ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΒΙΟΜΕΤΡΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΠΡΟΣΤΑΣΙΑ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ: Η ΠΕΡΙΠΤΩΣΗ ΤΗΣ ΑΝΑΓΝΩΡΙΣΗΣ ΠΡΟΣΩΠΟΥ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

ΝΑΛΜΠΑΝΤΗ ΙΩΑΝΝΗ

16/2/2024

Επιβλέπουσα: ΔΙΑΜΑΝΤΟΠΟΥΛΟΥ ΒΑΣΙΛΙΚΗ

Μέλη εξεταστικής επιτροπής: ΚΑΡΥΔΑ ΜΑΡΙΑ, ΜΗΤΡΟΥ ΕΥΑΓΓΕΛΙΑ

Πρόλογος και ευχαριστίες

Η παρούσα Διπλωματική Εργασία εκπονήθηκε κατά την εαρινή περίοδο του Ακαδημαϊκού Έτους 2021-2022, στα πλαίσια του Προπτυχιακού Προγράμματος Σπουδών του Πανεπιστήμιου Αιγαίου του τμήματος Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων.

Η εργασία πραγματοποιήθηκε υπό την επίβλεψη της κα. Διαμαντοπούλου Βασιλικής, Καθηγήτρια του Τμήματος.

Αντικείμενο της εργασίας αποτελεί η προστασία της ιδιωτικότητας πάνω στα βιομετρικά συστήματα που χρησιμοποιούνται τα τελευταία χρόνια κατά κόρον.

Στο σημείο αυτό, οφείλω να εκφράσω τις θερμές μου ευχαριστίες, προς την επιβλέπουσα της εργασίας, Καθηγήτρια κα. Διαμαντοπούλου Βασιλικής, για την καθοδήγησή της, και την πολύτιμη βοήθεια που προσέφερε σε κάθε στάδιο εκπόνησης της διπλωματικής εργασίας μου.

Τέλος, ευχαριστώ θερμά την οικογένεια και τους φίλους μου, για την κατανόηση και συμπαράσταση που έδειξαν ολόκληρη την περίοδο εκπόνησης της εργασίας αυτής.

Πίνακας περιεχομένων

Λίστα Εικόνων

Λίστα Πινάκων

Ακρωνύμια

AI	Artificial Intelligence (Τεχνητή Νοημοσύνη)
SAS	Statistical Analysis System (Σύστημα Στατιστικής Ανάλυσης)
PII	Personally identifiable information (Προσωπικά αναγνωρίσιμα στοιχεία)
FPS	Frame per Second (Καρέ ανά δευτερόλεπτο)

Περίληψη

Στη παρούσα διπλωματική εργασία επικεντρωνόμαστε στα βιομετρικά συστήματα και στις απειλές τους. Επίσης παρουσιάζουμε τον βαθμό προστασίας των προσωπικών δεδομένων και της ανωνυμίας των ατόμων που αναγνωρίζονται από τα σύστημα αυτά και δίνουμε μια αναλυτικότερη παρουσία στο σύστημα της αναγνώρισης προσώπου. Η εργασία παρουσιάζει τα τρωτά σημεία των βιομετρικών συστημάτων από συγκεκριμένες ενέργειες και επιπτώσεις, δηλαδή τα σημεία στα οποία παραβιάζεται η ιδιωτικότητα των ανθρώπων.

Συγκεκριμένα, για τη προστασία της ιδιωτικότητας δίνονται, έπειτα από βιβλιογραφική έρευνα, οι αιτίες και οι αστοχίες των βιομετρικών συστημάτων ως προς την συλλογή ,την αποθήκευση και τη διατήρηση των δεδομένων . Οι αστοχίες οφείλονται είτε στον ανθρώπινο παράγοντα είτε στον τεχνολογικό παράγοντα. Επίσης, παρουσιάζονται και μέτρα για την ασφάλεια και την πρόληψη της διαρροής των προσωπικών δεδομενων και τη θωράκιση των συστημάτων ή βάσεων δεδομένων που διαχειρίζονται τα βιομετρικά δεδομένα. Συμπληρωματικά εισάγουμε τη πλευρά των κυβερνήσεων και των βιομηχανιών, στο πως αντιμετωπίζουν την τεχνολογική αυτή πρόοδο , αλλά και τον τρόπο με τον οποίο προσεγγίζουν το θέμα των βιομετρικών συστημάτων και δεδομενων διάφορες χώρες σε Ευρώπη, Αμερική και Ασία.

Επιπρόσθετα, ένα μεγάλο κομμάτι της παρούσας διπλωματικής εργασίας έχει αφιερωθεί στο βιομετρικό σύστημα της αναγνώρισης προσώπου. Είναι ίσως το πιο διαδεδομένο βιομετρικό σύστημα ως προς τον απλό πολίτη και το οποίο κρύβει αρκετές απειλές. Εν συνεχεία ενσωματώνουμε στην τεχνολογία της αναγνώρισης προσώπου ,την τεχνολογία της τεχνητής νοημοσύνης για να αναδείξουμε τα αποτελέσματα τα οποία προκύπτουν από έναν τέτοιο συνδυασμό. Έναν συνδυασμό ο οποίος αποτελείται από δυο ταχείας αναπτυξιακά τεχνολογικές προόδους που απασχολούν μέρα με τη μέρα όλο και περισσότερο το κόσμο.

Τελικώς υπάρχει προστασία της ιδιωτικότητας στα βιομετρικά συστήματα που διαχειρίζονται τα προσωπικά δεδομένα μας; Ποια είναι η στάση των ανθρώπων σε αυτή τη νέα τεχνολογία; Τι σχέση έχει η τεχνητή νοημοσύνη με την αναγνώριση προσώπου; Θετικός ή αρνητικός ο συνδυασμός της τεχνητής νοημοσύνης με την αναγνώριση προσώπου; Αυτές οι ερωτήσεις θα απαντηθούν στην παρούσα εργασία.

Abstract

In this thesis focuses on biometric systems and their threats. We also present the degree of privacy and anonymity protection of the individuals identified by these system in and give a more detailed presentation of the facial recognition system. The paper presents the vulnerabilities of biometric systems from specific actions and effects, such as the points where people's privacy is violated.

Specifically, for privacy protection, the causes and failures of biometric systems in terms of data collection ,storage and retention are given, following a literature survey. The failures are due either to the human factor or to the technological factor. Measures to secure and prevent the leakage of personal data and to shield the systems or databases managing the biometric data are also presented. In addition, we introduce the governments and industries' perspective on how they deal with this technological advancement , and how different countries in Europe, America and Asia approach the issue of biometric systems and data.

In addition, a large part of this thesis has been devoted to the biometric system of facial recognition. It is probably the most widespread biometric system as far as the ordinary citizen is concerned and which hides several threats. Subsequently, we integrate the technology of facial recognition ,the technology of artificial intelligence to highlight the results which result from such a combination. A combination which consists of two rapidly developing technological advances that are increasingly engaging the world day by day.

Finally, is there privacy protection in the biometric systems that manage our personal data? What is the attitude of people to this new technology? What does artificial intelligence have to do with facial recognition? Is the combination of artificial intelligence and facial recognition positive or negative? These questions will be answered in this paper.

1 Εισαγωγή

1.1 Περιγραφή της έρευνας

Τα τελευταία χρόνια, τα συστήματα ταυτοποίησης και ελέγχου ταυτότητας που βασίζονται σε βιομετρικά στοιχεία έχουν γίνει πιο διαδεδομένα και έχουν εξεταστεί για εφαρμογή σε πολλούς τομείς εφαρμογών.

Η βιομετρία είναι η επιστήμη της αναγνώρισης ατόμων με βάση τη συμπεριφορά και τα βιολογικά τους χαρακτηριστικά όπως το πρόσωπο, τα δακτυλικά αποτυπώματα, την ίριδα, τη φωνή, το βάδισμα, και την υπογραφή. Ένα τυπικό βιομετρικό σύστημα μπορεί να θεωρηθεί ως σύστημα ταξινόμησης προτύπων που χρησιμοποιεί προηγμένα σχήματα επεξεργασίας σημάτων για σύγκριση, στα οποία αντιστοιχούν τα βιομετρικά δεδομένα.

Η ετυμολογία της λέξης βιομετρία προέρχεται από τις ελληνικές λέξεις: βίος (ζωή) και μετρικός (μέτρο). Οι βιομετρικές τεχνολογίες βασίζονται στο ποιος είσαι (physiological) ή στο τι κάνεις (behavioural), σε αντίθεση με τις συμβατικές μεθόδους, οι οποίες βασίζονται σε αυτό που ΄΄γνωρίζετε΄΄ (γνώση κωδικών πρόσβασης ή μοτίβα, όπως κρυπτογραφικά κλειδιά) ή/και σε αυτά που ΄΄κατέχετε΄΄(π.χ. ως σύμβολο ή ταυτότητα).

Την τελευταία δεκαετία υπήρξαμε μάρτυρες μιας ταχείας αύξησης της βιομετρικής έρευνας τόσο σε μη στρατιωτικές εφαρμογές όσο και σε εφαρμογές επιβολής του νόμου. Παραδείγματα εφαρμογών που ενσωματώνουν βιομετρική αναγνώριση περιλαμβάνουν:

- συστήματα λογικής και φυσικής πρόσβασης
- επιχειρήσεις επιτήρησης για την καταπολέμηση της απάτης και του οργανωμένου εγκλήματος
- συστήματα ελέγχου της μετανάστευσης και ασφάλειας των συνόρων
- εθνικά προγράμματα ταυτότητας
- συστήματα διαχείρισης ταυτότητας
- τον προσδιορισμό ΄΄φίλου΄΄ ή εχθρού στις στρατιωτικές εγκαταστάσεις.

Η ταχεία πρόοδος των βιομετρικών τεχνολογιών και η διευρυμένη χρήση τους στις αρχές τις άνθισης τους έφερναν συγκεκριμένες ανησυχίες από νομικής άποψης, ιδίως η νομοθεσία που αφορά την προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων. Λαμβάνοντας υπόψη ότι όλα τα βιομετρικά συστήματα λειτουργούν με προσωπικά δεδομένα, αυτό σημαίνει ότι η επεξεργασία δεδομένων πληροφοριών που αφορούν

συγκεκριμένα άτομα, ή πληροφορίες που μπορούν να οδηγήσουν στην ταυτοποίηση ατόμων, θα πρέπει να είναι σύμφωνη με τις νομικές απαιτήσεις που ισχύουν. Αυτού του είδους τα προσωπικά δεδομένα είναι ειδικής φύσης, καθώς σχετίζονται με τα συμπεριφορικά και φυσιολογικά χαρακτηριστικά ενός ατόμου και μπορεί να επιτρέπουν τη μοναδική ταυτοποίησή του.

Σε πολλές χώρες θεσπίστηκαν νόμοι για την προστασία της ιδιωτικής ζωής για την αποτροπή παραβιάσεων του απορρήτου σε όλα τα στάδια της επεξεργασίας δεδομένων, όπως η παράνομη αποθήκευση ή αποθήκευση ανακριβών προσωπικών δεδομένων ή η κατάχρηση ή η μη εξουσιοδοτημένη αποκάλυψη προσωπικών δεδομένων. Όταν αναφερόμαστε στους διαφορετικούς κανονισμούς μεταξύ των διαφόρων νομικών συστημάτων σχετικά με την προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων, ιδίως μεταξύ της ΕΕ και άλλων χωρών (εκτός ΕΕ), μπορεί να διαπιστωθεί ένα κοινό πλαίσιο αρχών. Δηλαδή μεταξύ των χωρών της ΕΕ, οι νομικές διατάξεις, το πλαίσιο λειτουργίας αλλά και τρόπος καταγραφής, επεξεργασίας και αποθήκευσης που αφορούν τα βιομετρικά συστήματα τους έχουν μια κοινή μορφή(μοιάζουν ή είναι ίδιες).

Επίσης, τα βιομετρικά συστήματα έχουν μπει για τα καλά στη καθημερινότητα μας (π.χ. κινητά τηλέφωνα, κλείδωμα-ξεκλείδωμα πορτών κατοικιών, κάμερες παρακολούθησης κ.α.). Σε κάποιες περιπτώσεις με τη συγκατάθεση μας, όπως είναι στα κινητά τηλέφωνα στα οποία επιλέγουμε αν θέλουμε να εισάγουμε τα βιομετρικά χαρακτηριστικά μας στη συσκευή, και σε κάποιες όχι, όπως οι δημόσιες κάμερες παρακολούθησης. Σε κάποιες περιπτώσεις το θεωρούμε σημαντικό και χρήσιμο και σε κάποιες όχι. Γενικά υπάρχει μια αναταραχή γύρω από αυτό το ζήτημα. Πόσο ασφαλή είναι τα βιομετρικά συστήματα; Υπάρχουν νόμοι και διατάξεις για την προστασία της ιδιωτικότητας μας; Χρειάζεται να γνωρίζουμε ότι κάποιος μας παρακολουθεί και μας καταγράφει; Ποιος μπορεί να διαχειρίζεται τέτοια συστήματα και κατά πόσο είμαστε σίγουροι ότι η συμβολή του θα είναι ακέραιη και ασφαλής; Υπάρχουν άλλα συστήματα τα οποία μπορούν να βοηθήσουν στη διασφάλιση της ιδιωτικότητας από τα βιομετρικά συστήματα; Αυτά και άλλα ερωτήματα που θα μας δημιουργηθούν στη συνέχεια καλούμαστε να απαντήσουμε στη παρούσα έρευνα

1.2 Στόχος της ερευνάς

Η παρούσα εργασία στοχεύει:

- Να αναλύσει και να αξιολογήσει τη συμμόρφωση των βιομετρικών συστημάτων με την ισχύουσα νομοθεσία σε Ευρωπαϊκό επίπεδο και μη.
- Να εντοπίσει πιθανά τρωτά σημεία τα οποία έρχονται σε αντίθεση με τις αρχές που πρέπει να ακολουθούν τα βιομετρικά συστήματα, οι οποίες επιβάλλονται από την αντίστοιχη νομοθεσία των χωρών που θα ασχοληθούμε.

Επίσης, σκοπεύουμε να αναλύσουμε πιο ειδικά το βιομετρικό σύστημα αναγνώρισης προσώπου καθώς αποτελεί ένα από τα πιο διαδεδομένα βιομετρικά συστήματα αναγνώρισης και ένα από τα πιο οικεία στον άνθρωπο. Επίσης, και

- την ένταξη του στα συστήματα της τεχνητής νοημοσύνης και
- τις ανησυχίες ή μη που αυτό εγείρει γύρω από την εκτεταμένη χρήση του.

1.3 Οργάνωση της έρευνας

Σε αυτήν την υποενότητα παρουσιάζονται συνολικά τα περιεχόμενα της παρούσας εργασίας, ξεκινώντας από βασικές γνώσεις για την κατανόηση των όσων αναφέρονται, ειδικές αναφορές πάνω σε νομοθετικά ζητήματα και τέλος μια εκτεταμένη αναφορά σε ένα βιομετρικό σύστημα.

Η παρούσα διπλωματική περιέχει 7 κεφάλαια. Για τη διεξαγωγή της έρευνας ακολουθήθηκε συνδυασμός ποιοτικών και ποσοτικών μεθόδων ώστε να εξεταστεί το θέμα με τρόπο πολύπλευρο. Μελετήθηκαν άρθρα, αναφορές και έρευνες μέχρι και προ 10ετιας για να μπορέσουμε να καταλάβουμε τη διαδρομή και την ανάπτυξη του ερευνητικού θέματος μας. Λόγω της ραγδαίας τεχνολογικής προόδου οι αλλαγές που συναντήσαμε ανά τακτά χρονικά διαστήματα είναι πολλές, κυρίως από νομοθετικά θέματα, διότι μαζί με τη τεχνολογία αυξάνονται και οι ανάγκες των ανθρώπων για καλύτερη, πιο ποιοτική και ασφαλέστερη ζωή. Λόγω του γενικού θέματος που μας απασχολεί στην παρούσα έρευνα (η προστασία της ιδιωτικότητας κατά τη χρήση βιομετρικών συστημάτων), μελετήθηκαν οι

αρχές του GDPR (General Data Protection Regulation), άρθρα και έρευνες από τη βάση δεδομένων του Google Scholar αλλά και αναρτήσεις και άρθρα σε ιστοσελίδες επιστημονικού ενδιαφέροντος.

Αναλυτικά, το περιεχόμενου κάθε κεφαλαίου παρουσιάζεται παρακάτω.

Η επόμενη ενότητα είναι αφιερωμένη σε μια σύντομη ανασκόπηση των βιομετρικών μεθόδων και τεχνικών. Αρχικά, ξεκινάμε με μια ιστορική αναδρομή και έπειτα αναλύουμε τον κλάδο της βιομετρίας καθώς, επίσης, τεχνικές και απειλές της.

Στην 3η ενότητα θα γίνει αναφορά στη σχέση μεταξύ των βιομετρικών συστημάτων και της προστασίας της ιδιωτικότητας. Γίνεται μελέτη για το πώς και εάν υπάρχει προστασία της ιδιωτικότητας, και παρουσιάζονται παραδείγματα χωρών με διαφορετικά επίπεδα ελευθερίας στη χρήση των βιομετρικών συστημάτων.

