



«Τραπεζική, Χρηματοοικονομική & Χρηματοοικονομική
Τεχνολογία (FinTech)»

Διπλωματική Εργασία

«Το πρόβλημα της εξακρίβωσης στοιχείων των
πελατών στις μεγάλες επιχειρήσεις στη Μύκονο -
Μελέτη περίπτωσης των μεγάλων ξενοδοχειακών
μονάδων της Μυκόνου»

Παναγιώτης Βασίλειος Πατσαρούχας

Επιβλέπων καθηγητής: Ηρειώτης Νικόλαος

Β' Επιβλέπων καθηγητής: Βασιλείου Δημήτριος

Αθήνα, Φεβρουάριος 2026

*Πατσαρούχας Παναγιώτης Βασίλειος, «Το πρόβλημα της εξακρίβωσης
στοιχείων των πελατών στις μεγάλες επιχειρήσεις στη Μύκονο - Μελέτη περίπτωσης των
μεγάλων ξενοδοχειακών μονάδων της Μυκόνου»*

Η παρούσα εργασία αποτελεί πνευματική ιδιοκτησία του φοιτητή (Πατσαρούχα Παναγιώτη Βασιλείου) που την εκπόνησε. Στο πλαίσιο της πολιτικής ανοικτής πρόσβασης ο συγγραφέας/δημιουργός εκχωρεί στο ΕΑΠ, μη αποκλειστική άδεια χρήσης του δικαιώματος αναπαραγωγής, προσαρμογής, δημόσιου δανεισμού, παρουσίασης στο κοινό και ψηφιακής διάχυσής τους διεθνώς, σε ηλεκτρονική μορφή και σε οποιοδήποτε μέσο, για διδακτικούς και ερευνητικούς σκοπούς, άνευ ανταλλάγματος και για όλο το χρόνο διάρκειας των δικαιωμάτων πνευματικής ιδιοκτησίας. Η ανοικτή πρόσβαση στο πλήρες κείμενο για μελέτη και ανάγνωση δεν σημαίνει καθ' οιονδήποτε τρόπο παραχώρηση δικαιωμάτων διανοητικής ιδιοκτησίας του συγγραφέα/δημιουργού ούτε επιτρέπει την αναπαραγωγή, αναδημοσίευση, αντιγραφή, αποθήκευση, πώληση, εμπορική χρήση, μετάδοση, διανομή, έκδοση, εκτέλεση, «μεταφόρτωση» (downloading), «ανάρτηση» (uploading), μετάφραση, τροποποίηση με οποιονδήποτε τρόπο, τμηματικά ή περιληπτικά της εργασίας, χωρίς τη ρητή προηγούμενη έγγραφη συναίνεση του συγγραφέα/δημιουργού. Ο συγγραφέας/δημιουργός διατηρεί το σύνολο των ηθικών και περιουσιακών του δικαιωμάτων.

στοιχείων των πελατών στις μεγάλες επιχειρήσεις στη Μύκονο - Μελέτη περίπτωσης των μεγάλων ξενοδοχειακών μονάδων της Μυκόνου»

Περίληψη

Η επαλήθευση των στοιχείων των πελατών σε μεγάλα ξενοδοχεία αποτελεί μια κρίσιμη λειτουργική, νομική και στρατηγική πρόκληση στο σύγχρονο τουριστικό περιβάλλον. Οι αυξημένες απειλές για την ασφάλεια, οι υποχρεώσεις συμμόρφωσης με τους κανονισμούς και οι αυξανόμενες προσδοκίες των επισκεπτών για απρόσκοπτη και γρήγορη εξυπηρέτηση έχουν αποκαλύψει δομικές αδυναμίες στις παραδοσιακές πρακτικές ταυτοποίησης, όπως η χειροκίνητη επιθεώρηση των εγγράφων ταυτότητας και ο έλεγχος πρόσβασης με κάρτες-κλειδιά. Σε μεγάλης κλίμακας ξενοδοχειακές εγκαταστάσεις, όπου η εναλλαγή των πελατών είναι υψηλή και τα σημεία πρόσβασης πολλαπλά, οι επαναλαμβανόμενες διαδικασίες ελέγχου ταυτότητας μπορεί να δημιουργήσουν εμπόδια στην εξυπηρέτηση, λειτουργικές ανεπάρκειες και ευπάθειες που σχετίζονται με απάτη και ψευδείς πληροφορίες πελατών. Η μελέτη αυτή είχε ως στόχο να εξετάσει τις πρακτικές επαλήθευσης και διαχείρισης των δεδομένων πελατών που εφαρμόζουν οι ξενοδοχειακές επιχειρήσεις στη Μύκονο, εστιάζοντας στο επίπεδο τυποποίησης, τεχνολογικής ενσωμάτωσης και μηχανισμών εσωτερικού ελέγχου. Τα ευρήματα αποκαλύπτουν ότι, ενώ η βασική ταυτοποίηση μέσω δελτίων ταυτότητας ή διαβατηρίων εφαρμόζεται σχεδόν καθολικά, οι συμπληρωματικές πρακτικές επαλήθευσης και οι δομημένες πολιτικές «Γνωρίστε τον πελάτη σας» (KYC) εφαρμόζονται με ασυνέπεια. Είναι σημαντικό να σημειωθεί ότι 15 από τα 20 ξενοδοχεία ανέφεραν προηγούμενα περιστατικά που αφορούσαν ψευδείς πληροφορίες πελατών, υπογραμμίζοντας την πρακτική σημασία του ζητήματος. Η περιορισμένη υιοθέτηση εργαλείων ανίχνευσης απάτης και η συχνή αντιμετώπιση περιστατικών κατά περίπτωση υπογραμμίζουν περαιτέρω τα κενά στην τυποποίηση των διαδικασιών. Η ενίσχυση των κανονιστικών κατευθυντήριων γραμμών, η τυποποίηση των εσωτερικών πρωτοκόλλων και η ενσωμάτωση προηγμένων ψηφιακών και βιομετρικών τεχνολογιών επαλήθευσης ταυτότητας είναι απαραίτητες για τη βελτίωση της ασφάλειας, της λειτουργικής αποτελεσματικότητας και της εμπιστοσύνης των πελατών.

Λέξεις κλειδιά

Επαλήθευση ταυτότητας, ξενοδοχεία, ασφάλεια στον τουρισμό, βιομετρική τεχνολογία.

Abstract

Verifying guest information in large hotels is a critical operational, legal, and strategic challenge in today's tourism environment. Increased security threats, regulatory compliance obligations, and rising guest expectations for seamless and fast service have exposed structural weaknesses in traditional identification practices, such as manual inspection of identity documents and key card access control. In large-scale hotel facilities, where customer turnover is high and access points are numerous, repetitive identity verification procedures can create service barriers, operational inefficiencies, and vulnerabilities related to fraud and false customer information. This study aimed to examine the customer data verification and management practices implemented by hotel businesses in Mykonos, focusing on the level of standardization, technological integration, and internal control mechanisms. The findings reveal that while basic identification through ID cards or passports is almost universally applied, supplementary verification practices and structured "Know Your Customer" (KYC) policies are applied inconsistently. It is important to note that 15 of the 20 hotels reported previous incidents involving false customer information, underscoring the practical significance of the issue. The limited adoption of fraud detection tools and the frequent handling of incidents on a case-by-case basis further highlight gaps in the standardization of procedures. Strengthening regulatory guidelines, standardization of internal protocols, and integration of advanced digital and biometric identity verification technologies are essential to improve security, operational efficiency, and customer trust.

Keywords

Identity verification, hotels, tourism security, biometric technology.

ΚΑΤΑΛΟΓΟΣ ΠΕΡΙΕΧΜΕΝΩΝ

Abstract.....	5
1. Εισαγωγή.....	9
1.1. Σύντομη παρουσίαση του θέματος και της σημασίας του στο σύγχρονο τουριστικό περιβάλλον.....	9
1.2. Παρουσίαση λέξεων-κλειδιών.....	11
1.3. Σκοπός και στόχοι της εργασίας.....	12
1.4. Δομή και μεθοδολογική προσέγγιση.....	13
2. Θεωρητική και Βιβλιογραφική Προσέγγιση του Προβλήματος.....	15
2.1. Διαχείριση ταυτότητας και πρόσβασης (IAM).....	15
2.2. Blockchain για τη διαχείριση της ψηφιακής ταυτότητας των επισκεπτών.....	19
2.3. Αυτοματοποιημένη ψηφιακή επαλήθευση ταυτότητας.....	23
2.4. Βιομετρική τεχνολογία.....	25
2.4.1. Αναγνώριση προσώπου.....	27
2.4.2. Συστήματα αναγνώρισης δακτυλικών αποτυπωμάτων.....	31
2.4.3. Αναγνώριση ίριδας.....	32
2.4.4. Αναγνώριση φωνής.....	33
2.4.5. Αναγνώριση φλεβών παλάμης.....	34
2.4.6. Συστήματα αναγνώρισης βάδισης.....	35
2.5. Οφέλη της βιομετρικής τεχνολογίας στον τομέα του τουρισμού και της φιλοξενίας 37	
2.5.1. Προκλήσεις χρήσης βιομετρικών δεδομένων.....	40
2.5.2. Επιπτώσεις της χρήσης της βιομετρικής τεχνολογίας.....	42
2.6. Επαλήθευση ταυτότητας στον τομέα της φιλοξενίας.....	43
3. Μεθοδολογία.....	49

στοιχείων των πελατών στις μεγάλες επιχειρήσεις στη Μύκονο - Μελέτη περίπτωσης των
μεγάλων ξενοδοχειακών μονάδων της Μυκόνου»

3.1.	Σκοπός και Ερευνητικά Ερωτήματα	49
3.2.	Ερευνητικός Σχεδιασμός.....	50
3.3.	Πληθυσμός και Δείγμα	50
3.4.	Ερευνητικό Εργαλείο	51
3.5.	Διαδικασία Συλλογής Δεδομένων.....	52
3.6.	Στατιστική Ανάλυση	52
3.7.	Ηθικά Ζητήματα	53
3.8.	Περιορισμοί της Έρευνας	53
4.	Αποτελέσματα.....	54
	Συμπεράσματα	66
	Βιβλιογραφία	69
	Παράρτημα.....	79

*Πατσαρούχας Παναγιώτης Βασίλειος, «Το πρόβλημα της εξακρίβωσης
στοιχείων των πελατών στις μεγάλες επιχειρήσεις στη Μύκονο - Μελέτη περίπτωσης των
μεγάλων ξενοδοχειακών μονάδων της Μυκόνου»*

1. Εισαγωγή

1.1. Σύντομη παρουσίαση του θέματος και της σημασίας του στο σύγχρονο τουριστικό περιβάλλον

Η τεχνολογία, που έχει γίνει το δεύτερο μυαλό των ανθρώπων, εξελίσσεται με ταχείς ρυθμούς και διαδραματίζει καθοριστικό ρόλο στη διαμόρφωση και τη βελτίωση διαφόρων πτυχών της εμπειρίας των πελατών και της λειτουργικής αποδοτικότητας. Η τεχνολογία αναπτύσσεται λόγω της παγκοσμιοποίησης και έχει αναδειχθεί σε κυρίαρχη δύναμη στη διαμόρφωση διαφόρων πτυχών της παγκόσμιας κοινωνίας μας (Selian & McKnight, 2017). Έχει συγκεκριμένα φέρει επανάσταση στις επιχειρήσεις σε όλο τον κόσμο και αποτελεί τον ακρογωνιαίο λίθο της προόδου, προωθώντας την καινοτομία, την αποδοτικότητα και τη συνδεσιμότητα σε όλους τους τομείς της κοινωνίας (Brynjolfsson & McAfee, 2012).

Η ταυτότητα στον τομέα της φιλοξενίας δεν είναι αυτή που ήταν παλιά. Για μερικούς ανθρώπους, η ταυτότητα είναι απλά ένα διαβατήριο, ίσως μια άδεια οδήγησης. Για άλλους, η ταυτότητα μπορεί να περιλαμβάνει επίσης μια κάρτα πιστότητας ή μια κάρτα πρόσβασης. Για πολλούς, πρόκειται για ένα όνομα χρήστη και έναν κωδικό πρόσβασης για να έχουν πρόσβαση σε κάποιον ιστότοπο ή ακόμα και μια διεύθυνση ηλεκτρονικού ταχυδρομείου. Η αλήθεια είναι ότι η ταυτότητα είναι όλα αυτά. Αυτά είναι απλά παραδείγματα συγκεκριμένων πτυχών της ταυτότητάς μας στον τομέα της φιλοξενίας. Η διαχείριση της ταυτότητας των επισκεπτών αποτελεί σημαντικό βάρος για τους ξενοδόχους στον κλάδο της φιλοξενίας (Βασιλείου, & Ηρειώτης, 2008). Πρώτον, οι ξενοδόχοι πρέπει να καθιερώσουν διαδικασίες και συστήματα επαλήθευσης για να επιβεβαιώσουν την ταυτότητα των επισκεπτών, κάτι που μπορεί να περιλαμβάνει την αίτηση εγγράφων ταυτοποίησης, όπως διαβατήρια ή άδειες οδήγησης, και τη διασταύρωσή τους με τα στοιχεία της κράτησης. Δεύτερον, η επαλήθευση των επισκεπτών προσθέτει πολυπλοκότητα και τριβές στη διαδικασία του check-in, οδηγώντας σε μεγαλύτερους χρόνους αναμονής, δυσαρέσκεια των επισκεπτών και, τελικά, χαμηλότερα έσοδα ανά διαθέσιμο δωμάτιο. Το προσωπικό πρέπει να επικεντρώνεται σε αλληλεπιδράσεις

υψηλής αξίας με τους επισκέπτες, οι οποίες προσθέτουν στην κορυφαία γραμμή του ξενοδοχείου, αντί να πληκτρολογεί αριθμούς πίσω από ένα γραφείο (Bilgihan et al., 2013).

Ένα από τα προβλήματα στη διαχείριση της ταυτότητας στον τομέα της φιλοξενίας είναι όλα τα ανακριβή δεδομένα που κυκλοφορούν στις βάσεις δεδομένων των ξενοδοχείων, τα οποία απλώς πληκτρολογήθηκαν λανθασμένα και δημιουργούν επιπλέον έξοδα και μπορούν να καταστήσουν τις ιδιοκτησίες μη συμμορφούμενες με την εθνική νομοθεσία. Ωστόσο, το μεγαλύτερο πρόβλημα είναι ότι οι ιδιοκτησίες αποθηκεύουν πάρα πολλές προσωπικές πληροφορίες και θα είναι υπεύθυνες για τυχόν παραβιάσεις (Martínez et al., 2013).

Η τεχνολογία χρησιμοποιείται σε πολλούς κλάδους, όπως η εκπαίδευση, οι μεταφορές, η μεταποίηση, η ψυχαγωγία, ο τουρισμός και η φιλοξενία. Ο τουρισμός και η φιλοξενία είναι ένας κρίσιμος κλάδος που μπορεί να επωφεληθεί από την τεχνολογία. Η τεχνολογία διαδραματίζει κρίσιμο ρόλο στον κλάδο του τουρισμού και της φιλοξενίας, βελτιώνοντας διάφορες πτυχές της εμπειρίας των πελατών, της λειτουργικής αποδοτικότητας, του μάρκετινγκ και της διαχείρισης (Καρακούδα, 2014). Ορισμένες μορφές τεχνολογίας περιλαμβάνουν τις πλατφόρμες online κρατήσεων, τα συστήματα διαχείρισης ακινήτων (PMS), τα συστήματα διαχείρισης πελατειακών σχέσεων (CRM), τα κλειστά κυκλώματα τηλεόρασης (CCTV), τα συστήματα αναγνώρισης ομιλίας (SRS) και την τεχνητή νοημοσύνη (AI). Μια σημαντική τεχνολογία που εφαρμόζεται στον κλάδο του τουρισμού και της φιλοξενίας είναι η βιομετρική τεχνολογία. Στο πλαίσιο του κλάδου του τουρισμού και της φιλοξενίας, η βιομετρική τεχνολογία διαδραματίζει σημαντικό ρόλο στη βελτίωση της ασφάλειας, στην απλοποίηση των διαδικασιών και στην εξατομίκευση των εμπειριών για τους επισκέπτες και τους φιλοξενούμενους. Η βιομετρική τεχνολογία επιτρέπει την ταυτοποίηση και την επαλήθευση της ταυτότητας των ατόμων με βάση τα βιολογικά ή συμπεριφορικά χαρακτηριστικά τους. Ωστόσο, η εφαρμογή βιομετρικών τεχνολογιών σε τουριστικές και ξενοδοχειακές εγκαταστάσεις αντιμετωπίζει εμπόδια (Bilgihan et al., 2013).

Σύμφωνα με την Έρευνα Διαχείρισης Ταυτότητας του 2004 (Electronic Data System, 2005), οι καταναλωτές επιθυμούν οι μέθοδοι ταυτοποίησης να είναι εξίσου ασφαλείς και βολικές, ενώ πλέον είναι πιο ανοιχτοί σε εναλλακτικές μεθόδους επαλήθευσης της ταυτότητας. Η έρευνα μέτρησε επίσης το ενδιαφέρον των καταναλωτών για καινοτόμες μεθόδους επαλήθευσης της ταυτότητας, όπως η βιομετρία. Η βιομετρία είναι η αυτοματοποιημένη χρήση

φυσιολογικών ή συμπεριφορικών χαρακτηριστικών, όπως τα δακτυλικά αποτυπώματα, για τον προσδιορισμό ή την επαλήθευση της ταυτότητας (Nanavati, 2004).

Σύμφωνα με τα αποτελέσματα της έρευνας, περισσότερο από το 69% ήταν ανοιχτό στην ιδέα της χρήσης βιομετρικών στοιχείων για τη διαχείριση ταυτότητας. Μόνο το 12% απέρριψε τη χρήση βιομετρικών στοιχείων, ενώ το 19% ήταν αβέβαιο (Electronic Data System Corporation, 2005). Η έρευνα αυτή εξέτασε το ζήτημα ότι οι πελάτες ξενοδοχείων που αποκαλύπτουν σημαντικές προσωπικές πληροφορίες και απαιτούν υψηλό επίπεδο ασφάλειας θα πρέπει να εκτιμούν σαφώς αυτή τη νέα τεχνολογία. Οι ειδικοί στον τομέα της φιλοξενίας προβλέπουν επίσης ότι η βιομετρία θα διαδραματίσει σημαντικό ρόλο στο μέλλον, λόγω του μειωμένου κόστους της τεχνολογίας και της αυξημένης αποδοχής από τους καταναλωτές (Rinehart, 2000). Μαζί με την αύξηση της ζήτησης, τα έσοδα από τις πωλήσεις βιομετρικών στοιχείων αυξήθηκαν σε 1,2 δισεκατομμύρια δολάρια το 2004 και αναμένεται να αυξηθούν σε 4,6 δισεκατομμύρια δολάρια έως το 2008 (International Biometric Group, 2005).

Παρά αυτές τις θετικές εκτιμήσεις, υπάρχουν επίσης κρίσιμα ζητήματα που πρέπει να ληφθούν υπόψη από την πλευρά των πελατών των ξενοδοχείων, όπως η προστασία της ιδιωτικής ζωής. Επειδή οι πελάτες των ξενοδοχείων είναι οι τελικοί χρήστες της βιομετρίας, οι διευθυντές ξενοδοχείων, οι κατασκευαστές και οι προμηθευτές βιομετρικών συστημάτων πρέπει να κατανοήσουν τους λόγους για τους οποίους οι πελάτες αποδέχονται ή απορρίπτουν τη βιομετρία (Anderson, et. al., 2025).

1.2. Παρουσίαση λέξεων-κλειδιών

Η διαχείριση είναι ο όρος που περιγράφει όλα τα στάδια που περιλαμβάνονται στον σχεδιασμό, την οργάνωση, την καθοδήγηση και τον έλεγχο των πόρων ενός οργανισμού, ώστε να μπορεί να επιτύχει τους στρατηγικούς και επιχειρησιακούς στόχους του (Hallin & Marnburg, 2008). Η διαχείριση είναι πολύ σημαντική στον ξενοδοχειακό κλάδο, καθώς καθορίζει τις πολιτικές και τις διαδικασίες για τις λειτουργίες, την ποιότητα των υπηρεσιών και τη διαχείριση κινδύνων. Η σωστή διαχείριση των πληροφοριών των πελατών είναι πολύ σημαντική, καθώς η σωστή συλλογή, έλεγχος και προστασία των δεδομένων βοηθά την

επιχείρηση να ακολουθεί τους κανόνες και να διατηρεί τη φήμη και την αξιοπιστία της (Brotherton, & Wood, 2013).

Η απάτη, η εξαπάτηση και η παραβίαση της εμπιστοσύνης είναι όλες παράνομες δραστηριότητες που εμπίπτουν στην κατηγορία των οικονομικών εγκλημάτων. Τα παραδείγματα οικονομικών εγκλημάτων περιλαμβάνουν την απάτη, το ξέπλυμα χρήματος, την πλαστογράφηση εγγράφων και τη χρήση πλαστών στοιχείων ταυτότητας. Στις ξενοδοχειακές δραστηριότητες, τα οικονομικά εγκλήματα μπορεί να προκύψουν λόγω ανεπαρκούς επαλήθευσης των πελατών, αυξάνοντας την πιθανότητα παράνομων συναλλαγών, φοροδιαφυγής ή χρήσης εγκαταστάσεων για παράνομες δραστηριότητες. Οι μηχανισμοί διαχείρισης και εταιρικού ελέγχου (Hua, & Zhang, 2020) ενδιαφέρονται ιδιαίτερα για την καταπολέμηση και τον εντοπισμό των οικονομικών εγκλημάτων.

Η διοίκηση μιας εταιρείας εφαρμόζει ένα σύστημα κανόνων, διαδικασιών και μηχανισμών που ονομάζεται εσωτερικός έλεγχος, προκειμένου να διασφαλίσει την ομαλή λειτουργία της επιχείρησης, την προστασία των περιουσιακών της στοιχείων και την ακρίβεια των πληροφοριών. Στον ξενοδοχειακό κλάδο, ο εσωτερικός έλεγχος συνδέεται στενά με τη διαχείριση κινδύνων, την τήρηση των κανόνων και την καταπολέμηση των οικονομικών προβλημάτων (Erkan, et. al., 2017). Δίνεται ιδιαίτερη έμφαση στην επαλήθευση και τη διαχείριση των δεδομένων των πελατών, καθώς αυτά είναι απαραίτητα για τον περιορισμό της απάτης και τη βελτίωση της διαφάνειας και της λογοδοσίας εντός του οργανισμού (Wang, & Alexander, 2013).

1.3. Σκοπός και στόχοι της εργασίας

Η παρόν εργασία έχει ως στόχο να εξετάσει την επαλήθευση και τη διαχείριση των δεδομένων πελατών σε ξενοδοχεία της Μυκόνου, με έμφαση στις μεγάλες επιχειρήσεις φιλοξενίας. Η μελέτη επιδιώκει να αναδείξει τόσο το θεωρητικό πλαίσιο που διέπει τις διαδικασίες ταυτοποίησης πελατών όσο και τις πρακτικές που εφαρμόζονται στην πράξη

από τα ξενοδοχεία, λαμβάνοντας υπόψη τις ιδιαιτερότητες ενός τουριστικού προορισμού διεθνούς χαρακτήρα με υψηλή επισκεψιμότητα.

Συγκεκριμένα, οι κύριοι στόχοι της διατριβής είναι:

- να εξετάσει τον τρόπο με τον οποίο τα ξενοδοχεία στη Μύκονο ταυτοποιούν τους πελάτες τους,
- να διαπιστώσει τις προκλήσεις και τους κινδύνους που αντιμετωπίζουν τα ξενοδοχεία κατά τη συλλογή, επαλήθευση και διαχείριση των δεδομένων πελατών,
- τέλος, να σχεδιάσει στρατηγικές για τη βελτίωση των διαδικασιών επαλήθευσης και την ενίσχυση των εσωτερικών ελέγχων.

1.4. Δομή και μεθοδολογική προσέγγιση

Το άρθρο είναι δομημένο σε δύο κύρια μέρη. Το πρώτο μέρος αφορά τη θεωρητική και βιβλιογραφική προσέγγιση του προβλήματος. Σε αυτό το τμήμα περιγράφονται οι βασικές αρχές που αφορούν την επαλήθευση των πελατών και τα πρωτόκολλα ταυτότητας στον ξενοδοχειακό τομέα. Η ανάλυση βασίζεται σε επιστημονικά άρθρα, μελέτες, κατευθυντήριες γραμμές διεθνών οργανισμών και τεκμηριωμένες επαγγελματικές πρακτικές τόσο στη διεθνή όσο και στην ελληνική βιβλιογραφία.

Το δεύτερο τμήματα καλύπτει την εμπειρική έρευνα που διεξήχθη μέσω μιας μελέτης περίπτωσης ξενοδοχειακών μονάδων στη Μύκονο. Η επιλεγμένη μεθοδολογία της μελέτης είναι ποσοτική, χρησιμοποιώντας ένα δομημένο ερωτηματολόγιο που απευθύνεται σε στελέχη ή διευθυντές ξενοδοχείων. Το 1ο μέρος του εμπειρικού τμήματος παρουσιάζει το σχεδιασμό του ερωτηματολογίου και τα κριτήρια επιλογής των ξενοδοχειακών μονάδων, όπως το μέγεθος, ο αριθμός των κλινών και το επίπεδο των παρεχόμενων υπηρεσιών. Το 2ο μέρος αναλύει τις απαντήσεις και παρουσιάζει τα κύρια θέματα που προέκυψαν, όπως οι διαδικασίες ταυτοποίησης των πελατών, οι δυσκολίες εφαρμογής, ο ρόλος του προσωπικού και τα μέτρα εσωτερικού ελέγχου. Η ανάλυση δίνει τη δυνατότητα σύγκρισης μεταξύ ξενοδοχειακών

Πατσαρούχας Παναγιώτης Βασίλειος, «Το πρόβλημα της εξακρίβωσης στοιχείων των πελατών στις μεγάλες επιχειρήσεις στη Μύκονο - Μελέτη περίπτωσης των μεγάλων ξενοδοχειακών μονάδων της Μυκόνου»

μονάδων και εξαγωγής συμπερασμάτων σχετικά με τις ομοιότητες και τις διαφορές στις πρακτικές που ακολουθούνται.

Η εργασία ολοκληρώνεται με ένα τμήμα σχετικά με τα Συμπεράσματα και τις Συστάσεις, στο οποίο συνοψίζονται τα βασικά ευρήματα της έρευνας, προσδιορίζονται οι ελλείψεις και οι ανάγκες των ξενοδοχείων στη διαχείριση δεδομένων πελατών και προτείνονται στρατηγικές για τη βελτίωση του εσωτερικού ελέγχου και της αποτελεσματικότητας των διαδικασιών επαλήθευσης.

2. Θεωρητική και Βιβλιογραφική Προσέγγιση του Προβλήματος

2.1. Διαχείριση ταυτότητας και πρόσβασης (IAM)

Το IAM είναι μια μέθοδος που παρέχει επαρκές επίπεδο προστασίας για τους πόρους και τα δεδομένα ενός οργανισμού μέσω κανόνων και πολιτικών που επιβάλλονται στους χρήστες με διάφορες τεχνικές, όπως η επιβολή κωδικών πρόσβασης, η εκχώρηση προνομίων στους χρήστες και η παροχή λογαριασμών χρηστών (Almulla, & Yeun, 2010). Επίσης, το IAM έχει δύο συνιστώσες, τη Διαχείριση Ταυτότητας και τη Διαχείριση Πρόσβασης. Τα συστήματα διαχείρισης ταυτότητας συμβάλλουν στην παροχή ενός υπερσύνολου συστημάτων παροχής χρηστών που διευκολύνουν τη διαχείριση των διαπιστευτηρίων των χρηστών και των πληροφοριών ταυτότητάς τους σε χρήστες και άλλα άτομα που χρειάζονται αυτές τις πληροφορίες. Ομοίως, τα συστήματα διαχείρισης πρόσβασης παρέχουν ισχυρή λύση ελέγχου ταυτότητας και εξουσιοδότησης χρησιμοποιώντας ενιαία σύνδεση (SSO), WebSEAL και προσεγγίσεις βάσει πολιτικών για τον προσδιορισμό του ποιος μπορεί να έχει πρόσβαση στον πόρο και σε ποιο επίπεδο (Thakur & Gaikwad, 2015).

