TECNOLOGIA DIGITALE
E SICUREZZA NEGLI AMBIENTI PORTUALI

Roberto Sammarchi - AIAS

rsammarchi@networkaias.it

Avvocato specialista in diritto dell'informazione,
della comunicazione digitale e della tutela dei dati personali

Abstract

Il testo analizza il rapporto tra tecnologia digitale, sicurezza e quadro normativo negli ambienti portuali e nel dominio sottomarino. La prima parte esamina il contesto regolatorio, dalla Convenzione UNCLOS alle direttive europee (MSFD, MSP, Direttiva Offshore), evidenziando la frammentazione delle competenze in Italia e le ambiguità normative per le nuove tecnologie come i veicoli sottomarini autonomi (AUV) e l'Internet delle Cose Sottomarine (IoUT). La seconda parte si concentra sull'impatto dell'Intelligenza Artificiale (IA) nella sicurezza portuale, illustrando opportunità di monitoraggio, prevenzione incidenti e ottimizzazione logistica. Viene approfondito l'AI Act europeo, che classifica i sistemi in base al rischio e impone rigorosi obblighi di conformità (governance dei dati, cybersicurezza, sorveglianza umana) per i sistemi ad "alto rischio" utilizzati in ambito portuale, anche in relazione alla Direttiva NIS 2. Il testo sottolinea l'urgenza di un quadro normativo aggiornato per affrontare le sfide poste dalle nuove tecnologie e dalle vulnerabilità delle infrastrutture sottomarine, evidenziando la necessità di un approccio responsabile e di cooperazione multilaterale per garantire sicurezza e sviluppo sostenibile.

1. Il quadro regolatorio nel dominio underwater: tra sostenibilità, sicurezza e nuova tecnologia intelligente

1.1. Introduzione

Siamo in attesa dell'approvazione delle nuove norme sul lavoro subacqueo, contenute nel disegno di legge n. 1462, XIX Legislatura. Le disposizioni in materia di sicurezza delle attività subacquee mirano a garantire la protezione delle persone e degli operatori che svolgono attività, sia ricreative sia professionali, e a regolamentare le interferenze tra attività subacquee civili, militari e di polizia. Il nuovo disegno di legge, assegnato in sede redigente alla Commissione Ambiente ed Energia del Senato, stabilisce principi fondamentali e disciplina qualifiche professionali e requisiti per l'esercizio della professione.

Altri interventi affronteranno nei dettagli la disciplina della sicurezza nel lavoro subacqueo; mi soffermerò quindi sul quadro normativo generale e su alcuni approfondimenti relativi alla disciplina della nuova tecnologia digitale e al suo sviluppo nel complesso quadro geopolitico attuale.

Il dominio sottomarino, tradizionalmente percepito come un mero mezzo di transito o luogo nel quale sfruttare risorse, si è trasformato in uno spazio denso, conteso e di rilevanza strategica per l'economia globale, il flusso di dati e la sicurezza energetica.

L'analisi che segue delineerà in primo luogo l'ordine giuridico fondamentale che governa queste attività, per poi esaminare gli imperativi specifici di sicurezza e sostenibilità, analizzare l'impatto delle nuove tecnologie intelligenti e, infine, sintetizzare questi temi nell'attuale contesto strategico.

1.2. La costituzione degli oceani

La Convenzione delle Nazioni Unite sul Diritto del Mare (UNCLOS), ratificata dall'Italia con la Legge 689/1994, è il trattato fondamentale che fornisce il "quadro generale" o la "costituzione" per gli oceani. Il suo principio cardine è che tutte le problematiche degli spazi oceanici sono strettamente collegate e devono essere considerate in modo unitario. Questo approccio ha posto le basi per le successive politiche europee più specifiche.

La Convenzione stabilisce le zone essenziali per comprendere quale Stato ha il diritto di regolamentare e controllare le attività sottomarine.

Le zone marittime definite dalla UNCLOS presentano livelli decrescenti di sovranità statale:

- **Acque Interne** (Internal Waters): Comprendono porti, baie ed estuari. In queste acque, lo Stato costiero esercita una sovranità piena e assoluta, paragonabile a quella sul suo territorio terrestre. Questa è la zona di operatività primaria per un'Autorità di Sistema Portuale.