Στην 4η ενότητα ασχολούμαστε και περιγράφουμε ειδικότερα το βιομετρικό σύστημα της αναγνώρισης προσώπου, ξεκινώντας με το τι είναι, σε ποιες χώρες χρησιμοποιείται και ποιος είναι ο τρόπος λειτουργίας του.

Στην 5η ενότητα παρουσιάζουμε του κινδύνους που εγκυμονεί η γενικευμένη βιντεοεπιτήρηση με την τεχνολογία της αναγνώρισης προσώπου αλλά και πώς αυτή σχετίζεται με τις βιομηχανίες και τις κυβερνήσεις.

Τέλος, στην 6η ενότητα μελετούμε συνδυαστικά την τεχνητή νοημοσύνη και την αναγνώριση προσώπου. Αναλύουμε τον τρόπο και τον σκοπό λειτουργίας των δύο αυτών περιοχών άλλα και τα προβλήματα που εγείρονται.

2 Ανάλυση των βιομετρικών συστημάτων

2.1 Ιστορική αναδρομή

Οι αρχικές περιπτώσεις βιομετρικών στοιχείων χρονολογούνται από τη Βαβυλωνιακή αυτοκρατορία, το πρώτο σύστημα βιομετρικής αναγνώρισης αναπτύχθηκε μέχρι το 1800. Ένας Παριζιάνος, ο Alphonse Bertillon, δημιούργησε μια μέθοδο ταξινόμησης και σύγκρισης εγκληματιών με βάση τις μετρήσεις του σώματός τους. Αν και ατελές, το σύστημα του Bertillon ήταν ο καταλύτης για τη χρήση φυσικών χαρακτηριστικών ως μέσο εξακρίβωσης της ταυτότητας.

Πρωτοπόρος στη χρήση βιομετρικών χαρακτηριστικών ήταν ο Bertillon ο οποίος ήταν επικεφαλής του τμήματος της εγκληματολογίας (στην αστυνομία του Παρισιού) στο τομέα της αναγνώρισης-ταυτοποίησης . Ο Bertillon χρησιμοποίησε την ανθρωπομετρία, δηλαδη τη χρήση των διαφορετικών μεγεθών του σώματος και των αναλογιών) για τον εντοπισμό των εγκληματιών. Η μέθοδος αυτή , η λεγόμενη μέθοδος του Bertillon, έδωσε τη θέση της το 1900 περίπου, στη μέθοδο την αναγνώρισης μέσω των δακτυλικών αποτυπωμάτων, τα οποία απετέλεσαν ένα ανεκτίμητο εργαλείο στο πλαίσιο ποινικών ερευνών.

Στη δεκαετία του 1880 τα δακτυλικά αποτυπώματα άρχισαν να χρησιμοποιούνται τακτικά ως τρόπος εντοπισμού εγκληματιών και υπογραφής συμβολαίων. Έγινε κοινή γνώση ότι οι άνθρωποι είχαν μοναδικά δακτυλικά αποτυπώματα, τα οποία συμβολίζουν την ταυτότητα κάποιου. Αν και δεν είναι 100% βέβαιο ποιος άρχισε να χρησιμοποιεί δακτυλικά αποτυπώματα για αναγνώριση, γνωρίζουμε ότι ο Edward Henry ανέπτυξε το πρότυπο δακτυλικών αποτυπωμάτων του συστήματος ταξινόμησης Henry. Αυτό το σύστημα ήταν το πρώτο που χρησιμοποιήθηκε για αναγνώριση και εξαρτιόταν από τις μοναδικές λεπτομέρειες των δακτυλικών αποτυπωμάτων. Οι αρχές επιβολής του νόμου κατάργησαν γρήγορα τις μεθόδους του Bertillon και άρχισαν να χρησιμοποιούν το σύστημα ταξινόμησης Henry ως το πρότυπο για τον ελέγχου εγκληματικής ταυτότητας [1].

2.1.1 Σημαντικοί περίοδοι για την πρόοδο της βιομετρίας

Δεκαετία 1800:

- **1858**: Ο Sir William Herschel πιστώνεται για την πρώτη συστηματική λήψη εικόνων με δάχτυλα και χέρια που ελήφθησαν για σκοπούς επαλήθευσης ταυτότητας. Ο Χέρσελ εργαζόταν στη Δημόσια Υπηρεσία της Ινδίας και κατέγραψε τα αποτυπώματα των χεριών των εργαζομένων στο πίσω μέρος των συμβάσεων των εργαζομένων τους, έτσι μπορούσε να καταλάβει ποιοι ήταν οι πραγματικοί υπάλληλοι την ημέρα πληρωμής.
- **1870**: Ο Bertillon ανέπτυξε ανθρωπομετρίες (ή Bertillonage), η οποία είναι μια μέθοδος που χρησιμοποιείται για την αναγνώριση ατόμων με βάση συγκεκριμένα αρχεία των μετρήσεων του σώματός τους, τις φωτογραφίες τους και τις φυσικές τους περιγραφές.
- **1892**: Ο Sir Francis Galton συνέταξε μια εις βάθος μελέτη των δακτυλικών αποτυπωμάτων, σε αυτήν τη μελέτη, πρότεινε ένα σύστημα ταξινόμησης που χρησιμοποιούσε αποτυπώματα και από τα 10 δάχτυλα.
- **1896**: Ο Sir Edward Henry, ο οποίος ήταν ο Γενικός Επιθεωρητής της Αστυνομίας της Βεγγάλης, συνεργάστηκε με τον Sir Francis Galton για να επινοήσει μια μέθοδο ταξινόμησης και αποθήκευσης πληροφοριών δακτυλικών αποτυπωμάτων, ώστε να μπορούν να χρησιμοποιηθούν εύκολα και αποτελεσματικά.
- **Δεκαετία του 1900**: Σημαντικές ανακαλύψεις στη βιομετρία σημειώθηκαν τη δεκαετία του 1900, συμπεριλαμβανομένης της χρήσης μοτίβων ίριδας και γεωμετρίας χεριών για προσωπική αναγνώριση. Από τα μέσα έως τα τέλη του 1900 ξεκίνησε η μελέτη και η εισαγωγή της τεχνολογίας για την αναγνώριση προσώπου ,για προσωπική αναγνώριση.
- **Δεκαετία 2000**: Ο 21ος αιώνας έχει δει τα βιομετρικά στοιχεία να αυξάνονται αλματωδώς. Τα συστήματα λειτουργούν πιο γρήγορα και πιο αποτελεσματικά, η κοινωνική αποδοχή της αναγνώρισης προσώπου αυξάνεται και οι φορητές βιομετρικές λύσεις έχουν γίνει κοινές.
- **Δεκαετία 2020**: Οι ειδικοί στη βιομετρία προβλέπουν ότι θα παρουσιαστούν περισσότερες επιλογές τα επόμενα χρόνια – για παράδειγμα, η ανίχνευση καρδιακών παλμών και βάδισης μπορεί να γίνει πιο συνηθισμένη. Μέχρι το 2030 μπορεί να είμαστε μια κοινωνία χωρίς κωδικό πρόσβασης.

2.2 Συστήματα ελέγχου ταυτότητας και ταυτοποίησης που βασίζονται σε βιομετρικά στοιχεία.

Τα συστήματα που βασίζονται σε βιομετρικά στοιχεία επιτρέπουν την αυτόματη αναγνώριση ή/και τον έλεγχο ταυτότητας ατόμων. Ο έλεγχος ταυτότητας απαντά στην ερώτηση: «Είμαι αυτός που ισχυρίζομαι ότι είμαι;». Το σύστημα επαληθεύει την ταυτότητα του ατόμου επεξεργάζοντας βιομετρικά δεδομένα, τα οποία αναφέρονται στο άτομο που ρωτά και παίρνει μια απόφαση ναι/όχι (σύγκριση 1:1). Από την άλλη πλευρά, η αναγνώριση απαντά στην ερώτηση: «Ποιος είμαι;». Το σύστημα αναγνωρίζει το άτομο που ρωτά, διαφοροποιώντας το από άλλα άτομα των οποίων τα βιομετρικά δεδομένα αποθηκεύονται επίσης στη βάση δεδομένων. Σε αυτή την περίπτωση το σύστημα παίρνει 1-από- n απόφαση, και απαντά ότι το άτομο που ρωτά είναι το X, εάν τα βιομετρικά του δεδομένα είναι αποθηκευμένα στη βάση δεδομένων ή ότι δεν υπάρχει καθόλου αντιστοίχιση. Αν και η συνάρτηση αναγνώρισης θα πρέπει να θεωρείται διαφορετική από τον έλεγχο ταυτότητας από την οπτική γωνία της εφαρμογής, συχνά τα συστήματα που χρησιμοποιούν βιομετρικά στοιχεία ενσωματώνουν λειτουργίες ταυτοποίησης και ελέγχου ταυτότητας, καθώς η πρώτη είναι μια επαναλαμβανόμενη εκτέλεση της δεύτερης. [29]

Οποιαδήποτε ανθρώπινα φυσιολογικά ή συμπεριφορικά χαρακτηριστικά μπορούν να χρησιμεύσουν ως βιομετρικά στοιχεία είτε για έλεγχο ταυτότητας είτε για ταυτοποίηση, εάν πληρούν τις ακόλουθες ιδιότητες:

• Universality (Καθολικότητα): το βιομετρικό στοιχείο υπάρχει σε όλους τους ανθρώπους. Από αυτή την άποψη, δεν είναι όλα τα βιομετρικά στοιχεία ισοδύναμα και ο ρυθμός διάκρισης ενός ατόμου από τον άλλο είναι πολύ διαφορετικός, ανάλογα με τον τύπο των βιομετρικών στοιχείων που χρησιμοποιούνται.

• Distinctiveness (Διακριτότητα): το βιομετρικό στοιχείο πρέπει να είναι διακριτικό για κάθε άτομο, δηλαδή κανένα άτομο δεν πρέπει να είναι το ίδιο όσον αφορά τα βιομετρικά στοιχεία. Τα δακτυλικά αποτυπώματα έχουν μεγάλη διαφοροποίηση και η πιθανότητα δύο ατόμων να έχουν την ίδια ίριδα εκτιμάται ως αμελητέα. Τα πιο χαρακτηριστικά στοιχεία φαίνεται να είναι το DNA, η ίριδα, ο αμφιβληστροειδής και το δακτυλικό αποτύπωμα.

• Permanence (Μονιμότητα): η ιδιότητα του βιομετρικού στοιχείου παραμένει αμετάβλητη με την πάροδο του χρόνου για κάθε άτομο. Ενώ ορισμένα βιομετρικά στοιχεία, όπως η ίριδα, παραμένουν σταθερά για δεκαετίες, άλλα βιομετρικά στοιχεία όπως το

πρόσωπο ενός ατόμου ή η δυναμική της υπογραφής του αλλάζουν με την πάροδο του χρόνου. Επίσης, τα δάχτυλα τραυματίζονται συχνά.

• Collectibility (Συλλεκτικότητα): τα βιομετρικά χαρακτηριστικά πρέπει να είναι ποσοτικά μετρήσιμα και να συλλέγονται εύκολα. Η σάρωση αμφιβληστροειδούς και η ανάλυση DNA είναι αρκετά παρεμβατικές, σε αντίθεση με τα χαρακτηριστικά που σχετίζονται με το πρόσωπο, τα οποία είναι εύκολο να αποκτηθούν.

• Performance (Αποδοτικότητα): θα πρέπει να ικανοποιούνται οι απαιτήσεις ακρίβειας, ταχύτητας και πόρων, προκειμένου ένα σύστημα που βασίζεται σε βιομετρικά στοιχεία να είναι πρακτικό.

• Acceptability (Αποδεκτότητα): υποδηλώνει τον βαθμό στον οποίο ένα σύστημα είναι αβλαβές και αποδεκτό από τους προβλεπόμενους χρήστες, προκειμένου να έχει πρακτική αξία.

• Circumvention (Καταστρατήγηση): αναφέρεται στην ευρωστία ενός συστήματος έναντι διαφόρων δόλιων μεθόδων και επιθέσεων, για παράδειγμα έναντι πλαστών δακτυλικών αποτυπωμάτων.

Σύμφωνα με την κατηγορία των χαρακτηριστικών που χρησιμοποιούνται, μπορούμε να ταξινομήσουμε τα βιομετρικά συστήματα ως βασισμένα στα φυσιολογικά χαρακτηριστικά του ανθρώπινου σώματος και στα συμπεριφοριστικά χαρακτηριστικά. Ωστόσο, υπάρχουν και τεχνικές που βασίζονται τόσο σε φυσιολογικά χαρακτηριστικά όσο και σε χαρακτηριστικά της συμπεριφοράς. Οι τεχνικές που βασίζονται σε φυσιολογική βάση, οι οποίες μετρούν τα βιολογικά χαρακτηριστικά ενός ατόμου, περιλαμβάνουν, μεταξύ άλλων, επαλήθευση δακτυλικών αποτυπωμάτων, αναγνώριση ίριδας, ανάλυση αμφιβληστροειδούς, αναγνώριση προσώπου, περίγραμμα σχεδίων χεριών, αναγνώριση σχήματος αυτιού, ανίχνευση οσμών σώματος, επαλήθευση ηχείου, την ανάλυση του μοτίβου του DNA και ανάλυση πόρων ιδρώτα. Οι τεχνικές που βασίζονται στη συμπεριφορά, οι οποίες μετρούν τη συμπεριφορά ενός ατόμου, περιλαμβάνουν χειρόγραφη επαλήθευση υπογραφής, ανάλυση πληκτρολόγησης, αναγνώριση φωνής, ρυθμό πληκτρολόγησης και ανάλυση βάδισης [3].

2.3 Τεχνικές Βιομετρικής

Η παλαιότερη βιομετρική τεχνική είναι η ηλεκτρονική αναγνώριση δακτυλικών αποτυπωμάτων, πάνω στην οποία έχει γίνει εκτεταμένη έρευνα και ανάπτυξη, ειδικά τις τελευταίες τρεις δεκαετίες, κυρίως λόγω της εκμετάλλευσής της από τις αρχές επιβολής του νόμου. Υπάρχουν δύο τεχνικές αντιστοίχισης που σχετίζονται με τα δακτυλικά αποτυπώματα, που βασίζονται σε μικροσκοπικά χαρακτηριστικά και βάσεις συσχέτισης. Τα μικροσκοπικά χαρακτηριστικά είναι μοναδικά χαρακτηριστικά, όπως απολήξεις κορυφογραμμών, διακλαδώσεις και αποκλίσεις. Τα δακτυλικά αποτυπώματα περιέχουν μεγάλο όγκο δεδομένων, τα οποία επιτρέπουν την εξάλειψη των ψευδών ποσοστών αντιστοίχισης σε ένα μικρό ποσοστό των συγκρίσεων που επιχειρήθηκαν.

Η αναγνώριση του αμφιβληστροειδούς βασίζεται στο μοτίβο των αιμοφόρων αγγείων του αμφιβληστροειδούς. Αυτή η τεχνολογία είναι προσωπικά επεμβατική και απαιτεί ειδικευμένους χειριστές. Έχει ως αποτέλεσμα κάποιους ΄΄κωδικούς΄΄ αμφιβληστροειδούς 96 bytes όταν χρησιμοποιούνται για έλεγχο ταυτότητας και σε ορισμένα Kbyte στην περίπτωση αναγνώρισης. Οι τεχνικές αναγνώρισης προσώπου εκμεταλλεύονται χαρακτηριστικά όπως τη σχετική θέση των ματιών, της μύτης και του στόματος και οι αποστάσεις μεταξύ τους.

Οι τεχνικές γεωμετρίας χεριών εκμεταλλεύονται χαρακτηριστικά του σχήματος του χεριού, όπως το μήκος και το πλάτος των δακτύλων. Αυτό οδηγεί σε αρκετά μικρό όγκο δεδομένων (περίπου 9 byte), περιορίζοντας έτσι την εφαρμογή τους μόνο σε απλούς σκοπούς ελέγχου ταυτότητας. Επίσης, η συμπεριφορά τους σε σχέση με την εκπλήρωση των παραπάνω ιδιοτήτων είναι μέτρια.

Η ίριδα, η κυκλική έγχρωμη μεμβράνη που περιβάλλει την κόρη του ματιού, είναι μια μοναδική δομή που αποτελείται από συγκεκριμένα χαρακτηριστικά όπως ραβδώσεις, αυλάκια, δακτυλίους, κρύπτες, νήματα και στέμματα. Τα σχέδια της ίριδας χαρακτηρίζονται από πολύ υψηλή διακριτικότητα, ακόμη και τα δίδυμα έχουν διαφορετικά. Η πιθανότητα δύο άτομα να έχουν το ίδιο σχέδιο ίριδας είναι περίπου 10^{-52}. Η πιθανότητα δύο διαφορετικά σχέδια ίριδας να καταλήγουν στον ίδιο κωδικό ίριδας που χρησιμοποιείται (περίπου 256 bytes) από ένα βιομετρικό σύστημα είναι αμελητέα (περίπου 10^{-78}), επιτρέποντας έτσι σχεδόν την τέλεια αντιστοίχιση-ακρίβεια.

