Per una protezione integrata dei cavi sottomarini: la legge n. 9/2026 alla prova di un paradigma *data-oriented*

Annalisa Triggiano*

SOMMARIO: 1. La vulnerabilità dei cavi sottomarini: geopolitica e diritto 2. Le iniziative europee a tutela dei cavi sottomarini: brevi cenni 3. Un "mare di dati" da solcare: verso un cambio di paradigma 3.1 Per una governance proporzionata dei dati marini: i modelli AGOR e CTR 4. L'Italia e la protezione dei cavi sottomarini: tra passato… 4.1 …presente: Il Codice delle Comunicazioni Elettroniche 4.2 … e futuro: la nuova centralità della "dimensione subacquea" 4.3 Analisi delle definizioni normative e proposte di miglioramento 4.4 L'Agenzia per la Sicurezza delle Attività Subacquee: una gestione accentrata dell'ecosistema sottomarino 5. Valutazioni conclusive e spunti di riflessione

1. *La vulnerabilità dei cavi sottomarini: geopolitica e diritto*

L'interesse verso il tema della protezione dei cavi sottomarini – nella presente indagine, i cavi per le telecomunicazioni (trasporto di dati), con esclusione dei cavi per l'energia elettrica – sorge in relazione al fatto che, da un lato, essi trasportano gran parte del

*Assegnista di Ricerca, Scuola Superiore di Studi Universitari Sant'Anna, Pisa, contributo cofinanziato dal progetto *Horizon Europe SMAUG* (S*mart Maritime and Underwater Guardian*), GA 101121129.

ISSN 2038-1662

traffico dati internazionale ([1]) e, dall'altro, si tratta di infrastrutture vulnerabili, poco protette ([2]). Come evidenziano recenti analisi ([3]), il rischio sistemico che grava su queste reti è in forte aumento, alimentato oltremodo dalle recenti tensioni geopolitiche, da sabotaggi mirati, incidenti fisici e, soprattutto, da capacità di riparazione globali poco rapide e dunque complessivamente insufficienti.

Secondo quanto riportato da alcune testate giornalistiche, solo nell'ultimo biennio sono stati registrati, pubblicamente, 44 danni a cavi sottomarini ([4]): le cause principali includono dragaggio di ancore ([5]), fenomeni naturali e attività sospette di navi legate a Russia e Cina. La guerra in Ucraina e le pressioni su Taiwan sembrano aver

([1])https://digital-strategy.ec.europa.eu/it/library/subsea-telecommunication-cables-are-essential-europes-digital-connectivity

([2])F. BECHIS, *Undersea Cables: The Great Data Race Beneath the Oceans*, ISPI, 28 maggio 2021, https://www.ispionline.it/en/pubblicazione/undersea-cables-great-data-race-beneath-oceans-30651; M. COLOMBO, F. SOLFRINI, A. VARVELLI, *Network Effects: Europe's Digital Sovereignty in the Mediterranean – European Council on Foreign Relations*, https://ecfr.eu/publication/network-effectseuropes-digital-sovereignty-in-the-mediterranean/; V. FRANCOLA, G. A. MENSAH, *L'industria dei cavi sottomarini: qualche elemento introduttivo*, in *Astrid Rassegna* (Laboratorio sull'Ecosistema Digitale Astrid, 2021)

([3]) Submarine Cable Security at Risk Amid Geopolitical Tensions & Limited Repair Capabilities

([4]) V. BALOCCO, *Sabotaggi, capacità di riparazione limitata e tensioni internazionali mettono a rischio il 99% del traffico dati mondiale*, in *Corriere Comunicazioni*, 19 agosto 2025, sul sito web https://www.corrierecomunicazioni.it/telco/cavi-sottomarini-minacce-in-aumento-necessaria-una-strategia-globale/

([5]) Sul sito web Damage to Submarine Cables from Dragged Anchors

ISSN 2038-1662

intensificato le attività di sabotaggio. Quattro incidenti nel Mar Baltico e cinque attorno a Taiwan sono stati attribuiti a manovre sospette compiute da navi di proprietà opaca ([6]). Queste operazioni, pur difficili da attribuire formalmente quanto alla loro responsabilità, sono destinate ad aumentare, sfruttando la fragilità delle rotte secondarie, la scarsa diversificazione dei percorsi e la limitata capacità di riparazione. Le zone con poche rotte alternative, come l'Africa occidentale, le isole del Pacifico e alcune tratte europee risultano particolarmente vulnerabili ([7]).

La protezione della sicurezza dei cavi sottomarini, un tempo confinata al diritto del mare, oggi coinvolge ormai questioni di sovranità, sicurezza nazionale e gestione dei dati ([8]).

Il presente contributo indaga e valorizza tale trasformazione, elaborando un modello di protezione teorico-applicativo *data-oriented* originale, capace di ricucire le fratture tra spazio marittimo e spazio informativo, superando approcci limitati e tradizionali e proponendo, alla luce del modello stesso, indicazioni di *policy* per

([6]) M. SAVINI ZANGRANDI, *Il ruolo geostrategico dei cavi sottomarini: le interconnessioni digitali come possibile ambito sanzionatorio*, in *GeoTrade: rivista di geopolitica e commercio estero*, 2, 2021, 28 ss.

([7])C. BUEGER, T. LIEBETRAU, *Protecting hidden infrastructure: The security politics of the global submarine data cable network*, in *Contemporary Security Policy*, 42, 3, 2021, 391 ss., nel sito web https://doi.org/10.1080/13523260.2021.1907129

([8]) Nel sito web https://www.ispionline.it/it/pubblicazione/cavi-sottomarini-le-nuove-autostrade-dei-dati-193654

ISSN 2038-1662

l'integrazione della recentissima normativa sulla protezione delle strutture subacquee.

Nel contesto del diritto internazionale, ampiamente sceverato in letteratura, la protezione dei cavi sottomarini si fonda su un impianto normativo ibrido, che combina convenzioni storiche come la *Convention for the Protection of Submarine Telegraph Cables* (1884) con le disposizioni (relativamente) moderne della Convenzione delle Nazioni Unite sul Diritto del Mare (UNCLOS, 1982) ([9]). La convenzione del 1884 criminalizzava, tra l'altro, il danneggiamento volontario o negligente di cavi sottomarini su acque internazionali, e imponeva obblighi di riparazione in caso di interferenze con altri cavi. La Convenzione UNCLOS, pur non recependo integralmente ogni previsione del trattato del 1884, riconosce la libertà di posa e manutenzione di cavi nei mari internazionali (art. 87) e obbliga gli Stati a prevedere sanzioni per chi danneggia tali infrastrutture (art. 113). Tuttavia, questo quadro normativo internazionale presenta lacune rilevanti, in qualche caso già evidenziate dagli studiosi ([10]) e

([9]) Si rinvia a C. VAGAGGINI, *Il regime giuridico dei cavi sottomarini: gli sviluppi normativi nello scenario internazionale, europeo e nazionale*, in questa *Rivista,* 2022, 179 ss., con citazione della bibliografia precedente

([10]) Y. TAKEI, *Law and Policy for International Submarine Cables: an Asia-Pacific Perspective*, in *Asian Journal of International Law*, 2.2, 2012, 231 ss.; G. GALLO, *I cavi sottomarini e il diritto internazionale: quale protezione per le cosiddette "arterie" della globalizzazione?*, in *Comunità internazionale. Rivista trimestrale della Società Italiana per l'Organizzazione Internazionale*, 77, 3, 2022, 409; S. KAYE, *International Measures to Protect Oil Platforms, Pipelines and Submarine Cables from Attack*, in *Tulane Maritime Law Journal*, 31.2, 2007, 422 e ss. Recentemente, con un approccio simile, si v. anche E.

ISSN 2038-1662

appare, rispetto al contesto tecnologico e geopolitico attuale, ormai desueto.

In primo luogo, l'efficacia delle norme dipende in larga misura dalla volontà degli Stati di ratificare e attuare le convenzioni internazionali o di integrare obblighi analoghi nei propri ordinamenti. Molti Stati non disciplinano adeguatamente la responsabilità per atti di sabotaggio, in particolare quando le condotte si verificano in zone di mare non soggette alla giurisdizione esclusiva di uno Stato. In secondo luogo, l'attribuzione degli atti dannosi (soprattutto quelli condotti con tecnica indiretta o di «*plausible deniability*»)([11]) risulta spesso impraticabile ([12]), poiché l'applicazione delle norme internazionali richiede interventi da parte dello Stato di Bandiera o l'adozione di procedure internazionali complesse ([13]). In terzo luogo, non esistono obblighi positivi di sorveglianza continua o condivisione obbligatoria delle informazioni sui rischi: la cooperazione rimane spesso lasciata alla discrezionalità degli Stati[14] e dei fornitori infrastrutturali.

NIGRO, *I cavi sottomarini tra problemi giuridici e problemi spaziali*, in *Rivista Diritto dei Trasporti,* 37,1, 2024, 95 ss.

([11]) M. POZNANSKY, *Revisiting plausible deniability*, in *Journal of Strategic Studies*, 45.4, 2020, 511 ss.

([12]) A. TETI, *Spionaggio sottomarino. Attività di intelligence e siti segreti*, in *Gnosis,* 20, 3, 2014, 67 ss.

([13]) M. CARDILLO, *Navigating International Law Safeguards for Submarine Cables: Charting a Course for Effective Protections*, in *The Yale Journal of International Law*, 49, 2024, 320 ss.

([14])Si pensi, ad esempio, alla c.d. *Quad Partnership for Cable Connectivity and Resilience* nell'Oceano Pacifico

ISSN 2038-1662

La proposta – evocata nel titolo di questo lavoro – di una protezione *data-oriented* nasce dall'esigenza di superare una visione frammentata della sicurezza delle infrastrutture sottomarine, tradizionalmente limitata alla loro tutela fisica o alla difesa cibernetica dei sistemi che le gestiscono. In un contesto globale in cui il dato costituisce una delle principali risorse strategiche, la sicurezza non può più essere misurata soltanto in termini di continuità operativa o di resilienza tecnica, ma deve includere la protezione del valore informativo che le infrastrutture generano, trasportano e custodiscono.

Parlare di protezione *data-oriented* significa, dunque, collocare il dato al centro del sistema di tutela, riconoscendogli una funzione non accessoria, ma strutturale. Il dato è un elemento costitutivo della sicurezza, le cui integrità e tracciabilità condizionano la stabilità dell'intero ecosistema marittimo-digitale. L'idea sottesa a questa indagine è quella, pertanto, di individuare e proporre una sicurezza relazionale e multilivello, in cui i soggetti, le tecnologie e le informazioni interagiscono in un equilibrio dinamico di responsabilità. A differenza della protezione fisica, che si fonda sul controllo dello spazio, e di quella cibernetica, centrata sulla prevenzione o identificazione tecnica degli attacchi, la protezione *data-oriented* si concentra sul governo del flusso informativo e dunque sulle regole di accesso, sulle modalità di condivisione e sugli obblighi di rendicontazione che ne derivano.

ISSN 2038-1662

In questa prospettiva, innovativa, quantomeno se si guardi al panorama degli studi italiani ([15]), la sicurezza delle infrastrutture subacquee assume un'inedita natura ibrida, nella quale la dimensione materiale del cavo si intreccia con quella immateriale dei dati. La tutela fisica e quella informativa non si escludono, anzi possono completarsi: la prima garantisce la continuità del supporto, la seconda ne assicura la legittimità e l'affidabilità funzionale. Il paradigma *data-oriented* tenta, così, di reinterpretare la sicurezza dei cavi sottomarini come un ecosistema informativo integrato, dove la protezione non riguarda soltanto ciò che si trova sotto il mare, ma anche ciò che dal mare fluisce verso le reti terrestri e i sistemi di governo dei dati. È una prospettiva che tenta di ampliare l'orizzonte tradizionale del diritto marittimo, estendendolo al dominio della *governance* informativa e della responsabilità condivisa.

Va precisato che la protezione *data-oriented* ([16]) non designa in questo lavoro una categoria meramente tecnica, ma un principio ordinatore capace di guidare la costruzione di modelli giuridici e organizzativi fondati sulla proporzionalità del rischio e sulla trasparenza reciproca. Essa costituisce il fondamento teorico da cui

([15]) Oltre a Vagaggini e Nigro, citate in precedenza, cfr. anche il lavoro approfondito e ricco di indicazioni di *policy* di F. MARTINI, *Tutela delle infrastrutture subacquee di interesse strategico per il Paese: modelli possibili di sorveglianza, intervento e deterrenza*, Roma, 2024, pubblicazioni del Centro Alti Studi per la Difesa.

([16]) AA.VV., *Exploitation techniques and defenses for data-oriented attacks*, in *2019 IEEE Cybersecurity Development,* sul sito web https://arxiv.org/abs/1902.08359

ISSN 2038-1662

discendono i modelli che ho denominato AGOR (Apertura Graduata Orientata al Rischio) e CTR (Contratto di Trasparenza Reciproca), i quali traducono in termini operativi la necessità di una sicurezza informativa graduata, cooperativa e verificabile e che verranno presentati e discussi nei paragrafi successivi.

2. *Le iniziative europee a tutela dei cavi sottomarini: brevi cenni*

In uno scenario geopolitico mutevole, come quello descritto nel paragrafo precedente, non era possibile, per l'Unione Europea, restare a lungo inerti: soprattutto i ripetuti attacchi nel Mar Baltico hanno indotto a promuovere alcune iniziative specificamente pensate per la protezione dei cavi sottomarini. Il tema della sicurezza e resilienza delle infrastrutture dei cavi sottomarini è stato affrontato dalla Raccomandazione europea del 2024 sulla «Sicurezza e la resilienza delle infrastrutture dei cavi sottomarini ([17])», nonché nel Libro Bianco a tema «*How to master Europe's digital infrastructure needs*» ([18]). Per attuare la Raccomandazione, la Commissione europea ha istituito un gruppo *ad hoc* di esperti, composto dalle autorità degli Stati membri, tra cui l'Italia, e dall'ENISA. Ulteriore tassello di questa strategia complessiva è rappresentato una Comunicazione congiunta della Commissione europea e

([17])[C(2024) 1181] https://digital-strategy.ec.europa.eu/en/library/recommendation-security-and-resilience-submarine-cable-infrastructures

([18])https://digital-strategy.ec.europa.eu/en/library/white-paper-how-master-europes-digital-infrastructure-needs

ISSN 2038-1662

dell'Alto rappresentante dell'Ue per gli Affari Esteri ([19]), che costituisce lo strumento normativo più recente, comprensivo di un piano che promuove azioni specifiche lungo tre direttrici.

La prima è quella della prevenzione, attraverso il finanziamento di cavi di nuova generazione per migliorare la tenuta e la resistenza del sistema. Altri ambito rilevante è quello del rilevamento-*detection*, da rafforzare migliorando la capacità di monitoraggio delle minacce dal Mediterraneo al Baltico, per ricevere *alert* in tempo reale, tramite l'utilizzo di droni a doppio uso, immagini satellitari e una rete di sensori sottomarini. Sul piano della risposta e recupero, una piattaforma di condivisione dei dati dovrebbe aiutare Paesi e operatori a reagire prontamente alla minaccia in modo coordinato e a ridurre i tempi di riparazione. Sul piano della deterrenza, sono allo studio strumenti di «diplomazia sottomarina»([20]), come sanzioni contro gli autori dei sabotaggi. Da ultimo, degna di nota è la recentissima iniziativa europea del Submarine Cable Security Toolbox, la quale propone investimenti, azioni a medio termine, e progetti di ricerca correlati al mantenimento della sicurezza nell'ambiente sottomarino[21].

