Elementi di Cyber Security *on line* per lo sviluppo del turismo nautico intelligente. Il caso studio della Sardegna

Gavino Mariotti ([a]), Maria Veronica Maria Camerada ([b]), Enrico Panai ([c]), Silvia Carrus ([d])[1]

([a]) Università degli Studi di Sassari, via Roma 151, tel 079-229633, fax 079 229645, e-mail: mariotti@uniss.it,
([b]) Università degli Studi di Sassari, via Roma 151, tel 079-229637, fax 079 229645, e-mail: vcamerada@uniss.it,
([c]) Università degli Studi di Sassari, via Roma 151, tel 079-229637, fax 079 229645 e-mail: enricopanai@gmail.com
([d]) Università degli Studi di Sassari, via Roma 151, tel 079-229637, fax 079 229645 e-mail: scarrus@uniss.it

Abstract
L'ingresso delle *ICT* nell'industria turistica ha generato una crescita costante ed esponenziale degli utenti che in maniera autonoma organizzano la propria vacanza su *Internet*. La rete estende la competizione nel mercato *on line*, imponendo ai territori e alle imprese che operano nel comparto di modificare i canali e gli strumenti di promozione e vendita dei propri beni turistici, per adeguare la propria offerta alle regole del *digital tourism*. Questa rivoluzione offre maggiore visibilità alle destinazioni e alle imprese, ma comporta un crescente flusso di dati e informazioni sul *web*. I siti *Internet,* infatti, sono divenuti, rapidamente, la principale porta di accesso verso le destinazioni vacanziere e il cardinale canale di promozionale di interi sistemi turistici. Con la stessa velocità con la quale si diffonde la comunicazione nella rete, si sarebbero dovute implementare imponenti misure di tutela dei dati che gravitano nella realtà cibernetica, per garantire massima tutela ai consumatori e maggiori livelli di competitività alle imprese. Spesso questo non accade. Il *paper* analizza il sistema dell'offerta turistica nautica che si sviluppa nella dimensione *on line,* ed effettua un monitoraggio dei siti *web* dei porti e delle marine della Sardegna, per verificare quale sia il livello della sicurezza informatica degli stessi.

1 Dimensioni e caratteristiche della portualità turistica italiana. Lo scenario sardo e la presenza sul *web*

Il comparto nautico va assumendo un ruolo sempre più importante per l'industria turistica italiana, grazie ad una domanda del settore che, più di altre, si è mostrata resiliente alla crisi economica internazionale[2] (Mazzanti, 2010), e alla massiccia presenza di luoghi da navigare (mari, aree marine protette, laghi) di indiscussa bellezza. Tuttavia, l'offerta ricettiva portuale del Bel Paese, intesa come il complesso delle infrastrutture, dei posti barca e dei servizi a disposizione dei diportisti, viene da più autori (Mazzanti, 2010; Ugolini, 2010; Benevolo 2015) ritenuta incapace di soddisfare le esigenze di mercato, in termini sia quantitativi, sia qualitativi.
L'utilizzo di imbarcazioni con finalità di svago è andato progressivamente perdendo il suo carattere prettamente elitario, interessando, nel tempo, una percentuale sempre più significativa della popolazione nazionale. Due terzi dei diportisti italiani è proprietario del mezzo di navigazione utilizzato, ma cresce progressivamente il numero di chi si avvale della barca di parenti e amici o ne noleggia una, arrivando a trascorrere in mare una media di quindici giornate all'anno.
Si tratta di un'utenza che ricerca nel viaggio e nel soggiorno in mare il benessere psicofisico, la libertà, l'avventura, il rischio e il piacere dell'auto-organizzazione (Benevolo 2008; Benevolo 2010). La vacanza in barca viene pianificata sempre più in maniera autonoma dal turista nautico che sul *web* ricerca la meta, individua le tappe, prenota il posto barca, e scopre-seleziona-acquista le escursioni fruibili in terraferma. I siti *Internet* rappresentano il biglietto da visita virtuale di ciò che il turista si aspetta di trovare nella realtà, e la qualità o l'inefficienza percepita nell'usabilità e completezza dello strumento *web* concorrono, pertanto, alla costruzione di un pregiudizio sul luogo di vacanza e sui suoi servizi.
Il *framework* della percezione del turista digitale include, però, un ulteriore fattore che contribuisce a definire la reputazione del sito e del territorio; si tratta della sicurezza nelle connessioni e nel trattamento delle informazioni – "elementi intangibili che sottendono l'innovazione tecnologica e digitale" di una destinazione

[1] Mentre l'impostazione e la ricerca bibliografica è comune a tutti gli autori, a Gavino Mariotti è attribuibile il par. 3, a Maria Veronica Camerada il par. 4 a Silvia Carrus il par. 1 e a Enrico Panai il par. 2.

[2] Mazzanti (2010) rileva la sufficiente tenuta del comparto della nautica la quale utenza, considerato il costo delle imbarcazioni, è in buona parte costituita da diportisti dallo status socio economico abbastanza elevato.

