ISSN 1126-7798

Supplemento a Geotema - Rivista Quadrimestrale - Anno XXII n. 3 settembre/dicembre 2018 - Pàtron Editore - Via Badini 12 - Quarto Inferiore - 40057 Granarolo dell'Emilia (BO)

ANTROPIZZAZIONE, TURISMO E INNOVAZIONE TECNOLOGICA. UN APPROCCIO MULTISCALARE PER L'ANALISI DELLO SVILUPPO SOSTENIBILE E INTELLIGENTE DEL TERRITORIO

a cura di
Marina Sechi Nuvole

supplemento geotema

Pàtron Editore

AGEI - Geotema, Supplemento 2018 Anno XXII 2018
ISSN 1126-7798

Antropizzazione, turismo e innovazione tecnologica. Un approccio multiscalare per l'analisi dello sviluppo sostenibile e intelligente del territorio

a cura di Marina Sechi Nuvole

ISSN 1126-7798

Per eventuali indicazioni e richieste di carattere editoriale, rivolgersi al prof. Claudio Cerreti, Università Roma Tre, Dipartimento di Studi Umanistici, Via Ostiense 234, 00146 Roma (*claudio.cerreti@uniroma3.it*).
Per informazioni sull'allestimento e sull'invio di testi per «Geotema», consultare le indicazioni redazionali riportate nell'ultima pagina di questo fascicolo e le informazioni riportate nella pagina *web* di «Geotema» (*https://www.ageiweb.it/pubblicazioni/geotema/*).

Abbonamento cartaceo Italia	**€ 60,00**
Abbonamento cartaceo estero	**€ 75,00**
Fascicoli singoli cartacei Italia	**€ 22,00**
Fascicoli singoli cartacei estero	**€ 25,00**
Abbonamento on-line Privati	**€ 55,00**
Abbonamento on-line Enti, Biblioteche, Università	**€ 130,00**
PDF singoli articoli	**€ 14,00**

Per abbonamenti e ordini di arretrati, rivolgersi all'Ufficio Abbonamenti: **abbonamenti@patroneditore.com** o collegarsi al sito **www.patroneditore.com/riviste.html.**
I pdf dei singoli articoli e gli abbonamenti online possono essere ri-chiesti solo collegandosi al sito **www.patroneditore.com/riviste.html.**
Gli abbonamenti hanno decorrenza gennaio-dicembre, con diritto di ricevimento dei fascicoli già pubblicati, se sottoscritti in corso d'anno. I fascicoli cartacei non pervenuti vengono reintegrati non oltre 30 giorni dopo la spedizione del numero successivo.

Modalità di pagamento:
Versamento anticipato adottando una delle seguenti soluzioni:
• c.c.p. n. 000016141400 intestato a Pàtron editore - via Badini 12 - Quarto Inferiore - 40057 Granarolo dell'Emilia - Bologna – Italia
• bonifico bancario a INTESA SAN PAOLO SPA, Filiale, Ag. 68 IT58V0306936856074000000782BIC BCITITMM
• carta di credito o carta prepagata a mezzo PAYPAL (**www.paypal.it**) specificando l'indirizzo e-mail **amministrazione@patroneditore.com** nel modulo di compilazione, per l'invio della conferma di pagamento all'Editore.

Stampa: Li.Pe. Litografia Persicetana, San Giovanni in Persiceto, Bologna, nel mese di novembre 2019.

Gavino Mariotti, Enrico Panai, Maria Veronica Camerada

Piattaforma per la sicurezza informatica per il comparto turistico: dalla prospettiva nazionale all'azione reale. *Focus* sulle strutture ricettive

Ogni impresa operante nel mercato dovrebbe adottare delle misure preventive in termini di sicurezza informatica. Gli enti nazionali dei paesi più avanzati sono coscienti delle problematiche legate ai temi della sicurezza informatica e hanno sviluppato dei protocolli tecnici e legislativi al fine di mitigare l'impatto e la frequenza degli attacchi informatici. Nonostante tali sforzi, i rischi sono ancora alti. Questo perché le piattaforme proposte sono spesso complesse e di difficile adozione per le imprese e per le organizzazioni di dimensioni minori. Una maggiore complessità si rileva nell'implementazione di buone pratiche di protezione e prevenzione cyber *nel settore turistico. In particolare, si riscontrano problemi di prevenzione per le strutture ricettive, caratterizzate da ritmi lavorativi stagionali ed intensi picchi di attività. Questo articolo si propone di riprendere e riadattare la Piattaforma nazionale per la sicurezza informatica (Framework nazionale per la cyber security) alla stagionalità, tipica del comparto turistico italiano, con l'obiettivo di ridisegnare la cornice della tutela informatica, rendendola più efficace e attuabile nella microimpresa impegnata nelle ricettività, assicurando maggior competitività dei territori a forte vocazione turistica.*

Cyber Security Framework for the Tourism Sector: From the National Perspective to the Real Action. Focus on Accommodation Facilities
Every company operating in the market should take preventive measures in terms of IT security. The national bodies of the most advanced countries are aware of the problems related to cyber security issues and they have developed technical and legislative protocols in order to mitigate the impact and frequency of cyber attacks. Despite these efforts, the risks are still high. This is because the proposed frameworks are often complex and difficult to adopt for companies and smaller organizations. Greater complexity is noted as an obstacle in the implementation of good cyber protection and prevention practices in the tourism sector. In particular, there are problems of prevention for accommodation facilities, characterized by seasonal workflows and intense peaks of activity. The paper aims to resume and readjust the national framework for cyber security to the seasonality, typical of the Italian tourism sector, with the aim of redesigning the framework of IT protection, making it more effective and feasible in the micro-enterprise involved in receptivity, by ensuring a greater competitiveness of the territories with a strong touristic vocation.