([19])[JOIN(2025) 9 final] https://digital-strategy.ec.europa.eu/en/library/joint-communication-strengthen-security-and-resilience-submarine-cables

[20] Sul sito web https://www.esteri.it/wp-content/uploads/2024/07/CESI_Il-quasi-dominio-sottomarino-dipendenze-minacce-e-prospettive-per-proteggere-operare-e-primeggiare-negli-abissi.pdf

[21] https://digital-strategy.ec.europa.eu/en/library/submarine-cable-security-toolbox-and-cable-projects-european-interest

ISSN 2038-1662

Nella prospettiva qui scelta, la protezione dei cavi sottomarini si colloca, allora, tra governance dei dati e diritto europeo della cybersicurezza, prospettando un approccio multilivello capace di assicurare, nel contempo, prevenzione, resilienza e cooperazione informativa. È proprio su quest'ultimo profilo che vale la pena soffermarsi[22].

Il quadro giuridico che disciplina a livello sovranazionale i cavi sottomarini – retaggio, come si accennava, di un 'diritto del mare' di concezione e matrice novecentesca – li considera ancora come opere di (pur sofisticatissima) ingegneria, ignorando, o comunque ponendo in ruolo subalterno la natura dinamica e cognitiva dei dati che generano, trasmettono e custodiscono. Un ripensamento, su questi principi, potrebbe essere quantomai opportuno.

3. *Un "mare di dati" da solcare: verso un cambio di paradigma*

Un aspetto cruciale e non sempre adeguatamente considerato ai fini della protezione dei cavi sottomarini e dell'ambiente subacqueo in generale, ma che oggi merita una maggiore attenzione, è la condivisione dei dati e delle informazioni, volta soprattutto ad

[22]La presente indagine non affronta il tema se i dati trasmessi attraverso i cavi sottomarini necessitino di una declinazione specifica della disciplina europea in materia di dati (personali e non) e di intelligenza artificiale – disciplina che, nella trattazione, costituisce invece il contesto regolatorio di riferimento. Si tratta di una questione di sicuro rilievo, che potrebbe formare oggetto di uno sviluppo autonomo in una successiva versione del lavoro.

ISSN 2038-1662

alimentare una risposta concertata e tempestiva in caso di attività sospette o, ancor peggio, di gravi incidenti. La capacità di trasmettere e processare imponenti moli di dati è del resto fondamentale per la sicurezza nazionale ([23]). Il ruolo dei dati assume infatti sempre più importanza nel processo di *intelligence*, e *decision-making*; anche la digitalizzazione degli strumenti bellici causa un vertiginoso aumento dei dati a disposizione degli apparati di sicurezza. Non sorprende, dunque, che i siti di atterraggio e approdo dei cavi sottomarini siano stati inclusi dal U.S. *State Department*, per esempio, nell'elenco delle infrastrutture più critiche per gli Stati Uniti ([24]).

Il dominio marittimo sta diventando inevitabilmente e intrinsecamente *data-driven* ([25]). Ciò implica, in parole più chiare, che ogni nave, porto e infrastruttura costiera produce quotidianamente una quantità massiccia di informazioni: dati meteorologici, geospaziali, AIS (*Automatic Identification System*), *log* di navigazione, sensori di bordo, immagini satellitari, e

([23]) B. CLARK, *Undersea cables and the future of submarine competition*, in *Bulletin of the Atomic Scientists*, 72, 4 , 2016, 234 ss.
([24]) D. RUNDE, E. MURPHY, T. BRYIA, *Safeguarding Subsea Cables. Protecting Cyber Infrastructures and Great Power Competition*, in *Center For Strategic and International Studies Report,* 2024, sul sito web https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-08/240816_Runde_Subsea_Cables.pdf?VersionId=hn4OBAvGOF.c3WSZD9uJo6mGJviXZJWh
([25]) AA.VV., *Data-driven framework for extracting global maritime shipping networks by machine learning*, in *Ocean Engineering*, 269, 2023, sul sito web https://doi.org/10.1016/j.oceaneng.2022.113494

ISSN 2038-1662

informazioni sulle merci trasportate ([26]). Tuttavia, tali dati sono spesso frammentati, inaccessibili o soggetti a vincoli proprietari che ne limitano l'uso congiunto da parte di autorità marittime, forze di sicurezza, operatori privati e centri di ricerca.

Nel settore delle infrastrutture critiche, la condivisione dei dati si inserisce nell'ambito della cooperazione in materia di 1) sorveglianza e intelligence congiunta: la raccolta e lo scambio di informazioni su anomalie, segnali di interferenza o guasti (mediante piattaforme interoperabili di monitoraggio) costituiscono strumenti essenziali per implementare un sistema di allerta precoce ([27]); 2) coordinazione operativa nella riparazione e risposta: la condivisione tempestiva dei dati tecnici (localizzazione, tipologia di danno, condizioni ambientali) fra Stati, operatori infrastrutturali e organismi internazionali può ridurre significativamente i tempi di intervento e facilitare la cooperazione nella logistica e nell'assistenza tecnica.

Alla luce di ciò, una riforma del regime internazionale di protezione dei cavi sottomarini potrebbe includere, senza pretese di esaustività:

([26])AA.VV., *AI in Maritime Security: Applications, Challenges, Future Directions, and Key Data Sources*, in *Information*, 16.8, 2025, sul sito web https://doi.org/10.3390/info16080658

([27])F. SJÖLANDER, M. SKÖLD, K. BARQUET, *Navigating security challenges: the future of marine infrastructure in European seas*, in *Policy brief. Mistra Geopolitics*, 2024, sul sito web https://www.mistra-geopolitics.se/sustainable-oceans/

ISSN 2038-1662

- L'introduzione di obblighi di trasparenza e cooperazione multilaterale vincolanti, che impongano agli Stati di notificare tempestivamente gli incidenti e di condividere formule tecniche e dati diagnostici con le controparti interessate, in uno schema paragonabile ai meccanismi di «*critical infrastructure information sharing*», peraltro già presenti in altri settori ([28]).
- L'estensione dei doveri di regolamentazione interna affinché gli Stati includano nei loro ordinamenti obblighi sanzionatori efficaci per atti di danneggiamento, anche in riferimento a entità non statali e attività transnazionali[29].
- L'armonizzazione delle piattaforme di interoperabilità regionali e sovranazionali, ispirate al modello europeo del Regolamento (UE) 2023/2854 (*Data Act*) affinché i dati tecnici relativi ai cavi possano essere scambiati in tempo reale su basi legali certe, come si vedrà a breve.

([28])AA.VV., *Cyber Situational Awareness and Information Sharing in Critical Infrastructure Organizations*, in *Information & Security: An International Journal*, 43.2, 2019, 236 ss.

([29]) M. S. NAVARRO, *Modern challenges within the law of state responsibility for human rights violations committed by non-state actors*, 2020, sul sito web https://dirittifondamentali.it/wp-content/uploads/2020/11/Navarro-Modern-challenges-within-the-law-of-state-responsibility-for-human-rights-violations-committed-by-non-state-actors....pdf?utm; e, soprattutto, T. DAVENPORT, *Intentional Damages to Submarine Cable Systems by States*, Stanford, 2024, sul sito web https://www.hoover.org/sites/default/files/research/docs/Davenport_finalfile_WebReadyPDF.pdf?

ISSN 2038-1662

- Maggiori strumenti di attribuzione e responsabilità: potenziare la capacità investigativa internazionale e introdurre regimi di responsabilità più stringenti per danni accertati, comprese sanzioni multilaterali o meccanismi di risarcimento obbligatorio[30].
- Rafforzamento e valorizzazione di organismi internazionali specializzati, come il Comitato Internazionale per la Protezione dei Cavi (ICPC), per fungere da *hub* tecnico-legislativo nella promozione di linee guida e standard comuni (ad esempio per la protezione, la sorveglianza e la risposta) ([31]).

A ben vedere, nel passaggio da un'ottica principalmente tecnica a una prospettiva (anche) giuridica, di respiro potenzialmente internazionale, una chiave strategica potrebbe risiedere in meccanismi di condivisione obbligatoria dei dati e nella cooperazione multilaterale. Soltanto attraverso l'adozione di strumenti normativi vincolanti che integrino obblighi di trasparenza, responsabilità e interoperabilità sarà possibile rafforzare la resilienza delle infrastrutture sottomarine e tutelare efficacemente la connettività globale. E vi è di più. La costruzione (in questo caso pensando su scala regionale) di un vero e proprio diritto europeo dei dati può essere letta come un processo graduale di

([30]) T. DIAS, *Countermeasures in International Law and their role in Cyberspace*, in *Chatham House, Research Paper*, 2024, sul sito web https://www.chathamhouse.org/sites/default/files/2024-05/2024-05-23-countermeasures-international-law-cyberspace-dias.pdf
([31]) D.R. BURNETT, *Submarine Cables and International Law*, in *International Law Studie*s, 2021, 1661 ss.

ISSN 2038-1662

istituzionalizzazione della fiducia (*trust by design*), che porterebbe progressivamente, sulla scia di alcuni studi condotti sull'argomento, a trasformare il dato da oggetto tecnico a bene giuridico relazionale, fondato sulla trasparenza e sulla cooperazione ([32]).

L'Europa ha contribuito attivamente e senza sosta a costruire una strategia potenzialmente globale per il "mercato dei dati", attraverso una serie coordinata di iniziative normative rilevanti ai fini del presente contributo[33]. Il Regolamento (UE) 2016/679 in materia di protezione dei dati personali (*GDPR*) può essere considerato la prima pietra di questa complessa intelaiatura, introducendo la cultura della responsabilizzazione (*accountability*) [(Artt. 5 (1)(c) e 25] e della minimizzazione ([34]) del trattamento come presupposti di legittimità.

([32]) AA.VV., *Trust by Design: An Ethical Framework for Collaborative Intelligence Systems in Industry 5.0*, in *Electronics*, 14(10), 2025,1952; J. ISOHANNI, L. GOULDEN, K. M. HERMSEN, M. ROSS, J. VANBOCKRYCK, *Disposable identities; enabling trust-by-design to build more sustainable data driven value,* in *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, Rhodes, 2021, 378-383; D. FERRARIS, C. FERNANDEZ-GAGO, J. LOPEZ, *A Trust-by-Design Framework for the Internet of Things*, in *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, Paris, 2018, 1 ss.

([33])Ampiamente, v. D. AMRAM, *Comparing EU Initiatives on Data: Addressing Risks and Enhancing Harmonisation Opportunities*, in *Opinio Juris in Comparatione*, 2023, 2 ss.

([34]) G. COMANDÈ, G. SCHNEIDER, *Differential Data Protection Regimes in Data-Driven Research: Why the GDPR is More Research-Friendly Than You Think*, in *German Law Journal*, 23, 2022, 559 ss. Utili comparazioni con il diritto statunitense in J. FRANCIS, *Unpacking the Shift Toward Substantive Data Minimization Rules in Proposed Legislation*, in *IAPP (May 22, 2024)*, sul sito web https://iapp.org/news/a/unpacking-the-shift-towards-substantive-data-

ISSN 2038-1662

Non si protegge unicamente la privacy individuale, ma si riconosce che la circolazione controllata dei dati è condizione (anche) di libertà e di sicurezza collettiva (Considerando 7 GDPR).

Il successivo *Data Governance Act* (Reg. UE 2022/868) ha ampliato il quadro, istituendo la figura dell'intermediario dei dati (artt. 10-12) ([35]) e introducendo il principio di altruismo dei dati (artt. 16-20)([36]), cioè la possibilità data ai soggetti interessati di

---

minimization -rules-in-proposed-legislation. Altro quadro generale in ID., *Data Minimization's Substantive Turn: Key Questions and Operational Challenges Posed by New State Privacy Legislation* (June 05, 2025), sul sito web SSRN: https://ssrn.com/abstract=5309096

([35]) D. POLETTI, *Gli intermediari dei dati. Data Intermediaries*, in *European Journal of Privacy Law & Technologies*, 1, 2022; F. Bravo, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in *Contr. e Impresa Europa*, 1.1, 2021, 199-256; D. SBORLINI, *Cooperative di dati e principio di neutralità dei fornitori di servizi di intermediazione dei dati: questioni critiche*, in AA.VV., *EU Data Cooperatives. L'ingresso delle cooperative di dati nell'ordinamento europeo*, Torino, 2024, 707 ss.

([36]) S. TRANQUILLI, *Il nuovo citoyen européen nell'epoca del Data governance act*, in *Rivista di Digital Politics*, *2*(1-2), 2023, 179 ss.; F. BRAVO, *Il principio di solidarietà tra* data protection e data governance, in *Il Diritto dell'Informazione e dell'Informatica*, 3, 2023, 481-518; L. PASERI, *The ethical and legal challenges of data altruism for the scientific research sector*, in *The leading role of smart ethics in the digital world*, 2024, 189-200; W.VEIL, *Data altruism: How the EU is screwing up a good idea*, in *Algorithm Watch*, 2021,1 ss.; AA.VV., *Addressing Challenges and Opportunities in Data Sharing for the Common Good: The Case of Europe's First Data Altruism Organisation*, in *2024 IEEE Smart Cities Futures Summit (SCFC)*, 2024, 45 ss. G. CHASSANG, L. FERIOL, *Data Altruism, Personal Health Data and the Consent Challenge in Scientific Research: A Difficult Interplay between EU Acts,* in *European Data Protection Law Review*, 10(1), 2024, 57 ss.; C. KRUESZ, F. ZOPF, *The concept of data altruism of the draft dga and the gdpr:*

ISSN 2038-1662

condividere dati per finalità di interesse generale sotto garanzie di neutralità e trasparenza ([37]). Parafrasando quanto già espresso nel 2020 dalla Commissione europea nel suo *Report sulla Strategia Europea per i Dati* ([38]), tale figura rappresenta un nuovo modello di fiducia istituzionale, in cui la governance non si fonda sull'esclusività del possesso, ma sulla credibilità dei processi di condivisione. La Direttiva (UE) 2022/2555 (NIS2) ha poi esteso gli obblighi di sicurezza informatica a un numero molto più ampio di settori critici, includendo per la prima volta il dominio marittimo e subacqueo ([39]). In tal modo, la sicurezza informatica è divenuta parte integrante della resilienza marittima europea e ciò implica che la protezione dei dati costituisca un elemento essenziale, un corollario si direbbe, della protezione delle infrastrutture fisiche. Infine, il Regolamento (UE) 2023/2854 (*Data Act*) ha completato l'edificio

inconsistencies and why regulatory sandbox model may facilitate data sharing in the Eu, in *European Data Protection Law Review,* 7(4), 2021,569 ss.

([37]) I.A. CAGGIANO, *Modelli negoziali di condivisione di dati: prospettive applicative e la sostenibilità ambientale*, in *Collana di Diritto Digitale*, 2024, 83 ss.