(Mariotti et al, 2018, p. 19) - e che spesso vengono a mancare, divenendo pertanto nello spazio cibernetico un vantaggio competitivo per destinazioni virtuose che ambiscono a raggiungere un profilo "*smart*" (Gretzel et al., 2015). La presenza e qualità della comunicazione via *web* delle imprese è oggigiorno oggetto di diversi studi, prevalentemente incentrati sull'osservazione dell' accessibilità, dei tempi e modalità di fruizione, della completezza e accuratezza dei contenuti, della presenza di funzioni coerenti rispetto alle aspettative del *target* turistico di riferimento (es. l'opportunità di prenotare e/o acquistare un determinato servizio). Talvolta questo tipo di analisi vengono affrontate con un approccio geo-economico (La Foresta, 2016), ma di rado gli studi condotti in quest'ambito disciplinare contemplano aspetti inerenti la *cyber security*.
Il settore del turismo nautico non fa eccezione e "l'intelligenza" delle marine, dei porti e dei porticcioli italiani, nonché quella dei *competitors* che si affacciano sul Mediterraneo (es.: Croazia, Spagna, Francia) è sovente oggetto d'indagine (Benevole e Morchio, 2015; Benevolo e Spinelli, 2018) ma una visione geo-economica del ruolo rivestito dalla *cyber sicurezza* nella competizione territoriale nautica e diportistica è difficilmente reperibile in letteratura, sebbene la geografia da oltre un ventennio rivolga la propria attenzione all'evoluzione del concetto di spazio (Giorda, 2000) e ai mutamenti dello stesso nell'epoca dell'informazione digitalizzata.
Lo studio qui condotto intende indagare il livello di *cyber* sicurezza dei siti *web* delle marine, dei porti e dei punti di ormeggio della Sardegna, in considerazione del ruolo strategico rivestito da questi nel contesto turistico mediterraneo.
Ai fini del lavoro, viene preliminarmente illustrato lo scenario nazionale dell'offerta dei porti turistici, approfondendo l'analisi a livello regionale per il territorio sardo. La *performance* in termini di *cyber* sicurezza dei siti *web* della ricettività portuale sarda viene valutata attraverso tre indicatori, due dei quali calcolati su parametri tecnici, per rilevare la qualità di trasmissione delle informazioni, il terzo invece, riferito alla conformità o *compliance* del sito rispetto al GDPR (*General Data Protection Regulation*), ovvero al *regolamento generale europeo sulla protezione dei dati*. I risultati prodotti dall'applicazione dei suddetti indicatori confluiscono in una griglia valutativa globale che consente di inquadrare rapidamente la *cyber* sicurezza dei siti *Internet* osservati.

La ricettività portuale italiana, sistematicamente fotografata nei rapporti elaborati dal Ministero dei Trasporti, da UCINA (unione Cantieri Industrie Nautiche e Affini) e da pubblicazioni scientifiche di settore mostra come il turismo nautico sia stato interessato nell'ultimo ventennio da notevoli cambiamenti che hanno riguardato sia la normativa di riferimento a livello nazionale e regionale (Di Monte, 2009; Madau e Contini, 2009), sia le caratteristiche delle infrastrutture portuali, dei posti barca e dei servizi.
Prima di procedere con l'osservazione della dimensione, distribuzione e *trend* dell'offerta dei porti e ormeggi turistici a livello nazionale, appare necessario definire preliminarmente l'articolazione del comparto che contempla le seguenti tre categorie[3]: porti turistici, porti polifunzionali e punti di ormeggio. I *porti turistici (le marine)* sono spazi progettati per fornire ospitalità e servizi alle imbarcazioni; si tratta di strutture utilizzate esclusivamente per il diporto, elemento questo che le distingue dai *porti polifunzionali*, infrastrutture pubbliche impiegate non esclusivamente per la nautica da diporto (Ugolini, 2010). A quest'ultima categoria afferiscono: i "porti", che possono svolgere funzioni anche di tipo commerciale ed economico e che sono in grado di ospitare differenti tipologie di imbarcazioni, cui possono garantire il più elevato numero di servizi, e "porti canale" e "darsene" con un livello di servizi offerti inferiore e più simile a quello delle marine. Infine esistono i punti di ormeggio ossia: "banchine/pontili", "spiagge attrezzate" e "rade" destinate all'ormeggio, alaggio/varo o rimessaggio di piccole barche cui possono essere forniti un numero estremamente limitato di servizi accessori.
Entrando nel merito della dimensione e dinamica del comparto, osservato attraverso i dati riferiti agli anni 2009 (Ugolini, 2010) e 2017 (UCINA, 2019), si evince come l'offerta portuale nazionale nell'arco di quasi un decennio si sia notevolmente potenziata (+49%). Tale *performance* risulta ancora modesta, se confrontata con quella degli altri *competitors* dell'area euro-mediterranea, quali Francia e Spagna (UCINA, 2019). Le regioni italiane con il maggior numero di strutture dedicate al diporto sono quelle delle due isole maggiori (Sicilia, 138 e Sardegna, 118) ma è la Liguria, con 71 unità, ad ospitare il maggior numero di imbarcazioni (23.254 posti barca contro i 16.452 della Sicilia). La forma di ricettività portuale prevalente è quella dei porti polifunzionali (59%) mentre sono ancora poco diffusi i porti turistici-marine (11%) che rappresentano le strutture più moderne, articolate e in grado di accogliere il maggior numero di imbarcazioni (dimensione

[3] La classificazione riportata è quella adottata dall'Osservatorio Nautico Nazionale che integra la distinzione tipologica fissata dall'art.2 del DP.R. 509/97 con le informazioni rinvenibili sulla pubblicazione Pagine Azzurre ritenuta dall'Osservatorio la fonte statistica più omogenea e dettagliata.

