Melissa Capelli

I diversi volti della cybersecurity: da adempimento a vantaggio competitivo. Cenni al settore turistico

Abstract: Oggi viviamo costantemente "connessi". La tecnologia presenta molte opportunità, ma anche alcuni rischi. Di recente, infatti, gli attacchi informatici sono aumentati quantitativamente, in termini di impatto e di sofisticazione, costituendo un rischio per ogni settore economico. Il legislatore europeo è quindi intervenuto sul piano normativo per rispondere alle sfide odierne. L'aumento della digitalizzazione e della connettività, infatti, rischia di compromettere la tutela dei diritti e delle libertà fondamentali. Lo scopo di questo contributo è quello di rivedere e analizzare la legislazione in materia per verificare se può essere efficace nel proteggere i diritti fondamentali e promuovere la competitività all'interno dei mercati. Per rispondere, viene proposto un breve studio sull'applicazione della cybersecurity nel settore del turismo. In questo settore, lo sviluppo delle TIC non ha avuto un impatto solo sui consumatori e sugli operatori, ma anche sulle destinazioni. L'innovazione tecnologica diventa un driver fondamentale per la crescita dei territori: la cybersecurity diventa quindi non solo una condizione necessaria per garantire i diritti dei turisti, ma soprattutto un vantaggio competitivo.

Keywords: Cybersecurity, Turismo, Diritti, Competitività, Smart Destinations.

Sommario: 1. Luci ed ombre dell'*IoT* – 2. Le principali soluzioni normative europee ed italiane: un breve *excursus* – 3. Gli effetti dello sviluppo delle tecnologie sul settore turistico – 4. Conclusioni e sfide future.

1. Luci ed ombre dell'*IoT*

La società moderna è caratterizzata da elevati ritmi di vita, contraddistinti da cambiamenti rapidi da un tempo cronometrico, lineare, parcellizzato e non qualitativo. Si vive costantemente ´connessí e la tecnologia permea ogni aspetto della vita quotidiana. Oggigiorno, grazie al proprio *smartphone* è possibile, non solo effettuare telefonate e inviare messaggi, ma ricevere e inviare email, partecipare a videochiamate, effettuare operazioni finanziarie tramite *homebanking*, godersi un film collegandosi alle *smart tv* e perfino controllare alcuni elettrodomestici. Tutto ciò è reso possibile dallo sviluppo del settore *ICT*. "Negli ultimi venti anni, la diffusione delle nuove tecnologie dell'informazione e delle comunicazioni ha progressivamente focalizzato il centro delle attività umane di carattere sociale, politico ed econo-

Teoria e Critica della Regolazione Sociale, n. 2, 2024 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320786 • DOI: 10.7413/197054760145

mico all'interno di una nuova dimensione, denominata cibernetica"[1]. Ecco che, nel tempo, si è creata quella che viene definita *Internet of Things* (*IoT*), ossia una

> rete di oggetti dotati di tecnologie di identificazione, collegati fra di loro, in grado di comunicare sia reciprocamente sia verso punti nodali del sistema, ma soprattutto in grado di costituire un enorme *network* di cose dove ognuna di esse è rintracciabile per nome e in riferimento alla posizione.[2]

Alla luce di tale definizione, l'*IoT* offre nuove opportunità per l'automazione e l'efficienza: i diversi dispositivi, infatti, raccolgono, elaborano e trasmettono dati utili per automatizzare processi, migliorare la sicurezza, ottimizzare le prestazioni e fornire servizi personalizzati. Attraverso i progressi tecnologici, l'*IoT* è in continua espansione, permettendo di spalancare un intero universo di nuove opportunità ed innovazioni in diversi settori: dalla sanità all'agricoltura, dalla produzione industriale alla gestione delle città intelligenti[3].

Con l'incremento delle innovazioni, tuttavia, non crescono unicamente le opportunità, ma anche la dipendenza tecnologica e soprattutto, il rischio di essere vittime di *cyber* attacchi. I crimini informatici crescono nel tempo sia numericamente che qualitativamente, diventando sempre più sofisticati (alcuni attacchi sfruttano perfino l'*AI*)[4]. Per quantificare tale fenomeno, basti pensare che, nel primo semestre del 2023, il numero di nuovi *malware* si avvicina ai 2 milioni e mezzo. Sia l'*ENISA Threat Landscape* (ETL), che la relazione dell'ACN testimoniano come il 2023 sia stato un anno particolarmente prolifico per i *cyber* attacchi: nel dettaglio, l'ETL rileva che, tra luglio 2022 e giugno 2023 vi sia stata una crescita esponenziale degli attacchi rispetto all'anno precedente, con circa 2580 incidenti, cui ne vanno sommati altri 220 che hanno colpito due o più Stati membri dell'UE[5]; mentre la relazione annuale dell'ACN conta 1.411 attacchi *cyber* trattati dalla stessa (+29% rispetto al 2022)[6]. Se tali dati non fossero sufficienti a testimoniare la gravità della

1 Cencetti 2014: 11.

2 Cfr. Treccani.

In realtà tale locuzione non è affatto recente: essa è stata coniata nel 1999 dall'ingegnere inglese Kevin Ahston.

3 "Lo spazio cibernetico ha permesso immense opportunità di sviluppo economico, grazie alle quali le economie dei paesi più avanzati hanno subito una forte accelerazione".

Cencetti 2014.

4 "I sistemi digitali sono divenuti così complessi che è impossibile impedire tutti gli attacchi. Per rispondere a questa sfida occorre una rapida azione di rilevazione e risposta".