Με βάση τους Almulla και Yeun (2010), η διαχείριση ταυτότητας και πρόσβασης προσφέρει διάφορες υπηρεσίες, όπως:

1. Υπηρεσίες ελέγχου ταυτότητας: Ο κύριος σκοπός του ελέγχου ταυτότητας είναι η επαλήθευση των διαπιστευτηρίων του χρήστη για να επιτραπεί η πρόσβαση σε προστατευμένους πόρους. Η παραδοσιακή μέθοδος είναι η χρήση ονόματος χρήστη και κωδικού πρόσβασης. Ωστόσο, το IAM απαιτεί έλεγχο ταυτότητας βάσει πολλαπλών παραγόντων (όπως το token υλικού). Η ισχυρή πιστοποίηση μπορεί να χρησιμοποιεί δύο ή περισσότερους παράγοντες, όπως δακτυλικό αποτύπωμα, κωδικό μιας χρήσης (OTP) κ.λπ. Στην πιστοποίηση βάσει κινδύνου, το επίπεδο κινδύνου υπολογίζεται στο τέλος κάθε συναλλαγής για να αξιολογηθεί ο κίνδυνος εμπιστοσύνης στον αιτούντα παράγοντα, με βάση τη γεωγραφική θέση, το ιστορικό, τη συμπεριφορά και άλλους παράγοντες. Η συναλλαγή μπορεί να εγκριθεί ή να απορριφθεί με βάση το υπολογισμένο επίπεδο κινδύνου (χαμηλό ή υψηλό).

2. Υπηρεσίες διαχείρισης εξουσιοδοτήσεων: Ο κύριος στόχος είναι να γνωρίζουμε σε τι έχει πρόσβαση ο χρήστης, το οποίο θα πρέπει να είναι μόνο οι υπηρεσίες και οι πόροι στους οποίους έχει δικαίωμα με βάση τον ρόλο του χρήστη που έχει ορίσει ο οργανισμός. Επομένως, θα πρέπει να εφαρμόζονται κατάλληλες πολιτικές και η πρόσβαση θα πρέπει να εγκρίνεται ή να απορρίπτεται με βάση αυτές τις πολιτικές.

3. Διαχείριση ταυτότητας: Σημαίνει τη δημιουργία μιας ψηφιακής ταυτότητας ή ενός λογαριασμού για να επιτρέπεται στους χρήστες η πρόσβαση σε πόρους. Κάθε φορά που ένας υπάλληλος προσλαμβάνεται (αποχωρεί) από μια εταιρεία, του απονέμεται μια ψηφιακή ταυτότητα από την εταιρεία για να του επιτρέπεται (απαγορεύεται) η πρόσβαση στο αποθετήριο της για την εκτέλεση των εργασιών που του έχουν ανατεθεί. Μπορεί να χρησιμοποιηθεί από το Lightweight Directory Access Protocol (LDAP) και τις υπηρεσίες ενεργού καταλόγου (Καίκη, 2004).

4. Ομοσπονδιακή ταυτότητα: Δημιουργεί εμπιστοσύνη μεταξύ πολλαπλών εφαρμογών ή οργανισμών μέσω ενός τρίτου παρόχου. Ο διακομιστής ομοσπονδίας στον πάροχο ταυτότητας αποθηκεύει τις πληροφορίες και τα διαπιστευτήρια των χρηστών και επιτρέπει την SSO χωρίς κωδικούς πρόσβασης. Κάθε φορά που ένας χρήστης προσπαθεί να συνδεθεί σε μια υπηρεσία, αντί να παρέχει διαπιστευτήρια στον πάροχο της υπηρεσίας, ο πάροχος ταυτότητας παρουσιάζει στον πάροχο της υπηρεσίας ένα διακριτικό χρησιμοποιώντας τυπικά πρωτόκολλα ταυτότητας, όπως Security Assertion Markup Language (SAML), Open Authorization (OAuth), OpenId κ.λπ. Ο πάροχος της υπηρεσίας δέχεται αυτό το διακριτικό, καθώς εμπιστεύεται τον πάροχο ταυτότητας και τον πιστοποιημένο χρήστη. Ως εκ τούτου, το SSO εξαλείφει την ανάγκη να θυμάστε πολλαπλά αναγνωριστικά/κωδικούς πρόσβασης για πολλαπλές εφαρμογές.

5. Διαχείριση συμμόρφωσης: Απαιτεί κατάλληλη παρακολούθηση και αναφορά για ελέγχους. Είναι η διαδικασία αναθεώρησης και εξέτασης των αρχείων εξουσιοδότησης και πιστοποίησης για να ελεγχθεί η συμμόρφωση με προκαθορισμένα πρότυπα και πολιτικές ασφαλείας. Όπως φαίνεται στο Σχ. 1, που παρουσιάζει τις φάσεις διαχείρισης του κύκλου ζωής της ταυτότητας.

Η διαχείριση ταυτότητας και πρόσβασης (IAM) είναι μια κρίσιμη πτυχή κάθε οργανισμού, συμπεριλαμβανομένου του τομέα του τουρισμού και της φιλοξενίας. Το IAM βοηθά στη διαχείριση και τον έλεγχο της πρόσβασης σε πόρους, συστήματα και δεδομένα εντός ενός οργανισμού. Ο τομέας του τουρισμού και της φιλοξενίας έχει δει μια αύξηση στη χρήση τεχνικών IAM για την προστασία των πληροφοριών των επισκεπτών, τη διαχείριση της πρόσβασης των υπαλλήλων και τη βελτίωση της συνολικής ασφάλειας. Μία από τις κύριες τεχνικές IAM που χρησιμοποιούνται στον τομέα του τουρισμού και της φιλοξενίας είναι η πολυπαραγοντική πιστοποίηση (MFA). Η MFA περιλαμβάνει τη χρήση πολλαπλών παραγόντων ελέγχου ταυτότητας, όπως κωδικός πρόσβασης, βιομετρικά δεδομένα ή έξυπνη κάρτα, για την επαλήθευση της ταυτότητας των χρηστών (Almulla, & Yeun, 2010).

Σύμφωνα με τη Liu (2022), η MFA είναι αποτελεσματική στην πρόληψη της μη εξουσιοδοτημένης πρόσβασης και στη μείωση του κινδύνου παραβίασης δεδομένων στον κλάδο της φιλοξενίας. Μια άλλη τεχνική IAM που κερδίζει δημοτικότητα στον τομέα του τουρισμού και της φιλοξενίας είναι η ομοσπονδία ταυτότητας (IF). Η IF επιτρέπει στους χρήστες να έχουν πρόσβαση σε πόρους και υπηρεσίες σε πολλαπλούς οργανισμούς χρησιμοποιώντας ένα μόνο σύνολο διαπιστευτηρίων. Η IF μπορεί να βελτιώσει την εμπειρία του χρήστη, να μειώσει την κούραση από τους κωδικούς πρόσβασης και να ενισχύσει την ασφάλεια (Mohammed, 2019). Η IF μπορεί να χρησιμοποιηθεί για να διευκολύνει την ασφαλή πρόσβαση σε υπηρεσίες για τους επισκέπτες, όπως κρατήσεις ξενοδοχείων, χωρίς να χρειάζεται οι επισκέπτες να δημιουργήσουν νέους λογαριασμούς ή να θυμούνται πολλαπλούς κωδικούς πρόσβασης (Καπίκη, 2004). Ο έλεγχος πρόσβασης βάσει ρόλου (RBAC) είναι μια άλλη τεχνική IAM που χρησιμοποιείται συνήθως στον τομέα του τουρισμού και της φιλοξενίας. Το RBAC περιλαμβάνει την ανάθεση ρόλων στους χρήστες με βάση τις εργασιακές τους λειτουργίες και, στη συνέχεια, την παροχή δικαιωμάτων πρόσβασης με βάση αυτούς τους ρόλους. Αυτή η προσέγγιση διασφαλίζει ότι οι χρήστες έχουν πρόσβαση μόνο στους πόρους και τα συστήματα που χρειάζονται για την εκτέλεση των εργασιακών τους καθηκόντων (Sagar & Vitalii Syrovatskyi, 2022).

Σύμφωνα με τους Gao και συν. (2022), το RBAC μπορεί να χρησιμοποιηθεί για τη διαχείριση της πρόσβασης των εργαζομένων σε ευαίσθητα δεδομένα, όπως οικονομικές πληροφορίες, και για τη βελτίωση της συνολικής ασφάλειας στον κλάδο της φιλοξενίας. Τα

τελευταία χρόνια, έχει δοθεί μεγαλύτερη έμφαση στη χρήση της τεχνητής νοημοσύνης (AI) και της μηχανικής μάθησης (ML) για τη βελτίωση του IAM στον κλάδο του τουρισμού και της φιλοξενίας. Η AI και η ML μπορούν να χρησιμοποιηθούν για την ανάλυση της συμπεριφοράς των χρηστών και την ανίχνευση ανώμαλων δραστηριοτήτων, όπως προσπάθειες μη εξουσιοδοτημένης πρόσβασης (Azhar, 2015).

Σύμφωνα με τους Sestino και De Mauro (2021), η AI και η ML μπορούν επίσης να χρησιμοποιηθούν για την αυτοματοποίηση διαδικασιών IAM, όπως η παροχή πρόσβασης σε χρήστες και η πιστοποίηση πρόσβασης, οι οποίες μπορούν να βελτιώσουν την αποδοτικότητα και να μειώσουν τα σφάλματα. Οι τεχνικές IAM μπορούν επίσης να χωριστούν με βάση τον σκοπό χρήσης της τεχνικής αυτής ως εξής: Τεχνικές πιστοποίησης. Η πιστοποίηση είναι η διαδικασία επαλήθευσης της ταυτότητας ενός ατόμου. Στον τουρισμό και τη φιλοξενία, οι τεχνικές πιστοποίησης χρησιμοποιούνται για να διασφαλιστεί ότι μόνο εξουσιοδοτημένο προσωπικό μπορεί να έχει πρόσβαση σε ευαίσθητα δεδομένα (Karie et al., 2020). Πρόσφατα, η πολυπαραγοντική πιστοποίηση (MFA) έχει κερδίσει δημοτικότητα στον κλάδο. Η MFA απαιτεί από τους χρήστες να παρέχουν τουλάχιστον δύο διαφορετικούς τύπους μεθόδων αυθεντικοποίησης, όπως κωδικούς πρόσβασης, βιομετρικά στοιχεία ή έξυπνες κάρτες, για να έχουν πρόσβαση σε ευαίσθητα δεδομένα. Πολλές μελέτες έχουν δείξει ότι η MFA είναι μια αποτελεσματική τεχνική για τη μείωση του κινδύνου μη εξουσιοδοτημένης πρόσβασης και παραβιάσεων δεδομένων (Taher et al., 2019).

Τεχνικές εξουσιοδότησης. Η εξουσιοδότηση είναι η διαδικασία χορήγησης πρόσβασης σε συγκεκριμένους πόρους, δεδομένα ή πληροφορίες με βάση την ταυτότητα και το επίπεδο πρόσβασης του χρήστη. Ο έλεγχος πρόσβασης βάσει ρόλου (RBAC) είναι μια τεχνική που χρησιμοποιείται συχνά στον τουρισμό και τη φιλοξενία (Son, & Chen, 2019). Το RBAC διασφαλίζει ότι μόνο οι εξουσιοδοτημένοι χρήστες έχουν πρόσβαση σε συγκεκριμένους πόρους με βάση τον ρόλο ή τη θέση τους. Πρόσφατα, ο έλεγχος πρόσβασης βάσει χαρακτηριστικών (ABAC) έχει κερδίσει δημοτικότητα. Το ABAC επιτρέπει αποφάσεις πρόσβασης με βάση χαρακτηριστικά του χρήστη, όπως η τοποθεσία, η συσκευή και η ώρα της ημέρας. Ο ABAC παρέχει έναν πιο λεπτομερή μηχανισμό ελέγχου πρόσβασης από τον RBAC (Chen et al., 2022).

Τεχνικές κρυπτογράφησης. Η κρυπτογράφηση είναι η διαδικασία μετατροπής ευαίσθητων δεδομένων σε μια μορφή που δεν μπορεί να γίνει εύκολα κατανοητή χωρίς κλειδί. Η κρυπτογράφηση χρησιμοποιείται ευρέως στον τουρισμό και την φιλοξενία για να διασφαλιστεί η εμπιστευτικότητα των ευαίσθητων δεδομένων (Pulido-Gaytan et al., 2021).

Πρόσφατα, η ομομορφική κρυπτογράφηση (HE) έχει αποκτήσει δημοτικότητα στον κλάδο. Η HE επιτρέπει την κρυπτογράφηση και την επεξεργασία των δεδομένων χωρίς να αποκρυπτογραφούνται, γεγονός που μειώνει τον κίνδυνο παραβίασης των δεδομένων. Συστήματα διαχείρισης ταυτότητας Τα συστήματα διαχείρισης ταυτότητας (IMS) είναι συστήματα λογισμικού που διαχειρίζονται την αυθεντικοποίηση και την εξουσιοδότηση των χρηστών. Πρόσφατα, τα συστήματα διαχείρισης ταυτότητας που βασίζονται στο cloud (CIMS) έχουν κερδίσει δημοτικότητα στον τουρισμό και τη φιλοξενία (Compagnucci, et. al., 2019).

Τα CIMS προσφέρουν πολλά οφέλη, όπως επεκτασιμότητα, οικονομική αποδοτικότητα και ευκολία χρήσης. Πολλές μελέτες έχουν δείξει ότι τα CIMS είναι μια αποτελεσματική τεχνική για τη διαχείριση ταυτοτήτων στον τουρισμό και τη φιλοξενία (Wynn & Jones, 2022). Ανάλυση συμπεριφοράς χρηστών Η ανάλυση συμπεριφοράς χρηστών (UBA) είναι η διαδικασία ανάλυσης της συμπεριφοράς των χρηστών για την ανίχνευση ανωμαλιών και πιθανών απειλών ασφαλείας. Η UBA έχει αποκτήσει δημοτικότητα στον τουρισμό και τη φιλοξενία για τον εντοπισμό εσωτερικών απειλών και παραβιάσεων δεδομένων (Kwon et al., 2020). Πρόσφατα, τεχνικές μηχανικής μάθησης (ML) έχουν χρησιμοποιηθεί στην UBA για τη βελτίωση της ακρίβειας του εντοπισμού ανωμαλιών. Πολλές μελέτες έχουν δείξει ότι η UBA που βασίζεται σε ML είναι μια αποτελεσματική τεχνική για τον εντοπισμό εσωτερικών απειλών στον τουρισμό και τη φιλοξενία (Sharma et al., 2021).

2.2. Blockchain για τη διαχείριση της ψηφιακής ταυτότητας των επισκεπτών

Η τεχνολογία blockchain επιτρέπει στα μέρη που εμπλέκονται στις συναλλαγές να έχουν ανοιχτή πρόσβαση στο ιστορικό. Αυτό δημιουργεί ένα περιβάλλον αμοιβαίας εμπιστοσύνης μεταξύ των χρηστών, εξασφαλίζοντας ακριβείς και ενημερωμένες πληροφορίες.

Στα συμβατικά συστήματα κρατήσεων, οι μεσάζοντες διαθέτουν όλα τα στοιχεία της συναλλαγής, τα οποία μπορούν να χρησιμοποιηθούν καταχρηστικά (Williams, 2019).

- Κρατήσεις βάσει έξυπνων συμβολαίων

Οι πελάτες μπορούν να χρησιμοποιούν έξυπνα συμβόλαια βασισμένα στην τεχνολογία blockchain ως αυτοματοποιημένες συμφωνίες για κρατήσεις ξενοδοχείων, χρηματοοικονομικές συναλλαγές και ακυρώσεις κρατήσεων (Βασιλείου, Ηρειώτης & Μπάλιος 2009). Το αυτοματοποιημένο σύστημα αυξάνει την αποδοτικότητα, δεν προκαλεί καθυστερήσεις στις κρατήσεις και διευκολύνει την εμπειρία κράτησης τόσο για τους πελάτες όσο και για τα ξενοδοχεία. Τα έξυπνα συμβόλαια καθιστούν τη διαδικασία πληρωμής πιο ασφαλή, σαφή και χωρίς άγχος, χωρίς τη χρήση μεσαζόντων (Williams, 2019).

Η τεχνολογία blockchain βελτιώνει τις κρατήσεις ξενοδοχείων χρησιμοποιώντας έξυπνα συμβόλαια ως αυτοματοποιημένες συμφωνίες για κρατήσεις ξενοδοχείων που λειτουργούν αυτόνομα. Το σύστημα κρατήσεων ξενοδοχείων βελτιώνεται με την αυτοματοποίηση μέσω της εφαρμογής έξυπνων συμβολαίων. Τα έξυπνα συμβόλαια αποθηκεύουν τα δεδομένα των κρατήσεων και διατηρούν όλους τους προσφερόμενους όρους, όπως τις ημερομηνίες πληρωμής και τις απαιτήσεις check-in. Αυτή η αυτοματοποίηση εξαλείφει τη συμμετοχή τρίτων κατά τη διάρκεια των λειτουργιών. Το σύστημα εκτελεί τις λειτουργίες έγκαιρα και ομαλά, καθώς πραγματοποιεί τις πληρωμές όταν πληρούνται οι απαιτούμενες προϋποθέσεις (Tere, 2022). Η διαδικασία των επιστροφών χρημάτων και των ακυρώσεων γίνεται πιο απλή, καθώς τα έξυπνα συμβόλαια χειρίζονται αυτές τις λειτουργίες αυτόματα. Τα έξυπνα συμβόλαια παρέχουν αρχεία που δεν μπορούν να παραποιηθούν, αποτρέποντας την απάτη και διασφαλίζοντας την ακρίβεια. Μόλις η αλυσίδα μπλοκ καταγράψει πληροφορίες όπως κρατήσεις, αρχεία συναλλαγών ή στοιχεία επισκεπτών στο σύστημα, αυτές δεν μπορούν να αλλάξουν. Τα οφέλη των έξυπνων συμβολαίων στις κρατήσεις συζητούνται ως εξής (Demirel et al., 2021):

- Λιγότερα λάθη: Η αυτοματοποίηση των κρατήσεων μειώνει τα λάθη, όπως η υπεράριθμη κράτηση ή οι λανθασμένες χρεώσεις.
- Καλύτερη εμπειρία πελατών: Οι επισκέπτες απολαμβάνουν μια γρήγορη, ομαλή διαδικασία κράτησης με σαφείς πολιτικές.

· Εμπιστοσύνη και αξιοπιστία: Τόσο τα ξενοδοχεία όσο και οι επισκέπτες διαθέτουν ένα ασφαλές αρχείο της συναλλαγής, αποτρέποντας παρεξηγήσεις.

Ο τομέας της φιλοξενίας χρειάζεται μια ασφαλή διαδικασία για τη διαχείριση των ταυτοτήτων των επισκεπτών, καθώς και για τη βελτίωση της λειτουργικής αποδοτικότητας. Το blockchain παρέχει αρχεία που δεν μπορούν να παραποιηθούν και προσφέρει καλύτερες υπηρεσίες στους πελάτες, μειώνει τους κινδύνους απάτης και παρέχει ασφάλεια πληροφοριών. Οι επισκέπτες μπορούν να χρησιμοποιούν ψηφιακές ταυτότητες για την επαλήθευση της ταυτότητάς τους και δεν χρειάζεται να έχουν πάντα μαζί τους τα πρωτότυπα έγγραφα. Χρησιμοποιεί τρεις βασικές έννοιες, όπως επαναχρησιμοποιήσιμες ψηφιακές ταυτότητες, μειωμένους κινδύνους κλοπής ταυτότητας και KYC (Know Your Customer) βασισμένο σε blockchain, για να παρέχει μεγαλύτερη ασφάλεια. Οι βασικές υπηρεσίες περιλαμβάνουν (Irannezhad & Mahadevan, 2020):

- Έξυπνα συστήματα check-in

Για τη διαχείριση και την αποθήκευση πιστοποιημένων διαπιστευτηρίων, οι επισκέπτες μπορούν να χρησιμοποιούν ψηφιακά πορτοφόλια ταυτότητας. Χρησιμοποιώντας το ψηφιακό πορτοφόλι, οι επισκέπτες δεν χρειάζεται να επιδεικνύουν επανειλημμένα την ταυτότητά τους κατά τη διάρκεια διαφόρων αλληλεπιδράσεων φιλοξενίας (Hsieh et al., 2022). Αυτό μπορεί να βοηθήσει σε (Youssef, et. al., 2024):

· Ελαχιστοποίηση των επαναλαμβανόμενων ελέγχων KYC: Μόλις επαληθευτεί η ταυτότητα ενός επισκέπτη, μπορεί να επαναχρησιμοποιήσει τα διαπιστευτήριά του χωρίς να υποβάλλεται σε νέα επαλήθευση σε κάθε ξενοδοχείο.

· Απλοποιημένη διαδικασία check-in: Η άμεση επαλήθευση της ταυτότητας επιτρέπει ταχύτερη και πιο βολική εγγραφή των επισκεπτών.

· Ασφαλής πρόσβαση στην ταυτότητα

Η αλυσίδα μπλοκ χρησιμοποιεί πολιτικές KYC (Know Your Customer) για τη βελτίωση της ασφάλειας και της ευκολίας των επισκεπτών στον κλάδο της φιλοξενίας. Οι επισκέπτες δεν χρειάζεται να επαληθεύουν επανειλημμένα την ταυτότητά τους, αλλά μόνο μία

φορά, καθώς τα δεδομένα τους αποθηκεύονται με ασφάλεια στο σύστημα αλυσίδας μπλοκ. Τα βασικά πλεονεκτήματα περιλαμβάνουν (Erceg et al., 2020):

- Πρόληψη απάτης: Οι κρυπτογραφικά ασφαλείς ταυτότητες μετριάζουν τους κινδύνους που σχετίζονται με την κλοπή ταυτότητας και τις παραβιάσεις δεδομένων.
- Αυτοκυρίαρχη ταυτότητα (SSI): Οι επισκέπτες διατηρούν τον πλήρη έλεγχο των προσωπικών τους δεδομένων, αποφασίζοντας ποιες πληροφορίες θα μοιραστούν με τους παρόχους υπηρεσιών.
- Αδιάβλητα αρχεία ταυτότητας: Μόλις αποθηκευτούν στο blockchain, τα δεδομένα ταυτότητας δεν μπορούν να αλλοιωθούν ή να πλαστογραφηθούν, εξασφαλίζοντας την ακεραιότητα των δεδομένων.
- Έξυπνα συστήματα check-in

Μια διαδικασία KYC βασισμένη στο blockchain επιτρέπει στα ξενοδοχεία και στους παρόχους φιλοξενίας να επεξεργάζονται τα check-in με γρήγορο και ασφαλή τρόπο. Αυξάνει την αποδοτικότητα του κόστους και βελτιώνει την ευκολία των επισκεπτών, αποτρέποντας τις επαναλαμβανόμενες διαδικασίες KYC. Αυτό βοηθά σε (Buhalis et al., 2019):

- Λειτουργική αποδοτικότητα: Τα ξενοδοχεία μπορούν να μειώσουν σημαντικά το χρόνο και τους πόρους που δαπανώνται για επαναλαμβανόμενες επαληθεύσεις KYC.
- Ταχύτερη διαδικασία check-in των επισκεπτών: Με προ-επαληθευμένα διαπιστευτήρια, οι επισκέπτες μπορούν να κάνουν check-in γρήγορα χωρίς να παρουσιάζουν φυσικά έγγραφα κάθε φορά.
- Παγκόσμια χρηστικότητα: Η ψηφιακή ταυτότητα ενός επισκέπτη μπορεί να χρησιμοποιηθεί σε διεθνείς αλυσίδες φιλοξενίας, απλοποιώντας τις διατυπώσεις ταξιδιού και διαμονής.
- Εξατομικευμένες υπηρεσίες

Οι προτιμήσεις, οι συμπάθειες και οι αντιπάθειες των επισκεπτών αποθηκεύονται με ασφάλεια, κάτι που μπορεί να βοηθήσει την επιχείρηση να ξεχωρίσει παρέχοντας εξατομικευμένη και βελτιωμένη εμπειρία χρήστη (Buhalis et al., 2019).

2.3. Αυτοματοποιημένη ψηφιακή επαλήθευση ταυτότητας

Η επίτευξη της τέλει ισορροπίας μεταξύ αυστηρής επαλήθευσης και ομαλής εμπειρίας για τους επισκέπτες μπορεί να είναι δύσκολη. Η αυτοματοποιημένη ψηφιακή επαλήθευση ταυτότητας προσφέρει μια λύση στους ξενοδόχους για να μειώσουν το βάρος της επαλήθευσης των επισκεπτών, να μειώσουν τα λειτουργικά κόστη και να βελτιώσουν την συνολική εμπειρία των επισκεπτών. Ουσιαστικά, επιτρέπει το απομακρυσμένο check-in: οι επισκέπτες μπορούν απλά να τραβήξουν μια φωτογραφία της ταυτότητάς τους και ένα selfie για να επικυρώσουν την ταυτότητά τους και στη συνέχεια όλες οι πληροφορίες των επισκεπτών μπορούν να ληφθούν με ακρίβεια από το σύστημα διαχείρισης ακινήτων, όπως συνήθως. Χωρίς χειροκίνητη παρέμβαση, όλα κυλούν ομαλά. Το check-in είναι η πρώτη επαφή των ξενοδοχείων με έναν επισκέπτη. Στιγμές όπως αυτές μπορούν να καθορίσουν την εμπειρία τους. Δυστυχώς, η αναμονή στη ρεσεψιόν και η συμπλήρωση εγγράφων είναι συνηθισμένα σημεία τριβής. Το τελευταίο πράγμα που θέλει κανείς μετά από ένα μακρύ ταξίδι είναι να φτάσει στο ξενοδοχείο, κουρασμένος από το ταξίδι, και να πρέπει να περιμένει μέχρι να επαληθευτεί η ταυτότητά του και να εισαχθούν τα δεδομένα του στο σύστημα. Η ψηφιακή ταυτότητα μπορεί να λύσει πολλές από τις προκλήσεις που αντιμετωπίζει σήμερα ο κλάδος της φιλοξενίας, συμπεριλαμβανομένης της τριβής στην εμπειρία των επισκεπτών και της λειτουργικής αναποτελεσματικότητας (Wang, & Alexander, 2013).

Δεν είναι μυστικό ότι ο κλάδος της φιλοξενίας αντιμετωπίζει πολλές προκλήσεις, πολλές από τις οποίες σχετίζονται με την ταυτότητα των επισκεπτών. Τα ζητήματα προστασίας των δεδομένων προσωπικού χαρακτήρα έχουν φτάσει σε ιστορικά υψηλά επίπεδα και οι επισκέπτες έχουν γίνει πολύ επιφυλακτικοί όσον αφορά την κοινοποίηση των προσωπικών τους στοιχείων. Δεν είναι πλέον αποδεκτό να ζητείται πλήρης σάρωση του διαβατηρίου, η οποία αποθηκεύεται εκτός του ελέγχου του επισκέπτη, αγνοώντας πλήρως όλες τις αρχές προστασίας της ιδιωτικής ζωής, μόνο και μόνο επειδή ο επισκέπτης έχει δώσει τη συγκατάθεσή του (Asorona & Ateeq, 2024).

Μια αναδυόμενη έννοια, η αποκεντρωμένη ψηφιακή ταυτότητα, προσφέρει βελτιωμένη προστασία της ιδιωτικής ζωής των πελατών και απλοποιημένες διαδικασίες που μπορούν να βοηθήσουν τους ξενοδόχους να μειώσουν τα λειτουργικά τους έξοδα. Με την ψηφιακή

ταυτότητα, το προσωπικό δεν χρειάζεται να αφιερώνει χρόνο στη συλλογή πληροφοριών για τους πελάτες και μπορεί να επικεντρωθεί στη δημιουργία πιο εξατομικευμένων εμπειριών. Και χάρη στον αποκεντρωμένο χαρακτήρα της, τα ζητήματα προστασίας της ιδιωτικής ζωής επιλύονται εκ των προτέρων. Με απλά λόγια, είναι ένας τρόπος διαχείρισης των δεδομένων ταυτότητας που δεν αποθηκεύει προσωπικά δεδομένα σε μια κεντρική βάση δεδομένων και ελέγχεται πλήρως από τον χρήστη. Ας το συγκρίνουμε με ένα κεντρικό σύστημα ταυτότητας, όπου οι ταυτότητές μας συνήθως διαχειρίζονται και αποθηκεύονται από έναν μόνο φορέα, όπως η κυβέρνηση ή κάποια ιδιωτική εταιρεία. Τα προσωπικά δεδομένα δεν βρίσκονται στα χέρια των ατόμων και διαχειρίζονται εξ ολοκλήρου από φορείς. Το βάρος της διαχείρισης, της προστασίας και της ασφάλειας των δεδομένων βαρύνει τους οργανισμούς. Επιπλέον, η ταυτότητα μπορεί να τεθεί σε κίνδυνο εάν ο κεντρικός φορέας υποστεί παραβίαση ή τα δεδομένα δεν προστατεύονται κατάλληλα (Asorona & Ateeq, 2024).