media di 511 posti barca per porto). Si rileva, infine, che i punti di ormeggio, seppur contribuendo in maniera modesta a soddisfare la domanda di posti barca (una media di 68 barche per scalo), siano più che raddoppiati nell'ultimo decennio passando da 110 a 236.
La Sardegna con 1.849 Km di costa rappresenta una meta turistica privilegiata per il diportista nautico italiano ed estero, che può contare su un sistema portuale esteso lungo tutto il perimetro costiero. L'elaborazione di UCINA (2019) sui dati Pagine Azzurre 2018 consente di affermare che nella regione esista un'offerta sviluppata di 20.000 posti barca distribuiti su 118 infrastrutture, (in sostanza è presente un porto ogni 15,6 km di costa). Si tratta prevalentemente di porti polifunzionali (42 porti propriamente detti; 3 porti canale; 5 darsene) che possono potenzialmente ospitare 11.165 barche. Presso tali infrastrutture è possibile fruire di numerosi servizi, sia per l'imbarcazione, sia per il diportista. Le marine presenti in Sardegna (13), distribuite prevalentemente nel Nord dell'Isola, rappresentano strutture moderne e dagli elevati standard qualitativi in termini di servizi, che possono ospitare circa 5.000 imbarcazioni; infine i punti di ormeggio, che in linea con l'andamento nazionale, sono più che raddoppiati rispetto al 2009, passando da 25 a 56, garantiscono ospitalità a quasi 4.000 barche. A fronte dell'apprezzabile dotazione infrastrutturale, il comparto appare tuttavia ancora sottodimensionato rispetto alla domanda potenziale in relazione a posti barca e adeguatezza dei servizi offerti, soprattutto se ci si confronta con le altre destinazioni che si affacciano sul Mediterraneo (Tola e al., 2013). Considerando, inoltre, le modalità attraverso cui le strutture portuali si interfacciano con la potenziale clientela *web,* si rileva come la *performance* globale dei siti delle marine della Sardegna risulti «complessivamente molto scarsa e, per la maggior parte, decisamente insufficiente» (Benevole e Marchi, 2015, p. 307).
Appare evidente che l'offerta di *facilities* delle quali possano godere imbarcazione e diportista rivesta un ruolo rilevante nel contesto generale dell'offerta turistica nautica, ma, la sola esistenza di servizi diportistici, anche di elevata qualità, nell'era del digitale, non appare più sufficiente in termini di competitività turistica. In assenza di un adeguato sistema infrastrutturale digitale, strategici approdi rischiano di rimanere invisibili o, nella peggiore delle ipotesi, di trasmettere una generale sensazione di "insicurezza" all'imponente flotta di cybernauti che viaggia per mare e che organizza la propria vacanza attraverso il *web.* Oggigiorno, efficaci strategie di gestione e valorizzazione delle risorse turistiche si sviluppano in rete (La Foresta, op. cit.), dove «i flussi delle informazioni raggiungono il loro obiettivo in tempo reale, prescindendo dalla distanza» (Giorda, op. cit, p.7). La qualità dei servizi *on line* è strettamente legata alla solidità dei siti *Internet.* Ne consegue che anche il livello di sicurezza di questi divenga un parametro di qualità laddove l'interconnessione tra persone e luoghi avviene in una realtà virtuale. Partendo da tali considerazioni si è ritenuto opportuno elaborare un approccio metodologico che permetta di misurare il livello di *cyber security* di un sito *web,* per poi proporre la sua applicazione alla realtà diportistica sarda.

2 Metodologia

Un primo elemento di valutazione nella definizione della *cyber security* di un sito *web* è il livello di sicurezza della connessione.
Come noto, la trasmissione delle informazioni sul *web* avviene attraverso un protocollo di accesso: l'HTTP (*HyperText Transfer Protocol*). Sebbene l'http sia ancora ampiamente utilizzato, esiste fin dai primi anni novanta un'estensione più sicura denominata *HyperText Transfer Protocol Secure* (HTTPS) che, attraverso una certificazione (SSL o, la più diffusa TLS)[4], consente di trasmettere i pacchetti di dati all'interno di una connessione crittografata.
In pratica, una volta protetta da certificato TLS, la connessione tra il *browser web* e il sito *web* dovrebbe garantire la *privacy* e l'integrità dei dati trasmessi tra *client* e *server*.
Tuttavia, una connessione HTTPS e un certificato TLS non garantiscono una totale sicurezza nella trasmissione dei dati. Per poter garantire un trasferimento delle informazioni, i certificati TLS devono essere emessi da un'autorità di certificazione indipendente che attesti l'autenticità del certificato e la chiave di crittografia pubblica del *server*. In alternativa, può essere utilizzato un certificato auto-firmato o generato per un altro dominio, del quale, però, non si ha certezza della qualità in termini di sicurezza. Pertanto, durante la navigazione, nel caso il portale sia sprovvisto di un certificato valido, potrebbe comparire una schermata di avvertimento e il blocco del sito (Figura 1), ovvero, nell'ipotesi in cui il certificato sia auto-firmato, nella

[4] Inizialmente si utilizzava l'ormai deprecato SSL (Secure Sockets Layer), mentre attualmente è l'estensione TLS (Transport Layer Security) ad essere la norma (Barnes et al., 2015).

barra dell'URL dei *browser*, l'utente potrebbe leggere l'indicazione "Non sicuro" (Figura 2), suscitando nell'internauta una sensazione di allarme e insicurezza.

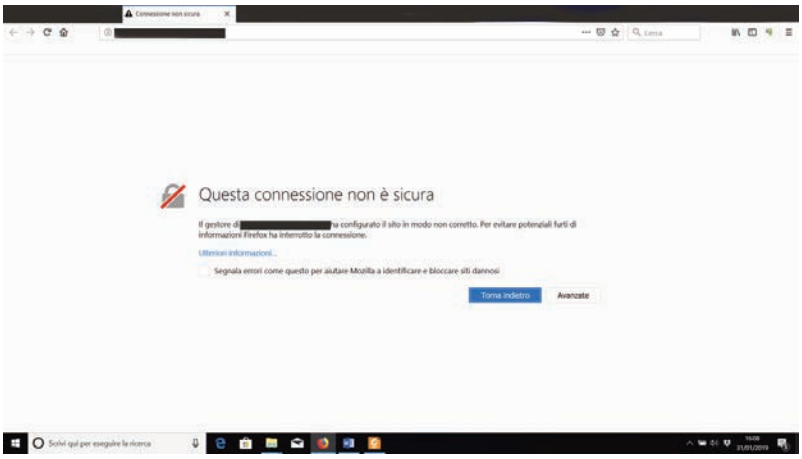

Figura 1: Schermata di avvertimento del browser nei casi di certificato "non valido" o "auto firmato".