([38])https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52020DC0066

([39]) al *Considerando 97*, si menziona testualmente il…

«…*s*ostenere la disponibilità, l'integrità e la riservatezza del nucleo pubblico dell'open internet, inclusa, ove pertinente, la sicurezza informatica dei cavi di comunicazione sottomarini*». A*nche nell'art. 7 (Strategie nazionali), al comma 2, lettera d), è previsto che le strategie nazionali includano misure relative al nucleo pubblico dell'Internet aperto, «compresa, se del caso, la sicurezza informatica dei cavi di comunicazione sottomarini»: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX%3A32022L2555

ISSN 2038-1662

normativo, configurando un regime generale di accesso equo e di condivisione regolata dei dati generati da dispositivi connessi. Esso alle autorità pubbliche il diritto di ottenere dati privati in situazioni eccezionali di emergenza, attraverso un equilibrio normativo chiamato a bilanciare tra interesse pubblico e proprietà informativa privata (artt. 14 ss.)

Come sottolinea autorevole dottrina, l'Europa sta transitando dunque dalla logica della protezione alla logica della condivisione responsabile, spostando il baricentro del contemperamento degli interessi dalla *privacy* individuale alla fiducia sistemica ([40]). Non si tratta di un percorso privo di ostacoli, ma le premesse normative già esistenti rendono questo obiettivo realisticamente perseguibile. In uno scenario così ripensato, i cavi sottomarini possono rappresentare davvero un caposaldo della società dell'informazione globale e la loro protezione richiede ormai inevitabilmente una convergenza tra diritto del mare e diritto dei dati ([41]). Tale visione è stata ulteriormente avvalorata dalla *European Maritime Security Strategy* [COM(2023) 224 final] ([42]), che riconosce la fiducia e la trasparenza dei flussi informativi come elementi costitutivi della resilienza

([40]) L. FLORIDI, *Data, Democracy, and the Ethics of Sharing*, in *Philosophy & Technology*, 36(2), 2023, 17 ss.
([41]) J. HALOG, P. MARGAT, M. STADERMANN, *Submarine Infrastructures and the International Legal Framework*, in *Transactions on Maritime Science*, 13(1), 2024, 3 ss.
([42])https://oceans-and-fisheries.ec.europa.eu/ocean/blue-economy/other-sectors/maritime-security-strategy_en

ISSN 2038-1662

marittima europea. Nel "mare" dei dati, la fiducia non può assumere il ruolo di mero presupposto etico, ma deve tradursi, prosaicamente quasi, in un'infrastruttura giuridica, per acquisire il rango di un principio operativo di sicurezza.

Nel loro insieme, se valorizzate opportunamente, le disposizioni fin qui citate possono avallare l'idea che il dato sostanzi anche un bene comune, relazionale, che possa fondare un ecosistema di interoperabilità etica. Applicato al dominio marino, questo paradigma potrebbe agevolare, se non proprio produrre, un cambiamento importante. Il diritto del mare, storicamente costruito intorno ai concetti di sovranità, libertà e giurisdizione, si può aprire oggi anche alla dimensione informativa: le condizioni normative e tecnologiche perché ciò avvenga ci sono tutte.

3.1 *Per una governance proporzionata dei dati marini: i modelli AGOR e CTR*

Una domanda è sottesa a questa parte della trattazione: è allora ipotizzabile e sostenibile un vero diritto (del mare) dei dati, in cui la sovranità non coincida più con il controllo esclusivo, ma con la capacità di condividere responsabilmente — secondo una logica di trasparenza proporzionata e cooperazione multilivello? Il valore del dato marino risiederebbe nella capacità di essere utilizzato in modo sicuro, tracciabile e coordinato, in un equilibrio dinamico tra apertura e sicurezza. La trasparenza, per essere sostenibile, dovrebbe essere tuttavia graduata e proporzionata: non tutto può essere reso pubblico,

ISSN 2038-1662

ma, per contro, nulla può restare completamente oscuro. È su questa intuizione che si basa il modello AGOR (Apertura Graduata Orientata al Rischio), concepito qui come proposta operativa originale per una *governance* proporzionata dei dati marini.

L'Apertura Graduata Orientata al Rischio rappresenta un modello concettuale e operativo di gestione della sicurezza delle infrastrutture critiche — in particolare dei cavi sottomarini di comunicazione — fondato sull'equilibrio dinamico, direi duttile, tra trasparenza, cooperazione e riservatezza. Nel dominio marittimo, la crescente ibridazione tra rischi fisici e digitali (*cyber-physical risks*) rende necessaria una forma di apertura regolata dei dati, delle informazioni e dei protocolli operativi, che consenta la collaborazione tra attori pubblici e privati senza compromettere la sicurezza nazionale o commerciale. L'AGOR potrebbe configurare una risposta sistemica alla tensione tra esigenze di condivisione (per il monitoraggio e la prevenzione) e necessità di protezione (per evitare vulnerabilità e attacchi).

Il principio di Apertura Graduata Orientata al Rischio si fonda, come il nome stesso suggerisce, su tre assi:

1. Gradualità – l'accesso alle informazioni e la con divisione dei dati avvengono in modo progressivo, differenziato in base al livello di rischio, alla sensibilità delle informazioni e alla tipologia dell'attore coinvolto;

ISSN 2038-1662

2. Orientamento al rischio – la misura dell'apertura è definita in funzione del *risk assessment*, cioè della probabilità e dell'impatto di un evento dannoso (fisico o *cyber*);

3. Proporzionalità e *accountability* – ogni decisione di apertura o restrizione dei flussi informativi deve essere tracciabile, giustificata e proporzionata rispetto all'obiettivo di sicurezza perseguito ([43]).

Tale impostazione, a ben vedere, sembra riflettere l'evoluzione del diritto europeo dei dati, che, a partire dal GDPR, ha spostato l'attenzione dalla mera protezione (in un'ottica, diremmo, statica e passiva) alla responsabilità attiva (e dunque molto più dinamica) nella gestione informativa, basata sulla valutazione del rischio. In particolare, si può valorizzare l'articolo 5, paragrafo 1, lettera c) del GDPR, il quale sancisce il principio di minimizzazione ([44]), imponendo che i dati siano trattati «in modo adeguato, pertinente e limitato a quanto necessario rispetto alle finalità per le quali sono raccolti». Questo precetto, combinato con l'articolo 24 sul principio di *Accountability*, costituisce un primo fondamento concettuale e normativo del modello AGOR: la trasparenza non è, e non può essere

([43]) Aa.Vv., *A Taxonomy of Systemic Risks from General-Purpose AI,* in *RAND Working Paper Series Forthcoming*, 2024, sul sito web: https://ssrn.com/abstract=5030173

([44])L. CALIFANO, *Spunti problematici sul trattamento dei dati personali raccolti tramite droni*, in *Cultura giuridica e diritto vivente*, 2020, *7*; F. FAINI, *Dati, algoritmi e Regolamento europeo 2016/679*, in AA.VV. (a cura di R. Mantelero, D. Poletti), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, Pisa, 2018, 333 ss.

ISSN 2038-1662

naturalmente, assoluta, ma commisurata al rischio e alla funzione sociale del dato (e di quel singolo dato, in quel singolo istante).

Il *Data Governance Act* permette poi di estendere tale logica agli intermediari dei dati anche per finalità di altruismo dei dati. L'AGOR si colloca nel solco di questa visione complessiva, proponendo una trasparenza graduata, controllata, che consenta di indentificare, nel caso di specie, il bilanciamento tra interesse pubblico, sicurezza cibernetica e tutela della sovranità informativa ([45]).

Un ulteriore fondamento normativo deriva dalla Direttiva NIS2, che estende gli obblighi di sicurezza alle infrastrutture critiche, comprese quelle marittime e sottomarine (Allegato I, punto 4). L'articolo 21 della Direttiva impone alle imprese e agli enti pubblici di adottare misure tecniche e organizzative adeguate «in funzione del rischio», rendendo così il principio di graduazione un obbligo giuridico generale, non più una buona prassi tecnica. L'AGOR assume questa prospettiva e la estende all'intera catena informativa: non solo proteggere il dato, ma regolare il grado di apertura in modo verificabile e documentabile.

Infine, ai fini della proposta qui elaborata si consideri *Data Act***,** il quale definisce le condizioni di accesso equo e di condivisione regolata dei dati generati da dispositivi connessi e consente, come

([45])E. SORRENTINO, A.F. SPAGNUOLO, *Cybersecurity e sovranità digitale nella protezione dei dati personali*, in *Rivista italiana di informatica e diritto*. 6, 2, 2024, 685 ss.

ISSN 2038-1662

evidenziato, alle Autorità pubbliche di ottenere dati detenuti da soggetti privati «in circostanze eccezionali di necessità pubblica», a condizione che l'accesso sia proporzionato, limitato nel tempo e adeguatamente tracciato. Questa norma incarna un pilastro del modello AGOR: la trasparenza come atto di fiducia regolata.

In termini applicativi, il modello AGOR suggerisce la classificazione dei dati secondo livelli di apertura progressiva i quali riflettono, a loro volta, la natura e il potenziale impatto conseguente alla loro eventuale divulgazione. Si propone di distinguere, così, cinque categorie (v. appendice finale):

1. dati pubblici o ambientali, liberamente accessibili e riutilizzabili ai sensi della Direttiva (UE) 2019/1024;
2. dati aggregati o anonimizzati, condivisibili con licenza standard;
3. dati tecnici o operativi, accessibili previa valutazione di sicurezza;
4. dati infrastrutturali strategici, riservati a soggetti pubblici autorizzati;
5. dati sensibili di sicurezza nazionale, protetti da regimi di accesso ristretto e cifratura conforme agli standard ENISA.

Il passaggio tra i livelli di apertura dovrebbe avvenire attraverso una valutazione dinamica e attenta del rischio, fondata sui criteri di probabilità, impatto e reversibilità del danno (articolo 32 del GDPR). Un approccio teorico del genere consentirebbe di adattare più agevolmente la governance dei dati a contesti variabili — crisi

ISSN 2038-1662

geopolitiche, incidenti informatici, emergenze ambientali — senza compromettere la necessaria continuità informativa.

Nel dominio marino e subacqueo, il modello AGOR può assumere una funzione di grande utilità. I dati generati dai cavi sottomarini, dai sensori oceanografici e dalle piattaforme di sorveglianza rappresentano, lo si è detto più volte, informazioni molto rilevanti[46]. La loro circolazione non può essere totalmente libera, ma nemmeno rigidamente chiusa: deve essere graduata, monitorata e "auditabile", in coerenza con il principio di *shared situational awareness* ([47]) ricavabile dalla *European Maritime Security Strategy* ([48]). L'AGOR,

([46])T. NEUMANN, *Cybersecurity in Maritime Industry*, in *The International Journal on Marine Navigation and Safety of Sea Transportation*, 18, 4, 2024, 765 ss.

([47])G. DUCA, F.M. MUSTO, G. TRUPIANO, *Gestione delle informazioni e Situational Awareness nelle emergenze ambientali*, in *Rivista Italiana di Ergonomia*, 2016, 171 ss. e, soprattutto, E. SIMETTI, F. ODONE, *Situational Awareness in Maritime Environments*, in *Robotics and Intelligent Machines*, 28, 2016, 12 ss.

([48])https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52023JC0008; L. LANDMAN, *The EU Maritime Security Strategy: Promoting or Absorbing European Defence Cooperation?* in *Clingendael Policy Brief. Nederlands Instituut voor Internationale Betrekkingen 'Clingendael',* 2015; C. BUEGER, T. EDMUNDS, *The European Union's Quest to Become a Global Maritime-Security Provider*, in *Naval War College Review*, 76,2, Article 6, 2023; M. RIDDERVOLD, *The EU and the governance of the Maritime Global Space*, in *Journal of European Integration*, 45(8), 2023, 1143 ss.; B. GERMOND, *The maritime dimension of European security: Seapower and the European Union*, 2015; C. BUEGER, *What is maritime security*?, in *Marine policy*, 53, 2015, 159 ss.

ISSN 2038-1662

dunque, arricchisce il paradigma della sicurezza con la dimensione di una fiducia computabile.

A questo proposito, si propone anche un modello negoziale, già chiamato in precedenza Contratto di Trasparenza Reciproca (CTR), come strumento giuridico concreto e complementare all'approccio AGOR, concepito per istituzionalizzare la fiducia e la responsabilità condivisa tra gli attori coinvolti in progetti tecnologici complessi, in particolare nel dominio della sicurezza sottomarina. Si tratta di un modello contrattuale di *soft law*, pensato per promuovere la fiducia e la cooperazione tra gli attori pubblici e privati coinvolti nella gestione, manutenzione e sicurezza di infrastrutture che, pur essendo invisibili e spesso trascurate, costituiscono l'ossatura fisica della comunicazione globale.

L'idea alla base del CTR è quella di tradurre in forma giuridicamente vincolante i principi di trasparenza, reciprocità e responsabilità condivisa, creando un quadro regolatorio flessibile ma efficace che consenta la condivisione bilanciata delle informazioni tra soggetti diversi per natura, interessi e prerogative. In un settore in cui la frammentazione delle competenze e la riservatezza commerciale ostacolano spesso la cooperazione, il CTR propone un modello di interazione strutturata, fondato su scambi informativi sicuri, verificabili e protetti.

L'obiettivo è garantire un equilibrio dinamico tra riservatezza, interoperabilità e *accountability*, fondando la collaborazione su

ISSN 2038-1662

obblighi bilaterali di trasparenza informativa, tracciabilità delle decisioni e verificabilità delle operazioni.

Il CTR si basa, anch'esso, come l'AGOR, su tre pilastri, che richiamano la denominazione:

1. Reciprocità informativa, che impone uno scambio continuo e simmetrico di dati e report di sicurezza tra le parti;
2. Trasparenza procedurale, che consente la puntuale ricostruzione *ex post* delle decisioni tecniche e amministrative, anche ai fini di audit o revisione indipendente;
3. Resilienza contrattuale, intesa come capacità del rapporto di adattarsi a variazioni tecnologiche o normative, mediante clausole di revisione e adattamento progressivo[49].

Nel contesto della sicurezza sottomarina, il CTR diventa uno strumento di garanzia multilivello, capace di sostenere l'attuazione dell'AGOR e di assicurare una *governance* trasparente, verificabile e flessibile delle infrastrutture critiche. Da un punto di vista dell'inquadramento teorico, il CTR trova giustificazione nella

([49]) S. LANDINI, *Vincolatività dell'accordo e clausole di rinegoziazione. L'importanza della resilienza nelle condizioni contrattuali*, in *Contratto e Impresa*, 2016, 1, 179 ss.; A. GALLARATI, *La resilienza del contratto*, Torino, 2020 e, ancora, cfr. M. ELIZA, *The Resilience of Contract Law in Light of Technological Change*, in AA.VV. (a cura di M. Furmston), *Future of the Law of Contract*,New York, 2020; T. DOLLA, N. THOUNAOJAM, G. DEVKAR, B. LAISHRAM, *Proactive Contract Theory-Based Resilience Framework Development for Public–Private Partnerships*, in *Construction Economics and Building*, 25.2, 2024, 253 ss.

ISSN 2038-1662

necessità di sperimentare soluzioni tecnologiche in ambiente controllato e regolato([50]).