Αντίθετα, ένα αποκεντρωμένο σύστημα εξαλείφει την ανάγκη για κεντρική αρχή, μειώνοντας τον κίνδυνο παραβιάσεων ή διαρροών δεδομένων. Σε τέτοια συστήματα, οι πελάτες έχουν τον πλήρη έλεγχο του ποιος έχει πρόσβαση στα δεδομένα ταυτότητάς τους και για πόσο χρονικό διάστημα, μέσω επαληθεύσιμων διαπιστευτηρίων. Μπορούν να επιλέξουν να μοιραστούν μόνο τα απαραίτητα δεδομένα, όπως το όνομα ή την εθνικότητα, αντί να μοιραστούν όλες τις πληροφορίες ταυτότητας ή σαρώσεις διαβατηρίων, παρέχοντας έτσι ένα επιπλέον επίπεδο προστασίας της ιδιωτικής ζωής (Anderson, et. al., 2025).

Ο συνδυασμός της αποκεντρωμένης ψηφιακής ταυτότητας με τη βιομετρική επαλήθευση ταυτότητας μέσω προσώπου στον κλάδο της φιλοξενίας έχει τη δυνατότητα να φέρει επανάσταση στην εμπειρία των επισκεπτών. Η επαλήθευση ταυτότητας μέσω αναγνώρισης προσώπου προσφέρει έναν βολικό και ασφαλή τρόπο επαλήθευσης της ταυτότητας, εξαλείφοντας την ανάγκη για φυσικά έγγραφα ή ταυτότητες. Με τη λήψη και ανάλυση βιομετρικών στοιχείων του προσώπου, οι επισκέπτες μπορούν να αποδείξουν την ταυτότητά τους από οπουδήποτε, ανά πάσα στιγμή, χρησιμοποιώντας μόνο τα smartphone τους — κατά τη διαδικασία check-in ή όποτε απαιτείται ταυτοποίηση (Atsushi Ugajin, 2023).

Όταν αυτές οι δύο τεχνολογίες συνδυάζονται στον κλάδο της φιλοξενίας, προκύπτουν πολλά οφέλη. Πρώτον, η διαδικασία check-in μπορεί να επιταχυνθεί και να γίνει πιο αποτελεσματική. Οι επισκέπτες δεν χρειάζεται πλέον να συμπληρώνουν φόρμες ή να

παρουσιάζουν φυσικά έγγραφα ταυτότητας. Θα παρουσιάσουν την ταυτότητά τους μία φορά και στη συνέχεια θα δημιουργηθεί ένα επαληθεύσιμο διαπιστευτήριο, το οποίο θα μπορούν να χρησιμοποιούν κάθε φορά που διαμένουν στο ξενοδοχείο σας. Αυτή η απλοποιημένη διαδικασία εξοικονομεί χρόνο τόσο για τους επισκέπτες όσο και για το προσωπικό του ξενοδοχείου, μειώνοντας τους χρόνους αναμονής και βελτιώνοντας τη συνολική εμπειρία των επισκεπτών (Kumar Saha et al., 2023).

Επιπλέον, ο συνδυασμός αυτών των τεχνολογιών επιτρέπει στα ξενοδοχεία να προσφέρουν εξατομικευμένες και προσαρμοσμένες υπηρεσίες στους επισκέπτες τους. Μόλις επαληθευτεί η αποκεντρωμένη ψηφιακή ταυτότητα ενός επισκέπτη, το προσωπικό του ξενοδοχείου μπορεί να έχει πρόσβαση σε σχετικές πληροφορίες σχετικά με τις προτιμήσεις, τις προηγούμενες διαμονές και τα ειδικά αιτήματά του. Αυτό επιτρέπει μια πιο εξατομικευμένη εμπειρία check-in, όπου οι επισκέπτες μπορούν να χαιρετιστούν με το όνομά τους, να τους προσφερθούν οι προτιμώμενες ανέσεις του δωματίου τους ή να τους παρουσιαστούν εξατομικευμένες προτάσεις και προσφορές με βάση τις προηγούμενες προτιμήσεις τους. Με την ενσωμάτωση της βιομετρικής αναγνώρισης προσώπου με την αποκεντρωμένη ψηφιακή ταυτότητα, οι ξενοδόχοι μπορούν να παρέχουν στους επισκέπτες πλήρη έλεγχο της ταυτότητάς τους και ταυτόχρονα καλύτερη εξυπηρέτηση πελατών (Figini et al., 2020).

2.4. Βιομετρική τεχνολογία

Ο ξενοδοχειακός κλάδος έχει καλά τεκμηριωμένες ιδιαιτερότητες, όπως η επαλήθευση της ταυτότητας ενός επισκέπτη πριν από την κατανάλωση του προϊόντος, η παροχή πρόσβασης στους επισκέπτες επανειλημμένα σε διάφορους χώρους ενός κτιρίου ή ενός συγκροτήματος που τελικά γίνονται ο ιδιωτικός χώρος των επισκεπτών κατά τη διάρκεια μιας περιόδου παροχής υπηρεσιών, ενώ παράλληλα δίνεται έμφαση στις πάντα ευγενικές αλληλεπιδράσεις με τους επισκέπτες. Η παραδοσιακή διαδικασία επαλήθευσης της ταυτότητας των επισκεπτών αποτελεί αναμφισβήτητο το πιο κρίσιμο σημείο συμφόρησης στην παροχή υπηρεσιών, αλλά παραμένει η βάση της ασφάλειας για τους επισκέπτες, το προσωπικό και το κοινό. Για να προσφέρουν μια απρόσκοπτη εμπειρία που εκτιμάται ιδιαίτερα από τους επισκέπτες και να

αντιμετωπίσουν αυτό το εμπόδιο, τα ξενοδοχεία έχουν αναπτύξει νέες τεχνολογίες και μοντέλα υπηρεσιών με στόχο την αύξηση της αυτοματοποίησης της πιστοποίησης, όπως περίπτερα αυτοεξυπηρέτησης, συστήματα αυτοεξυπηρέτησης για check-in μέσω κινητού τηλεφώνου, πλατφόρμες ανταλλαγής μηνυμάτων που παρέχουν πληροφορίες για την εκτιμώμενη ώρα άφιξης των καταναλωτών και προγραμματισμό πρόσθετου προσωπικού κατά τις ώρες αιχμής. Ωστόσο, παρά τις προσπάθειες των ξενοδοχείων, τα εμπόδια στην πιστοποίηση ενδέχεται να εξακολουθούν να υπάρχουν και να προκαλούν απογοήτευση τόσο στους καταναλωτές όσο και στο προσωπικό. Επιπλέον, η εγκατάλειψη της παραδοσιακής χειροκίνητης πιστοποίησης υπέρ της αυτοματοποιημένης πιστοποίησης με βάση το σύστημα πληροφοριών (IS) μπορεί να αυξήσει τον κίνδυνο ασφάλειας (Morosan & Hilton, 2020).

Η βιομετρική τεχνολογία έχει περιγραφεί με διάφορους τρόπους από τους ερευνητές (Singh et al., 2021). Η βιομετρική τεχνολογία εκφράζεται ως εφαρμογές που αφορούν την ταυτοποίηση και την πιστοποίηση ατόμων με βάση τα βιολογικά ή συμπεριφορικά χαρακτηριστικά τους. Η βιομετρική τεχνολογία είναι το πιο πρακτικό μέσο για την ταυτοποίηση και την πιστοποίηση ατόμων με αξιόπιστο και γρήγορο τρόπο μέσω μοναδικών βιολογικών χαρακτηριστικών (Jain et al., 2004). Ενώ οι Dargan και Kumar (2020) ανέφεραν ότι η βιομετρική τεχνολογία αναφέρεται στη μέτρηση και τη στατιστική ανάλυση των μοναδικών φυσικών και συμπεριφορικών χαρακτηριστικών των ανθρώπων. Ως εκ τούτου, ο σκοπός της τεχνολογίας είναι να καθορίσει και να επιβεβαιώσει την ταυτότητα ενός ατόμου με βάση αυτά τα διακριτικά χαρακτηριστικά. Αυτά τα βιομετρικά χαρακτηριστικά μπορούν να συλλεχθούν ή να δειγματοληφθούν εύκολα χρησιμοποιώντας διάφορα βιομετρικά συστήματα ή συσκευές.

Τα βιομετρικά χαρακτηριστικά ή ιδιότητες είναι μοναδικά για κάθε άτομο και η μοναδικότητά τους αποτελεί τη βάση για αξιόπιστη ταυτοποίηση και πιστοποίηση. Τα βιομετρικά χαρακτηριστικά παρουσιάζουν διακριτά χαρακτηριστικά ή μοτίβα που μπορούν να χρησιμοποιηθούν για τη διαφοροποίηση ενός ατόμου από ένα άλλο (Jain et al., 2016). Αυτά τα χαρακτηριστικά περιλαμβάνουν φυσιολογικά χαρακτηριστικά όπως δακτυλικά αποτυπώματα, μοτίβα ίριδας, χαρακτηριστικά προσώπου και DNA, καθώς και συμπεριφορικά χαρακτηριστικά όπως μοτίβα φωνής, ρυθμός πληκτρολόγησης και βάδισμα. Για παράδειγμα, σχεδόν όλοι έχουν δακτυλικά αποτυπώματα, αν και τα συγκεκριμένα μοτίβα διαφέρουν από

άτομο σε άτομο. Αυτά τα διακριτικά χαρακτηριστικά επιτρέπουν στα βιομετρικά συστήματα να ταυτοποιούν με ακρίβεια άτομα με παρόμοια χαρακτηριστικά, ακόμη και σε μεγάλους πληθυσμούς. Η μετρησιμότητά τους επιτρέπει την ακριβή και αξιόπιστη ταυτοποίηση και επαλήθευση της ταυτότητας. Σε αντίθεση με τις παραδοσιακές μορφές ταυτοποίησης, όπως οι κωδικοί πρόσβασης ή οι ταυτότητες, που μπορούν εύκολα να κλαπούν ή να πλαστογραφηθούν, τα βιομετρικά χαρακτηριστικά είναι εγγενή στο άτομο και δύσκολο να πλαστογραφηθούν. Αν και τα βιομετρικά χαρακτηριστικά είναι εγγενώς δύσκολο να πλαστογραφηθούν ή να αναπαραχθούν και είναι σχετικά σταθερά στο χρόνο, ενδέχεται να αλλάξουν ελαφρώς λόγω γήρανσης ή τραυματισμού (Alay & Al-Baity, 2020).

Τα βιομετρικά συστήματα είναι συσκευές που καταγράφουν συγκεκριμένα χαρακτηριστικά ή μοτίβα βιομετρικών χαρακτηριστικών και τα μετατρέπουν σε ψηφιακά δεδομένα για σύγκριση και ανάλυση (Tripathi, 2011). Τα βιομετρικά συστήματα είναι ικανά να αναγνωρίζουν και να πιστοποιούν με μοναδικό τρόπο τα άτομα χρησιμοποιώντας τα φυσιολογικά ή συμπεριφορικά χαρακτηριστικά τους. Αυτά τα χαρακτηριστικά είναι διακριτικά για κάθε άτομο και μπορούν να περιλαμβάνουν δακτυλικά αποτυπώματα, χαρακτηριστικά προσώπου, μοτίβα ίριδας, φωνητικά αποτυπώματα, αποτυπώματα παλάμης και βάδισμα. Τα βιομετρικά συστήματα καταγράφουν και αναλύουν τέτοια χαρακτηριστικά για να επαληθεύσουν την ταυτότητα ενός ατόμου ή να παραχωρήσουν πρόσβαση σε ασφαλείς περιοχές, συσκευές ή συστήματα στη βιομηχανία. Αν και υπάρχουν διάφορα βιομετρικά συστήματα που αναγνωρίζουν συγκεκριμένα χαρακτηριστικά (Dargan & Kumar, 2020).

2.4.1. Αναγνώριση προσώπου

Οι ξενοδοχειακές υπηρεσίες βασίζονται ουσιαστικά στην ιδέα της πώλησης στους καταναλωτές προσωρινής πρόσβασης σε εγκαταστάσεις παροχής υπηρεσιών σε ένα ξενοδοχείο, συμπεριλαμβανομένης της πρόσβασης σε χώρους για τους επισκέπτες (π.χ. δωμάτια, σουίτες, πισίνα, γυμναστήριο, επιχειρηματικό κέντρο) και υπηρεσιών για τους επισκέπτες, όπως φαγητό, ποτά και προϊόντα διαδικτύου ή ψυχαγωγίας. Η πρόσβαση και οι υπηρεσίες παρέχονται με βάση την πιστοποίηση του καταναλωτή και την υπόσχεση πληρωμής (Chathoth et al., 2014). Γενικά, όταν τελειώνουν οι υπηρεσίες, οι καταναλωτές πληρώνουν για την πρόσβαση/τις υπηρεσίες και κάνουν check-out. Ενώ αυτό το παραδοσιακό μοντέλο

υπηρεσιών παρέμεινε ουσιαστικά αμετάβλητο τα τελευταία 50 χρόνια, οι σημερινές κοινωνικές δυναμικές θέτουν διάφορες προκλήσεις στα ξενοδοχεία, όπως η ανάγκη μείωσης της απάτης και αύξησης της ασφάλειας των καταναλωτών, η αυξανόμενη ζήτηση των καταναλωτών για εξατομικευμένες υπηρεσίες και η ανάπτυξη διαδικτυακών πλατφορμών όπου οι καταναλωτές μπορούν να εκφράσουν την άποψή τους σχετικά με τις εμπειρίες τους από τις υπηρεσίες (Nusair et al., 2013).

Αυτό το όλο και πιο περίπλοκο περιβάλλον προκάλεσε μια πρόσφατη αλλαγή παραδείγματος στις ξενοδοχειακές υπηρεσίες, σύμφωνα με την οποία οι εμπειρίες των καταναλωτών πρέπει να είναι απρόσκοπτες. Ωστόσο, λόγω των εμποδίων που δημιουργεί, η αρχική πιστοποίηση των επισκεπτών που φτάνουν στο κατάλυμα αποτελεί σημαντικό εμπόδιο για μια απρόσκοπτη εμπειρία εξυπηρέτησης. Οι καταναλωτές που φτάνουν πρέπει να υποβληθούν σε μια αρχική υποχρεωτική διαδικασία πιστοποίησης και εγγύησης πληρωμής, χωρίς την οποία δεν μπορεί να γίνει το check-in και η επακόλουθη πρόσβαση στον χώρο των επισκεπτών. Η πιστοποίηση είναι ιδιαίτερα κρίσιμη, καθώς αποτελεί τη βάση για την επαναλαμβανόμενη πρόσβαση του επισκέπτη στο δωμάτιό του και την πληρωμή για διάφορες υπηρεσίες καθ' όλη τη διάρκεια της διαμονής του (Kim, 2016).

Αυτή η διαδικασία επιβραδύνεται από παραδοσιακές εργασίες, όπως η ανάκτηση κρατήσεων, η λήψη εξουσιοδότησης από μια μέθοδο πληρωμής για τυχόν επιπλέον χρεώσεις, η εγγραφή καρτών-κλειδιών και η παροχή πληροφοριών σχετικά με το κατάλυμα (π.χ. ο δρόμος προς το δωμάτιο, ο κωδικός πρόσβασης στο Wi-Fi και διάφορες πληροφορίες μάρκετινγκ). Τέτοιες διαδικασίες μπορεί να επιβραδυνθούν περαιτέρω σε περιπτώσεις όπου πολλοί επισκέπτες φτάνουν ταυτόχρονα στο κατάλυμα, όπου μεταξύ των επισκεπτών υπάρχουν τόσο τακτικοί όσο και σπάνιοι ταξιδιώτες με διαφορετικό βαθμό εξοικείωσης με το κατάλυμα ή τις διαδικασίες check-in, κατά τη διάρκεια μη κανονικών λειτουργιών (π.χ. κακές καιρικές συνθήκες που προκαλούν ακυρώσεις πτήσεων) ή όταν ένα ξενοδοχείο έχει έλλειψη προσωπικού ή οι υπάλληλοι της ρεσεψιόν δεν είναι επαρκώς εκπαιδευμένοι λόγω της εναλλαγής προσωπικού (Farrell, 2016).

Για να αντισταθμιστεί αυτό, έχουν αναπτυχθεί πολλαπλά συστήματα, μεταξύ των οποίων το FRS φαίνεται να αντιμετωπίζει κατάλληλα τις τρέχουσες προκλήσεις πιστοποίησης, μειώνοντας ταυτόχρονα τα σημεία συμφόρησης στην εξυπηρέτηση. Το FRS έχει αναπτυχθεί

για να διευκολύνει εργασίες παρόμοιες με την πιστοποίηση σε ξενοδοχεία, ώστε να αυξάνεται η ακρίβεια της πιστοποίησης των ταξιδιωτών και να μειώνονται τα σημεία συμφόρησης σε ευαίσθητους τομείς, όπως το check-in στα αεροδρόμια, οι περιοχές ελέγχου μετανάστευσης και η βελτίωση της ασφάλειας (Farrell, 2016).

Τα FRS θα μπορούσαν να διευκολύνουν τη γρήγορη και λιγότερο παρεμβατική αυτόματη πιστοποίηση, εξασφαλίζοντας παράλληλα χαμηλό ποσοστό σφάλματος. Επιπλέον, η τεχνολογία αναγνώρισης προσώπου είναι επίσης διαθέσιμη σε ορισμένα smartphone και εφαρμογές ιστού. Έτσι, τα FRS μπορούν να χρησιμοποιηθούν για το σχεδιασμό νέων μοντέλων ξενοδοχειακών υπηρεσιών, τα οποία συνδυάζουν τη βιομετρική + βιογραφική αυτόματη πιστοποίηση και τα μοντέλα αυτοεξυπηρέτησης για τη βελτιστοποίηση της ροής των καταναλωτών μέσω των παραδοσιακών διαδικασιών που εξακολουθούν να κυριαρχούν στις ξενοδοχειακές υπηρεσίες. Το σύστημα αναγνώρισης προσώπου είναι ένα εξελιγμένο βιομετρικό σύστημα που αναλύει και αναγνωρίζει άτομα με βάση τα χαρακτηριστικά του προσώπου τους (Taskiran et al., 2020).

Η βιομετρική τεχνολογία που χρησιμοποιείται στα συστήματα αναγνώρισης προσώπου βοηθά σε προοδευτικές διαδικασίες για την ανίχνευση, τη λήψη και την επεξεργασία των χαρακτηριστικών του προσώπου των ατόμων, όπως το μέγεθος και το σχήμα των ματιών, της μύτης, του στόματος και άλλων διακριτικών παραγόντων. Τα μοναδικά χαρακτηριστικά του προσώπου τους μετατρέπονται στη συνέχεια σε ένα ψηφιακό πρότυπο ή «αποτύπωμα προσώπου» για σκοπούς σύγκρισης και αναγνώρισης. Το σύστημα ανιχνεύει και εντοπίζει ανθρώπινα πρόσωπα σε εικόνες ή ροές βίντεο εντός εμβέλειας. Μόλις ανιχνευθούν τα πρόσωπα, χορηγούνται οι άδειες (Oloyede et al., 2020).

Η τεχνολογία αναγνώρισης προσώπου έχει καταστεί βάση στον κλάδο του τουρισμού και της φιλοξενίας, μεταρρυθμίζοντας τον τρόπο με τον οποίο ο κλάδος διαχειρίζεται την ασφάλεια, εξατομικεύει τις εμπειρίες των επισκεπτών και εξορθολογίζει τις λειτουργίες του (Gangwar & Reddy, 2023). Η τεχνολογία αναγνώρισης προσώπου χρησιμοποιείται για σκοπούς σύγκρισης και ταυτοποίησης στον κλάδο του τουρισμού και της φιλοξενίας. Με την ανάλυση των χαρακτηριστικών του προσώπου των ατόμων, όπως τα μάτια, η μύτη και το στόμα, η αναγνώριση προσώπου επιτρέπει μια σειρά εφαρμογών στον κλάδο του τουρισμού και της φιλοξενίας, όπως διαδικασίες check-in, έλεγχος πρόσβασης σε δωμάτια και

εγκαταστάσεις ξενοδοχείων και εξατομικευμένες αλληλεπιδράσεις με τους επισκέπτες στον κλάδο (Oloyede et al., 2020).

Η τεχνολογία επιτρέπει στον κλάδο να συλλέγει πολύτιμα δεδομένα σχετικά με τις προτιμήσεις και τις συμπεριφορές των επισκεπτών ή των φιλοξενούμενων, επιτρέποντας στοχευμένες στρατηγικές μάρκετινγκ και εξατομίκευση των υπηρεσιών. Όταν αυτή η τεχνολογία υιοθετείται με υπευθυνότητα και ηθική, ο τουριστικός και ξενοδοχειακός κλάδος μπορεί να αναβαθμίσει τις υπηρεσίες που προσφέρει, διατηρώντας παράλληλα τα υψηλότερα πρότυπα ιδιωτικότητας και ασφάλειας των επισκεπτών. Λόγω της ικανότητάς της να ενισχύει τα μέτρα ασφαλείας στον τουριστικό και ξενοδοχειακό κλάδο, αποτρέποντας την παράνομη πρόσβαση σε περιορισμένες περιοχές και ελαχιστοποιώντας τον κίνδυνο κλοπής ή βανδαλισμού, η τεχνολογία αναγνώρισης προσώπου εξασφαλίζει ένα ασφαλέστερο περιβάλλον τόσο για τους επισκέπτες όσο και για τους υπαλλήλους (Anderson, et. al., 2025).

Αν και η χρήση του FRS στα ξενοδοχεία είναι χαμηλή, οι σημερινοί προμηθευτές λογισμικού για ξενοδοχεία ενσωματώνουν όλο και περισσότερο τη βιομετρική πιστοποίηση στα τρέχοντα προϊόντα τους. Για παράδειγμα, η Agilysys έχει αναπτύξει μια νέα πλατφόρμα που αναγνωρίζει τους καταναλωτές καθώς εισέρχονται σε ένα ξενοδοχείο και παρέχει πληροφορίες για αυτούς τους καταναλωτές στο προσωπικό της ρεσεψιόν (Burt 2018). Γενικά, ένας επισκέπτης μπορεί να αναγνωριστεί μετά την παροχή μιας εικόνας προσώπου σε ένα FRS, η οποία μαζί με τις βιογραφικές πληροφορίες του χρήστη μπορεί να χρησιμοποιηθεί για αυτόματη πιστοποίηση. Μετά την αρχική εγγραφή, ένας επισκέπτης θα μπορούσε να παρακολουθείται αυτόματα μεταξύ άλλων επισκεπτών (π.χ. σε ένα πολυσύχναστο λόμπι) και στη συνέχεια να πιστοποιείται για σκοπούς πρόσβασης και εξυπηρέτησης. Ενώ τα FRS έχουν αποδειχθεί πολλά υποσχόμενα στα περιβάλλοντα όπου έχουν εφαρμοστεί, μπορεί επίσης να έχουν αρνητικές συνειρμούς. Για παράδειγμα, τα FRS μπορούν να χαρακτηρίζονται από αποτυχία εγγραφής (π.χ. ένας χρήστης δεν μπορεί να εγγραφεί λόγω ακατάλληλης ανάγνωσης μιας εικόνας προσώπου) και εγγενή σφάλματα που σχετίζονται με τον αλγόριθμο αποδοχής/απόρριψης (Morosan, 2012). Επιπλέον, τα βιομετρικά συστήματα μπορεί γενικά να προκαλέσουν αρνητικά συναισθήματα στους χρήστες, λόγω της προηγούμενης χρήσης τους στην επιβολή του νόμου, σε κυβερνητικές δραστηριότητες ή πιθανής ασυμφωνίας με τις πεποιθήσεις ενός ατόμου (Jain et al., 2011).

2.4.2. Συστήματα αναγνώρισης δακτυλικών αποτυπωμάτων

Τα συστήματα αναγνώρισης δακτυλικών αποτυπωμάτων χρησιμοποιούν εξειδικευμένους σαρωτές δακτυλικών αποτυπωμάτων για να καταγράψουν και να αναλύσουν τα μοναδικά μοτίβα των δακτύλων ενός ατόμου. Η τεχνολογία αναγνώρισης δακτυλικών αποτυπωμάτων χρησιμοποιεί τα μοναδικά μοτίβα των κορυφογραμμών και των κοιλάδων που υπάρχουν στα δάχτυλα ενός ατόμου για να επαληθεύσει την ταυτότητά του. Αυτά τα μοτίβα καταγράφονται χρησιμοποιώντας είτε οπτικούς αισθητήρες, είτε χωρητικούς αισθητήρες, είτε αισθητήρες υπερήχων. Μόλις ληφθεί η εικόνα του δακτυλικού αποτυπώματος, το σύστημα εξάγει συγκεκριμένα χαρακτηριστικά από το δάχτυλο. Η καταγεγραμμένη εικόνα παρέχει μια λεπτομερή αναπαράσταση των μοναδικών μοτίβων κορυφογραμμών και κοιλάδων στην άκρη του δακτύλου. Εάν το καταγεγραμμένο δακτυλικό αποτύπωμα ταιριάζει στενά με ένα από τα αποθηκευμένα πρότυπα εντός ενός αποδεκτού ορίου, χορηγείται η πιστοποίηση (Ye et al., 2020).

Η αναγνώριση δακτυλικών αποτυπωμάτων αποτελεί μια βασική βιομετρική τεχνολογία στον τομέα του τουρισμού και της φιλοξενίας, προσφέροντας μια πληθώρα βοηθημάτων για την ασφάλεια, την ευκολία και την λειτουργική αποδοτικότητα (Boo & Chua, 2022). Η τεχνολογία χρησιμοποιεί τα μοναδικά μοτίβα κορυφογραμμών και κοιλάδων που υπάρχουν στα δάχτυλα ενός ατόμου για να επαληθεύσει την ταυτότητά του κάθε φορά που επισκέπτεται τον τομέα του τουρισμού και της φιλοξενίας. Στον τουρισμό και τη φιλοξενία, η αναγνώριση δακτυλικών αποτυπωμάτων βρίσκει ποικίλες εφαρμογές, όπως τον έλεγχο πρόσβασης σε δωμάτια ξενοδοχείων, ντουλάπια και ασφαλείς περιοχές, καθώς και την παρακολούθηση της παρουσίας του προσωπικού και το σύστημα διαχείρισης χρόνου (Moisa & Michopoulou, 2022).

Παρέχει μια εξαιρετικά ακριβή και αξιόπιστη μέθοδο αναγνώρισης ατόμων όταν επισκέπτονται τον κλάδο. Η υψηλή ακρίβειά της εξασφαλίζει την αποτελεσματική πρόληψη της μη εξουσιοδοτημένης πρόσβασης, προστατεύοντας τα αντικείμενα των επισκεπτών και τις ευαίσθητες πληροφορίες που αποθηκεύονται σε ασφαλείς περιοχές. Η ευκολία της αναγνώρισης δακτυλικών αποτυπωμάτων επεκτείνεται τόσο στους επισκέπτες όσο και στο προσωπικό, επιτρέποντας την απρόσκοπτη πρόσβαση χωρίς την ανάγκη φυσικών κλειδιών ή

καρτών-κλειδιών (Ratnoday et al., 2025). Αυτό όχι μόνο εξαλείφει τον κίνδυνο απώλειας ή απώλειας κλειδιών, αλλά και απλοποιεί τη διαχείριση της πρόσβασης για το προσωπικό, εξασφαλίζοντας ότι μόνο εξουσιοδοτημένο προσωπικό εισέρχεται σε περιορισμένες ζώνες. Η ενσωμάτωση με συστήματα χρόνου και παρουσίας ενισχύει περαιτέρω την αποδοτικότητα, αυτοματοποιώντας την παρακολούθηση της παρουσίας του προσωπικού. Οι υπάλληλοι μπορούν εύκολα να χρονομετρήσουν την είσοδο και την έξοδο τους χρησιμοποιώντας τα δακτυλικά τους αποτυπώματα, εξαλείφοντας τις χειροκίνητες μεθόδους χρονομέτρησης και βελτιώνοντας την ακρίβεια στην επεξεργασία των μισθών. Η τεχνολογία αναγνώρισης δακτυλικών αποτυπωμάτων προσφέρει σημαντικά πλεονεκτήματα για τον τουρισμό και τον κλάδο της φιλοξενίας, συμπεριλαμβανομένης της ενισχυμένης ασφάλειας, της ευκολίας και της λειτουργικής αποδοτικότητας. Όταν αυτή η τεχνολογία υιοθετηθεί σωστά, ο κλάδος μπορεί να αναβαθμίσει τις υπηρεσίες που προσφέρει, διατηρώντας παράλληλα τα υψηλότερα πρότυπα ιδιωτικότητας των επισκεπτών και των υπαλλήλων (Srinivasan, 2018).