- **Mare Territoriale** (Territorial Sea): Si estende fino a 12 miglia nautiche dalla linea di base. La sovranità dello Stato costiero si estende al fondale marino e al suo sottosuolo. Il Codice della Navigazione italiano recepisce questo limite. La principale limitazione a questa sovranità è il diritto di "passaggio inoffensivo" per le navi straniere, a condizione che tale passaggio non pregiudichi la pace, il buon ordine o la sicurezza dello Stato costiero.

- **Zona Economica Esclusiva** (ZEE): Si estende fino a 200 miglia nautiche. Qui, lo Stato costiero gode di diritti sovrani per l'esplorazione, lo sfruttamento, la conservazione e la gestione delle risorse naturali, sia viventi che non viventi, del fondale marino e del sottosuolo. È in questa zona che si colloca una parte significativa dei progetti energetici offshore. Gli altri Stati mantengono le libertà di navigazione e di posa di cavi e condotte sottomarine.

- **Alto Mare** (High Seas): Le acque oltre la giurisdizione nazionale, governate dal principio di libertà, inclusa la libertà di navigazione e di posa di cavi sottomarini.

Tali definizioni non sono astratte. Determinano il potere legale dello Stato di autorizzare e regolamentare attività come l'installazione di un parco eolico offshore, la posa di un cavo o l'implementazione di una zona di sicurezza attorno al porto.

Per quanto riguarda l'Adriatico, Italia e Croazia hanno firmato un accordo il 24 maggio 2022 per delimitare le rispettive ZEE. L'accordo, ratificato dall'Italia con la Legge n. 62 del 15 maggio 2023, stabilisce che il confine tra le due zone economiche esclusive segue la linea di demarcazione già fissata per la piattaforma continentale dall'accordo tra Italia e l'ex Jugoslavia nel 1968. Poiché il Mar Adriatico è un bacino stretto, questa linea corrisponde essenzialmente a una linea mediana tra le coste dei due Paesi.

La Convenzione crea una tensione fondamentale tra i diritti sovrani dello Stato costiero e le libertà degli altri Stati. Da un lato, garantisce i diritti sovrani sulle risorse nella ZEE, base giuridica per autorizzare progetti di insediamento al di fuori delle acque territoriali come ad esempio la realizzazione di un parco eolico. Dall'altro, preserva la libertà per tutti gli Stati di compiere alcune operazioni come posare cavi sottomarini nella stessa ZEE. Ciò genera un

potenziale conflitto quando, ad esempio, l'area di un parco eolico interseca la rotta pianificata per un cavo dati internazionale.

La tensione descritta si manifesta oggi in forme nuove e più complesse. La struttura dell'UNCLOS, concepita in un'era pre-digitale, genera ambiguità crescenti. Un veicolo sottomarino autonomo (AUV), ad esempio, non rientra chiaramente in nessuna delle categorie tradizionali come 'nave', 'installazione' o 'condotta'. Non è chiaro se un AUV goda della libertà di navigazione o se la sua attività di raccolta dati debba essere classificata come 'ricerca scientifica marina', che nella ZEE richiede il consenso dello Stato costiero. Questa incertezza crea un'area grigia che può essere sfruttata per condurre ad esempio attività di sorveglianza mascherate da ispezioni tecniche.

1.3. Il quadro europeo

L'Unione Europea ha arricchito il quadro UNCLOS con una serie di direttive volte a creare una politica marittima integrata, sostenibile e sicura, traducendo i principi generali del diritto internazionale in obblighi specifici e vincolanti per gli Stati membri.

Il Pilastro Ambientale: Direttiva quadro sulla strategia per l'ambiente marino (MSFD) 2008/56/CE.

L'obiettivo di questa direttiva è raggiungere un "Buono Stato Ecologico" (Good Environmental Status - GES) in tutte le acque marine dell'UE. Essa impone agli Stati membri di sviluppare strategie marine nazionali attraverso un processo ciclico di valutazione, definizione di obiettivi, monitoraggio e attuazione di misure. Il GES è definito attraverso 11 descrittori qualitativi, che fungono da parametri di riferimento per la salute ambientale. Tra questi, di particolare rilevanza per le attività portuali e offshore vi sono la biodiversità (Descrittore 1), l'integrità del fondale marino (Descrittore 6), i rifiuti marini (Descrittore 10) e, soprattutto, il rumore sottomarino (Descrittore 11).

Il Pilastro della Pianificazione: Direttiva sulla pianificazione dello spazio marittimo (MSP) 2014/89/UE.

