-se à exigência de saída imediata e busca pela responsabilização do Estado de bandeira no plano internacional. A possibilidade da adoção de medidas coercitivas, de investigação e penalização não são contempladas pelo Direito do Mar, de modo que eventuais providências dessa natureza dependem de previsão no ordenamento jurídico interno, o que não há, ficando, então, ao arbítrio do Estado de bandeira aplicar a sua jurisdição sobre os seus navios e nacionais.

Na ZEE e na PC, o Direito do Mar não confere competência para o exercício de jurisdição sobre atividades de interceptação de cabos submarinos, não permitindo que um navio de guerra brasileiro aborde ou apreenda uma embarcação suspeita de praticar tais atividades, salvo se houver violação concreta aos seus direitos de soberania afetos à fruição de recursos econômicos e em caso de dano ambiental. Mesmo que a legislação brasileira criminalize a interceptação, isso recairia apenas sobre nacionais e navios com bandeira brasileira, por força da sistemática estabelecida pela CNUDM.

O exame dos instrumentos jurídicos brasileiros revelou que o ordenamento jurídico doméstico ainda não dispõe de nenhum instrumento dedicado exclusivamente à proteção dos cabos submarinos, evidenciando que o Brasil ainda não efetivou a obrigação imposta pela CNUDM quanto à adoção de leis e regulamentos sancionatórios a danos nessas infraestruturas. O tripé regulatório das infraestruturas críticas no Brasil revela forte conteúdo programático a ser alcançado, demonstrando a relevância político-estratégica desses ativos, todavia, suas disposições ainda são carentes de medidas concretas, assim como ocorre no âmbito internacional.

O PL nº 270/2025, ainda em tramitação por ocasião do encerramento da presente pesquisa, surge como uma tentativa de colmatar as lacunas e estabelecer um marco regulatório interno das infraestruturas de cabos. Todavia, quanto ao aspecto da repressão penal das atividades de interceptações ilícitas, apesar do seu texto contemplar a criminalização de condutas que atentem contra o perfeito funcionamento do sistema de cabos, sua redação encontra óbice no princípio da legalidade, de modo que, caso seja assim aprovada, sua aplicação em face das atividades de interceptação ilícita pode ser refutada. A análise apresentou também que não se mostra correto dogmaticamente o enquadramento das condutas de interceptação clandestina de cabos submarinos ao crime de espionagem tal como tipificado no Código Penal brasileiro, uma vez que são distintos os seus elementos, sendo desejável a criação de um tipo penal específico voltado à interceptação dos dados em cabos.

O Brasil tem avançado significativamente na proteção de suas infraestruturas críticas mediante o estabelecimento de normas nos níveis político, estratégico e operacional, mas ainda existem lacunas normativas consideráveis, sobretudo considerando que a sua abordagem atual incide apenas sobre a dimensão física e operacional dos cabos submarinos, assim como se verifica no plano internacional.

A Marinha do Brasil desempenha papel relevante na proteção das infraestruturas de cabos submarinos, atuando ora como Poder Naval com atuação voltada à defesa da pátria e viés de *maritime security*, e ora como Autoridade Marítima com escopo de atuação voltado para a segurança da navegação e viés de *maritime safety*. Quanto a este último modo de atuação, ficou demonstrado ser dotado de robusta regulamentação, a qual se mostra satisfatória para uma resposta a danos não intencionais. Por outro lado, o mesmo não pode ser dito quanto às atribuições afetas ao Poder Naval, uma vez que a ausência de disposições

específicas sobre danos intencionais e interceptação acabam por limitar uma resposta estatal que seja eficaz.

Portanto, conclui-se pela confirmação da hipótese de pesquisa no sentido de que o arcabouço jurídico atualmente vigente, tanto no plano internacional quanto no nacional, é inadequado para a proteção jurídica da infraestrutura de cabos submarinos nas AJB, especialmente quanto às interceptações clandestinas e outras ameaças intencionais.

REFERÊNCIAS

ANATEL. **Informe N° 192/2023/COQL/SCO**. Cabos submarinos como infraestrutura crítica: recomendações convergentes entre Agência Nacional de Telecomunicações (Anatel) e Gabinete de Segurança Institucional (GSI/PR). Brasília, 2025. 15 p. Disponível em: https://sei.anatel.gov.br/sei/controlador_externo.php?acao=documento_conferir&codigo_verificador=10791528&codigo_crc=064304DA&hash_do_wnload=cdf86eaea69d5f8e34c5ccc2612e56c963717d8ad46a821774c1a68007414e84d5a669b200b923c94f245a89ee6f13d16002b8f147be9138ca46dbfb4f00efaf&visualizacao=1&id_orgao_acesso_externo=0. Acesso em: 06 abr. 2025.

ANDRADE, Isabela Piacentini de. Responsabilidade internacional do estado por violação do jus cogens. **Revista Brasileira de Direito Internacional**, Curitiba, v. 5, 2007. Disponível em: <https://scholar.google.com.br/scholar?cluster=17469165120405723883&hl=pt-BR&as_sdt=0,5>. Acesso em: 19 jan. 2026.

AZARIA, Danai; DAVENPORT, Tara. **Interim Report**. International Law Association, Committee on Submarine Cables and Pipelines in International Law. 2020. 42 p. Relatório. Disponível em: <<https://discovery.ucl.ac.uk/id/eprint/10149627/>>. Acesso em: 22 dez. 2025.

BADIN, Michelle Ratton Sanchez; KROETZ, Maria Eugênia do Amaral; MORAIS, Ana Maria; MISRA, Manu. Infraestrutura crítica e o controle de investimento externo: a regulação do Brasil em contraste. **Boletim de Economia e Política Internacional – BEPI**, n. 36, p. 27-58, 2024. Disponível em: <<https://repositorio.ipea.gov.br/server/api/core/bitstreams/db575f6b-493a-49b1-848a-e417e37a8610/content>>. Acesso em: 6 jan. 2026.

BARRETO, Rafael Zelesco. El concepto de Aguas Jurisdiccionales Brasileñas y la protección de los espacios marinos internacionales por el Estado ribereño. **Revista de Derecho Público**, n. 101, p. 19-45, 2024. DOI 10.5354/0719-5249.2024.76541. Disponível em: <<https://pt.scribd.com/document/895425437/Zelesco-Vf>>. Acesso em: 29 dez. 2025.

BAUDER, Harald; MUELLER, Rebecca. Westphalian vs. indigenous sovereignty: challenging colonial territorial governance. **Geopolitics**, v. 28(1), p. 156–173, 2021. <https://doi.org/10.1080/14650045.2021.1920577>.

BECKMAN, Robert. Protecting submarine cables from intentional damage - the security gap. In: BURNETT, Douglas R.; BECKMAN Robert C.; DAVENPORT, Tara M. **Submarine cables: the handbook of law and policy**. Leiden: Martinus Nijhoff Publishers, 2014, p. 281-297.

BEIRÃO, André Panno. O complexo exercício da jurisdição penal no mar. **Revista de Direito e Negócios Internacionais da Maritime Law Academy - International Law and Business Review**, v. 3, n. 2, p. 104–134, 26 dez. 2023.

BEIRÃO, A. P. Políticas públicas voltadas ao mar: um longo caminho já iniciado. In: SANTOS, Thauan; BEIRÃO, André P.; ARAÚJO FILHO, Moacyr C.; CARVALHO, Andréa B. (org.). **Economia Azul: vetor para o desenvolvimento do Brasil**. Rio de Janeiro: Essential Idea, nov. 2022. Disponível em:

<https://ciencianomar.mctic.gov.br/wp-content/uploads/2023/08/Economia-Azul_vetor-para-o-desenvolvimento-do-Brasil.pdf>. Acesso em: 25 mar. 2025.