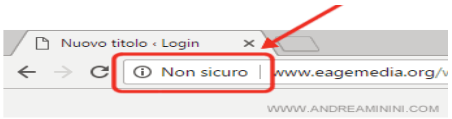

Figura 2: Schermata nei casi di connessione non sicura poiché in assenza di certificato.

L'effetto indiretto della connessione non sicura è riconducibile all'erosione della reputazione *online* del sito *Internet*. Da qualche anno un'importante campagna per aumentare il livello di sicurezza dei siti *Internet* ha spinto l'industria del *web* e dei *browser* a preferire un protocollo più sicuro e a mostrare ogni incongruenza nell'utilizzo di HTTPS e TLS. Si è consci, infatti, che le pagine di avvertimento di uso di un certificato non valido hanno un impatto diretto sulla qualità della navigazione dei visitatori (Sunshine et al., 2009) e uno indiretto sulla reputazione *online* del sito *web* (Bartsch et al., 2013). Inoltre, anche la visibilità del sito nei motori di ricerca può essere danneggiata. Per esempio, il motore di ricerca *Google* (*Google Search*) penalizza i siti *web* che non possiedono un certificato TLS valido facendoli retrocedere nel posizionamento dei risultati[5]. L'estensione, originariamente teorizzata dalla *Netscape* per i suoi *browser*, ha iniziato ad essere utilizzata rapidamente con lo scopo di aumentare il livello di *cyber security* nel *world wide web* (Oppliger, 2016). Nonostante tutti i principali *browser* e motori di ricerca abbiano negli anni lavorato con lo stesso obiettivo, la diffusione dei certificati SSL e TLS non è ancora sufficientemente estesa[6].
Un secondo elemento di valutazione nella definizione della *cyber security* di un sito è la sua conformità rispetto al Regolamento generale sulla protezione dei dati (UE) n. 2016/679. La maggior parte di siti *web* gestisce dati personali indirettamente o direttamente. Al fine di regolare l'uso di tali informazioni, il 25 maggio 2018 è stato varato il *General Data Protection Regulation* (GDPR)[7] che definisce precise norme ai fini della protezione degli stessi. Tra queste: avere una mappatura dei dati attraverso registri delle attività di trattamento (art. 30), limitare il tempo di conservazione degli stessi (art. 5) e evitarne il trasferimento in paesi che non proteggano la *privacy* (art. 45). L'insieme delle norme del GDPR obbligano i gestori del sito a prendere coscienza del loro livello di maturità *cyber* (*Cyber Security Awareness*) e porre in essere azioni che aumentino la *cyber* sicurezza del proprio sito *web*.

La presente ricerca propone e impiega un modello di misurazione della sicurezza digitale dei siti *web* che può essere ritenuto applicabile alle varie forme di offerta turistica digitalizzata, inclusa quella portuale.
Nella prima fase del lavoro sono stati ricercati e selezionati i siti *web* delle infrastrutture per il diporto nautico della Sardegna. In assenza di una fonte ufficiale l'individuazione è avvenuta immedesimandosi nel turista nautico e utilizzando tre strumenti disponibili online: *i)* l'applicazione mobile Navily, *ii)* Google Maps e *iii)* Google Search.
Navily (www.navily.com) è una applicazione per telefoni mobile "che consente di trovare gli ancoraggi e prenotare un posto barca". Grazie ai più di 600 porti turistici catalogati in Europa, è stato considerato lo strumento più adatto per uno *screening* iniziale. L'applicazione è disponibile per i principali dispositivi in

[5] Moving towards a more secure web (September 8, 2016). Google Retrieved June 15, 2019 from https://security.googleblog.com/2016/09/moving-towards-more-secure-web.html Last.
[6] Why You Should Move Your Site to HTTPS: SEMrush Data Study. Retrieved June 15, 2019 from https://www.semrush.com/blog/why-you-should-move-your-site-to-https-semrush-data-study/
[7] https://www.gdpr.net/

commercio, ed è stata cofinanziata dall'Unione Europea e Région Sud della Francia (Provence, Alpes, Côte d'Azur). Google Maps (maps.google.it) è lo strumento di cartografia interattiva online gratuito di Google che consente la geolocalizzazione dei servizi commerciali e professionali presenti in un territorio.
Infine, Google Search (www.google.it), il principale motore di ricerca di pagine web al mondo (92,37% nel mondo e il 96,91% tra agosto 2018 e agosto 2019), ha permesso di affinare e verificare le ricerche con i servizi precedenti.
Le infrastrutture di ormeggio, una volta individuate, sono state successivamente classificate per macro-aree geografiche regionali, così suddivise: Sassari (SS), Olbia-Tempio (OT), Nuoro (NU), Ogliastra (OG), Cagliari (CA), Carbonia-Iglesias (CI), Medio Campidano (VS), Oristano (OR) (Tabella 1).

Carbonia-Iglesias (CI)	**Cagliari (CA)**	**Olbia –Tempio (OT)**	
Porto Calasetta Porto di Porto Pino	Marina del Sole	Cala Camiciotto	Marina Santa Teresa di Gallura
Oristano (OR)	Marina di Bonaria	Circolo Nautico Olbia	Mavalmare Marina di Cugnana
Marina di Bosa Marina di Torregrande Nautica Pinna	Marina di Cagliari	Mare Azzurro Cala Finanza	Pontile Albatros
	Marina di Capitana	Marina Cala Capra	Pontile Ceccherini
Nuoro (NU)	Marina di Portoscuso	Marina Cala Dei Sardi	Pontile dei Fiori
Circolo Nautico La Caletta Porto di Cala Gonone	Marina di Teulada	Marina dei Giardinelli	Pontile del Fico
	Marina di Villaputzu	Marina del Ponte	Pontile Destriero
	Marina di Villasimius	Marina Dell'Isola	Pontile il Cormorano
Ogliastra (OG)	Marina Perd'e Sali	Marina Dell'Orso	Pontile La Sciumara
Marina di Arbatax Marina di Baunei	Marina Piccola	Marina di Asfodeli	Pontile Sa Jaga Brujada
	Marina Sant'Elmo	Marina di Baia Caddinas	Porto Marana
	Motomar Sarda	Marina di Cannigione	Porto Palau
	Porto Cala Verde	Marina di Olbia – Moys	Porto Pozzo
	Portus Karalis	Marina di Portisco	Porto Rafael
		Marina di Porto Cervo	Spurlatta
		Marina Isola Rossa	Yachting Club Vela Blu
		Marina Porto Ottiolu Marina Porto Rotondo	
		Marina Porto San Paolo	