Questa direttiva istituisce un quadro comune per gestire le intense e concorrenti pressioni sullo spazio marittimo (energia, trasporti, pesca, conservazione) al fine di promuovere la crescita sostenibile della "blue economy". Obbliga gli Stati membri costieri a elaborare piani di gestione dello spazio marittimo per mappare e organizzare le attività umane, applicando un approccio ecosistemico e considerando le interazioni terra-mare. Questo strumento è fondamentale per risolvere i conflitti di utilizzo dello spazio marino.

Il Pilastro della Sicurezza: Direttiva 2013/30/UE sulla sicurezza delle operazioni offshore e infrastrutture critiche.

La Direttiva 2013/30/UE sulla sicurezza offshore, nata dopo il disastro della Deepwater Horizon, stabilisce requisiti minimi per prevenire incidenti gravi nelle operazioni in mare riguardanti idrocarburi, imponendo agli operatori di redigere una "Relazione sui grandi rischi". Più di recente, episodi di sabotaggio nel Mar Baltico hanno spinto l'UE a sviluppare un piano d'azione per la protezione delle infrastrutture critiche sottomarine, come i cavi energetici e di dati. Il piano si articola su prevenzione (es. finanziamento di "smart cables" dotati di sensori), rilevamento (sorveglianza potenziata), risposta (una flotta UE per le riparazioni) e deterrenza (sanzioni), collegandosi a normative sulla cyber-resilienza come la Direttiva NIS 2.

Il pacchetto legislativo dell'UE crea un "triangolo di mandati concorrenti": lo sviluppo economico (MSP), la protezione ambientale (MSFD) e la sicurezza operativa (Direttiva Offshore/Infrastrutture Critiche).

1.4. L'attuazione italiana: dalle direttive europee al diritto nazionale

L'Italia ha recepito i mandati europei attraverso specifici atti legislativi, creando un quadro normativo nazionale articolato.

D.Lgs. 190/2010 (attuazione MSFD): ha trasposto la Direttiva sulla Strategia Marina, designando il Ministero dell'Ambiente (ora MASE) come autorità competente e istituendo un comitato tecnico per coordinare la strategia per le tre sottoregioni marine italiane (Mediterraneo occidentale, Adriatico, Ionio).

D.Lgs. 201/2016 (attuazione MSP): ha recepito la Direttiva sulla Pianificazione dello Spazio Marittimo, individuando nel Ministero delle Infrastrutture e dei Trasporti (MIT) l'autorità competente e istituendo un tavolo interministeriale di coordinamento per l'elaborazione dei piani. L'approvazione di questi piani, avvenuta con un ritardo di tre anni, ha rappresentato un ostacolo significativo per lo sviluppo di progetti offshore.

D.Lgs. 145/2015 (attuazione Direttiva Offshore): Ha implementato la Direttiva sulla sicurezza offshore, introducendo l'obbligo della Relazione sui grandi rischi e stabilendo la responsabilità per i danni ambientali.

Accanto a questa legislazione specialistica, il Codice della Navigazione mantiene un ruolo fondamentale, regolando aspetti pratici della navigazione, le competenze delle Capitanerie di Porto e il regime giuridico del mare territoriale.

L'attuazione italiana ha generato un panorama amministrativo complesso e talvolta frammentato, con competenze suddivise tra molteplici ministeri (MASE per l'ambiente, MIT per la pianificazione, MIMIT per l'industria, Difesa per la sicurezza). Questa divisione, nonostante l'esistenza di organi di coordinamento, può causare ritardi burocratici e requisiti contrastanti. Il ritardo nell'approvazione dei piani di gestione dello spazio marittimo ne è una chiara testimonianza. Per un proponente di progetto l'iter autorizzativo diventa un percorso complesso che richiede non solo eccellenza tecnica, ma anche una sofisticata capacità di navigazione amministrativa.

1.5. Cenni alla peculiare situazione regolatoria degli Stati Uniti

La posizione degli Stati Uniti rispetto alla Convenzione delle Nazioni Unite sul Diritto del Mare (UNCLOS) è unica e complessa. Sebbene siano stati una forza trainante nella sua elaborazione, gli Stati Uniti non hanno mai ratificato il trattato. Ciononostante, accettano e aderiscono alla maggior parte delle sue disposizioni, considerandole come riflesso del diritto internazionale consuetudinario. L'unica eccezione significativa è la Parte XI, che disciplina lo sfruttamento minerario dei fondali marini profondi.