BEIRÃO, André Panno. Segurança no mar: que segurança? *In*: BEIRÃO, André Panno; PEREIRA, Antônio Celso Alves (org.). **Reflexões sobre a Convenção do Direito do Mar**. Brasília: FUNAG, 2014. 589 p. Disponível em: <https://funag.gov.br/loja/download/1091-Convencao_do_Direito_do_Mar.pdf>. Acesso em: 28 out. 2025.

BELARMINO, Misael Aguiar. **Investigação científica marinha: aspectos jurídicos**. 2020. 120 f. Dissertação (Mestrado em Estudos Marítimos) - Escola de Guerra Naval, Rio de Janeiro, 2020.

BETTAUER, Ronald J. Questions relating to the seizure and detention of certain documents and data (Timor-Leste v. Australia). **American Journal of International Law**, v. 108, n. 4, p. 763-769, 2014.

BID. **Cybersecutity report 2025: vulnerability and maturity challenges to bridging the gaps in Latin America and the Caribeean**. Washington, DC: Inter-American Development Bank, 2025. 191 p. Relatório. Disponível em: <<https://publications.iadb.org/en/2025-cybersecurity-report-vulnerability-and-maturity-challenges-bridging-gaps-latin-america-and>>. Acesso em: 31 jan. 2026.

BOTUA, Hafidz L; DEWI, Chloryne Trie Isana; SISWANDI, R. Achmad Gusman Catur. Wiretapping on Submarine Communications Cable: questioning its legality amidst long standing practice. **Padjadjaran Journal of International Law**, v. 6, n. 1, p. 20-42, 2022. DOI 10.23920/pjil/v6i1.772. Disponível em: <https://www.academia.edu/87217874/Wiretapping_on_Submarine_Communications_Cable_Questioning_Its_Legality_Amidst_Long_Standing_Practice>. Acesso em: 24 ago. 2025.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 07 out. 2025.

BRASIL. **Decreto Legislativo nº 45, de 15 de outubro de 1968**. Autoriza o Presidente da República a dar adesão do Governo brasileiro a quatro Convenções sobre o Direito do Mar, concluídas em Genebra, a 29 de abril de 1958. Diário do Congresso Nacional, Poder Legislativo, Brasília, DF, 16 out. 1968. Seção 1. p. 7215. Disponível em: <<https://www2.camara.leg.br/legin/fed/decleg/1960-1969/decretolegislativo-45-15-outubro-1968-346852-publicacaooriginal-1-pl.html>>. Acesso em: 02 nov. 2025.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Diário Oficial da União, Poder Executivo, Brasília, DF, 31 dez. 1940. p. 23911. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm>. Acesso em: 6 jan. 2026.

BRASIL. **Decreto nº 1.530, de 22 de junho de 1995**. Declara a entrada em vigor da Convenção das Nações Unidas sobre o Direito do Mar, concluída em Montego Bay, Jamaica, em 10 de dezembro de 1982. Diário Oficial da União, Poder Executivo, Brasília, DF, 23 jun. 1995. Seção 1. p. 9199. Disponível em: <https://www2.camara.leg.br/legin/fed/decret/1995/decreto-1530-22-junho-1995-435606-publicacaooriginal-1-pe.html>. Acesso em: 27 nov. 2024.

BRASIL. **Decreto nº 4.394, de 26 de setembro de 2002.** Promulga a Convenção Internacional sobre a Supressão de Atentados Terroristas com Bombas, com reserva ao parágrafo 1 do art. 20. Diário Oficial da União, Poder Executivo, Brasília, DF, 29 set. 2002. Seção 1. p. 5. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto/2002/d4394.htm>. Acesso em: 06 nov. 2025.

BRASIL. **Decreto nº 5.417, de 13 de abril de 2005.** Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções Gratificadas do Comando da Marinha, do Ministério da Defesa, e dá outras providências. Diário Oficial da União, Poder Executivo, Brasília, DF, 14 abr. 2005. Seção 1. p. 1. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2005/decreto/d5417.htm>. Acesso em: 8 jan. 2026.

BRASIL. **Decreto nº 9.573, de 22 de novembro de 2018.** Aprova a Política Nacional de Segurança de Infraestruturas Críticas. Diário Oficial da União, Poder Executivo, Brasília, DF, 23 nov. 2018. Seção 1. p. 40. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/d9573.htm. Acesso em: 30 nov. 2024.

BRASIL. **Decreto nº 9.843, de 14 de janeiro de 1888.** Manda que se observe o Regulamento para execução das bases adoptadas pela Convenção internacional de 14 de Março de 1884, com o fim de proteger os cabos submarinos. Coleção de Leis do Império do Brasil – 1888, p. 61, v. 1. Disponível em: <https://www2.camara.leg.br/legin/fed/decret/1824-1899/decreto-9843-14-janeiro-1888-542179-publicacaooriginal-49834-pe.html>. Acesso em: 21 dez. 2024.

BRASIL. **Decreto nº 10.569, de 9 de dezembro de 2020.** Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas. Diário Oficial da União, Poder Executivo, Brasília, DF, 10 dez. 2020. Seção 1. p. 8. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10569.htm. Acesso em: 30 nov. 2024.

BRASIL. **Decreto nº 11.200, de 15 de setembro de 2022.** Aprova Plano Nacional de Segurança de Infraestruturas Críticas. Diário Oficial da União, Poder Executivo, Brasília, DF, 16 set. 2022. Seção 1. p. 9. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Decreto/D11200.htm. Acesso em: 30 nov. 2024.

BRASIL. **Decreto nº 12.725, de 18 de novembro de 2025.** Aprova a Política Nacional de Defesa, a Estratégia Nacional de Defesa e o Livro Branco de Defesa Nacional. Diário Oficial da União, Poder Executivo, Brasília, DF, 19 nov. 2025. Edição 221, seção 1. p. 2. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/D12725.htm>. Acesso em: 03 jan. 2026.

BRASIL. **Decreto nº 19.841, de 22 de outubro de 1945.** Promulga a Carta das Nações Unidas, da qual faz parte integrante o anexo Estatuto da Corte Internacional de Justiça, assinada em São Francisco, a 26 de junho de 1945, por ocasião da Conferência de Organização Internacional das Nações Unidas. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto/1930-1949/d19841.htm>. Acesso em: 28 set. 2025.

BRASIL. **Decreto nº 56.435, de 8 de junho de 1965.** Promulga a Convenção de Viena sobre Relações Diplomáticas. Disponível em:

<https://www.planalto.gov.br/ccivil_03/decreto/antigos/d56435.htm>. Acesso em: 06 nov. 2025.

BRASIL. Decreto nº 80.068, de 2 de agosto de 1977. Promulga a Convenção sobre o Regulamento Internacional para Evitar Abalroamentos no Mar, 1972. Diário Oficial da União, Poder Executivo, Brasília, DF, 01 set. 1977. Seção 1. p. 11.554. Disponível em: <<https://www2.camara.leg.br/legin/fed/decret/1970-1979/decreto-80068-2-agosto-1977-428971-publicacaooriginal-1-pe.html>>. Acesso em: 19 dez. 2025.

BRASIL. Decreto nº 87.566, de 16 de setembro de 1982. Promulga o texto da convenção sobre Prevenção da Poluição Marinha por Alijamento de Resíduos e Outras Matérias, concluída em Londres, a 29 de dezembro de 1972. Diário Oficial da União, Poder Executivo, Brasília, DF, 17 set. 1982. Seção 1. p. 17.484. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto/1980-1989/1980-1984/D87566.htm>. Acesso em: 19 dez. 2025.