Sassari (SS)			
Ambrosio Servizi Aquatica Marina Base Nautica Usai Consorzio Porto di Alghero	Cormorano SRL Servizio Yachting Marina di Sant'Elmo Marina di Sant'Elmo	Marina di Stintino Marina Turritana Porto Conte Marina Porto di Castelsardo	Ser-Mar Alghero Yacht Club Alghero

Tabella 1 Tabella 1 Le infrastrutture della ricettività turistica nautica rinvenibili sul web ed oggetto dello studio. Nostra elaborazione, 2019.

Si è pertanto proceduto con la raccolta e analisi dei dati attraverso il modello ispirato da Benevolo e Spinelli (Benevolo e Spinelli, op. cit.); tale modello ricorreva ad una valutazione di un *panel* di esperti per l'indagine sulla qualità di un sito web. Al contrario, il modello *Hospitality Multidisciplinary Model* (HMM) sviluppato in tale ambito dall'Università di Sassari per raccogliere informazioni sulle attività turistiche attraverso l'analisi della loro comunicazione o*nline*, ha usato principalmente dati categoriali binari.

Le rilevazioni dei dati sono avvenute durante i periodi di alta e bassa stagione turistica. La prima ha avuto luogo a fine agosto 2018 (periodo di alta stagione turistica) esclusivamente per le strutture di Alghero (9). La seconda rilevazione è stata realizzata tra settembre e novembre 2018 (media e bassa stagione) e ha coinvolto le restanti marine regionali (63). Il risultato è stato la costituzione di una lista (Tabella 2) di 72 unità di cui l'86,1% (62) risulta in possesso di un sito web autonomo, il 12,5% (9) con un solo sotto dominio e una sola marina con un sito web non raggiungibile (1,4%). La rilevazione è stata ripetuta in alta stagione l'anno successivo (luglio 2019), permettendo un'analisi longitudinale del campione[8].

Sito web autonomo		62	86,1%	
Sotto dominio		9	12,5%	
Sito scaduto/Eliminato		1	1,4%	*Escluso dall'analisi*
Totale		**72**	**100%**	

Tabella 2. Caratteristiche del campione di siti web analizzato Nostra elaborazione, 2019

Si è pertanto proceduto con l'analisi della *performance* dei siti in termini di *cyber* sicurezza impiegando come indicatori: la presenza di connessione HTTPS, la verifica della certificazione TLS e il livello di conformità o *compliance* del sito rispetto al regolamento generale europeo sulla protezione dei dati o GDPR.

La presenza di connessione HTTPS è stata verificata manualmente (aggiungendo la S al protocollo HTTP://) attraverso la manipolazione dell'indirizzo dell'URL nel *browser* nel caso in cui non fosse presente un reindirizzamento automatico all'HTTPS://.

In un secondo tempo, solamente per i siti con HTTPS esistente è stata verificata la certificazione TLS attraverso l'applicazione *online* SSL *SHOPPER* (https://www.sslshopper.com). Per ogni sito sono stati registratati i risultati completi dell'analisi (quantità di errori, tipo di errore, tipo di *server*, giorni mancanti alla scadenza). Sono state identificate tre tipologie di errore: i) *Expired* (per i certificati scaduti), ii) *No-match* (per i certificati non corrispondenti al dominio utilizzato), iii) *Self-signed* (per i certificati autogenerati e non validati da un'autorità esterna), così come illustrato in Tabella 3.

Un'analisi sostanziale è stata svolta per verificare la conformità al GDPR. In questo caso sono stati osservati i *disclaimers* di ogni sito e/o le note sulla *privacy* nei formulari. Gli *output* sono stati di tre tipi, come visibile in Tabella 4: i) *Compliant* (il sito dichiara di rispettare la normativa GDPR e i formulari sono conformi alla normativa); ii) *Partially compliant* (il sito non è GDPR compliant ma utilizza le migliori pratiche per la privacy e concorda almeno con le legge precedenti, il D.Lgs 196/2003, la Direttiva n. 95/46/CE e la Direttiva 2009/136/CE); iii) *No compliant* (nessuna menzione viene fatta a una normativa della privacy e le richieste di dati personali sono palesemente irregolari).

HTTPS	TLS	NOTES	Peso
Si	Si	Connessione sicura	10
No	No	Connessione non sicura	5
Si	Auto firmato	Schermata di avvertimento di browser	0
Si	Scaduto	Schermata di avvertimento di browser	0
Err	Non corrisp.	Schermata di avvertimento di browser	0
-	-	Es. sito *under construction*	3

Tabella 3: Le tipologie di errore e i pesi utilizzati ai fini della valutazione della sicurezza della connessione web, nostra elaborazione, 2019.

GDPR	NOTES	Peso
Compliant	Sito conforme alla normativa	10
Partially compliant	*Compliant* con normative precedenti	5
No compliant	Sito non conforme ad alcuna normativa	0

Tabella 4 I livelli di conformità al GDPR e relativi pesi utilizzati ai fini della valutazione della protezione dei dati offerta dal sito, nostra elaborazione, 2019.

[8] Sono stati analizzati solo i siti attivi nel 2018 (71). Nel 2019 uno dei siti era in fase di ricostruzione (under costruction), quindi non si è potuto rilevare i dati.

