La privacy non va in vacanza: cosa insegnano i furti di dati in hotel

L'estate 2025 ha acceso una luce sull'importanza della privacy e della cybersecurity nel settore alberghiero, dopo i casi di furti di documenti: ecco la situazione e cosa dice la legge
(Fonte: **https://www.agendadigitale.eu/** 30 settembre 2025)

L'estate 2025 resterà impressa come un campanello d'allarme per il settore alberghiero italiano. Nel mese di agosto, in piena stagione turistica, un gruppo di criminali informatici è riuscito a sottrarre migliaia di copie digitali di documenti d'identità custoditi da diverse strutture ricettive. Quelle stesse immagini, che gli ospiti consegnano con fiducia al momento del check-in, sono finite in vendita nei meandri del dark web, offerte come merce rara a chi vive di frodi identitarie e truffe finanziarie.
La notizia, diffusa dalle prime segnalazioni del CERT-AgID e poi confermata dal Garante per la protezione dei dati personali, ha aperto un'istruttoria tuttora in corso. È stato lo stesso Garante ad annunciare che l'indagine non si limiterà a verificare i tempi di notifica della violazione, ma si concentrerà soprattutto sulle misure tecniche e organizzative che gli hotel avrebbero dovuto adottare per proteggere informazioni così delicate.

Indice degli argomenti

Il caso

La vicenda rappresenta un caso da manuale su come la gestione dei dati personali possa diventare il punto debole di un intero comparto economico. Le strutture alberghiere sono obbligate per legge a identificare i propri ospiti e a comunicare alcuni dati alle autorità di pubblica sicurezza (art. 109 TULPS). Fin qui nulla di illegittimo. Tuttavia, **la prassi di fotocopiare o scansionare integralmente i documenti e conservarne copie per mesi o addirittura anni è spesso frutto di abitudine più che di necessità normativa**. È proprio questo eccesso di zelo – in realtà un difetto organizzativo – che ha spalancato la porta all'attacco informatico. I criminali non hanno dovuto inventare nulla di nuovo: è bastato penetrare sistemi debolmente protetti, trovare cartelle condivise o archivi gestionali poco aggiornati e copiare immagini di passaporti e carte d'identità che non avrebbero dovuto trovarsi lì, in quel formato, così a lungo.

Cosa dice il Gdpr

Sul piano normativo, il quadro è chiaro. **Il GDPR, all'articolo 5, stabilisce principi cardine come la minimizzazione dei dati e la limitazione della conservazione**: significa che si possono trattare soltanto le informazioni strettamente necessarie e per un periodo proporzionato alla finalità. L'articolo 32 obbliga inoltre i titolari del trattamento ad adottare misure di sicurezza adeguate al rischio. Ora, se il dato trattato è una scansione di un documento d'identità – materiale che consente di aprire conti bancari, contrarre abbonamenti o mettere in atto frodi sofisticate – il livello di protezione richiesto non può essere quello di un archivio qualunque. **È qui che l'istruttoria del Garante promette di incidere**: un hotel non può limitarsi a dire "abbiamo un antivirus" o "abbiamo la password al gestionale", ma deve dimostrare di aver costruito un sistema coerente di difese, aggiornato e proporzionato al rischio.

Furto di documenti in hotel, come avviene

Per comprendere come l'attacco sia stato possibile bisogna guardare alla realtà quotidiana di molte reception. I sistemi informatici del settore alberghiero spesso convivono **con tecnologie obsolete**, patch di sicurezza installate in ritardo, password generiche condivise tra più operatori e reti interne poco segmentate. In molti casi la stessa rete ospiti, quella a cui i clienti si collegano con lo smartphone, dialoga senza barriere significative con i server che custodiscono i dati amministrativi. A questo si aggiungono pratiche di comodo: la scansione del documento salvata sul desktop per agevolare la registrazione, la cartella "documenti clienti" accessibile da più postazioni, le sessioni del gestionale lasciate aperte al cambio turno. In un simile scenario, l'attaccante non ha bisogno di tecniche raffinatissime: basta sfruttare una credenziale debole, un accesso remoto non protetto, o un malware piazzato su una postazione per avere in breve tempo accesso a centinaia di documenti.

Il danno che deriva da una simile fuga di dati **è ben più grave di quello legato ad altri tipi di violazioni**. A differenza di una password, che si può cambiare, un documento d'identità non può essere sostituito con la stessa facilità. Una volta che la copia digitale di una carta o di un passaporto finisce in mano a criminali organizzati, il titolare di quel documento rischia per anni di vedersi intestati contratti telefonici, richieste di credito, acquisti online fraudolenti. È un danno che si traduce in perdita di tempo, costi legali, complicazioni burocratiche, ma anche in un impatto psicologico significativo per chi scopre di non avere più il controllo della propria identità.