BRASIL. Instrução Normativa nº 3/MB/MD, de 15 de dezembro de 2022. Estabelece o conceito para a expressão “Águas Jurisdicionais Brasileiras” perante a Marinha do Brasil. Diário Oficial da União, Poder Executivo, Brasília, DF, 16 dez. 2022. Seção 1. p. 72. Disponível em: <<https://www.marinha.mil.br/sites/default/files/atos-normativos/gcm/in-3-2022-mb-md.html>>. Acesso em: 29 dez. 2025.

BRASIL. Lei Complementar nº 97, de 9 de junho de 1999. Dispõe sobre as normas gerais para a organização, o preparo e o emprego das Forças Armadas. Poder Executivo, Brasília, DF, 10 jun. 1999. Publicado em diário extra. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp97.htm>. Acesso em: 7 jan. 2026.

BRASIL. Lei nº 9.296, de 24 de julho de 1996. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Diário Oficial da União, Poder Executivo, Brasília, DF, 25 jul. 1996. P. 13757. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/19296.htm>. Acesso em: 26 jan. 2026.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Diário Oficial da União, Poder Executivo, Brasília, DF, 24 abr. 2014. Seção 1. p. 1. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 15 ago. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Diário Oficial da União, Poder Executivo, Brasília, DF, 15 ago. 2018. Seção 1. p. 59. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm>. Acesso em: 5 jan. 2026.

BRASIL. Lei nº 14.197, de 1º de setembro de 2021. Acrescenta o Título XII na Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), relativo aos crimes contra o Estado Democrático de Direito; e revoga a Lei nº 7.170, de 14 de dezembro de 1983 (Lei de Segurança Nacional), e dispositivo do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais). Diário Oficial da União, Poder Executivo, Brasília, DF, 2 set. 2021. Seção 1. p. 3. Disponível em:

<https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Lei/L14197.htm#art2>. Acesso em: 6 jan. 2026.

BRASIL. Marinha do Brasil. **Fundamentos Doutrinários da Marinha** (EMA-301), 1ª edição. Brasília, DF, 2023. Disponível em: <<https://www.marinha.mil.br/sites/default/files/ema-301-fdm-1ed.pdf>>. Acesso em: 7 jan. 2026.

BRASIL. Marinha do Brasil. **Política Naval**. Brasília, DF, 2019. Disponível em: <<https://www.marinha.mil.br/politicanaval>>. Acesso em: 7 jan. 2026.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **Portaria GSI/PR nº 93, de 18 de outubro de 2021**. Aprova o glossário de segurança da informação. Diário Oficial da União, Poder Executivo, Brasília, DF, 19 out. 2021. Seção 1. p. 36. Disponível em: <<https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-93-de-18-de-outubro-de-2021-353056370>>. Acesso em: 24 ago. 2025.

BRASIL. **Projeto de Lei nº 270, de 5 de fevereiro de 2025**. Institui a Política Nacional de Infraestruturas de Cabos Subaquáticos (PNICS) e dá outras providências. Brasília, 2025. Disponível em: <<https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2482914>>. Acesso em: 6 jan. 2026.

BRASIL. **Resolução nº 740, de 21 de dezembro de 2020**. Aprova o Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações. Diário Oficial da União, Poder Executivo, Brasília, DF, 24 dez. 2020. Seção 1. p. 55. Disponível em: <<https://informacoes.anatel.gov.br/legislacao/resolucoes/2020/1497-resolucao-740>>. Acesso em: 11 out. 2025.

BRASIL. Supremo Tribunal Federal (2. Turma). Inquérito 4720. Princípio da legalidade penal e da proibição da analogia in malam partem. Relator: Edson Fachin, Relator para o Acórdão: Gilmar Mendes. Julgado em 22 ago. 2021. **Diário da Justiça Eletrônico** nº 238. Publicado em 2 dez. 2021. Disponível em: <<https://jurisprudencia.stf.jus.br/pages/search/sjur456894/false>>. Acesso em: 6 jan. 2026.

BRUTON, Elizabeth. **The cable wars: military and state surveillance of the british telegraph cable network during world war one**. Historicizing Infrastructure, 2017. Disponível em: https://www.academia.edu/37096519/_The_Cable_Wars_Military_and_State_Surveillance_of_the_British_Telegraph_Cable_Network_During_World_War_One?auto=download. Acesso em 02 set. 2025.

BUCHAN, R. J. **The International Legal Regulation of Cyber Espionage**. In: OSULA, A-M; RÖIGAS, H (Eds.). International cyber norms: legal, policy & industry perspectives. NATO CCD COE Publications, Tallinn, Estonia. p. 65–86. ISBN 9789949954469, 9789949954476.

BUEGER, Christian; EDMUNDS, Timothy. Beyond seablindness: a new agenda for maritime security studies. **International Affairs**, v. 93, n. 6, p. 1293-1311, 2017. Disponível em: <<https://scholar.google.com.br/citations?user=p31l-xsAAAAJ&hl=pt-BR&oi=sra>>. Acesso em: 24 jan. 2026.

BUEGER, Christian; LIEBETRAU, Tobias. **Protecting hidden infrastructure: The security politics of the global submarine data cable network**. Contemporary Security Policy, 2021, v. 42, n. 3, p. 391-413, mar. 2021.

BUENO, Cassio Scarpinella. **Manual de direito processual civil**, v. único. 5ª ed. São Paulo: Saraiva, 2019.

BUENO, Guilherme. **Paz de Vestfália: guerra dos 30 anos, soberania, sistema de estados e o jogo do poder**. ESRI, 2024. Disponível em: <<https://esri.net.br/entenda-a-paz-de-vestfalia>> Acesso em: 25 set. 2025.

BUFITHIS, Gregory. **The cable wars: surveillance of the British telegraph cable networking during World War One**. Publicado em 15 jul. 2021. Atualizado em 01 ago. 2021. Disponível em: < https://www.gregorybufithis.com/2021/07/15/the-cable-wars-surveillance-of-the-british-telegraph-cable-network-during-world-war-one/?utm_source=chatgpt.com>. Acesso em: 03 set. 2025.

BURNETT, Douglas R. **Submarine cable security and international law**. International Law Studies, v. 97, p. 1659-1682, 2021.

BURNETT, Douglas R. The 1884 international convention for protection of submarine cables provisions not in UNCLOS deserve attention now. In: **Workshop on the Protection of Submarine Cables**, Singapore. 2011. p. 14-15. Disponível em: <https://cil.nus.edu.sg/wp-content/uploads/2011/04/Douglas-Burnett_1884_International_Convention_for_Protection_of_Submarine_Cables_Provisions_Not_in_UNCLOS_De1.pdf>. Acesso em: 12 dez. 2025.

CARVALHO FILHO, José dos Santos. **Manual de Direito Administrativo**. 32. ed. São Paulo: Atlas, 2018. ISBN 978-85-97-01589-8.

CARVALHO, Manuela Bocayuva. **Os meios para a solução de controvérsias previstos na Convenção das Nações Unidas sobre o Direito do Mar de 1982**. 2018. 122 f. Dissertação (Mestrado profissionalizante em Direito Internacional e Relações Internacionais) – Faculdade de Direito, Universidade de Lisboa, Lisboa, Portugal, 2018.