Corte dei conti europea 2019: 5.

5 A titolo meramente esemplificativo, l'ETL rileva un aumento sostanziale degli incidenti legati al *ransomware*, soprattutto a partire dal mese di marzo 2023 (+ 91% rispetto al mese precedente e + 62% rispetto a marzo 2022); nonché un incremento del 135% degli attacchi che sfruttano le tecnologie dell'*AI* nel mese di febbraio 2023 rispetto al mese precedente. Per approfondimenti si veda ENISA 2023.

6 Nel dettaglio, l'ACN sottolinea che il numero dei soggetti colpiti è triplicato (da 1.150 a 3.302), rilevando un forte aumento anche degli incidenti (da 126 a 303) e delle segnalazioni (da 81 a 349). Per approfondimenti, ACN 2024.

situazione, Assintel ha rilevato un incremento del 184% di *cyber* attacchi nel mondo (con un totale di 7.068), dei quali il 61% proveniente dal *Dark Web*[7]. Dietro a ciò, naturalmente, si nasconde anche un danno economico[8].

Ecco quindi che, in una società nella quale si parla di rete 5g, di servizi *multicloud* e di digitalizzazione delle informazioni, la *cybersecurity* diventa essenziale. Non esiste una definizione univoca di *cybersecurity*, ma a livello europeo, essa può essere definita come "l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche"[9]. È quindi chiaro come vi rientrino sia le attività di prevenzione che quelle relative all'individuazione degli incidenti informatici[10], nonché le risposte agli stessi ed il successivo recupero.

2. Le principali soluzioni normative europee ed italiane: un breve *excursus*

Alla luce di quanto illustrato, non deve stupire il fatto che il Legislatore europeo abbia inserito la *cybersecurity* tra le proprie priorità fondamentali, intervenendo sul lato normativo al fine di rispondere alle sfide odierne. L'incremento della digitalizzazione[11] e della connettività, infatti, rischia di minare la tutela di diritti e di libertà fondamentali, quali la protezione della vita privata e dei dati personali, la libertà d'impresa e la protezione della proprietà o la dignità e l'integrità della persona.

La prima criticità inerente tale intervento è costituita dalla mancanza di una definizione di sicurezza informatica tra gli atti legislativi vincolanti. Il primo approc-

7 Assintel 2024, *Cyber Report 2023*.

8 Uno studio del 2020 del Joint Research Centre ha stimato che il costo globale della criminalità informatica raggiungerà i 5,5 trilioni di euro entro la fine del 2020, rispetto ai 2,7 trilioni di euro del 2015. Le stime per il 2025 arrivano a 10,5 trilioni di dollari. Il costo medio globale di una violazione dei dati nel 2022 è stato stimato in 4,35 milioni di dollari. Tali importi vanno parametrati e cambiano in relazione al settore (le violazioni dei dati sanitari ammontano in media a 10,10 milioni di dollari), al tipo di attacco (gli attacchi distruttivi ammontano in media a 5,12 milioni di dollari) ed alla regione interessata (le violazioni dei dati negli Stati Uniti ammontano in media a 9,44 milioni di dollari). Oltre a ciò, si ricorda che il danno del *cybercrime* non è limitato solo alle entità colpite: oltre il 45% delle violazioni, infatti, riguarda dati personali, esponendo così i cittadini di tutto il mondo a vari rischi, come il furto di identità e la frode finanziaria.

Cfr. Vandezande 2024: 2.

9 https://www.consilium.europa.eu/it/policies/cybersecurity/.

"In termini ampi, essa designa il complesso di tutele e misure adottate per difendere i sistemi informativi e i relativi utenti da accessi non autorizzati, attacchi e danni al fine di assicurare la riservatezza, l'integrità e la disponibilità dei dati".

Corte dei conti europea 2019: 7.

10 Tra gli incidenti informatici si possono annoverare: attacchi a imprese ed infrastrutture critiche, furto di dati, frodi, divulgazione accidentale di dati. Indipendentemente dalla fattispecie, tuttavia, tutti possono avere potenzialmente effetti dannosi di ampia portata su persone fisiche, organizzazioni e comunità. A mero titolo esemplificativo, il *ransomware Wannacry* e il *wiper NotPetya* hanno colpito, nel 2017, in totale oltre 320.000 soggetti in circa 150 Paesi. Per approfondimenti si veda Greenberg 2017.

11 Per eventuali approfondimenti, Golisano 2022.

cio alla materia si ha nel 2013 tramite la Comunicazione "Strategia dell'Unione europea per la cybersicurezza: un cyberspazio aperto e sicuro", che ha fornito una descrizione completa di cosa s'intenda per cybersicurezza ed ha accompagnato la strategia dell'UE sulla *cybersecurity* del 2013 (EUCSS 2013). Essa, per la prima volta, ha fissato l'obiettivo di sviluppare una linea a livello comunitario in tale ambito. In tale pacchetto, rientra la direttiva UE 2016/1148 (c.d direttiva NIS). Tale strumento giuridico è molto importante perché, non solo costituisce la prima iniziativa legislativa orizzontale vincolante dell'UE su questa tematica, ma rappresenta una sintesi della maggior parte delle indicazioni incluse nelle precedenti comunicazioni della Commissione. Alla direttiva soggiacciono due obiettivi complementari: la protezione delle infrastrutture critiche e la promozione e potenziamento del mercato interno dell'UE.