Plateforme pour la sécurité informatique du secteur touristique: de la perspective nationale a l'action réelle. Focus sur les structures de réception
Toute entreprise opérant sur le marché devrait prendre des mesures préventives en matière de sécurité informatique. Les organismes nationaux des pays les plus avancés sont conscients des problèmes liés à la cyber sécurité et ont élaboré des protocoles techniques et législatifs afin d'atténuer l'impact et la fréquence des cyber attaques. Malgré ces efforts, les risques restent élevés. En effet, les plateformes proposées sont souvent complexes et difficiles à adopter pour les PME et les TPE. Une plus grande complexité est un frein dans la mise en œuvre de bonnes pratiques de protection et de prévention de la cyber-protection dans le secteur du tourisme. En particulier, il existe des problèmes de prévention pour les établissements d'hébergement, caractérisés par des flux de travail saisonniers et des pics d'activité intenses. Le document vise à reprendre et à réajuster la plateforme nationale de cyber sécurité au caractère saisonnier, typique du secteur du tourisme italien, dans le but de le remodeler, de le rendre plus efficace et plus réalisable dans la microentreprise impliquée dans la réceptivité. Pour conclure, l'étude vise à augmenter la compétitivité des territoires à forte vocation touristique.

Parole chiave: *sicurezza informatica, industria dell'ospitalità, piattaforma di* cyber *igiene*

Keywords: *cyber security, hospitality industry, cyber hygiene framework*

Mots-clés: *cyber sécurité, industrie hôtelière, plateforme de cyber hygiène*

Gavino Mariotti, Università di Sassari, Dipartimento di scienze umanistiche e sociali – mariotti@uniss.it

Enrico Panai, Università di Sassari, Dipartimento di scienze umanistiche e sociali - epanai1@uniss.it

Maria Veronica Camerada, Università di Sassari, Dipartimento di scienze umanistiche e sociali - vcamerada@uniss.it

Nota: *il lavoro è attribuito per i paragrafi 1 e 2 a Gavino Mariotti, per il paragrafo 3 a Maria Veronica Camerada e per i paragrafi 4 e 5 a Enrico Panai.*

1. Premessa

La rete rappresenta certamente il più importante mezzo di diffusione del fenomeno della globalizzazione al quale assistiamo (Santos, 1996) costruendo *geocyberspazi* (Bakis e Roche, 1998) che sono fondamentali per valutare l'emergere di funzioni spaziali e sociali. All'interno di questi la sicurezza informatica è diventata un argomento centrale in ogni campo di attività. Il massivo utilizzo delle tecnologie comunicative ha modificato le geografie delle attività commerciali e, in particolare, del turismo. L'importanza delle reti informatiche e comunicative ha spinto a pensare alla necessità di sviluppare nuovi concetti di turismo sostenibile con l'avvento e lo sviluppo di Internet già agli albori del *web* (Inkpen, 1994). Con l'aumento di quella che Castells chiama società della rete (Castells, 1996), Internet ha fatto acquisire alla geografia nuovi significati. L'uso di termini spaziali conferma la «spazializzazione» di Internet (Kellerman, 2007). In effetti, il *cyberspazio* è stato visto come una metafora geografica (Graham, 2013) in cui il *cyberspazio* spesso riflette lo spazio geo-economico (Warf, 2013). In questo spazio possiamo tracciare confini legati all'influenza economica o informativa. E anche se un pezzo di informazione, quando è virtualizzato, si mette fuori-da-qui (*hors-là*), si de-territorializza (Lévy, 1995); gran parte dell'attività umana su Internet assomiglia a modelli di attività umane nello spazio reale (Kellerman, 2014).

Lavorare in maniera multidisciplinare allo sviluppo di modelli per la protezione delle attività virtualizzate, serve per ritracciare dei confini che nel cyberspazio sembrano essere fluidi o nebulosi. Data l'importanza strategica della materia, i governi, gli enti pubblici e privati cercano di conformarsi agli standard ufficiali, con lo scopo di proteggere le proprie organizzazioni. In particolare, in relazione ai processi di trasformazione digitale e alla convivenza tra il mondo reale e quello virtuale (Lévy, 1997; Carbone, 2007), si rileva che nel mercato turistico, considerato, soprattutto, nella sua dimensione geografica digitale (Mercatanti e Sabato, 2018), l'importanza della sicurezza informatica possa avere un impatto anche sulla sicurezza nazionale (Paradiso, 2013), perché gli ospiti viaggiano con il proprio bagaglio di dati privati e professionali. Pertanto, proteggere un turista significa tutelare il suo universo informativo e, allo stesso tempo, la reputazione di un'intera destinazione. Come è stato dimostrato da Bailetti e altri (2018), partire dal territorio può essere utile anche nel settore della sicurezza informatica. Effettivamente, l'approccio *glocal*, nel quale l'azione locale implica degli effetti globali, permette di fare azioni reali a livello territoriale per produrre benefici a livello nazionale. Infatti, consapevoli dei rischi, i governi di tutto il mondo hanno istituito apposite agenzie per migliorare l'igiene informatica delle organizzazioni e intrapreso campagne per aumentare la consapevolezza della sicurezza informatica dei viaggiatori. Tuttavia, le direttive nazionali sono spesso troppo complesse e poco gestibili per le piccole imprese.