CARVALHO, Phelipe Swiantek de. Ações telemáticas desenvolvidas exclusivamente sobre aplicativos de trocas de mensagens instantâneas. **RECIMA21 - Revista Científica Multidisciplinar**, v. 4, n. 12, 2023. Disponível em <<https://recima21.com.br/index.php/recima21/article/view/4653>>. Acesso em: 24 jan. 2026.

CASTILHO, Carlos Alberto Campos. **A segurança cibernética na proteção das infraestruturas críticas brasileiras**. 2023. 25 f. Trabalho de Conclusão de Curso (Curso Superior de Segurança e Defesa Cibernética) – Departamento de Altos Estudos, Escola Superior de Guerra, Rio de Janeiro, 2023. Disponível em: <https://repositorio.esg.br/bitstream/123456789/1931/1/Ensaio_Academico_Cel_CASTILHO_EB%20%281%29.pdf>. Acesso em: 6 jan. 2026.

CATE, Fred H.; KUNER, Christopher; SVANTESSON, Dan Jerker B.; LYNSKEY, Orla; MILLARD, Christopher. The Rise of Cybersecurity and Its Impact on Data Protection. **International Data Privacy Law**, 2017, v. 2, n. 2. Disponível em:

<https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=3634&context=facpub>. Acesso em: 14 jan. 2026.

CCDCOE. **International Law Applies to Cyber Operations, Tallinn Manual 2.0 Reaffirms**. Tallinn, 2025. Disponível em: <<https://ccdcoe.org/news/2017/international-law-applies-to-cyber-operations-tallinn-manual-2-0-reaffirms/>>. Acesso em: 27 jan. 2026.

CEIA, Eleonora Mesquita. O impacto do Tratado de Lisboa sobre o treaty-making power e o processo de conclusão de tratados internacionais pela União Europeia. **Novos Estudos Jurídicos**, v. 16, n. 2, p. 170-187, 2011. Disponível em: <<https://periodicos.univali.br/index.php/nej/article/view/3279>>. Acesso em: 18 jan. 2026.

CENTRE FOR INTERNATIONAL LAW. **1884 Convention for the Protection of Submarine Telegraph Cables**. Última modificação em 03 out. 2024. Disponível em: <<https://cil.nus.edu.sg/databasecil/1884-convention-for-the-protection-of-submarine-telegraph-cables-3/>>. Acesso em: 12 dez. 2025.

CHESTERMAN, Simon. The spy who came in from the Cold War: Intelligence and international law. **Michigan Journal of International Law**, v. 27, p. 1071, 2006. Disponível em: <https://scholar.google.com/scholar?hl=pt-BR&as_sdt=0%2C5&q=Simon+Chesterman%2C+The+Spy+Who+Came+in+from+the+Cold+War%3A+Intelligence+and+International+Law%2C+27&btnG=>>. Acesso em: 16 set. 2025.

CHIRCOP, Luke. Territorial sovereignty in cyberspace after 'Tallinn Manual 2.0'. **Melbourne journal of international law**, v. 20, n. 2, p. 349-377, 2019. Disponível em: <https://law.unimelb.edu.au/__data/assets/pdf_file/0004/3533746/Chircop-advance-copy.pdf>. Acesso em: 15 set. 2025.

CIA. **Reports on USS submarine spying on soviets 25 years old**. Washington: Central Intelligence Agency, 1986. 2 p. Relatório. Disponível em: <<https://www.cia.gov/readingroom/docs/CIA-RDP90-00965R000605470008-5.pdf>> Acesso em: 03 set. 2025.

CIJ. **Questions relating to the seizure and detention of certain documents and data (Timor-Leste v. Australia)**. Haia: Corte Internacional de Justiça, 2014, p. 147. Relatório. Disponível em: <<https://www.icj-cij.org/sites/default/files/case-related/156/156-20140303-ORD-01-00-EN.pdf>>. Acesso em 27 jan. 2026.

CONSELHO DA EUROPA. **Convenção Europeia de Direitos Humanos**. Conselho da Europa, Roma, 1950. Disponível em: <https://www.echr.coe.int/documents/d/echr/convention_por>. Acesso em: 07 out. 2025.

CORTE INTERNACIONAL DE JUSTIÇA. **Atividades militares e paramilitares na e contra a Nicarágua (Nicarágua v. Estados Unidos da América)**. Julgamentos de mérito, Relatórios da CIJ, v.14, 1986.

COSTA, Álvaro Mayrink da. Direito Penal e proteção dos bens jurídicos. **Revista da EMERJ**, v. 14, n. 53, p. 7-15, 2011. Disponível em: <https://www.emerj.tjrj.jus.br/revistaemerj_online/edicoes/revista53/Revista53_7.pdf>. Acesso em: 15 jan. 2026.

DAVENPORT, Tara. Submarine cables, cybersecurity and international law: an intersectional analysis. **Catholic University Journal of Law and Technology**, v. 24, n. 1, p. 57-109, dez. 2015.

DEPARTAMENTO DE POLÍCIA FEDERAL. **Instrução Normativa nº 2, de 5 de agosto de 1999**. Disciplina a Organização e o Funcionamento das Atividades dos Núcleos Especiais de Polícia Marítima (NEPOM), estabelece competências e atribuições e dá outras providências. Brasília, 1999. Disponível em: <https://www.marinha.mil.br/dpc/sites/www.marinha.mil.br.dpc/files/legislacao/instru-normativa/inst_norm2.pdf>. Acesso em: 9 jan. 2026.

DEVANNY, Joe; MARTIN, Ciaran; STEVENS, Tim. On the strategic consequences of digital espionage. **Journal of Cyber Policy**, v. 6, n. 3, p. 429-450, 2021. Disponível em: <<https://www.tandfonline.com/doi/pdf/10.1080/23738871.2021.2000628>> Acesso em: 16 set. 2025.

DPC. **Missão, visão de futuro e valores**, 2026. Disponível em: <<https://www.marinha.mil.br/dpc/institucional/miss%C3%A3o-vis%C3%A3o-de-futuro-e-valores-organizacionais>>. Acesso em: 8 jan. 2026.

ENISA. **Commission recommendation of 26.2.2024 on secure and resilient submarine cable infrastructures**, Bruxelas, 2024. Disponível em: <<https://digital-strategy.ec.europa.eu/en/library/recommendation-security-and-resilience-submarine-cable-infrastructures>>. Acesso em: 17 jan. 2026.

EVANS, Graham; PAGE, Monique. The planning and surveying of submarine cable routes. *In*: BURNETT, Douglas; BECKMAN, Robert C.; DAVENPORT, Tara M (ed.). **Submarine cables: the handbook of law and policy**. Leiden: Martinus Nijhoff Publishers, 2014. cap. 4, p. 93-122.

FARIA, Duarte Lynce. Os cabos submarinos: infraestruturas críticas que desafiam a jurisdição de Portugal e do Direito Internacional. **Nação e Defesa**, n. 169, p. 43-84, 2024. Disponível em: <<https://revistas.rcaap.pt/nacao/article/view/40245>>. Acesso em: 05 dez. 2025.

FLINDERS, Rede; SMALLEY, Ian. **What is log analysis with AI?** IBM site. Nova Iorque, 2025. Disponível em: <<https://www.ibm.com/think/topics/ai-for-log-analysis>>. Acesso em: 5 jan. 2026.

FORD-RAMSDEN, Keith; DAVENPORT, Tara M. The manufacture and laying of submarine cables. *In*: BURNETT, Douglas R.; BECKMAN Robert C.; DAVENPORT, Tara M. **Submarine cables: the handbook of law and policy**. Leiden: Martinus Nijhoff Publishers, 2014.