Tale impostazione è coerente con i principi di proporzionalità, *accountability* e sicurezza sistemica introdotti dal Regolamento (UE) 2024/1689 sull'Intelligenza Artificiale([51]). Il fondamento giuridico di questo modello operativo si può rintracciare anche nei principi già codificati (e sopra richiamati) nel *Data Governance Act*, che, come si è osservato, impone agli intermediari di dati di garantire neutralità, trasparenza e tracciabilità nei rapporti tra i soggetti che condividono dati, e negli articoli che richiedono meccanismi contrattuali di sicurezza e *accountability*.

Il CTR si ispira a un modello ibrido, che unisce la dimensione privatistica del contratto con la funzione pubblicistica della fiducia. Esso può essere inteso come un accordo multilaterale — tra enti pubblici, operatori privati, centri di ricerca o autorità indipendenti — volto principalmente a disciplinare:

1. le modalità di condivisione dei dati (periodicità, formato, standard di interoperabilità);
2. le misure di sicurezza e anonimizzazione adottate (in conformità all'articolo 32 del *GDPR*);

([50]) Sul punto, cfr. già M. CARR, *Public–private partnerships in national cyber-security strategies*, in *International Affairs*, 92. 1, 2016, 43 ss.
([51]) F. SERINI, *Collective cyber situational awareness in EU. A political project of difficult legal realisation*?, in *Computer Law & Security Review*, 55, 2024, 1 ss.

ISSN 2038-1662

3. le condizioni di riuso o di trasferimento dei dati a terzi (articoli 9–12 del *Data Governance Act*);

4. le responsabilità in caso di violazione o perdita informativa (articoli 83–84 del *GDPR*).

In tale prospettiva, il CTR opera anche come contratto-quadro di interoperabilità, garantendo che ogni scambio informativo avvenga entro limiti verificabili e sulla base di criteri oggettivi di rischio. Può essere stipulato per via amministrativa — come convenzione di cooperazione tra Istituzioni — o per via negoziale privata, tra operatori economici, all'interno degli Spazi Europei dei Dati (*European Common Data Spaces*) ([52]).

La gestione dei dati marittimi richiede, si ribadisce, un equilibrio tra esigenze di condivisione e vincoli di sicurezza nazionale. Il CTR ambisce a fornire questo equilibrio, fungendo da cuscinetto giuridico tra apertura e segretezza: stabilisce regole di interoperabilità che consentono l'uso dei dati a fini pubblici senza compromettere la riservatezza degli elementi sensibili ([53]). Un fondamento teorico del

([52])Si veda il Report Tecnico sul sito web https://op.europa.eu/fr/publication-detail/-/publication/dcac6aee-0e7a-11ee-b12e-01aa75ed71a1/language-en

([53])G. AMPRATWUM, R. OSEI-KYEI, V.W.Y. TAM, *Exploring the concept of public-private partnership in building critical infrastructure resilience against unexpected events: A systematic review*, in *International Journal of Critical Infrastructure Protection*, 39, 2022, 679 ss.

Cercando di proporre un punto di vista più concreto, il CTR può essere configurato come un accordo quadro pubblico-privato, articolato in tre sezioni fondamentali:

a) Clausole di trasparenza

Stabiliscono:

ISSN 2038-1662

CTR può inoltre rinvenirsi nei meccanismi di co-regolazione pubblico-privata propri dei settori strategici a rischio elevato ([54]). Nel contesto della sicurezza sottomarina, il CTR diventa uno strumento di garanzia multilivello.

Volendo esemplificare concretamente, un CTR stipulato tra un'Autorità Marittima Nazionale e un Gestore di Infrastruttura Subacquea potrebbe prevedere che:

- quali categorie di informazioni possono essere condivise (dati tecnici, di manutenzione, geospaziali, di rischio, ecc.);
- a quale livello di dettaglio e con quali limitazioni d'uso;
- attraverso quali canali o piattaforme sicure (es. *data trust* o *secure maritime data spaces*).

b) Clausole di reciprocità e verifica

Definiscono gli obblighi simmetrici tra le parti:

- scambio periodico e verificabile di informazioni critiche;
- diritto di *audit* incrociato per verificare la correttezza dei dati condivisi;
- tracciabilità e *logging* delle operazioni di accesso ai dati;
- obbligo di notifica tempestiva in caso di anomalie, incidenti o tentativi di accesso non autorizzato.

c) Clausole di tutela e responsabilità

Prevedono:

- meccanismi di responsabilità proporzionata al livello di accesso o di gestione dei dati sensibili;
- regimi di riservatezza contrattuale compatibili con le norme sulla sicurezza nazionale e con il GDPR;

procedure di risoluzione alternativa delle controversie (ADR) per ridurre tempi e costi, specie in contesti transfrontalieri

([54])O. PALLOTTA, *L'intervento governativo nei settori economici strategici alla luce del Diritto dell'Unione Europea*, in *GiustAmm, Rivista di Diritto Pubblico*, 2025

ISSN 2038-1662

- i dati ambientali e tecnici non sensibili siano messi a disposizione in tempo reale per scopi scientifici;
- i dati operativi sui flussi o sulle anomalie vengano condivisi solo con autorità di sicurezza previa cifratura;
- la gestione del rischio e la verifica delle misure di sicurezza siano sottoposte a audit annuale congiunto.

Si immagini, ancora, un episodio di danneggiamento sospetto di un cavo sottomarino localizzato in acque internazionali, con conseguente interruzione parziale del traffico dati verso l'Europa. In tale ipotesi, il modello AGOR consentirebbe di classificare i flussi informativi da condividere secondo il livello di rischio: i dati tecnici sul danno (localizzazione, tipologia, profondità) verrebbero messi a disposizione delle autorità competenti europee e dell'Intermediario Neutrale dei Dati Marini, mentre i dati infrastrutturali strategici resterebbero accessibili solo a soggetti pubblici autorizzati, sotto vincolo di cifratura e *audit* periodico.

Il successivo intervento contrattuale disciplinato dal Contratto di Trasparenza Reciproca regolerebbe i termini di scambio tra operatori privati e autorità nazionali, garantendo tracciabilità, adeguatezza e correttezza informativa e protezione delle fonti. In tal modo, il sistema combinato AGOR–CTR assicurerebbe un equilibrio dinamico tra trasparenza, sicurezza e cooperazione internazionale, traducendo in pratica la 'fiducia regolata' che costituisce l'obiettivo politico del *Data Act*. L'obiettivo non è, e non potrebbe essere, quello

ISSN 2038-1662

di "aprire tutto", ma di istituzionalizzare la fiducia, rendendola verificabile[55].

L'impianto teorico-applicativo qui proposto trova, complessivamente, una sua ispirazione nella letteratura recente sull'etica della condivisione dei dati marini, in particolare negli studi di Mingting Zhu et al. (2024) ([56]) e di Borja et al. (2022) ([57]), i quali sono fautori di un equilibrio tra utilità scientifica, sicurezza e giustizia informativa.

Affinchè una nuova *Governance* dei dati marini diventi effettiva è indispensabile, però, che gli Stati membri Europei aggiornino in primo luogo le proprie legislazioni interne sui cavi sottomarini (come peraltro già suggerito di recente, ma ad altri fini, da qualche Studioso) ([58]).

Tre parrebbero, senza pretese di esaustività, i fronti principali su cui si potrebbe agire in prima battuta:

([55])Sul punto, si rinvia alla trattazione di F. SERINI, *Il sistema europeo di cooperazione informativa per il contrasto alle minacce informatiche. Verso una definizione di cybersicurezza integrata*?, in *Medialaws*, 2024, 145 ss.

([56])M. ZHU, W. ZHANG, C.XU, *Ethical governance and implementation paths for global marine science data sharing*, in *Frontiers in Marine Science*, 2024, sul sito web https://www.frontiersin.org/journals/marine-science/articles/10.3389/fmars.2024.1421252/full

([57])A. BORJA, J. KARSTENSEN, M. SCOBIE, M. BARBIER, *Editorial: Ocean Sciences and Ethics*, in *Frontiers in Marine Science*, 2022, sul sito web https://www.frontiersin.org/journals/marine-science/articles/10.3389/fmars.2022.871856/full

([58])E. NIGRO, *I cavi*, cit., 99

ISSN 2038-1662

1. Riconoscimento giuridico della dimensione informativa dei cavi, inserendo la categoria di "infrastruttura di dati" nei codici e/o nelle leggi sulla sicurezza marittima.
2. Obblighi di interoperabilità e condivisione, in linea con il *Data Act* e con la NIS2, prevedendo protocolli comuni e *audit* di conformità.
3. Coordinamento istituzionale con un registro europeo dei cavi e dei dati marini, gestito dall'EMSA e integrato nel sistema CISE.

Un tale adeguamento consentirebbe di contemperare, o, meglio ancora, di armonizzare il diritto del mare e il diritto dei dati, garantendo una sovranità informativa europea integrata e rendendo operativa la fiducia multilivello che il *Data Act* prefigura e prospetta in linea teorica. Nei prossimi paragrafi si analizza il quadro normativo nazionale per la tutela dei cavi sottomarini, arricchitosi di recente di un intervento legislativo organico che verrà valutato nella sua efficacia e completezza anche alla luce del paradigma di protezione qui proposto.

4. *L'Italia e la protezione dei cavi sottomarini: tra passato…*

L'Italia si è distinta, negli ultimi anni, per la rapidità e la proattività con cui ha recepito e sviluppato la normativa europea in materia di sicurezza cibernetica e intelligenza artificiale. È stata, infatti, tra i primi Stati membri ad attuare la direttiva NIS2, con il decreto

ISSN 2038-1662

legislativo 138 del 4 settembre 2024 ([59]) che ha riorganizzato in modo organico l'architettura nazionale di cybersicurezza, estendendo gli obblighi di resilienza digitale a un numero crescente di operatori e servizi essenziali. E, in tempi recentissimi (l. 23 settembre 2025, n. 132) si è dotata del primo quadro normativo organico in tema di Intelligenza Artificiale, in stretta aderenza con l'europeo *AI Act* (Regolamento UE 2024/1689) ([60]).Condivisibilmente, dunque, è stato affermato che, per quello che riguarda il nostro Paese, «sebbene la normativa nazionale in materia di sicurezza informatica sia sufficientemente aggiornata, coerentemente con gli indirizzi europei, ad oggi, risulta ancora carente una disciplina *ad hoc* riferita alla tutela dei cavi sottomarini» ([61]).

La prima legge organica sulla protezione dei cavi ("telegrafici") sottomarini è la l. 19 dicembre 1956, n. 1447, che ha modificato sensibilmente la l. 1 gennaio 1886, n. 3620, di ratifica della Convenzione internazionale di Parigi del 1884 ([62]). Va precisato che

([59]) F. CASAROSA, *L'armonizzazione degli obblighi di notifica: il DDL Cybersicurezza verso la NIS 2*, in *Rivista italiana di informatica e diritto*, 6(1), 2024, 11 ss.; R. RAZZANTE, P. SPANÒ, *La NIS2 e il Decreto cybersicurezza*, Roma, 2025

([60]) Primi commenti alla normativa in M. FRANCAVIGLIA, *IA e funzioni giurisdizionali: alcune questioni preliminari alla luce del quadro costituzionale*, in *Rivista italiana di informatica e diritto*, 7, 1, 2025, 13 ss.

([61]) F. Vagaggini, *Il regime*, cit., 90 s.

([62])https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:1956-12-19;1447#:~:text=Modifiche%20alla%20legge%201%20gennaio%201886%2C%20n.,conclusa%20a%20Parigi%20il%2014%20marzo%201884 . La

ISSN 2038-1662

la normativa, a sua volta riformatrice del Codice postale approvato con r.d. 27 febbraio 1936, n. 645, fa riferimento – come è ovvio, visto il contesto storico ormai risalente – ai cavi telegrafici sottomarini e non ai cavi in fibra ottica modernamente utilizzati per la trasmissione di dati internet. Ma non mancano motivi di interesse nelle disposizioni ivi contenute ([63]).

A ben vedere, la legge in questione, pur essendo ormai datata, rappresenta un precedente giuridico significativo nella storia della protezione penale delle infrastrutture sottomarine di comunicazione; ha un'impostazione rigorosa e ben avrebbe potuto essere adattata, con un sostanzioso aggiornamento, alle moderne discipline in materia di *cybersecurity* marittima, cavi in fibra ottica e infrastrutture critiche. Basti, per meglio spiegare quanto affermato, considerare

Convenzione UNCLOS, invece, è stata ratificata dall'Italia con legge 2 dicembre 1984, n. 689: https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:1994-12-02;689#:~:text=Ratifica%20ed%20esecuzione%20della%20convenzione,York%20il%2029%20luglio%201994.

([63]) Un interessante dibattito sull'approvazione della Legge può leggersi nei resoconti stenografici assembleari del mese di Novembre 1956: https://documenti.camera.it/_dati/leg02/lavori/stencomm/08/Leg/Serie010/1956/1114/stenografico.pdf

ISSN 2038-1662

l'art. 1([64]) e, ancora di più, l'art. 3 ([65]). In merito a quest'ultimo, è evidente come esso introduca tre livelli di tutela penale, che possono essere idealmente letti come tre "cerchi concentrici" di protezione ([66]). Il disegno appare abbastanza chiaro: il Legislatore del 1956

([64]) «Chiunque rompe o guasta, entro o fuori delle acque territoriali, un cavo o altro ordigno di una comunicazione telegrafica o telefonica sottomarina legalmente posta e che tocca il territorio, una colonia o un possedimento di uno o più degli Stati contraenti della Convenzione del 14 marzo 1884 o aderenti alla medesima, ed in tal modo interrompe o impedisce, in tutto o in parte, le comunicazioni telegrafiche o telefoniche, è punito con la reclusione da uno a tre anni e con la multa da lire 40.000 a lire 400.000». L'art. 1 è tuttora interessante per i seguenti, motivi, necessariamente sintetizzati:

- contiene già il concetto moderno di *jurisdictional reach* oltre le acque territoriali;
- tratta il danneggiamento dei cavi come reato contro la sicurezza collettiva, non come mero danno patrimoniale;
- riconosce che i cavi, anche inattivi o in manutenzione, restano beni giuridici protetti.

([65]) «Chiunque imbarca strumenti atti esclusivamente a spezzare o distruggere comunicazioni telegrafiche o telefoniche sottomarine è punito con l'ammenda da lire 40.000 a lire 400.000.
È punito con la stessa pena chiunque imbarca strumenti atti anche a spezzare o distruggere comunicazioni telegrafiche o telefoniche sottomarine, qualora non sia autorizzato a svolgere attività che richiedano l'impiego di tali strumenti.
Colui che, svolgendo le attività indicate nel comma precedente, rompe o guasta volontariamente un cavo od altro ordigno di una comunicazione telegrafica o telefonica sottomarina è punito a sensi dell'art. 1, ma le pene sono aumentate».

([66]) Punizione della mera imbarcazione di strumenti destinati esclusivamente a distruggere cavi telegrafici o telefonici sottomarini, comereato di pericolo astratto; punizione dell'imbarcazione di strumenti idonei anche a danneggiare tali cavi, in assenza di autorizzazione, come reato di pericolo concreto, subordinato al mancato possesso di titolo; punizione aggravata per chi,

ISSN 2038-1662

intendeva prevenire ogni possibile minaccia all'integrità dei cavi, trattandoli come beni strategici, essenziali per la sicurezza nazionale e le comunicazioni internazionali. L'ottica utilizzata è marcatamente general-preventiva: punire il fatto che vengano imbarcati strumenti significa intervenire a monte della lesione, nella logica di un diritto penale "di sicurezza" *ante litteram*.