Una complessità maggiore nel governo della tutela informatica si rileva nelle aziende turistiche di modeste dimensioni, caratterizzate da stagionalità e intermittenti gradi di intensità del lavoro. Proprio per questo in alcuni paesi, come l'Italia, dopo aver creato una piattaforma nazionale dedicata alla *cyber* sicurezza, è divenuta necessaria una semplificazione. Al fine di avere delle norme attuative più realistiche e operativa, è stata pubblicata una lista semplificata di «Controlli Fondamentali» (*Cyber essential controls*) con lo scopo di facilitare l'applicazione della Piattaforma nazionale per la sicurezza informatica (*Cyber aecurity framework*)[1] alle piccole e medie imprese. Tuttavia, noi riteniamo che sia necessario adottare ulteriori misure per adeguare i «Controlli Fonda-

mentali» e la Piattaforma nazionale per la sicurezza informatica al mercato del turismo. Basandoci su un approccio processuale, lo studio qui condotto propone un'ulteriore riduzione delle complessità. Lo scopo del presente lavoro è quello di contribuire alla preparazione della verticalizzazione della piattaforma nazionale per adattarla al comparto turistico. Nello specifico, si tende a rimodulare la Piattaforma nazionale per la sicurezza informatica a favore delle strutture ricettive di piccole dimensioni e indipendenti. L'obiettivo finale è quello di garantire una migliore efficienza organizzativa delle destinazioni.

Lo studio parte dall'analisi di contesto (le strutture ricettive locali) per giungere alla proposta di una «Piattaforma per la sicurezza informatica nel turismo». Negli ultimi anni si è assistito al fiorire di direttive e procedure dedicate alla «sicurezza informatica». In generale, questo incremento dei controlli ha generato un affaticamento negli utenti, rendendoli controproducenti (quote). Tali elementi sono particolarmente rilevanti nel settore turistico, dove i ritmi e i cicli delle attività sono diversi rispetto ad altri settori. Tutti questi fattori hanno ispirato un quesito: possiamo avere un approccio teorico per la sicurezza informatica, che sia contemporaneamente applicabile pragmaticamente al mercato turistico?

Nel presente lavoro si tenta di modificare il paradigma della *cyber* protezione (*cyber shield*) introducendo un approccio al processo. Infine, si è applicato tale approccio al caso italiano, arrivando a proporre una «Piattaforma per la Sicurezza Informatica nel Turismo».

2. La diffusione delle piattaforme dedicate alla sicurezza informatica

Al fine di prevenire gli attacchi via *web*, la maggior parte delle agenzie di sicurezza dei paesi avanzati ha sviluppato e diffuso specifiche tecniche e buone pratiche per garantire la sicurezza informatica delle imprese e delle organizzazioni nazionali. In Europa, l'agenzia dell'Unione Europea per la sicurezza delle reti e dell'informazione (ENISA) ha sviluppato nel 2013 un sistema di *cyber* sicurezza per i membri dell'Unione. Tra gli obiettivi più importanti del sistema ENISA si evidenziano: la lotta contro la criminalità informatica, l'equilibrio tra sicurezza e vita privata (*privacy*) e l'aumento della consapevolezza dei cittadini attraverso la formazione e i programmi educativi. Si tratta di obiettivi comuni presenti in ogni piattaforma di sicurezza informatica.

Tuttavia, vista l'importanza strategica dell'argomento, diversi paesi hanno deciso di attuare i propri sistemi nazionali di sicurezza informatica. In Francia, a causa del crescente numero di attacchi informatici contro gli interessi nazionali, nel 2008 il governo ha riconosciuto come priorità strategica la necessità di rafforzare la *cyber* sicurezza delle infrastrutture più esposte agli attacchi attraverso le norme del Critical infrastructures information protection (CIIP). Nel 2013 è stato istituito un quadro normativo dedicato al CIIP e conosciuto come la «legge CIIP»[2]. Nel Regno Unito, il *National cyber security center* (NCSC) ha sviluppato un metodo sistematico di valutazione della misura in cui un'organizzazione dovrebbe gestire adeguatamente i propri rischi di sicurezza informatica. Questo metodo di valutazione, altrimenti noto come il *Cyber assessment framework* (CAF), ha lo scopo di aiutare l'industria del Regno Unito, i dipartimenti governativi, le infrastrutture nazionali critiche e le PMI private a ridurre il rischio di attacchi informatici[3]. Negli Stati Uniti, il National institute of standards and technology (NIST) ha pubblicato nel febbraio 2014 la prima versione, aggiornata nell'aprile 2018 con la versione 1.1, di una piattaforma per migliorare l'infrastruttura della sicurezza informatica (Framework for improving critical infrastructure cyber security)[4].

In Italia, il centro di ricerca CIS (Cyber intelligence and information security research Center) dell'Università Sapienza di Roma ha sviluppato una piattaforma ispirata a quella del NIST per il miglioramento della sicurezza informatica delle proprie infrastrutture. L'obiettivo è stato quello di tracciare uno schema generale per creare un linguaggio condiviso tra esperti e aziende, introducendo, inoltre, un *corpus* di conoscenze sulla gestione del rischio per combattere le minacce informatiche e ridurre le violazioni.

Le piattaforme sopra elencate rappresentano alcuni esempi tra tutte quelle elaborate, in ambito governativo mondiale, per la sicurezza informatica. Un elenco completo è disponibile nell'archivio del National strategies of international telecommunications union (ITU)[5]. L'attività dei vari paesi mostra come la *cyber* igiene, e in generale la consapevolezza dei rischi informatici, siano diventati un argomento fondante delle politiche nazionali. Nonostante questo sforzo, la complessità di tali

sistemi può essere controproducente, soprattutto per le strutture più piccole preposte all'ospitalità. Infatti, le norme di *cyber* sicurezza sono spesso incardinate all'interno di protocolli estremamente articolati e di difficile implementazione. Il che induce le piccole strutture turistiche indipendenti a trascurare anche le più elementari operazioni di *cyber* igiene. La fatica può rendere inutili le piattaforme di sicurezza informatica. A settembre 2016, il NIST ha pubblicato uno studio dal titolo *Affaticamento da sicurezza* (*Security Fatigue*). Il lavoro dimostra che la maggior parte degli utenti assume un atteggiamento rischioso in termini di sicurezza informatica, sia sul lavoro, sia nella vita personale, quando le norme sono troppo vincolanti. I ricercatori Stanton, Theofanos, Prettyman e Furman (2016) hanno sostenuto che, anche se nel protocollo dell'intervista da loro condotta la fatica non è mai menzionata, più della metà dei partecipanti ha citato il termine correlandolo alla sicurezza; in generale i soggetti intervistati «hanno espresso il senso di dimissioni, perdita di controllo, fatalismo, minimizzazione del rischio ed elusione delle decisioni», elementi comuni di un meccanismo mentale noto come «affaticamento da sicurezza».