Οι τεχνικές αναγνώρισης φωνής βασίζονται σε φωνητικά χαρακτηριστικά που εξαρτώνται από το μέγεθος ή τις διαστάσεις των φωνητικών χορδών, του στόματος, των ρινικών κοιλοτήτων κ.λπ. Η αναγνώριση φωνής δεν είναι παρεμβατική, αλλά ευαίσθητη

στον θόρυβο του περιβάλλοντος και είναι ευάλωτη σε επιθέσεις επανάληψης, εκτός εάν συνδυάζεται με πρόκληση/απόκριση μηχανισμών. Όπως και στην περίπτωση των τεχνικών γεωμετρίας προσώπου και χεριών, η αναγνώριση φωνής χαρακτηρίζεται από μια αρκετά μέτρια εκπλήρωση των παραπάνω ιδιοτήτων. Ο Πίνακας 1 που βασίζεται σε βιομετρικά στοιχεία παρουσιάζει τα αποτελέσματα σύγκρισης των τεχνικών αναγνώρισης δακτυλικών αποτυπωμάτων, αμφιβληστροειδούς, προσώπου, χειρός, ίριδας και αναγνώρισης φωνής σε σχέση με την εκπλήρωση των παραπάνω ιδιοτήτων.

(Biometric) Βιομετρική	(Fingerprint) Δακτυλικό αποτύπωμα	(retina) Αμφιβληστροειδής	(Face) Πρόσωπο	(Hand Geometry) Χέρι	(Iris) Γεωμετρία Ίριδας	(Voice) Φωνή
Εμπόδια για καθολικότητα	Φθαρμένες κορυφογραμμές, απομειώσεις δαχτύλου	Αμφιβληστροειδής χιτώνας	Κανένα	Βλάβη χεριού	Οπτική βλάβη	Φωνητική βλάβη
Διακριτικότητα	Υψηλή	Χαμηλή(ασθενής)	Χαμηλή	Μεσαία	Υψηλή	Χαμηλή
Μονιμότητα	Υψηλός	Υψηλή	Μεσαία	Μεσαία	Υψηλή	Χαμηλή
Συλλεκτικότητα	Μεσαία	Υψηλή	Υψηλή	Υψηλή	Μεσαία	Μεσαία
Εκτέλεση	Υψηλή	Χαμηλή	Χαμηλή	Μεσαία	Υψηλή	Χαμηλή
Αποδοχή	Μεσαία	Υψηλός	Υψηλή	Μεσαία	Μεσαία	Υψηλή
Δυνητικότητα	Χαμηλή	Χαμηλή	Υψηλή	Μεσαία	Μεσαία	Υψηλή

Πίνακας 1 :Σύγκριση βιομετρικών τεχνολογιών

Η συλλογή βιομετρικών δειγμάτων, τα λεγόμενα βιομετρικά δεδομένα (για παράδειγμα το δακτυλικό αποτύπωμα κ.α) πραγματοποιείται κατά τη διαδικασία εγγραφής του βιομετρικού χαρακτηριστικού στη βάση δεδομένων με τη χρήση συσκευής εισαγωγής συγκεκριμένης για κάθε τύπο βιομετρίας. Δεν είναι όλες οι πληροφορίες των βιομετρικών δεδομένων σχετικές με τη διάκριση ατόμων. Το βιομετρικό σύστημα εξάγει από τα βιομετρικά δεδομένα χαρακτηριστικά ειδικά για τον χρήστη για να δημιουργήσει ένα κύριο πρότυπο ή έναν βιομετρικό κώδικα. Έτσι, το πρότυπο είναι μια δομημένη μείωση μιας βιομετρικής εικόνας ή βιομετρικών μετρήσεων.

Μόλις εγγραφούν σε ένα βιομετρικό σύστημα τα άτομα ή οι χρήστες μπορούν να πιστοποιηθούν ή να ταυτοποιηθούν. Η διαδικασία αναγνώρισης αποτελείται από τέσσερα βήματα: απόκτηση, δημιουργία, σύγκριση και απόφαση. Στο βήμα απόκτησης, τα τρέχοντα βιομετρικά δεδομένα συλλέγονται από το άτομο που πρόκειται να πιστοποιηθεί ή να

αναγνωριστεί. Αυτά τα δεδομένα χρησιμοποιούνται για τη δημιουργία χαρακτηριστικών χρήστη, δηλαδή ενός νέου προτύπου χρήστη. Το νέο πρότυπο συγκρίνεται με το κύριο πρότυπο της διεκδικούμενης ταυτότητας σε περίπτωση ελέγχου ταυτότητας ή με όλα τα πρότυπα που δημιουργήθηκαν και αποθηκεύτηκαν στη διαδικασία εγγραφής σε περίπτωση αναγνώρισης. Στο τελευταίο βήμα, το σύστημα αποφασίζει να αποδεχτεί ή να απορρίψει τη διεκδικούμενη ταυτότητα. Στην περίπτωση αναγνώρισης, το σύστημα αναγνωρίζει ή όχι τον χρήστη.

2.3.1 Βιομετρικά συστήματα και σφάλματα

Τα συστήματα ελέγχου ταυτότητας και ταυτοποίησης που βασίζονται σε βιομετρικά στοιχεία μπορούν κάνουν δύο τύπους σφαλμάτων:

(1) όσον αφορά τις βιομετρικές μετρήσεις από δύο διαφορετικά άτομα που προέρχονται από το ίδιο άτομο (ψευδής αντιστοίχιση ή ψευδής αποδοχή) και το αντίστροφο,
(2) όσον αφορά τις βιομετρικές μετρήσεις από το ίδιο άτομο που προέρχονται από δύο διαφορετικά άτομα (ψευδής απόρριψη).

Το ποσοστό ψευδούς αντιστοίχισης (FMR) και το ποσοστό ψευδούς απόρριψης (FRR) είναι αντιστρόφως ανάλογο μεταξύ τους, δηλαδή εάν ο σχεδιαστής ενός συστήματος μειώσει ένα όριο συστήματος για να το κάνει πιο ανεκτικό στις παραλλαγές εισόδου και στον θόρυβο, τότε το FMR αυξάνεται. Εάν το όριο του συστήματος αυξηθεί για να γίνει πιο ασφαλές, τότε το FRR αυξάνεται και το FMR μειώνεται.

Αυτά τα σφάλματα προέρχονται από το γεγονός ότι οι διαφορετικές βιομετρικές μετρήσεις του ίδιου ατόμου δεν είναι ίδιες, οδηγώντας έτσι σε διαφορετικά πρότυπα. Επομένως, ανάλογα με τη μεταβλητότητα αυτών των μετρήσεων, τόσο όσον αφορά τις μετρήσεις του ίδιου ατόμου όσο και τις μετρήσεις διαφορετικών ατόμων, εκφρασμένες σε αντίστοιχες συναρτήσεις κατανομής, οι διάφορες βιομετρικές τεχνικές δείχνουν χαμηλή, μεσαία ή υψηλή απόδοση.

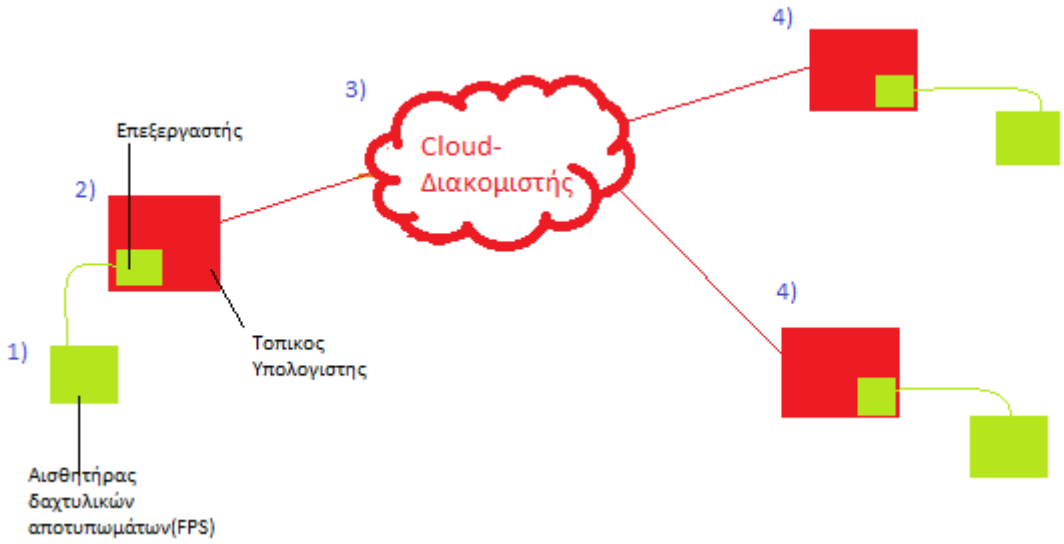
2.3.2 Απειλές για τα βιομετρικά συστήματα

Μπορεί να κατασκευαστούν βιομετρικά δείγματα ή ακόμα και πρότυπα, για παράδειγμα τεχνητά δάχτυλα μπορούν να χρησιμοποιηθούν από επιτιθέμενους. Για να ανταπεξέλθουν

σε αυτές τις απειλές, τα βιομετρικά συστήματα πρέπει να ανιχνεύουν τη ζωτικότητα. Επιπλέον, είναι σημαντικό να θεωρήσουμε ότι τα βιομετρικά χαρακτηριστικά δεν είναι μυστικά, για παράδειγμα εμείς αφήνουμε δαχτυλικά αποτυπώματα παντού ή οι ίριδες των ανθρώπων είναι εμφανείς και υπάρχει περίπτωση μια κάμερα να τις φωτογραφήσει. Συνεπώς, τα βιομετρικά συστήματα είναι ευάλωτα σε επιθέσεις επανάληψης (όπου ο εισβολέας παρακολουθεί το κανάλι επικοινωνίας κατά τη λήψη των βιομετρικών δεδομένων και στη συνέχεια τροποποιεί αυτά τα δεδομένα για πρόσβαση στο σύστημα ως νόμιμος χρήστης), εκτός εάν υπάρχει ειδική προστασία ώστε να λαμβάνονται μέτρα για τη διασφάλιση της ζωτικότητας και του χρόνου του παρεχόμενου στις βιομετρικές μετρήσεις [3].

2.4 Απειλές και τα τρωτά σημεία των βιομετρικών συστημάτων

Στην Εικόνα 1 παρακάτω απεικονίζεται ένα κατανεμημένο μοντέλο συστήματος ελέγχου ταυτότητας με δακτυλικά αποτυπώματα, το οποίο διαθέτει έναν αυθαίρετο αριθμό τοπικών υπολογιστών εξοπλισμένων με αισθητήρες δακτυλικών αποτυπωμάτων (FPS) που είναι συνδεδεμένοι στο διαδίκτυο μέσω απομακρυσμένων διακομιστών στο cloud. Μια εικόνα του δακτυλικού αποτυπώματος λαμβάνεται από ένα τοπικό FPS (1) και υποβάλλεται σε επεξεργασία στον συνδεδεμένο τοπικό υπολογιστή για να καταστεί δυνατή η εξαγωγή χαρακτηριστικών (2). Το πρότυπο που προκύπτει μετατρέπεται σε μια ασφαλή δομή δεδομένων, ένα ΄΄θησαυροφυλάκιο΄΄, που αποθηκεύεται σε μια βάση δεδομένων (3) στο cloud και μπορεί να προσπελαστεί από άλλους τοπικούς υπολογιστές για επαλήθευση κάποιας οντότητας που προσπαθεί να ταυτοποιηθεί (4). Αυτή η λειτουργία μπορεί να εκτελεστεί πολλές φορές και η εγγραφή και η επαλήθευση ενός δακτυλικού αποτυπώματος μπορεί να πραγματοποιηθεί σε οποιονδήποτε τοπικό υπολογιστή.[2]



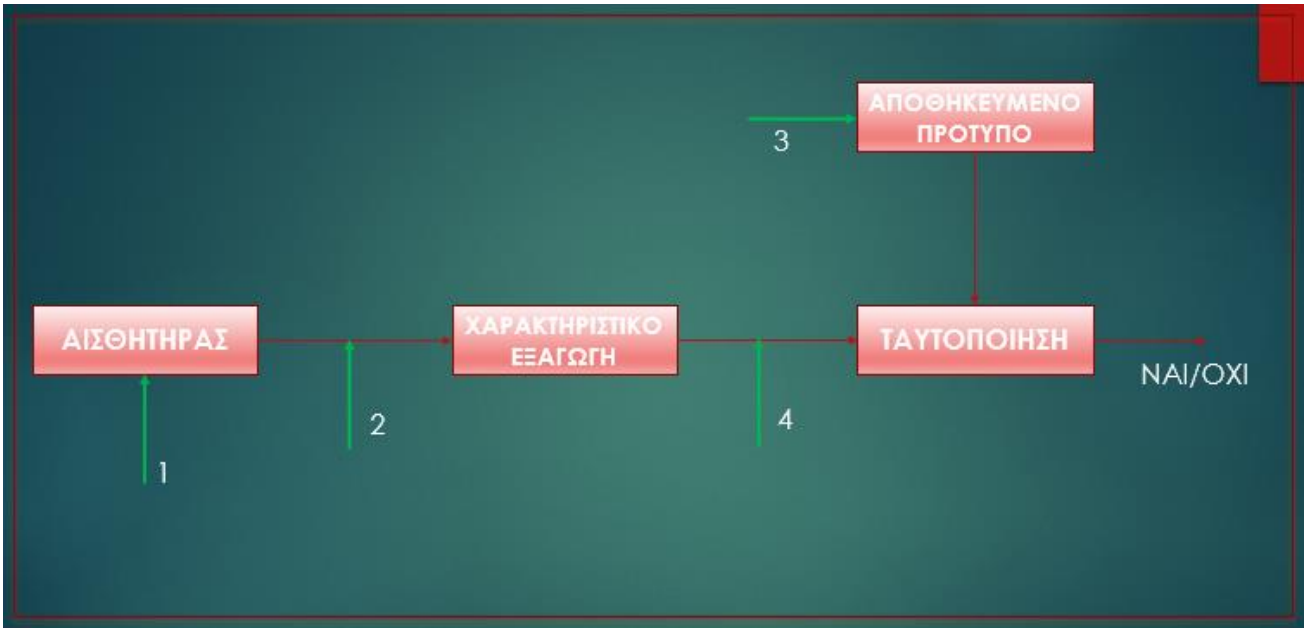
Εικόνα 1:Αρχιτεκτονική ενός συστήματος εξοπλισμένο με αισθητήρες δακτυλικών αποτυπωμάτων

Ο εισβολέας είτε έχει την πρόθεση να αποσπάσει πολύτιμα περιουσιακά στοιχεία είτε θέλει να αποκτήσει μη εξουσιοδοτημένη πρόσβαση εξαπατώντας το βιομετρικό σύστημα. Θεωρούμε ότι ο εισβολέας είναι επιτυχημένος εάν μπορεί να προσδιορίσει τις αυθεντικές λεπτομέρειες σε ένα μη ταξινομημένο ΄θησαυροφυλάκιο΄, το οποίο επιτρέπει την κλοπή ταυτότητας ή εάν μπορεί να πραγματοποιήσει επιτυχή έλεγχο ταυτότητας σε ένα μη ταξινομημένο θησαυροφυλάκιο χωρίς τα κατάλληλα βιομετρικά στοιχεία που του επιτρέπει να αποκτήσει μη εξουσιοδοτημένη πρόσβαση και να πραγματοποιήσει επίσης κλοπή ταυτότητας. Τα αξιόπιστα και τα μη αξιόπιστα μέρη απεικονίζονται στην Εικόνα 1 με πράσινο και κόκκινο χρώμα, αντίστοιχα. Υποθέτουμε ότι το FPS είναι απευθείας συνδεδεμένο με έναν αξιόπιστο επεξεργαστή και η εφαρμογή μας εκτελείται σε ασφαλές περιβάλλον εκτέλεσης. Ούτε τα στοιχεία εκτός του επεξεργαστή στον τοπικό υπολογιστή, ούτε οι συνδέσεις με τον διακομιστή και τον ίδιο τον διακομιστή υποθέτουμε ότι είναι αξιόπιστα. Αυτό σημαίνει ότι δεν μπορούμε να είμαστε βέβαιοι για την ασφάλεια και την αξιοπιστία των δεδομένων που αποθηκεύονται στον υπολογιστή , των συνδέσεων με το διαδίκτυο, και ακόμη και του διακομιστή στον οποίο συνδεόμαστε. Αυτή η πρόταση τονίζει τη σημασία της διατήρησης προσοχής και προστασίας της ιδιωτικότητας μας, καθώς η ασφάλεια στον ψηφιακό κόσμο δεν είναι πάντα εγγυημένη.

Ένα γενικό βιομετρικό σύστημα μπορεί να τοποθετηθεί στο πλαίσιο ενός συστήματος αναγνώρισης προτύπων. Τα στάδια ενός τέτοιου γενικού συστήματος φαίνονται στην Εικόνα 2 Το πρώτο στάδιο περιλαμβάνει τη λήψη βιομετρικού σήματος από τον χρήστη

(π.χ. η σάρωση δακτυλικών αποτυπωμάτων χωρίς μελάνι).Το σήμα που λαμβάνεται διαφέρει σημαντικά από το σήμα που έστειλαν πριν την αποστολή του. Ως εκ τούτου, βασίζονται καθαρά σε pixel οι τεχνικές αντιστοίχισης και δεν λειτουργούν αξιόπιστα. Γι αυτο το λογο ,το δεύτερο στάδιο επεξεργασίας σήματος επιχειρεί να οικοδομήσει μια πιο αμετάβλητη αναπαράσταση αυτού του βασικού σήματος εισόδου.

Προσδιορίσαμε 4 θέσεις στο γενικό βιομετρικό σύστημα της Εικόνας 2 όπου μπορεί να συμβούν επιθέσεις.