2.4.3. Αναγνώριση ίριδας

Το σύστημα αναγνώρισης ίριδας αποτελεί μια πρωτοποριακή βιομετρική λύση, προσφέροντας απaráμιλλη ακρίβεια, ευκολία και ασφάλεια για διάφορες εφαρμογές. Με τη σάρωση των μοναδικών μοτίβων στο χρωματιστό μέρος του ματιού (ίριδα), η αναγνώριση ίριδας παρέχει μια αξιόπιστη μέθοδο αναγνώρισης ατόμων. Φημισμένη για την εξαιρετική ακρίβεια και αξιοπιστία της, η αναγνώριση ίριδας ξεπερνά πολλές άλλες βιομετρικές μεθόδους. Τα πολύπλοκα και εξαιρετικά μοναδικά μοτίβα της ίριδας εξασφαλίζουν αξιόπιστη πιστοποίηση, καθιστώντας τα συστήματα αναγνώρισης ίριδας ιδανικά για τον έλεγχο πρόσβασης σε βιομηχανικά περιβάλλοντα (Musa et al., 2022).

Η τεχνολογία αναγνώρισης ίριδας προσφέρει ενισχυμένα μέτρα ασφαλείας για εγκαταστάσεις, ιδιαίτερα σε VIP περιοχές ή ευαίσθητες τοποθεσίες, συμβάλλοντας στην εξατομικευμένη εμπειρία των επισκεπτών στον τομέα της φιλοξενίας. Με τη συλλογή και αποθήκευση βιομετρικών δεδομένων ίριδας, τα ξενοδοχεία μπορούν να προσαρμόσουν τις υπηρεσίες και τις ανέσεις τους με βάση τις ατομικές προτιμήσεις. Οι επισκέπτες που είναι εγγεγραμμένοι σε ένα σύστημα αναγνώρισης ίριδας μπορούν να επωφεληθούν από ταχύτερες διαδικασίες check-in, εξατομικευμένες ρυθμίσεις δωματίου ή αποκλειστική πρόσβαση σε

εγκαταστάσεις VIP. Η τεχνολογία αναγνώρισης ίριδας προσφέρει σημαντικά πλεονεκτήματα για τον τουρισμό και τον κλάδο της φιλοξενίας, όπως απaráμιλλη ακρίβεια, ευκολία και ασφάλεια. Με την υιοθέτηση αυτής της τεχνολογίας, ο κλάδος μπορεί να βελτιώσει την εμπειρία των επισκεπτών, να ενισχύσει τα μέτρα ασφαλείας και να απλοποιήσει τις λειτουργικές διαδικασίες, προωθώντας τελικά ένα ασφαλέστερο, αποδοτικότερο και πιο εξατομικευμένο περιβάλλον φιλοξενίας (Musa et al., 2022).

2.4.4. Αναγνώριση φωνής

Σύστημα Το σύστημα αναγνώρισης φωνής, γνωστό και ως σύστημα αναγνώρισης ομιλίας ή βιομετρικά στοιχεία φωνής, είναι ένα εξελιγμένο σύστημα που επιτρέπει την αναγνώριση και επεξεργασία φωνητικών προτύπων στην ομιλούμενη γλώσσα για την εκτέλεση διάφορων εργασιών και λειτουργιών. Τα φωνητικά μοτίβα περιλαμβάνουν τον τόνο, την χροιά και την προφορά. Επιτρέπει στους υπολογιστές ή τις συσκευές να κατανοούν, να ερμηνεύουν και να ανταποκρίνονται σε προφορικές εντολές ή ερωτήσεις από τους χρήστες. Τα συστήματα αναγνώρισης φωνής βρίσκουν ευρεία εφαρμογή σε διάφορους κλάδους, όπως οι τηλεπικοινωνίες, η αυτοκινητοβιομηχανία, η υγειονομική περίθαλψη, η χρηματοοικονομική και η φιλοξενία (Βασιλείου, Ηρειώτης & Μπάλιος 2009).

Η τεχνολογία αναγνώρισης φωνής αναδεικνύεται ως ένα βασικό εργαλείο στον κλάδο του τουρισμού και της φιλοξενίας, φέρνοντας επανάσταση στις αλληλεπιδράσεις με τους επισκέπτες, την παροχή υπηρεσιών και τα μέτρα ασφαλείας (Štilić et al., 2023). Ειδικά στον κλάδο του τουρισμού και της φιλοξενίας, η τεχνολογία αναγνώρισης φωνής χρησιμοποιείται για διάφορους σκοπούς. Η αναγνώριση φωνής προσφέρει μια απρόσκοπτη και εξατομικευμένη εμπειρία στους επισκέπτες, ενώ παράλληλα βελτιώνει την λειτουργική αποδοτικότητα του κλάδου. Η αναγνώριση φωνής επιτρέπει την απρόσκοπτη πιστοποίηση μέσω τηλεφώνου, απλοποιώντας τις διαδικασίες κράτησης και τις ερωτήσεις. Οι επισκέπτες μπορούν να επαληθεύσουν την ταυτότητά τους χωρίς κόπο, εξαλείφοντας την ανάγκη για δυσκίνητες διαδικασίες επαλήθευσης και ενισχύοντας τη συνολική ικανοποίηση. Επιπλέον, διευκολύνονται οι εξατομικευμένες αλληλεπιδράσεις, καθώς τα συστήματα αναγνώρισης φωνής αναγνωρίζουν τους επισκέπτες που επιστρέφουν, επιτρέποντας στο προσωπικό να έχει πρόσβαση σε πληροφορίες προφίλ και να προσαρμόζει τις υπηρεσίες ανάλογα. Οι βοηθοί

ενεργοποίησης φωνής που χρησιμοποιούνται στα δωμάτια των επισκεπτών ή στους κοινόχρηστους χώρους δίνουν τη δυνατότητα στους επισκέπτες να ελέγχουν τις ρυθμίσεις του δωματίου, να έχουν πρόσβαση σε πληροφορίες ή να ζητούν υπηρεσίες μέσω διαισθητικών φωνητικών εντολών. Αυτή η αλληλεπίδραση χωρίς χρήση χεριών δημιουργεί ένα φιλικό προς τον χρήστη περιβάλλον, προωθώντας την εμπλοκή και την ικανοποίηση των επισκεπτών. Η τεχνολογία αναγνώρισης φωνής ικανοποιεί τις διαφορετικές ανάγκες των επισκεπτών, υποστηρίζοντας πολλές γλώσσες (Tanrisever, et. al., 2024).

Ο τουριστικός και ξενοδοχειακός κλάδος μπορεί να προσφέρει υπηρεσίες ενεργοποιημένες με φωνή σε διάφορες γλώσσες, εξασφαλίζοντας απρόσκοπτη επικοινωνία για τους διεθνείς επισκέπτες και προωθώντας την ένταξη, η οποία βελτιώνει τη συνολική εμπειρία των επισκεπτών και διευκολύνει την αποτελεσματική επικοινωνία πέρα από τα πολιτισμικά όρια. Η διαφανής επικοινωνία με τους επισκέπτες σχετικά με τις πρακτικές χειρισμού δεδομένων και η λήψη συγκατάθεσης για τη συλλογή φωνητικών δεδομένων ενισχύει την εμπιστοσύνη και διασφαλίζει τη συμμόρφωση με τους κανονισμούς περί απορρήτου. Η τεχνολογία αναγνώρισης φωνής αποτελεί μια μετασχηματιστική δύναμη στον κλάδο του τουρισμού και της φιλοξενίας, ενισχύοντας τις αλληλεπιδράσεις με τους επισκέπτες, την λειτουργική αποδοτικότητα και τα μέτρα ασφαλείας. Όταν αυτή η τεχνολογία αξιοποιείται σωστά, ο κλάδος μπορεί να δημιουργήσει μια απρόσκοπτη και εξατομικευμένη εμπειρία που ενισχύει την αφοσίωση και την ικανοποίηση των επισκεπτών (Tanrisever, et. al., 2024).

2.4.5. Αναγνώριση φλεβών παλάμης

Το σύστημα αναγνώρισης φλεβών της παλάμης είναι ένα βιομετρικό σύστημα που καταγράφει και αναλύει τα μοναδικά μοτίβα των φλεβών κάτω από την επιφάνεια του δέρματος στην παλάμη του χεριού. Σε αντίθεση με το σύστημα αναγνώρισης δακτυλικών αποτυπωμάτων, το οποίο μπορεί να απαιτεί φυσική επαφή με έναν αισθητήρα ή μια επιφάνεια, το σύστημα αναγνώρισης φλεβών της παλάμης δεν απαιτεί καμία άμεση επαφή. Οι επισκέπτες απλά πρέπει να τοποθετήσουν την παλάμη τους κοντά σε ένα σαρωτή, καθιστώντας το μια ιδανική λύση για εφαρμογές όπου η υγιεινή είναι προτεραιότητα. Τα συστήματα αναγνώρισης φλεβών της παλάμης προσφέρουν υψηλό επίπεδο ακρίβειας και ασφάλειας στην αναγνώριση ατόμων. Τα μοτίβα των φλεβών κάτω από την επιφάνεια του δέρματος στην παλάμη είναι

μοναδικά για κάθε άτομο και είναι δύσκολο να αναπαραχθούν ή να παραποιηθούν. Αυτό καθιστά τα συστήματα αναγνώρισης φλεβών της παλάμης εξαιρετικά αξιόπιστα για τον έλεγχο πρόσβασης, την πιστοποίηση επισκεπτών και τα ασφαλή συστήματα πληρωμών (Wu et al., 2019).

Η τεχνολογία αναγνώρισης φλεβών της παλάμης έχει πολλαπλές εφαρμογές στον τομέα του τουρισμού και της φιλοξενίας. Χρησιμοποιείται για διάφορους σκοπούς, όπως διαδικασίες check-in, ενοικίαση θυρίδων, εγγραφή σε προγράμματα πιστότητας και ασφαλείς συναλλαγές πληρωμών. Δεδομένου ότι η τεχνολογία αναγνώρισης φλεβών της παλάμης είναι ιδιαίτερα κατάλληλη για εφαρμογές που απαιτούν μια λύση χωρίς επαφή και υγιεινή, παρέχει μια ιδανική λύση για εφαρμογές στον τομέα του τουρισμού και της φιλοξενίας, όπως ο έλεγχος πρόσβασης στις εισόδους ξενοδοχείων, η πιστοποίηση επισκεπτών και τα ασφαλή συστήματα πληρωμών σε εστιατόρια. Τα συστήματα αναγνώρισης φλεβών της παλάμης μπορούν να ενσωματωθούν απρόσκοπτα στην υπάρχουσα υποδομή των ξενοδοχειακών μονάδων. Αυτό περιλαμβάνει την ενσωμάτωση με συστήματα διαχείρισης ακινήτων (PMS), συστήματα ελέγχου πρόσβασης, τερματικά σημείων πώλησης (POS) και πλατφόρμες προγραμμάτων πιστότητας. Τα συστήματα αναγνώρισης φλεβών της παλάμης στον τομέα του τουρισμού και της φιλοξενίας πρέπει να συμμορφώνονται με αυστηρά πρότυπα απορρήτου και ασφάλειας για την προστασία των δεδομένων των επισκεπτών (Anderson, et. al., 2025).

Ο κλάδος πρέπει να εφαρμόσει ισχυρά μέτρα για την προστασία των βιομετρικών δεδομένων των φλεβών της παλάμης, συμπεριλαμβανομένης της κρυπτογράφησης, της ασφαλούς αποθήκευσης και των ελέγχων πρόσβασης. Τα ξενοδοχεία και τα θέρετρα μπορούν να αξιοποιήσουν την αναγνώριση των φλεβών της παλάμης για να ενισχύσουν τα μέτρα ασφάλειας, να βελτιστοποιήσουν τις λειτουργίες τους και να προσφέρουν μια απρόσκοπτη και βολική εμπειρία στους επισκέπτες (Wu et al., 2019).

2.4.6. Συστήματα αναγνώρισης βάδισης

Τα συστήματα αναγνώρισης βάδισης αναλύουν τον μοναδικό τρόπο με τον οποίο περπατούν τα άτομα, συμπεριλαμβανομένου του μήκους του διασκελισμού, της ταχύτητας και του ρυθμού περπατήματος. Αν και χρησιμοποιείται λιγότερο συχνά σε σύγκριση με άλλες

βιομετρικές μεθόδους, όπως η αναγνώριση προσώπου ή η αναγνώριση δακτυλικών αποτυπωμάτων, η αναγνώριση βάδισης προσφέρει ένα ξεχωριστό πλεονέκτημα, καθώς δεν απαιτεί φυσική επαφή με αισθητήρα ή επιφάνεια (Álvarez-Aparicio et al., 2022). Τα συστήματα αναγνώρισης βάδισης μπορούν να χρησιμοποιηθούν για την παρακολούθηση και την επιτήρηση της ασφάλειας εντός των εγκαταστάσεων των ξενοδοχείων. Αναλύοντας τα μοτίβα βάδισης των ατόμων που καταγράφονται από τις κάμερες παρακολούθησης, τα ξενοδοχεία μπορούν να εντοπίζουν και να παρακολουθούν ύποπτη συμπεριφορά, να παρακολουθούν την κίνηση του πλήθους σε δημόσιους χώρους, όπως λόμπι ή διάδρομοι, και να ενισχύουν τα συνολικά μέτρα ασφαλείας (Wang et al., 2018).

Η τεχνολογία αναγνώρισης βάδισης αναλύει τον μοναδικό τρόπο με τον οποίο περπατούν τα άτομα, συμπεριλαμβανομένου του μήκους του διασκελισμού, της ταχύτητας και του ρυθμού περπατήματος. Η αναγνώριση βάδισης μπορεί να χρησιμοποιηθεί για σκοπούς παρακολούθησης και επιτήρησης της ασφάλειας σε διάφορα περιβάλλοντα, όπως αεροδρόμια, σιδηροδρομικοί σταθμοί και δημόσιοι χώροι (Vaniya & Bharathi, 2016). Η τεχνολογία αναγνώρισης βάδισης μπορεί να χρησιμοποιηθεί για τον έλεγχο πρόσβασης σε ασφαλείς εγκαταστάσεις ή περιορισμένες περιοχές στη βιομηχανία. Τα ξενοδοχεία μπορούν να χρησιμοποιήσουν την τεχνολογία αναγνώρισης βάδισης ως μέρος των συστημάτων ελέγχου πρόσβασης για την ασφάλεια περιοχών με περιορισμένη πρόσβαση, όπως ζώνες αποκλειστικά για το προσωπικό, αποθήκες ή αίθουσες VIP. Αναλύοντας τα μοτίβα βάδισης του εξουσιοδοτημένου προσωπικού, το σύστημα μπορεί να παραχωρήσει πρόσβαση μόνο σε άτομα με αναγνωρισμένα μοτίβα βάδισης, ενισχύοντας τα μέτρα ασφαλείας (Álvarez-Aparicio et al., 2022).

Αναλύοντας τα μοτίβα βάδισης των τακτικών ή διακεκριμένων επισκεπτών, το προσωπικό μπορεί να λαμβάνει ειδοποιήσεις και να παρέχει εξατομικευμένες χαιρετισμούς ή υπηρεσίες κατά την άφιξή τους, ενισχύοντας την εμπειρία των επισκεπτών και προωθώντας την αφοσίωσή τους. Η τεχνολογία αναγνώρισης βάδισης μπορεί να συμβάλει στα συνολικά μέτρα ασφαλείας εντός των εγκαταστάσεων του ξενοδοχείου, παρακολουθώντας και εντοπίζοντας ύποπτα άτομα ή απόπειρες μη εξουσιοδοτημένης πρόσβασης. Τα ξενοδοχεία μπορούν να χρησιμοποιήσουν την τεχνολογία αναγνώρισης βάδισης για σκοπούς διαχείρισης του προσωπικού, όπως η παρακολούθηση των κινήσεων και της παρουσίας των εργαζομένων στον

κλάδο. Η τεχνολογία αναγνώρισης βάδισης θα μπορούσε ενδεχομένως να χρησιμοποιηθεί για τη συλλογή πληροφοριών σχετικά με τη συμπεριφορά και τις προτιμήσεις των επισκεπτών. Αναλύοντας τα μοτίβα βάδισης των επισκεπτών καθώς κινούνται στις εγκαταστάσεις του ξενοδοχείου, τα ξενοδοχεία μπορούν να αποκτήσουν πολύτιμα δεδομένα σχετικά με τη ροή της κυκλοφορίας, τις δημοφιλείς ανέσεις και τις περιοχές ενδιαφέροντος, επιτρέποντάς τους να βελτιστοποιήσουν τη διάταξη των εγκαταστάσεων, τις υπηρεσίες και τις προσφορές, ώστε να ανταποκρίνονται καλύτερα στις ανάγκες των επισκεπτών (Anderson, et. al., 2025).

2.5. Οφέλη της βιομετρικής τεχνολογίας στον τομέα του τουρισμού και της φιλοξενίας

Η βιομετρική τεχνολογία διαδραματίζει σημαντικό ρόλο στον τομέα του τουρισμού και της φιλοξενίας, καθώς ενισχύει την ασφάλεια παρέχοντας μια αποτελεσματική τεχνική αναγνώρισης και επαλήθευσης ταυτότητας με βάση ειδικά ανθρώπινα χαρακτηριστικά, όπως δακτυλικά αποτυπώματα, μοτίβα ή χαρακτηριστικά του προσώπου (Lehto et al., 2021). Η βιομετρική πιστοποίηση προσφέρει μια εξαιρετικά ασφαλή μέθοδο επαλήθευσης της ταυτότητας των επισκεπτών, των εργοδοτών και των εργαζομένων. Σε αντίθεση με τις παραδοσιακές μεθόδους πιστοποίησης, όπως οι κωδικό πρόσβασης ή οι ταυτότητες, τα βιομετρικά χαρακτηριστικά, όπως τα δακτυλικά αποτυπώματα ή τα χαρακτηριστικά του προσώπου, είναι μοναδικά για κάθε άτομο, γεγονός που τα καθιστά εξαιρετικά δύσκολο να πλαστογραφηθούν ή να επαναληφθούν. Αυτό βοηθά στην πρόληψη της κλοπής ταυτότητας και της απάτης, ιδίως σε κρίσιμους τομείς όπως η εγγραφή στο front office, όπου ανταλλάσσονται ευαίσθητες πληροφορίες. Η βιομετρική τεχνολογία ενσωματώνεται μερικές φορές σε υπάρχοντα μέτρα ασφαλείας, όπως συστήματα ελέγχου πρόσβασης και κάμερες παρακολούθησης, για την ενίσχυση της συνολικής ασφαλείας εντός της εγκατάστασης. Αυτή η ενσωμάτωση διασφαλίζει ότι μόνο εξουσιοδοτημένα άτομα έχουν πρόσβαση σε περιορισμένες περιοχές, μειώνοντας τον κίνδυνο κλοπής, καταστροφής ή άλλων παραβιάσεων ασφαλείας. Επιπλέον, η βιομετρική τεχνολογία επιτρέπει την ταχεία και ακριβή ταυτοποίηση των επισκεπτών σε διάφορα σημεία επαφής (Ratnoday et al., 2025).

Μειώνει τους χρόνους αναμονής και τις ουρές σε διάφορα τμήματα, όπως check-in, εγγραφές και εισόδους, γεγονός που οδηγεί σε βελτίωση της ικανοποίησης των πελατών και της λειτουργικής αποδοτικότητας στον τομέα του τουρισμού και της φιλοξενίας. Ομοίως, η βιομετρική τεχνολογία εξαλείφει την ανάγκη για φυσικά έγγραφα, όπως διαβατήρια, κάρτες επιβίβασης και κλειδιά ξενοδοχείων, απλοποιώντας τη διαδικασία του ταξιδιού και μειώνοντας τον κίνδυνο απώλειας ή κλοπής. Εξαλείφοντας την ανάγκη για χειροκίνητες διαδικασίες επαλήθευσης και φυσικά έγγραφα, η βιομετρική τεχνολογία μειώνει σημαντικά τους χρόνους αναμονής και τις ουρές, ειδικά κατά τις περιόδους αιχμής των ταξιδιών (Moisa & Michoroulou, 2022).

Αυτό οδηγεί σε ομαλότερες λειτουργίες και βελτιωμένη αποδοτικότητα για ξενοδοχεία, αεροδρόμια και άλλα καταλύματα φιλοξενίας. Οι μικρότεροι χρόνοι αναμονής και οι απρόσκοπτες διαδικασίες check-in συμβάλλουν σε υψηλότερα επίπεδα ικανοποίησης των πελατών. Οι επισκέπτες εκτιμούν την ευκολία και την ταχύτητα που προσφέρει η βιομετρική ταυτοποίηση, η οποία βελτιώνει τη συνολική εμπειρία τους κατά τη διάρκεια της διαμονής τους. Ελαχιστοποιώντας τις καθυστερήσεις και τις απογοητεύσεις που συνδέονται με τις παραδοσιακές διαδικασίες check-in, τα ξενοδοχεία και άλλες τουριστικές επιχειρήσεις μπορούν να αφήσουν θετική εντύπωση στους επισκέπτες, ενθαρρύνοντας τις επαναλαμβανόμενες επισκέψεις και τις θετικές κριτικές. Στο ίδιο πνεύμα, η βιομετρική τεχνολογία που ενσωματώνεται στην ανάλυση δεδομένων στον τομέα του τουρισμού και της φιλοξενίας βοηθά στην απόκτηση πληροφοριών σχετικά με τη συμπεριφορά, τις προτιμήσεις και τα δημογραφικά στοιχεία των ταξιδιωτών (Morosan, 2010).

Αυτό επιτρέπει στις επιχειρήσεις τουρισμού και φιλοξενίας να προσαρμόσουν τις στρατηγικές μάρκετινγκ και τις προσφορές τους πιο αποτελεσματικά. Για παράδειγμα, η τεχνολογία αναγνώρισης προσώπου μπορεί να διευκολύνει την υποδοχή των επισκεπτών με το όνομά τους κατά την άφιξη και να προσαρμόσει τις υπηρεσίες με βάση τις προτιμήσεις τους, ώστε να κάνουν τη διαμονή ή το ταξίδι τους αξέχαστο. Αναλύοντας τα βιομετρικά δεδομένα μαζί με άλλες πληροφορίες για τους επισκέπτες, όπως το ιστορικό κρατήσεων, τα μοτίβα δαπανών και τα σχόλια, οι επιχειρήσεις μπορούν να αποκτήσουν πολύτιμες πληροφορίες για τη συμπεριφορά και τις προτιμήσεις των ταξιδιωτών. Η τεχνολογία αναγνώρισης προσώπου μπορεί επίσης να παρακολουθεί τις κινήσεις των επισκεπτών σε όλη την ιδιοκτησία και τον

τρόπο με τον οποίο οι επισκέπτες αλληλεπιδρούν με διαφορετικές περιοχές του αξιοθέατου, του ξενοδοχείου ή του θέρετρου. Οι επιχειρήσεις τουρισμού και φιλοξενίας μπορούν να προσαρμόσουν τις στρατηγικές μάρκετινγκ τους για να στοχεύσουν πιο αποτελεσματικά συγκεκριμένα τμήματα επισκεπτών. Για παράδειγμα, εάν η ανάλυση δεδομένων αποκαλύψει ότι ένα σημαντικό μέρος των επισκεπτών απολαμβάνει υπηρεσίες σπα, το ξενοδοχείο μπορεί να δημιουργήσει στοχευμένες καμπάνιες μάρκετινγκ που προωθούν πακέτα σπα σε αυτούς τους επισκέπτες, αυξάνοντας έτσι την πιθανότητα επιπλέον πωλήσεων και επαναλαμβανόμενων κρατήσεων στις εγκαταστάσεις του. Η βιομετρική τεχνολογία βελτιστοποιεί τις διαδικασίες διαχείρισης του προσωπικού στον τομέα του τουρισμού και της φιλοξενίας (Dijmărescu, et. al., 2022).

Με την εφαρμογή βιομετρικών συστημάτων χρόνου και παρουσίας, ο κλάδος μπορεί να παρακολουθεί με ακρίβεια τις ώρες εργασίας των υπαλλήλων. Τα συστήματα ελέγχου πρόσβασης που χρησιμοποιούν βιομετρική τεχνολογία διασφαλίζουν ότι μόνο τα εξουσιοδοτημένα μέλη του προσωπικού έχουν πρόσβαση σε περιορισμένες περιοχές εντός της εγκατάστασης. Κατά συνέπεια, αυτά τα συστήματα προσφέρουν μια πιο αξιόπιστη και ασφαλή μέθοδο παρακολούθησης της παρουσίας σε σύγκριση με τις παραδοσιακές μεθόδους, όπως οι κάρτες διάτρησης ή τα χειρόγραφα φύλλα εγγραφής, τα οποία είναι εκτεθειμένα σε χειραγώγηση ή δόλιες πρακτικές. Τα συστήματα που απαιτούν από τους υπαλλήλους να επαληθεύουν την ταυτότητά τους χρησιμοποιώντας τα βιομετρικά τους δεδομένα για την είσοδο και την έξοδο, μπορούν να αποτρέψουν την κλοπή χρόνου και να διασφαλίσουν ότι οι υπάλληλοι αμείβονται με ακρίβεια για τις ώρες εργασίας τους (Anderson, et. al., 2025).

Τα συστήματα χρόνου και παρουσίας που χρησιμοποιούν βιομετρική τεχνολογία απλοποιούν επίσης τις διοικητικές εργασίες που σχετίζονται με την επεξεργασία των μισθών, καθώς καταγράφουν και αποθηκεύουν αυτόματα τα δεδομένα παρουσίας σε ένα κεντρικό σύστημα, μειώνοντας την ανάγκη για χειροκίνητη εισαγωγή και συμφωνία δεδομένων. Υπάρχει μια αυξανόμενη ζήτηση για ανέπαφες λύσεις στον τομέα του τουρισμού και της φιλοξενίας. Η βιομετρική τεχνολογία αυθεντικοποίησης προσφέρει μια ανέπαφη εναλλακτική λύση στις παραδοσιακές μεθόδους ταυτοποίησης, μειώνοντας τον κίνδυνο μετάδοσης ιών μεταξύ των επισκεπτών και του προσωπικού. Οι ανέπαφες βιομετρικές λύσεις, όπως η αναγνώριση προσώπου ή η σάρωση της ίριδας, επιτρέπουν στους επισκέπτες να επαληθεύουν

την ταυτότητά τους χωρίς φυσική επαφή, συμβάλλοντας σε ένα ασφαλέστερο και πιο υγιεινό περιβάλλον. Ως εκ τούτου, με την εφαρμογή της βιομετρικής πιστοποίησης, τα ξενοδοχεία και τα θέρετρα αποδεικνύουν τη δέσμευσή τους να δίνουν προτεραιότητα στην ασφάλεια και την ευημερία των επισκεπτών. Αυτό μπορεί να ενισχύσει την εμπιστοσύνη στο κατάλυμα και να ενθαρρύνει τους επισκέπτες να επιλέγουν καταλύματα που δίνουν προτεραιότητα στα πρότυπα υγείας και υγιεινής (Anderson, et. al., 2025).

2.5.1. Προκλήσεις χρήσης βιομετρικών δεδομένων

Τα βιομετρικά δεδομένα, όπως τα δακτυλικά αποτυπώματα, οι σαρώσεις προσώπου και η αναγνώριση ίριδας, εγείρουν σημαντικά ζητήματα προστασίας της ιδιωτικής ζωής (Singh et al., 2021). Σε αντίθεση με τους κωδικούς πρόσβασης ή τις ταυτότητες, τα βιομετρικά δεδομένα είναι μοναδικά και, όταν παραβιάζονται, δεν μπορούν να επαναρυθμιστούν ή να αλλάξουν. Η ανησυχία εντείνεται από την πιθανή κατάχρηση ή τον ακατάλληλο χειρισμό αυτών των δεδομένων από τρίτους. Οι επιχειρήσεις στον τομέα της φιλοξενίας και του τουρισμού ενδέχεται να συνεργάζονται με εξωτερικούς προμηθευτές για την αποθήκευση ή την επεξεργασία δεδομένων, γεγονός που αυξάνει τον κίνδυνο παράνομης πρόσβασης. Οι τουρίστες ή οι πελάτες των ξενοδοχείων ενδέχεται να μην αισθάνονται άνετα να μοιράζονται τα βιομετρικά τους στοιχεία (Lehto et al., 2021).