Lo studio ha sostenuto che gli utenti prendono decisioni sbagliate in merito alla sicurezza perché ci sono troppe scelte da effettuare e sono stanchi di dover continuamente sorvegliare il problema. L'importanza della fatica sulle decisioni è stata sottolineata nel 1973 da Amos Tversky e dal premio Nobel per l'economia Daniel Kahneman. Essenzialmente, i due scienziati hanno affermato che quando le persone assumono decisioni e si trovano in una situazione di prostrazione, ricorrono all'euristica e sono soggette ai pregiudizi cognitivi, chiamati anche *biases* (Baumeister, 2003). Dagli anni Settanta è stato pubblicato un gran numero di articoli sull'importanza della fatica nel processo decisionale. Tali studi hanno mostrato come la qualità delle decisioni sia direttamente proporzionale al momento in cui queste sono prese, dalla completezza delle informazioni che le persone gestiscono, dai limiti cognitivi delle loro menti (Acquisti e Grossklags, 2005) e dal luogo di lavoro in cui lavorano (Furnell e Thomson, 2009).

«Non importa quanto siamo intelligenti o laboriosi, la nostra capacità di prendere buone decisioni alla fine si esaurisce» (Oto, 3 aprile 2012) e contestualmente appare irrilevante lo stato d'avanzamento della tecnologia, in quanto l'atteggiamento, il comportamento, la consapevolezza dei dipendenti giocheranno sempre un ruolo significativo nell'aiutare a far fronte alle sfide della sicurezza informatica.

Tuttavia, il fattore umano è ancora una delle prime cause di attacco. Secondo *The Black Report 2018: Decoding the Mind of Hackers*[6], l'88% dei pirati informatici (*hackers*) dichiara di aver usato l'ingegneria sociale per raccogliere informazioni su un determinato obiettivo.

L'affaticamento da sicurezza appare dunque tra maggiori rischi per il buon funzionamento di una piattaforma di sicurezza informatica. Al fine di ridurre tali rischi, risulta pertanto fondamentale e strategico ridurre la complessità delle piattaforme proposte.

3. Dai rischi della prospettiva nazionale all'azione reale: interazione di globale e locale

Lo sviluppo degli spazi virtuali e delle metafore del *cyberspazio* non hanno eliminato la dimensione geografica territoriale, né gli orizzonti settoriali: la compenetrazione di globale e locale, virtuale e reale, è inarrestabile. Ed è effettivamente con questo approccio glocale che abbiamo concepito la Piattaforma di sicurezza informatica per il turismo. Sapendo che (Bailetti e altri, 2018) i processi di «glocalizzazione» possono avvenire dal basso verso l'alto (globalizzazione del locale), dall'alto verso il basso (localizzazione del globale) e orizzontalmente (migrazione del locale e disseminazione del globale), abbiamo sviluppato la nostra azione nel seguente ordine: globalizzazione del locale, identificando i problemi di applicazione delle norme legate alla sicurezza informatica globale nell'orizzonte turistico locale; localizzazione del globale, trasformando la Piattaforma nazionale per la sicurezza informatica in «Piattaforma per la Sicurezza Informatica nel Turismo».

Naturalmente, riteniamo che questo approccio possa portare nel futuro alle altre azioni orizzontali: migrazione del locale, attraverso la diffusione della piattaforma ad altri territori; disseminazione del globale, attraverso azioni di *governance* nazionale che invitino il settore turistico ad adattare una Piattaforma nazionale per la sicurezza informatica nel turismo.

Le piattaforme elaborate per tutelare la sicurezza informatica possono aiutare a limitare i danni, ma uno sforzo per ridurre l'affaticamento legato alla sicurezza informatica permetterebbe di rendere più efficaci i protocolli proposti. In realtà,

che i sistemi nazionali possano essere strumenti troppo complessi per le realtà produttive più piccole, è stato già constatato in diversi paesi.

In Italia, ad esempio, dopo il rilascio della Piattaforma nazionale per la sicurezza informatica da parte della CIS, il governo ha intuito la difficoltà che le piccole e medie imprese avevano ad applicarlo. Di fatto, il 95% delle aziende italiane sono composte da una media di 3,9 dipendenti (ANSA, 2015), e ciò ha reso il protocollo CIS inapplicabile per la maggior parte dell'imprenditoria nazionale. Per tale ragione lo stesso CIS nel 2016 ha deciso di sviluppare un microsistema ridotto a 15 «Controlli Fondamentali» per la sicurezza informatica (Baldoni, Montanari e Querzoni, 2017), al fine di consentire a un amministratore di sistema di una piccola o media impresa, senza una specifica conoscenza della sicurezza informatica, di raggiungere il livello minimo di conformità alla *cyber* sicurezza.