Εικόνα 2: Γενικό βιομετρικό σύστημα

2.4.1 Επίθεση με παρουσία

Οι επιθέσεις με παρουσία περιλαμβάνουν έναν κακόβουλο χρήστη που χρησιμοποιεί ένα τεχνούργημα κάποιου είδους για να μιμηθεί ένα άτομο που *έχει* εγγραφεί στο σύστημα. ***Για παράδειγμα:*** Εάν μπορεί να αποτυπωθεί ένα δακτυλικό αποτύπωμα του εγγεγραμμένου ατόμου, αυτό θα μπορούσε να χρησιμοποιηθεί για να δημιουργήσει ένα αντίστοιχο τεχνούργημα. Για την αναγνώριση προσώπου, μια φωτογραφία πορτρέτου του στόχου μπορεί εύκολα να ληφθεί κρυφά και να χρησιμοποιηθεί για τη δημιουργία ενός τεχνουργήματος.

2.4.2 Υποκλοπή στην έξοδο του αισθητήρα

Ένας εισβολέας μπορεί να επιδιώξει να τροποποιήσει ή να υποκλέψει τα δεδομένα που εξάγονται από τον αισθητήρα. Ένα δείγμα που έχει ληφθεί προηγουμένως μπορεί να αναπαραχθεί ξανά ή ένα βιομετρικό δείγμα που έχει ληφθεί θα μπορούσε να αντικατασταθεί με βιομετρικά δεδομένα διαφορετικού ατόμου κατά την εγγραφή.

Τα υποκλαπέντα δεδομένα ενδέχεται να χρησιμοποιηθούν από έναν εισβολέα για να αποκτήσει τα βιομετρικά χαρακτηριστικά ενός εγγεγραμμένου ατόμου για χρήση σε μελλοντικές επιθέσεις. Οι ενσωματωμένες λειτουργίες ασφαλείας που υποστηρίζουν την ασφαλή λήψη και επεξεργασία βιομετρικών δεδομένων σε φορητή συσκευή μπορούν να χρησιμοποιηθούν για τον μετριασμό αλλά και για την εξολοκλήρου προστασία από την υποκλοπή της εξόδου του αισθητήρα.

2.4.3 Αναφορές και τρωτά σημεία που σχετίζονται με τη βάση δεδομένων

Ένας εισβολέας μπορεί να στοχεύσει δεδομένα κατά τη μετάδοση ή την αποθήκευση από το βιομετρικό σύστημα. Για παράδειγμα, μια βιομετρική αναφορά στη βάση δεδομένων εγγραφής θα μπορούσε να τροποποιηθεί ώστε να περιλαμβάνει τα βιομετρικά χαρακτηριστικά ενός κακόβουλου χρήστη.

Σε εφαρμογές όπου τα βιομετρικά δεδομένα αποθηκεύονται σε μια συσκευή που κατέχει το άτομο, όπως κινητό τηλέφωνο, διαβατήριο ή ταυτότητα, ένας εισβολέας που έχει στην κατοχή του τη συσκευή θα έχει απεριόριστη πρόσβαση στα βιομετρικά δεδομένα, εκτός εάν η συσκευή προστατεύεται από ενσωματωμένο χαρακτηριστικό ασφαλείας. Με τον όρο ενσωματωμένο χαρακτηριστικό ασφαλείας εννοούμε ένα βιομετρικό σύστημα, όπως η αναγνώριση δακτυλικού αποτυπώματος, το οποίο θα είναι ενσωματωμένο πάνω στην ΄΄κάρτα΄΄ και για να χρησιμοποιηθεί η κάρτα θα χρειάζεται το δακτυλικό αποτύπωμα του κατόχου της κάρτας. Μια προσέγγιση για την προστασία των βιομετρικών δεδομένων είναι η διατήρηση τους κεντρικά, με ασφαλή μετάδοση και αποθήκευση.

2.4.4 Ακεραιότητα εγγραφής

Υπάρχει πιθανότητα να ανατραπεί η διαδικασία εγγραφής, επιτρέποντας την αποδοχή ακατάλληλων δεδομένων εγγραφής. Για παράδειγμα, εάν ένα τεχνούργημα (δηλαδή κάτι

το οποίο έγινε κρυφά-μυστικά είναι εγγεγραμμένο στο σύστημα, τότε ένας εισβολέας μπορεί αργότερα να μπορέσει να χρησιμοποιήσει το ίδιο τεχνούργημα για να αναγνωριστεί.

Εναλλακτικά, εάν σε μια καταγραφή βιομετρικών χαρακτηριστικών, περιέχονται βιομετρικά δεδομένα δύο ατόμων (για παράδειγμα το δεξί χέρι είναι σωστά εγγεγραμμένο, αλλά το εγγεγραμμένο αριστερό είναι αυτό ενός άλλου ατόμου ή εάν μια εγγραφή προσώπου χρησιμοποιεί μια εικόνα που μεταμορφώνει μαζί φωτογραφίες δύο ατόμων) μπορεί να επιτρέψει σε ένα άτομο να υποδυθεί το άλλο. Ως εκ τούτου, είναι σημαντικό η διαδικασία εγγραφής να έχει σχεδιαστεί για να αντιμετωπίσει την πιθανότητα υπονόμευσης.

2.4.5 Επιθέσεις συστήματος

Οι επιθέσεις κατά του υποκείμενου αυτού στο οποίο λειτουργεί το βιομετρικό σύστημα είναι οπωσδήποτε εφικτές και πρέπει να λαμβάνονται υπόψη σε περιπτώσεις όπου τα περιουσιακά στοιχεία που προστατεύονται είναι σημαντικής αξίας και όπου οι επιτιθέμενοι είναι σχετικά εξελιγμένοι.

Γενικά, ο μετριασμός τέτοιων επιθέσεων βασίζεται σε παραδοσιακές μεθόδους ασφάλειας IT που δεν είναι συγκεκριμένες για βιομετρικά συστήματα. Ωστόσο, η αποθήκευση μιας βάσης δεδομένων βιομετρικών δεδομένων δημιουργεί έναν σημαντικό όγκο PII (personally identifiable information) που πρέπει να προστατεύεται, καθώς αυτές οι πληροφορίες εκτιμώνται ιδιαίτερα από τους εισβολείς.

2.4.6 Εσωτερική απειλή

Όλα τα συστήματα ασφαλείας είναι ευάλωτα σε επίθεση από έναν αξιόπιστο διαχειριστή ή χειριστή συστήματος. Λόγω του επιπέδου πρόσβασης και εμπιστοσύνης που κατέχουν τέτοια άτομα, οι επιθέσεις εμπιστευτικών πληροφοριών σε ένα βιομετρικό σύστημα μπορεί να λάβουν οποιαδήποτε από τις μορφές που περιγράφονται παραπάνω.

2.5 Τεχνικές προστασίας και κρυπτογράφησης

Στην ενότητα αυτή, δίνουμε έμφαση στις μεθόδους προστασίας των βιομετρικών προτύπων που αποτελούν σημαντική ανησυχία, όπως στα διακριτά διακριτικά (μοναδικά και αναγνωρίσιμα ψηφία ή σύμβολα που χρησιμοποιούνται για να προσδιορίσουν έναν

χρήστη) και στους κωδικούς πρόσβασης, έτσι και στα βιομετρικά πρότυπα θα πρέπει να είναι δυνατή η ακύρωση ή η ανανέωσή τους, όταν απαιτείται.

Στις μέρες μας η χρήση κωδικών πρόσβασης είναι πολύ συνήθης και επαναλαμβανόμενο φαινόμενο μέσα στη μέρα μας, από τη χρήση τους σε κινητά τηλέφωνα έως και κάρτες τραπεζών. Όμως, η χρήση των κωδικών πρόσβασης δεν εξυπηρετεί τα συμφέροντα μας για την προστασία των βιομετρικών προτύπων. Αυτό συμβαίνει διότι οι κωδικοί πρόσβασης δεν είναι τόσο ισχυροί και δεν παρέχουν την ασφάλεια που απαιτείται. Η τεχνική προστασίας του βιομετρικού προτύπου θα πρέπει να ικανοποιεί τις ιδιότητες της διαφορετικότητας, της δυνατότητας ανάκλησης, της ασφάλειας και της απόδοσης. Οι βιομετρικές πληροφορίες αποτελούν ένα εξωτερικό κλειδί, το οποίο είναι κρυπτογραφημένο σε μορφή αριθμών – συμβόλων. Αυτό γίνεται ώστε να μην υπάρχουν στη βάση δεδομένων οι πρωτότυπες μορφές των βιομετρικών χαρακτηριστικών. Για παράδειγμα, αντί να υπάρχει το δαχτυλικό αποτύπωμα σε μορφή φωτογραφίας στη βάση δεδομένων, υπάρχει ένας μυστικός κωδικός (αποτελούμενος από νούμερα – σύμβολα) ο οποίος καλείται να κάνει την επαλήθευση της ταυτότητας του ατόμου όταν χρειαστεί. Γι' αυτόν τον λόγο είναι απαραίτητο να πληρούνται οι παρακάτω ιδιότητες που αναφέραμε.

- Ποικιλομορφία: Αυτή η ιδιότητα αναφέρεται στην ΄΄ειδική προϋπόθεση΄΄ στην οποία δεν επιτρέπεται στο προστατευμένο πρότυπο να συγκριθεί με άλλα πρότυπα στη βάση δεδομένων. Αυτή η ιδιότητα επιβεβαιώνει την ιδιότητα της μυστικότητας του χρήστη (της οντότητας που προσπαθεί να ταυτοποιηθεί).
- Ανάκληση: Αυτή η ιδιότητα διασφαλίζει ότι οι τεχνικές προστασίας προτύπων είναι ικανές να δημιουργήσουν ένα διαφορετικό πρότυπο ανάλογα με τα αρχικά βιομετρικά στοιχεία του χρήστη και να ακυρώσει το παλιό πρότυπο που έχει, ίσως, παραβιαστεί.
- Ασφάλεια: Αυτή η ιδιότητα διασφαλίζει ότι το αυθεντικό πρότυπο των βιομετρικών στοιχείων δεν μπορεί ποτέ να ληφθεί από το ασφαλισμένο πρότυπο. Επομένως, αποκλείει έναν εισβολέα από την παραγωγή ενός αντιγράφου του αρχικού βιομετρικού προτύπου.
- Απόδοση: Διάφορες στρατηγικές για την προστασία του βιομετρικού προτύπου δεν θα πρέπει να υποβαθμίζουν την αποτελεσματικότητα των συστημάτων που βασίζονται σε βιομετρικά χαρακτηριστικά κατά την αναγνώριση του πιστοποιημένου χρήστη. Η αποτελεσματικότητα ενός συστήματος που βασίζεται σε βιομετρικά χαρακτηριστικά χαρακτηρίζεται από το ποσοστό αποδοχής (FAR) και από το ποσοστό ψευδούς απόρριψης (FRR). Μια ακριβής βιομετρική υποδομή δεν πρέπει να

έχει καμία αναληθή απόρριψη και αναληθή αποδοχή. Αυτό σημαίνει ότι τα βιομετρικά συστήματα πρέπει να αποδέχονται κάθε αυθεντικό χρήστη και να απορρίπτουν κάθε περίπτωση ψευδούς ταυτότητας. Τα FAR και τα FRR είναι αντιστρόφως ισοδύναμα μεταξύ τους. Εάν το FAR είναι μεγαλύτερο, τότε το FRR μειώνεται. Το βιομετρικό σύστημα που παράγει υψηλό FRR εγγυάται υψηλή ασφάλεια [16].

Το σημαντικό όμως σε όλα τα παραπάνω είναι ότι αυτές οι απαιτήσεις θα πρέπει να συμμορφώνονται ανάλογα με τις αλλαγές που γίνονται στα συστήματα προστασίας προτύπων. Για παράδειγμα μπορεί να υπάρξει μια νέα καταγραφή αμφιβληστροειδή ενός ανθρώπου σε διαφορετικές συνθήκες φωτισμού, ή μια νέα σάρωση ενός προσώπου το οποίο είχε γένια σε μια παλαιότερη καταγραφή. Τα συστήματα θα πρέπει να είναι ικανά με βάση τις απαιτήσεις που αναφέραμε να κάνουν και τις σωστές καταχωρίσεις.

Οι απαιτήσεις που παρουσιάσαμε παραπάνω θα πρέπει να είναι συμβατές με τον σχεδιασμό των συστημάτων προστασίας προτύπων.

Μία από τις πρώτες τεχνικές για τη βελτίωση του απορρήτου των βιομετρικών προτύπων βασιζόταν κυρίως στη χρήση τεχνικών κρυπτογράφησης όπως η κρυπτογράφηση DES, AES, RSA ή ECC. Στην Κρυπτογραφία, οι βιομετρικές πληροφορίες μετατρέπονται σε μη αναγνώσιμη μορφή δεδομένων όπως φαίνεται στην Εικόνα 3, όπου στη περίπτωση που ο επιτιθέμενος θελήσει να το διαβάσει, να μην μπορεί. Η διαδικασία μετασχηματισμού ονομάζεται κρυπτογράφηση. Απαιτείται ένα υπολογιστικό εργαλείο για την αποκρυπτογράφηση των κρυπτογραφημένων βιομετρικών δεδομένων. Ωστόσο, το πρόβλημα της χρήσης αυτής της τεχνικής είναι ότι δίνει τη δυνατότητα στον επιτιθέμενο να παρατηρήσει ότι μεταδίδεται κάτι χρήσιμο, δηλαδή ότι μέσα στη μετάδοση αυτή υπάρχει η πληροφορία που ψάχνει. Αυτό προσελκύει το ενδιαφέρον του να προσπαθήσει να το αποκρυπτογραφήσει χρησιμοποιώντας διαφορετικούς τρόπους. Γενικά, η διαδικασία κρυπτογράφησης δεν περιορίζει την ίδια την ύπαρξη των κρυφών δεδομένων.

Εικόνα 3:Κρυπτογράφηση δακτυλικού αποτυπώματος

Ένα άλλο πρόβλημα για τη χρήση της προσέγγισης κρυπτογράφησης για την εξασφάλιση της ακεραιότητας των βιομετρικών δεδομένων είναι ότι, ως επί το πλείστο, οι αλγόριθμοι κρυπτογράφησης παράγουν μια σημαντικά διακριτή σύνοψη ακόμη και με μικρές διακυμάνσεις στην είσοδο. Στην πραγματικότητα, όλα τα βιομετρικά δεδομένα αλλάζουν ανάλογα με τις περιβαλλοντικές συνθήκες. Για παράδειγμα, τα βιομετρικά στοιχεία του προσώπου και της ίριδας επηρεάζονται σοβαρά από τις συνθήκες φωτισμού. Κατά συνέπεια, πρακτικά αυτές οι τεχνικές δεν μπορούν να χρησιμοποιηθούν άμεσα, παρά το γεγονός ότι θεωρητικά είναι εξαιρετικά ισχυρές όταν εφαρμόζονται μόνο σε ακριβή δεδομένα. Επιπλέον, όταν τα βιομετρικά δεδομένα είναι κρυπτογραφημένα, απαιτείται αποκρυπτογράφηση για να πραγματοποιηθεί η αντιστοίχιση, κάτι που δημιουργεί ένα πιθανό σημείο επίθεσης για πρόσβαση στα αποκρυπτογραφημένα πρότυπα.

Λόγω αυτών των ζητημάτων, το βιομετρικό πρότυπο δεν μπορεί να αποθηκευτεί χρησιμοποιώντας παραδοσιακές κρυπτογραφικές μεθόδους, όπως οι αλγόριθμοι RSA και ο AES που ακολουθείται από πλήρη αντιστοίχιση δεδομένων στην κρυπτογραφημένη περιοχή. Τα βιομετρικά πρότυπα που προκύπτουν μετά την κρυπτογράφηση ενδέχεται να διαφέρουν σε μεγάλο βαθμό λόγω της μικρής διαφοροποίησης των αρχικών δεδομένων που σχετίζονται με τα βιομετρικά στοιχεία του χρήστη. Επομένως, δεν είναι χρήσιμοι στην περίπτωση προτύπων που σχετίζονται με βιομετρικά στοιχεία. Η κρυπτογράφηση του αρχικού προτύπου που σχετίζεται με τα βιομετρικά στοιχεία του χρήστη, ακολουθούμενη από αποκρυπτογράφηση του προτύπου αφήνει το πρότυπο ανοιχτό για επίθεση κατά τη διάρκεια κάθε προσπάθειας ελέγχου ταυτότητας. Για τον λόγο αυτό, οι τυπικές μέθοδοι κρυπτογράφησης δεν είναι πολύ χρήσιμες για την ασφάλεια των βιομετρικών προτύπων.

Μια άλλη τυπική τεχνική, όπως η μέθοδος του κατακερματισμού δεν ισχύει για το βιομετρικό πρότυπο. Δεν είναι δυνατή η αναστροφή σε μονόδρομες συναρτήσεις κατακερματισμού. Αυτές οι λειτουργίες μπορούν να δημιουργήσουν μια διαφορετική σύνοψη όποτε υπάρχει η παραμικρή αλλαγή στην είσοδο. Οι φυσικές συνθήκες επηρεάζουν τα βιομετρικά πρότυπα. Για παράδειγμα τα βιομετρικά στοιχεία της ίριδας και του προσώπου αλλάζουν από τις αλλαγές στο επίπεδο φωτισμού.