Nonostante l'importanza di tale strumento, lo stesso è stato criticato[12], in quanto la NIS si occupa di sicurezza, un'area in cui UE e Stati membri condividono le competenze legislative. Tali critiche sono cessate in seguito ad una lettura attenta del considerando 5, il quale afferma che, in assenza di standard di protezione condivisi, non si avrebbe un'adeguata protezione dei consumatori e delle imprese. Nonostante l'evidente importanza della direttiva NIS, essa non può essere considerata un traguardo, in quanto si concentra maggiormente sull'armonizzazione degli aspetti procedurali per gestire i rischi piuttosto che fornire sostanziali chiarimenti in merito a quali siano i rischi e le minacce per cui tali procedure devono essere adottate. Tale strumento normativo, inoltre, è risultato di difficile attuazione[13], quindi, la direttiva NIS è stata novellata dalla direttiva UE 2022/2555 (c.d. NIS2) ed abrogata a decorrere dal 18 ottobre 2024. La *ratio* è quella di affrontare un panorama di minacce mutato radicalmente e ovviare, al tempo stesso, le problematiche che hanno impedito alla direttiva NIS di ottenere i risultati sperati[14]. Uno dei punti cardine della NIS2 è quello di affrontare esplicitamente la protezione della *supply chain*[15].

12 La stessa Commissione ha effettuato una valutazione sulla direttiva, evidenziando che la stessa non copre tutti i settori che forniscono servizi chiave all'economia e alla società, ma che soprattutto, la normativa avesse concesso poteri discrezionali troppo ampi agli Stati membri.

13 Gli Stati membri hanno infatti recepito la direttiva in modo difforme, vanificando l'intento della normativa stessa e creando, di fatto, un'insufficiente risposta alle nuove e mutevoli sfide della sicurezza informatica.

14 La NIS2, infatti, amplia la portata della direttiva NIS, aumentandone la copertura dei settori: rispetto alle aziende assoggettate alla NIS che venivano identificate da decisioni delle Autorità nazionali competenti, la nuova normativa introduce un singolo criterio per le aziende nei settori elencati, in base al quale devono essere identificate principalmente *ipso iure*, ovvero le dimensioni di un'azienda.

Per approfondire le caratteristiche della Direttiva NIS2 ed apprenderne le principali sfide, si veda Sievers 2021.

15 Per un confronto tra direttiva NIS e NIS2, si consiglia N. Vandezande 2024. Per un approfondimento su NIS2 e *supply chain*, invece, si veda van 't Schip, 2024, nel quale, comunque emergono alcune imperfezioni dell'ultima direttiva.

La strategia europea[16] è stata poi modificata nel 2017 attraverso un pacchetto di norme che comprende misure, vincolanti e non, con le quali la Commissione ha inteso affrontare le nuove sfide in tale ambito. Se la direttiva NIS era il fiore all'occhiello della precedente strategia, questa volta, la punta di diamante è il Regolamento UE 2019/881 (il c.d. *Cybersecurity Act*). Tale regolamento spinge verso un nuovo approccio proattivo, che porti alla costruzione di un sistema condiviso di comprensione dei rischi peculiari della *cybersecurity*.

Rispetto alla presente trattazione, la seconda parte del regolamento, cioè quella relativa alla creazione di un sistema di certificazione della *cybersecurity* dell'UE per prodotti, servizi e processi *ICT*, risulta indubbiamente più interessante. Senza entrare nel dettaglio, il *cybersecurity act* mira a rafforzare il ruolo dell'UE nello scenario globale, migliorando il coordinamento transfrontaliero, dando impulso a misure volte all'armonizzazione sostanziale e procedurale in ambito di cybersicurezza ed infine, promuovendo uno standard europeo in tale ambito. In questa breve disamina non può mancare la proposta di nuovo regolamento, già approvata dal Parlamento europeo: il *Cyber Resilience Act* (CRA)[17], il cui obiettivo è salvaguardare i consumatori e le imprese che acquistano o utilizzano prodotti o *software* con un componente digitale, andando ad integrare la direttiva NIS2[18]. Alla luce di tale carrellata, appare chiaro come,

> nel gergo delle politiche dell'UE, il termine cybersicurezza non è riferito esclusivamente alla sicurezza delle reti e dei sistemi informativi, bensì designa qualsiasi attività illecita che comporti l'impiego di tecnologie digitali nel cyberspazio. Può comprendere quindi reati informatici quali gli attacchi con virus informatici e le frodi perpetrate con mezzi di pagamento diversi dai contanti, travalicando la separazione fra sistemi e contenuti, come nel caso della diffusione online di materiale pedopornografico. Può anche riguardare campagne di disinformazione volte a influenzare il dibattito online e produrre presunte interferenze nelle consultazioni elettorali. In aggiunta, Europol nota una convergenza tra criminalità informatica e terrorismo.[19]

Nonostante le azioni degli anni '90 (l. n. 547 del 23 dicembre 1993 e l. n. 269 del 3 agosto 1998), che hanno definito i reati informatici, apportando importanti modifiche al Codice penale e a quello di procedura penale, dal punto di vista della normativa italiana, gli interventi sono tutti abbastanza recenti. Nel 2002, si è

16 Tale strategia si basa su tre pilastri: resilienza, sovranità tecnologica e *leadership*; capacità operativa per prevenire, scoraggiare e rispondere; ed infine, cooperazione per promuovere un cyberspazio globale e aperto.