La ragione storica principale di questa mancata ratifica risiede nell'obiezione dell'amministrazione Reagan, nel 1982, alla Parte XI. Questa parte istituiva l'Autorità Internazionale dei Fondali Marini (ISA) per governare le attività di estrazione mineraria in alto mare, designate come "patrimonio comune dell'umanità". Gli Stati Uniti percepirono questo regime come una limitazione inaccettabile delle proprie libertà commerciali e come un sistema di regolamentazione internazionale sfavorevole ai propri interessi.

La politica statunitense in materia è stata formalmente avviata dall'Executive Order 13817 del 20 dicembre 2017, "A Federal Strategy to Ensure Secure and Reliable Supplies of

Critical Minerals", che per primo ha definito una lista ufficiale di minerali critici e ha incaricato le agenzie federali di elaborare una strategia per ridurre la dipendenza dalle importazioni.

In una mossa volta a rafforzare la catena di approvvigionamento nazionale e a contrastare la posizione dominante della Cina, il Presidente Trump ha firmato, il 24 aprile 2025, l'Ordine Esecutivo "Unleashing America's Offshore Critical Minerals and Resources". Questo ordine non è solo una dichiarazione di intenti, ma un atto operativo che incarica le agenzie federali di accelerare le procedure di autorizzazione per l'esplorazione e lo sfruttamento minerario. In particolare, fa leva sul Deep Seabed Hard Mineral Resources Act (DSHMRA) del 1980 per autorizzare unilateralmente le aziende statunitensi a operare in acque internazionali, sfidando di fatto il regime multilaterale gestito dall'Autorità Internazionale dei Fondali Marini (ISA).

1.6. Il deserto normativo per i veicoli sottomarini autonomi e a guida remota

I punti svolti fin qui riguardano il quadro regolatorio e i soggetti competenti per le regole. Passiamo ora ad esaminare l'applicazione di regole alla tecnologia marina nel dominio subacqueo.

Mentre esiste un quadro normativo maturo e dettagliato per i droni aerei (UAS), sotto l'egida di EASA ed ENAC, un regime paragonabile per i Veicoli Sottomarini Autonomi e a Pilotaggio Remoto (AUV/UUV) è in gran parte assente.

L'asimmetria è sorprendente, dato che la tecnologia è già ampiamente dispiegata. Grandi operatori utilizzano AUV per rilievi ad alta risoluzione del fondale marino per progetti infrastrutturali critici. La tecnologia spazia da piccoli ROV (Remotely Operated Vehicles) filoguidati per ispezioni a sofisticati AUV per missioni autonome a lungo raggio. Il Porto di Ravenna stesso è un banco di prova per queste tecnologie, in particolare attraverso il progetto UNDERSEC, finanziato dal programma Horizon Europe, che mira a migliorare le capacità di rilevamento e sorveglianza sottomarina per la sicurezza portuale.

Le normative per i droni aerei coprono la registrazione dell'operatore, la certificazione del pilota, le zone di volo e metodologie di valutazione del rischio come il SAIL. Per i droni sottomarini, invece, non esiste un quadro equivalente. Tale vuoto normativo solleva questioni legali urgenti: quale status giuridico ha un AUV? È una "nave" ai sensi del diritto di bandiera e delle convenzioni internazionali sulla navigazione? Chi è responsabile in caso di collisione con un cavo sottomarino o un operatore subacqueo? Quali sono gli standard di formazione per i suoi operatori?

D'altra parte, il modello normativo aereo (EASA/ENAC) non è direttamente trasferibile al dominio subacqueo. Concetti come il volo a vista (VLOS), il geofencing basato su GPS e la registrazione del pilota non sono immediatamente esportabili a un ambiente tridimensionale, opaco alle onde elettromagnetiche e privo di segnali di posizionamento globali.

I modelli di riferimento più pertinenti provengono dal settore marittimo stesso. L'Organizzazione Marittima Internazionale (IMO) sta sviluppando un codice per le navi di superficie a guida autonoma (MASS), che ha già definito quattro gradi di autonomia e identificato le questioni legali chiave (status del 'comandante', responsabilità dell'operatore remoto). A livello europeo, la guida SARUMS BPG dell'Agenzia Europea per la Difesa (EDA), sebbene non vincolante, offre un modello tecnico-operativo avanzato basato su un approccio al rischio (ALARP) e sulla definizione di un "Concept of Operations" (CONOPS) per ogni tipologia di sistema.

In assenza di un quadro organico, la prassi nazionale si basa attualmente su autorizzazioni ad hoc, come le ordinanze delle Capitanerie di Porto per specifici test tecnologici.