Η Ομάδα Εργασίας του Άρθρου 29 [15] έχει ήδη αναφέρει ότι τα βιομετρικά δεδομένα αποτελούν στις περισσότερες περιπτώσεις δεδομένα προσωπικού χαρακτήρα. Στις περιπτώσεις όπου τα βιομετρικά δεδομένα αποθηκεύονται με τρόπο που αποτρέπει οποιαδήποτε ανεπιθύμητη χρήση από τον αναλύοντα ή άλλα πρόσωπα για τον αναγνωρισμό του προσώπου στο οποίο αναφέρονται τα δεδομένα, αυτά τα δεδομένα δεν πρέπει να θεωρούνται προσωπικά. Ως εκ τούτου, μπορούν να υποβάλλονται σε επεξεργασία μόνο εφόσον υπάρχει νομική βάση και η επεξεργασία είναι κατάλληλη, συναφής προς το θέμα και όχι υπερβολική με όσον αφορά τους σκοπούς για τους οποίους αυτά συλλέγονται και/ή υφίστανται περαιτέρω επεξεργασία. Προϋπόθεση για την επεξεργασία και αποθήκευση των στοιχείων βιομετρίας θα πρέπει είναι ο σαφής ορισμός του λόγου και του σκοπού για τους οποίους τα βιομετρικά στοιχεία - δεδομένα θα πρέπει να επεξεργαστούνε αλλά και να αποθηκευτούνε, λαμβάνοντας υπόψιν τη διασφάλιση των ανθρωπίνων δικαιωμάτων και την ανθρώπινη ελευθερία. Η Ομάδα Εργασίας του Άρθρου 29 ήδη από το έγγραφο WP80 έχει ήδη αναφέρει τη σημασία της αυστηρής διάκρισης μεταξύ της επεξεργασίας των βιομετρικών δεδομενων για δημόσια παρακολούθηση-σκοπούς, όπως ο έλεγχος εισόδου στη χώρα και εκείνης που γίνεται για κάποιους απλούς σκοπούς με τη συγκατάθεση όμως των ενδιαφερόντων [15].

3 Βιομετρικά συστήματα και προστασία της ιδιωτικότητας

3.1 Ανάλυση βιομετρικών συστημάτων και προστασία της ιδιωτικότητας

Στον χώρο των βιομετρικών συστημάτων, τα βιομετρικά χαρακτηριστικά που συλλέγονται και δέχονται επεξεργασία αποτελούν προσωπικά δεδομένα τα οποία θα πρέπει να προστατεύονται από θεμελιώδεις νόμους και αρχές (GDPR). Άρα, ως προσωπικά δεδομένα ορίζουμε, οποιαδήποτε πληροφορία σχετίζεται με ένα ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο. όμως, κατά τη συλλογή και επεξεργασία των βιομετρικών χαρακτηριστικών, εάν κάποια χαρακτηριστικά δεν ταυτοποιούνται με κάποιο φυσικό πρόσωπο, τότε αυτά τα χαρακτηριστικά δε θεωρούνται προσωπικά δεδομένα και δεν εμπίπτουν στο πεδίο εφαρμογής του νόμου.

Ο αρχικός σκοπός της χρήσης των βιομετρικών χαρακτηριστικών ήταν για να διευκολύνει τους σκοπούς των αρχών της επιβολής του νόμου. Με τη χρήση των βιομετρικών χαρακτηριστικών οι Αρχές γλίτωναν σημαντικό χρόνο στη εύρεση υπόπτων, εγκληματιών και εξαφανισμένων ανθρώπων. Στο σενάριο τα συστήματα αυτά να μοιράσουν τις βάσεις δεδομένων σε επιχειρήσεις, οι οποίες βλέπουν πόσο εξυπηρετικά είναι και πόση ασφάλεια παρέχουν, για να διευκολύνουν, για παράδειγμα, την είσοδο των ανθρώπων στις τράπεζες και τις δημοσιές υπηρεσίες. Πόσο σίγουροι μπορεί να είμαστε ότι τα τρίτα μέρη αυτά που θα έχουν στη διάθεση τους τόσο ευαίσθητα προσωπικά δεδομένα ότι θα τα χρησιμοποιήσουν μόνο για τον αρχικό σκοπό χρήσης τους; Αυτά τα τρίτα μέρη μπορεί να περιλαμβάνουν αρχές επιβολής του νόμου, οι οποίες πρέπει να τηρούν συγκεκριμένους όρους κατά την επεξεργασία προσωπικών δεδομένων. Ειδικότερα, να δεσμεύονται από συγκεκριμένα νομοθετικά μέτρα.

3.2 Σκοπός και αναλογικότητα

Αναφορικά με τους σκοπούς ελέγχου της πρόσβασης, τα βιομετρικά συστήματα που αφορούν βιολογικά χαρακτηριστικά χωρίς ίχνη, όπως είναι το σχήμα του χεριού, δημιουργούν λιγότερους κινδύνους για τη προστασία των δικαιωμάτων των ανθρώπων. Διάφορες αρχές προστασίας δεδομενων εχουν υποστηρίξει αυτήν την άποψη, και προτειναν

ότι καλύτερο θα ήταν τα βιομετρικά στοιχεία να αποθηκεύονται σε συσκευές που ελέγχονται αποκλειστικά από το χρήστη ,όπως κάρτες με μικροτσίπ, κινητά τηλέφωνα ή τραπεζικές κάρτες.

Η χρήση βιομετρικών δεδομενων προϋποθέτει την αναλογικότητα και τη αλληλεξάρτηση προς το σκοπό επεξεργασίας τους . Πρέπει να αξιολογείται προσεκτικά η χρήση στοιχείων βιομετρίας , καθώς αυτά μπορεί να περιέχουν περισσότερες πληροφορίες από ότι είναι απαραίτητες για τους σκοπούς αναγνώρισης ή επαλήθευσης . Επι πρόσθετα , ορισμένα από αυτά μπορεί να αποκαλύπτουν ευαίσθητες πληροφορίες , όπως τη φυλετική καταγωγή ή θέματα υγείας. Είναι σημαντικό να διαγράφονται τα περιττά δεδομένα το συντομότερο δυνατό.

Τελικώς, η οργάνωση της χρήσης βιομετρικών συστημάτων μπορεί να βελτιώσει τη προστασία της ιδιωτικής ζωής, μειώνοντας την επεξεργασία άλλων προσωπικών δεδομενων ,όπως το ονοματεπώνυμο και τη διεύθυνση.

[3].

3.3 Παραδείγματα χωρών σχετικά με την προστασία προσωπικών δεδομένων σε συστήματα με χρήση βιομετρικών δεδομένων

Οι αρχές προστασίας δεδομένων έχουν εκφράσει την άποψη ότι ένας τρόπος αποτροπής της επαναχρησιμοποίησης των βιομετρικών δεδομένων από μη εξουσιοδοτημένα άτομα, είναι η αποθήκευση των βιομετρικών δεδομένων να μην πραγματοποιείται σε μια βάση δεδομένων μαζί με άλλα βιομετρικά δεδομένα άλλων ανθρώπων, αλλά να μένουν στο υποκείμενο στο οποίο ανήκουν τα δεδομένα αυτά. Δηλαδή, θα μπορούσε η αποθήκευση των δεδομένων αυτών να γίνεται σε μια έξυπνη κάρτα, ένα κινητό τηλέφωνο ή μια τραπεζική κάρτα. Δηλαδή, σε αντικείμενα που πρόσβαση θα έχει μόνο ο κάτοχος τους. Το ζήτημα του συμβατού σκοπού εγείρει επίσης το ζήτημα της διαλειτουργικότητας διαφορετικών συστημάτων που χρησιμοποιούν βιομετρικά στοιχεία, δηλαδή, κατά πόσο θα είναι λειτουργικές οι χρήσεις των καρτών, για παράδειγμα σε περισσότερα από ένα βιομετρικά σύστημα, και να μη χρειάζεται κάθε σύστημα να δέχεται ξεχωριστή κάρτα με τα αποθηκευμένα δεδομένα.

Παραδείγματα χωρών σχετικά με την αποθήκευση και τη χρήση των βιομετρικών δεδομένων:

- Στη Γαλλία και στο Ηνωμένο Βασίλειο οι αρχές προστασίας δεδομένων των χωρών αυτών εισήγαγαν ένα σύστημα αναγνώρισης της γεωμετρίας του χεριού και δαχτυλικών αποτυπωμάτων αντίστοιχα για την είσοδο των παιδιών στο σχολικό κυλικείο.
- Στη Γερμάνια, η γερμανική αρχή προστασίας δεδομένων ανακοίνωσε κατάλληλη απόφαση για την εισαγωγή βιομετρικών χαρακτηριστικών στα έγγραφα ταυτότητας προκειμένου να αποτραπεί η παραποίηση τους, υπό την προϋπόθεση ότι τα δεδομένα αποθηκεύονται στο μικροτσίπ της κάρτας (της ταυτότητας) και όχι σε βάση δεδομένων για σύγκριση με τα δακτυλικά αποτυπώματα του ιδιοκτήτη.
- Στην Πορτογαλία και στην Ελλάδα, από την άλλη μεριά, παρόμοιες μέθοδοι δεν ενστερνίστηκαν και δεν υποστηρίχτηκαν όπως στις δυο προηγούμενες χώρες. Η Ελλάδα και η Πορτογαλία θεωρούν την εφαρμογή των βιομετρικών συστημάτων για τον έλεγχο της εισόδου σε σχολεία ή σε δημοσίους φορείς για τον έλεγχο της προσέλευσης των η εργαζομένων υπερβολικό και δυσανάλογο για τον σκοπό αυτό [3].

Μια συγκεκριμένη δυσκολία μπορεί να προκύψει στο γεγονός ότι τα βιομετρικά δεδομένα περιέχουν συχνά περισσότερες πληροφορίες από όσες είναι απαραίτητες για τις λειτουργίες αναγνώρισης ή επαλήθευσης ταυτότητας. Για παράδειγμα, ορισμένα βιομετρικά δεδομένα μπορεί να αποκαλύπτουν φυλετική προέλευση ή να αφορούν την υγεία, τα οποία είναι ευαίσθητα δεδομένα που απαιτούν ενισχυμένη προστασία σύμφωνα με τη νομοθεσία περί προστασίας δεδομένων. Οι υπεύθυνοι επεξεργασίας δεδομένων έχουν πρόσθετες υποχρεώσεις να ενημερώνουν τους ανθρώπους από τους οποίους κάνουν συλλογή των δεδομένων τους, σχετικά με τον ακριβή ορισμό του σκοπού , αλλά και να γνωστοποιούν την εφαρμογή βιομετρικών τεχνικών στις αρχές προστασίας δεδομένων.

Τα συστήματα που χρησιμοποιούν διακριτή αναγνώριση προσώπου, συλλογή δακτυλικών αποτυπωμάτων, ηχογράφηση φωνής κ.λπ. ή συλλογή βιομετρικών δεδομένων χωρίς γνώση των υποκειμένων των δεδομένων, έχουν προφανώς περισσότερες δυσκολίες στη συμμόρφωση με τις απαιτήσεις προστασίας δεδομένων. Τέτοια συστήματα θα πρέπει να χρησιμοποιούνται για την προστασία πολύ συγκεκριμένων συμφερόντων όπως η δημόσια ασφάλεια ή η πρόληψη, η διερεύνηση, ο εντοπισμός και η δίωξη ποινικών αδικημάτων κ.λπ., και θα πρέπει να αποτελούν εξαίρεση. Από την άλλη πλευρά, πρέπει να αναφερθεί ότι η χρήση βιομετρικών δεδομένων μπορεί να συνεπάγεται μείωση της επεξεργασίας άλλων προσωπικών δεδομένων όπως όνομα, διεύθυνση, κατοικία κ.λπ. Στο

πλαίσιο αυτό τα βιομετρικά στοιχεία μπορούν να βελτιωθούν ως συστήματα φιλικά προς την προστασία της ιδιωτικότητας, σε σύγκριση με τα παραδοσιακή επεξεργασία προσωπικών δεδομένων.

3.4 Μέτρα ασφάλειας

Η ασφάλεια των δεδομένων είναι ένα από τα πιο σημαντικά μέρη της νομοθεσίας για την προστασία της ιδιωτικής ζωής. Οι υπεύθυνοι επεξεργασίας δεδομένων πρέπει να λαμβάνουν όλα τα κατάλληλα τεχνικά και οργανωτικά μέτρα ασφαλείας για την προστασία των προσωπικών δεδομένων από:

- τυχαία ή παράνομη καταστροφή,
- τυχαία απώλεια,
- τροποποίηση,
- μη εξουσιοδοτημένη αποκάλυψη ή πρόσβαση, ιδίως όταν η επεξεργασία περιλαμβάνει τη μετάδοση βιομετρικών δεδομένων μέσω δικτύου.

Πρέπει να λαμβάνονται μέτρα ασφαλείας κατά την επεξεργασία βιομετρικών δεδομένων (αποθήκευση, μετάδοση, εξαγωγή χαρακτηριστικών και σύγκριση, κ.λπ.) και ειδικότερα, εάν ο υπεύθυνος επεξεργασίας διαβιβάζει τα δεδομένα αυτά μέσω δημόσιων και μη ασφαλών δικτύων, όπως το Διαδίκτυο. Τα μέτρα ασφαλείας θα μπορούσαν να περιλαμβάνουν την κρυπτογράφηση των προτύπων ή τον έλεγχο της πρόσβασης και ιδίως τα κλειδιά κρυπτογράφησης. Επιπλέον, η ανωνυμία ή η χρήση ψευδωνύμων πρέπει να υπόκειται σε υψηλή προτεραιότητα ελέγχου, δηλαδή όταν δε χρησιμοποιείται το πραγματικό όνομα του υποκειμένου θα πρέπει να δίνεται μεγαλύτερη προσοχή στον έλεγχο του για να μπορεί να ταυτοποιηθεί ορθά. Για την απαραίτητη ασφάλεια θα πρέπει να λαμβάνονται μέτρα από την αρχή της επεξεργασίας του βιομετρικού στοιχείου, ιδίως κατά τη φάση εγγραφής όπου τα βιομετρικά δεδομένα πρέπει να μετατραπούν στα πρότυπα τους. Μετά τον μετασχηματισμό και την αποθήκευση των προτύπων, όλα τα δεδομένα που δεν απαιτούνται πλέον πρέπει να καταστραφούν.

Ένας άλλος τομέας ανησυχίας σχετίζεται με τον κίνδυνο σφαλμάτων, δηλαδή την ψευδή απόρριψη εξουσιοδοτημένων προσώπων και την ψευδή αποδοχή μη εξουσιοδοτημένων προσώπων. Είναι αποδεκτό ότι η χρήση βιομετρικών δεδομένων θα πρέπει να μειώσει τον κίνδυνο αυτού του είδους σφαλμάτων. Ωστόσο, αυτό μπορεί επίσης να δημιουργήσει την

ψευδαίσθηση ότι η αναγνώριση ή η πιστοποίηση του υποκειμένου των δεδομένων είναι πάντα σωστή. Επομένως, οι συνέπειες ενός λάθους μπορεί να είναι πολύ σημαντικές για το υποκείμενο των δεδομένων. Για παράδειγμα, ένα σύστημα μπορεί εσφαλμένα να προσδιορίσει ένα υποκείμενο δεδομένων ως άτομο που δεν πρέπει να του επιτραπεί να ταξιδέψει με αεροπλάνο ή δεν πρέπει να εισέλθει σε μια συγκεκριμένη χώρα.

Τέλος, η χρήση βιομετρικών στοιχείων ενδέχεται να βελτιώσει τις διαδικασίες ελέγχου στην περίπτωση πρόσβασης σε προσωπικά δεδομένα που σχετίζονται με τρίτους (π.χ. όταν γίνεται κάποια πληρωμή μέσω IBANK και χρειάζεται έγκριση). Πρέπει να ληφθούν υπόψη οι μηχανισμοί που έχουν τεθεί σε εφαρμογή για την επίλυση των προβλημάτων που προκύπτουν από απώλεια, κλοπή ή φθορά καρτών. Όπου γίνεται επεξεργασία ευαίσθητων δεδομένων, πρέπει να λαμβάνονται πολλά πρόσθετα μέτρα από τους υπεύθυνους επεξεργασίας δεδομένων και αίτηση για άδεια από τις Αρχές Προστασίας Δεδομένων, εφόσον απαιτείται από τη νομοθεσία.

3.5 Βιομετρικά συστήματα φιλικά προς την προστασία των προσωπικών δεδομένων.

Σύμφωνα με το προηγούμενο κεφάλαιο, η χρήση βιομετρικών συστημάτων εγείρει μεγάλες ανησυχίες σχετικά με το απόρρητο και απαιτεί τον εκ των προτέρων έλεγχο στη χρήση του και έγκριση από την Αρχή Προστασίας Δεδομένων. Ωστόσο, η νομοθεσία για την προστασία της ιδιωτικότητας (περί προσωπικών δεδομένων) επιτρέπει την εφαρμογή βιομετρικών συστημάτων σε ορισμένες περιπτώσεις, υπό την προϋπόθεση ότι πληρούνται οι αρχές του σκοπού και της αναλογικότητας και λαμβάνονται τα κατάλληλα μέτρα ασφαλείας. Σε ορισμένες περιπτώσεις, ωστόσο, τα βιομετρικά συστήματα μπορεί να θεωρηθούν ως συστήματα ενίσχυσης της ιδιωτικής ζωής, σε σύγκριση με μηχανισμούς ελέγχου ταυτότητας που βασίζονται στην κατοχή ή στη γνώση, εάν οδηγούν σε μείωση των προσωπικών δεδομένων που συλλέγονται και επεξεργάζονται, και έχουν ως αποτέλεσμα τη μείωση του κινδύνου παραβίασης της ιδιωτικής ζωής.