FRAZIER, Kevin. Policy proposals for the United States to protect the undersea cable system. **Journal of Law, Technology and the Internet**, 2021, v. 13, n. 1. Disponível em: <https://scholar.google.com.br/citations?view_op=view_citation&hl=pt-BR&user=V0cJ09kAAAAJ&citation_for_view=V0cJ09kAAAAJ:u-x6o8ySG0sC>. Acesso em: 17 jan. 2026.

GALLAGHER, Jill C. **Undersea telecommunication cables: technology overview and issues for congress**. Washington: Library of Congress, 2022. 25 p. Relatório. Disponível em: <https://www.everycrsreport.com/files/2022-09-13_R47237_a284971dfaed5fa65bc26fe860ed7d5d2985d242.pdf>. Acesso em: 06 fev. 2026.

GILL, Terry G. Non-intervention in the cyber context. *In*: ZIOLKOLWSKI, Katharina (ed.). **Peacetime regime for state activities in cyberspace: international law, international relations na diplomacy**. Tallinn: NATO CCD COE Publication, 2013. p. 217-237.

GÓES, Guilherme de Toledo; SANTIN, Janice. Uma definição de Estado Democrático de Direito para o direito penal: democracia combativa e crimes contra as instituições democráticas. **Revista do Instituto de Ciências Penais**, Belo Horizonte, v. 9, n. 1, p. 116-156, 2024. DOI: 10.46274/1809-192XRICP2024v9n1p116-156. Disponível em: <<https://www.ricp.org.br/index.php/revista/article/view/181>>. Acesso em: 6 jan. 2026.

GONÇALVES, Marcus Vinicius Rios. **Direito processual civil esquematizado**. 2ª ed. São Paulo: Saraiva, 2012.

GRECO, Rogério. **Curso de Direito Penal: parte geral, volume 1**. 19ª ed. Niterói: Impetus, 2017. 984 p. ISBN 978-85-7626-930-4.

GREEN, Mick; BURNETT, Douglas. Protecting cables engaged in cable operations. *In*: BURNETT, Douglas R.; BECKMAN Robert C.; DAVENPORT, Tara M. **Submarine cables: the handbook of law and policy**. Leiden: Martinus Nijhoff Publishers, 2014.

GREENWALD, Glenn. **No place to ride: Edward Snowden, the NSA and the Surveillance State**. Londres: Penguin Books Ltd, 2014. ISBN: 978-0-241-96900-7. Disponível em: <[https://ia800802.us.archive.org/25/items/pdfy-jczuhqxxCAsjKlM0/no%20place%20to%20hide%20\(edward%20snowden%20and%20glen%20greenwald\)%20complete.pdf#page=168.85](https://ia800802.us.archive.org/25/items/pdfy-jczuhqxxCAsjKlM0/no%20place%20to%20hide%20(edward%20snowden%20and%20glen%20greenwald)%20complete.pdf#page=168.85)>. Acesso em 02 set. 2025.

GRISHACHEV, V. **Traffic intercept in optical network: method of optical tunneling**. Photonics. v. 14, n. 8, p. 280-294, 2020. DOI: 10.22184/1993-7296.Fros.2020.14.8.680.695. Disponível em: <https://www.photonics.su/files/article_pdf/8/article_8588_157.pdf>. Acesso em: 25 ago. 2025.

GUEDES, Armando M. Marques. Introdução ao Direito da Guerra. **Revista Negócios Estrangeiros**, Lisboa, v. 10, p. 175-203, fev. 2007. Disponível em: <https://idi.mne.gov.pt/images/Revista_NE/PDF/19-2007_02_n_10.pdf>. Acesso em: 19 dez. 2025.

GUZMAN, Andrew T.; MEYER, Timothy L. International soft law. **Journal of Legal Analysis**, v. 2, n. 1, p. 171-225, 2010. Disponível em: <<https://academic.oup.com/jla/article/2/1/171/846831?login=false>>. Acesso em: 22 dez. 2025.

HEINEGG, Wolff Heintschel Von. **Protecting critical submarine cyber infrastructure: legal status and protection of submarine communications cables under international law**. *In*: ZIOLKOLWSKI, Katharina (ed.). **Peacetime regime for state activities in cyberspace: international law, international relations na diplomacy**. Tallinn: NATO CCD COE Publication, 2013. p. 291-318.

IBGE. **Atlas geográfico escolar: ensino fundamental – do 6º ao 9º ano**. 2 ed. Rio de Janeiro: IBGE, 2015. 170 p. ISBN 978-85-240-4358-1. Disponível em: <<https://biblioteca.ibge.gov.br/index.php/biblioteca-catalogo?view=detalhes&id=2100881.pdf>>. Acesso em: 29 dez. 2025.

ICPC. **Government Best Practices for protecting and promoting resilience of submarine telecommunications cables**, [ca. 2020), version 1.2, 12 p. Disponível em: <<https://www.iscpc.org/publications/icpc-best-practices/>>. Acesso em: 17 jan. 2026.

ICPC. **ICPC Recommendations**. Londres, 2024. Disponível em: <<https://www.iscpc.org/publications/recommendations/>>. Acesso em: 22 dez. 2025.

IMO. **Convention on the Prevention of Marine Pollution by Dumping of Wastes and Other Matter**. Londres, 2025. Disponível em: <<https://www.imo.org/en/ourwork/environment/pages/london-convention-protocol.aspx>>. Acesso em: 19 dez. 2025.

ITU. **Facts and figures 2024**. Disponível em: <<https://www.itu.int/itu-d/reports/statistics/2024/11/10/ff24-internet-use/>>. Acesso em: 08 set. 2025.

JENSEN, Eric Talbot. The Tallinn manual 2.0: Highlights and insights. **Geo. J. Int'l L.**, v. 48, p. 735, 2016. Disponível em: <<https://heinonline.org/HOL/LandingPage?handle=hein.journals/geojintl48&div=30&id=&page=>>> Acesso em: 15 set. 2025.

JORNAL DA ECONOMIA DO MAR. **A nova realidade dos cabos submarinos**. X Grande Conferência do Jornal de Economia do Mar (57 min). Disponível em: <<https://www.youtube.com/watch?v=lhbZNMlKUlc&t=2038s>>. Acesso em: 24 ago. 2025.

KELLO, Lucas. **The virtual weapon and international order**. New Haven: Yale University Press, 2017. ISBN 978-03-002-2023-0. Disponível em: <<https://dokumen.pub/the-virtual-weapon-and-international-order-9780300226294.html>>. Acesso em: 6 jan. 2026.

KHADER, Eliana; FRANÇA, Gisela. O conceito de bem jurídico na doutrina de Juarez Tavares. **Boletim IBCCRIM**. Ano 32, n. 374, p. 9-14, jan. 2024. Disponível em: <https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/795>. Acesso em: 15 jan. 2026.

KWAN, Martin Yat-cheung. Gaps in accountability for submarine cable protection: inadequacies in the current Legal framework. **Ocean and Coastal Law Journal**, v. 30, n. 1, p. 1-30, 2025. Disponível em: <Gaps in Accountability for Submarine Cable Protection: Inadequacies in the Current Legal>. Acesso em: 04 dez. 2025.

LEINER, Barry M. et al. **A brief history of the Internet**. ACM SIGCOMM computer communication review, v. 39, n. 5, p. 22-31, 2009. Disponível em: <https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-History-of-the-Internet_1997.pdf>. Acesso em: 08 set. 2025.