1.7. L'Internet delle cose sottomarine (IoUT) e il porto guidato dai dati

Il dispiegamento di reti di sensori sottomarini connessi (Internet of Underwater Things o IoUT) sta rivoluzionando la capacità di monitorare e gestire l'ambiente marino in tempo reale. Questa tecnologia prevede l'installazione di una rete di sonde intelligenti che comunicano in modalità wireless sott'acqua (ad esempio, tramite modem acustici) per trasmettere dati a una stazione di superficie. Notevoli sperimentazioni sono già state effettuate nei mari italiani per monitorare i parametri ambientali durante i lavori sottomarini, dimostrando il potenziale strategico della tecnologia.

Questo approccio crea un potente collegamento tra i mandati legali di sostenibilità (MSFD) e sicurezza (Infrastrutture Critiche). L'IoUT costituisce un modo tecnicamente elegante ed efficiente per soddisfare la domanda di dati ambientali continui richiesta dalla MSFD e le esigenze di monitoraggio della sicurezza delle infrastrutture critiche.

Le questioni legali sollevate dall'IoUT richiedono un'analisi strutturata. In primo luogo, la governance dei dati deve definire chiaramente la proprietà e i diritti di accesso ai flussi di dati. In secondo luogo, la cybersecurity di queste reti è essenziale: si tratta di infrastrutture digitali critiche che ricadono pienamente nell'ambito della Direttiva NIS2, con i relativi obblighi di sicurezza e notifica degli incidenti. Infine, va definita una chiara catena di responsabilità (liability) in caso di danni derivanti da malfunzionamenti o attacchi informatici.

L'IoUT non è solo uno strumento di conformità, ma un asset strategico in grado di creare un "gemello digitale" dell'ambiente sottomarino, consentendo manutenzione predittiva, gestione ambientale adattiva e sicurezza potenziata. Per farlo con successo, devono essere affrontate le questioni legali di governance dei dati, cybersecurity e responsabilità nei contratti con i fornitori di tecnologia e negli accordi con gli enti regolatori.

1.8. Conclusione e prospettive

Il dominio sottomarino, da ambiente periferico, è diventato uno spazio strategico vitale che richiede un quadro normativo aggiornato. Nonostante l'esistenza di solide basi (UNCLOS, direttive UE, leggi nazionali), persistono criticità come la frammentazione delle competenze in Italia e un ritardo normativo per le nuove tecnologie intelligenti (AUV/UUV e IoUT).

La vulnerabilità delle infrastrutture sottomarine è stata confermata da eventi recenti, come il sabotaggio dei gasdotti Nord Stream, il danneggiamento di cavi dati nel Mar Baltico nel 2024, le minacce del movimento Houthi alle navi posacavi nel Mar Rosso e le continue attività di navi spia in prossimità di infrastrutture critiche europee.

È necessario riconoscere che lo sviluppo e la sostenibilità delle tecnologie marine, centrale per la "blue economy", dipende da un contesto geopolitico pacifico e da un approccio multilaterale. In uno scenario di ostilità, la vulnerabilità delle infrastrutture sottomarine critiche – quali gasdotti, cavi energetici e per dati, o parchi eolici o solari offshore – emerge prepotentemente. La loro potenziale distruzione può richiedere costi logistici e tattici minimi per un attore ostile, mentre gli impatti possono essere devastanti per l'economia e la sicurezza energetica e digitale dei territori costieri colpiti.

Nel dibattito geopolitico odierno, dominato in Europa dal tema del riarmo, è altrettanto prioritario concentrarsi sulla sicurezza delle infrastrutture, sulla resilienza dei sistemi essenziali e sulla sovranità tecnologica che costituisce uno dei cardini della attesa legge italiana sull'intelligenza artificiale. Questo disegno di legge (S. 1146-B), il cui iter parlamentare è in fase avanzata, introduce obblighi di trasparenza e sicurezza e prevede un'aggravante specifica per i reati commessi tramite sistemi di IA, aspetto di diretta rilevanza per la sicurezza marittima.

La sovranità tecnologica, per non ridursi a un concetto ideologico o a un sogno autarchico, deve tradursi in una visione di sistema che promuova una capacità strategica di relazione fra pari nell'ordinamento internazionale. Solo attraverso una cooperazione multilaterale e una governance condivisa si potrà garantire la protezione delle infrastrutture vitali e lo sviluppo sostenibile del dominio sottomarino in un'ottica di stabilità e pace.