17 Per approfondimenti in merito, si veda Chiara 2023.

18 Il *Cyber Resilience Act*, infatti, prevede requisiti di sicurezza informatica per prodotti, *hardware* e *software*, con elementi digitali, anche non coperti da NIS2, con l'obiettivo di affrontare il problema legato al fatto che i dispositivi, come computer e *smartphone*, vengono spesso immessi sul mercato con vulnerabilità di sicurezza e/o una mancanza di aggiornamenti di sicurezza per tutto il loro ciclo di vita. Per approfondimenti, si veda Vandezande 2024

19 Corte dei conti europea 2019: 7.

Per una panoramica più approfondita sulla normativa inerente la sicurezza informatica dell'*IoT*, si veda Chiara 2022.

iniziato ad occuparsi di protezione delle informazioni in formato digitale raccolte dalle PA; mentre, l'anno successivo è stato istituito l'Osservatorio permanente per la sicurezza e la tutela delle reti e delle comunicazioni. Da questo momento, diversi interventi si sono susseguiti: il D.Lgs. n. 196 del 30 giugno 2003 (Codice della privacy), il D.Lgs. n. 259 del 1° agosto 2003 (Codice delle comunicazioni elettroniche), il D.Lgs. n. 82 del 7 marzo 2005 (Codice dell'amministrazione digitale), la l. n. 38 del 6 febbraio 2006 (Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet). In questa breve disamina, non possono mancare il D.lgs. 18 maggio 2018 n. 65 (c.d. D.Lgs. NIS) che ha introdotto una serie di obblighi di sicurezza a carico degli operatori e fornitori dei servizi digitali nell'adozione di misure di sicurezza e notifica degli incidenti e ha previsto la creazione del CSIRT; il D.L. n. 105 del 2019, adottato con lo scopo di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, nonché degli enti e degli operatori nazionali, pubblici e privati; il D.L. n. 162 del 2019, che ha novellato la normativa precedente; il D.L. 14 giugno 2021, n. 82 "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale", convertito in legge dalla l. del 04 agosto 2021, n. 109 (si ricorda infatti che la *cybersecurity* è tra gli interventi previsti nel PNRR). Ultimo intervento che si ritiene utile citare è l. n. 90 del 28 giugno 2024 (ex D.D.L. Cybersicurezza) [20], che pone al centro l'importanza della formazione: proprio l'assenza di formazione nei campi *ICT* e sicurezza informatica rappresenta uno dei punti sul quale si tornerà nel proseguo.

"La *ratio* comune alla recente normativa italiana ed alla Strategia Europea risiede nella volontà di fornire strumenti di contrasto più flessibili nel contrasto ad un fenomeno in continua evoluzione capace di adattarsi ai mutamenti sociali ed economici"[21].

3. Gli effetti dello sviluppo delle tecnologie sul settore turistico

Il turismo non poteva certo rimanere immune da digitalizzazione e piattaformizzazione: Internet e le piattaforme *eCommerce* hanno fatto il loro prepotente ingresso in tale ambito, innovandolo profondamente e modificandone le caratteristiche (sia dal lato della domanda che dell'offerta). Fra le innovazioni è possibile citare la nascita delle *Online Travel Agencies* (OTA), lo sviluppo degli *home restaurant* e delle piattaforme di *home exchange* e locazioni brevi, tutte realtà fiorite nell'ambito della *sharing economy*. Nel tempo, infatti, la pratica turistica è mutata e con essa è cambiata la domanda: oggi, il 67% delle persone che progetta un viaggio effettua una ricerca su internet, 2 viaggi su 3 vengono prenotati online, ma non

20 Per maggiori dettagli su interventi normativi e relative evoluzioni, si veda Paganelli 2021.

21 Mattarella 2022: p. 828.

solo, il turista 2.0 resta costantemente connesso anche durante la vacanza ed ama condividere le sue impressioni attraverso *feedback*, commenti e foto[22]. Tutto ciò è esploso in seguito alla pandemia: i dati elaborati dalla Commissione europea, infatti, testimoniano come nel 2019, gli italiani che prenotavano i viaggi online fossero solo il 39%, ma non solo: i servizi internet presso le destinazioni erano di qualità inferiore, così come il ricorso all'*e-commerce* era ben inferiore rispetto alla media europea[23].

> Il processo di digitalizzazione delle destinazioni turistiche richiede un ammodernamento strutturale e globale dell'impianto tecnologico e delle procedure in esso presenti. In particolare, il trattamento e la trasmissione delle informazioni diventano un punto nevralgico del settore dell'ospitalità che rende necessario un nuovo inquadramento concettuale degli spazi interessati all'accoglienza, dei flussi e all'offerta dei prodotti turistici.[24]

L'offerta turistica deve quindi mutare ed adeguarsi alle nuove caratteristiche del turista: nascono le possibilità di ´visitare´ la destinazione attraverso la realtà aumentata, di effettuare il *check-in* online o tramite i dispostivi mobili, nonché la diffusione di app dedicate a hotel.

La crescente proliferazione e diffusione dell'*ICT* nelle infrastrutture delle città ha incrementato l'interesse verso le *Smart Cities*, il cui fine ultimo è quello di migliorare la qualità dei servizi forniti ai cittadini e, di conseguenza, migliorare la loro qualità della vita[25]. Ma l'evoluzione turistica non si è fermata qui: ecco quindi che, dalle *smart cities*, si è giunti alle *smart destinations*, che non solo stanno rivoluzionando il concetto di offerta turistica, ma aprono nuove frontiere di studio e analisi. Alla luce di ciò, le *smart destinations* devono essere intese come un nuovo ecosistema[26], basato

> su uno spazio turistico innovativo e accessibile consolidato su un'infrastruttura tecnologica all'avanguardia che garantisce lo sviluppo sostenibile del territorio, le *smart*

22 Ecco come i consumatori hanno acquisito un ruolo attivo nella co-creazione delle proprie esperienze. In questo contesto, grazie alle tecnologie, si assiste, da un lato alla personalizzazione dei servizi turistici in base alle esigenze e alle preferenze dei singoli turisti e, dall'altro, l'utilizzo di informazioni in tempo reale per migliorare il processo decisionale. Per approfondimenti, Buhalis, Amaranggana, 2015.