A una medesima *ratio* – e alla medesima impronta criminalistica, che manterrebbe, si ribadisce, una sua attualità e una sua efficacia – sono ispirate anche la (tuttora vigente, sebbene ammodernata) legislazione britannica (*Submarine Telegraph Act* 1885) ([67]), che pure prevede pene per chiunque danneggi (dolosamente o anche colposamente) un cavo sottomarino ([68]), e quella australiana

autorizzato a operare sui cavi, li danneggi volontariamente, comereato di danno aggravato da abuso di qualifica o funzione.

([67]) https://www.legislation.gov.uk/ukpga/Vict/48-49/49

([68]) «*Punishment for violation of Article 2 of Convention.*
(1)A person shall not unlawfully and wilfully, or by culpable negligence, break or injure any submarine cable to which the Convention for the time being applies, in such manner as might interrupt or obstruct in whole or in part telegraphic communication.
(2)Any person who acts or attempts to act in contravention of this section shall be guilty of a misdemeanour, and on conviction—
(a)if he acted wilfully, shall be liable to penal servitude for a term not exceeding five years, or to imprisonment, ... , for a term not exceeding two years, and to a fine either in lieu of or in addition to such penal servitude or imprisonment; and
*(b)if he acted by culpable negligence, shall be liable to imprisonment for a term not exceeding three months. . , and to a fine not exceeding **o**ne hundred pounds either in lieu of or in addition to such imprisonment*».

ISSN 2038-1662

(*Telecommunication Act* del 1997, *Schedule* 3A), la quale consente all'*Australian Communications and Media Authority* (ACMA) di dichiarare zone di protezione per cavi sottomarini di "rilevanza nazionale". In queste zone, talune condotte pericolose (reti da pesca, ancoraggio vicino al fondale, scavo, ecc.) sono proibite o limitate, e danneggiare un cavo può comportare penalità fino a 10 anni di reclusione, multa, o entrambe ([69]).

In prospettiva, la legge italiana avrebbe potuto essere aggiornata trasformando il reato in un "danneggiamento di infrastruttura critica sottomarina", con estensione quindi della fattispecie e dell'alveo applicativo alle reti digitali, alla fibra ottica, e alle condotte attuabili in dominio *cyber* che ne compromettano il funzionamento. Ma così non è avvenuto.

Oltre a tale testo vi è poi il più recente Codice delle Comunicazioni Elettroniche (d. lgs. 1 agosto 2003 n. 259) ([70]), le cui ultime modifiche, tuttavia (avvenute ad opera della l. 22 aprile 2021, n. 55) ([71]), non hanno inciso sulla regolamentazione dei cavi sottomarini, come vedremo nelle prossime pagine.

([69]) https://classic.austlii.edu.au/au/legis/cth/consol_act/ta1997214/sch3a.html?utm_

([70]) https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003;259

([71]) https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2021-04-22;55

ISSN 2038-1662

4.1 *... presente: Il Codice delle Comunicazioni ElettronicheTelecomunicazioni*

Il Codice delle Comunicazioni Elettroniche è ispirato – per quanto, naturalmente, concerne la protezione dei cavi sottomarini – alla medesima, rigorosa matrice criminalistica che, come si è visto, caratterizza la normativa del 1956 ([72]).

A una valutazione d'insieme, non si può non evidenziare che manca, in Italia (e a dire il vero anche in altre Legislazioni europee,

([72]) A essere rilevanti – ai fini del discorso che qui si va conducendo – sono, in questo caso, gli articoli da 146 in poi. In particolare, l'art. 146 punisce chiunque rompe o guasta un cavo sottomarino o altro apparato facente parte di un impianto di comunicazione elettronica sottomarino; legalmente posto (cioè installato in conformità alle norme internazionali e nazionali) entro o fuori dalle acque territoriali, dunque con portata extraterritoriale, in coerenza con la Convenzione del 1884, che tutela anche le tratte internazionali, provocando un'interruzione o impedimento, totale o parziale, delle comunicazioni elettroniche. Inoltre – e riprendendo quanto già previsto e analizzato sopra a proposito della Legge del 1956 – l'art. 148 punisce «*c*hiunque imbarca strumenti atti a spezzare o distruggere impianti sottomarini di comunicazione elettronica è punito con la sanzione amministrativa pecuniaria da euro 150,00 a euro 1.500,00, salvo che non sia autorizzato a svolgere attività che richiedano l'impiego di tali strumenti». Infine, l'art. 149: esso si colloca in continuità logica con l'art. 146, ma con una differente impostazione soggettiva: mentre l'art. 146 punisce il danneggiamento doloso, l'art. 149 reprime il danneggiamento colposo dei cavi sottomarini di comunicazione elettronica. La *ratio* è evidente: anche un comportamento non intenzionale, se imprudente o negligente, può compromettere gravemente la sicurezza e la funzionalità delle comunicazioni elettroniche internazionali. L'art. 149 rappresenta un tassello fondamentale della responsabilità colposa in ambito marittimo e tecnologico, una sorta di "norma di chiusura" ed è volto a impedire che la pur minima leggerezza o l'imperizia compromettano la stabilità di un'infrastruttura su cui poggia l'intera economia digitale globale.

ISSN 2038-1662

comunque abbastanza complete, come quelle di Svezia, Finlandia, Norvegia, per citarne solo alcune), una definizione univoca completa e soprattutto aggiornata di cavo sottomarino, idonea a delinearne la natura giuridica e a distinguere chiaramente tra le diverse tipologie di infrastrutture sottomarine. Nel punire, dunque, il danneggiamento dei cavi sottomarini di comunicazione elettronica le norme limitano il loro ambito operativo al danno fisico e non si estendono pienamente al tema della protezione integrata delle informazioni trasmesse. Ciò evidenzia come, pur avendo già una base normativa di tutela, sarebbe quantomai opportuno ampliare questo perimetro.

Inoltre, non risulta siano mai stati elaborati criteri puntuali e trasparenti per la determinazione dei percorsi di posa, tali da orientare in modo equilibrato l'autonomia negoziale tra operatori di telecomunicazioni e grandi imprese tecnologiche. Si rileva, altresì, l'assenza di una disciplina chiara del regime proprietario dei cavi, che tenga conto della crescente partecipazione statale ai progetti di costruzione e posa e consenta di individuare con precisione i soggetti obbligati agli interventi di riparazione in caso di danneggiamento. Infine, sarebbe stata opportuna una modifica delle norme suggestiva di una più puntuale tipizzazione delle ipotesi di attacchi fisici e soprattutto informatici alle infrastrutture sottomarine, a cui avrebbe dovuto corrispondere quantomeno un proporzionale inasprimento e aggiornamento delle sanzioni, sia penali sia amministrative, sulla

ISSN 2038-1662

falsariga, ad esempio, della (molto rigida sul punto) legislazione specifica australiana ([73]).

4.2 … *e futuro: la nuova centralità della "dimensione subacquea"*

Un ulteriore passo verso il riconoscimento della rilevanza della dimensione subacquea è stato costituito dall'approvazione della l. 11 novembre 2022, n. 173 ([74]), a seguito della quale è stato poi stilato il

([73])L'articolo specifico che prevede pene criminali per danneggiamento di cavi sottomarini nelle «*protection zones*» è contenuto nella Telecommunications Act 1997 (Cth) — nello *Schedule* 3A – *Protection of submarine cables*, in particolare nella Division 4 (Offences), clausola 36 (*Offences in relation to a Protection Zone*) https://classic.austlii.edu.au/au/legis/cth/consol_act/ta1997214/sch3a.html?utm_source=chatgpt.com

([74])In base alla l. 16 dicembre 2022, n. 204, è stato istituito presso la Presidenza del Consiglio dei Ministri il Comitato interministeriale per le politiche del mare (CIPOM), con il compito di garantire — nel rispetto delle competenze delle singole Amministrazioni — la definizione e il coordinamento degli indirizzi strategici relativi alle politiche marittime nazionali. Il Comitato è presieduto dal Ministro per la Protezione civile e le Politiche del mare, delegato a tale funzione dal Presidente del Consiglio dei Ministri, e comprende i Ministri: per gli Affari europei, il Sud, le Politiche di coesione e il PNRR; degli Affari esteri e della Cooperazione internazionale; della Difesa; dell'Economia e delle finanze; delle Imprese e del Made in Italy; dell'Agricoltura, della Sovranità alimentare e delle Foreste; dell'Ambiente e della Sicurezza energetica; delle Infrastrutture e dei Trasporti; della Cultura; del Turismo; nonché il Ministro per gli Affari regionali e le autonomie. Il Comitato è supportato dalla Struttura di missione per le Politiche del mare, istituita presso la Presidenza del Consiglio dei Ministri e composta anche da dieci esperti di comprovata competenza. Con cadenza triennale, il CIPOM elabora e approva il "Piano del mare", documento programmatico che definisce gli indirizzi strategici e le linee guida della politica marittima nazionale.

ISSN 2038-1662

«Piano del Mare 2023-2025», corposo documento approvato il 31 luglio 2023 ([75]). Si tratta di uno strumento di programmazione strategica nazionale che orienta, in modo unitario e coordinato, tutte le politiche del mare e all'interno del quale, tuttavia, non si è andato oltre il riconoscimento, per vero piuttosto formale e scarno, della rilevanza strategica dei cavi sottomarini. Da ultimo, altra iniziativa da considerare in questa direzione è il d.p.r. 26 settembre 2025 il quale attua l'articolo 1, comma 2, della l. 14 giugno 2021, n. 91, che, in conformità a quanto previsto dalla Convenzione UNCLOS, consente di istituire una Zona Economica Esclusiva (fino a 200 miglia dal limite esterno del mare territoriale), con decreto del Presidente della Repubblica, da notificare agli Stati il cui territorio è adiacente al territorio dell'Italia o lo fronteggia ([76]).

([75]) piano-del-mare.pdf

([76])Nella Zona Economica Esclusiva (ZEE), lo Stato costiero esercita diritti sovrani per finalità di esplorazione, sfruttamento, conservazione e gestione delle risorse naturali, siano esse biologiche o non biologiche, presenti nelle acque sovrastanti il fondo marino, nel fondo stesso e nel relativo sottosuolo. Inoltre, lo Stato esercita la propria giurisdizione in materia di installazione e utilizzo di isole artificiali, impianti e strutture in mare, nonché in tema di ricerca scientifica marina e di protezione e conservazione dell'ambiente marino. L'estensione di tali diritti sovrani nella ZEE consente, in particolare, di promuovere lo sfruttamento sostenibile delle fonti di energia rinnovabile, tra cui l'eolico e il fotovoltaico offshore, oltre alla forza delle maree e delle correnti. Essa favorisce, inoltre, un miglior controllo e una gestione più efficiente dei giacimenti di idrocarburi situati nella piattaforma continentale sottostante, inclusi quelli condivisi con Stati limitrofi lungo le linee di delimitazione. Per un inquadramento della ZEE dal punto di vista teorico, si rinvia a M. DI LOLLO, *Il regime giuridico del Mar Mediterraneo e la zona economica esclusiva italiana: sicurezza energetica, ambiente e altre questioni*

ISSN 2038-1662

Dopo aver delineato i presupposti teorici della protezione *data-oriented* e i suoi strumenti di attuazione nei modelli AGOR e CTR, è possibile misurare la portata e la adattabilità di tale approccio al contesto nazionale. La recentissima Legge n. 9 del 2026 offre un banco di prova significativo: si tenterà, operativamente, di valutare in che misura la normativa italiana stia recependo, o al contrario trascuri, o almeno possa recuperare, la dimensione informativa della sicurezza marittima.

4.3 *Analisi delle definizioni normative e proposte di miglioramento*

La legge («Disposizioni in materia di sicurezza delle attività subacquee»), è stata approvata in via definitiva dalla Camera dei Deputati nella seduta del 21 gennaio 2026. Essa, stando alla Relazione Accompagnatoria, ha l'ambizione di disciplinare «l'accesso agli spazi subacquei, la protezione delle infrastrutture subacquee di interesse, energetiche e di comunicazione, la regolamentazione dei mezzi sottomarini e dei lavori subacquei e promuove la conoscenza e la protezione della dimensione subacquea nel suo complesso. In particolare […] disciplina le attività destinate

aperte, in *Il diritto marittimo*, 2, 2024, 434 ss.; A. LEANDRO, *Verso una zona economica esclusiva italiana*, in *Rivista di diritto internazionale*, 2021, 1081 ss.; ID., *La zona economica esclusiva italiana: ragioni, ambito, delimitazioni e sfide*, Bari, 2021

ISSN 2038-1662

a svolgersi nella dimensione subacquea in aree sottoposte alla sovranità o comunque alla giurisdizione nazionale e, limitatamente alle infrastrutture di interesse nazionale, nell'alto mare, per esigenze di sicurezza delle infrastrutture e di tutela della vita e delle persone operanti nella dimensione subacquea» (pag. 3) ([77]).

Il provvedimento, di iniziativa governativa, è nato dunque con l'obiettivo di garantire la sicurezza delle attività subacquee, disciplinando un settore finora regolato in modo, come si è constatato, comunque frammentario. Tra i meriti vi è senza dubbio proprio quello di riconoscere la necessità di una cornice normativa unitaria, aggiornata, per le operazioni svolte sotto la superficie marina: ma la legge, come vedremo, conserva un'impostazione tradizionale, interamente incentrata sulla sicurezza fisica delle persone e dei mezzi, in nulla innovando rispetto al Codice delle Comunicazioni Elettroniche. Il Legislatore muove dalla consapevolezza, tardiva ma purtuttavia necessaria, che i fondali marini siano oggi una delle principali superfici di rischio per la sicurezza nazionale.

Le proposte di miglioramento della legge qui suggerite introducono, ove necessario, una visione ancora più ampia e aggiornata: considerano, come più volte evidenziato, l'ambiente marino *tout-court* come spazio informativo non soltanto fisico e le attività subacquee come fonte di dati strategici, non solo come operazioni tecniche. Ponendo come metro di valutazione questa

([77]) https://documenti.camera.it/leg19/dossier/Pdf/TR0188.pdf

ISSN 2038-1662

prospettiva, la legge non tutelerebbe più soltanto i sub e gli operatori, ma anche l'ecosistema informativo che sottende le infrastrutture sottomarine.

Veniamo, in primo luogo, a un'analisi strutturale del Provvedimento, che si compone di 35 articoli distribuiti in 6 Capi: - il Capo I disciplina le «Politiche della dimensione subacquea» (artt. 1- 3); - il Capo II regolamenta l'istituenda «Agenzia per la sicurezza delle attività subacquee» (artt. 4-9); - il Capo III disciplina la «Navigazione subacquea, mezzi e infrastrutture subacquee» (artt. 10-17), articolandosi a sua volta in 4 sezioni; - il Capo IV regola le attività subacquee e iperbariche (artt. 18-25) articolandosi a sua volta in 3 sezioni; - il Capo V stabilisce le sanzioni applicabili (artt. 26-27); - il Capo VI reca le disposizioni finali e transitorie (28-35).