2. Tecnologia digitale e intelligenza artificiale: l'impatto delle nuove regole europee sulla sicurezza negli ambienti portuali

2.1. Introduzione

La trasformazione digitale sta ridisegnando il volto degli ambienti portuali, introducendo un livello di automazione e intelligenza senza precedenti. In questo scenario, l'Intelligenza Artificiale (IA) emerge come una tecnologia chiave, in grado di ottimizzare le operazioni, aumentare l'efficienza e, soprattutto, innalzare gli standard di sicurezza sul lavoro. Tuttavia, l'adozione di sistemi di IA complessi solleva interrogativi in termini di affidabilità, trasparenza e responsabilità.

Per governare questa rivoluzione tecnologica, l'Unione Europea ha varato l'AI Act, il primo quadro normativo organico al mondo sull'intelligenza artificiale. Questa legislazione mira a garantire che i sistemi di IA immessi sul mercato europeo siano sicuri e rispettosi dei diritti fondamentali, inclusa la tutela della salute e della sicurezza dei lavoratori.

Questa parte del documento si propone di esaminare in dettaglio le implicazioni dell'AI Act per la sicurezza negli ambienti portuali. Analizzeremo le opportunità offerte dall'IA per una gestione proattiva dei rischi e, al contempo, delineeremo con precisione gli adempimenti normativi che le imprese e le organizzazioni portuali dovranno affrontare a partire dal 2 agosto 2025, data di applicazione delle nuove regole.

2.2. L'intelligenza artificiale per la sicurezza negli ambienti portuali: opportunità e scenari applicativi

L'ambiente portuale, per sua natura complesso e dinamico, presenta molteplici rischi per la sicurezza. L'IA offre un arsenale di strumenti innovativi per mitigare questi rischi in modo più efficace rispetto ai sistemi tradizionali.

Monitoraggio e prevenzione attiva degli incidenti

Visione artificiale: Sistemi di telecamere intelligenti possono analizzare in tempo reale i flussi video per rilevare automaticamente situazioni di pericolo come:

- La caduta di un operatore ("uomo a terra").
- Collisioni imminenti tra mezzi (gru, carrelli elevatori) e personale a piedi.
- L'accesso a zone riservate o pericolose da parte di personale non autorizzato.
- Il mancato o scorretto utilizzo dei Dispositivi di Protezione Individuale (DPI).

Droni autonomi: L'impiego di droni equipaggiati con sensori e telecamere ad alta risoluzione permette di effettuare ispezioni di sicurezza in aree ad alto rischio o difficilmente accessibili (es. sommità di gru, facciate di edifici, stive delle navi), riducendo l'esposizione umana al pericolo.

Analisi predittiva: Algoritmi di machine learning possono analizzare dati storici su incidenti e "quasi incidenti" (near miss) per identificare pattern ricorrenti e aree ad alta probabilità di rischio, consentendo di implementare misure preventive mirate.

Ottimizzazione della gestione del traffico e della logistica

Gestione intelligente del traffico: Sistemi basati su IA possono regolare il flusso di camion, treni e mezzi operativi all'interno delle aree portuali, ottimizzando i percorsi, riducendo le congestioni e minimizzando il rischio di incidenti stradali.

Pianificazione sicura delle operazioni: L'IA può contribuire a pianificare le complesse operazioni di carico e scarico delle merci in modo da ridurre l'interferenza tra diverse attività e minimizzare l'esposizione dei lavoratori a carichi sospesi o macchinari in movimento.

Dispositivi indossabili (wearable) e tutela del lavoratore

Monitoraggio dei parametri vitali: Sensori indossabili (integrati in elmetti, giubbotti, ecc.) possono monitorare in tempo reale parametri come la frequenza cardiaca, la temperatura corporea e i livelli di affaticamento, allertando il lavoratore e la centrale di controllo in caso di superamento delle soglie di sicurezza, specialmente in condizioni di lavoro gravose (es. stress termico).

Geolocalizzazione e allarmi di prossimità: Dispositivi di geolocalizzazione consentono una rapida individuazione del personale in caso di emergenza. Possono inoltre attivare allarmi sonori o a vibrazione quando un lavoratore si avvicina troppo a macchinari in funzione o a zone pericolose.

Manutenzione predittiva e sicurezza delle infrastrutture

Prevenzione dei Guasti: Attraverso l'analisi dei dati provenienti da sensori (vibrazioni, temperature, pressioni) installati su gru, nastri trasportatori e altre attrezzature critiche, gli algoritmi di IA possono prevedere l'insorgere di guasti. Ciò consente di pianificare interventi di manutenzione "just in time", evitando cedimenti improvvisi che potrebbero causare gravi incidenti.