23 "Tali considerazioni assumono una valenza assoluta per quanto attiene l'industria turistica in generale, in considerazione delle evoluzioni apportate al comparto dalle recenti dinamiche riconducibili a nuove tipologie di turismo (*smart/digital tourism*). Negli ultimi vent'anni si è assistito a un mutamento radicale nel settore del turismo, sia a livello quantitativo, con una crescita costante del numero di viaggiatori, sia qualitativo: il turista, grazie all'innovazione nel sistema dei trasporti e al consolidamento dei voli *low cost*, è sempre più globale; nella vacanza ricerca l'aspetto locale, la qualità dei servizi e l'autenticità delle esperienze, ma soprattutto è sempre più giovane e digitalmente interconnesso e fa ampio utilizzo delle tecnologie per l'organizzazione delle vacanze".

Cfr. Mariotti, Carrus, Panai, Martinez, Camerada 2018: 65.

24 Mariotti, Carrus, Panai, Martinez, Camerada 2018: 59.

25 Per approfondimenti, si veda Khatoun, Zeadally 2017.

26 Per approfondimenti, si consigliano Boes, Buhalis, Inversini 2016; Gretzel, Werthner, Koo, Lamsfus 2015

> *destination* facilitano l'interazione e l'integrazione dei turisti nell'ambiente e migliorano l'esperienza dei visitatori nonché la qualità della vita dei residenti.[27]

I territori, dunque, non possono trascurare il ruolo degli elementi intangibili che sottendono l'innovazione tecnologica e digitale. Ecco quindi, che le interconnessioni tra i diversi attori all'interno della *smart destination* si moltiplicano e, se questo da un lato provoca una maggiore integrazione del prodotto turistico, dal punto di vista strettamente informatico, ogni attore porta nuove vulnerabilità per l'intera catena e, a sua volta, per il prodotto *ICT* creato dalla catena stessa.

Lo sviluppo della tecnologia, quindi, non ha impattato unicamente su consumatori e operatori turistici, ma persino sulle destinazioni, incrementandone la competitività. L'innovazione tecnologica diviene un *driver* fondamentale della crescita dei territori: la *cybersecurity* diventa, quindi, non solo una condizione necessaria al fine di garantire i diritti dei turisti, ma soprattutto un elemento di distinzione rispetto ai propri *competitors*. Nonostante il turismo sia fortemente radicato sul territorio, molte destinazioni vengono precedentemente ´visitate´ virtualmente: ecco che la competizione è una partita giocata su un terreno non più solo fisico. I *driver* e le dinamiche competitive dei territori sono numerosi ma, per quanto riguarda lo scopo della presente trattazione, si ritiene di concentrarsi principalmente sul legame esistente tra *cybersecurity* e reputazione turistica. Quest'ultima va naturalmente intesa sia come reputazione territoriale, che come reputazione delle aziende che operano nella specifica filiera turistica. Come anticipato, infatti, il turista odierno vive costantemente connesso ed il fatto che le piattaforme digitali siano sempre più interattive, consentendo agli utenti di creare e pubblicare contenuti, permette alle imprese turistiche e alle destinazioni di beneficiare di un'attività di marketing personalizzato[28] rappresentata dall'*electronic word-of-mouth*, cioè una forma di comunicazione online che influisce fortemente sulle dinamiche di scelta e acquisto dei beni e servizi di una destinazione turistica e ne forgia la *web reputation*[29]. Proprio la necessità di tutelare quest'ultima, impone sia alla *governance* aziendale che a quella territoriale, di osservarla, analizzarla, interpretarla e monitorarla, facendo emergere il forte legame che intercorre tra competitività, progettazione della destinazione e *cybersecurity*.

> Tale nesso implica la necessità di contemplare, nel processo di progettazione territoriale turistica, interventi connessi all'implementazione di sistemi informatici sicuri di gestione delle *ICT*, in ogni singola azienda che opera nel comparto. Per poter procedere in tal senso è opportuno diffondere tra gli *stakeholders* un'adeguata cultura in termini di *cyber-igiene*, per permettere al territorio di acquisire un profilo turistico più competitivo.[30]

27 Cfr. Sustacha, Baños-Pino, Del Valle 2023: 1.

28 Per la definizione di marketing personalizzato, si rimanda a R. Moro Visconti 2020: 76.

29 Per approfondimenti, Sweeney, Soutar, Mazzarol 2008: 344-364.
A tal riguardo, appare d'uopo ricordare che la diffusione dei *social network* ha notevolmente potenziato la fruibilità delle informazioni, trasformandosi in uno strumento avanzato di marketing personalizzato e *digital branding*. Si veda Moro Visconti 2020.

30 Mariotti, Carrus, Panai, Martinez, Camerada 2018: 67.

Alla luce di ciò, quindi, domanda ed offerta concorrono alla creazione del valore, arricchendo sempre più l'esperienza turistica[31]: la fruizione della stessa è radicalmente mutata nel tempo, sia dal punto di vista di esperienza in loco sia da quello del prodotto, il cui livello di personalizzazione è in costante crescita[32].