I risultati sono stati trasformati in valori numerici per ottenere una griglia valutativa globale.
Per la valutazione delle connessioni con criptazione sono stati assegnati i seguenti punteggi: 10 punti per i siti sicuri (con TLS valido); 5 punti per i siti non sicuri (senza TLS); 0 punti per i siti che generano una pagina di avvertimento nei *browser* (con TLS non valido); 3 punti per altro (es. sito *under construction*).
Per il GDPR sono stati assegnati i punteggi: 10 punti per i siti conformi al GDPR; 5 punti per i siti conformi a legislazioni sulla *privacy* precedenti al GDPR; 0 punti per i siti non conformi.
Infine, una volta sommati i valori, ad ogni quartile è stata assegnata un'icona colorata per rendere più rapida l'interpretazione del risultato ottenuto: un cerchio verde per il primo quartile, un cerchio blu per il secondo quartile, un cerchio giallo per il terzo quartile e un cerchio rosso per il quarto quartile.

primo quartile secondo quartile terzo quartile quarto quartile

3 La qualità della trasmissione delle informazioni dei siti web delle strutture portuali sarde

Su un totale di 71 siti analizzati, la maggior parte (87,3%) è riferita a strutture per la nautica da diporto situate nelle zone Nord-Est, Nord-Ovest e Sud della regione, corrispondenti alle zone di Olbia-Tempio (OT), Sassari (SS) e Cagliari (CA), (tabella 5 e Figura 3). Tale suddivisione ha permesso di produrre un *ranking* finale del livello di *cybersecurity compliance*.

Provincia	Siti analizzati (numero)	Siti analizzati (%)
CA	14	19,7%
CI	2	2,8%
NU	2	2,8%
OG	2	2,8%
OR	3	4,2%
OT	35	49,3%
SS	13	18,3%
Totale	**71**	**100%**

Tabella 5. Distribuzione del campione di siti web analizzato. Nostra elaborazione, 2019.

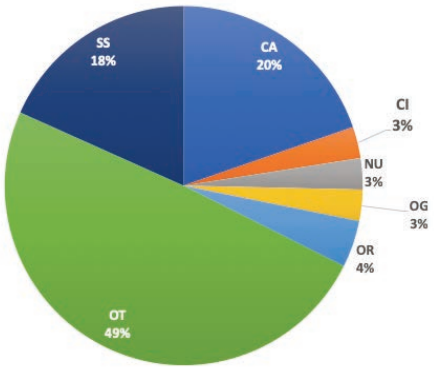

Figura 3. Distribuzione del campione. Nostra elaborazione, 2019.

In linea generale la ricerca mostra la tendenza dei siti *web* ad avere una certificazione TLS per le transazioni sicure. I dati rilevati nel 2018 e nel 2019 consentono un'investigazione longitudinale e indicano i *trends* rappresentati in Tabella 6 e nelle Figure 4 e 5.

STATUS	2018	2019	TREND
NO HTTPS	23	14	-39%
NO TLS	20	25	25%
SECURE	28	31	11%
SITE UNDER CONSTRUCTION		1	

Tabella 6. Il livello di sicurezza delle connessioni ai siti web osservato nel biennio 2018-2019. Nostra elaborazione, 2019.

Sebbene appaia chiaramente visibile la predominanza dei siti *web* non sicuri (figura 4) fa ben sperare il leggero miglioramento conseguito nel 2019 (figura 5).

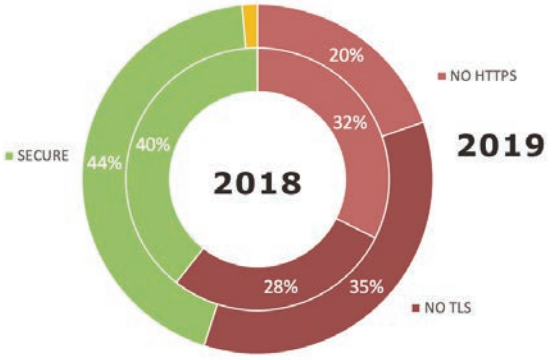

Figura 4. La sicurezza della connessione web nel biennio 2018-2019. Nostra elaborazione, 2019.

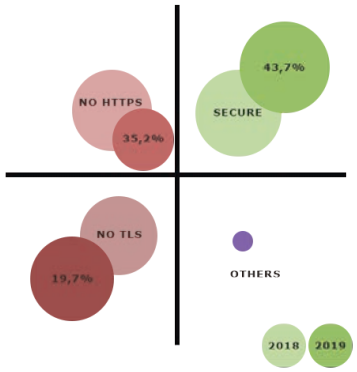

Figura 5. La sicurezza della connessione della connessione web nel biennio 2018-2019. Nostra elaborazione, 2019

Complessivamente, rispetto alla rilevazione del 2018, il tasso di non conformità è diminuito del 39,1% dei siti rispetto a quelli del 2018. Contemporaneamente è stata evidenziata una tendenza ad abbassare lo *standard* qualitativo in termini di sicurezza (figura 6). In particolare, 5 siti che possedevano una certificazione TLS valida nel 2018, hanno attuato un "*downgrade*" del sistema di certificazione rispetto al periodo precedente (certificazione scaduta, auto firmata o non corrispondente al sito), mentre è stato rilevato un caso, ad inizio estate, di costruzione (*under construction*). L'effetto finale è stato un incremento dei siti sicuri del 10,7% rispetto al periodo precedente.

Figura 6. La sicurezza della connessione web nel biennio 2018-2019. Nostra elaborazione 2019.

Ciò che colpisce è il basso tasso di progressione verso le connessioni più sicure (figura 6). Ipotizzando un *trend* del 10% annuo e nessun intervento propulsore esterno, si prevede che i siti *web* delle marine della Sardegna potrebbero raggiungere un livello minimo sicurezza solo nel 2027. Di conseguenza, si ritiene che importanti interventi esterni siano necessari per velocizzare questo processo.