Come difendersi

Dal punto di vista **delle contromisure**, la prima lezione è evidente: raccogliere meno dati significa ridurre la superficie d'attacco. Se per adempiere agli obblighi di legge basta registrare alcune informazioni anagrafiche, conservare una copia digitale del documento è una scelta rischiosa e difficilmente giustificabile. L'albergatore deve imparare a distinguere tra ciò che è richiesto per legge e ciò che viene fatto per consuetudine, perché nel secondo caso è molto più difficile

dimostrare la legittimità del trattamento. Dove **la scansione è ritenuta indispensabile**, deve comunque avere una vita brevissima e deve essere custodita con criteri stringenti: cifratura immediata, accesso ristretto a pochi soggetti autorizzati, cancellazione automatica dopo pochi giorni. Non ci si può affidare al promemoria dell'operatore, ma a sistemi progettati per distruggere il dato al termine della sua utilità.
Altrettanto cruciale **è la sicurezza delle infrastrutture**. In un hotel moderno non è accettabile che la rete dei clienti e quella amministrativa condividano le stesse risorse. Serve un isolamento rigoroso delle reti, firewall interni che impediscano movimenti laterali, autenticazioni a più fattori per ogni accesso remoto e aggiornamenti costanti dei sistemi. Anche il rapporto con i fornitori di software deve cambiare: non si tratta solo di acquistare un gestionale, ma di pretendere clausole contrattuali che impongano patch di sicurezza tempestive, log dettagliati e audit di terza parte. La responsabilità dell'hotel non si esaurisce nello scaricare colpe sul fornitore: il GDPR parla chiaramente di corresponsabilità e di obblighi di controllo.

L'importanza dell'incident response
Un ulteriore elemento che la vicenda mette in luce è la mancanza di capacità di rilevare e rispondere agli incidenti. Molte strutture hanno scoperto la violazione solo leggendo notizie sul web o i comunicati delle Autorità. **Questo significa che i sistemi non erano monitorati**, i log non erano centralizzati, e nessuno aveva predisposto procedure di allerta in caso di comportamenti anomali. Una politica di sicurezza matura prevede invece di raccogliere e analizzare i log di accesso, di impostare regole di allarme in caso di trasferimenti sospetti di grandi quantità di dati e di effettuare test regolari di ripristino. Non è necessario spendere molto: esistono servizi gestiti che abilitano anche le piccole organizzazioni alla rilevazione e alla gestione tempestiva degli incidenti.

Le soluzioni sul mercato
Sono disponibili **soluzioni software che acquisiscono i documenti d'identità degli ospiti**, li archiviano in repository sicuri e cifrati, consentendo di impostare politiche di conservazione *(data retention*) e rendendo gli archivi accessibili tramite autenticazione a più fattori (MFA), e, in parallelo, popolano il gestionale alberghiero (PMS), così da adempiere alle finalità di legge e velocizzare il check-in in totale sicurezza.
Per fare un breve riassunto le misure tecniche-organizzative da adottare potrebbero essere le seguenti:

- Raccogliere **solo i dati personali necessari** a formalizzare il check-in e restituire subito il documento all'ospite (niente copie).
- Archiviare in modo cifrato (PMS o repository sicuro) e **vietati salvataggi locali** su PC/USB.
- **Accessi con MFA e ruoli a minimo privilegio**; account nominali, niente condivisioni.

- Data Retention chiara (es. fino all'invio su portale Alloggiati/chiusura soggiorno) con cancellazione automatica.
- Trasmissione sicura (solo HTTPS/TLS); vietata email non cifrata con allegati di documenti.
- Backup cifrati e test di ripristino periodici.
- Log degli accessi (chi vede/esporta/cancella) e controlli a campione.
- Procedure **data breach**: referente, modulo interno, valutazione e notifica entro 72h.
- Fornitori **sotto contratto** (art. 28): PMS/scanner con cifratura, MFA, retention e data center UE.
- Persone e postazioni: informativa al desk, istruzioni e procedure al personale, formazione annuale;

Guardando al futuro, **il caso di agosto deve spingere il settore alberghiero a un cambio di mentalità**. La protezione dei dati non è un optional, né un semplice adempimento burocratico, ma un elemento di fiducia verso il cliente. Un ospite che consegna il proprio documento al check-in ha diritto di sapere come sarà trattato, per quanto tempo e con quali garanzie. Gli albergatori più attenti non dovrebbero temere queste domande, ma anzi farne un punto di forza, spiegando con chiarezza che i dati vengono raccolti al minimo necessario e custoditi con misure di sicurezza concrete. Un'informativa trasparente e un comportamento coerente valgono più di mille campagne promozionali, perché la fiducia è il capitale più prezioso in un mercato competitivo.

Le responsabilità

Infine, è bene ricordare che la normativa non lascia spazio a zone grigie. L'articolo 33 del GDPR impone la notifica al Garante entro settantadue ore, l'articolo 34 prevede la comunicazione agli interessati in caso di rischio elevato per i loro diritti, e l'articolo 25 richiama **il principio di privacy by design e by default**, cioè la necessità di progettare i sistemi fin dall'inizio con la protezione dei dati come criterio centrale. La violazione di questi obblighi può comportare non solo sanzioni pecuniarie rilevanti, ma anche un danno reputazionale difficilmente rimediabile.

Il furto di documenti d'identità avvenuto negli hotel italiani non è stato un evento eccezionale, ma la conseguenza naturale di pratiche deboli e di una sottovalutazione del rischio. È la prova che il settore ricettivo deve uscire dall'illusione che "tanto non siamo una banca" e comprendere che la posta in gioco è la stessa: i dati personali sono la moneta **più preziosa della nostra epoca**, e chi li custodisce ha il dovere di difenderli con ogni mezzo. Solo così gli hotel potranno garantire non solo un soggiorno confortevole, ma anche un'esperienza sicura e rispettosa della dignità digitale di ogni ospite.