Tuttavia, una serie di interviste qualitative condotte al fine della presente ricerca su un campione di operatori turistici del nord Sardegna ha mostrato come questa riduzione non sia percepita come adatta alla propria struttura aziendale. In special modo, gli operatori, gli imprenditori del settore ricettivo, titolari di piccole strutture preposte all'accoglienza non collegate ad aziende multinazionali, hanno riscontrato elevate difficoltà di attuazione del suddetto protocollo. Il problema emerso tramite le interviste ha permesso di operare ulteriori riflessioni: l'industria alberghiera è caratterizzata da periodi di attività e di chiusura, ritmati da uno o più picchi lavorativi in cui è possibile riconoscere diversi gradi di stagionalità (Lozato-Giotart, 2008; Dewailly e Flament, 1996; Bencardino, 2010). Esistono aziende turistiche per le quali il periodo di apertura al pubblico può corrispondere con l'intero anno solare, ed esercizi prettamente estivi, che rimangono attivi solo pochi mesi. In ambito turistico la stagionalità (Bencardino e Greco, 2010; Panella, 2010), ossia l'intervallo di tempo tra l'apertura e la chiusura della struttura, rappresenta l'elemento centrale sul quale elaborare ogni strategia, sia essa riferita alla vendita del prodotto o al governo dell'azienda (Dallari e Grandi, 2005). Secondo Butler e Mao (1996), ci sono quattro diversi modelli di stagionalità: *a*) stagionalità a un picco: è la più comune ed è definita da un singolo, chiaramente identificabile e relativamente fisso, arco temporale di massima espressione della domanda; *b*) stagionalità a due picchi: caratterizzata da due intervalli di tempo, chiaramente identificabili e fissi, di espansione della domanda; *c*) stagionalità non di picco, nella quale il *trend* della domanda rimane costante; *d*) stagionalità dinamica: caratterizzata da uno o più intervalli temporali di picco, che tuttavia non sono fissi.

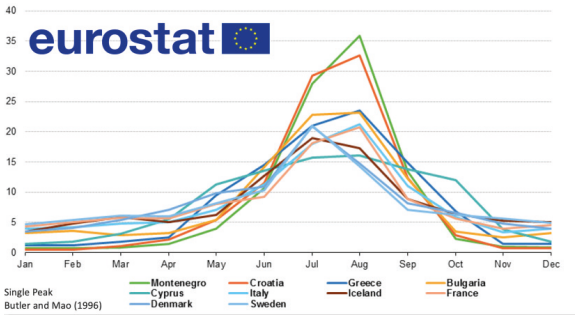

Fig. 1. Paesi europei a picco unico
Fonte: Eurostat, 2017

I diversi periodi di attività e tipi di stagionalità possono causare importanti cambiamenti nell'organizzazione globale della struttura ricettiva (Bencardino e Greco, op.cit.). Ad esempio, secondo Eurostat (2015), gli alberghi con una singola stagionalità possono avere una elevata rotazione dei dipendenti (*turnover*) e, conseguentemente, una significativa perdita del patrimonio delle conoscenze implicite.

Inoltre, ogni stagionalità prevede diversi gradi di intensità lavorativa, e ciò determina un differente ritmo di operatività. La conoscenza dell'intensità con la quale il lavoro deve essere affrontato gioca un ruolo fondamentale nel predefinire il comportamento dei dipendenti presenti in azienda. È evidente che differenti stagionalità (Panella, op.cit.) e particolari ritmi lavorativi implichino diversi comportamenti e un grado variabile di attenzione da parte dei lavoratori. Per quanto attiene la *cyber* sicurezza bisognerebbe ridurre le attività legate alla protezione e tutela informatica nei periodi più intensi del lavoro, e rimodulare le stesse nei mesi di minore tensione, in quanto esiste il rischio che durante i periodi di «picco», ogni dipendente si senta sovraccaricato di lavoro e provi affaticamento, diventando meno zelante nell'applicazione delle regole sulla sicurezza informatica. La condizione vissuta dall'individuo nei periodi di maggior carico lavorativo produce una tensione, che si esaspera quando si introducono, in aggiunta alle mansioni classiche, compiti legati alla gestione della sicurezza informatica. Si ingenera in questi casi il già citato «affaticamento da sicurezza», che

produce un esasperante rifiuto anche delle più elementari norme di igiene informatica.

Nel caso specifico, l'Italia, un territorio a forte vocazione turistica, è considerato un paese la cui attività turistica si caratterizza per elevati gradi di stagionalità (Bencardino, 2010). Questa è una condizione comune a molti territori come Montenegro, Cipro, Danimarca, Croazia, Svezia, Grecia, Islanda, Bulgaria e Francia (Eurostat, 2015) (fig. 1), pertanto i soggetti che operano nel comparto sono sottoposti ad alti picchi di lavoro intenso.

Partendo da tale considerazione, pare opportuno affrontare il tema della *cyber* sicurezza adattando le piattaforme alle realtà economiche specifiche, piuttosto che all'universo aziendale generale. Al contrario, le piattaforme nazionali di sicurezza informatica prese in considerazione dallo studio qui condotto, sembrano essere progettate per le grandi aziende, senza distinzioni di sorta. Inoltre, esse sono state implementate per rispondere a qualsiasi tipo di problema di sicurezza informatica (dalla *governance*, agli argomenti di natura strettamente tecnica) e per tale ragione risultano troppo complicate per le piccole imprese, nelle quali spesso manca una figura, con mansioni specifiche, dedicata a tale tema. Pertanto, sebbene il CIS abbia semplificato la Piattaforma nazionale per la sicurezza informatica, questa continua a non considerare le peculiarità di ciascuna tipologia lavorativa. Finanche la lista semplificata dei «controlli fondamentali» (composta da soli 15 controlli), potrebbe rivelarsi ancora troppo complessa per determinate realtà imprenditoriali.