Η ασφάλεια των βιομετρικών δεδομένων έχει καταστεί κρίσιμη πρόκληση (Oloyede et al., 2020). Στον κλάδο του τουρισμού και της φιλοξενίας, τα ξενοδοχεία, οι αεροπορικές εταιρείες και άλλοι πάροχοι υπηρεσιών αποθηκεύουν τεράστιες ποσότητες ευαίσθητων πληροφοριών, γεγονός που τους καθιστά πρωταρχικούς στόχους για κυβερνοεπιθέσεις. Οι χάκερ που παραβιάζουν μια βιομετρική βάση δεδομένων μπορούν να έχουν πρόσβαση σε μόνιμες προσωπικές πληροφορίες, όπως δακτυλικά αποτυπώματα ή προφίλ προσώπου (Malik, 2024). Οι συνέπειες τέτοιων παραβιάσεων μπορεί να είναι πιο σοβαρές από τις παραδοσιακές παραβιάσεις δεδομένων, καθώς τα κλεμμένα βιομετρικά δεδομένα μπορούν να οδηγήσουν σε κλοπή ταυτότητας σε μεγάλη κλίμακα. Οι εταιρείες πρέπει να εξετάσουν πόσο καιρό αποθηκεύονται αυτά τα δεδομένα και αν διαθέτουν τα κατάλληλα συστήματα για τη διαγραφή

των δεδομένων μετά την ολοκλήρωση της προβλεπόμενης χρήσης τους. Τα βιομετρικά συστήματα απαιτούν σημαντικές επενδύσεις τόσο σε υλικό όσο και σε λογισμικό (Van & Basie Von Solms, 2014).

Τα συστήματα αναγνώρισης προσώπου μπορεί να απαιτούν την εγκατάσταση καμερών, ενώ τα συστήματα δακτυλικών αποτυπωμάτων χρειάζονται εξειδικευμένους σαρωτές πριν από τη λειτουργία τους. Οι επιχειρήσεις χρειάζονται ασφαλείς εγκαταστάσεις αποθήκευσης δεδομένων, οι οποίες συχνά απαιτούν πρόσθετη υποδομή. Τα έξοδα συντήρησης αποτελούν πρόβλημα για τα βιομετρικά συστήματα (Van & Basie Von Solms, 2014). Για επιχειρήσεις όπως μπουτίκ ξενοδοχεία ή τοπικοί ταξιδιωτικοί πράκτορες, τα έξοδα μπορεί να είναι απαγορευτικά, δημιουργώντας ένα ψηφιακό χάσμα μεταξύ των μεγαλύτερων, τεχνολογικά εξελιγμένων εταιρειών και των μικρότερων επιχειρήσεων. Το κόστος εκπαίδευσης του προσωπικού στη χρήση και διαχείριση αυτών των συστημάτων μπορεί να προστεθεί στα συνολικά έξοδα, καθιστώντας δύσκολη την αιτιολόγηση για ορισμένες επιχειρήσεις. Τα βιομετρικά συστήματα δεν είναι πάντα αξιόπιστα. Ένας σαρωτής δακτυλικών αποτυπωμάτων μπορεί να μην καταφέρει να διαβάσει το δακτυλικό αποτύπωμα ενός επισκέπτη λόγω βρώμικων χεριών, ή το λογισμικό αναγνώρισης προσώπου μπορεί να δυσκολευτεί σε συνθήκες κακού φωτισμού. Περιβαλλοντικοί παράγοντες, όπως η υγρασία ή η θερμοκρασία, μπορούν επίσης να επηρεάσουν την απόδοση αυτών των συστημάτων (Abdarahmane Wone et al., 2021).

Ομοίως, μπορεί να υπάρχουν προβλήματα με την ενσωμάτωση του συστήματος, ειδικά όταν οι εταιρείες προσπαθούν να εφαρμόσουν τη βιομετρική τεχνολογία παράλληλα με τα παλαιά συστήματα. Οι αστοχίες στα βιομετρικά συστήματα, όπως η εσφαλμένη αναγνώριση ή η διακοπή λειτουργίας του συστήματος, μπορούν να οδηγήσουν σε μεγάλες καθυστερήσεις, απογοητευμένους πελάτες και διακοπές στην παροχή υπηρεσιών. Στον τομέα του τουρισμού και της φιλοξενίας, όπου η ικανοποίηση των πελατών είναι κυρίαρχη, ακόμη και μια μικρή ταλαιπωρία που προκαλείται από ένα τεχνικό πρόβλημα μπορεί να επηρεάσει αρνητικά την εμπειρία ενός επισκέπτη (Algarni et al., 2020).

2.5.2. Επιπτώσεις της χρήσης της βιομετρικής τεχνολογίας

Η βιομετρική τεχνολογία εξασφαλίζει στις επιχειρήσεις ένα ασφαλέστερο περιβάλλον τόσο για τους εργαζομένους όσο και για τους πελάτες, με αποτέλεσμα τη μείωση των περιπτώσεων απάτης και παραβίασης δεδομένων (Selian & McKnight, 2017). Οι βιομηχανίες πρέπει να είναι προσεκτικές κατά τον χειρισμό των ευαίσθητων δεδομένων βιομετρικών στοιχείων, καθώς η ακατάλληλη διαχείριση μπορεί να οδηγήσει σε κινδύνους ασφαλείας και ανησυχίες για την προστασία της ιδιωτικής ζωής των πελατών. Όταν μειώνονται τα σημεία τριβής στις σχέσεις με τους πελάτες, τα βιομετρικά στοιχεία μπορούν να βελτιώσουν σημαντικά την ικανοποίηση των πελατών, συμβάλλοντας στην επανάληψη των συναλλαγών και στις θετικές αξιολογήσεις (Štilić et al., 2023).

Η επιτυχία των υπηρεσιών που βασίζονται στη βιομετρία θα εξαρτηθεί από το πόσο άνετοι αισθάνονται οι πελάτες με την τεχνολογία και από το αν εμπιστεύονται τις επιχειρήσεις για την προστασία των βιομετρικών τους πληροφοριών. Οι επιχειρήσεις που υιοθετούν τη βιομετρική τεχνολογία μπορούν να βελτιώσουν τις διαδικασίες τους, να μειώσουν το κόστος εργασίας και να βελτιώσουν την κατανομή των πόρων (Gupta, 2008). Το αρχικό κόστος υιοθέτησης βιομετρικών συστημάτων μπορεί να είναι υψηλό, γεγονός που μπορεί να αποθαρρύνει τις μικρότερες επιχειρήσεις από την υιοθέτηση της τεχνολογίας. Επιπλέον, η βιομετρική τεχνολογία εγείρει σημαντικά ζητήματα ιδιωτικότητας και ηθικής, τα οποία οι επιχειρήσεις πρέπει να αντιμετωπίσουν μέσω σαφών πολιτικών, αυστηρών πρωτοκόλλων προστασίας δεδομένων και συμμόρφωσης με τους κανονισμούς. Οι εταιρείες που χρησιμοποιούν βιομετρικά συστήματα πρέπει να διασφαλίζουν την πλήρη συμμόρφωση με τους κανονισμούς προστασίας δεδομένων, προκειμένου να αποφύγουν νομικές συνέπειες (Hilsman, 2024).

Πρέπει επίσης να ενημερώνονται για τις εξελίξεις στο νομικό τοπίο, καθώς οι νόμοι σχετικά με τη χρήση βιομετρικών δεδομένων βρίσκονται ακόμη σε εξέλιξη σε πολλές χώρες. Ο τουριστικός και ο ξενοδοχειακός κλάδος που επιδιώκουν να υιοθετήσουν βιομετρικά συστήματα πρέπει να αξιολογήσουν τις κοινωνικοπολιτισμικές στάσεις απέναντι στη βιομετρία πριν από την εφαρμογή της τεχνολογίας (Lacaci et al., 2024). Η προσφορά εναλλακτικών λύσεων για όσους αισθάνονται άβολα με τα βιομετρικά συστήματα και η

ενημέρωση των πελατών σχετικά με τα οφέλη και την ασφάλεια της τεχνολογίας μπορούν να συμβάλουν στην άμβλυση των αντιδράσεων και να ενθαρρύνουν την ευρύτερη αποδοχή της. Οι ισχυρές πρακτικές ασφάλειας δεδομένων είναι ζωτικής σημασίας για την πρόληψη της παράνομης πρόσβασης σε βιομετρικές βάσεις δεδομένων και για τη διατήρηση της εμπιστοσύνης των πελατών (Moisa & Michoroulou, 2022).

Δεδομένου ότι, μια παραβίαση δεδομένων που περιλαμβάνει βιομετρικές πληροφορίες θα μπορούσε να έχει μακροχρόνιες επιπτώσεις τόσο για την επιχείρηση όσο και για τους πελάτες της (Singh et al., 2021). Η εκπαίδευση των υπαλλήλων στην αποτελεσματική χρήση των βιομετρικών συστημάτων είναι ζωτικής σημασίας για την εξασφάλιση ομαλής λειτουργίας και την ελαχιστοποίηση των σφαλμάτων (Βασιλείου, & Ηρειώτης, 2008). Οι επιχειρήσεις πρέπει να επενδύσουν στη συνεχή εκπαίδευση του προσωπικού τους, ώστε να συμβαδίζουν με τις τεχνολογικές εξελίξεις, κάτι που μπορεί να απαιτεί πρόσθετους πόρους και χρόνο. Ο κλάδος πρέπει να διατηρεί σχέδια έκτακτης ανάγκης σε περίπτωση βλάβης των βιομετρικών συστημάτων, εξασφαλίζοντας τη διαθεσιμότητα χειροκίνητων διαδικασιών ως εφεδρικών λύσεων. Αυτές μπορεί να περιλαμβάνουν παραδοσιακές μορφές ταυτοποίησης ή ελέγχου πρόσβασης, ώστε να ελαχιστοποιούνται οι διαταραχές κατά τη διάρκεια διακοπών λειτουργίας του συστήματος. Αυτές οι προκλήσεις καθιστούν την υιοθέτηση της βιομετρικής τεχνολογίας μια προσεκτική απόφαση για τον κλάδο της φιλοξενίας και του τουρισμού (Gupta, 2008).

2.6. Επαλήθευση ταυτότητας στον τομέα της φιλοξενίας

Ο κλάδος της φιλοξενίας αντιμετωπίζει ολοένα και μεγαλύτερες προκλήσεις όσον αφορά την επαλήθευση της ταυτότητας, την πρόληψη της απάτης και την ασφάλεια. Οι επιχειρήσεις πρέπει να γνωρίζουν ακριβώς ποιοι είναι οι πελάτες τους, εξασφαλίζοντας παράλληλα μια ομαλή και απρόσκοπτη εμπειρία. Φανταστείτε μια εταιρεία κρουαζιέρας που διαχειρίζεται αποτελεσματικά χιλιάδες επισκέπτες που φτάνουν σε διαφορετικά λιμάνια ή ένα ξενοδοχείο που απλοποιεί τη διαδικασία check-in για να μεταφέρει τους επισκέπτες στα δωμάτιά τους πιο γρήγορα. Σε κάθε περίπτωση, η επαλήθευση της ταυτότητας είναι ζωτικής σημασίας για τη διασφάλιση της ασφάλειας και της ικανοποίησης των πελατών. Παραδοσιακά,

η επαλήθευση της ταυτότητας στον τομέα της φιλοξενίας βασίζεται σε χειροκίνητες διαδικασίες. Οι υπάλληλοι των αεροπορικών εταιρειών ελέγχουν τις ταυτότητες και τα πρόσωπα των επιβατών. Η ικανότητά τους να εντοπίζουν πλαστές ταυτότητες είναι περιορισμένη χωρίς εκτενή εκπαίδευση στην επαλήθευση εγγράφων (Srinivasan et al., 2024).

Το ίδιο ισχύει για το προσωπικό της ρεσεψιόν των ξενοδοχείων ή το προσωπικό επιβίβασης των κρουαζιερόπλοιων. Οι άνθρωποι κάνουν λάθη, κουράζονται και οι περισσότεροι δεν διαθέτουν εμπειρία στην επαλήθευση εγγράφων, γεγονός που συμβάλλει στη δημιουργία κενών στην ασφάλεια. Οι μηχανές δεν κουράζονται και επεξεργάζονται τις πληροφορίες πολύ πιο γρήγορα και με μεγαλύτερη ακρίβεια από τους ανθρώπους. Οι αλγόριθμοι μπορούν να εκπαιδευτούν ώστε να εντοπίζουν πλαστά έγγραφα ταυτότητας και κλεμμένες ταυτότητες, ξεπερνώντας τους απατεώνες που βρίσκουν τα αδύνατα σημεία των ανθρώπων και γίνονται όλο και πιο εξελιγμένοι στο έγκλημα (Jirsa, 2020).

Η τεχνητή νοημοσύνη (AI) παρεμβαίνει όπου οι χειροκίνητοι έλεγχοι δεν επαρκούν. Η επαλήθευση ταυτότητας με τεχνητή νοημοσύνη μεταμορφώνει τον κλάδο της φιλοξενίας, αυτοματοποιώντας τις διαδικασίες και βελτιώνοντας την ακρίβεια. Για παράδειγμα, ορισμένα ξενοδοχεία διαθέτουν περίπτερα αυτόματου check-in. Οι επισκέπτες σαρώνουν τα πιστοποιητικά ταυτότητάς τους και τραβούν μια γρήγορη φωτογραφία. Το σύστημα επαληθεύει την ταυτότητα και την ηλικία τους σε δευτερόλεπτα. Αυτή η τεχνολογία είναι ανεκτίμητη για την επαλήθευση της ηλικίας, διασφαλίζοντας ότι μόνο οι επιλέξιμοι επισκέπτες μπορούν να έχουν πρόσβαση σε καζίνο, να αγοράζουν αλκοόλ ή να εισέρχονται σε χώρους με περιορισμούς ηλικίας. Με την απρόσκοπτη ενσωμάτωση αυτών των μέτρων ασφαλείας, η τεχνητή νοημοσύνη ενισχύει την ασφάλεια και βελτιστοποιεί την εμπειρία των επισκεπτών (Wu et al., 2019).

Οι αεροπορικές εταιρείες έχουν αρχίσει να εφαρμόζουν ψηφιακά συστήματα προ-ελέγχου, όπου οι επιβάτες ανεβάζουν τα στοιχεία του διαβατηρίου τους εκ των προτέρων, επιτρέποντας την ταχεία επαλήθευση στην πύλη. Για παράδειγμα, το Delta FlyReady, ένα ψηφιακό εργαλείο, βοηθά τους πελάτες να επαληθεύσουν ότι πληρούν τις απαιτήσεις διαβατηρίου και βίζας του προορισμού τους πριν από το ταξίδι. Οι εταιρείες κρουαζιέρας υιοθετούν παρόμοιες προσεγγίσεις, διασφαλίζοντας ότι οι επισκέπτες που επιβιβάζονται σε πλοία ή έχουν πρόσβαση σε λιμάνια ταυτοποιούνται σωστά χωρίς μεγάλους χρόνους αναμονής

ή χειροκίνητους ελέγχους. Πέρα από την ευκολία, η επαλήθευση ταυτότητας με βάση την τεχνητή νοημοσύνη παρέχει ένα σημαντικό πλεονέκτημα ασφάλειας. Σε αντίθεση με τους ανθρώπους, ένα σύστημα τεχνητής νοημοσύνης που έχει εκπαιδευτεί σε χιλιάδες αυθεντικά και πλαστά έγγραφα μπορεί να εντοπίσει τις μικρότερες ασυνέπειες που υποδηλώνουν πλαστά πιστοποιητικά ταυτότητας. Αυτή η ανίχνευση είναι κρίσιμη σε κλάδους όπου η απάτη μπορεί να έχει σοβαρές οικονομικές και νομικές συνέπειες, όπως ξενοδοχεία, καζίνο και κρουαζιερόπλοια. Η τεχνολογία αναγνώρισης προσώπου ενισχύει περαιτέρω αυτή τη διαδικασία, ταιριάζοντας τα βιομετρικά δεδομένα με σχεδόν τέλεια ακρίβεια, μειώνοντας δραστικά τις πιθανότητες να περάσει κάποιος απατεώνας (Štilić et al., 2023).

Ας σκεφτούμε έναν απατεώνα που χρησιμοποιεί κλεμμένη ταυτότητα και πιστωτική κάρτα για να κάνει κράτηση σε πολυτελές ξενοδοχείο ή να αποκτήσει πρόσβαση σε καζίνο με υψηλά στοιχήματα. Χωρίς προηγμένη επαλήθευση, το προσωπικό μπορεί να παραβλέψει λεπτές ασυμφωνίες, επιτρέποντας στον εγκληματία να περάσει απαρατήρητος. Η τεχνητή νοημοσύνη, ωστόσο, μπορεί να διασταυρώσει τα χαρακτηριστικά του προσώπου, να αναλύσει την αυθεντικότητα των εγγράφων και να επισημάνει ασυμφωνίες μέσα σε λίγα δευτερόλεπτα, σταματώντας την απάτη (Singh et al., 2018).

Αυτό ισχύει και για την απάτη από εσωτερικούς παράγοντες. Οι υπάλληλοι μπορεί να μπουκν στον πειρασμό να κάνουν κατάχρηση προσωπικών δεδομένων ή να χειραγωγήσουν συναλλαγές για προσωπικό όφελος. Αξιοποιώντας αυτοματοποιημένα συστήματα επαλήθευσης, οι επιχειρήσεις μπορούν να ελαχιστοποιήσουν την ανθρώπινη πρόσβαση σε ευαίσθητες πληροφορίες πελατών, διασφαλίζοντας ότι τα δεδομένα παραμένουν εντός ασφαλών ψηφιακών πλαισίων και μειώνοντας τις ευκαιρίες για εσωτερική εκμετάλλευση (Singh et al., 2018).

Η υιοθέτηση εργαλείων επαλήθευσης ταυτότητας στον τομέα της φιλοξενίας έχει σημειώσει σημαντική άνοδο τα τελευταία χρόνια, ωθούμενη από τη διπλή δύναμη της τεχνολογικής προόδου και των μεταβαλλόμενων προσδοκιών των καταναλωτών. Οι σημερινοί επισκέπτες απαιτούν όχι μόνο ασφάλεια αλλά και ευκολία, προσδοκώντας γρήγορες και απρόσκοπτες διαδικασίες check-in που δεν θέτουν σε κίνδυνο την ασφάλεια ή την ιδιωτικότητά τους. Η ικανοποίηση αυτών των προσδοκιών απαιτεί την απομάκρυνση από τις

παραδοσιακές, εργοβόρες μεθόδους επαλήθευσης προς πιο εξελιγμένα, αυτοματοποιημένα εργαλεία (Srinivasan et al., 2024).

Τα εργαλεία επαλήθευσης ταυτότητας διαθέτουν χαρακτηριστικά που έχουν σχεδιαστεί για να ικανοποιούν αυτές τις ανάγκες. Οι δυνατότητες επαλήθευσης σε πραγματικό χρόνο επιτρέπουν την άμεση πιστοποίηση εγγράφων και βιομετρικών δεδομένων, μειώνοντας σημαντικά τους χρόνους αναμονής. Οι προηγμένοι αλγόριθμοι ανίχνευσης απάτης μπορούν να εντοπίζουν και να επισημαίνουν πιθανά ζητήματα ασφάλειας πριν αυτά εξελιχθούν σε προβλήματα, προσφέροντας ένα επιπλέον επίπεδο προστασίας. Επιπλέον, αυτά τα εργαλεία έχουν σχεδιαστεί για να είναι φιλικά προς τον χρήστη, ελαχιστοποιώντας την καμπύλη εκμάθησης για το προσωπικό και εξασφαλίζοντας μια ομαλή εμπειρία για τους επισκέπτες (Jackson, 2009).

Τα οφέλη από τη χρήση τέτοιων εργαλείων είναι πολυδιάστατα. Καταρχάς, προσφέρουν υψηλότερο επίπεδο ακρίβειας στην επαλήθευση ταυτότητας, μειώνοντας τις πιθανότητες ανθρώπινου λάθους. Παρέχουν επίσης ένα πιο ασφαλές περιβάλλον, τόσο για τους επισκέπτες όσο και για το προσωπικό, αποτρέποντας αποτελεσματικά τις δόλιες δραστηριότητες. Επιπλέον, η αποτελεσματικότητα και η ταχύτητα των μεθόδων ψηφιακής επαλήθευσης μπορούν να βελτιώσουν την λειτουργική αποδοτικότητα, απελευθερώνοντας το προσωπικό ώστε να επικεντρωθεί σε άλλες πτυχές της εξυπηρέτησης των επισκεπτών (Srinivasan et al., 2024).

Η αυξανόμενη εξάρτηση από αυτά τα εργαλεία αντικατοπτρίζει μια ευρύτερη τάση στον κλάδο της φιλοξενίας προς την ψηφιακή μεταμόρφωση. Καθώς οι επιχειρήσεις επιδιώκουν να καινοτομήσουν και να βελτιώσουν τις υπηρεσίες τους, η υιοθέτηση τεχνολογίας που ενισχύει την ασφάλεια και την αποδοτικότητα έχει καταστεί προτεραιότητα. Τα εργαλεία επαλήθευσης ταυτότητας, με την ικανότητά τους να ικανοποιούν αυτές τις ανάγκες, βρίσκονται στην πρώτη γραμμή αυτής της αλλαγής, αναδιαμορφώνοντας τον τρόπο λειτουργίας των επιχειρήσεων φιλοξενίας και τον τρόπο αλληλεπίδρασής τους με τους επισκέπτες τους (Davenport et al., 2018).

Η υιοθέτηση συστημάτων επαλήθευσης ταυτότητας από τον κλάδο της φιλοξενίας έχει αλλάξει τα δεδομένα στη διαχείριση των ταυτοτήτων των πελατών. Αυτά τα συστήματα έχουν

σχεδιαστεί για να προσφέρουν απρόσκοπτη ενσωμάτωση στη ροή εργασιών του κλάδου της φιλοξενίας, επιτρέποντας μια ομαλή διαδικασία check-in που βελτιώνει την εμπειρία των πελατών, διατηρώντας παράλληλα υψηλά πρότυπα ασφάλειας. Αυτοματοποιώντας τη διαδικασία επαλήθευσης, αυτά τα συστήματα μειώνουν σημαντικά το περιθώριο σφάλματος στο οποίο είναι επιρρεπείς οι χειροκίνητοι έλεγχοι. Λειτουργούν με τη σάρωση και την επαλήθευση εγγράφων σε πραγματικό χρόνο, χρησιμοποιώντας προηγμένους αλγόριθμους για την ανίχνευση τυχόν ανακολουθιών ή πλαστογραφιών που μπορεί να υποδηλώνουν δόλια δραστηριότητα (Ashqar et al., 2024).

Ένα από τα βασικά πλεονεκτήματα αυτών των συστημάτων είναι η δυνατότητα ενσωμάτωσής τους σε υπάρχουσες πλατφόρμες κρατήσεων και διαχείρισης. Αυτή η ενσωμάτωση επιτρέπει μια απλοποιημένη διαδικασία, όπου οι πληροφορίες των πελατών επαληθεύονται αυτόματα σε σχέση με τα επίσημα έγγραφα ως μέρος της διαδικασίας κράτησης. Αυτό απλοποιεί τις λειτουργίες για τις επιχειρήσεις φιλοξενίας και παρέχει μια απρόσκοπτη εμπειρία για τους επισκέπτες, οι οποίοι συχνά μπορούν να ολοκληρώσουν τα απαραίτητα βήματα επαλήθευσης μέσω μιας εφαρμογής για κινητά ή ενός ιστότοπου πριν από την άφιξή τους (Ashqar et al., 2024).

Επιπλέον, η έμφαση στην εμπειρία του χρήστη είναι υψίστης σημασίας. Τα σύγχρονα συστήματα επαλήθευσης ταυτότητας έχουν σχεδιαστεί με γνώμονα τον τελικό χρήστη, εξασφαλίζοντας ότι η διαδικασία είναι όσο το δυνατόν πιο διαισθητική και απλή. Αυτή η εστίαση συμβάλλει στη μείωση τυχόν εντάσεων που θα μπορούσαν να αποτρέψουν τους επισκέπτες από την ολοκλήρωση της διαδικασίας επαλήθευσης, εξισορροπώντας έτσι την ανάγκη για ασφάλεια με την επιθυμία για μια ομαλή εμπειρία πελάτη. Το αποτέλεσμα είναι μια εμπειρία check-in που φαίνεται σύγχρονη, αποτελεσματική και ασφαλής, συμβάλλοντας σε μια θετική πρώτη εντύπωση που καθορίζει τον τόνο για ολόκληρη τη διαμονή του επισκέπτη (Grobbelaar et al., 2024).

Κοιτώντας μπροστά, η επαλήθευση ταυτότητας στον τομέα της φιλοξενίας είναι έτοιμη να γίνει ταχύτερη, ασφαλέστερη και σχεδόν αβίαστη. Οι ψηφιακές ταυτότητες, που έχουν ήδη εισαχθεί σε ορισμένες πολιτείες των ΗΠΑ, είναι έτοιμες να εξαλείψουν την ανάγκη για φυσικά έγγραφα. Αντί να παραδίδουν το διαβατήριό ή το δίπλωμα οδήγησης, οι επισκέπτες θα επαληθεύουν την ταυτότητά τους αμέσως μέσω κρυπτογραφημένων κινητών συσκευών,

μειώνοντας την ανάγκη για ανθρώπινη παρέμβαση και ελαχιστοποιώντας τους κινδύνους ασφαλείας. Εν τω μεταξύ, η τεχνητή νοημοσύνη και τα μεγάλα γλωσσικά μοντέλα (LLM) θα συνεχίσουν να εξελίσσονται, γίνονται ακόμη πιο ικανά να ανιχνεύουν δόλια συμπεριφορά και ασυνέπειες στα έγγραφα, εντοπίζοντας μερικές φορές λεπτομέρειες που ακόμη και οι πιο έμπειροι επαγγελματίες της ασφάλειας μπορεί να παραβλέψουν (Grobbelaar et al., 2024).

Με την πρόοδο της τεχνητής νοημοσύνης, ενδέχεται να δούμε chatbots και εικονικούς βοηθούς ικανούς να χειρίζονται ολόκληρη τη διαδικασία επαλήθευσης ταυτότητας μέσω φυσικής συνομιλίας. Σύντομα, οι πράκτορες τεχνητής νοημοσύνης θα είναι ο κανόνας για τους επισκέπτες που κάνουν κρατήσεις και πληρωμές. Αυτό υπογραμμίζει την ανάγκη για απόδειξη της ύπαρξης ενός πραγματικού ατόμου σε έναν κόσμο όπου κυριαρχεί το ψηφιακό. Αντί να περιμένουν στην ουρά για να κάνουν check-in σε ένα ξενοδοχείο, οι επισκέπτες θα μπορούν να επαληθεύουν την ταυτότητά τους με μια γρήγορη, τεχνητή νοημοσύνη-καθοδηγούμενη αλληλεπίδραση στο τηλέφωνό τους (Ashqar et al., 2024). Οι εταιρείες κρουαζιέρας θα μπορούν να χρησιμοποιούν αυτοματοποιημένη επαλήθευση σε πολλαπλά σημεία ελέγχου, εξασφαλίζοντας μια ομαλή εμπειρία χωρίς καθυστερήσεις. Με τις μηχανές να αναλαμβάνουν παραδοσιακά ανθρώπινες εργασίες, η ανάγκη για πρόσωπο με πρόσωπο αλληλεπίδραση στον τομέα της φιλοξενίας θα μπορούσε να μειωθεί σημαντικά. Αυτή η αλλαγή βελτιώνει την αποδοτικότητα και την ασφάλεια, αλλά εγείρει ερωτήματα σχετικά με το μέλλον των ρόλων εξυπηρέτησης πελατών στον κλάδο (Bodkhe et al., 2019).