Δεδομένα που δεν μπορούν να σχετίζονται με συγκεκριμένα άτομα δεν αντιμετωπίζονται ως προσωπικά δεδομένα, δεν εμπίπτουν στο πεδίο εφαρμογής του νόμου. Τα βιομετρικά συστήματα, επομένως, τα οποία είναι σε θέση να ανωνυμοποιήσουν ή να καταστήσουν αδύνατη την επαναναγνώριση ενός ατόμου, είναι τα πιο φιλικά προς το απόρρητο. Μια απλή μέθοδος που έχει ήδη προταθεί στην τεχνική βιβλιογραφία, προβλέπει την

αποθήκευση και σύγκριση μιας σύνοψης αντί προτύπων, υπολογισμένη κατά την εγγραφή και την απόκτηση. Για τον υπολογισμό των αναλύσεων, μπορούν να χρησιμοποιηθούν συναρτήσεις κατακερματισμού μονής κατεύθυνσης. Επίσης, μπορούν να χρησιμοποιηθούν αλγόριθμοι κρυπτογράφησης.

Τέτοιες λύσεις συνεπάγονται ότι τα βιομετρικά δεδομένα εξάγονται μόνο για τον υπολογισμό ενός μοναδικού κλειδιού ή μυστικού (κωδικού πρόσβασης) μέσω μιας (με κλειδί) μονόδρομης συνάρτησης ή αλγόριθμου κρυπτογράφησης, αλλά όχι περαιτέρω επεξεργασία ή αποθήκευση.

Δυστυχώς, τα βιομετρικά δεδομένα δεν είναι σταθερά, όπως δείχνουν οι τύποι σφαλμάτων που εισήχθησαν παραπάνω. Τα βιομετρικά πρότυπα που εξάγονται και υπολογίζονται για έναν χρήστη σε διαφορετικές χρονικές στιγμές δεν είναι τα ίδια. Αυτό το πρόβλημα καθιστά ανέφικτο τον συνδυασμό βιομετρικών συστημάτων με μονόδρομες λειτουργίες και αλγόριθμους κρυπτογράφησης για τον σχεδιασμό ενός τέλειου βιομετρικού συστήματος φιλικό προς το απόρρητο.

4 Συστήματα αναγνώρισης προσώπου

4.1 Τι είναι το σύστημα αναγνώρισης προσώπου;

Το σύστημα αναγνώρισης προσώπου (facial recognition system) αναφέρεται στην αυτόματη αναγνώριση ή ταυτοποίηση ενός προσώπου από μια ψηφιακή εικόνα ή ένα βίντεο. Μία προσέγγιση για την επίτευξη αυτού είναι η σύγκριση επιλεγμένων χαρακτηριστικών του προσώπου από την εικόνα που λαμβάνεται με τα χαρακτηριστικά άλλων προσώπων σε μια βάση δεδομένων. Συνήθως χρησιμοποιείται σε συστήματα ασφαλείας και μπορεί να συγκριθεί με άλλες βιομετρικές μεθόδους, όπως η αναγνώριση δακτυλικών αποτυπωμάτων ή της ίριδας του ματιού.

Στον τομέα της ψυχολογίας, το πρόσωπο αποτελεί πλούσια πηγή πληροφοριών για την ανθρώπινη συμπεριφορά. Οι κινήσεις του προσώπου αποτυπώνουν συναισθήματα, ρυθμίζουν την κοινωνική αλληλεπίδραση, αποκαλύπτουν τη δραστηριότητα του εγκεφάλου και μεταφέρουν αισθήματα στα βρέφη. Η αναγνώριση προσώπου αναπτύσσει την ταυτοποίηση ανθρώπων χωρίς τη χρήση έγγραφων ή άλλων συστημάτων επαφής, όπως η αναγνώριση δακτυλικών αποτυπωμάτων ή της ίριδας του ματιού. Ο όρος αναγνώριση προσώπων αναφέρεται σε δύο διαφορετικά σενάρια εφαρμογής, την ταυτοποίηση (identification) και την πιστοποίηση (verification ή authentication).

Και στις δύο περιπτώσεις, πριν από την αναγνώριση, πραγματοποιείται η καταγραφή των εικόνων όπου η ταυτότητα ή η έκφραση του προσώπου είναι γνωστή. Κατά την καταγραφή, υπολογίζονται τα χαρακτηριστικά των προσώπων και αποθηκεύονται σε μια βάση δεδομένων που αποτελεί τη συλλογή του συστήματος. Μετά την καταγραφή, το σύστημα είναι έτοιμο να δεχτεί νέα, άγνωστα πρόσωπα δοκιμής και να αναγνωρίσει την ταυτότητα ή την έκφρασή τους. [6].

4.1.1 Ταυτοποίηση

Κατά τη διαδικασία της ταυτοποίησης , το σύστημα πρέπει να εντοπίσει την ταυτότητα ενός ατόμου μέσω της συλλογής στην οποία ανήκει η εικόνα δοκιμής. Αντιμετωπίζει το

ερώτημα «Ποιος είναι;» το προσώπου που απεικονίζεται . Αυτή η διαδικασία χωρίζεται σε δυο περιπτώσεις , τη ταυτοποίηση ανοικτού και κλειστού συνόλου. Στη ταυτοποίηση κλειστού συνόλου , η εικόνα δοκιμής ανήκει σε ένα από τα άτομα της συλλογής. Στην ταυτοποίηση ανοικτού συνόλου, η εικόνα δοκιμής υπάρχει περίπτωση να ανήκει και σε ένα άτομο που δεν έχει προηγουμένως καταγραφεί στη συλλογή.

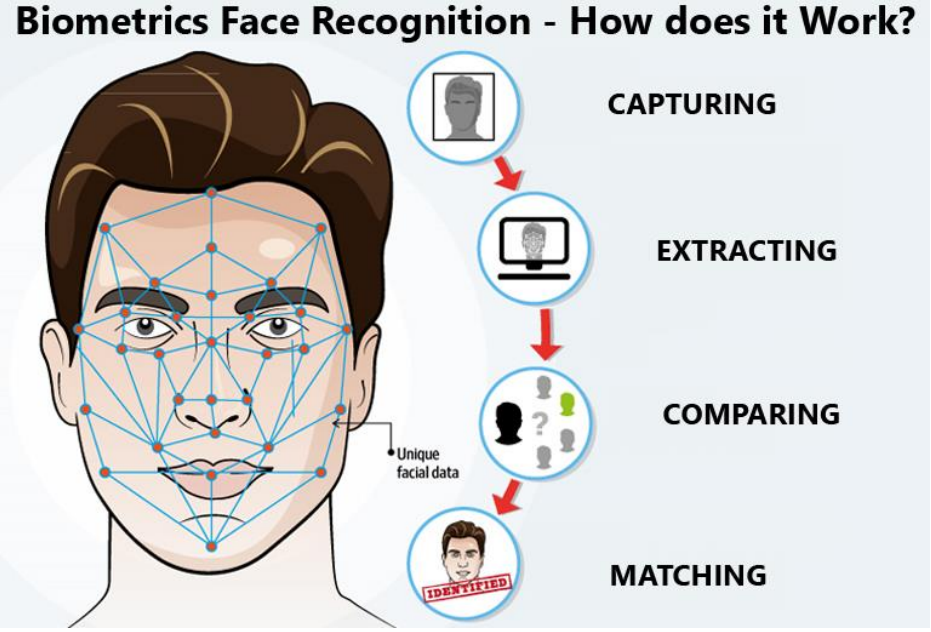
- Στην ταυτοποίηση κλειστού συνόλου, το σύστημα συγκρίνει την εικόνα δοκιμής με κάθε εικόνα της συλλογής για να εκτιμήσει την ομοιότητα και να αποφασίσει σε ποιο άτομο ανήκει

- Στην ταυτοποίηση ανοικτού συνόλου, αξιολογείται το καλύτερο μέτρο ομοιότητας σε σχέση με ένα κατώφλι, προκειμένου να ελεγχθεί εάν η εικόνα δοκιμής δεν ανήκει σε κανένα άτομο της συλλογής. Κατά τη διάρκεια της κάθε δοκιμής, δημιουργείται ένας μονοδιάστατος πίνακας με τα μέτρα ομοιότητας μεταξύ της εικόνας δοκιμής και κάθε εικόνας της συλλογής. Στη συνέχεια, τα άτομα στη συλλογή ταξινομούνται με φθίνουσα σειρά βάσει των μέτρων ομοιότητας, και τέλος επιστρέφεται η ταυτότητα του ατόμου με το υψηλότερο μέτρο.

Το επόμενο υποκεφάλαιο περιγράφει την έννοια της πιστοποίησης. Υπενθυμίζεται ότι η ταυτοποίηση και η πιστοποίηση είναι τα δυο διαφορετικά σενάρια εφαρμογής του όρου ‘αναγνώρισης προσώπου’.

4.1.2 Πιστοποίηση

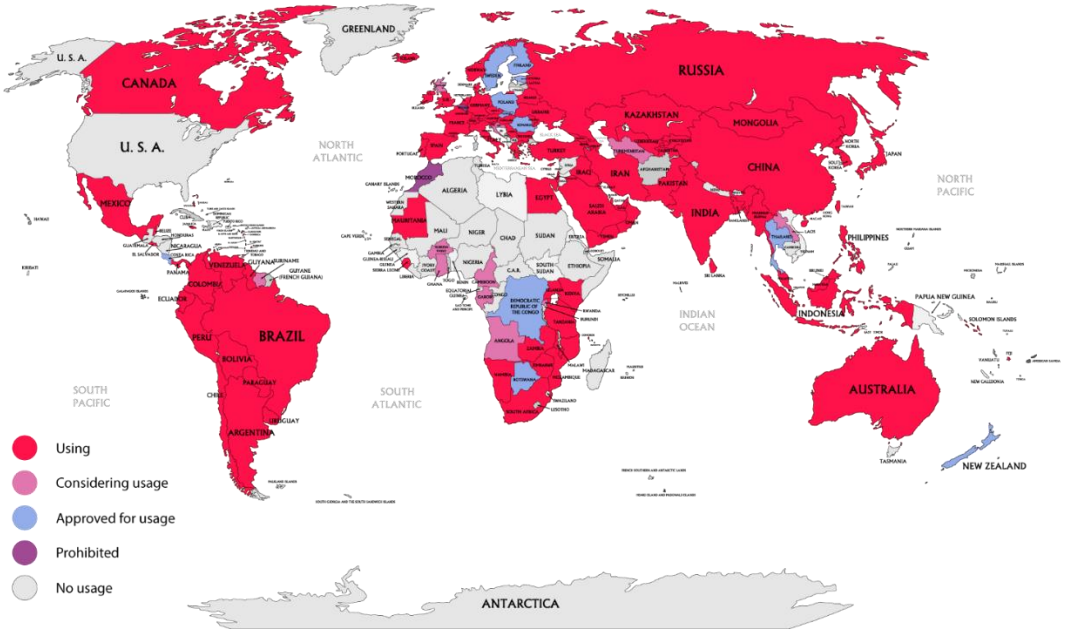
Στη πιστοποίηση , το σύστημα αναγνώρισης προσώπου θα κληθεί να εξακριβώσει την αληθή ταυτότητα του χρήστη που δηλώνει. Αντιμετωπίζει το ερώτημα « Είναι πράγματι αυτός που υποστηρίζει ότι είναι ;» και πρέπει να διακρίνει μεταξύ εξουσιοδοτημένου χρήστη και πλαστοπροσωπίας. Η εικόνα δοκιμής συγκρίνεται με εικόνες στη συλλογή του ατόμου που δηλώνει την ταυτότητα του , στη συνέχεια το επίπεδο ομοιότητας αξιολογείται έναντι ενός κατωφλίου για να αποφασιστεί εάν γίνεται αποδοχή του αιτήματος ή όχι. Ενώ λοιπόν η ταυτοποίηση αφορα μια σύγκριση ενός προς πολλούς (1:N) , η πιστοποίηση αφορα τη σύγκριση έναν προς έναν (1:1) .



Εικόνα 4:Τρόπος λειτουργείας συστήματος αναγνώρισης προσώπου

4.2 Σε ποιες χώρες χρησιμοποιείται η αναγνώριση προσώπου;

Η παρακάτω εικόνα παρουσιάζει τις χώρες και το επίπεδο χρήσης της τεχνολογίας αναγνώρισης προσώπου [6]. Η αναγνώριση προσώπου έχει καταστεί ευρέως διαδεδομένη σε πολλές χώρες παγκοσμίως. Ο αριθμός αυτός συνεχίζει να αυξάνεται καθώς πολλές χώρες έχουν εγκρίνει τη χρήση της τεχνολογίας αναγνώρισης προσώπου, αλλά δεν την έχουν ακόμη εφαρμόσει πλήρως. Αυτήν τη στιγμή, μόνο τρεις χώρες απαγορεύουν εντελώς τη χρήση της τεχνολογίας αναγνώρισης προσώπου(Β. Αμερική , Λουξεμβούργο , Βέλγιο).



Εικόνα 5:Σε ποιες χώρες χρησιμοποιείται η αναγνώριση προσώπου(Νοέμβριος του 2020)Πηγή:RecFaces

4.3 Τρόπος λειτουργίας των συστημάτων αναγνώρισης προσώπου

Συνολικά, στα συστήματα αναγνώρισης προσώπου χρησιμοποιούνται κυρίως δύο μέθοδοι. Η πρώτη μέθοδος, η γεωμετρική προσέγγιση, εστιάζει σε συγκεκριμένα χαρακτηριστικά του προσώπου, όπως η απόσταση μεταξύ των ματιών ή η σχέση του στόματος με τη μύτη. Αυτά τα χαρακτηριστικά χρησιμοποιούνται για να παράγουν πληροφορίες που στη συνέχεια χρησιμοποιούνται για σύγκριση μεταξύ διαφορετικών εικόνων. Η δεύτερη μέθοδος, η εικονογραφική προσέγγιση, είναι πιο περίπλοκη, καθώς καταγράφει ολόκληρη την εικόνα του προσώπου και χρησιμοποιεί όλες τις διαθέσιμες πληροφορίες. Αυτές οι πληροφορίες υποβάλλονται σε διάφορους υπολογιστικούς αλγορίθμους, όπως η μηχανική μάθηση, για τη δημιουργία συγκεκριμένων περιγραφών. Μια τέτοια βάση δεδομένων είναι φυσικά πιο αξιόπιστη, αν και το κόστος της μπορεί να είναι υψηλότερο.

Το ανθρώπινο πρόσωπο είναι ένα απαιτητικό πρότυπο για αναγνώριση, καθώς η βασική του δομή είναι σταθερή, ενώ υπάρχουν πολλοί παράγοντες που μπορούν να επηρεάσουν την εμφάνισή του. Οι συνθήκες φωτισμού, οι εκφράσεις του προσώπου, η χρήση καλλυντικών, τα διαφορετικά στιλ στα μαλλιά, η παρουσία αξεσουάρ όπως γυαλιά και γενειάδα είναι μερικοί από αυτούς τους παράγοντες. Η μεγάλη μεταβλητότητα των εικόνων, ειδικά όταν προέρχονται από διαφορετικές χρονικές στιγμές ή διαφορετικά

περιβάλλοντα, αποτελεί το κύριο πρόβλημα στην αναγνώριση προσώπου. Μια λύση για αυτό το πρόβλημα είναι η ενσωμάτωση επιπρόσθετων εικόνων στη βάση δεδομένων του συστήματος, καλύπτοντας έτσι την ποικιλομορφία των προσωπικών χαρακτηριστικών.

4.4 Η ακρίβεια των συστημάτων αναγνώρισης προσώπου

Παρόλο που η χρήση της τεχνολογίας επιτήρησης και αναγνώρισης προσώπου είναι ευρέως διαδεδομένη και συνεχώς αυξάνεται, αυτά τα συστήματα είναι ακόμη σε αρχικό στάδιο και συχνά μπορεί να είναι ανακριβή. Το μεγαλύτερο πρόβλημα είναι ότι είναι «hit and miss», δηλαδή χτυπούν εκείνον τον στόχο και φέρουν σε πέρας την αποστολή τους αλλά δεν είναι τόσο αξιόπιστα.

Οι περισσότεροι άνθρωποι επικροτούν την τεχνολογία αναγνώρισης προσώπου εάν αποτρέπει τη διάπραξη τρομοκρατικών χτυπημάτων και άλλων σοβαρών εγκλημάτων. Αλλά αυτό παραμένει ένα πολύ μεγάλο «αν» και τα πιθανά οφέλη πρέπει να σταθμιστούν σε σχέση με το κόστος για όλους μας από την καταγραφή των ίδιων μας των εαυτών και αυτών των στοιχείων στην αστυνομία. Η αστυνομία και άλλες υπηρεσίες επιβολής του νόμου θα πρέπει να είναι επιφυλακτικοί στο να βλέπουν τις νέες τεχνολογίες ως πανάκεια και άξιες χρήσης απλώς και μόνο επειδή η λέξη «ψηφιακή» μπορεί να χρησιμοποιηθεί για να τις περιγράψει.