Un piano sulla sicurezza informatica è generalmente centrato sul rischio informatico a cui sono sottoposte attività costanti nel tempo, ossia attive tutto l'anno senza picchi di lavoro. Lo studio qui presentato propone uno schema specifico concepito tenendo conto delle effettive esigenze espresse dalle strutture alberghiere. L'obiettivo è quello di aumentare l'igiene della sicurezza informatica senza influenzare le prestazioni e la qualità del servizio turistico. Per raggiungere tale obiettivo, si è cercato di armonizzare la Piattaforma nazionale per la sicurezza informatica, riorganizzandola in relazione alla stagionalità. In pratica, invece di utilizzare un approccio centrato sulla funzionalità della sicurezza informatica, ci si è ispirati ad una concezione incentrata sul processo («process centered design»; Gruhn, 2002), per progettare una nuova piattaforma che tenga conto dell'andamento ciclico del lavoro. In effetti, è noto che l'utilizzo di un approccio basato sul processo è utile per ridurre al minimo lo sforzo di conformità (Ciommer, 2003) a diversi sistemi di qualità. La mappatura dei processi è uno strumento funzionale alla rilevazione dell'importanza della stagionalità nel mercato dell'ospitalità. Esso inoltre aiuta a comprendere in che maniera evolve il lavoro dei dipendenti, e nel caso specifico ha mostrato come i periodi di lavoro influenzassero la capacità di prendere decisioni e di applicare, correttamente, un protocollo di sicurezza. Porre la stagionalità al centro del ragionamento, permette di riorganizzare il sistema della sicurezza informatica in maniera sostenibile, garantendo il raggiungimento di un livello di tutela ottimale, a favore dell'azienda e della destinazione turistica nel suo complesso.

4. Verso una piattaforma di sicurezza informatica per il comparto turistico

In tutti i paesi europei l'agenzia nazionale per la sicurezza informatica ha fornito raccomandazioni per imprese, industrie e amministrazioni (Pires, 2012). In Italia, come accennato in precedenza, l'azione principale intrapresa in tale ambito è stata ispirata dalla piattaforma per il miglioramento delle infrastrutture critiche della sicurezza informatica, sviluppato dal NIST[7], il National institute of standards and technology degli USA. Pertanto, per adattarsi meglio al contesto italiano, il CIS dell'Università Sapienza di Roma, ha adottato delle modifiche, considerando che in Italia, la netta maggioranza delle aziende è di dimensioni medie, piccole e molto piccole (Celant e Ferri, 2009) e generalmente, queste realtà imprenditoriali non prevedono al proprio interno delle risorse umane dedicate al settore della sicurezza informatica. Queste ragioni hanno spinto il CIS a realizzare uno strumento più elementare ed efficiente, che consta di solamente 15 «controlli fondamentali» per la sicurezza informatica. Questi controlli possono essere adottati e implementati da medie, piccole o microimprese, per ridurre la vulnerabilità dei loro sistemi e aumentare la consapevolezza del rischio informatico nel personale, al fine di far fronte ai *cyber* attacchi più comuni (Baldoni, Montanari e Querzoni, 2017).

Si è precedentemente rilevato che tale semplificazione potrebbe essere utile, ma non sufficiente per il settore alberghiero. Sulla base di quanto asserito e traendo ispirazione dalla progettazione orientata al processo, il gruppo di ricerca

impegnato nel presente studio ha rielaborato la Piattaforma nazionale per la sicurezza informatica del CIS e contestualizzato le sue 21 sottocategorie in una piattaforma stagionale, più adatta ai modelli di processo dell'industria alberghiera italiana. Per completezza, anche i 15 «controlli fondamentali» di sicurezza informatica sono stati integrati alla nuova piattaforma, modificando leggermente la numerazione originale.

4.1. Metodologia

In una prima fase della ricerca, attraverso le interviste rivolte a responsabili del settore alberghiero del nord Sardegna, è stato possibile delineare il modello di base del ritmo che caratterizza il lavoro stagionale del settore. Contestualmente si è associato ad ogni periodo di lavoro un differente grado di tempestività ed efficienza decisionale.

Per quanto attiene il ritmo del lavoro, si è rilevata una stagionalità di un picco, composta da tre periodi, cadenzati come segue (fig. 2): *a*) periodo precedente. Precede l'apertura stagionale della struttura e rappresenta il momento in cui la direzione progetta e pianifica l'attività a livello globale; in questa fase la direzione ha il tempo di lavorare sulla *governance*; *b*) periodo di bassa attività. Temporalmente, la fase immediatamente precedente al picco; è il momento adatto per testare e migliorare l'efficienza del processo; *c*) picco. In questa fase di lavoro intenso i dipendenti dovrebbero essere perfettamente formati e le comunicazioni interne sulla sicurezza informatica devono diventare fluide.

Studiando il tipo di frequenza delle attività legate alla piattaforma del CIS, ogni norma è stata rapportata ad un ritmo lavorativo e associata ad una delle 3 fasi operative che compongono il piano di sicurezza informatica qui proposto: *a*) fase 1: verifica delle precondizioni; *b*) fase 2: manutenzione regolare e analisi dei rischi; *c*) fase 3: esigenze giornaliere.

Mentre l'analisi delle precondizioni costituisce l'elemento statico, rilevabile al momento «zero» (periodo precedente all'apertura stagionale), le altre attività, che caratterizzano le fasi 2 e 3, rappresentano il fattore dinamico, e sono suscettibili di varie rimodulazioni in relazione all'intensità lavorativa.

Per tracciare un parallelo, la struttura di approccio stagionale è come un'antica fortezza in cui le precondizioni stagionali sono come muri, ponti levatoi, fossati e torri di avvistamento; la manutenzione regolare e l'analisi dei rischi della fortezza rappresentano l'attività svolta da maestri

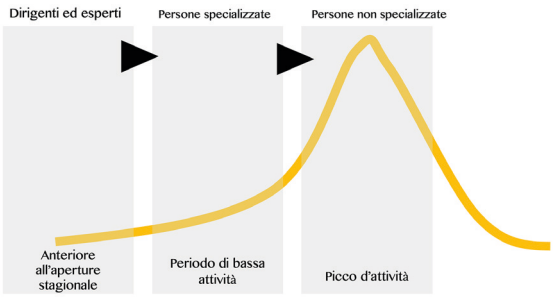

Fig. 2. Periodi di attività
Fonte: elaborazione degli autori

artigiani e strateghi militari; le esigenze quotidiane potrebbero essere associate ai guardiani. Come per questi ultimi, anche per i dipendenti deve essere costante una forma di vigile attenzione, sollecitata dalla consapevolezza del rischio. Le basi per la sicurezza informatica dovrebbero essere poste all'inizio di un periodo, attraverso precondizioni stagionali, per poi verificare, con sistematicità, che le risorse funzionino e siano adattate ai nuovi rischi, attraverso la manutenzione e le analisi periodiche. Infine, dovrebbe essere sempre attiva una forma di consapevolezza sulla sicurezza informatica riferita alle azioni che si compiono giornalmente, in base alle esigenze quotidiane.