LONGO, Airton Ronaldo. O debate em busca do consenso – as negociações para os termos finais da Convenção da Jamaica. In: BEIRÃO, André Panno; PEREIRA, Antônio Celso Alves (org.). **Reflexões sobre a Convenção do Direito do Mar**. Brasília: FUNAG, 2014. 589 p. Disponível em: <https://funag.gov.br/loja/download/1091-Convencao_do_Direito_do_Mar.pdf>. Acesso em: 28 out. 2025.

LUBIN, Asaf. **A espionagem como direito soberano no direito internacional e seus limites**. ILSA Quart., v. 24, p. 22, 2015. Disponível em: <<https://heinonline.org/HOL/LandingPage?handle=hein.jessup/ilsaqrtly0024&div=30&id=&page=>>>. Acesso em: 08 set. 2025.

MARGOLIS, Gabriel. **The lack of HUMINT: a recurring intelligence problem**. Global Security Studies, v. 4, issue 2, 2013. Disponível em: https://www.academia.edu/37164453/The_Lack_of_HUMINT_A_Recurring_Intelligence_Problem. Acesso em: 02 set. 2025.

MARINHA DO BRASIL. **Estratégia de Defesa Marítima (EMA-310)**. 1ª Ed. Brasília: Estado-Maior da Armada, 2023. Disponível em: <<https://www.marinha.mil.br/sites/default/files/ema-310-edm-1ed.pdf>>. Acesso em: 8 jan. 2026.

MARINHA DO BRASIL. **Normas da Autoridade Marítima para Obras e Atividades Afins em Águas sob Jurisdição Brasileira (NORMAM-303/DPC)**. Rio de Janeiro: Diretoria de Portos e Costas, 2023. Disponível em: <<https://www.marinha.mil.br/dpc/normas-e-legisla%C3%A7%C3%B5es>>. Acesso em: 8 jan. 2026.

MARTINS, Eliane Maria Octaviano. **Curso de Direito Marítimo, volume I**. 3 ed. Barueri: Manole, 2008. ISBN 978-85-204-2674-6.

MELLO FILHO, Eduardo Cavalcanti; GUEDES, Henrique Lenon Farias. **O modelo tradicional do Direito do Mar e a proteção de interesses da comunidade**. In: MENEZES, Wagner (org.). Direito Internacional em expansão. Volume XII. Anais do 15º Congresso Brasileiro de Direito Internacional. Belo Horizonte: Arraes Editores, 2017. cap. 17, p. 268-286.

MENEZES, Wagner. **O Direito do Mar**. Brasília: FUNAG, 2015. 238 p. ISBN 978-85-7631-548-3. Disponível em: <https://funag.gov.br/loja/download/1119-O_Direito_do_Mar.pdf>. Acesso em: 30 dez. 2025.

MORAN, Christopher R.; BURTON, Joe; CHRISTOU, George. The U.S. intelligence community, global security, and AI: from secret intelligence to smart spying. **Journal of Global Security Studies**, v. 8, 2023. Disponível em: <<https://doi.org/10.1093/jogss/ogad005>> Acesso em: 18 set. 2025.

NAJEM, Fawaz; ALJAHANI, Abdelnaser. The legality of espionage in peacetime. **Access to Justice in Eastern Europe**. p. 120-151, 2025. Disponível em: <https://ajee-journal.com/upload/attaches/att_1755430699.pdf>. Acesso em: 27 jan. 2025.

NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION. **Submarine cables - international framework**. Última modificação em 24 jul. 2025. Disponível em:

<<https://www.noaa.gov/general-counsel/gc-international-section/submarine-cables-international-framework>>. Acesso em: 12 dez. 2025.

OCDE. **Digital security risk management for economic and social prosperity**: OECD recommendation and companion document. Paris: OECD Publishing, 2015. Disponível em: <https://www.oecd.org/en/publications/digital-security-risk-management-for-economic-and-social-prosperity_9789264245471-en.html>. Acesso em 15 jan. 2026.

OEA. **Convenção Americana de Direitos Humanos**. Conferência Interamericana Especializada sobre Direitos Humanos, 1969. Disponível em: <<https://www.oas.org/pt/cidh/mandato/Basicos/convencion.asp>>. Acesso em: 07 out. 2025.

OLIVEIRA, Liziane Paixão Silva; BERTOLDI, Márcia Rodrigues. A importância do soft law na evolução do direito internacional. In: **XIX Congresso Nacional do CONPEDI**. 2010. p. 6265-6289. Disponível em: <https://www.cidp.pt/revistas/ridb/2012/10/2012_10_6265_6289.pdf>. Acesso em 20 jan. 2026.

OLMOS, Olívia Martins de Quadros; FAVERA, Rafaela Bolson Dalla. A Ciberespionagem e a Privacidade sob o Crivo dos Direitos Humanos. **Direito & TI**, [S. l.], v. 1, n. 5, p. 5, 2016. DOI: 10.63451/ti.v1i5.57. Disponível em: <<https://direitoeti.com.br/direitoeti/article/view/57>>. Acesso em: 28 jan. 2026.

ONU. Assembleia Geral. **Declaração Universal dos Direitos Humanos**. Resolução nº 217A, Sessão III, 1948. Disponível em: <https://brasil.un.org/sites/default/files/2025-03/ONU_DireitosHumanos_DUDH_UNICRio_20250310.pdf>. Acesso em: 06 out. 2025.

ONU. Assembleia Geral. **Pacto Internacional sobre Direitos Civis e Políticos**. Resolução nº 2200A, Sessão XXI, 1969. Disponível em: <<https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>>. Acesso em: 06 out. 2025.

ONU. Assembleia Geral. **Resolução nº 65/37, de 7 de dezembro de 2010**. Dispõe sobre questões relevantes relativas à Convenção das Nações Unidas sobre o Direito do Mar. Disponível em: <https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_RES_65_37.pdf>. Acesso em: 27 nov. 2024.

ONU. **Comentário Geral nº 16 do CCCP: artigo 17 (direito à privacidade), o direito ao respeito à privacidade, à família, ao lar e à correspondência, e à proteção da honra e da reputação**. Nova Iorque: Comitê de Direitos Humanos, 1988. 3 p. Disponível em: <<https://www.refworld.org/legal/general/hrc/1988/en/27539>>. Acesso em: 20 jan. 2026.

ONU. **Developments in the Field of Informations and Telecommunications in the Context of International Security**. A/75/816. Nova Iorque: Assembleia Geral, 2021. 38 p. Relatório. Disponível em: <<https://docs.un.org/en/A/75/816>>. Acesso em 16 jan. 2026.

ONU. **Report of Group of Governmental Experts on Developments in the Field of Informations and Telecommunications in the Context of International Security**.

A/70/174. Nova Iorque: Assembleia Geral, 2015. 17 p. Relatório. Disponível em: <<https://undocs.org/A/70/174>>. Acesso em: 16 jan. 2026.

ONU. **The right to privacy in the digital age.** A/HRC/27/37. Nova Iorque: Conselho de Direitos Humanos, 2014. 16 p. Relatório. Disponível em: <<https://undocs.org/A/HRC/27/37>>. Acesso em: 16 jan. 2026.

ONU. **United Nations Convention against Cybercrime.** A/Res/79/43. Nova Iorque: Assembleia Geral, 2024. Disponível em: <<https://www.unodc.org/unodc/en/cybercrime/convention/home.html>>. Acesso em: 18 jan. 2026.

PAIK, Amy Min-Jung. **Building an International Regulatory Regime in Submarine Cables and Global Marine Communications.** 2022. Tese de Doutorado. The Johns Hopkins University. Disponível em: <https://jscholarship.library.jhu.edu/server/api/core/bitstreams/b291352c-ef99-4036-bb09-c6085c61c5ae/content>. Acesso em: 12 jan. 2026.