Di particolare rilievo, ai fini del discorso che qui si va conducendo, è sicuramente l'art. 2, il quale contiene una serie di "definizioni": tra esse, consideriamo le…

n) «infrastrutture subacquee di interesse nazionale»: le infrastrutture subacquee che possiedono uno o più requisiti tra quelli di seguito indicati, individuate con decreto del Presidente del Consiglio dei ministri o dell'Autorità politica delegata per le politiche del mare ove nominata, sentiti il Comitato interministeriale per le politiche del mare e, per i profili di competenza, l'Agenzia per la cybersicurezza nazionale, su proposta del Ministro delle imprese e del made in Italy, del Ministro della difesa, del Ministro dell'università e della ricerca, del Ministro delle infrastrutture e dei

ISSN 2038-1662

trasporti o del Ministro dell'ambiente e della sicurezza energetica, secondo le rispettive competenze:

1) essere di proprietà di soggetti di nazionalità italiana o di amministrazioni pubbliche di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, ovunque localizzate;

2) essere rilevanti per la connessione, le comunicazioni e i servizi digitali o il rifornimento del territorio nazionale o di installazioni nazionali situate nella zona economica esclusiva nazionale o nella piattaforma continentale;

3) presentare potenziali rischi di carattere ambientale per il territorio nazionale o per le zone marittime sottoposte alla giurisdizione nazionale».

Tra le infrastrutture (non definite critiche ma) di interesse nazionale rientrano, implicitamente, per le caratteristiche delineate dalla norma, i cavi sottomarini. Essi, configurati in modo incidentale come elementi infrastrutturali, non vengono tuttavia definiti né qualificati come oggetto autonomo di tutela. Il testo, dunque, resta ancorato a una concezione puramente materiale: il mare come ambiente fisico, il cavo come manufatto ingegneristico, (uno dei tanti, neanche il più rilevante forse) e la sicurezza come protezione da (soli) eventi meccanici o accidentali. Questa impostazione non appare, a mio avviso, sufficiente. I cavi, si ribadisce, oggi sono sistemi informativi intelligenti, capaci di generare e trasmettere dati in tempo reale su condizioni ambientali, tensione, temperatura e traffico di rete. La loro integrità non dipende solo dalla robustezza

ISSN 2038-1662

del materiale, ma dalla sicurezza dei flussi informativi che li attraversano. L'impressione che si ricava è che il Legislatore avrebbe potuto dire, e fare, sul punto, di più.

Una definizione alternativa, idealmente una lettera *n-bis*, completa e aderente alle moderne caratteristiche dei cavi sottomarini sin qui evidenziate potrebbe essere la seguente:

«cavo sottomarino: infrastruttura fisica costituita da uno o più conduttori o fibre ottiche, installata sul fondale marino, destinata alla trasmissione di energia, dati o segnali elettronici tra due o più punti costieri o subacquei; essa comprende i sistemi ausiliari di alimentazione, i sensori integrati, i nodi di amplificazione e i dispositivi di monitoraggio. I cavi sottomarini costituiscono infrastrutture di comunicazione e di dati, e sono pertanto soggetti alle norme di sicurezza fisica e informativa della presente legge. I cavi sottomarini che trasportano dati o energia, anche a uso misto, costituiscono infrastrutture critiche nazionali ed europee ai sensi della Direttiva (UE) 2022/2555 (NIS2)».

Tale formulazione prospetterebbe una svolta non solo terminologica, ma sostanziale: implicherebbe che i cavi siano soggetti non soltanto a controlli tecnici, ma anche agli obblighi di protezione e trasparenza previsti dal diritto europeo dei dati. In tal modo, la legge nazionale si allineerebbe al *Data Act*, alla Direttiva NIS2 e al *Data Governance Act*, collocando la sicurezza subacquea entro la più ampia cornice della sovranità digitale europea. La novità

ISSN 2038-1662

consiste nel cambiare l'oggetto giuridico: il bene da tutelare non è soltanto la struttura, ma l'informazione che la struttura veicola.

Un'ulteriore ramificazione della definizione potrebbe, poi, comprendere anche il concetto, utile da un punto di vista normativo, di "dato subacqueo", per tale intendendosi «qualsiasi informazione, di natura tecnica, ambientale, operativa o digitale, generata o trasmessa da infrastrutture subacquee o da apparati connessi». Importanti, poi – nell'ottica complessiva della proposta operativa qui suggerita – risulterebbero anche le definizioni di …

*«…d) I*ntermediario Neutrale dei Dati Marini: soggetto pubblico o privato accreditato ai sensi del Regolamento (UE) 2022/868 (Data Governance Act), incaricato di garantire la tracciabilità, la cifratura e la neutralità dei flussi di dati marini e subacquei;

e) accesso graduato ai dati: regime di apertura proporzionata fondato sul modello di Apertura Graduata Orientata al Rischio (AGOR);

f) contratto di trasparenza reciproca (CTR): accordo giuridico tra soggetti pubblici o privati volto a regolare scopi, limiti, auditabilità e reciprocità nell'uso dei dati marini e subacquei*».*

Idealmente, un articolo 2 *bis* potrebbe essere dedicato, dopo aver posto la definizione dei cavi sottomarini stessi, al loro specifico regime giuridico, con un tenore letterale di tal fatta:

1. «I cavi sottomarini sono sottoposti a misure di protezione fisica, informatica e informativa coerenti con le migliori pratiche tecniche europee.

ISSN 2038-1662

2. I gestori e gli operatori dei cavi sottomarini hanno l'obbligo di:

a) predisporre sistemi di monitoraggio continuo e di raccolta dati relativi all'integrità fisica e alle condizioni ambientali del cavo;

b) condividere con l'Intermediario Neutrale dei Dati Marini (INDM) i dati tecnici essenziali per la prevenzione di guasti o interferenze, secondo i protocolli stabiliti dal regolamento attuativo;

c) segnalare tempestivamente alle autorità competenti ogni anomalia o incidente che possa compromettere la sicurezza fisica o informativa del cavo.

3. I dati generati dalle infrastrutture sottomarine sono considerati dati a rilevanza pubblica strategica. Essi sono soggetti al principio di accesso graduato (AGOR) e al regime di trasparenza reciproca (CTR), garantendo la possibilità di utilizzo per finalità di sicurezza, ricerca scientifica e cooperazione internazionale.

4. Il Governo promuove accordi con altri Stati e organizzazioni internazionali per assicurare la protezione coordinata dei cavi sottomarini, nel rispetto del principio di sovranità informativa cooperativa e delle disposizioni della Convenzione UNCLOS».

4.4 *L'Agenzia per la Sicurezza delle Attività Subacquee: una gestione accentrata dell'ecosistema sottomarino*

Tornando all'esame del testo di legge, poniamo l'attenzione sull'art. 4, istitutivo, per la prima volta nell'ordinamento italiano, di

ISSN 2038-1662

un' Agenzia per la Sicurezza delle Attività Subacquee, la cui organizzazione e le cui molteplici e rilevanti funzioni sono regolate in dettaglio dagli articoli successivi. Le prerogative attribuite dalla legge all'Agenzia sono articolate e rilevanti, sul piano tecnico, della sicurezza, e anche della promozione della ricerca e della divulgazione scientifica([78]).

([78])Art. 6. *(Funzioni dell'Agenzia)*
«1. L'Agenzia, in particolare:
a) coordina, in raccordo con il Ministero degli affari esteri e della cooperazione internazionale e il Ministero delle infrastrutture e dei trasporti, la cooperazione internazionale ed europea nella materia subacquea. Ferme restando le competenze dei predetti Ministeri, cura i rapporti con i competenti organismi, istituzioni ed enti europei e internazionali, nonché segue nelle competenti sedi istituzionali le tematiche della dimensione subacquea in relazione ai compiti ad essa assegnati, fatta eccezione per gli ambiti in cui la legge attribuisce specifiche competenze ad altre amministrazioni. In tali casi, è comunque assicurato il raccordo con l'Agenzia al fine di garantire posizioni nazionali unitarie e coerenti con le politiche della subacquea, come definite dal Presidente del Consiglio dei ministri o dall'Autorità politica delegata per le politiche del mare ove nominata, ai sensi dell'articolo 3;
b) coordina e controlla le attività subacquee civili, al fine di evitare interferenze tra attività subacquee militari, di polizia e civili ai sensi di quanto previsto dagli articoli 10 e 12;
c) autorizza la navigazione in immersione dei sommergibili civili battenti bandiera diversa da quella italiana durante il passaggio inoffensivo nelle acque territoriali o la messa a mare da navi battenti bandiera diversa da quella italiana di veicoli subacquei ai sensi di quanto previsto dall'articolo 10;
d) segnala alle competenti amministrazioni le situazioni di interferenza tra attività subacquee, rilevate nello svolgimento degli altri compiti istituzionali;
e) definisce, in conformità agli standard internazionali, le misure necessarie per prevenire, attenuare o eliminare pericoli gravi e imminenti al territorio nazionale e alle zone marittime sottoposte alla giurisdizione nazionale, imputabili ad attività antropica rischiosa svolta nella dimensione subacquea, ai

ISSN 2038-1662

sensi di quanto previsto dall'articolo 13, fatto salvo quanto previsto dal codice della protezione civile, di cui al decreto legislativo 2 gennaio 2018, n. 1;
f) promuove l'analisi e lo studio dei rischi connessi alla presenza nella dimensione subacquea di manufatti, relitti e infrastrutture pericolosi per la sicurezza della navigazione subacquea, adottando linee guida non vincolanti ai sensi di quanto previsto dall'articolo 17;
g) definisce la regolamentazione tecnica, nel rispetto di quanto previsto dagli articoli 15, 16 e 21, dei requisiti per l'abilitazione al comando e alla conduzione di mezzi subacquei, delle caratteristiche e delle dotazioni minime di sicurezza dei mezzi subacquei non militari idonei alla navigazione subacquea, nonché, ai sensi di quanto previsto dall'articolo 21, del percorso di formazione per l'iscrizione nel registro degli operatori subacquei e iperbarici professionali e delle modalità di accertamento dell'idoneità alla mansione ai fini dell'iscrizione nel medesimo registro;
h) promuove lo sviluppo della capacità nazionale di soccorso ed estrazione di persone da mezzi subacquei civili sinistrati ai sensi di quanto previsto dall'articolo 14;
i) concorre alla promozione, perseguendo obiettivi di eccellenza negli ambiti di competenza, mediante il coinvolgimento del Ministero dell'università e della ricerca e del sistema dell'università e della ricerca, della Marina militare, del Servizio nazionale della protezione civile, del Ministero della cultura, del Ministero delle imprese e del made in Italy, del Ministero delle infrastrutture e dei trasporti nonché del sistema produttivo nazionale, dello sviluppo di competenze e capacità tecnologiche e scientifiche in materia subacquea, anche ai sensi di quanto previsto dall'articolo 17;
l) promuove, in collaborazione con l'Istituto idrografico della Marina militare nonché con le università e gli enti pubblici di ricerca, la conoscenza multidisciplinare dell'ambiente subacqueo, dal punto di vista idrografico, oceanografico e geofisico, raccordando tutte le conoscenze tecnologiche e scientifiche e le attività di rilievo opportunamente validate;
m) promuove la cultura della sicurezza in relazione alla navigazione e alle attività subacquee attraverso l'organizzazione di eventi, convegni, giornate di studio e attività divulgativa nelle scuole e nelle università;
n) promuove accordi internazionali, nonché stipula in nome proprio intese tecniche, anche con il coinvolgimento del settore privato, con istituzioni, enti e

ISSN 2038-1662

organismi di altri Paesi per la partecipazione dell'Italia a programmi sulla dimensione subacquea, assicurando il necessario raccordo con le altre amministrazioni a cui la legge attribuisce competenze in materia subacquea, ferme restando le competenze del Ministero degli affari esteri e della cooperazione internazionale e del Ministero delle infrastrutture e dei trasporti;
o) valorizza i risultati dell'attività di ricerca e innovazione condotta nell'ambito di iniziative nazionali, europee e internazionali alle quali partecipano gli enti pubblici di ricerca e le università;
p) svolge attività di comunicazione e promozione della consapevolezza in materia subacquea, al fine di contribuire allo sviluppo di una cultura nazionale in materia;
q) promuove, in collaborazione con il Ministero dell'università e della ricerca e con le università e gli enti pubblici di ricerca, la formazione, la crescita tecnico-professionale e la qualificazione delle risorse umane in ambito subacqueo, in particolare favorendo l'attivazione di percorsi formativi universitari in materia, anche attraverso l'assegnazione di borse di studio e di dottorato e di contratti di collaborazione alla ricerca, sulla base di apposite convenzioni con soggetti pubblici e privati;
r) può predisporre attività di formazione specifica, in collaborazione con le università e gli enti pubblici di ricerca, riservate ai giovani che aderiscono al servizio civile universale regolate sulla base di apposite convenzioni. In ogni caso, il servizio prestato è, a tutti gli effetti, riconosciuto come servizio civile universale;
s) concorre, ai sensi di quanto previsto dall'articolo 19, nella regolazione delle attività subacquee e iperbariche di protezione civile di cui all'articolo 18, comma 3;
t) può prescrivere, per ragioni di interesse pubblico, l'installazione su infrastrutture e mezzi che afferiscono alla dimensione subacquea di apparati, strumenti di misura e sensori, con riferimento alle migliori tecnologie disponibili, per il monitoraggio sismico, ambientale e di sicurezza, la rilevazione di eventuali minacce nonché la condivisione di dati e informazioni in tal modo acquisiti, ai sensi di quanto previsto dall'articolo 15, prevedendo forme di coinvolgimento del Ministero della cultura in relazione all'individuazione di possibili interferenze con il patrimonio culturale;

ISSN 2038-1662

Sembra assumere un certo rilievo il compito di definire misure di protezione per le infrastrutture subacquee, inclusi i cavi sottomarini([79]). Si prevede – e la misura appare adeguata e quantomai

u) accerta il carattere temporaneo e occasionale della prestazione professionale e si pronuncia sulle domande di riconoscimento della relativa qualifica professionale conseguita all'estero ai sensi di quanto previsto dall'articolo 22;
v) concorre nella regolazione del libretto personale informatico degli operatori subacquei e iperbarici professionali ai sensi di quanto previsto dall'articolo 24».

([79]) Art. 6 Funzioni dell'Agenzia, lett. *e)* [L'Agenzia, n.d.a.]… «definisce, in conformità agli standard internazionali, le misure necessarie per prevenire, attenuare o eliminare pericoli gravi e imminenti al territorio nazionale e alle zone marittime sottoposte alla giurisdizione nazionale, imputabili ad attività antropica rischiosa svolta nella dimensione subacquea, ai sensi di quanto previsto dall'articolo 13, fatto salvo quanto previsto dal codice della protezione civile, di cui al decreto legislativo 2 gennaio 2018, n. 1».