2.3. L'AI Act Europeo: un nuovo quadro regolatorio per la sicurezza sul lavoro

L'AI Act introduce un approccio normativo basato sulla valutazione del rischio, classificando i sistemi di IA in quattro categorie. Le applicazioni di IA per la sicurezza sul lavoro ricadono prevalentemente nella categoria ad "alto rischio".

I principi fondamentali dell'AI Act

Approccio basato sul rischio: L'intensità degli obblighi normativi è direttamente proporzionale al livello di rischio che un sistema di IA può generare per la salute, la sicurezza o i diritti fondamentali delle persone.

Sistemi a rischio inaccettabile: Vietati (es. sistemi di "social scoring").

Sistemi ad alto rischio: Ammessi ma soggetti a rigorosi requisiti di conformità.

Sistemi a rischio limitato: Soggetti a obblighi di trasparenza (es. chatbot).

Sistemi a rischio minimo: Liberamente utilizzabili.

2.4. L'Identificazione dei sistemi di IA ad alto rischio in ambito portuale

Secondo l'Allegato III dell'AI Act, sono considerati ad alto rischio i sistemi di IA che costituiscono un componente di sicurezza di un prodotto o che sono essi stessi un prodotto soggetto a determinate normative di armonizzazione dell'UE. In ambito portuale, rientrano prevedibilmente in questa categoria:

- Sistemi per la gestione e il funzionamento di infrastrutture critiche, come la gestione del traffico portuale.
- Componenti di sicurezza di macchinari (es. sistemi anti-collisione basati su IA).
- Sistemi utilizzati in ambito lavorativo per il reclutamento, la promozione, la valutazione delle prestazioni e il monitoraggio del comportamento dei lavoratori.

La classificazione di un sistema come "ad alto rischio" non è automatica e richiede un'attenta valutazione del contesto specifico di utilizzo e della sua finalità.

2.5. Adempimenti per le imprese e le organizzazioni portuali (in vigore dal 2 agosto 2025)

Con l'applicazione dell'AI Act, le organizzazioni che sviluppano o utilizzano sistemi di IA ad alto rischio dovranno conformarsi a una serie di nuovi obblighi.

Obblighi per i fornitori di sistemi di IA ad alto rischio

Chi sviluppa e immette sul mercato un sistema di IA ad alto rischio deve:

- Implementare un sistema di gestione del rischio per tutta la durata del ciclo di vita del sistema.
- Garantire un'elevata qualità dei set di dati di addestramento per ridurre al minimo i rischi e i risultati discriminatori.
- Redigere una documentazione tecnica dettagliata che dimostri la conformità del sistema.
- Garantire un'adeguata sorveglianza umana ("human oversight") per prevenire o minimizzare i rischi.
- Raggiungere un livello adeguato di accuratezza, robustezza e cybersicurezza.
- Effettuare una valutazione di conformità e apporre la marcatura "CE".
- Registrare il sistema nella banca dati pubblica dell'UE.

Obblighi per gli utenti di sistemi di IA ad alto rischio (le imprese e organizzazioni portuali)

Le imprese e organizzazioni portuali che utilizzano un sistema di IA ad alto rischio (es. per il monitoraggio della sicurezza) nel quadro dell'AI Act sono considerate "utenti" e hanno obblighi specifici:

- Utilizzare il sistema conformemente alle istruzioni fornite dal produttore.
- Garantire che la sorveglianza umana sia effettiva, assegnando a persone competenti, adeguatamente formate e dotate dell'autorità necessaria il compito di supervisionare il sistema.
- Monitorare il funzionamento del sistema e, qualora si verifichi un incidente grave o un malfunzionamento, segnalarlo al fornitore e alle autorità nazionali competenti.
- Conservare i log (registrazioni delle operazioni) generati automaticamente dal sistema per un periodo adeguato.
- Prima di mettere in servizio il sistema, informare i lavoratori e i loro rappresentanti che saranno soggetti al suo utilizzo.
- Effettuare una valutazione d'impatto sulla protezione dei dati (DPIA) ai sensi del GDPR, data la probabile natura del trattamento dei dati personali dei lavoratori.

Trasparenza e coinvolgimento dei lavoratori

L'AI Act pone un forte accento sulla trasparenza. I lavoratori hanno il diritto di essere informati in modo chiaro e comprensibile quando sono soggetti a un sistema IA che ne monitora le prestazioni o prende decisioni che li riguardano. È fondamentale il

coinvolgimento dei Rappresentanti dei Lavoratori per la Sicurezza (RLS) nel processo di valutazione dei rischi legati all'introduzione di queste nuove tecnologie.