4.2. Verticalizzazione del sistema nazionale

Le regole della Piattaforma nazionale della sicurezza informatica e i 15 «controlli fondamentali» sono stati distribuiti nei periodi, ottenendo una piattaforma multilivello adattata alle esigenze delle strutture ricettive di piccole dimensioni (fig. 3). Il piano di sicurezza informatica rimodulato in funzione della stagionalità (fig. 4) permetterà di limitare un sovraffaticamento del personale dipendente, garantendo un più alto livello di igiene informatica.

5. Conclusioni

La sicurezza informatica è considerata una questione importante in qualsiasi organizzazione, ma la discussione tende a non oltrepassare il livello tecnico, senza considerarne aspetti fondamentali, quali la sostenibilità di un'azione di prevenzione da parte delle piccole imprese e lo *stress* ingenerato sul personale dipendente dall'applicazione

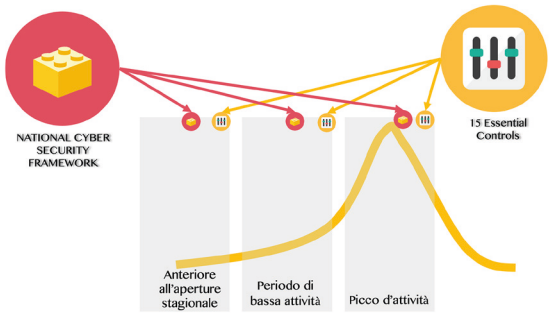

Fig. 3. Modello per la distribuzione di norme e controlli
Fonte: elaborazione degli autori

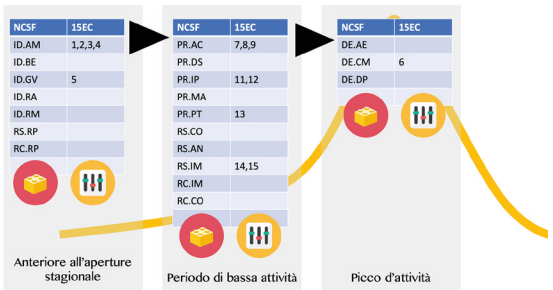

Fig. 4. Distribuzione delle regole durante il picco
Fonte: elaborazione degli autori

di protocolli complessi. Gli approcci comportamentali, assunti in riferimento al problema della sicurezza informatica dalla prospettiva dell'atteggiamento soggettivo al problema, si concentrano principalmente sul comportamento individuale connesso alla modalità con cui ci si avvicina alla gestione delle informazioni, in modalità sicura (Acquisti e altri, 2017). Tuttavia, si è discusso molto poco su come ridurre il carico cognitivo riadattando una piattaforma generale di prevenzione informatica, a un sistema organizzativo di modeste dimensioni. Il presente lavoro ha sottolineato l'importanza di rimodulare il protocollo di sicurezza informatica al processo che caratterizza il comparto turistico, rivolgendo l'attenzione alle strutture ricettive di piccola dimensione. Si ritiene che altrettanto vada fatto per altre imprese che operano nei vari settori economici, adattando il sistema nazionale della sicurezza informatica alle differenti tipologie di attività economiche.

La ricerca qui condotta ha cercato soluzioni pratiche per ridurre il peso fisico e cognitivo della *cyber* protezione sul soggetto individuale, considerando il carico lavorativo stagionale. Il gruppo di ricerca ha rimodulato la Piattaforma nazionale per la sicurezza informatica e i suoi «controlli fondamentali» al ritmo reale di una struttura ricettiva di piccole dimensioni, con l'intento di contrastare «l'affaticamento da sicurezza», considerato uno dei fattori che più incidono sulla capacità di prendere la decisione giusta al momento giusto. Tale approccio permette di aumentare il livello di *cyber* igiene aziendale e, in generale, di assicurare maggiori livelli di tutela a favore dei territori a vocazione turistica. Un elemento essenziale emerso dallo studio è che il tema della sicurezza informatica debba essere affrontato con un approccio multidisciplinare, al fine di combinare più aspetti: la *governance*, la gestione d'impresa, le competenze tecniche, gli aspetti comportamentali e decisionali. Solo un approccio olistico, e l'adeguamento del sistema alle varie realtà dimensionali dell'impresa, garantiscono il raggiungimento di un ottimale standard di sicurezza.

Riferimenti bibliografici

Acquisti Alessandro, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, Yang Wang e Shomir Wilson (2017), *Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online*, in «ACM Computing Surveys» 50, 3, articolo 44.

Acquisti Alessandro e Jens Grossklags (2005), *Privacy and Rationality in Individual Decision Making*, in «IEEE Security and Privacy», 3, 1, pp. 26-33.

ANSA (2015), *Istat: in Italia 4,2 milioni di microimprese, 95 % del totale*, 20 maggio.

Bailetti Tony, Alexandre Enkerli, Daniel Craigen e Stoyan Tanev (2018), *Applying Glocalization Principles to Enhance a Cybersecurity Ecosystem of Ecosystems*, in *Proceedings of The ISPIM Innovation Forum, (Boston, 25-28 marzo 2018)*.

Bakis Henry e Edward Mozley Roche (1998), *Cyberspace - The Nervous System of Emerging Societies and its Spatial Functions*, in «Cybergeo: European Journal of Geography», pp. 1-12.