Il compito, proprio dell'Agenzia, di proteggere le infrastrutture critiche, e in particolare proprio i cavi sottomarini, viene delineato, però, più chiaramente in un altro articolo (art.10): «*c*hiunque intenda svolgere attività della dimensione subacquea nelle acque marine interne o nel mare territoriale, ovvero, in relazione alla piattaforma continentale o alla zona economica esclusiva, attività della dimensione subacquea relative a diritti o poteri giurisdizionali attribuiti allo Stato costiero dalle norme internazionali vigenti, comunica all'Agenzia, con un preavviso minimo di quindici giorni, fatti salvi i casi di urgenza e le operazioni di soccorso e protezione civile, le attività da svolgere, il giorno o i giorni in cui le stesse saranno svolte, con l'indicazione dell'ora della programmata attività, nonché gli eventuali titoli amministrativi abilitativi, rilasciati dalle competenti amministrazioni pubbliche, sulla base dei quali le attività saranno svolte.
2. L'Agenzia trasmette senza indugio la comunicazione di cui al comma 1 alle competenti autorità militari, marittime, di pubblica sicurezza e di polizia giudiziaria e, entro dieci giorni dalla medesima comunicazione, adotta le misure di cui al comma 3 qualora le attività di cui al comma 1:
a) interferiscano con attività subacquee civili precedentemente comunicate ai sensi del comma 1 o autorizzate ai sensi del comma 4;

ISSN 2038-1662

opportuna – la mappatura preventiva delle aree sensibili, il monitoraggio tramite la Marina Militare e il coinvolgimento delle autorità marittime e di sicurezza anche per quello che riguarda la delicata fase della pianificazione della posa dei cavi sottomarini stessi nelle traiettorie che insistano sulla piattaforma continentale nazionale([80]).

b) interferiscano con altre attività civili che si svolgono in superficie precedentemente comunicate o autorizzate dall'autorità marittima competente ai sensi della disciplina vigente;
c) interferiscano con attività subacquee o di superficie militari o civili segnalate all'Agenzia dall'autorità competente entro cinque giorni dal ricevimento della comunicazione di cui all'alinea;
d) **siano idonee a determinare la manomissione, il danneggiamento o la distruzione di cavi, condotte sottomarine, isole artificiali, installazioni o altre strutture** (grassetto nostro)
3. Al ricorrere delle condizioni previste dalle lettere da a) a d) del comma 2, l'Agenzia, con proprio provvedimento, adotta le misure di mitigazione dei rischi di interferenza necessarie per permettere lo svolgimento in sicurezza dell'attività comunicata. A tali fini, l'Agenzia può, altresì, ordinare il rispetto di apposite zone di sicurezza o individuare un diverso contesto spaziale o temporale in cui può essere svolta l'attività comunicata. Il provvedimento di cui al primo periodo del presente comma è immediatamente trasmesso al soggetto che ha effettuato la comunicazione e alle autorità di polizia giudiziaria e di pubblica sicurezza che svolgono funzioni di polizia terrestre e marittima».

[80]Cfr., a tal riguardo, l'art. 13: «(Sicurezza delle infrastrutture subacquee)
1. Ferme restando le discipline nazionali di attuazione della direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, nonché della direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, e in raccordo con le autorità competenti ai sensi delle rispettive discipline attuative, l'Agenzia, nel rispetto delle direttive adottate dal Presidente del Consiglio dei ministri o dell'Autorità politica delegata per le politiche del mare ove nominata, ai sensi dell'articolo 3, comma 3, della presente legge definisce le misure di cui al comma 2 del presente articolo,

ISSN 2038-1662

Una delle novità più interessanti riguarda le modifiche (attraverso la tecnica della novellazione) al Codice dell'Ordinamento Militare: la Marina Militare potrà infatti ordinare ed eseguire l'ingaggio, la

necessarie per evitare rischi di interferenza in danno delle infrastrutture subacquee nelle zone marittime sottoposte alla giurisdizione nazionale e, limitatamente a quelle di interesse nazionale appartenenti a soggetti di nazionalità italiana, anche nell'alto mare.
2. L'Agenzia, nell'esercizio delle funzioni di cui al comma 1, può:
a) individuare e monitorare, avvalendosi della Centrale operativa e degli assetti della Marina militare, le attività subacquee che possono determinare, per tipologia, prossimità o quota, un rischio per piattaforme, isole artificiali, infrastrutture e strumentazione di ricerca, cavi e condotte in aree soggette alla giurisdizione nazionale;
b) concorrere a definire le misure per la verifica, la ricognizione, il monitoraggio e la sorveglianza dell'intera rete delle infrastrutture subacquee di interesse nazionale, promuovendo l'impiego sinergico dei rispettivi mezzi e la condivisione delle informazioni ottenute;
c) concorrere a definire i piani di emergenza per il ripristino della funzionalità di cavi e condotte oggetto di rottura, la prevenzione, la mitigazione e il contrasto degli inquinamenti anche in adempimento alla normativa europea e procedure per interventi di necessità e urgenza di manutenzione e riparazione di cavi e condutture posizionati sulla piattaforma continentale nazionale, fatto salvo quanto previsto dall'articolo 24, comma 8, del codice della protezione civile, di cui al decreto legislativo 2 gennaio 2018, n. 1;
d) promuovere il coordinamento tra le amministrazioni competenti, per definire le misure idonee a consentire il recupero di eccedenze di banda o di flusso tra i differenti utilizzatori al fine di sopperire a situazioni di interruzione o rottura di cavi e condutture;
e) concorrere a definire, in merito ad aspetti di sicurezza afferenti alle attività subacquee, il percorso dei cavi e delle condutture da posare sulla piattaforma continentale nazionale e, sentiti i gestori delle infrastrutture interessate, i criteri da osservare nelle fasi di studio dei corridoi per l'individuazione del percorso dei cavi e delle condutture».

ISSN 2038-1662

disabilitazione, la distruzione o il sequestro di mezzi che minaccino cavi sottomarini di interesse nazionale, nonché disporre il dirottamento dei mezzi stessi verso porti italiani([81]). Queste disposizioni si inseriscono nel solco di quanto comunque previsto dalla UNCLOS, che agli articoli 112-115 garantisce a tutti gli Stati il

[81] A tal riguardo, cfr. le disposizioni finali e transitorie di cui all'art. 28: «1. All'articolo 111, comma 1, del codice dell'ordinamento militare, di cui al decreto legislativo 15 marzo 2010, n. 66, dopo la lettera d) sono aggiunte le seguenti:
«d-bis) la regolamentazione tecnica della navigazione subacquea militare e, nel rispetto delle direttive in materia di politiche della dimensione subacquea del Presidente del Consiglio dei ministri o dell'Autorità politica delegata per le politiche del mare ove nominata, dei titoli abilitanti alla conduzione o al controllo di mezzi subacquei militari con equipaggio, autonomi o a pilotaggio remoto;
d-ter) la protezione dell'infrastruttura subacquea nazionale mediante uso della forza, nel rispetto della normativa vigente e in caso di violazione dei limiti posti dalla legge alla navigazione subacquea. A tale fine, ferme restando le competenze del Corpo della Guardia di finanza ai sensi del decreto legislativo 19 agosto 2016, n. 177, la Marina militare può **ordinare ed eseguire l'ingaggio, la disabilitazione, la distruzione, il sequestro o il dirottamento in un porto dello Stato di qualsiasi mezzo intento alla distruzione, al danneggiamento o alla manomissione di condutture e cavi sottomarini che approdano nel territorio nazionale o sono di interesse nazionale ai sensi della normativa vigente**; (grassetto nostro)
d-quater) il controllo nelle acque interne nazionali, nel mare territoriale nazionale e nella piattaforma continentale nazionale, per fini di difesa militare dello Stato e, per le medesime finalità, la prevenzione della navigazione subacquea non autorizzata;
d-quinquies) la cooperazione con le marine militari di Stati alleati o confinanti, nel rispetto delle direttive del Ministro della difesa, per la vigilanza delle infrastrutture subacquee».

ISSN 2038-1662

diritto di posare cavi sottomarini, unitamente ad obblighi di protezione e di riparazione in caso di danneggiamento. Spetta, poi, all'Agenzia promuovere lo sviluppo di tecnologie di soccorso subacqueo e interfacciarsi con organismi europei e internazionali: un ruolo di coordinamento già delineato dal cosiddetto «Piano del mare», ma che ora, finalmente, si consolida e si concretizza attraverso una struttura dedicata.

I rilievi da formulare a proposito delle norme disciplinanti il funzionamento dell'Agenzia possono investire il piano politico e quello tecnico-giuridico.

La nascita di un'Agenzia per la sicurezza subacquea rappresenta sicuramente un passo avanti notevole in termini di coordinamento, modernità e pianificazione. Ma l'efficacia della sua azione dipenderà dalla reale dotazione di risorse – finanziarie, tecnologiche e umane – che riceverà. L'esperienza di altre agenzie italiane dimostra che il rischio di duplicazioni burocratiche e sovrapposizioni di competenze sia tutt'altro che remoto. L'Agenzia, infatti, dovrà operare in costante raccordo con Marina Militare, Guardia di Finanza, Capitanerie di Porto e almeno due Ministeri chiave – Esteri e Infrastrutture. Un intreccio istituzionale che, se non adeguatamente gestito, rischia di trasformarsi in una *impasse* amministrativa difficile da snellire e ancor di più da coordinare.

Un secondo nodo critico riguarda i nuovi poteri attribuiti alla Marina Militare e in particolare l'uso della forza in alto mare. Una attribuzione che, seppur legittima nel quadro del diritto

ISSN 2038-1662

internazionale in presenza di minacce manifeste, espone l'Italia a scenari delicati e potenzialmente destabilizzanti. Identificare con certezza un "mezzo ostile" in ambiente subacqueo è tutt'altro che semplice: un errore di valutazione, o un intervento in acque internazionali contro un mezzo straniero, potrebbe talvolta innescare tensioni diplomatiche.

Ancora più complesso si prospetta il profilo operativo. Sorvegliare migliaia di chilometri di cavi e condotte sottomarine con strumenti convenzionali è un obiettivo tecnologicamente ambizioso ma logisticamente insostenibile. Il coinvolgimento della Marina rappresenta un primo passo importante, ma da solo non può assicurare né una copertura capillare, né una risposta tempestiva in caso di attacco o sabotaggio. La dipendenza da sensori, droni e satelliti civili o industriali introduce inoltre nuove vulnerabilità, soprattutto sul fronte della *cybersecurity* e del coordinamento intersettoriale.

Infine, meriterebbe maggiore attenzione il tema della cooperazione internazionale, imprescindibile poiché quasi nessun cavo sottomarino appartiene a un solo Stato. Il quadro normativo *in fieri* rischia così di rimanere ambizioso sul piano nazionale ma isolato sul piano strategico, se non accompagnato da una diplomazia tecnica proattiva con gli alleati europei e della NATO.

Dal punto di vista economico, la creazione dell'Agenzia può fungere positivamente da catalizzatore per lo sviluppo di un settore ad alto potenziale innovativo. Attraverso la promozione della ricerca

ISSN 2038-1662

scientifica e della collaborazione tra pubblico e privato, l'ente potrebbe sostenere la crescita di filiere tecnologiche avanzate legate alla cantieristica subacquea, alla manutenzione offshore, al monitoraggio ambientale e alle infrastrutture energetiche marine. Ciò avrebbe riflessi positivi anche sulla competitività internazionale delle imprese italiane, rafforzando il ruolo del Paese nei mercati emergenti legati alla cosiddetta *Blue Economy*.

Un ulteriore aspetto positivo riguarda, naturalmente, la tutela dell'ambiente marino e delle infrastrutture sottomarine. L'Agenzia avrebbe le competenze per fornire un supporto tecnico-specialistico alle autorità competenti per la protezione degli ecosistemi marini, per la gestione dei rischi ambientali e per la prevenzione di incidenti connessi alle attività subacquee. La possibilità di integrare le funzioni dell'Agenzia con le strategie nazionali sulla transizione ecologica rappresenta un elemento di grande valore, in linea con gli obiettivi europei di sostenibilità e resilienza delle infrastrutture critiche. L'Agenzia potrà fungere da raccordo tra Università, Centri di Ricerca e operatori del settore, promuovendo progetti congiunti, percorsi formativi specializzati e programmi di scambio a livello internazionale. Ciò contribuirebbe a creare una comunità scientifica e professionale più coesa, capace di alimentare innovazione e conoscenza nel campo, attualissimo, delle tecnologie subacquee e iperbariche.

Particolarmente interessante è anche la prospettiva di valorizzazione della subacquea civile, sportiva e culturale. La legge

ISSN 2038-1662

riconosce infatti l'importanza delle attività subacquee non solo come risorsa economica e tecnica, ma anche come strumento di promozione culturale e turistica. La tutela e la fruizione dei beni archeologici sommersi, la diffusione della cultura del mare e la promozione della subacquea ricreativa in sicurezza rientrano tra gli obiettivi di un approccio più ampio e inclusivo alla gestione del patrimonio marino.

Infine, l'istituzione dell'Agenzia presenta una chiara valenza strategica e geopolitica. L'Italia, al centro del Mediterraneo e sede di importanti infrastrutture sottomarine – dai gasdotti ai cavi di telecomunicazione – avrebbe la possibilità di rafforzare le proprie capacità di monitoraggio e protezione, contribuendo alla sicurezza energetica e informatica nazionale. In questo senso, l'Ente in questione si porrebbe anche come interlocutore tecnico nei programmi europei e internazionali sulla protezione delle infrastrutture critiche e sulla resilienza marittima, consolidando la posizione del Paese all'interno delle reti di cooperazione NATO e dell'Unione Europea.

Anche da un punto di vista più squisitamente tecnico-giuridico, l'istituzione di una Autorità governativa autonoma – incardinata nella Presidenza del Consiglio – specificamente dotata di poteri per monitorare rischi, definire misure di sicurezza, preparare piani di emergenza e coordinare il recupero di flussi interrotti, concorrere alla definizione del percorso di cavi e dei criteri da osservare per la sua l'individuazione, va salutata con favore. L'Italia si pone, sul punto,

ISSN 2038-1662

nella scia di Paesi all'avanguardia nella protezione dei cavi sottomarini, come l'Australia (in cui opera la c.d. *Australian Communications and Media Authority*, la quale, tra l'altro, come si è osservato può dichiarare «*protection zones*» attorno a cavi sottomarini considerati di «*national significance*», limitando alcune attività potenzialmente dannose)([82]) o Singapore([83]) (che ha istituito l'*Info-communications Media Development Authority*, la quale ha fissato regolamenti peraltro molto accurati per l'installazione, la manutenzione e la riparazione di sistemi di cavi sottomarini, con permessi e linee guida specifiche).

5. *Valutazioni conclusive e spunti di riflessione*

Nel complesso, dunque, la legge che disciplina le attività subacquee e iperbariche in Italia rappresenta un tentativo organico e ambizioso di colmare un vuoto normativo che da tempo caratterizzava il settore. Essa introduce principi di coordinamento, sicurezza e razionalizzazione amministrativa che, visti nel quadro generale, appaiono positivi. Tuttavia, un'analisi più approfondita rivela anche alcune criticità strutturali, in particolare per quanto riguarda la disciplina dei cavi sottomarini e, più in generale, la definizione del regime giuridico delle infrastrutture subacquee

([82]) https://www.acma.gov.au/submarine-cables
([83]) https://www.imda.gov.sg/regulations-and-licensing-listing/deployment-and-repair-of-submarine-cable-systems

ISSN 2038-1662

considerate nel loro potenziale rilevante per la circolazione dei dati sui fondali marini e non solo.