Η τεχνολογία αναγνώρισης προσώπου έχει δύο μεγάλα προβλήματα. Το πρώτο είναι ότι η ακρίβειά του δεν πλησιάζει το 100%, που σημαίνει ότι η χρήση της τεχνολογίας θα οδηγήσει σε πολλά ψευδή θετικά αποτελέσματα. Λίγοι αλγόριθμοι εκπαιδεύτηκαν σε ένα πραγματικά αντιπροσωπευτικό δείγμα, επομένως η αναγνώριση προσώπου θα επηρεάσει δυσανάλογα αρνητικά διαφορετικά δημογραφικά στοιχεία. Αλλά ακόμα κι αν λάβουμε την υψηλότερη δημογραφική ακρίβεια σήμερα, η οποία είναι περίπου 99% για τους λευκούς άνδρες, και χρησιμοποιούσαμε την τεχνολογία σε μια περιοχή υψηλής κυκλοφορίας για να προσπαθήσουμε να εντοπίσουμε γνωστούς τρομοκράτες, για παράδειγμα, το 1% όλων των περαστικών θα ήταν εσφαλμένη παρακολούθηση, γεγονός που θα μπορούσε γρήγορα να προσθέσει εκατοντάδες ή χιλιάδες σφάλματα την ημέρα.

Το δεύτερο σημαντικό πρόβλημα είναι ότι οι χρήστες δεν έχουν συναινέσει στη σάρωση. Η δημόσια έξοδος δεν μπορεί να είναι συναίνεση για παρακολούθηση. Είναι δυνατό για μια οντότητα να χρησιμοποιήσει την παρακολούθηση προσώπου για να δημιουργήσει πλήρη ιστορικά τοποθεσίας και προφίλ, αν και με πολλά σφάλματα

4.5 Εφαρμογές των συστημάτων αναγνώρισης προσώπου

4.5.1 Συστήματα αναγνώρισης προσώπου και μάρκετινγκ/διαφημίσεις

Τα συστήματα αναγνώρισης προσώπου μπορούν να συνδεθούν με το μάρκετινγκ με διάφορους τρόπους:

Διαφήμιση με στόχο: Η τεχνολογία αναγνώρισης προσώπου μπορεί να χρησιμοποιηθεί για τον προσδιορισμό της ηλικίας, του φύλου και της εθνικότητας ενός ατόμου. Οι πληροφορίες αυτές μπορούν να χρησιμοποιηθούν για την προβολή στοχευμένων διαφημίσεων σε άτομα σε πραγματικό χρόνο. Για παράδειγμα, ένα σύστημα αναγνώρισης προσώπου που είναι εγκατεστημένο σε ένα εμπορικό κέντρο μπορεί να σαρώνει τα πρόσωπα των περαστικών, να προσδιορίζει το φύλο και την ηλικία τους και να εμφανίζει διαφημίσεις για προϊόντα ή υπηρεσίες που μπορεί να τους ενδιαφέρουν.

Ανάλυση πελατών: Οι λιανοπωλητές μπορούν να χρησιμοποιήσουν την τεχνολογία αναγνώρισης προσώπου για να αναλύσουν τη συμπεριφορά των πελατών τους στο κατάστημα. Παρακολουθώντας την κίνηση των πελατών, οι λιανοπωλητές μπορούν να προσδιορίσουν ποια προϊόντα είναι δημοφιλή και σε ποιες περιοχές του καταστήματος συχνάζουν περισσότερο. Οι πληροφορίες αυτές μπορούν να χρησιμοποιηθούν για τη βελτίωση της διάταξης του καταστήματος, την αλλαγή της τοποθέτησης των προϊόντων ή τον προσδιορισμό της αποτελεσματικότητας των προωθητικών ενεργειών.

Εξατομικευμένη εμπειρία: Η τεχνολογία αναγνώρισης προσώπου μπορεί να χρησιμοποιηθεί για την εξατομίκευση της εμπειρίας του πελάτη. Για παράδειγμα, ένα σύστημα αναγνώρισης προσώπου μπορεί να αναγνωρίσει έναν πελάτη που επιστρέφει και να παρέχει εξατομικευμένες συστάσεις με βάση τις προηγούμενες αγορές ή τη συμπεριφορά του.

Ασφάλεια και ανίχνευση απάτης: Η τεχνολογία αναγνώρισης προσώπου μπορεί να χρησιμοποιηθεί για την πρόληψη της απάτης με την επαλήθευση της ταυτότητας των πελατών. Αυτό μπορεί να είναι χρήσιμο σε περιπτώσεις όπου οι πελάτες έχουν πρόσβαση σε ευαίσθητες πληροφορίες ή πραγματοποιούν αγορές υψηλής αξίας.

Συνολικά, τα συστήματα αναγνώρισης προσώπου μπορούν να παρέχουν πολύτιμες πληροφορίες σχετικά με τη συμπεριφορά, τις προτιμήσεις και τα δημογραφικά στοιχεία των πελατών, οι οποίες μπορούν να βοηθήσουν τους εμπόρους να βελτιώσουν τη στόχευσή τους

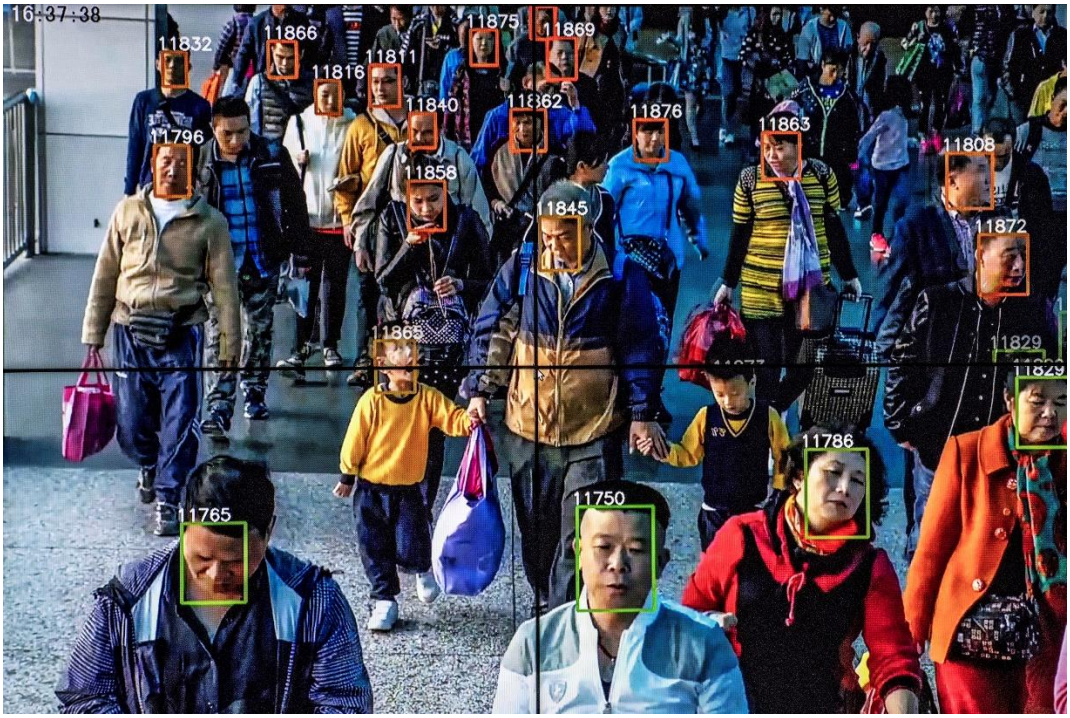
και να εξατομικεύσουν την εμπειρία των πελατών. Ωστόσο, είναι σημαντικό να λαμβάνονται υπόψη οι ανησυχίες για την προστασία της ιδιωτικής ζωής και να διασφαλίζεται ότι η χρήση της εν λόγω τεχνολογίας είναι διαφανής και ηθική.

4.5.2 Κίνα και συστήματα αναγνώρισης προσώπου

Το σύστημα αναγνώρισης προσώπου της Κίνας καταγράφει σχεδόν κάθε πολίτη στη χώρα, με ένα τεράστιο δίκτυο καμερών σε όλη τη χώρα. Μια διαρροή βάσης δεδομένων το 2019 έδωσε μια γεύση από το πόσο διάχυτα είναι τα εργαλεία επιτήρησης της Κίνας, με περισσότερα από 6,8 εκατομμύρια αρχεία από μια μέρα, τραβηγμένα από κάμερες τοποθετημένες γύρω από ξενοδοχεία, πάρκα, τουριστικά σημεία και τζαμιά, καταγράφουν στοιχεία για άτομα ηλικίας από 9 χρονών.

Η κινεζική κυβέρνηση κατηγορείται ότι χρησιμοποίησε την αναγνώριση προσώπου για να διαπράξει φρικαλεότητες κατά των Ουιγούρων Μουσουλμάνων, βασιζόμενη στην τεχνολογία για να πραγματοποιήσει τη μεγαλύτερη μαζική φυλάκιση ενός μειονοτικού πληθυσμού στον κόσμο σήμερα.

Η Κίνα χρησιμοποιεί την αναγνώριση προσώπου για τα προφίλ ατόμων Ουιγούρων, τα ταξινομεί με βάση την εθνικότητά τους και τα ξεχωρίζει για παρακολούθηση, κακομεταχείριση και κράτηση, όπως δήλωσε μια δικομματική ομάδα 17 γερουσιαστών σε επιστολή προς τον υπουργό Εξωτερικών Μάικ Πομπέο τον Μάρτιο του 2011. Αυτές οι τεχνολογίες αναπτύσσονται στην υπηρεσία ενός δυστοπικού οράματος για τη διακυβέρνηση της τεχνολογίας, που αξιοποιεί τα οικονομικά οφέλη του Διαδικτύου απουσία πολιτικής ελευθερίας και βλέπει τις εταιρείες τεχνολογίας ως όργανα κρατικής εξουσίας».



Εικόνα 6:Εικόνα από ένα monitor συστήματος αναγνώρισης προσώπου, όπου φαίνεται το ταυτόχρονο " κλείδωμα " πολλαπλών υποκειμένων σε ελάχιστο χρόνο.

4.5.3 Εποχή COVID_19 και συστήματα αναγνώρισης προσώπου

Τους τελευταίους μήνες η καθημερινότητα και ο τρόπος ζωής των ανθρώπων έχει αλλάξει, αιτία της αλλαγής αυτής είναι η πανδημία (covid-19) που έχει πλήξει το κόσμο. Υπάρχει ένα κοινό σημείο της πανδημίας με τα συστήματα αναγνώρισης προσώπου, και ποιο είναι αυτό; Η απάντηση θα μας δοθεί αν σκεφτούμε ότι ένα από τα αναπόσπαστα αξεσουάρ μας καθημερινά είναι η μάσκα μας, η οποία αποτελεί μεγάλο πρόβλημα στα συστήματα αυτά, αφού δεν μπορούν να καταγράψουν πλήρως τα χαρακτηριστικά του προσώπου.

Η Hanwang Technology (Κινέζικη εταιρεία) , με το προσωνύμιο Hanvon, υποστηρίζει ότι κυκλοφόρησε στην αγορά το πρώτο σύστημα αναγνώρισης προσώπου το οποίο μπορεί να κάνει αναγνωρίσεις προσώπων ακόμα και με τη χρήση μάσκας από το υποκείμενο ,την οποία μάσκα φορούν πλέον τόσοι άνθρωποι λόγω της νόσου Covid-19.

Το σύστημα αυτό :

- ✓ Εκτιμάται ακρίβεια περίπου της τάξης του 95% με μάσκα.

- ✓ Εάν επίσης συνδεθεί με εξωτερικά εργαλεία (αισθητήρες και IOT συστήματα) μπορεί μέσω της θερμοκρασίας του σώματος που θα μετράει να ελέγχει εάν έχει πυρετό κάποιος και εν συνεχεία να τον τακτοποιεί.

Η Ν. Κορέα θα δοκιμάσει την αναγνώριση προσώπου με τεχνητή νοημοσύνη για την παρακολούθηση περιπτώσεων COVID-19. Η Νότια Κορέα έχει ξεκινήσει ένα πιλοτικό έργο για τη χρήση AI(τεχνητής νοημοσύνης), για την παρακολούθηση της κίνησης των ανθρώπων που έχουν προσβληθεί από τον κορονοϊό ,ενώ παράλληλα εγείρονται οι ανησυχίες των ανθρώπων για παραβίαση της ιδιωτικής ζωής τους.

Το εθνικά χρηματοδοτούμενο έργο στο Bucheon,(πόλη της της Σεούλ με μεγάλο αριθμό πληθυσμού σε σχέση με την έκταση της πόλης), τέθηκε σε λειτουργία τον Ιανουάριο του 2022. Το σύστημα συνδυάζει τη τεχνολογία της AI και την τεχνολογία της αναγνώρισης προσώπου με σκοπό αναλύσει εγγραφές που συγκεντρώθηκαν από περίπου 11.000 κάμερες τύπου "CCV" . Με σκοπό να παρακολουθεί τις κινήσεις ενός μολυσμένου ατόμου και εν συνεχεία να φτιάχνει ένα <<μονοπάτι>> ώστε να δει με ποιους ανθρώπους ήρθε σε επαφή ,ποιοι από αυτούς δεν φορούσαν μάσκα και να εντοπίσει πιθανά άλλα κρούσματα.[25].

Ο αγώνας κατά του COVID-19 ανάγκασε τις κυβερνήσεις να διερευνήσουν νέες επιλογές και να διευρύνουν τα νομικά τους όρια. Χώρες όπως η Πολωνία, η Κίνα, η Ιαπωνία, η Ινδία, η Ρωσία και επιλεγμένες πολιτείες της Αμερικής έχουν ξεκινήσει ή σχεδιάζουν να πρωτοπορήσουν στην τεχνολογία αναγνώρισης προσώπου για τον εντοπισμό κρουσμάτων COVID-19. Αν και οι κανονισμοί απαιτούν από τους ασθενείς να δώσουν προηγούμενη συγκατάθεση, το σύστημα μπορεί να τους αναγνωρίσει και να τους ακολουθήσει με βάση τα ρούχα και το περίγραμμά τους, ακόμα κι αν αρνηθούν να εξουσιοδοτήσουν τη χρήση αναγνώρισης προσώπου. Ο Οργανισμός Ελέγχου και Πρόληψης Νοσημάτων της Κορέας (KDCA) δήλωσε ότι η χρήση αυτής της τεχνολογίας είναι νόμιμη, εφόσον χρησιμοποιείται εντός της σφαίρας της νομοθεσίας για τον έλεγχο και την πρόληψη ασθενειών. Το σχέδιο σάρωσης αναγνώρισης προσώπου AI έρχεται καθώς η χώρα πειραματίζεται με άλλες χρήσεις της αμφιλεγόμενης τεχνολογίας, από τον εντοπισμό κακοποίησης παιδιών σε παιδικούς σταθμούς μέχρι την παροχή αστυνομικής προστασίας [9].

4.5.4 Συστήματα αναγνώρισης προσώπου στα σώματα ασφαλείας και στις κυβερνητικές υπηρεσίες

Η ασφάλεια στο δημόσιο χώρο αποτελεί προτεραιότητα κάθε νομικού συστήματος, γεγονός που την καθιστά προτεραιότητα στο σχεδιασμό για την πρόληψη και την καταπολέμησή των εγκλημάτων. Η εμφάνιση νέων εγκληματικών μεθόδων και η χρήση της τεχνολογίας, για εγκληματικούς σκοπούς ,εχουν καταφέρει να αναγκάσουν τις αρχές επιβολής του νόμου να προσαρμοστούν γρήγορα στις νέες καταστάσεις. Από αυτή την άποψη, η ψηφιακή αναγνώριση προσώπου έχει γίνει αναπόσπαστο μέρος της εργαλειοθήκης της αστυνομίας παγκοσμίως, στόχος είναι να χρησιμοποιηθεί ως ένας ακόμη σύμμαχος στην πάταξη των εγκλημάτων. [5].

4.5.5 Η χρήση της τεχνολογίας αναγνώρισης προσώπου από την Αστυνομία και τις δημόσιες αρχές

Η αστυνομική βάση δεδομένων ,στο Ηνωμένο Βασίλειο, περιλαμβάνει περίπου 23 εκατομμύρια πρόσωπα . Οι αρχές επιβολής του νόμου - αστυνομικές αρχές κάνουν χρήση της τεχνολογίας αυτής για τη πρόληψη και τη πάταξη της εγκληματικότητας χωρίς όμως στην ενδοχώρα να έχει θεσπιστεί ένα κανονιστικό πλαίσιο χρήσης των συστημάτων αυτών. Σοβαρές ανησυχίες εξέφρασε ο Βρετανικός Επίτροπος Βιομετρίας (Biometrics Commissioner), ο οποίος στη έκθεσή του (το 2018) [5] επισημαίνει τον κίνδυνο ότι χωρίς νομικό πλαίσιο η ισορροπία μεταξύ ιδιωτικής ζωής και δημόσιου συμφέροντος αφήνεται στην αστυνομία, ενώ ταυτόχρονα η τεχνολογία αυτή λειτουργεί με τρόπο όπου λαμβάνουν χώρα διακρίσεις , αναγνωρίζοντας λανθασμένα περισσότερο γυναίκες και έγχρωμα άτομα.