4 La conformità al GDPR e considerazioni conclusive sulla Cyber Security nel settore della nautica sarda.

La valutazione sulla *compliance* al GDPR conduce ad un risultato complessivamente insufficiente: la maggior parte delle strutture non è risultata GDPR *compliant*. A causa di vincoli pratici, le rilevazioni sul GDPR risalgono solo al 2018, di conseguenza non è stato possibile produrre un'analisi longitudinale. Si osserva che in quell'anno solo 18 strutture su 71 (pari al 25,4% delle unità indagate) erano conformi alla direttiva GDPR, 23 (il 32,4%) adempievano a normative precedenti e 30 (il 42,3%) non si riferivano a nessuna legge sulla *privacy* e/o richiedevano l'uso di dati personali in maniera irregolare.
Sorprendentemente, si osserva che il livello di *compliance* al GDPR non risulta correlata alla dimensione della struttura. Di fatto nelle strutture col numero di posti barca disponibili più alto si rileva un livello di *compliance* al GDPR inferiore rispetto a quello delle realtà di più piccole dimensioni (figura 7).

Figura 7. La conformità al GDPR delle strutture portuali sarde. La dimensione dei cerchi raffigurati nel cartogramma esprime la capacità (posti barca) delle unità analizzate.

I risultati della ricerca hanno diversi risvolti pratici. In primo luogo, indicano che nel settore nautico la destinazione non garantisce un livello minimo di cybersicurezza per i visitatori. In secondo luogo, mostrano che la maggior parte dei siti *web* dei porti turistici regionali non sono ancora adatti allo sviluppo dell'*e-commerce*. Per ora solo 2,7% (2 su 72) dei siti *web* analizzati permette il pagamento *online*, ma è verosimile che il numero delle richieste di commercio *online* subisca un oncremento nei prossimi anni, e quindi che la necessità di un livello minimo di cybersicurezza diventi inderogabile. Si pensa quindi che l'aumento dei servizi *online* possa portare le strutture preposte alla fornitura di servizi diportistici a conformarsi al GDPR, per migliorare il livello di sicurezza delle transazioni per proteggere in maniera più efficace i dati personali dei clienti
Al fine di mostrare rapidamente il livello minimo di cybersicurezza di ogni marina nelle province della Sardegna, i risultati sono stati indicizzati e suddivisi secondo il loro quartile (tabella 7).

Provincia	Sigla	Valore medio	QUARTILE
Medio Campidano, VS	VS	0	ESCLUSO
Oristano, OR	OR	6,666666667	1 quartile
Carbonia-Iglesias, CI	CI	7,5	2 quartile
Sassari, SS	SS	8,153846154	2 quartile
Olbia-Tempio, OT	OT	9,857142857	3 quartile
Ogliastra, OG	OG	10	3 quartile
Cagliari, CA	CA	12,28571429	4 quartile
Nuoro, NU	NU	14	4 quartile

Tabella 7: suddivisione delle unità analizzate in quartili. Nostra elaborazione, 2019.

Dal punto di vista grafico, si è indicato col cerchio verde per il primo quartile, col cerchio blu il secondo quartile, col cerchio giallo il terzo quartile e col cerchio rosso per il quarto quartile. Si è ottenuta così un *Websites Cybersecurity Essential Dashboard* con i risultati globali, rappresentata cartograficamente nella figura 8.

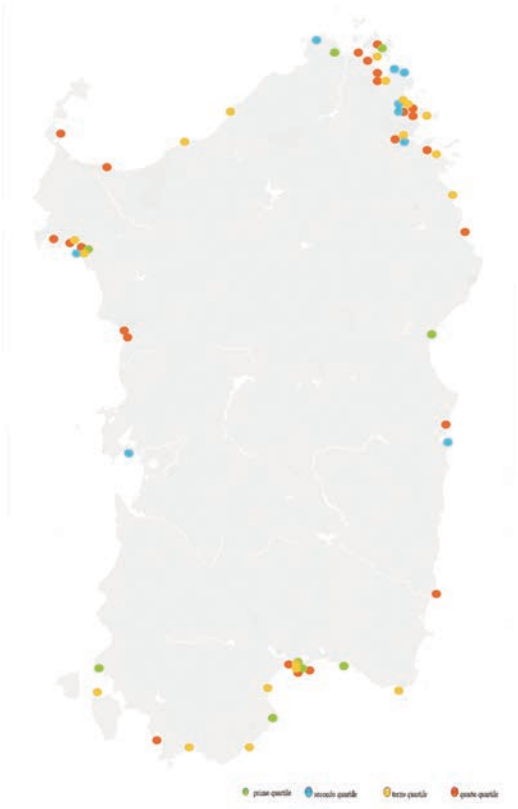

Figura 8: Websites Cybersecurity Essential Dashboard. Nostra elaborazione, 2019.

La rappresentazione dei risultati ottenuti, illustrata in figura 8, mette in evidenza l'eterogeneità della distribuzione territoriale dei porti e porticcioli della Sardegna provvisti di sito web, con una maggiore presenza degli stessi nel Nord Est dell'Isola. Se nella Sardegna meridionale si registra una concentrazione di strutture altamente performanti in termini di *cybersecurity*, nel Nord Est si rileva una più significativa diffusione di porti e porticcioli che denunciano una situazione complessivamente buona. Le strutture localizzate lungo la costa nord-occidentale evidenziano un risultato modesto ma con interessanti margini di miglioramento.
A corredo dell'analisi si riporta l'elenco dettagliato delle strutture sottoposte ad analisi, classificate in funzione del Websites Cybersecurity Essential Dashboard elaborato in questa sede (tabella 8)

TABELLA 8. Le strutture sottoposte ad analisi clasificate in funzione del Websites Cybersecurity Essential Dashboard. Elaborazione propria, 2019.