Nonostante quanto sinora sostenuto sull'importanza della *cybersecurity*, il panorama attuale appare alquanto frammentato: sebbene vi sia una maggiore consapevolezza, anche da parte delle imprese, dell'importanza di dotarsi si sistemi di prevenzione, molto spesso tali soluzioni vengono considerate troppo complesse o dispendiose dalle PMI. Alcuni studi, infatti, evidenziano una complessità maggiore nel governo della tutela informatica nelle aziende turistiche di modeste dimensioni, caratterizzate da stagionalità e intermittenti gradi di intensità del lavoro[33].

Si è accennato poco fa, alla *web reputation* ed alla necessità di monitorarla: oltre agli attacchi informatici, infatti, appare d'uopo ricordare altresì un altro grande pericolo della rete, ossia la diffusione delle c.d. *fake news*. Esse possono essere definite come informazioni false, ingannevoli o distorte rese pubbliche, e possono arrivare a minare il corretto svolgimento della concorrenza sul mercato. Possono comportare una distruzione di valore potenzialmente assai rilevante, cui sempre non è facile porre rimedio.

> Ai danneggiati può soccorrere, in talune fattispecie, il diritto all'oblio con la rimozione dei link che rimandano al contenuto online ritenuto lesivo. La portata delle *fake news* è peraltro ben più ampia e spesso travalica la sfera individuale, orientando vaste schiere di cibernauti fino a ingannare l'opinione pubblica una *fake news* contro un concorrente o un prodotto può costituire un atto di concorrenza sleale. Una *fake news* nel sistema della comunicazione pubblicitaria può costituire un atto di pubblicità decettiva e aggressiva o una forma di pubblicità occulta.[34]

4. Conclusioni e sfide future

Nel presente contributo si è analizzato l'impatto delle nuove tecnologie nella vita di tutti i giorni, evidenziandone sia gli aspetti positivi che, soprattutto i pericoli insiti negli stessi. Oltre alle varie risposte tecnologiche, alla necessità di formazione in tali campi e di sensibilizzazione dei cittadini, al fine di ridurre il più possibile i rischi derivanti da tali pericoli, si sono ripercorse le diverse risposte date dal Legislatore europeo e quello italiano nel tempo. Partendo dalla direttiva NIS, vera e propria ´prima pietra´ per una politica di sicurezza informatica all'interno dell'UE, si sono ripercorsi i diversi strumenti normativi adottati, osservando come, negli anni, essi abbiano ampliato sempre più il proprio raggio d'azione. Dalla necessità di fornire un livello comune di sicurezza informatica in tutta Europa, si è passati

31 Si veda Ballina, Vald´es, Del Valle 2019.
32 Sul tema, si consiglia Shoval, Birenboim 2019.
33 Mariotti, Panai, Camerada 2018.
34 Moro Visconti 2020: 82.

alla *cybersecurity* della *supply chain* ed infine ad un atteggiamento proattivo nei confronti del rischio stesso. Da questi primi passi, quindi, la sicurezza informatica è entrata a far parte dell'ordine del giorno dei Legislatori nazionali[35].

Al fine di dare maggiore concretezza a tali osservazioni, si è deciso di tratteggiare gli effetti delle nuove tecnologie su uno dei settori più importanti per l'economia italiana: quello turistico. Senza ripercorrere quanto osservato fin qui, si può affermare che le nuove tecnologie abbiano dunque impattato profondamente su tale settore, migliorandone, da un lato l'esperienza, ma dall'altro lato creando anche dei potenziali effetti negativi (si pensi ad esempio ai rischi legati alla privacy, all'esclusione, al *digital devide* e persino all'alienazione e alla perdita di autenticità)[36]. Considerare entrambe le facce della medaglia è fondamentale per non sopravvalutare gli effetti della tecnologia nel settore turistico. È quindi fondamentale che, all'interno di tale ambito, i diversi attori della filiera comprendano l'effettiva portata dell'*IoT* – nonché i relativi pericoli – al fine di migliorare l'esperienza turistica stessa, aumentando così la soddisfazione dei visitatori e la loro fidelizzazione.

Alla luce di quanto illustrato, emerge come la *cybersecurity* sia un aspetto che riguarda sia il viaggiatore, che le imprese turistiche e i territori: viaggiatori e imprese possono vestire la duplice veste di bersaglio, e di complici involontari degli attacchi informatici. Essi possono infatti essere vettori degli attacchi e della diffusione di disinformazione, in quanto esposti, senza saperlo, a vulnerabilità dei propri dispositivi o vittime di *social engineering*. Ecco quindi spiegata l'importanza della cybersicurezza, ma, nonostante ciò, tale aspetto viene ancora sottovalutato dai principali *stakeholders*. Oggi, infatti, si registra una crescente asimmetria tra le conoscenze possedute dagli *hacker* e quelle necessarie per difendersene: ecco, dunque, che sarebbe fondamentale non solo sensibilizzare sul tema, al fine di costruire un'efficace *cyberresilienza*, ma puntare sulla formazione di esperti in tutti i settori economici. Tale considerazione, che potrebbe apparire scontata, in realtà non è così banale, in quanto, alla luce di un sondaggio mondiale, un terzo delle organizzazioni preferirebbe pagare il riscatto chiesto dagli *hacker*, piuttosto che investire nella sicurezza delle informazioni[37]. Al fine di rendere operativa la sicurezza informatica della *supply chain* (in qualsiasi settore economico) occorrerebbe, quindi, applicare i principi del *Cyber Supply Chain Risk Management*[38], che com-

35 Per ulteriori approfondimenti sul tema delle risposte nazionali, soprattutto in tema di *cybersecurity* nelle *supply chian* si consiglia Ludvigsen, Nagaraja, Daly 2022.