PANORAMA. **XVIII Podcast: a geopolítica dos cabos submarinos.** Apresentação de Alexandre Alves e participação de Luís Manuel Brás Bernardino, 12 ago. 2025, 16 min. Podcast. Disponível em: <<https://www.youtube.com/watch?v=uj1MPGl-r1I>>. Acesso em: 24 ago. 2025.

PEDROZO, Raul Pete. Implementing Agreement to Enhance Protection of Critical Undersea Infrastructure. **International Law Studies**, v. 106, n. 1, p. 7, 2025. Disponível em: <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=3104&context=ils>. Acesso em: 12 jan. 2026.

PEDROZO, Raul Pete. Safeguarding and submarine cables and pipelines in times of peace or war. **International Law Studies**, v. 106, p. 45-65, 2025.

PEREIRA, Antônio Celso Alves; PEREIRA, João Eduardo de Alves. A liberdade de alto-mar – antecedentes históricos dos artigos de 87 a 90 da Convenção das Nações Unidas sobre o Direito do Mar. In: BEIRÃO, André Panno; PEREIRA, Antônio Celso Alves (org.). **Reflexões sobre a Convenção do Direito do Mar.** Brasília: FUNAG, 2014. 589 p. Disponível em: <https://funag.gov.br/loja/download/1091-Convencao_do_Direito_do_Mar.pdf>. Acesso em: 28 out. 2025.

PETTY, Jason. How hackers of submarine cables may be held liable und law of the sea. **Chicago Journal of International Law**, v. 22, n. 1, p. 260-298, 2021. Disponível em: <<https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1810&context=cjil>>. Acesso em: 12 dez. 2025.

PIÑON, Charles Pacheco. **A liberdade de navegação e as medidas de restrição e controle do tráfego marítimo na proteção de infraestruturas críticas.** 2016. 186 f. Dissertação (Mestrado em Estudos Marítimos) – Programa de Pós-Graduação em Estudos Marítimos – PPGEM, Escola de Guerra Naval, Rio de Janeiro, 2016. Disponível em: <<https://repositorio.marinha.mil.br/handle/ripcmb/26362>>. Acesso em: 8 jan. 2026.

PIRKER, Benedikt. Territorial sovereignty integrity and the challenges of the cyberspace. In: ZIOLKOLWSKI, Katharina (ed.). **Peacetime regime for state activities in cyberspace: international law, international relations na diplomacy**. Tallinn: NATO CCD COE Publication, 2013. p. 189-216.

POKEMPNER, Dinah. Cyberspace and state obligations in the área of human rights. In: ZIOLKOLWSKI, Katharina (ed.). **Peacetime regime for state activities in cyberspace: international law, international relations na diplomacy**. Tallinn: NATO CCD COE Publication, 2013. p. 239-260.

PONTIERI, Alexandre. **Marco civil da internet**. Consultor Jurídico, 2022. Disponível em: <<https://www.conjur.com.br/2022-abr-24/alexandre-pontieri-marco-civil-internet>>. Acesso em: 04 set. 2025.

PUN, Darien. **Rethinking espionage in the modern era**. Chicago Journal of International Law, v. 18, p. 353, 2017.

RAHA, Utpal Kumar; RAJU, K. D. **Submarine Cables Protection and Regulations: A comparative analysis and model framework**. Singapore: Springer Nature, 2021. DOI: <https://doi.org/10.1007/978-981-16-3436-9>.

RAIDMA, Kristi. **Tallinn Manual 2.0 – the invaluable guide for state action in cyber space**. Estonian World, 2017. Disponível em: <<https://estonianworld.com/security/tallinn-manual-2-0-invaluable-guide-state-action-cyber-space/>>. Acesso em: 27 jan. 2026.

RAMOS, André de Carvalho. Responsabilidade internacional do Estado por violação de direitos humanos. **Revista CEJ**, v. 9, n. 29, p. 53-63, 2005. Disponível em: <<https://scholar.google.com.br/citations?user=CrYs-NQAAAAJ&hl=pt-BR&oi=sra>>. Acesso em: 19 jan. 2026.

ROACH, J. Ashley; SMITH, Robert W. **Excessive Maritime Claims**. 3. ed. Leiden: Martinus Nijhoff Publishers, 2012.

ROSA, Cândido do Nascimento Alves. **Princípio da legalidade no sistema de precedentes à brasileira: a interpretação do STJ do princípio da legalidade aplicado ao Direito Penal em decisões qualificadas como precedentes**. 2024. 165 f. Dissertação (Mestrado em Direito, Regulação e Políticas Públicas) – Faculdade de Direito, Universidade de Brasília, Brasília, 2024. Disponível em: <https://repositorio.unb.br/bitstream/10482/50512/1/CandidoDoNascimentoAlvesRosa_DISSERT.pdf>. Acesso em: 6 jan. 2026.

SCHALLER, Christian. **Sabotagem of submarine cables and pipelines as a use of force and armed attack**. International Law Studies, v. 106, p. 173-205, 2025.

SCHMITT, Michael N. (Ed.). **Tallinn manual 2.0 on the international law applicable to cyber operations**. Cambridge University Press, 2017. Disponível em: <https://csrcl.huji.ac.il/sites/default/files/csrl/files/9781107177222_frontmatter.pdf>. Acesso em: 15 set. 2025.

SEMERARO, G. M.; NASSER, S. H. A conceituação do terrorismo: uma apresentação do campo nacional e global. **Campos Neutrais**. Rio Grande. v. 7, n. 2. p. 22-39, maio./ago. 2025. ISSN 2596-1314. Disponível em: <<https://periodicos.furg.br/cn/article/view/19870/12031>>. Acesso em: 22 dez. 2025.

SENADO FEDERAL. Espionagem cibernética: rede vulnerável. **Revista Em Discussão: os principais debates do Senado Federal**. Brasília: Senado Federal, Secretaria de Comunicação Social, v. 5, n. 21, jul. 2014. 66 p. Disponível em: <<https://www12.senado.leg.br/noticias/acervo-historico/em-discussao>>. Acesso em: 28 jan. 2026.

SENADO FEDERAL. **Relatório Final nº 1, de 2014**. Brasília: CPI da Espionagem, 2014. 322 p. Relatório. Disponível em: <<https://www2.senado.leg.br/bdsf/handle/id/609904>>. Acesso em: 07 fev. 2026.

SHAW, Malcolm N. **Direito Internacional**. Tradução de Marcelo Brandão Cipolla et al. São Paulo: Martins Fontes, 2010, p. 446 *apud* PEREIRA, Antônio Celso Alves; PEREIRA, João Eduardo de Alves. A liberdade de alto-mar – antecedentes históricos dos artigos de 87 a 90 da Convenção das Nações Unidas sobre o Direito do Mar. *In*: BEIRÃO, André Panno; PEREIRA, Antônio Celso Alves (org.). **Reflexões sobre a Convenção do Direito do Mar**. Brasília: FUNAG, 2014. 589 p. Disponível em: <https://funag.gov.br/loja/download/1091-Convencao_do_Direito_do_Mar.pdf>. Acesso em: 28 out. 2025.

SHVETS, Daria. **The international legal regime of submarine cables: a global public interest regime**. 2020. 386 f. Tese (PhD) - Pompeu Fabra University, Barcelona, Espanha, 2020. Disponível em: <https://www.tesisenred.net/bitstream/handle/10803/671344/tds.pdf?sequence=1&isAllowed=y>. Acesso em: 12 jan. 2026.