Με αυτές τις εξελίξεις έρχονται και ανησυχίες σχετικά με την προστασία της ιδιωτικής ζωής και την ασφάλεια των δεδομένων. Οι οργανισμοί φιλοξενίας που εφαρμόζουν επαλήθευση ταυτότητας με τεχνητή νοημοσύνη πρέπει να προστατεύουν τις ευαίσθητες πληροφορίες των πελατών από απειλές και παραβιάσεις στον κυβερνοχώρο και να διατηρούν τα δεδομένα ασφαλή. Ο στόχος είναι η ενίσχυση της ασφάλειας με παράλληλη διατήρηση της εμπιστοσύνης των πελατών. Η στροφή προς την επαλήθευση ταυτότητας με τεχνητή νοημοσύνη επιτυγχάνει ισορροπία μεταξύ της απρόσκοπτης εμπειρίας των επισκεπτών και της πρόληψης των απατεώνων. Ενώ αυτές οι καινοτομίες καθιστούν τα ταξίδια και τη φιλοξενία πιο βολικά και ασφαλή, η παρακολούθηση των συνεχώς εξελισσόμενων απειλών αποτελεί πρόκληση. Οι απατεώνες προσαρμόζονται συνεχώς, βρίσκοντας νέους τρόπους για να

εκμεταλλευτούν τα κενά. Τα συστήματα τεχνητής νοημοσύνης πρέπει να εξελίσσονται συνεχώς (Ashqar et al., 2024).

Καθώς αυτές οι τεχνολογίες ωριμάζουν, έχουν τη δυνατότητα να κάνουν τα ταξίδια πιο ομαλά, γρήγορα και ασφαλή, επιτρέποντας στους επισκέπτες να μετακινούνται χωρίς κόπο στα αεροδρόμια, τους τερματικούς σταθμούς κρουαζιέρας και τα check-in των ξενοδοχείων, χωρίς την ταλαιπωρία των χειροκίνητων ελέγχων ταυτότητας. Οι επιχειρήσεις που αγκαλιάζουν αυτό το μέλλον και χτίζουν ισχυρά θεμέλια στην τεχνητή νοημοσύνη και την ψηφιακή ασφάλεια θα ενισχύσουν την προστασία και θα επαναπροσδιορίσουν την έννοια της ευκολίας στον τομέα της φιλοξενίας (Martínez & Del Bosque, 2014; Ashqar et al., 2024).

3. Μεθοδολογία

3.1. Σκοπός και Ερευνητικά Ερωτήματα

Σκοπός της παρούσας έρευνας είναι η περιγραφική αποτύπωση των πρακτικών επαλήθευσης και διαχείρισης δεδομένων πελατών που εφαρμόζονται από ξενοδοχειακές επιχειρήσεις στη Μύκονο. Η μελέτη επικεντρώνεται στην καταγραφή των υφιστάμενων διαδικασιών ταυτοποίησης, της ύπαρξης πολιτικών KYC, των μηχανισμών εσωτερικού ελέγχου, καθώς και της εκπαίδευσης του προσωπικού σε ζητήματα πρόληψης και ανίχνευσης απάτης.

Η έρευνα επιδιώκει να παρουσιάσει την υφιστάμενη κατάσταση στον κλάδο, χωρίς τη διερεύνηση αιτιωδών σχέσεων ή τη διατύπωση υποθέσεων.

Με βάση τον παραπάνω σκοπό, τα ερευνητικά ερωτήματα διαμορφώνονται ως εξής:

- Ποιες πρακτικές ταυτοποίησης πελατών εφαρμόζονται από τις ξενοδοχειακές επιχειρήσεις;
- Υφίσταται θεσμοθετημένη πολιτική KYC στις επιχειρήσεις;
- Ποια τμήματα είναι υπεύθυνα για τις διαδικασίες επαλήθευσης στοιχείων;

- Σε ποιο βαθμό εκπαιδεύεται το προσωπικό σε ζητήματα εσωτερικού ελέγχου και αποτροπής απάτης;
- Έχουν καταγραφεί περιστατικά ψευδών στοιχείων πελατών;
- Πώς αξιολογείται η αποτελεσματικότητα των υφιστάμενων συστημάτων επαλήθευσης;
- Υπάρχει ανάγκη αναβάθμισης των εσωτερικών ελέγχων και ενίσχυσης των κατευθυντήριων οδηγιών;

3.2. Ερευνητικός Σχεδιασμός

Η παρούσα μελέτη ακολουθεί ποσοτική ερευνητική προσέγγιση και εντάσσεται στο πλαίσιο της περιγραφικής έρευνας. Στόχος της δεν είναι η διερεύνηση αιτιωδών σχέσεων ή η επαλήθευση υποθέσεων, αλλά η συστηματική καταγραφή και αποτύπωση των πρακτικών που εφαρμόζουν οι ξενοδοχειακές επιχειρήσεις αναφορικά με την επαλήθευση και διαχείριση δεδομένων πελατών.

Η έρευνα βασίστηκε στη συλλογή πρωτογενών δεδομένων μέσω δομημένου ερωτηματολογίου κλειστού τύπου, το οποίο περιλάμβανε ερωτήσεις πολλαπλής επιλογής και ονομαστικής ή τακτικής κλίμακας μέτρησης. Ο σχεδιασμός του ερωτηματολογίου επέτρεψε την ποσοτική αποτύπωση των απαντήσεων και τη μετατροπή τους σε αριθμητικά δεδομένα για στατιστική επεξεργασία.

Η ανάλυση των δεδομένων πραγματοποιήθηκε αποκλειστικά με περιγραφικές στατιστικές μεθόδους, μέσω υπολογισμού συχνοτήτων και ποσοστών, με σκοπό την παρουσίαση της υφιστάμενης κατάστασης στον εξεταζόμενο πληθυσμό.

3.3. Πληθυσμός και Δείγμα

Ο πληθυσμός της έρευνας αποτελείται από ξενοδοχειακές επιχειρήσεις που δραστηριοποιούνται στη Μύκονο. Η επιλογή της συγκεκριμένης γεωγραφικής περιοχής

βασίστηκε στον έντονο τουριστικό της χαρακτήρα και στη μεγάλη συγκέντρωση επιχειρήσεων φιλοξενίας.

Για τις ανάγκες της έρευνας, το ερωτηματολόγιο διανεμήθηκε σε συνολικά 100 ξενοδοχειακές επιχειρήσεις. Από αυτές, ανταποκρίθηκαν 20 επιχειρήσεις, οι οποίες και αποτελούν το τελικό δείγμα της μελέτης. Κάθε συμπληρωμένο ερωτηματολόγιο αντιστοιχεί σε μία επιχείρηση.

Η συλλογή των δεδομένων πραγματοποιήθηκε κατά το χρονικό διάστημα από 20/12 έως 20/02. Η επιλογή του δείγματος πραγματοποιήθηκε με μη πιθανολογική μέθοδο δειγματοληψίας, συγκεκριμένα με δειγματοληψία ευκολίας, καθώς η συμμετοχή βασίστηκε στη διαθεσιμότητα και την προθυμία των επιχειρήσεων να συμμετάσχουν.

Το ποσοστό ανταπόκρισης διαμορφώθηκε στο 20%, γεγονός που λαμβάνεται υπόψη κατά την ερμηνεία των αποτελεσμάτων. Το μέγεθος του δείγματος κρίνεται επαρκές για την περιγραφική αποτύπωση των πρακτικών που εφαρμόζονται στον εξεταζόμενο κλάδο, χωρίς ωστόσο να επιδιώκεται η γενίκευση των αποτελεσμάτων στο σύνολο του πληθυσμού.

3.4. Ερευνητικό Εργαλείο

Για τη συλλογή των δεδομένων χρησιμοποιήθηκε δομημένο ερωτηματολόγιο κλειστού τύπου. Το ερωτηματολόγιο σχεδιάστηκε με σκοπό την καταγραφή των πρακτικών που εφαρμόζουν οι ξενοδοχειακές επιχειρήσεις σχετικά με την ταυτοποίηση πελατών, τις διαδικασίες επαλήθευσης στοιχείων και τους μηχανισμούς εσωτερικού ελέγχου.

Οι ερωτήσεις ήταν διατυπωμένες με σαφή και κατανοητό τρόπο, ώστε να διευκολύνεται η συμπλήρωση από τους συμμετέχοντες και να επιτρέπεται η ποσοτική επεξεργασία των απαντήσεων. Το εργαλείο περιλάμβανε κυρίως ερωτήσεις πολλαπλής επιλογής και κλίμακες αξιολόγησης, επιτρέποντας την περιγραφική ανάλυση μέσω συχνοτήτων και ποσοστών.

Η χρήση ερωτηματολογίου κρίθηκε κατάλληλη για τον συγκεκριμένο σκοπό της μελέτης, καθώς επέτρεψε τη συστηματική αποτύπωση της υφιστάμενης κατάστασης στις επιχειρήσεις του δείγματος.

3.5. Διαδικασία Συλλογής Δεδομένων

Η συλλογή των δεδομένων πραγματοποιήθηκε κατά τη διάρκεια της ερευνητικής περιόδου μέσω της διανομής του ερωτηματολογίου σε ξενοδοχειακές επιχειρήσεις που δραστηριοποιούνται στη Μύκονο. Οι συμμετέχοντες ενημερώθηκαν για τον σκοπό της έρευνας και η συμπλήρωση του ερωτηματολογίου έγινε σε εθελοντική βάση.

Η διαδικασία συλλογής βασίστηκε στη συγκέντρωση πρωτογενών δεδομένων, τα οποία προήλθαν άμεσα από τις απαντήσεις των επιχειρήσεων. Μετά τη συλλογή, οι απαντήσεις καταγράφηκαν και κωδικοποιήθηκαν κατάλληλα, ώστε να είναι δυνατή η στατιστική τους επεξεργασία.

Η μελέτη ακολούθησε περιγραφική προσέγγιση, με στόχο την αποτύπωση των υφιστάμενων πρακτικών, χωρίς παρέμβαση ή πειραματική διαδικασία.

3.6. Στατιστική Ανάλυση

Η επεξεργασία των δεδομένων πραγματοποιήθηκε με τη χρήση περιγραφικών στατιστικών μεθόδων. Συγκεκριμένα, οι απαντήσεις κωδικοποιήθηκαν και αναλύθηκαν μέσω υπολογισμού συχνοτήτων και ποσοστών, με σκοπό την αποτύπωση της κατανομής των απαντήσεων ανά μεταβλητή.

Τα αποτελέσματα παρουσιάζονται σε πίνακες κατανομής συχνοτήτων, στους οποίους αποτυπώνονται οι απόλυτες συχνότητες (N) και τα αντίστοιχα ποσοστά (%). Η ανάλυση περιορίστηκε αποκλειστικά σε περιγραφικό επίπεδο και δεν πραγματοποιήθηκαν επαγωγικές στατιστικές δοκιμασίες ή έλεγχοι υποθέσεων.

Η επιλογή της περιγραφικής στατιστικής κρίνεται κατάλληλη, καθώς ο στόχος της έρευνας είναι η καταγραφή και παρουσίαση της υφιστάμενης κατάστασης στις επιχειρήσεις του δείγματος.

3.7. Ηθικά Ζητήματα

Η παρούσα έρευνα πραγματοποιήθηκε με σεβασμό στις βασικές αρχές της ερευνητικής δεοντολογίας. Η συμμετοχή των επιχειρήσεων ήταν εθελοντική και οι συμμετέχοντες ενημερώθηκαν για τον σκοπό της μελέτης πριν από τη συμπλήρωση του ερωτηματολογίου.

Διασφαλίστηκε η ανωνυμία και η εμπιστευτικότητα των απαντήσεων, καθώς δεν συλλέχθηκαν στοιχεία που να επιτρέπουν την ταυτοποίηση των συμμετεχουσών επιχειρήσεων. Τα δεδομένα χρησιμοποιήθηκαν αποκλειστικά για ακαδημαϊκούς σκοπούς και για την εξαγωγή περιγραφικών συμπερασμάτων σχετικά με τις πρακτικές επαλήθευσης στοιχείων στον ξενοδοχειακό κλάδο.

3.8. Περιορισμοί της Έρευνας

Η παρούσα μελέτη υπόκειται σε ορισμένους περιορισμούς. Αρχικά, το μέγεθος του δείγματος είναι σχετικά μικρό, καθώς περιλαμβάνει 20 ξενοδοχειακές επιχειρήσεις, γεγονός που δεν επιτρέπει τη γενίκευση των αποτελεσμάτων στο σύνολο των επιχειρήσεων του κλάδου.

Επιπλέον, η δειγματοληψία πραγματοποιήθηκε με τη μέθοδο ευκολίας, καθώς η συμμετοχή βασίστηκε στη διαθεσιμότητα και την προθυμία των επιχειρήσεων. Τέλος, η ανάλυση περιορίστηκε αποκλειστικά σε περιγραφικό επίπεδο, χωρίς τη χρήση επαγωγικών στατιστικών μεθόδων, γεγονός που δεν επιτρέπει τον έλεγχο σχέσεων ή διαφορών μεταξύ μεταβλητών.

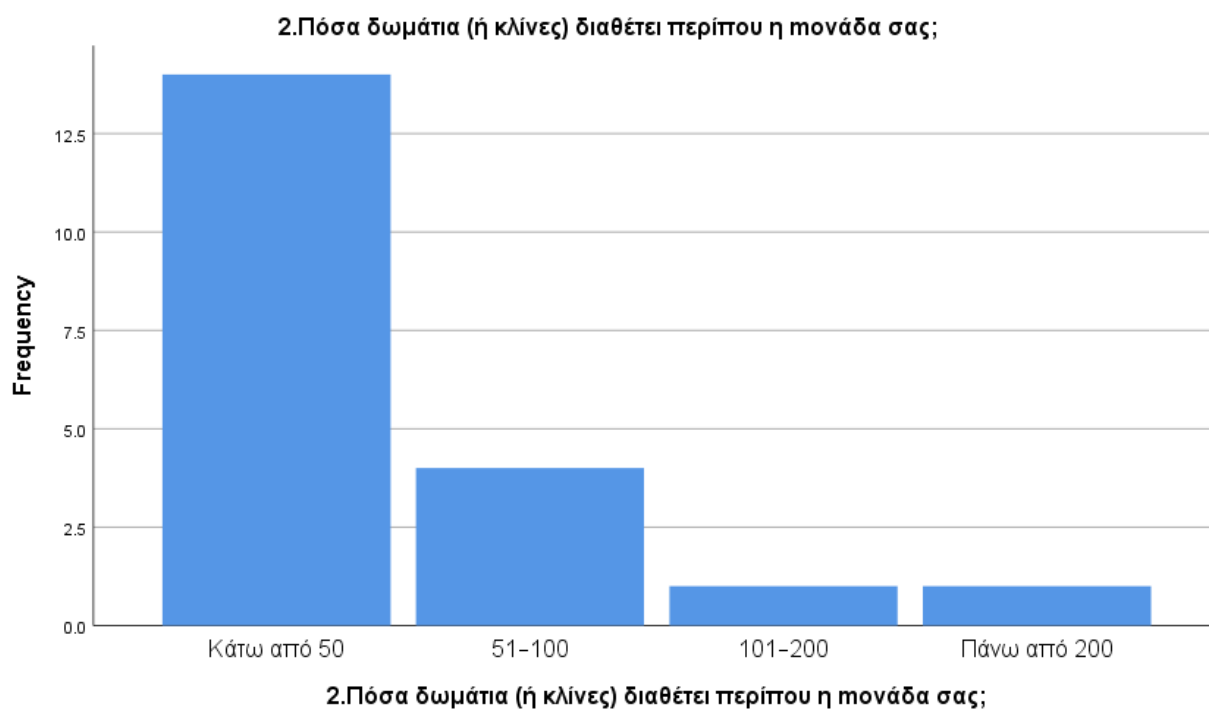
Παρά τους περιορισμούς αυτούς, η έρευνα προσφέρει μια χρήσιμη αποτύπωση των υφιστάμενων πρακτικών επαλήθευσης και εσωτερικού ελέγχου σε ξενοδοχειακές μονάδες της Μυκόνου.

4. Αποτελέσματα

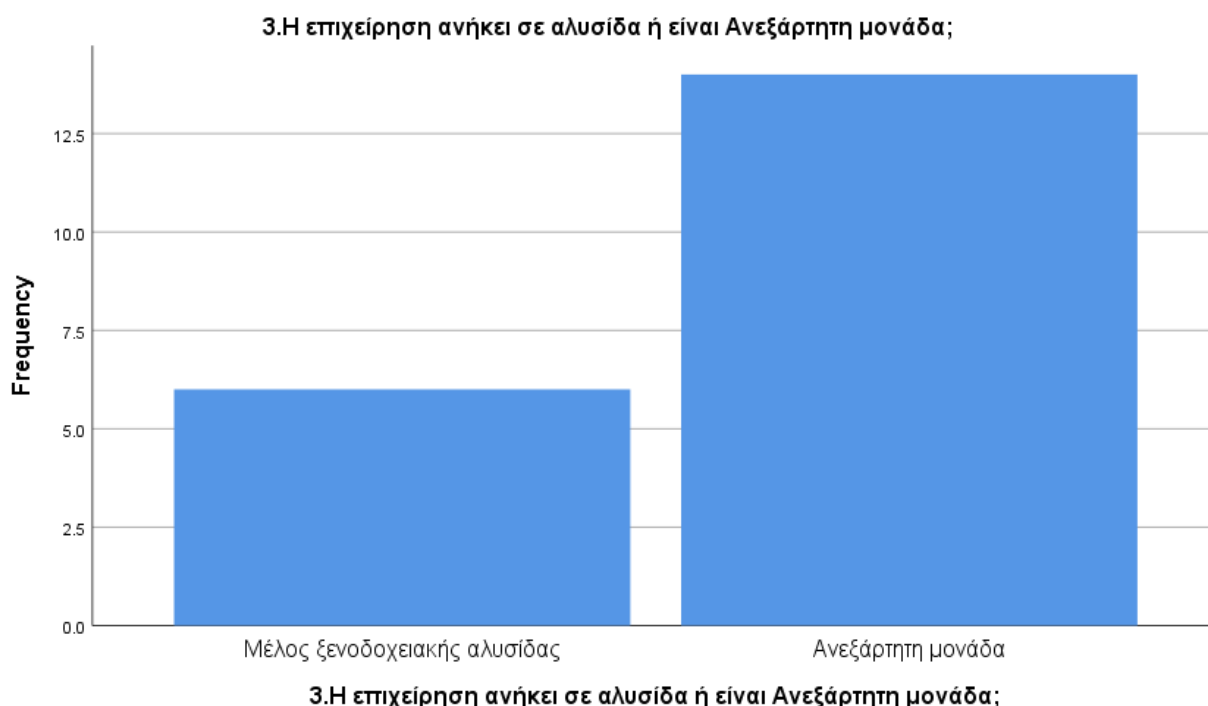
Στην πρώτη ερώτηση, που αφορά την κατηγορία της επιχείρησης, παρατηρείται ότι το μεγαλύτερο ποσοστό του δείγματος προέρχεται από ξενοδοχεία 5 αστέρων (45%), ενώ ακολουθούν τα ξενοδοχεία 4 αστέρων με ποσοστό 25%. Τα Boutique Hotels αντιστοιχούν στο 20% του δείγματος, ενώ οι κατηγορίες All-inclusive Resort και Rbnb εκπροσωπούνται οριακά (5% αντίστοιχα).



Στη δεύτερη ερώτηση, σχετικά με το μέγεθος της μονάδας, διαπιστώνεται ότι η πλειονότητα των επιχειρήσεων (70%) διαθέτει κάτω από 50 δωμάτια/κλίνες, γεγονός που δείχνει ότι το δείγμα αποτελείται κυρίως από μικρές ξενοδοχειακές μονάδες. Το 20% διαθέτει 51–100 δωμάτια, ενώ μόλις το 10% ξεπερνά τις 100 κλίνες.



Στην τρίτη ερώτηση, το 70% των επιχειρήσεων δηλώνει ότι λειτουργεί ως ανεξάρτητη μονάδα, ενώ το 30% αποτελεί μέλος ξενοδοχειακής αλυσίδας.



4.Ποιες πληροφορίες συλλέγετε κατά το check-in για την ταυτοποίηση των πελατών; (Πολλαπλές απαντήσεις)

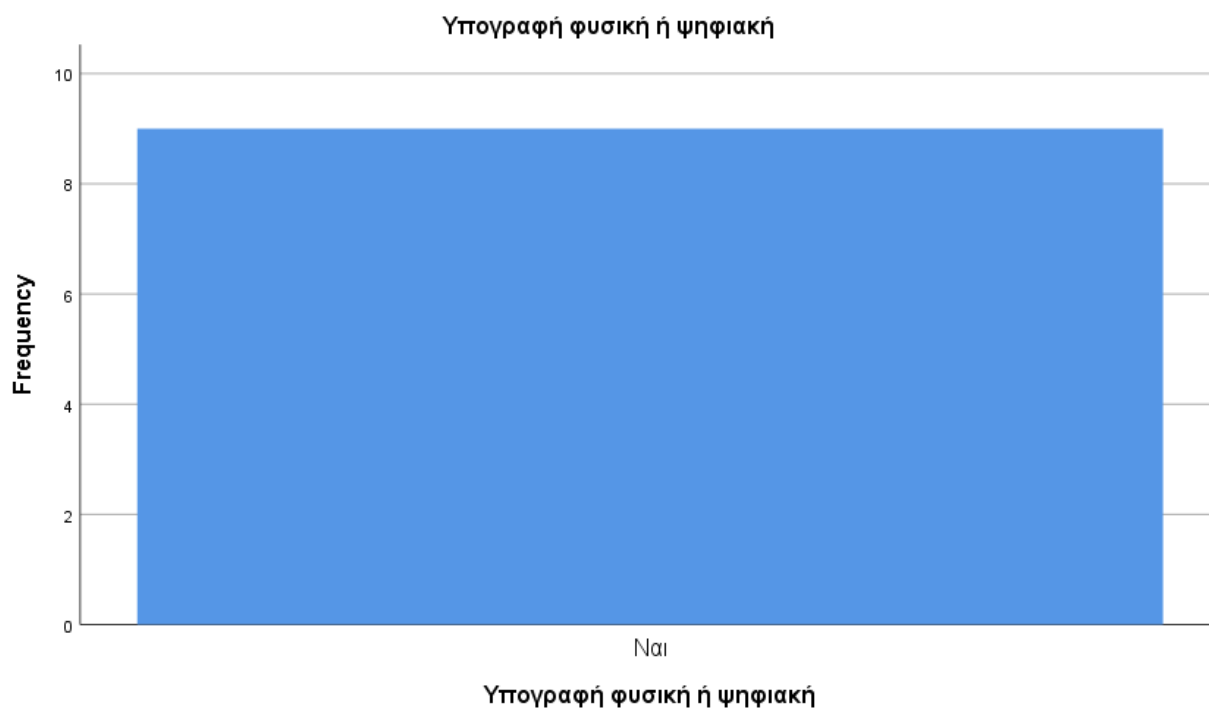
Στην ερώτηση 4, η οποία εξετάζει ποιες πληροφορίες συλλέγονται κατά το check-in για την ταυτοποίηση των πελατών, τα αποτελέσματα δείχνουν ότι σχεδόν όλες οι επιχειρήσεις του δείγματος ζητούν δελτίο ταυτότητας ή διαβατήριο, καθώς το 95% των συμμετεχόντων απάντησε θετικά. Το εύρημα αυτό επιβεβαιώνει ότι η βασική πρακτική ταυτοποίησης εφαρμόζεται σχεδόν καθολικά στις ξενοδοχειακές μονάδες, όπως προβλέπεται και από το θεσμικό πλαίσιο.

Αντίθετα, η συλλογή στοιχείων πιστωτικής κάρτας εμφανίζεται σημαντικά χαμηλότερη, καθώς μόνο το 40% των επιχειρήσεων δηλώνει ότι τα καταγράφει κατά τη διαδικασία check-in. Το αποτέλεσμα αυτό υποδηλώνει ότι οι περισσότερες μονάδες δεν χρησιμοποιούν την πιστωτική κάρτα ως κύριο εργαλείο επαλήθευσης ταυτότητας, πιθανόν λόγω περιορισμών προστασίας προσωπικών δεδομένων ή διαφορετικών πολιτικών πληρωμής.

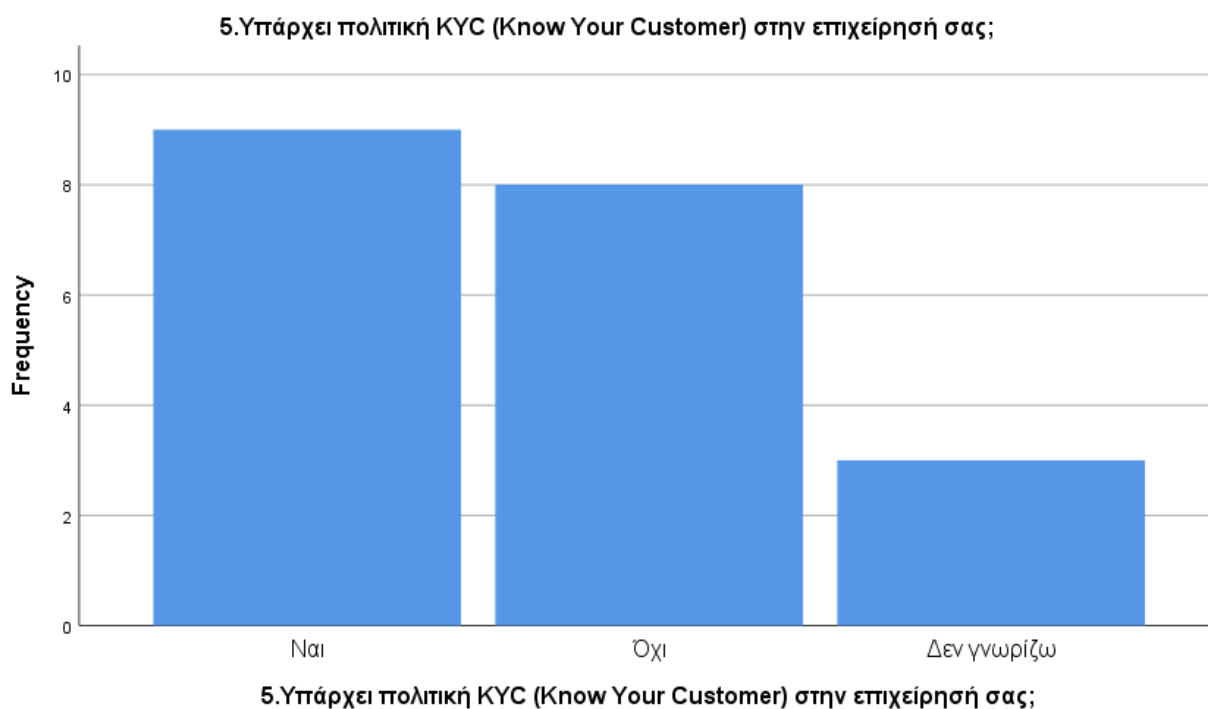
Παρόμοια εικόνα παρουσιάζεται και στη συλλογή υπογραφής, είτε φυσικής είτε ψηφιακής, όπου το 45% των επιχειρήσεων απαντά θετικά. Το γεγονός ότι πάνω από τις μισές μονάδες

δεν ζητούν υπογραφή δείχνει ότι η πρακτική αυτή δεν είναι πλήρως τυποποιημένη, πιθανώς επειδή αρκετές επιχειρήσεις βασίζονται σε ψηφιακές διαδικασίες ή περιορίζονται στην απλή επίδειξη εγγράφων.

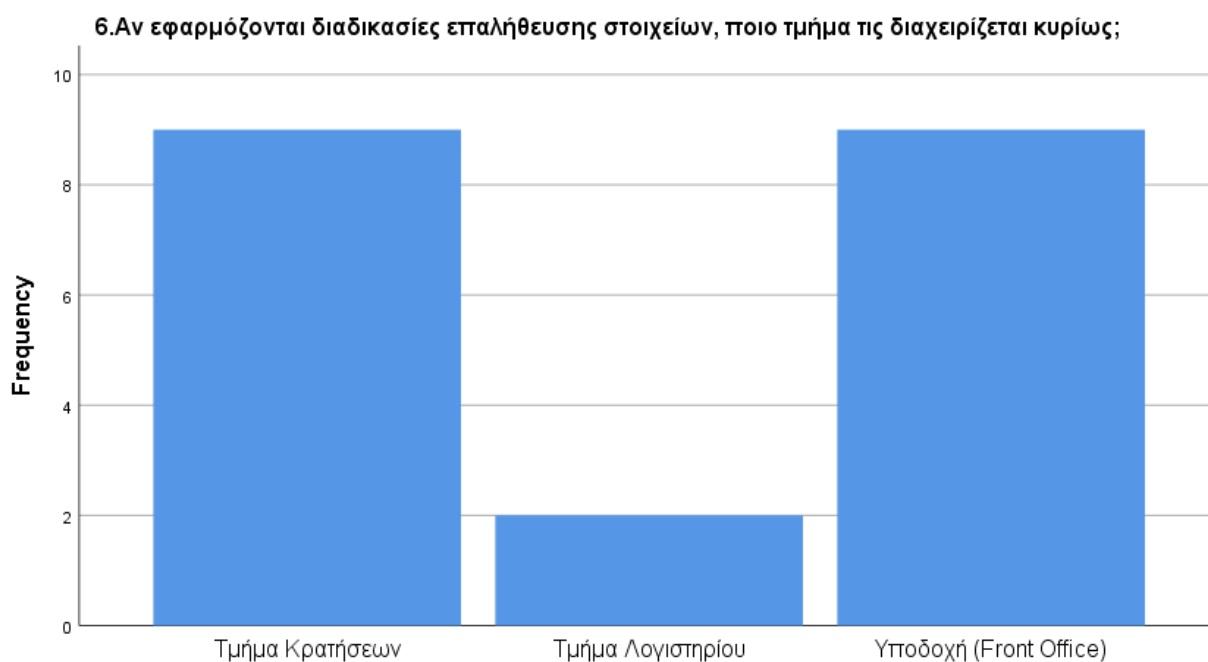




Στην ερώτηση 5, σχετικά με την ύπαρξη πολιτικής KYC, 9 επιχειρήσεις (45%) δήλωσαν ότι εφαρμόζουν σχετική πολιτική, 8 επιχειρήσεις (40%) απάντησαν αρνητικά, ενώ 3 επιχειρήσεις (15%) ανέφεραν ότι δεν γνωρίζουν.