36 L'uso eccessivo della tecnologia potrebbe diminuire la qualità dell'esperienza di viaggio, creando barriere all'evasione, al divertimento e una ´momentanea assenza mentale´ quando i turisti interagiscono online. Oltre a ciò, sembra che l'uso costante dei dispositivi mobili, al fine di preservare i ricordi, possa in realtà impedire ai turisti di ricordare l'esperienza stessa. Ecco, dunque, che oggigiorno si sente parlare anche di *technostress* o stress tecnologico e quindi nasce il bisogno di una disintossicazione e disconnessione digitale. In tema si veda Sustacha, Baños-Pino, Del Valle 2023, ove presenti ulteriori riferimenti bibliografici.

37 NTT Security 2018.

38 Questa disciplina si concentra sui seguenti tre elementi: resilienza informatica; investimenti collaborativi in sicurezza informatica richiesti per raggiungere tale resilienza ed infine, utilizzo di standard riconosciuti. Per approfondimenti: Melnyk *et al.* 2022.

bina aspetti tipici della sicurezza informatica, della gestione dei rischi aziendali e della gestione della *supply chain*. In altre parole, quindi, si dovrebbero mettere in campo una serie di sforzi al fine di accrescere la propria *cyber resilience*: tale risultato è raggiungibile solo attraverso un approccio di *cybersecurity* più ampio, che comprenda una strategia di investimenti collaborativi nonché l'uso di standard armonizzati all'interno della filiera[39].

Si è affermato che, ad oggi, le PMI[40] – soprattutto quelle del comparto turistico con attività stagionali – fatichino ad implementare soluzioni adeguate a garantire la sicurezza delle informazioni: a parere di chi scrive, occorrerebbe riadattare e semplificare la normativa, tenendo conto delle specificità e delle esigenze delle PMI, cercando di fornire loro idonee linee guida sull'applicazione dei requisiti in materia di sicurezza delle informazioni e di privacy e sulla mitigazione dei rischi tecnologici. Non bisogna infatti sottovalutare il fatto che i piccoli potrebbero non avere le necessarie conoscenze o risorse per la sicurezza informatica, quindi, occorrerebbe fornire loro incentivi o comunque sensibilizzarli sull'importanza della *cybersecurity*. Solo attraverso un maggiore coinvolgimento delle PMI e degli strumenti costruiti *ad hoc* per le stesse, tali attori economici potranno finalmente sentirsi parte di una strategia comune e non interpretare la *cybersecurity* come una delle tante obbligazioni alle quali adempiere. Questa, infatti, non può essere una battaglia che i soggetti privati possono vincere da soli: la collaborazione tra pubblico e privato è fondamentale, sia per la condivisione delle informazioni che per lo scambio delle buone pratiche. "Uno scarso coordinamento porta alla frammentazione, alla duplicazione degli sforzi e a una dispersione di competenze. Un efficace coordinamento può avere come risultato successi tangibili, come la chiusura di alcuni mercati del *dark web*"[41].

Si è infine accennato alla diffusione delle *smart cities* ed alla conseguente evoluzione nelle *smart destinations* e, di come, l'irruzione della tecnologia in tali contesti possa comportare diversi problemi di sicurezza e privacy.

> L'evolversi della tecnologia nella gestione delle città e degli enti che le governano aumenta i rischi legati ad intrusioni, usi impropri e attacchi alla sicurezza cibernetica per i quali a livello internazionale e nazionale si sta consolidando una legislazione rivolta alla difesa delle funzioni essenziali dello Stato.[42]

39 Per ulteriori approfondimenti, van 't Schip 2024.

40 Il rapporto dell'Osservatorio *Cybersecurity & Data Protection* della *School of Management* del Politecnico di Milano evidenzia, per l'anno 2023, un incremento della spesa in *cybersecurity* da parte delle grandi organizzazioni, sottolineando che le piccole imprese, invece, non riescano ad effettuare investimenti concreti, a causa di risorse limitate e di difficoltà nel reperire sul mercato, soluzioni che soddisfino le loro specifiche esigenze.

41 Corte dei conti europea 2019: 41-42.

42 Paganelli 2021: 681. L'autore sottolinea come, "la sola esistenza di telecamere che monitorano il territorio richiede una strategia di progettazione che definisca i confini dell'area urbana e ne permetta il presidio. […] questo sistema si è grandemente diffuso ed assicura una copertura abbastanza sistematica dei centri cittadini attraverso il controllo degli accessi, ma origina al contempo una quantità enorme di informazioni da trattare e archiviare. Se a questo aggiungiamo

Anche in questo caso, la normativa dovrebbe essere adattata alle nuove caratteristiche dei territori. Si ricorda infatti che, lo sviluppo delle nuove tecnologie ha determinato una profonda trasformazione nelle modalità di progettazione e governo degli stessi, incrementandone il livello di competizione, rendendo possibili persino le visite virtuali che fino a qualche anno fa erano impensabili.

Alla luce di tale osservazione, in un ambiente sempre più mediato dalla tecnologia, la mancanza di *compliance* nei requisiti di sicurezza e privacy in una destinazione può avere un impatto significativo sulla disponibilità dei turisti[43]: ecco quindi che tale requisito diventa fondamentale per mantenere una reputazione positiva nonché la propria quota di mercato. Non bisogna infatti dimenticare che, grazie alle nuove tecnologie, le *smart destinations* e gli operatori della filiera turistica riescono ad acquisire ed immagazzinare moltissimi dati dei turisti (cosa che, in passato non era neanche immaginabile).