Baldoni Roberto, Luca Montanari e Leonardo Querzoni (a cura di) (2017), *2016 Italian Cybersecurity Report, Controlli Essenziali di Cybersecurity*, Roma, CIS Sapienza.

Baumeister Roy F. (2003), *The Psychology of Irrationality*, in Isabelle Brocas e Juan D. Carrillo (a cura di), *The Psychology of Economic Decisions. Volume I: Rationality and well-being*, Oxford, Oxford University Press, pp. 1-15.

Bencardino Filippo (a cura di) (2010), *Turismo e territorio. L'impatto economico e territoriale del turismo in Campania*,

Milano, Angeli (pubblicazioni «DASES»).
Bencardino Massimiliano e Ilaria Greco (2010), *Il "Sistema locale dell'offerta turistica" nella provincia di Benevento: un modello allo stato embrionale*, in Filippo Bencardino (2010), pp. 144-180.
Butler Richard W e Baodi Mao (1996), *Conceptual and theoretical implications of tourism between partitioned states*, in «Asia Pacific Journal of Tourism Research», 1, pp. 25-34.
Carbone Luisa (2007), *L'informazione geografica e la rete*, in «Semestrale di Studi e Ricerche di Geografia», (strumenti di lettura), pp. 85-94.
Castells Manuel (1996), *The Information Age: Economy, Society and Culture. The Rise of the Network Society*, Oxford, Blackwell.
Celant Attilio e Maria Antonella Ferri (2009), *L'Italia. Il declino economico e la forza del turismo. Fattori di vulnerabilità e potenziale competitivo di un settore strategico*, Roma, Marchesi.
Ciommer Bernhard (2003), *Using a Process-Centered Approach to Minimize the Effort of Compliance*, in «Accreditation and Quality Assurance», 8, pp. 82-85.
Dallari Fiorella e Silvia Grandi (a cura di) (2005), *Economia e Geografia del Turismo. L'occasione dei GIS*, Bologna, Pàtron.
Dewailly Jean-Michel e Emile Flament (1996), *Geografia del turismo e delle attività ricreative*, Bologna, Clueb.
Eurostat (2015), *Seasonality in the Tourist Accommodation Sector*, vol. 2016, *http://ec.europa.eu/eurostat/statistics-explained/index.php/Seasonality_in_the_tourist_accommodation_sector* (ultimo accesso: 27.VI.2018).
Furnell Steven e Kerry-Lynn Thomson (2009), *Recognising and Addressing 'Security Fatigue'*, in «Computer Fraud and Security», 11, pp. 7-11.
Graham Mark (2013), *Geography/Internet: Ethereal Alternate Dimensions of Cyberspace or Grounded Augmented Realities?*, in «The Geographical Journal», 179, pp. 177-182.
Gruhn Volker (2002), *Process-Centered Software Engineering Environments, A Brief History and Future Challenges*, in «Annals of Software Engineering», 14, pp. 363-382.
Inkpen Gary (1994), *Information Technology for Travel and Tourism*, Londra, Pitman.
Kellerman Aharon (2007), *Cyberspace Classification and Cognition: Information and Communications Cyberspaces*, in «Journal of Urban Technology», 14, pp. 5-32.
Kellerman Aharon (2014), *The Internet as Second Action Space*, Londra, Routledge.
Lévy Pierre (1995), *Qu'est-ce que le virtuel?*, Parigi, La Découverte.
Lévy Pierre (1997), *Il virtuale*, Milano, Raffaello Cortina.
Lozato-Giotart Jean-Pierre (2008), *Geografia del turismo. Dallo spazio consumato allo spazio gestito*, (traduzione italiana di Alessia Mariotti e Enza Zabbini), Milano, Hoepli.
Mercatanti Leonardo e Gaetano Sabato (2018), *Geografie digitali. Spazi e socialità*, Milano, StreetLib.
Oto Brandon (2012), *When Thinking is Hard: Managing Decision Fatigue*, in «EMSWORLD», 3 aprile.
Panella Romina (2010), *Il turismo e il mercato del lavoro*, in Filippo Bencardino (2010), pp. 299-336.
Paradiso Maria (2013), *Per una geografia critica delle «smart cities». Tra innovazione, marginalità, equità, democrazia, sorveglianza*, in «Bollettino della Società Geografica Italiana», Serie XIII, vol. VI, pp. 679-693.
Pires Hindenburgo Francisco (2012), *Estados Nacionais, Soberania e Regulação da Internet*, in «Scripta Nova. Revista Electrónica de Geografía y Ciencias Sociales», vol. XVI, n. 418 (63), 1 novembre.
Santos Milton (1996), *A Natureza do Espaço*, San Paolo, Hucitec.
Stanton Brian, Mary F. Theofanos, Sandra Spickard Prettyman e Furman Susanne (2016), *Security Fatigue*, in «IT Professional», 18, 5, pp. 26-32.
Tversky Amos e Daniel Kahneman (1973), *Availability: A Heuristic for Judging Frequency and Probability*, in «Cognitive Psychology», 5, pp. 207-232.
Warf Barney (2013), *Global Geographies of the Internet*, Dordrecht, Springer.

Note

[1] *https:// www.cybersecurityframework.it* (ultimo accesso: 31.VII.2018).
[2] *The French CIIP Framework* (*https://www.ssi.gouv.fr/en/cybersecurity-in-france/ciip-in-france/*; ultimo accesso: 31.07.2018).
[3] *https://www.ncsc.gov.uk/guidance*; ultimo accesso: 31.07.2018.
[4] *National Institute of Standards and Technology* (*https://www.nist.gov/cyberframework/framework*; ultimo accesso: 31.07.2018).
[5] *https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx*; ultimo accesso: 31.VII.2018.
[6] *https://www.nuix.com*; ultimo accesso: 31.VII.2018.
[7] *https://www.nist.gov*; ultimo accesso: 31.VII.2018.