SOUZA, Luciano Anderson de. **Direito Penal: parte especial, volume 5**. Ed. 2023. São Paulo: Thomson Reuters Brasil, 2023. ISBN 978-65-260-0134-9. Disponível em: <<https://www.jusbrasil.com.br/doutrina/secao/801consideracoes-iniciais-capitulo-80-espionagem-art-359-k-direito-penal-vol-5-ed-2023/2092822832#a-323283465>>. Acesso em: 6 jan. 2026.

SILVA, Juracy Aparecida da. Aspectos da União Europeia e do Mercosul no âmbito do Direito. **APUD ACTA Revista jurídica**, v. 3127, p. 6, 2019. Disponível em: <https://uniesp.edu.br/sites/_biblioteca/revistas/20190131183356.pdf#page=19>. Acesso em: 18 jan. 2026.

STATISTA. **Global internet penetration rate as february 2025, by region**. Publicado em: 13 fev. 2025. Disponível em: <<https://www.statista.com/statistics/269329/penetration-rate-of-the-internet-by-region/>>. Acesso em: 08 set. 2025.

STOCO, Tatiana. Espionagem e a revelação de segredos estatais: uma análise do artigo 359-K, §4º, do Código Penal. **Revista do Instituto de Ciências Penais**. Belo Horizonte, v. 8, n. 1, p. 43-68, 2023. DOI: 10.46274/1809-192XRICP2023v8n1p43-68. Disponível em: <https://www.ricp.org.br/index.php/revista/article/view/141>. Acesso em: 6 jan. 2026.

SUNAK, Rishi. Undersea Cable: indispensable, insecure. Londres: **Policy Exchange**, 2017. 48 p. ISBN 978-1-810812-38-9. Disponível em:

<https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf>. Acesso em: 15 ago. 2025.

SUN, Zhen. **Finding a balance in the exclusive economic zone: conflict and stability in the law of the sea**. Cambridge: Cambridge University Press, 2025. Disponível em: <<https://www.cambridge.org/core/books/finding-a-balance-in-the-exclusive-economic-zone/resolving-conflicts-regarding-unattributed-rights-and-jurisdiction-in-the-exclusive-economic-zone/BADE3E605137630FAEE81EC50A93907F>>. Acesso em: 18 jan. 2026.

TANAKA, Yoshifumi. **The International Law of the Sea**. 3 ed. Cambridge: Cambridge University Press, 2019. ISBN 978-1-108-42421-9.

TAY, Xuan W. Reconstructing the principle of non-intervention and non-interference: electoral disinformation, Nicaragua, and the quilt-work approach. **Berkeley Journal of International Law**, v. 40, p. 39-94, 2022. Disponível em: <<https://heinonline.org/HOL/LandingPage?handle=hein.journals/berkjintl40&div=6&id=&page=>>>. Acesso em: 28 set. 2025.

THE GUARDIAN. **GCHQ taps fibre-optic cables for secret access to world's communications**. Publicado em: 21 jun. 2013. Disponível em: <<https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>>. Acesso em: 03 set. 2025.

THE NEW YORK TIMES. **New nuclear sub is said to have special eavesdropping ability**. Publicado em: 16 jul. 2013. Disponível em: <<https://www.nytimes.com/2005/02/20/politics/new-nuclear-sub-is-said-to-have-special-eavesdropping-ability.html>>. Acesso em: 24 ago. 2025.

VICHI, Leonardo Perin; PINTO, Danielle Jacon Ayres; SÁ, André Luiz Nery de. A Defesa da Infraestrutura de Cabos Submarinos: por uma interface entre a defesa cibernética e a segurança marítima no Brasil. *Revista da Escola de Guerra Naval*, Rio de Janeiro, v. 26, n. 2, p. 326-346, maio/ago. 2020.

WALDEN, Ian. International telecommunications law, the Internet and the regulation of cyberspace. In: ZIOLKOLWSKI, Katharina (ed.). **Peacetime regime for state activities in cyberspace: international law, international relations na diplomacy**. Tallinn: NATO CCD COE Publication, 2013. p. 260-289.

WARGO, Robert; DAVENPORT, Tara M. Protecting submarine cables from competing uses. In: BURNETT, Douglas R.; BECKMAN Robert C.; DAVENPORT, Tara M. **Submarine cables: the handbook of law and policy**. Leiden: Martinus Nijhoff Publishers, 2014.

ZANELLA, Tiago V. Águas Jurisdicionais Brasileiras: um estudo sobre a (i) legalidade do conceito de AJB. **Revista Jurídica Luso-Brasileira**. Ano, v. 4, p. 2831-2856, 2018. Disponível em: < https://www.cidp.pt/revistas/rjlb/2018/6/2018_06_2831_2856.pdf>. Acesso em: 29 dez. 2025.

ZANELLA, Tiago V. Jurisdição penal em mar territorial brasileiro: contributo para a análise da aplicação da lei penal e poder jurisdicional sobre o Mar Territorial do Brasil. **Revista Eletrônica de Direito Internacional**, v. 13, 2014. Disponível em:

<https://www.cidp.pt/revistas/ridb/2013/14/2013_14_17741_17768.pdf>. Acesso em: 31 dez. 2025.

ZANELLA, Tiago V. **Manual de Direito do Mar**. 2 ed. São Paulo: Editora D'Plácido, 2025. 880 p. ISBN 978-65-5150-006-0.

ZANELLA, Tiago V. **Segurança marítima: guia prático de aplicação do direito do mar (maritime law enforcement)**. Amazon, 2023. ISBN: 9798376023853. Disponível em: <https://www.academia.edu/97348317/SEGURAN%C3%87A_MAR%C3%8DTIMA_GUIA_PR%C3%81TICO_DE_APLICA%C3%87%C3%83O_DO_DIREITO_DO_MAR_MARITI_ME_LAW_ENFORCEMENT_>. Acesso em: 30 dez. 2025.

ZEGART, Amy B. **Spies, lies and algorithms: the history and the future of american intelligence**. Princetown University Press, 2022. Disponível em: <<https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/zegartmorell.pdf>> Acesso em: 16 set. 2025.

ZHANG, D.; LI, H. Research on the international legal regulation of willful or culpably negligent damage to submarine cables. **Marine Development**, n. 3, v. 19, 2025. Disponível em: <https://doi.org/10.1007/s44312-025-00064-3>. Acesso em: 12jan. 2026.

ZILLI, Marcos. Quem tem medo do direito penal internacional? **Revista Anistia Política e Justiça de Transição**, n. 8. Brasília: Ministério da Justiça, 2012, p. 132-150. Disponível em: <<https://www.gov.br/mdh/pt-br/navegue-por-temas/comissao-de-anistia/anexos/2013revistaanistia08.pdf>> Acesso em: 20 jan. 2026.

ZIOLKOWSKI, Katharina. Peacetime cyber espionage: new tendencies in public international law. In: ZIOLKOWSKI, Katharina (ed.). **Peacetime regime for state activities in cyberspace: international law, international relations na diplomacy**. Tallinn: NATO CCD COE Publication, 2013. p. 425-464.

ZUCCARO, Paulo Martino; BRAGA, André Luiz de Mello; SILVA, Rogerdson Fabiano da Costa Pereira da; FONSECA, Paulo José Chaves. **Os cabos submarinos e o poder naval brasileiro: impactos no preparo e emprego da Marinha**. Centro de Estudos Político-Estratégicos (CEPE-MB), 2025. 34 p. Relatório. Disponível em: <https://www.marinha.mil.br/cepe/sites/www.marinha.mil.br/cepe/files/Relatorio%20Tecnico_Cabos%20Submarinos.pdf>. Acesso em: 7 jan. 2026.