Cagliari (CA)

Marina del Sole
Marina di Bonaria
Marina di Cagliari
Marina di Capitana
Marina di Portoscuso
Marina di Teulada
Marina di Villaputzu
Marina di Villasimius
Marina Perd'e Sali
Marina Piccola
Marina Sant'Elmo
Motomar Sarda
Porto Cala Verde
Portus Karalis

Carbonia-Iglesias (CI)

Porto Calasetta
Porto di Porto Pino

Nuoro (NU)

Circolo Nautico La Caletta
Porto di Cala Gonone

Ogliastra (OG)

Marina di Arbatax
Marina di Baunei

Oristano (OR)

Marina di Bosa
Marina di Torregrande
Nautica Pinna

Olbia-Tempio (OT)

Cala Camiciotto
Circolo Nautico Olbia
Mare Azzurro Cala Finanza
Marina Cala Capra
Marina Cala Dei Sardi
Marina dei Giardinelli
Marina del Ponte
Marina Dell'Isola
Marina Dell'Orso
Marina di Asfodeli
Marina di Baia Caddinas
Marina di Cannigione
Marina di Olbia – Moys
Marina di Portisco
Marina di Porto Cervo
Marina Isola Rossa
Marina Porto Ottiolu
Marina Porto Rotondo
Marina Porto San Paolo
Marina Santa Teresa di Gallura
Mavalmare Marina di Cugnana
Pontile Albatros
Pontile Ceccherini
Pontile dei Fiori
Pontile del Fico
Pontile Destriero
Pontile il Cormorano
Pontile La Sciumara
Pontile Sa Jaga Brujada
Porto Marana
Porto Palau
Porto Pozzo
Porto Rafael
Spurlatta
Yachting Club Vela Blu

Sassari (SS)

Ambrosio Servizi
Aquatica Marina
Base Nautica Usai
Consorzio Porto di Alghero
Cormorano SRL Servizio Yachting
Marina di Sant'Elmo
Marina di Sant'Elmo
Marina di Stintino
Marina Turritana
Porto Conte Marina
Porto di Castelsardo
Ser-Mar Alghero
Yacht Club Alghero

Riferimenti bibliografici

Barnes R., Thomson M., Pironti A., Langley A. (2015), "Deprecating Secure Sockets Layer Version 3.0", *Internet Engineering Task Force* (IETF), Archived from the original on 2018-03-28.

Bartsch S., Volkamer M., Theuerling H., Karayumak F. (2013) , *Contextualized Web Warnings, and How They Cause Distrust*, in: Huth M., Asokan N., Čapkun S., Flechais I., Coles-Kemp L. (eds), *Trust and Trustworthy Computing. Trust 2013. Lecture Notes* in Computer Science, vol 7904. Springer, Berlin, Heidelberg.

Benevolo C, Spinelli R (2018), "The quality of web communication by Italian tourist ports", *Tourism: An International Interdisciplinary Journal*, Vol. 66 No. 1, 2018.

Benevolo C. (2008), *Luci ed ombre del turismo nautico*, in Quagli A. (a cura di), *Analisi gestionale dei porti turistici della nautica da diporto. Il caso di Imperia*, Milano, FrancoAngeli, pp. 212-253.

Benevolo C. (2010), "Turismo nautico. Una sfida per il "destination management*"*, *Rivista di Scienze del turismo, 3/2010*, pp. 108-109.

Benevolo C., Morchio E. (2015), *La qualità della comunicazione via web per la promozione del turismo nautico*, in *Economia e diritto del terziari*o, n. 2, FrancoAngeli, Milano, pp. 391-313.

Di Monte A. (2009), *Portualità turistica e sviluppo locale*, in Celant A. Ferri M.A. (a cura di), *L'italia. Il declino economico e la forza del turismo. Fattori di vulnerabilità e potenziale competitivo di un settore strategico*, Marchesi editore, Roma pp. 391-400.

Giorda C. (2000), *Cybergeografia. Estensione, rappresentazione e percezione dello spazio nell'epoca dell'informazione*, Tirrenia Stampatori, Torino.

Gretzel U., Sigala M., Xiang Z., Koo C. (2015), "Smart tourism: foundations and developments", *Electron Markets*, No. 25, Springer, pp. 179–188.

La Foresta D. (2016), "Turismo, comunicazione digitale e partecipazione sociale", *Bollettino AIC,* 518, pp.145-155.

Madau C., Contini M.V. (2009), *Portualità turistica e paesaggio in Sardegna*, in Scanu G. (a cura di), *Paesaggi e sviluppo turistico, Sardegna e altre realtà geografiche a confronto*, Atti di convegno di studi, Olbia 15-17 ottobre 2009, Carocci, Roma, pp. 555-568.

Mariotti G., Carrus S., Panai E., Martinez V. Camerada M.V (2018), "Competitività in ambito turistico. Il ruolo della Cyber Security", *Geotema*, Bologna, pp.13-32,.

Mazzanti R. (2010), "I porti turistici della Toscana", *Geotema* 40, Bologna, pp. 119-131.

Oppliger R. (2016), *SSL and TLS: Theory and Practice*, Artech House.

Sunshine J., Egelman S., Almuhimedi H., Atri N., Faith Cranor L. (2009), *Crying Wolf: An Empirical Study of SSL Warning Effectiveness*, in *Proceeding SSYM'09 Proceedings of the 18th conference on USENIX security symposium*, Montreal, Canada, pp. 399-416.

Tola A., Pinna M., Chessa S. (2013), *Il settore nautico: stato dell'arte e dinamiche di sviluppo*, in Tola A., *Il settore della nautica nel Nord Sardegna. Innovazione tecnologica, sviluppo competitivo e dinamica di crescita delle imprese*, FrancoAngeli, Milano, pp. 75-96.

UCINA (2019), *La Nautica in cifre. Analisi del mercato per l'anno 2018*, Genova, 2019.

Ugolini G.M. (2010), "Infrastrutture portuali e turismo nautico: un nodo da sciogliere scala regionale", *Geotema*, 40, Bologna, pp.110-118.

Pubblicazione finanziata col fondo di Ateneo per la ricerca 2019