Bibliografia

ACN 2024, *Relazione annuale al Parlamento 2023*.

Assintel 2024, *Cyber Report 2023*.

Ballina F. J., Vald´es L., Del Valle E. 2019, "The Phygital experience in the smart tourism destination", in *International Journal of Tourism Cities,* 5(4).

Boes, K., Buhalis D., Inversini, A. 2015, "Smart tourism destinations: Ecosystems for tourism destination competitiveness" in *International Journal of Tourism Cities,* 2(2).

Buhalis, D., Amaranggana, A. 2015, "Smart tourism destinations enhancing tourism experience through personalisation of services", in Tussyadiah,I., Inversini A. (Eds.), *Information and communication technologies in tourism 2015*, Springer.

Cencetti C. 2014, *Cybersecurity: Unione europea e Italia Prospettive a confronto*, Quaderni IAI, Roma: Edizioni Nuova Cultura.

Chiara p. G. 2022, "The IoT and the New EU Cybersecurity Regulatory Landscape", in *International Review of Law, Computers & Technology*, 1.

Chiara p. G. 2023, "Il Cyber Resilience Act: la proposta di regolamento della Commissione europea relativa a misure orizzontali di cybersicurezza per prodotti con elementi digitali", in *Rivista Italiana di Informatica e Diritto*, fasc. 1.

Corte dei conti europea 2019, *Le sfide insite in un'efficace politica dell'UE in materia di cibersicurezza. Documento di riflessione*.

European Union Agency for Cybersecurity (ENISA) 2023, *ENISA Threat Landscape 2023 (July 2022 to June 2023)*.

Greenberg G. 2017, "Hold North Korea Accountable For Wannacry—and the NSA, too", in *WIRED*.

Gretzel U., Werthner H., Koo C., Lamsfus C. 2015, "Conceptual foundations for understanding smart tourism ecosystems", in *Computers in Human Behavior,* 50.

le telecamere di enti pubblici e privati installate per motivi di sicurezza o funzionali alle attività svolte, allora la copertura è ancora più ampia e nel tempo questo sistema si integrerà in qualche modo, consentendo il passaggio delle informazioni da una rete di sorveglianza all'altra". A ciò si aggiungono altresì le prospettive del c.d. *city sensing*.

43 Per approfondimenti, Jeong, Shin 2020.

Golisano L. 2022, "Il governo del digitale: strutture di governo e innovazione digitale", in *Giornale di diritto amministrativo*, n. 6.
Jeong M., Shin, H. 2020, "Tourists' experiences with smart tourism technology at smart destinations and their behavior intentions", in *Journal of Travel Research, 59*(8).
Khatoun R., Zeadally S. 2017, "Cybersecurity and Privacy Solutions in Smart Cities", in *IEEE Communications Magazine*.
Ludvigsen K. R., Nagaraja S., Daly A. 2022, "Preventing or Mitigating Adversarial Supply Chain Attacks: A Legal Analysis", in *Proceedings of the 2022 ACM Workshop on Software Supply Chain Offensive Research and Ecosystem Defenses*.
Mariotti G., Carrus S., Panai E., Martinez V., Camerada M. V. 2018, "Smart destinations e competitività in ambito turistico. Il ruolo della cyber security", in *AGEI – Geotema*, Supplemento.
Mariotti G., Panai E., Camerada M. V. 2018, "Piattaforma per la sicurezza informatica per il comparto turistico: dalla prospettiva nazionale all'azione reale. Focus sulle strutture ricettive", in *AGEI – Geotema*, Supplemento.
Mattarella A. 2022, "Il cybercrime nell'ordinamento italiano e le nuove prospettive dell'Unione Europea e delle Nazioni Unite", in *Diritto penale e processo*, n. 6.
Melnyk S. A., Schoenherr T., Speier-Pero C., Peters C., Chang J. F., Friday D. 2022, "New Challenges in Supply Chain Management: Cybersecurity across the Supply Chain", in *International Journal of Production Research*, 60(4).
Moro Visconti R. 2020*,* "La valutazione dei social network", in *Il Diritto industriale*, n. 1.
NTT Security 2018, *Risk:Value 2018 Report*.
Paganelli G. 2021, "Perimetri di controllo e sicurezza cibernetica. Una verifica indispensabile", in *Azienditalia*, n. 4.
Shoval N., Birenboim, A. 2019, "Customization and augmentation of experiences through mobile technologies: A paradigm shift in the analysis of destination competitiveness", in *Tourism Economics,* 25(5).
Sievers T. 2021, "Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligations", in *Int. Cybersecur. Law Rev.*, 2.
Sustacha I., Baños-Pino J. F., Del Valle E. 2023, "The role of technology in enhancing the tourism experience in smart destinations: A meta-analysis", in *Journal of Destination Marketing & Management*, 30.
Sweeney J. C., Soutar G. N., Mazzarol T. 2008, "Factors Influencing Word of Mouth Effectiveness: Receiver Perspectives*",* in *European Journal of Marketing*, 42.
van 't Schip M. 2024, "The Regulation of Supply Chain Cybersecurity in the NIS2 Directive in the Context of the Internet of Things", in *European Journal of Law and Technology*, Vol. 15, No. 1.
Vandezande N. 2024, "Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor", in *Computer Law & Security Review*, 52.