Accanto ad aspetti positivi, emergono alcune debolezze concettuali e applicative che incidono sulla coerenza complessiva della legge. In particolare, si ribadisce che la disciplina delle infrastrutture sottomarine, e dei cavi sottomarini in specie, risulta ancora parziale e in alcuni punti ambigua. Pur alludendo a tali infrastrutture tra gli oggetti delle attività regolamentate, come si è evidenziato, la legge non fornisce una definizione chiara né ne specifica con precisione la natura giuridica. Non è esplicitato, di conseguenza, se i cavi sottomarini siano considerati beni di interesse pubblico soggetti a vincoli specifici, o se debbano essere trattati secondo il regime privatistico delle opere civili, con notevole incertezza a proposito di responsabilità, manutenzione e poteri di intervento dello Stato.

Anche il rapporto tra diritto interno e diritto internazionale del mare rimane poco sviluppato. La normativa non integra in modo sistematico i principi contenuti nella Convenzione UNCLOS, né chiarisce come intendere i limiti alla libertà di posa o le modalità di protezione dei cavi in acque internazionali o nella piattaforma continentale. La scelta di rinviare genericamente agli "obblighi internazionali" appare insufficiente in un contesto geopolitico in cui le infrastrutture subacquee, soprattutto i cavi di telecomunicazione e le condotte energetiche, sono divenute elementi strategici e vulnerabili della sicurezza nazionale.

ISSN 2038-1662

Un ulteriore punto debole riguarda l'assenza di una disciplina chiara in materia di protezione e responsabilità. La legge prevede strumenti di intervento, anche militari, in caso di minaccia alle infrastrutture, ma non stabilisce con sufficiente precisione le procedure di accertamento dei danni, gli obblighi di comunicazione o i meccanismi di indennizzo. Non è chiaro, ad esempio, come si articoli la responsabilità per danni causati da attività civili, o quale sia il regime assicurativo e risarcitorio in caso di incidenti che coinvolgano operatori privati. Questa lacuna rischia di rendere difficile l'attuazione concreta delle tutele previste e di alimentare contenziosi.

Va poi osservato che la legge non affronta in modo organico il tema del bilanciamento tra interessi pubblici e privati. Gran parte delle infrastrutture subacquee, in particolare i cavi di telecomunicazione, appartengono a soggetti privati o a consorzi internazionali([84]), mentre lo Stato conserva poteri di vigilanza e sicurezza. La mancanza di regole precise in merito alla ripartizione delle competenze e alla risoluzione dei conflitti di interesse (ad esempio in caso di interferenze tra opere civili e vincoli ambientali o militari) costituisce un elemento di incertezza che potrebbe ostacolare gli investimenti e rallentare i processi autorizzativi.

([84]) Fondamentale A. GANZ, M. CAMELLINI, E. HINE, C.NOVELLI, H. ROBERTS, L. FLORIDI, *Submarine Cables and the Risks to Digital Sovereignty*, in *Minds and Machines*, 34, 2024, 1 ss.

ISSN 2038-1662

Infine, la legge non prevede un regime transitorio chiaro per le infrastrutture già esistenti né per i progetti in corso di autorizzazione. Questo silenzio rischia di generare una discontinuità applicativa e di compromettere la certezza del diritto in un settore in cui i tempi di progettazione e realizzazione delle opere sono molto lunghi e richiedono stabilità normativa.

Nel valutare poi il profilo, ritenuto centrale in questo lavoro, della protezione dei dati personali e non, nella Legge commentata emerge un quadro ancora acerbo, incompleto, quasi frettoloso. Il testo normativo rappresenta un passo verso l'introduzione di garanzie specifiche in un settore che, per sua natura, implica il trattamento di una vasta gamma di dati – dai dati personali e professionali degli operatori, alle informazioni tecniche, infrastrutturali e di sicurezza – ma non riesce a fornire un sistema pienamente coerente con gli illustrati principi di *accountability* e trasparenza espressi nel GDPR e della normativa nazionale di attuazione.

Va riconosciuto al legislatore il merito di aver introdotto, sul punto, alcune previsioni di rilievo, come il vincolo di segretezza imposto al personale dell'Agenzia anche dopo la cessazione del rapporto di servizio([85]), e l'istituzione di un «libretto personale informatico» ([86])

([85]) Cfr. art. 8, comma 5: «Il personale che presta comunque la propria opera alle dipendenze o in favore dell'Agenzia è tenuto, anche dopo la cessazione di tale attività, al rispetto del segreto su ciò di cui sia venuto a conoscenza nell'esercizio o a causa delle proprie funzioni»
([86]) Cfr. art. 24

ISSN 2038-1662

per gli operatori subacquei, destinato a raccogliere dati identificativi e professionali.

Queste disposizioni, insieme all'art. 12, dedicato specificamente alla «cooperazione informativa», in cui è presente uno dei pochi riferimenti (se ne contano 5) ai "dati", testimoniano una consapevolezza, almeno iniziale, dell'importanza di disciplinare la circolazione e la tutela delle informazioni trattate nell'ambito delle attività subacquee.

Un'altra criticità riguarda la trasparenza nei confronti degli interessati. La legge non stabilisce procedure specifiche per garantire l'informativa, l'accesso, la rettifica o la cancellazione dei dati personali, né indica come tali diritti possano essere esercitati in contesti operativi complessi come quelli subacquei. La mancanza di un riferimento esplicito a questi diritti fondamentali rischia di rendere la tutela dei dati meramente formale, priva di strumenti concreti di attuazione.

Particolare attenzione avrebbero meritato, inoltre, i dati tecnici e infrastrutturali ([87]). Mappe dei fondali, percorsi dei cavi, coordinate delle condotte e sistemi di monitoraggio costituiscono informazioni ad alto rischio, non tanto per la tutela della *privacy* individuale, ma anche per la sicurezza nazionale e la protezione delle infrastrutture

([87]) S. YUNGRATOG, H. KIM, W. PUNURAI, S.THAMMABOOSADEE, *Risk assessment of data protection in the maritime industry using system-theoretic process analysis*, in *Results in Engineering*, 26, 2025, sul sito web https://doi.org/10.1016/j.rineng.2025.105153.

ISSN 2038-1662

critiche. Nonostante ciò, la legge non prevede misure di sicurezza adeguate – (se non il capo d) dell'art. 17, in cui è opportunamente attribuito all'Agenzia il potere di sviluppare soluzioni tecniche avanzate per la «mappatura dei fondali in collaborazione con il Ministero dell'università e della ricerca per quanto attiene all'acquisizione e alla condivisione di dati») – né stabilisce criteri minimi per la protezione dei dati sensibili di natura tecnica. L'assenza di disposizioni relative alla cifratura, alla segmentazione degli accessi, alla registrazione degli *audit log* o alla conservazione sicura delle informazioni lascia spazio a possibili vulnerabilità che potrebbero essere sfruttate da soggetti non autorizzati.

La questione si complica ulteriormente nel momento in cui le attività subacquee coinvolgono informazioni classificate o di rilevanza strategica per la difesa nazionale. La legge richiama il vincolo del "segreto", ma non articola in modo preciso il rapporto tra il regime di classificazione delle informazioni e la disciplina della protezione dei dati personali. In assenza di un coordinamento esplicito, il rischio è che esigenze di riservatezza e obblighi di trasparenza si trovino in conflitto, lasciando alle singole Amministrazioni la responsabilità di trovare un equilibrio caso per caso, secondo un'ottica di *Risk-based Approach*.

Nel complesso la legge pone in rilievo secondario la tutela dei dati personali e non raggiunge ancora un livello di "maturità" normativa sufficiente a garantire un'effettiva protezione dei diritti degli interessati. Per rafforzare il quadro complessivo sarebbe opportuno

ISSN 2038-1662

quantomeno introdurre una disciplina organica del trattamento dei dati nell'ambito delle attività subacquee, definendo con chiarezza ruoli e responsabilità, prevedendo misure di sicurezza specifiche per i dati tecnici e infrastrutturali, e assicurando il coordinamento con la normativa sulla sicurezza nazionale. Solo in questo modo la legge potrà coniugare la promozione della ricerca e dello sviluppo tecnologico con la piena tutela dei diritti fondamentali delle persone e con la salvaguardia degli interessi strategici dello Stato.

La prospettiva della protezione *data-oriented* avrebbe consentito di ripensarne l'impianto in chiave sistemica, introducendo strumenti giuridici capaci di garantire la continuità, l'integrità e la trasparenza del dato trasmesso, oltre alla mera integrità materiale del cavo. L'attuazione del paradigma *data-oriented* richiede inoltre un coordinamento istituzionale stabile tra autorità marittime, organismi di cybersicurezza e centri di governance dei dati. A più alto livello, l'istituzione di un quadro europeo di *marine data governance* potrebbe costituire il primo passo verso una effettiva sovranità informativa subacquea.

Dal punto di vista operativo e strutturale, la traduzione del paradigma più volte indicato nel testo normativo avrebbe potuto articolarsi lungo tre assi complementari:

1. **Asse della prevenzione informativa**, mediante l'introduzione di obblighi di monitoraggio continuo e di comunicazione degli incidenti che compromettano la qualità o comunque in maggiore sinergia con la sicurezza dei dati trasmessi.

ISSN 2038-1662

2. **Asse della responsabilità multilivello**, che preveda forme di corresponsabilità tra operatori pubblici e privati nella gestione dei rischi informativi, con specifici protocolli di interoperabilità e audit periodici.

3. **Asse della *governance* dei dati marini**, volto a istituire un quadro coordinato di scambio, protezione e valorizzazione dei dati raccolti dalle infrastrutture sottomarine.

Integrando e innestando questi tre assi nel quadro del provvedimento approvato, il Legislatore nazionale avrebbe potuto porre le basi per una prima normativa marittimo-informativa integrata, in grado di conciliare esigenze di sicurezza, innovazione e trasparenza. Si può, in definitiva, sostenere che questa Legge, pur lasciando intravedere buone potenzialità sul piano della *governance*, in qualche modo rappresenti, al momento, un intervento incompiuto ai fini di una protezione globale e credibile dei cavi sottomarini e dei dati che da essi transitano. Se si volesse recuperare e sfruttare appieno questa opportunità di riforma per certi versi epocale, bisognerebbe prevedere un'impostazione normativa che integri le tante dimensioni che oggi il fondale marino cela: regime infrastrutturale, responsabilità, cybersicurezza e interoperabilità con il diritto internazionale, senza lasciare lacune interpretative e anzi ampliando, decisamente, come è ancora possibile fare, l'orizzonte di intervento.

ISSN 2038-1662

Tabella AGOR – Appendice

Tabella – Livelli di apertura del modello AGOR (Apertura Graduata Orientata al Rischio) –

Livello	Tipologia dati	Regime d accesso	Riferimer normativi U	Livello rischio
1. Pubblico	Dati mbientali, ceanografici cientifici di nteresse gene	Accesso libe uso secondo andard open	Direttiva (U 019/1024 sul utilizzo dei d el settore ubblico	Minimo
2. Aggregat	Dati nonimizzati c atisticament attati	Condivision amite licenze andard e clau riuso	Reg. (UE) 022/868 (Dat overnance A rtt. 9–11; GD rt. 5(1)(c)	Basso
3. Tecnico	Dati operati on sensibili (anutenzione elemetria)	Accesso ondizionato revia valutazi sicurezza	Direttiva (U 022/2555 NIS2), art.20	Medio
4. nfrastrutturale	Dati relativi l'integrità e onfigurazion ei cavi	Accesso servato a sogg ubblici ccreditati	Reg. (UE) 023/2854 (Da ct), artt. 14–	Alto

ISSN 2038-1662

5. Strategico	Dati sensibili curezza e dif azionale	Accesso stretto, cifratu onforme a andard ENIS	GDPR art. 3 irettiva NIS2 llegato I – frastrutture igitali	Molto a

Commento finale alla tabella AGOR

La progressione delineata nella tabella evidenzia come il modello AGOR realizzi una graduazione proporzionale del rischio informativo, fondata su norme europee già vigenti di riferimento che combinano, opportunamente, apertura, sicurezza e responsabilità. Ogni livello esprime una diversa intensità di bilanciamento tra trasparenza e protezione, in coerenza con il principio di *accountability* introdotto dal *GDPR* e con la logica di fiducia regolata promossa dal *Data Governance Act* e dal *Data Act*. L'impianto complessivo conferma che la gestione dei dati marini e infrastrutturali non può più essere letta in chiave meramente tecnologica o settoriale: il paradigma *data-oriented* implica un nuovo diritto integrato dei dati e del mare, capace di armonizzare le esigenze di sicurezza strategica, innovazione e sostenibilità. In questa prospettiva, l'Italia — in quanto snodo cruciale del traffico digitale euro-mediterraneo — potrebbe assumere un ruolo di laboratorio normativo per la sperimentazione di modelli multilivello di *governance* dei dati sottomarini, allineati alla strategia europea di sovranità digitale.

ISSN 2038-1662

SUBMARINE CABLES' INTEGRATED PROTECTION: LAW NO. 9/2026 IN THE SPOTLIGHT OF A DATA-ORIENTED PARADIGM

ABSTRACT

L*'articolo mira ad analizzare la progressiva convergenza tra diritto del mare, diritto dei dati e sicurezza delle infrastrutture critiche, con particolare attenzione al ruolo dei cavi sottomarini nel sistema della sovranità digitale europea. Muovendo dal riconoscimento del dato come risorsa strategica, il contributo propone la nozione di protezione data-oriented, intesa come paradigma giuridico capace di integrare le dimensioni fisica, digitale e informativa della sicurezza marittima.*

A partire da tale cornice teorica, vengono proposti due originali modelli concettuali — AGOR (Apertura Graduata Orientata al Rischio) e CTR (Contratto di Trasparenza Reciproca) — che traducono i principi di proporzionalità, fiducia regolata e responsabilità condivisa nella gestione dei dati sottomarini. La parte, per così dire, applicativa del paper affronta l'analisi della protezione dei cavi sottomarini nel nostro ordinamento, con un commento critico alla Legge n.9/2026. Pur trattandosi di un intervento normativo dichiaratamente volto alla protezione delle infrastrutture critiche e delle comunicazioni strategiche, esso non sviluppa un approccio realmente data-oriented e non riconosce ai

ISSN 2038-1662

cavi sottomarini la funzione di infrastrutture informative integrate. Il contributo propone quindi di superare tale visione parziale e limitata, suggerendo un nuovo modello unitario e multilivello di marine data governance, più attuale e soprattutto aderente, anche in prospettiva evolutiva, alla strategia europea per la sovranità digitale.

This article aims to provide a first critical reading of Law No. 9/2026 on the protection of critical underwater infrastructures. Submarine cables — which have become, in recent years, the true backbone of global digital communications — are prominently among the infrastructures concerned, and have accordingly become easy targets for damage and incidents more or less attributable to state actors. The article develops a series of possible amendments and integrations to the approved legislation, preceded by a brief *excursus* on the historical protection of submarine cables under Italian law, with the aim of demonstrating how a convergence between data law and the law of the sea is both achievable and overdue, and of charting a path towards genuinely effective protection of the structural vulnerability of submarine cables.

ISSN 2038-1662