Αναφορικά με το τμήμα που διαχειρίζεται κυρίως τις διαδικασίες επαλήθευσης (ερώτηση 6), 9 επιχειρήσεις (45%) ανέφεραν το Τμήμα Κρατήσεων και 9 επιχειρήσεις (45%) την Υποδοχή (Front Office), ενώ μόλις 2 επιχειρήσεις (10%) δήλωσαν το Τμήμα Λογιστηρίου.



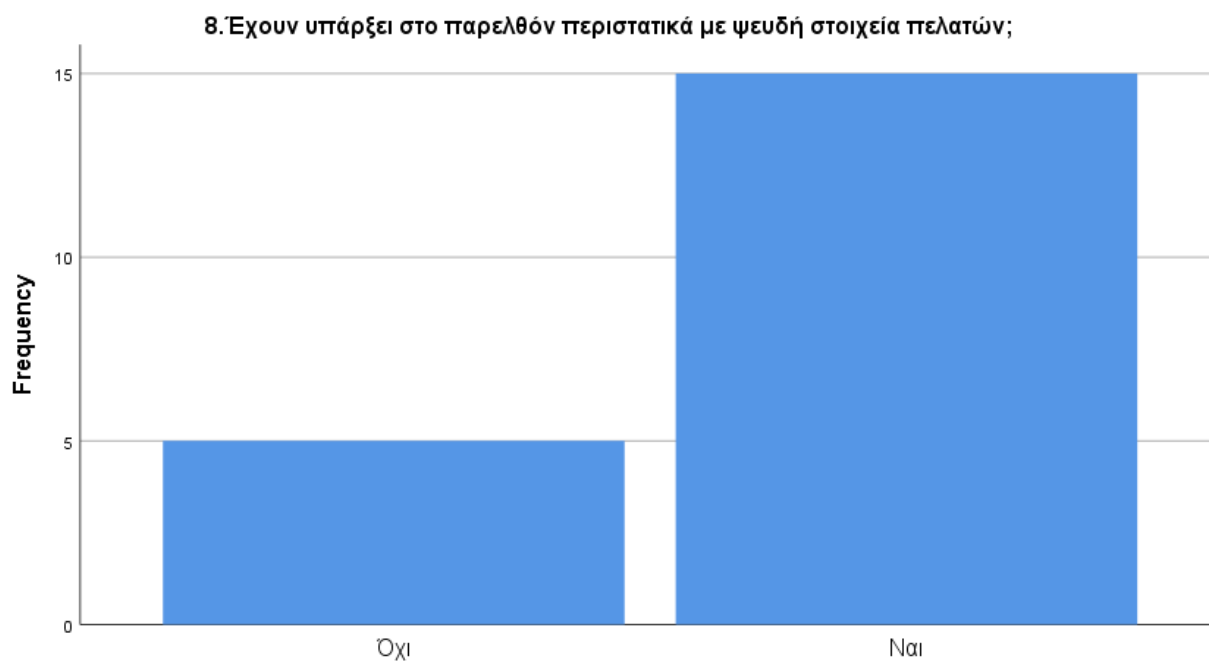
6.Αν εφαρμόζονται διαδικασίες επαλήθευσης στοιχείων, ποιο τμήμα τις διαχειρίζεται κυρίως;

Στην ερώτηση 7, σχετικά με την εκπαίδευση του προσωπικού σε θέματα εσωτερικού ελέγχου και αποτροπής απάτης, 11 επιχειρήσεις (55%) δήλωσαν ότι παρέχουν περιορισμένη εκπαίδευση, 7 επιχειρήσεις (35%) ότι εκπαιδεύουν σε τακτική βάση, ενώ 2 επιχειρήσεις (10%) ανέφεραν ότι δεν παρέχουν εκπαίδευση.



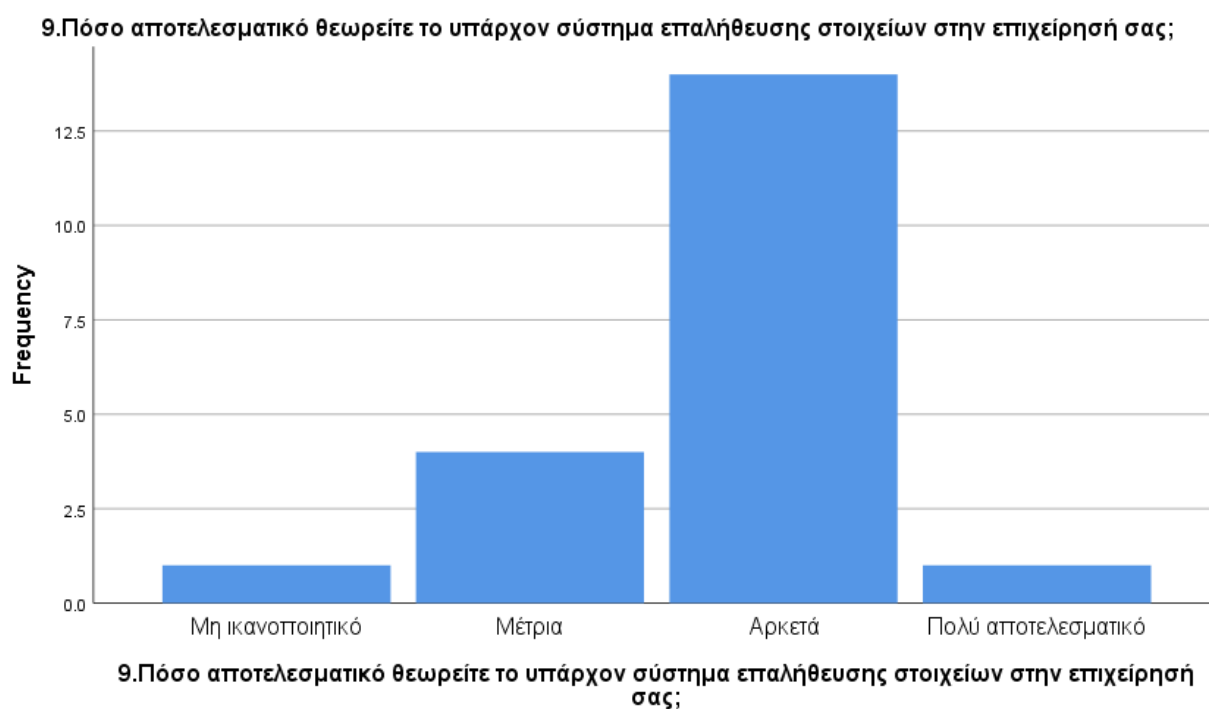
7. Έχετε εκπαιδεύσει το προσωπικό σας σε ζητήματα εσωτερικού ελέγχου και αποτροπής απάτης;

Στην ερώτηση 8, 15 επιχειρήσεις (75%) ανέφεραν ότι έχουν υπάρξει περιστατικά με ψευδή στοιχεία πελατών, ενώ 5 επιχειρήσεις (25%) απάντησαν αρνητικά.



8. Έχουν υπάρξει στο παρελθόν περιστατικά με ψευδή στοιχεία πελατών;

Όσον αφορά την αποτελεσματικότητα του υφιστάμενου συστήματος επαλήθευσης (ερώτηση 9), 14 επιχειρήσεις (70%) το αξιολόγησαν ως «αρκετά» αποτελεσματικό, 4 επιχειρήσεις (20%) ως «μέτρια», 1 επιχείρηση (5%) ως «πολύ αποτελεσματικό» και 1 επιχείρηση (5%) ως «μη ικανοποιητικό».

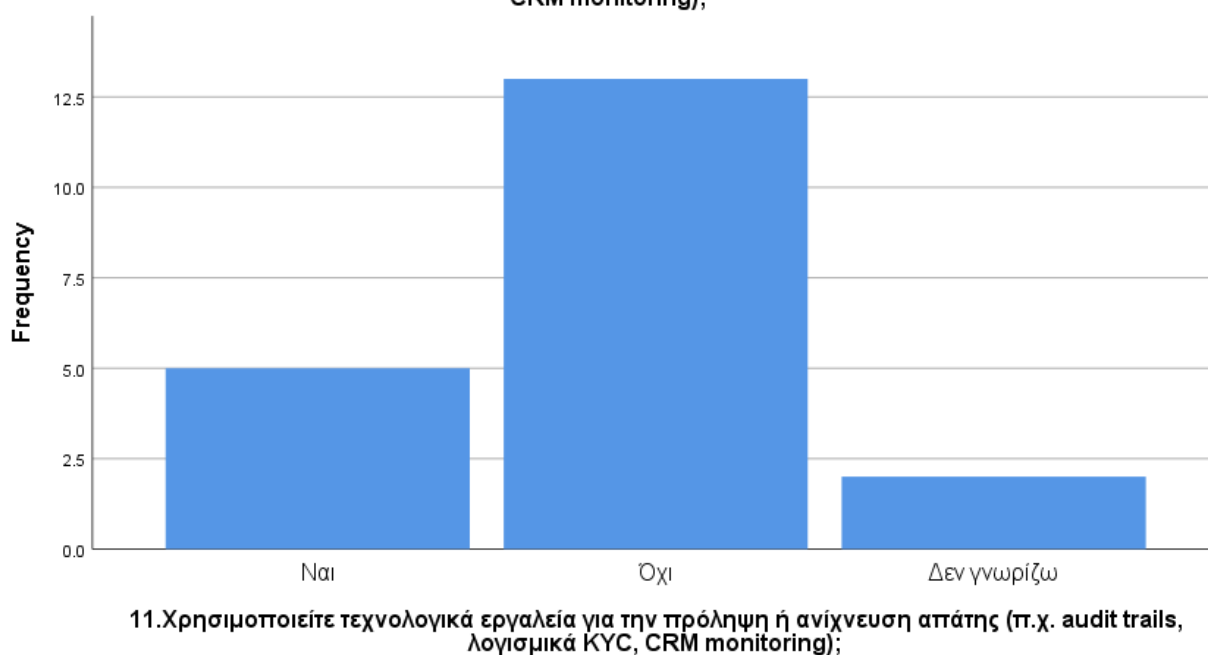


Στην ερώτηση 10, 10 επιχειρήσεις (50%) θεωρούν ότι απαιτείται αναβάθμιση των εσωτερικών ελέγχων, 7 επιχειρήσεις (35%) διαφωνούν, ενώ 3 επιχειρήσεις (15%) δηλώνουν ότι δεν γνωρίζουν.

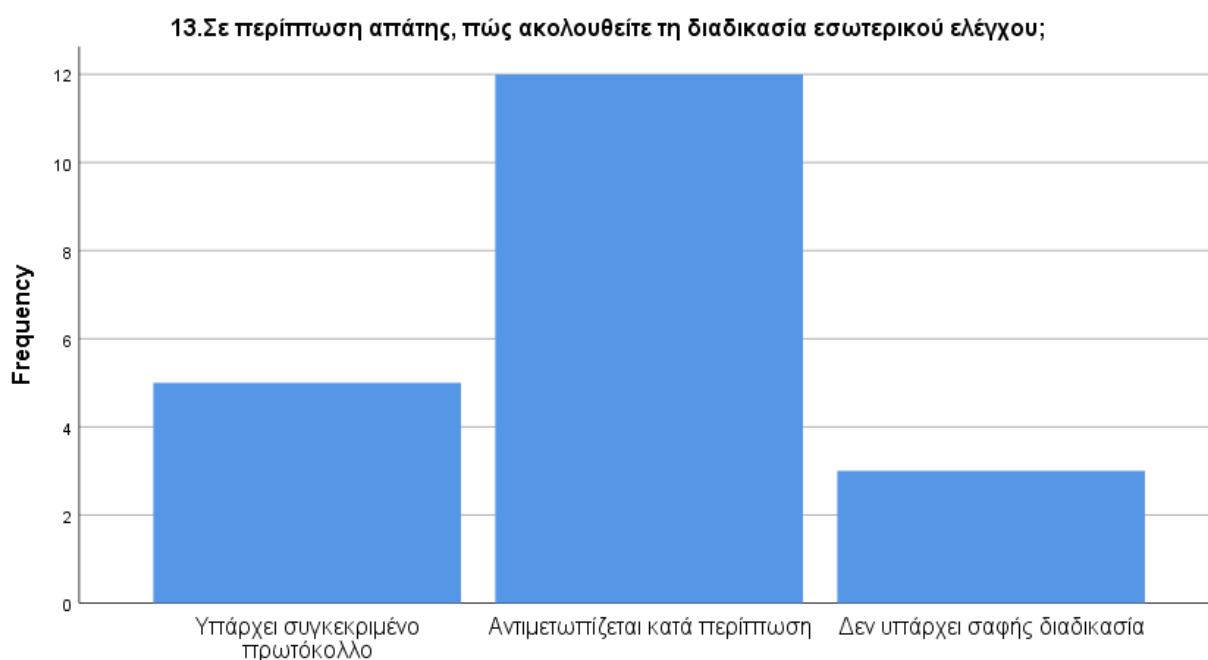


Σχετικά με τη χρήση τεχνολογικών εργαλείων (ερώτηση 11), 13 επιχειρήσεις (65%) δήλωσαν ότι δεν χρησιμοποιούν τέτοια εργαλεία, 5 επιχειρήσεις (25%) απάντησαν θετικά και 2 επιχειρήσεις (10%) δήλωσαν ότι δεν γνωρίζουν.

11. Χρησιμοποιείτε τεχνολογικά εργαλεία για την πρόληψη ή ανίχνευση απάτης (π.χ. audit trails, λογισμικά KYC, CRM monitoring);



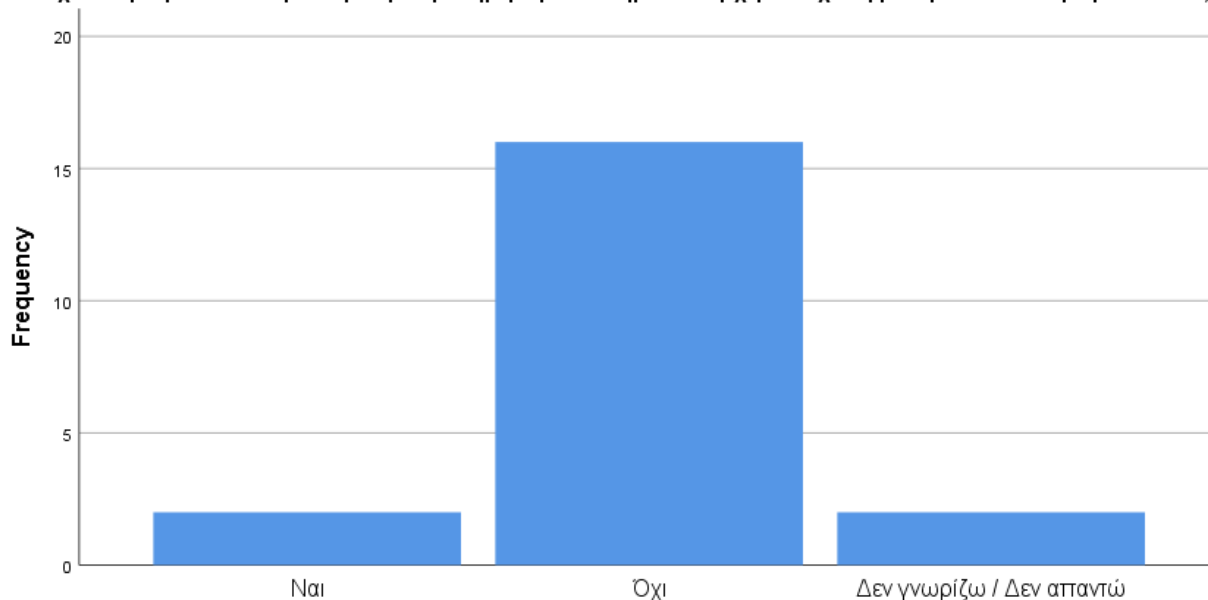
Αναφορικά με τη διαδικασία που ακολουθείται σε περίπτωση απάτης (ερώτηση 13), 12 επιχειρήσεις (60%) ανέφεραν ότι η αντιμετώπιση γίνεται κατά περίπτωση, 5 επιχειρήσεις (25%) ότι υπάρχει συγκεκριμένο πρωτόκολλο και 3 επιχειρήσεις (15%) ότι δεν υπάρχει σαφής διαδικασία.



13. Σε περίπτωση απάτης, πώς ακολουθείτε τη διαδικασία εσωτερικού ελέγχου;

Στην ερώτηση 14, 16 επιχειρήσεις (80%) δήλωσαν ότι δεν έχει επιβληθεί πρόστιμο ή παρατήρηση, 2 επιχειρήσεις (10%) ανέφεραν ότι έχει επιβληθεί, ενώ 2 επιχειρήσεις (10%) δεν γνώριζαν ή δεν απάντησαν.

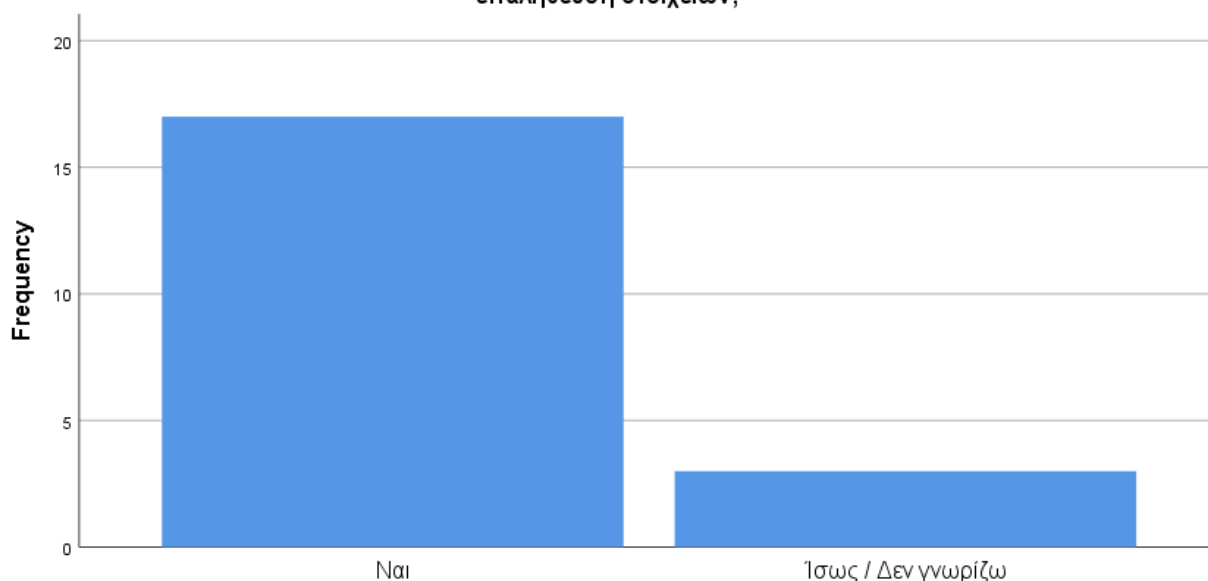
14. Έχει επιβληθεί ποτέ πρόστιμο ή παρατήρηση από δημόσια αρχή σε σχέση με την ταυτοποίηση πελατών;



14. Έχει επιβληθεί ποτέ πρόστιμο ή παρατήρηση από δημόσια αρχή σε σχέση με την ταυτοποίηση πελατών;

Στην ερώτηση 15, 17 επιχειρήσεις (85%) θεωρούν ότι χρειάζονται περισσότερες κατευθυντήριες οδηγίες από την Πολιτεία ή τις Αρχές, ενώ 3 επιχειρήσεις (15%) απάντησαν «Ίσως / Δεν γνωρίζω».

15. Θεωρείτε πως χρειάζονται περισσότερες κατευθυντήριες οδηγίες από την Πολιτεία ή τις Αρχές για την επαλήθευση στοιχείων;



15. Θεωρείτε πως χρειάζονται περισσότερες κατευθυντήριες οδηγίες από την Πολιτεία ή τις Αρχές για την επαλήθευση στοιχείων;

Συμπεράσματα

Η επαλήθευση των στοιχείων των πελατών σε μεγάλα ξενοδοχεία αποτελεί μια κρίσιμη λειτουργική και στρατηγική πρόκληση στο σύγχρονο τουριστικό περιβάλλον. Οι αυξανόμενοι κίνδυνοι ασφαλείας, οι απαιτήσεις συμμόρφωσης με τους κανονισμούς και οι αυξανόμενες προσδοκίες των επισκεπτών για απρόσκοπτη εξυπηρέτηση έχουν αποκαλύψει τους περιορισμούς των παραδοσιακών μεθόδων επαλήθευσης ταυτότητας, όπως η χειροκίνητη επιθεώρηση ταυτότητας και η επαλήθευση ταυτότητας με κάρτα-κλειδί. Σε μεγάλες εγκαταστάσεις, όπου η ροή των επισκεπτών είναι υψηλή και τα σημεία πρόσβασης είναι πολυάριθμα, οι επαναλαμβανόμενες διαδικασίες επαλήθευσης ταυτότητας συχνά δημιουργούν εμπόδια στην εξυπηρέτηση, λειτουργική αναποτελεσματικότητα και μείωση της ικανοποίησης των πελατών.

Η ενσωμάτωση συστημάτων διαχείρισης ταυτότητας και πρόσβασης (IAM), αυτοματοποιημένης ψηφιακής επαλήθευσης ταυτότητας και βιομετρικών τεχνολογιών —ιδίως συστημάτων αναγνώρισης προσώπου (FRS)— προσφέρει μια τεχνολογικά ισχυρή εναλλακτική λύση. Αυτά τα συστήματα βελτιώνουν την ακρίβεια, μειώνουν τους κινδύνους απάτης, απλοποιούν τον έλεγχο πρόσβασης σε περιορισμένες περιοχές και βελτιστοποιούν τις διαδικασίες check-in και πληρωμής. Ωστόσο, η εφαρμογή τους πρέπει να ισορροπείται προσεκτικά με τους κανονισμούς προστασίας δεδομένων, τα μέτρα ασφάλειας στον κυβερνοχώρο και τις ηθικές παραμέτρους που αφορούν την επεξεργασία βιομετρικών δεδομένων.

Το πρόβλημα της επαλήθευσης των στοιχείων των πελατών σε μεγάλα ξενοδοχεία δεν είναι απλώς ένα τεχνικό ζήτημα, αλλά ένα πολυδιάστατο ζήτημα διαχείρισης που αφορά την ασφάλεια, την λειτουργική αποδοτικότητα, την ιδιωτικότητα και την εμπειρία των πελατών. Η βιώσιμη υιοθέτηση προηγμένων τεχνολογιών ελέγχου ταυτότητας εξαρτάται από την επίτευξη ισορροπίας μεταξύ των ενισχυμένων ελέγχων ασφαλείας και της διατήρησης της εμπιστοσύνης και της άνεσης των επισκεπτών.

Πατσαρούχας Παναγιώτης Βασίλειος, «Το πρόβλημα της εξακρίβωσης στοιχείων των πελατών στις μεγάλες επιχειρήσεις στη Μύκονο - Μελέτη περίπτωσης των μεγάλων ξενοδοχειακών μονάδων της Μυκόνου»

Η μελέτη αυτή είχε ως στόχο να περιγράψει τις τεχνικές επαλήθευσης και διαχείρισης των δεδομένων πελατών που χρησιμοποιούν οι ξενοδοχειακές επιχειρήσεις στη Μύκονο. Τα ευρήματα έδειξαν ένα ποικίλο τοπίο όσον αφορά τη δομή, την τυποποίηση και την τεχνική υποστήριξη των διαδικασιών ταυτοποίησης.

Αρχικά παρατηρήθηκε ότι η βασική πρακτική της ταυτοποίησης μέσω ταυτότητας ή διαβατηρίου εφαρμόζεται σχεδόν καθολικά (19 από τις 20 επιχειρήσεις). Ωστόσο, οι συμπληρωματικές διαδικασίες επαλήθευσης, όπως η καταγραφή των στοιχείων της πιστωτικής κάρτας ή η λήψη υπογραφών, δεν εφαρμόζονται ομοιόμορφα από όλες τις επιχειρήσεις, γεγονός που υποδηλώνει μια διαφορά στο επίπεδο εποπτείας.

Ταυτόχρονα, λιγότερες από τις μισές επιχειρήσεις (9 από τις 20) ανέφεραν ότι διαθέτουν επίσημη πολιτική KYC, ενώ ένα σημαντικό ποσοστό είτε δεν εφαρμόζει τέτοια στρατηγική είτε δεν γνωρίζει την ύπαρξή της. Αυτό υποδηλώνει ότι οι διαδικασίες επαλήθευσης δεν ενσωματώνονται με συνέπεια σε μια συνεκτική ρυθμιστική δομή εντός του οργανισμού.

Σημειωτέον ότι 15 από τους 20 οργανισμούς έχουν αναφέρει περιστατικά εσφαλμένων πληροφοριών πελατών στο παρελθόν, υπογραμμίζοντας τη σημασία του ζητήματος. Ενώ η πλειονότητα των οργανισμών (14) αξιολογεί το τρέχον σύστημα ως «αρκετά» αποτελεσματικό, μόνο μία εταιρεία το θεωρεί «πολύ αποτελεσματικό» και δέκα εταιρείες υποστηρίζουν ότι οι εσωτερικοί έλεγχοι απαιτούν βελτίωση.

Επιπλέον, παρατηρήθηκε περιορισμένη εφαρμογή τεχνικών μέσων για την πρόληψη και τον εντοπισμό της απάτης, με 13 από τις 20 οργανώσεις να δηλώνουν ότι δεν χρησιμοποιούν τέτοιες λύσεις. Ταυτόχρονα, τα περιστατικά απάτης αντιμετωπίζονται κυρίως μεμονωμένα (12 οργανώσεις), ενώ μόνο 5 ανέφεραν ότι έχουν καθιερώσει μια συγκεκριμένη μεθοδολογία.

Η συντριπτική πλειοψηφία των επιχειρήσεων (17 από τις 20) υποστηρίζει ότι απαιτείται πρόσθετη καθοδήγηση από το κράτος ή τις αρμόδιες αρχές. Το εύρημα αυτό υποδηλώνει την ανάγκη ενίσχυσης της θεσμικής δομής και θέσπισης πιο σαφών κανόνων για την αποτελεσματική εφαρμογή των πρωτοκόλλων επαλήθευσης δεδομένων στον ξενοδοχειακό κλάδο.

Πατσαρούχας Παναγιώτης Βασίλειος, «Το πρόβλημα της εξακρίβωσης στοιχείων των πελατών στις μεγάλες επιχειρήσεις στη Μύκονο - Μελέτη περίπτωσης των μεγάλων ξενοδοχειακών μονάδων της Μυκόνου»

Τα ευρήματα δείχνουν ότι, αν και υπάρχουν βασικές μέθοδοι ταυτοποίησης, οι διαδικασίες επαλήθευσης και εσωτερικού ελέγχου δεν είναι ομοιόμορφα τυποποιημένες ή τεχνολογικά προηγμένες σε όλους τους οργανισμούς του δείγματος.