Governance dei dati e interconnessioni con il GDPR

L'efficacia e l'affidabilità di un sistema di IA dipendono dalla qualità dei dati con cui viene addestrato. L'AI Act richiede che questi dati siano pertinenti, rappresentativi, privi di errori e completi. Quando i dati utilizzati sono dati personali (es. video dei lavoratori, dati biometrici), l'intero processo deve essere conforme ai principi del Regolamento Generale sulla Protezione dei Dati (GDPR), come la minimizzazione dei dati, la limitazione della finalità e la garanzia di una base giuridica adeguata per il trattamento.

2.6. Cybersecurity e resilienza: proteggere i sistemi di IA da minacce informatiche

L'interconnessione dei sistemi di IA li espone a nuove e sofisticate minacce informatiche.

I nuovi rischi cyber legati all'IA

Avvelenamento dei dati (Data poisoning): Attaccanti potrebbero manipolare i dati di addestramento per "insegnare" al sistema comportamenti errati o pericolosi.

Attacchi avversari (Adversarial attacks): Input appositamente creati per ingannare il modello di IA, facendogli percepire una realtà distorta (es. far "vedere" a un sistema di visione un ostacolo che non c'è, o viceversa).

Violazione della riservatezza: Estrazione di dati sensibili utilizzati per l'addestramento del modello.

2.7. Misure di sicurezza previste dall'AI Act e dalla Direttiva NIS 2

L'AI Act impone ai sistemi di IA ad alto rischio di garantire un livello adeguato di resilienza agli attacchi informatici. Questo requisito si integra e si rafforza con gli obblighi previsti dalla Direttiva NIS 2 sulla sicurezza delle reti e dei sistemi informativi, che classifica i porti come "soggetti essenziali" tenuti ad adottare misure di gestione dei rischi di cybersecurity molto rigorose. L'applicazione congiunta delle due normative crea un quadro solido per la protezione delle infrastrutture portuali intelligenti.

2.8. Vigilanza e sanzioni

Per garantire l'effettiva applicazione della legge, l'AI Act istituisce un sistema di vigilanza e sanzioni.

Il ruolo delle Autorità di vigilanza

In ogni Stato membro, un'autorità nazionale (in Italia, l'Agenzia per l'Italia Digitale - AgID e l'Agenzia per la Cybersicurezza Nazionale - ACN) avrà il compito di vigilare sul mercato, effettuando controlli e ispezioni e avendo il potere di richiedere la modifica, la sospensione o il ritiro dal mercato dei sistemi di IA non conformi.

Il Regime sanzionatorio

L'AI Act prevede sanzioni amministrative pecuniarie significative in caso di violazioni:

- Fino a 35 milioni di euro o il 7% del fatturato mondiale annuo per l'immissione sul mercato di sistemi di IA vietati.

- Fino a 15 milioni di euro o il 3% del fatturato mondiale annuo per la violazione degli obblighi relativi ai sistemi ad alto rischio.
- Fino a 7,5 milioni di euro o l'1,5% del fatturato mondiale annuo per la fornitura di informazioni inesatte.

2.8. Conclusioni

L'Intelligenza Artificiale rappresenta una frontiera per il miglioramento della sicurezza negli ambienti portuali, promettendo una gestione dei rischi più intelligente, proattiva e basata sui dati. Tuttavia, questa tecnologia non è una soluzione priva di complessità o esente da rischi.

L'AI Act europeo traccia un percorso chiaro: l'innovazione deve procedere di pari passo con la responsabilità. Per le imprese e le organizzazioni portuali, questo si traduce nella necessità di avviare un percorso di adeguamento che non può essere procrastinato. L'adozione di sistemi di IA per la sicurezza, specialmente quelli classificabili come ad alto rischio, richiede un approccio olistico e multidisciplinare, che coinvolga il management, i responsabili della sicurezza, i dipartimenti IT e HR, e i rappresentanti dei lavoratori.

Considerare l'adeguamento all'AI Act non solo come un onere normativo, ma come un'opportunità strategica, permetterà di cogliere appieno i benefici di questa tecnologia. Investire in sistemi di IA conformi, sicuri e trasparenti significa investire nella costruzione di porti più efficienti, competitivi e, soprattutto, più sicuri per tutte le persone che vi operano.