Βιβλιογραφία

- Abdrahamane Wone, Manno, J. D., Charrier, C., & Rosenberger, C. (2021). *Impact Of Environmental Conditions On Fingerprint Systems Performance*. 1–5.
<https://doi.org/10.1109/pst52912.2021.9647754>
- Alay, N., & Al-Baity, H. H. (2020). Deep Learning Approach for Multimodal Biometric Recognition System Based on Fusion of Iris, Face, and Finger Vein Traits. *Sensors*, 20(19), 5523. <https://doi.org/10.3390/s20195523>
- Algarni, A. D., El Banby, G., Ismail, S., El-Shafai, W., El-Samie, F. E. A., & F. Soliman, N. (2020). Discrete Transforms and Matrix Rotation Based Cancelable Face and Fingerprint Recognition for Biometric Security Applications. *Entropy*, 22(12), 1361. <https://doi.org/10.3390/e22121361>
- Almulla, S. A., & Yeun, C. Y. (2010, March). Cloud computing security management. In *2010 Second International Conference on Engineering System Management and Applications* (pp. 1-7). IEEE.
- Álvarez-Aparicio, C., Guerrero-Higueras, Á. M., González-Santamarta, M. Á., Campazas-Vega, A., Matellán, V., & Fernández-Llamas, C. (2022). Biometric recognition through gait analysis. *Scientific Reports*, 12(1). <https://doi.org/10.1038/s41598-022-18806-4>
- Anderson, A. N., Arthur, H. A., & Ackon, J. (2025). Impacts of Biometric Technology in the Tourism and Hospitality Industry.
- Atsushi Ugajin. (2023). *Automation in Hospitals and Health Care*. 1209–1233.
https://doi.org/10.1007/978-3-030-96729-1_56
- Azhar, I. (2015, March 1). *The Interaction Between Artificial Intelligence and Identity & Access Management: An Empirical study*. Papers.ssrn.com.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3905771
- Bilgihan, A., Karadag, E., Cobanoglu, C., & Okumus, F. (2013). Research Note: Biometric Technology Applications and Trends in Hotels. *Rosen Faculty Scholarship and Creative Works*, 31(2). <https://stars.library.ucf.edu/rosenscholar/18/>

- Bodkhe, U., Bhattacharya, P., Tanwar, S., Tyagi, S., Kumar, N., & Obaidat, M. S. (2019, August 1). *BloHosT: Blockchain Enabled Smart Tourism and Hospitality Management*. IEEE Xplore. <https://doi.org/10.1109/CITS.2019.8862001>
- Boo, H. C., & Chua, B. L. (2022). An integrative model of facial recognition check-in technology adoption intention: the perspective of hotel guests in Singapore. *International Journal of Contemporary Hospitality Management*, 34(11), 4052-4079.
- Brotherton, B., & Wood, R. C. (2013). Hospitality and hospitality management. In *In search of hospitality* (pp. 134-156). Routledge.
- Brynjolfsson, E., & McAfee, A. (2012). *Race against the machine: How the digital revolution is accelerating innovation, driving productivity, and irreversibly transforming employment and the economy*. Brynjolfsson and McAfee.
- Buhalis, D., Harwood, T., Bogicevic, V., Viglia, G., Beldona, S., & Hofacker, C. (2019). Technological Disruptions in services: Lessons from Tourism and Hospitality. *Journal of Service Management*, 30(4), 484–506.
- Burt, C. (2018). Agilysys adds facial recognition to hospitality management system. *BiometricUpdate.com*.
- Chathoth, P. K., Ungson, G. R., Altinay, L., Chan, E. S. W., Harrington, R., & Okumus, F. (2014). Barriers affecting organisational adoption of higher order customer engagement in tourism service interactions. *Tourism Management*, 42, 181–193. <https://doi.org/10.1016/j.tourman.2013.12.002>
- Chen, L., Zhao, X., Zhao, R., Yuan, G., Zhang, S., Chen, S., & Wu, F. (2022). Mobile Internet Access Control Strategy Based on Trust Perception. *Lecture Notes in Computer Science*, 598–611. https://doi.org/10.1007/978-3-031-06791-4_47
- Compagnucci, M. C., Meszaros, J., Minssen, T., Arasilango, A., Ous, T., & Rajarajan, M. (2019). Homomorphic encryption: The'holy grail'for big data analytics and legal compliance in the pharmaceutical and healthcare sector?. *EPLR*, 3, 144.
- Dargan, S., & Kumar, M. (2020). A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities. *Expert Systems with Applications*, 143, 113114. <https://doi.org/10.1016/j.eswa.2019.113114>

- Davenport, T., Ronanki, R., Wheaton, J., & Nguyen, A. (2018). *Artificial Intelligence for the Real World*.
https://academicjptoday.com/assets/documents/Artificial_Intelligence_for_the_Real_World_-_HBR.pdf
- Delia Gabriela Moisa, & Michopoulou, E. (2022). IT and Well-Being in Travel and Tourism. *Springer EBooks*, 1715–1741. https://doi.org/10.1007/978-3-030-48652-5_106
- Demirel, E., Karagöz Zeren, S., & Hakan, K. (2021). Smart contracts in tourism industry: a model with blockchain integration for post pandemic economy. *Current Issues in Tourism*, 1–15. <https://doi.org/10.1080/13683500.2021.1960280>
- Dijmărescu, I., Iatagan, M., Hurloiu, I., Geamănu, M., Ruscescu, C., & Dijmărescu, A. (2022). Neuromanagement decision making in facial recognition biometric authentication as a mobile payment technology in retail, restaurant, and hotel business models. *Oeconomia Copernicana*, 13(1), 225-250.
- Electronic Data System. (2005). Survey finds consumers open to the use of innovative identification methods such as biometrics. Retrieved October, 7, 2005, from www.fndbiometrics.com/Pages/feature%20articles/innovative-uses.html
- Erceg, A., Damoska Sekuloska, J., & Kelić, I. (2020). Blockchain in the Tourism Industry—A Review of the Situation in Croatia and Macedonia. *Informatics*, 7(1), 5. <https://doi.org/10.3390/informatics7010005>
- Erkan, M., Okutmuş, E., & Ergül, A. (2017). The internal control system in the prevention of mistakes and fraud: An application in hospitality management. In *Sustainability and Management* (pp. 119-138). Routledge.
- Farrell, S. (2016). How airports can fly to self-service biometrics. *Biometric Technology Today*, 2016(1), 5–7. [https://doi.org/10.1016/s0969-4765\(16\)30016-9](https://doi.org/10.1016/s0969-4765(16)30016-9)
- Figini, P., Vici, L., & Viglia, G. (2020). A comparison of hotel ratings between verified and non-verified online review platforms. *International Journal of Culture, Tourism and Hospitality Research*, 14(2), 157–171. <https://doi.org/10.1108/ijcthr-10-2019-0193>
- Gangwar, V. P., & Reddy, D. (2023). *Hospitality Industry 5.0: Emerging Trends in Guest Perception and Experiences*. Wwww.igi-Global.com; IGI Global. <https://www.igi-global.com/chapter/hospitality-industry-50/320731>

Πατσαρούχας Παναγιώτης Βασίλειος, «Το πρόβλημα της εξακρίβωσης στοιχείων των πελατών στις μεγάλες επιχειρήσεις στη Μύκονο - Μελέτη περίπτωσης των μεγάλων ξενοδοχειακών μονάδων της Μυκόνου»

- Gao, N., Han, D., Weng, T.-H., Xia, B., Li, D., Castiglione, A., & Li, K.-C. (2022). Modeling and analysis of port supply chain system based on Fabric blockchain. *Computers & Industrial Engineering*, 172, 108527. <https://doi.org/10.1016/j.cie.2022.108527>
- Grobbelaar, W., Verma, A., & Shukla, V. K. (2024). Blockchain Integration in the Hospitality Industry. *Apple Academic Press EBooks*, 25–47. <https://doi.org/10.1201/9781003432951-3>
- Gupta, B. (2008). *Biometrics: Enhancing Security in Organizations E-Government/Technology Series*. <https://www.businessofgovernment.org/sites/default/files/GuptaReport.pdf>
- Hallin, C. A., & Marnburg, E. (2008). Knowledge management in the hospitality industry: A review of empirical research. *Tourism management*, 29(2), 366-381.
- Hammed Asorona, & Muhammad Ateeq. (2024). *Digitization and e-Verification of Medical Certificates In Alimosho General Hospital, Lagos, Nigeria*. <https://doi.org/10.1109/assic60049.2024.10508022>
- Hilsman, S. (2024). Toward a Biometric Privacy Act to Protect Individual Rights: What the United States Can Learn from the European Union and China. *Cardozo Int'l & Comp. L. Rev.*, 7, 993.
- Hsieh, M. Y., Weng, T. H., Wang, P. W., & Kao, C. H. (2022). Recommendation service for hotel applications on blockchain. *International Journal of Computational Science and Engineering*, 25(6), 629. <https://doi.org/10.1504/ijcse.2022.127184>
- Hua, N., Li, B., & Zhang, T. (2020). Crime research in hospitality and tourism. *International Journal of Contemporary Hospitality Management*, 32(3), 1299-1323.
- International Biometric Group. (2004). Biometric Market and Industry Report 2004- 2008. Retrieved September 1, 2005, from http://www.biometricgroup.com/reports/public/market_report.html
- Irannezhad, E., & Mahadevan, R. (2020). Is blockchain tourism's new hope? *Journal of Hospitality and Tourism Technology*, 12(1), 85–96. <https://doi.org/10.1108/jhtt-02-2019-0039>
- Jackson, L. A. (2009). Biometric technology: the future of identity assurance and authentication in the lodging industry. *International Journal of Contemporary*

Πατσαρούχας Παναγιώτης Βασιλείος, «Το πρόβλημα της εξακρίβωσης στοιχείων των πελατών στις μεγάλες επιχειρήσεις στη Μύκονο - Μελέτη περίπτωσης των μεγάλων ξενοδοχειακών μονάδων της Μυκόνου»

Hospitality Management, 21(7), 892–905.

<https://doi.org/10.1108/09596110910985340>

Jain, A. K., Nandakumar, K., & Ross, A. (2016). 50 years of biometric research:

Accomplishments, challenges, and opportunities. *Pattern Recognition Letters*, 79(79), 80–105. <https://doi.org/10.1016/j.patrec.2015.12.013>

Jain, A. K., Ross, A., & Prabhakar, S. (2004). An Introduction to Biometric Recognition.

IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 4–20.

<https://doi.org/10.1109/tcsvt.2003.818349>

Jain, A., Bolle, R., & Pankanti, S. (2011). Introduction to Biometrics. *Biometrics*, 1–41.

https://doi.org/10.1007/0-306-47044-6_1

Jirsa, P. (2020). *Strategies to Mitigate the Effects of Identity Theft in the Hospitality Industry*.

Proquest.com.

<https://search.proquest.com/openview/cab87a744b50ab85b77d4b81879f5f62/1?pq-origsite=gscholar&cbl=18750&diss=y>

Karie, N. M., Kebande, V. R., Ikuesan, R. A., Sookhak, M., & Venter, H. S. (2020).

Hardening SAML by Integrating SSO and Multi-Factor Authentication (MFA) in the Cloud. *Proceedings of the 3rd International Conference on Networking, Information Systems & Security*. <https://doi.org/10.1145/3386723.3387875>

Kim, J. (Sunny). (2016). An extended technology acceptance model in behavioral intention

toward hotel tablet apps with moderating effects of gender and age. *International Journal of Contemporary Hospitality Management*, 28(8), 1535–1553.

<https://doi.org/10.1108/ijchm-06-2015-0289>

Kwon, W., Lee, M., & Back, K.-J. (2020). Exploring the underlying factors of customer

value in restaurants: A machine learning approach. *International Journal of Hospitality Management*, 91, 102643. <https://doi.org/10.1016/j.ijhm.2020.102643>

Lehto, X. Y., Park, S., Mohamed, M. E., & Lehto, M. R. (2021). Traveler Attitudes Toward

Biometric Data-Enabled Hotel Services: Can Risk Education Play a Role? *Cornell Hospitality Quarterly*, 64(1), 193896552110632.

<https://doi.org/10.1177/19389655211063204>

- Liu, X. (2022). A Risk-based Approach to Cybersecurity: A Case Study of Financial Messaging Networks Data Breaches. *The Coastal Business Journal*, 18(1).
<https://digitalcommons.coastal.edu/cbj/vol18/iss1/2/>
- Malik, N. G. (2024). Biometric Authentication-Risks and advancements in biometric security systems. *Journal of Computer Science and Technology Studies*, 6(3), 159–180.
<https://doi.org/10.32996/jcsts.2024.6.3.14>
- Martínez, P., & Del Bosque, I. R. (2014). Analyzing Responsible Corporate Identity in the Hospitality Sector: A Case Study. *Tourism Culture & Communication*, 14(3), 183–197. <https://doi.org/10.3727/109830415x14213698267398>
- Martínez, P., Pérez, A., & Rodríguez del Bosque, I. (2013). Exploring the Role of CSR in the Organizational Identity of Hospitality Companies: A Case from the Spanish Tourism Industry. *Journal of Business Ethics*, 124(1), 47–66. <https://doi.org/10.1007/s10551-013-1857-1>
- Mohammed, I. A. (2019). Cloud identity and access management—a model proposal. *International Journal of Innovations in Engineering Research and Technology*, 6(10), 1-8.
- Moisa, D. G., & Michopoulou, E. (2022). IT and well-being in travel and tourism. In *Handbook of e-Tourism* (pp. 1-27). Cham: Springer International Publishing.
- Moisa, D. G., & Michopoulou, E. (2022). IT and well-being in travel and tourism. In *Handbook of e-Tourism* (pp. 1-27). Cham: Springer International Publishing.
- Morosan, C. (2010). Theoretical and Empirical Considerations of Guests' Perceptions of Biometric Systems in Hotels. *Journal of Hospitality & Tourism Research*, 36(1), 52–84. <https://doi.org/10.1177/1096348010380601>
- Morosan, C. (2012). Understanding the Antecedents of Perceived Value of Registered Traveler Biometric Systems. *Journal of Hospitality Marketing & Management*, 21(8), 872–896. <https://doi.org/10.1080/19368623.2012.631728>
- Morosan, C., & Hilton, C. (2020). HOTEL FACIAL RECOGNITION SYSTEMS: INSIGHT INTO GUESTS' SYSTEM PERCEPTIONS, CONGRUITY WITH SELF- IMAGE, AND ANTICIPATED EMOTIONS. *Journal of Electronic Commerce Research*, 21, 2020. http://jecr.org/sites/default/files/2020vol21no1_Paper2.pdf

- Musa, M., Rahman, P., Kang, Z., & Hossain, S. F. A. (2022). Technology Application in the Chinese Tourism Industry. *Technology Application in Tourism in Asia*, 219–239. https://doi.org/10.1007/978-981-16-5461-9_13
- Nanavati, S. (2004). Biometrics: Identity Verification in a Networked World. *Kybernetes: The International Journal of Systems & Cybernetics*, 33(5-6), 5-6.
- Nilesh Ratnoday, Naiya Rana Ratnoday, Sharma, C., Saxena, M., & Banerjee, A. (2025). *Facial Recognition Technology for Seamless Check-In and Personalized Guest Service*. 54(2), 542–551. <https://doi.org/10.48047/CU/54/02/542-551>
- Nilesh Ratnoday, Naiya Rana Ratnoday, Sharma, C., Saxena, M., & Banerjee, A. (2025). *Facial Recognition Technology for Seamless Check-In and Personalized Guest Service*. 54(2), 542–551. <https://doi.org/10.48047/CU/54/02/542-551>
- Nuria Ruiz Lacaci, Menéndez, A. R., & Belmonte, A. V. (2024). Understanding tourism consumer behavior using biometric technologies: bibliographic review and research agenda. *Tourism & Management Studies*, 20(4), 15–32. <https://dialnet.unirioja.es/descarga/articulo/9532038.pdf>
- Nusair, K. “Khal”, Bilgihan, A., Okumus, F., & Cobanoglu, C. (2013). Generation Y travelers’ commitment to online social network websites. *Tourism Management*, 35, 13–22. <https://doi.org/10.1016/j.tourman.2012.05.005>
- Oloyede, M. O., Hancke, G. P., & Myburgh, H. C. (2020). A review on face recognition systems: recent approaches and challenges. *Multimedia Tools and Applications*, 79(37-38), 27891–27922. <https://doi.org/10.1007/s11042-020-09261-2>
- Oloyede, M. O., Hancke, G. P., & Myburgh, H. C. (2020). A review on face recognition systems: recent approaches and challenges. *Multimedia Tools and Applications*, 79(37-38), 27891–27922. <https://doi.org/10.1007/s11042-020-09261-2>
- P Tripathi, K. (2011). A Comparative Study of Biometric Technologies with Reference to Human Interface. *International Journal of Computer Applications*, 14(5), 10–15. <https://doi.org/10.5120/1842-2493>
- Pulido-Gaytan, B., Tchernykh, A., Cortés-Mendoza, J. M., Babenko, M., Radchenko, G., Avetisyan, A., & Drozdov, A. Y. (2021). Privacy-preserving neural networks with Homomorphic encryption: Challenges and opportunities. *Peer-To-Peer Networking and Applications*, 14(3), 1666–1691. <https://doi.org/10.1007/s12083-021-01076-8>

- Rashed Isam Ashqar, Ashqar, H. I., & Ramos, Q. (2024). Identity and Access Management in Tourism and Hospitality. *Lecture Notes in Networks and Systems*, 323–332. https://doi.org/10.1007/978-3-031-44131-8_32
- Sagar, G., & Vitalii Syrovatskyi. (2022). Information Security: Safeguarding Resources and Building Trust. *Apress EBooks*, 275–324. https://doi.org/10.1007/978-1-4842-8658-6_6
- Selian, A. N., & McKnight, L. (2017). The Role of Technology in the History of Well-Being: Transformative Market Phenomena Over Time. *International Handbooks of Quality-of-Life*, 639–687. https://doi.org/10.1007/978-3-319-39101-4_19
- Sestino, A., & De Mauro, A. (2021). Leveraging Artificial Intelligence in Business: Implications, Applications and Methods. *Technology Analysis & Strategic Management*, 34(1), 1–14. <https://doi.org/10.1080/09537325.2021.1883583>
- Sharma, R., Kumar, A., & Chuah, C. (2021). Turning the blackbox into a glassbox: An explainable machine learning approach for understanding hospitality customer. *International Journal of Information Management Data Insights*, 1(2), 100050. <https://doi.org/10.1016/j.jjime.2021.100050>
- Singh, G., Bhardwaj, G., Singh, S. V., & Garg, V. (2021). Biometric Identification System: Security and Privacy Concern. *Artificial Intelligence for a Sustainable Industry 4.0*, 245–264. https://doi.org/10.1007/978-3-030-77070-9_15
- Singh, G., Bhardwaj, G., Singh, S. V., & Garg, V. (2021). Biometric Identification System: Security and Privacy Concern. *Artificial Intelligence for a Sustainable Industry 4.0*, 245–264. https://doi.org/10.1007/978-3-030-77070-9_15
- Singh, N., Agrawal, A., & Khan, R. A. (2018). Voice Biometric: A Technology for Voice Based Authentication. *Advanced Science, Engineering and Medicine*, 10(7), 754–759. <https://doi.org/10.1166/ asem.2018.2219>
- Son, H. X., & Chen, E. (2019). Towards a fine-grained access control mechanism for privacy protection and policy conflict resolution. *International Journal of Advanced Computer Science and Applications*, 10(2).
- Srinivasan, R. (2018). *Whose global village?: Rethinking how technology shapes our world*. NYU Press.

- Srinivasan, S., Raja, R., Jehan, C., S. Murugan, Srinivasan, C., & M. Muthulekshmi. (2024). *IoT-Enabled Facial Recognition for Smart Hospitality for Contactless Guest Services and Identity Verification*. <https://doi.org/10.1109/icrito61523.2024.10522363>
- Štilić, A., Nicić, M., & Puška, A. (2023). Check-In to the future: Exploring the impact of contemporary information technologies and artificial intelligence on the hotel industry. *Turističko Poslovanje*, 31. <https://doi.org/10.5937/turpos0-43739>
- Štilić, A., Nicić, M., & Puška, A. (2023). Check-In to the future: Exploring the impact of contemporary information technologies and artificial intelligence on the hotel industry. *Turističko Poslovanje*, 31. <https://doi.org/10.5937/turpos0-43739>
- Subir Kumar Saha, Sifat Nawrin Nova, & Md. Ishtiaq Iqbal. (2023). *Healthcare Professionals Credential Verification Model Using Blockchain-Based Self-sovereign Identity*. 381–392. https://doi.org/10.1007/978-981-19-9483-8_32
- Taher, K. A., Nahar, T., & Hossain, S. A. (2019). Enhanced Cryptocurrency Security by Time-Based Token Multi-Factor Authentication Algorithm. *2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)*. <https://doi.org/10.1109/icrest.2019.8644084>
- Tanrisever, C., Pamukçu, H., & Sharma, A. (Eds.). (2024). *Future Tourism Trends Volume 2: Technology Advancement, Trends and Innovations for the Future in Tourism* (Vol. 2). Emerald Group Publishing.
- Taskiran, M., Kahraman, N., & Erdem, C. E. (2020). Face recognition: Past, present and future (a review). *Digital Signal Processing*, 106(102809), 102809. <https://doi.org/10.1016/j.dsp.2020.102809>
- Tepe, Y. (2022). Decentralisation of hotel and tourism industry: Effects of blockchain technology in hotel booking systems.
- Thakur, M. A., & Gaikwad, R. (2015). User identity and Access Management trends in IT infrastructure- an overview. *2015 International Conference on Pervasive Computing (ICPC)*. <https://doi.org/10.1109/pervasive.2015.7086972>
- Van, D., & Basie Von Solms. (2014). *The poor man's biometric: Identifying cost-effective biometric system criteria for SMMEs*. <https://doi.org/10.1109/istafrica.2014.6880598>

- Vaniya, S. M., & B. Bharathi. (2016). *Exploring object segmentation methods in visual surveillance for human activity recognition*. 520–525.
<https://doi.org/10.1109/icgtspicc.2016.7955356>
- Wang, L., & Alexander, C. A. (2013). Automated Identification Technology and Information Security in Digital Hospitals. *International Journal of Information and Network Security*, 2(5), 348.
- Wang, Y., Chen, Y., Bhuiyan, M. Z. A., Han, Y., Zhao, S., & Li, J. (2018). Gait-based Human identification using acoustic sensor and deep neural network. *Future Generation Computer Systems*, 86, 1228–1237.
<https://doi.org/10.1016/j.future.2017.07.012>
- Williams, P. (2019). Can all sectors of the hospitality and tourism industry be influenced by the innovation of Blockchain technology? *Worldwide Hospitality and Tourism Themes*, 11(2), 112–120. <https://doi.org/10.1108/whatt-11-2018-0077>
- Wu, W., Elliott, S. J., Lin, S., Sun, S., & Tang, Y. (2019). Review of palm vein recognition. *IET Biometrics*, 9(1), 1–10. <https://doi.org/10.1049/iet-bmt.2019.0034>
- Wynn, M., & Jones, P. (2022). IT strategy in the hotel industry in the digital era. *Sustainability*, 14(17), 10705. <https://doi.org/10.3390/su141710705>
- Ye, Y., Zhang, C., He, C., Wang, X., Huang, J., & Deng, J. (2020). A Review on Applications of Capacitive Displacement Sensing for Capacitive Proximity Sensor. *IEEE Access*, 8, 45325–45342. <https://doi.org/10.1109/ACCESS.2020.2977716>
- Youssef, A. B., Dutta, P. K., Doshi, R., & Sajnani, M. (Eds.). (2024). *AI, blockchain, and metaverse in hospitality and tourism Industry 4.0: case studies and analysis*. CRC Press.
- Βασιλείου, Δ., & Ηρειώτης, Ν. (2008). Χρηματοοικονομική Διοίκηση. Θεωρία & Πρακτική, 2η έκδοση, Εκδόσεις Rosili, Αθήνα, 18.
- Βασιλείου Δ, Ηρειώτης Ν, Μπάλιος Δ, (2009). Αρχές Χρηματοοικονομικής Λογιστικής, Χρηματοοικονομική Ανάλυση και Λήψη Αποφάσεων. Εκδοτικός Οίκος Rosili.
- Κατίκη, Σ. (2004). Τήρηση Λογαριασμών Πελατών: Main-Courante Ξενοδοχείων (Front Office Accounting-Table of Contents). Available at SSRN 2690782.
- Καρακούδα, Ε. (2014). Η λογιστική παρακολούθηση των ξενοδοχειακών επιχειρήσεων.

Παράρτημα

ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ

Θέμα: Επαλήθευση και διαχείριση δεδομένων πελατών σε ξενοδοχειακές επιχειρήσεις

ΕΝΟΤΗΤΑ Α: Βασικά χαρακτηριστικά επιχείρησης

1. Ποια είναι η κατηγορία της επιχείρησής σας;
 - Ξενοδοχείο 4 αστέρων
 - Ξενοδοχείο 5 αστέρων
 - Boutique Hotel
 - All-inclusive Resort
 - Rbnb
2. Πόσα δωμάτια (ή κλίνες) διαθέτει περίπου η μονάδα σας;
 - Κάτω από 50
 - 51–100
 - 101–200
 - Πάνω από 200
3. Η επιχείρηση ανήκει σε αλυσίδα ή είναι ανεξάρτητη μονάδα;
 - Μέλος ξενοδοχειακής αλυσίδας
 - Ανεξάρτητη μονάδα

ΕΝΟΤΗΤΑ Β: Διαδικασίες ταυτοποίησης πελατών

4. Ποιες πληροφορίες συλλέγετε κατά το check-in για την ταυτοποίηση των πελατών; (Πολλαπλές απαντήσεις)
 - Δελτίο ταυτότητας ή διαβατήριο
 - Στοιχεία πιστωτικής κάρτας
 - Υπογραφή (φυσική ή ψηφιακή)
5. Υπάρχει πολιτική KYC (Know Your Customer) στην επιχείρησή σας;
 - Ναι
 - Όχι
 - Δεν γνωρίζω

Πατσαρούχας Παναγιώτης Βασίλειος, «Το πρόβλημα της εξακρίβωσης στοιχείων των πελατών στις μεγάλες επιχειρήσεις στη Μύκονο - Μελέτη περίπτωσης των μεγάλων ξενοδοχειακών μονάδων της Μυκόνου»

6. Αν εφαρμόζονται διαδικασίες επαλήθευσης στοιχείων, ποιο τμήμα τις διαχειρίζεται κυρίως;
- Τμήμα Κρατήσεων
 - Τμήμα Λογιστηρίου
 - Υποδοχή (Front Office)

ΕΝΟΤΗΤΑ Γ: Εσωτερικός έλεγχος και απάτη

7. Έχετε εκπαιδεύσει το προσωπικό σας σε ζητήματα εσωτερικού ελέγχου και αποτροπής απάτης;
- Όχι
 - Ναι, αλλά περιορισμένα
 - Ναι, σε τακτική βάση
8. Έχουν υπάρξει στο παρελθόν περιστατικά με ψευδή στοιχεία πελατών;
- Ναι
 - Όχι
9. Πόσο αποτελεσματικό θεωρείτε το υπάρχον σύστημα επαλήθευσης στοιχείων στην επιχείρησή σας;
- Μη ικανοποιητικό
 - Μέτρια
 - Αρκετά
 - Πολύ αποτελεσματικό
10. Πιστεύετε ότι απαιτείται αναβάθμιση των εσωτερικών ελέγχων σας;
- Ναι
 - Όχι
 - Δεν γνωρίζω

ΕΝΟΤΗΤΑ Δ: Τεχνολογία και διαδικασίες

11. Χρησιμοποιείτε τεχνολογικά εργαλεία για την πρόληψη ή ανίχνευση απάτης (π.χ. audit trails, KYC software, CRM monitoring);
- Ναι
 - Όχι
 - Δεν γνωρίζω

13. Σε περίπτωση απάτης, πώς ακολουθείτε τη διαδικασία εσωτερικού ελέγχου;

- Υπάρχει συγκεκριμένο πρωτόκολλο
- Αντιμετωπίζεται κατά περίπτωση
- Δεν υπάρχει σαφής διαδικασία

ΕΝΟΤΗΤΑ Ε: Θεσμικό πλαίσιο

14. Έχει επιβληθεί ποτέ πρόστιμο ή παρατήρηση από δημόσια αρχή σε σχέση με την ταυτοποίηση πελατών;

- Ναι
- Όχι
- Δεν γνωρίζω / Δεν απαντώ

15. Θεωρείτε πως χρειάζονται περισσότερες κατευθυντήριες οδηγίες από την Πολιτεία ή τις Αρχές για την επαλήθευση στοιχείων;

- Ναι
- Ίσως / Δεν γνωρίζω
- Όχι

5.