Στην Σουηδία, έχει επιβλήθηκε το πρώτο πρόστιμο που είχε να κάνει με την παράβαση του Γενικού Κανονισμού Προστασίας Δεδομένων και ειδικότερα την επεξεργασία αναγνώρισης προσώπου μέσω βιντεοεπιτήρησης σε σχολείο. Η επεξεργασία βιομετρικών δεδομένων απαγορεύεται επειδή, εκτός αν υπάρχει κάποια από τις εξαιρέσεις που προβλέπει το άρθρο 9 παράγραφος 2 του GDPR.

Στην Ελλάδα έχει εγκριθεί η προμήθεια τεχνολογίας αναγνώρισης προσώπου για την Ελληνική Αστυνομία αναγνώρισης προσώπου για την Ελληνική Αστυνομία. Μέχρι και το 2018 όμως δεν είχε θεσπιστεί νομοθεσία για το τρόπο χρήσης και επεξεργασίας των δεδομενων που θα συλλέγονται.

Οι περισσότερες δημοκρατικές χώρες, όπου γίνεται εκτεταμένη χρήση της τεχνολογίας αυτής, έχουν αρχίσει να εκδηλώνουν κινήματα που ζητούν την απαγόρευση των συστημάτων αναγνώρισης προσώπου. Παράλληλα, εμφανίζονται καθημερινά νέες προκλήσεις, όπως μάσκες ή ενδύματα με πολύπλοκα μοτίβα, που στόχο έχουν να ξεγελάσουν τους αλγόριθμους.

Η Ελληνική Αστυνομία συμμετέχει (από τον Αύγουστο του 2018 έως τον Ιούλιο του 2021) σε ένα ερευνητικό πρόγραμμα της Ευρωπαϊκής Ένωσης, με την ονομασία SPIRIT («Εξετάσιμη ανάλυση ιδιωτικού απορρήτου για την επίλυση ταυτοτήτων»).(Για περισσότερες πληροφορίες https://www.asktheeu.org/en/request/access_to_documents_request_rela_2#incoming-24429). [31]

4.6 Μη ορθολογική χρήση των συστημάτων αναγνώρισης προσώπου

Η επικίνδυνη και η λανθασμένη χρήση των συστημάτων αναγνώρισης προσώπου μπορεί να αποτυπωθεί από ένα περιστατικό το οποίο έχει καταγραφεί στο Detroit το 2018, όπου τα συστήματα αναγνώρισης προσώπου ΄΄κατηγόρησαν΄΄ για ένα έγκλημα λάθος άνθρωπο που παραλίγο να του κοστίσει την ελευθερία του. Η αιτία της λανθασμένης ταύτισης οφείλεται στη μη ανανέωση των αποθηκευμένων εικόνων που είχε η βάση δεδομένων, με αποτέλεσμα η παλιά εικόνα να μη συμβαδίζει με τη πραγματική εικόνα του ανθρώπου που ήταν όντως ο ένοχος.

Το παραπάνω γεγονός αποτελεί ένα ατράνταχτο παράδειγμα για τους κινδύνους αλλά και τα όρια που πρέπει να αναθεωρηθούν, ή ακόμα και να δημιουργηθούν νέα, από τις αρχές επιβολής του νόμου. Αποτελεί λογικό επακόλουθο το να έχει ο κόσμος απορία εάν είναι αρκετό ένα matching μιας φωτογραφίας από μια βάση δεδομενων για να κατηγορηθεί κάποιος για ένα έγκλημα. Γι αυτο θα πρέπει να δοθεί μια απάντηση για τη περίπτωση της ευθύνης μιας λανθασμένης ταυτοποίησης η οποία μπορεί να φέρει πολύ σοβαρές επιπτώσεις στη ζωή ενός ανθρώπου. Δηλαδή για το λάθος ενός υπολογιστή ποιος θα είναι υπόλογος;[7].

5 Κίνδυνοι της γενικευμένης βιντεοεπιτήρησης με τεχνολογία αναγνώρισης προσώπου

5.1 Συστήματα αναγνώρισης προσώπου και τεχνολογικοποίηση των διακρίσεων

Μέσα από τη βιβλιογραφική μελέτη , ήρθε στην επιφάνεια μια έρευνα του National Institute of Standards and Technology (NIST) η οποία αναφερότανε την εσφαλμένη αναγνώριση (false positives) από το facial recognition. Πιο ειδικά η έρευνα αυτή είχε αποδείξει ότι μέχρι και 100 φορές περισσότερο, σε σχέση με τους λευκούς ανθρώπους, γίνεται λάθος αναγνώριση σε ανθρώπους αφρικανική ή ασιατικής καταγωγής.

Ένα από τα βασικά προβλήματα που παρουσιάζουν τα τρία κύρια εργαλεία ψηφιακής αναγνώρισης προσώπων, τα οποία έχουν αναπτυχθεί από τεχνολογικούς γίγαντες όπως η Microsoft, η IBM και η Megvii, είναι ότι παρουσιάζουν σφάλματα σε περίπου ένα στα τρία κρούσματα κατά την αναγνώριση του φύλου μαύρων γυναικών. Αντίθετα, το ποσοστό σφάλματος στην ταυτοποίηση του φύλου λευκών ανδρών ανέρχεται μόλις στο 1%.

Σε μια παράλληλη έρευνα για το λογισμικό Rekognition της Amazon, προέκυψε ότι το πρόγραμμα έκανε εσφαλμένες ταυτοποιήσεις για 28 μέλη του Κογκρέσου, συνδέοντας τα ακούσια με άτομα που είχαν παλαιότερα συλληφθεί για εγκλήματα. Τα λάθη στις ταυτοποιήσεις κυρίως επηρέαζαν σε μεγάλο βαθμό μαύρους και Λατίνους. Ο υψηλός αριθμός λανθασμένων ταυτοποιήσεων σε βάρος των μαύρων ουσιαστικά ενισχύει την τεχνολογική επιβεβαίωση των ήδη υπαρχουσών διακρίσεων. [7]

5.2 Καθημερινές απειλές

Η τεχνολογία αναγνώρισης προσώπου δεν χρησιμοποιείται μόνο για την αναγνώριση εγκληματιών από τις αστυνομικές αρχές. Όσο περίεργο και αν ακούγεται και όσο αγχωτικό, τα συστήματα αυτά έχουν μπει πια στη καθημερινότητά μας και, πιο ειδικά, βρίσκονται ακόμα και μέσα στο σπίτι μας. Τα κινητά μας τηλέφωνα χρησιμοποιούνται ως διαμεσολαβητές ανάμεσα στα στοιχεία του προσώπου μας και της βάσης δεδομένων όπου αποθηκεύονται. Υπάρχουν προγράμματα τα οποία διαθέτουν συστήματα αυτόματης αναγνώρισης προσώπου με σκοπό να ταξινομούν τις φωτογραφίες, των χρηστών, σε

άλμπουμ σύμφωνα με τα πρόσωπα τα οποία εμφανίζονται ,στις φωτογραφίες. Κάποιες ενδεικτικές εφαρμογές είναι το Facebook , to windows Photo Gallery και το Picassa.

Είμαστε στον 21ο αιώνα και η τεχνολογία αναπτύσσεται ραγδαία μέρα με τη μέρα, με βάση τα επιτεύγματα της τεχνολογίας ,μπορούμε να υποθέσουμε ότι κάθε φωτογραφία που δημοσιεύεται στο διαδίκτυο, αναλύεται από κάποιο σύστημα αναγνώρισης προσώπου. Ένα απλό παράδειγμα, σε ένα από τα πιο γνωστά ΜΜΕ το Facebook κατά τη δημοσιοποίηση μιας φωτογραφίας, η εταιρία έχει ειδικό λογισμικό αναγνώρισης προσώπου και σε ρωτάει αν όντως στην φωτογραφία απεικονίζεται ο Χ. Η λειτουργία της αναγνώρισης προσώπου από το Facebook γίνεται έπειτα από ανάλογη ρύθμιση που έχουμε κάνει στις ρυθμίσεις του λογαριασμού μας και έχουμε αποδεχτεί την επεξεργασία και την αποθήκευση των στοιχείων του προσώπου. Πολυεθνικές όπως η Google και η Clearview AI χρησιμοποιούν αναγνώριση προσώπου με σκοπό να συλλέγουν διακριτικά εικόνες από το διαδίκτυο για να πουλήσουν τεχνολογία αναγνώρισης προσώπου στην αστυνομία εδώ και χρόνια.

5.3 Παραβίαση της ιδιωτικότητας.

Σύμφωνα με τον GDPR, οι ενσωματώσεις προσώπων για επεξεργασία απαγορεύονται από προεπιλογή και η επεξεργασία τους απαιτεί να πληρούνται ειδικοί όροι ή να υπόκεινται όλοι οι ενδιαφερόμενοι σε συναίνεση. Ωστόσο, η συναίνεση της βιντεοπαρακολούθησης, μπορεί να είναι πολύ δύσκολη. Τα υποκείμενα σε δημόσιους χώρους μπορεί να μην γνωρίζουν καν ότι παρακολουθούνται. Στον κόσμο της τεχνολογίας πολλές φορές δυο έννοιες οι οποίες ακούμε συχνά, απόρρητο και ασφάλεια, δε τις αποσαφηνίζουμε σωστά, αφήνοντας πολλές φορές την εντύπωση ότι είναι συνώνυμες, το οποίο δεν ισχύει. Για παράδειγμα, τα τελευταία χρόνια σχεδόν όλα τα κινητά τηλεφωνά (smartphone) έχουν βελτιώσει την ασφάλειά τους, χρησιμοποιώντας προηγμένη ασφάλεια κλειδώματος της συσκευής με κάποιο βιομετρικό χαρακτηριστικό (δαχτυλικό αποτύπωμα ή και αναγνώρισης προσώπου). Μέχρι εδώ βλέπουμε ότι η ασφάλεια που παρέχουν οι κινητές συσκευές ώστε να μην μπορούν να χρησιμοποιηθούν έμμεσα από κάποιον άλλον είναι πολύ δυνατή. Όμως από την άλλη μεριά οι συσκευές αυτές έχουν ενσωματωμένες βάσεις δεδομένων στις οποίες αποθηκεύονται τα βιομετρικά χαρακτηριστικά ώστε σε κάθε απόπειρα μας να ξεκλειδώσουμε τη συσκευή να τα συγκρίνει και να δίνει πρόσβαση ή όχι, αντίστοιχα. Αυτές οι βάσεις ό,τι καταγράφουν το κρατάνε για πάντα, ανάλογα με την εφαρμογή, ούτε το βιομετρικό πρότυπο ούτε τα μεταγενέστερα δείγματα προσώπου διαγράφονται από τη

συσκευή τους. Έτσι εάν το κινητό τηλέφωνο πέσει σε κάποιον ειδικό της τεχνολογίας και κακόβουλο άτομο, θα μπορέσει να πάρει πρόσβαση στη βάση δεδομένων μας. Το αποτέλεσμα σε αυτό το σενάριο είναι ότι τα προσωπικά δεδομένα μας και ειδικότερα τα βιομετρικά δεδομένα μας (που συζητάμε) θα είναι στη διάθεση του εκάστοτε κακόβουλου ατόμου. Τελικό συμπέρασμα του παραδείγματος είναι ότι η ασφάλεια και το απόρρητο δεν είναι συνώνυμες λέξεις, μπορούν όμως να συνυπάρχουν μαζί.

Η τεχνολογία αναγνώρισης προσώπου είναι πλέον κοινωνικά αποδεκτή επειδή οι άνθρωποι έχουν συνηθίσει να την έχουν στα smartphone τους. Ωστόσο, η σημαντική διαφορά είναι ότι αυτό γίνεται από δική τους επιλογή προκειμένου να προστατεύσουν τα δικά τους περιουσιακά στοιχεία.

Η επιτήρηση με αναγνώριση προσώπου θα γίνει πιθανώς πιο συνηθισμένη, ειδικά σε δημόσιους χώρους, όπως συγκοινωνιακά κέντρα και μεγάλες εκδηλώσεις. Αλλά ακόμη και σε έναν δημόσιο χώρο, έχουμε έναν ορισμένο βαθμό ανωνυμίας, καθώς η συντριπτική πλειονότητα των ανθρώπων δεν γνωρίζει ποιοι είμαστε, υποθέτοντας ότι δεν είμαστε δημόσιο-αναγνωρίσιμο πρόσωπο. Μπορούμε να μπούμε στο μετρό χωρίς να μας αναγνωρίσει κανείς. Ωστόσο, εάν μια κάμερα ασφαλείας εξοπλισμένη με αναγνώριση προσώπου μας αναγνωρίσει, μπορεί να συνδέσει τη φυσική μας ταυτότητα (χαρακτηριστικά σώματος) με την ψηφιακή σας ταυτότητα, και μπορεί να το κάνει χωρίς να λάβει πρώτα τη συγκατάθεσή μας.

5.4 Η επιτήρηση σε δημόσιους χώρους

Ένα καλό παράδειγμα της χρήσης της βιντεοεπιτήρησης αποτελεί ο τελικός του αμερικανικού ποδοσφαίρου (Super Bowl) ο οποίος γίνεται κάθε χρόνο στην Αμερική. Αυτός ο τελικός είναι το πιο σημαντικό γεγονός παγκοσμίως. Όλα αυτά συμβάλλουν τον να είναι νούμερο ένα στόχος τρομοκρατικής ή άλλης επικίνδυνης επίθεσης.

Τα πρώτα Super Bowl βασίστηκαν σε ελικόπτερα, αστυνομικούς σκύλους και υπηρεσίες ασφαλείας για να διασφαλίσουν τη δημόσια ασφάλεια. Αυτού του είδους τα μέτρα ασφαλείας είναι κορυφαία και αναμφίβολα λειτουργούν ως ισχυροί αποτρεπτικοί παράγοντες. Ωστόσο, δεν μπορούν να εμποδίσουν γνωστούς κακοποιούς στις αρχές, (δηλαδή τους ψάχνουν ή τους είχαν συλλάβει παλιότερα και έχουν φωτογραφίες τους) να εισέλθουν στο γήπεδο και εκεί είναι που τα συστήματα αναγνώρισης προσώπου λύνουν τα χεριά των αρχών. Οι κάμερες σαρώνουν πρόσωπα, το λογισμικό συγκρίνει τις καταγεγραμμένες λίστες παρακολούθησης, το ανθρώπινο προσωπικό εξετάζει τους πιθανούς αγώνες και στη συνέχεια η ασφάλεια του χώρου ξεκινά τη διαδικασία αφαίρεσης μετά τον αγώνα. επιβεβαιωμένος. Όπως καταλαβαίνουμε, η σημασία της βιντεοεπιτήρησης σε τέτοια συμβάντα είναι απαραίτητη για την ασφάλεια του κόσμου. Αλλά σίγουρα υπάρχει και η άλλη πλευρά η οποία υποστηρίζει ότι θα πρέπει να υπάρχει άμεση ενημέρωση των πολίτων όταν μπαίνουν σε χώρο που καταγράφονται από συστήματα αναγνώρισης προσώπου, ώστε να τους δοθεί η δυνατότητα να αποφασίσουν αν θέλουν να εισέλθουν στον χώρο ή όχι.

Αλλά τι γίνεται αν ένα άτομο είναι μόνο για ανάκριση; Ή τι γίνεται αν οι αρχές θέλουν απλώς να παρακολουθούν πού πηγαίνει ένα συγκεκριμένο άτομο και με ποιον συναντά; Πρέπει να τηρείται μόνιμο αρχείο για το πότε η εικόνα ενός ατόμου καταχωρίστηκε στη λίστα παρακολούθησης και κατόπιν αιτήματος ποιου; Είναι σαφές ότι απαιτείται κάποιο επίπεδο επίσημης διαδικασίας προκειμένου να αποφευχθεί η κατάχρηση. Ένας καχύποπτος σύζυγος μπορεί να μπει στον πειρασμό να θέλει να παρακολουθεί τη σύζυγό του. Ένα άτομο που διεκδικεί ένα αξίωμα μπορεί να θέλει να μάθει ποιον επισκέπτεται ένας αντίπαλος. Τέτοιες καταχρήσεις εξουσίας δεν είναι φυσικά καινούριες με την τεχνολογία αναγνώρισης προσώπου.

5.4.1 Αρχειοθέτηση εικόνων

Μια άλλη πιθανή ανησυχία είναι η μαζική αρχειοθέτηση εικόνων για πιθανή μελλοντική χρήση. Οι μόνες εικόνες ανιχνευτών που αποθηκεύονται από το σύστημα είναι αυτές που καταγράφουν μια πιθανή αντιστοίχιση σε κάποιον στη συλλογή. Ωστόσο, δεν υπάρχει πραγματικός τεχνικός περιορισμός για την αρχειοθέτηση όλων των εικόνων προσώπων που έχουν ληφθεί από το σύστημα. Το αρχείο των εικόνων θα μπορούσε στη συνέχεια να «εξαχθεί» στο μέλλον για να διαπιστωθεί εάν ένα συγκεκριμένο άτομο βρισκόταν στο σημείο ελέγχου στο παρελθόν.

5.4.2 Βάσεις δεδομένων

Ένα θέμα που γενικά αυξάνει την ένταση όλων των άλλων ανησυχιών είναι αυτό των συστημάτων και βάσεων δεδομένων δικτυακής αναγνώρισης. Όπως αρχικά οραματιζόμαστε, ένα σύστημα αναγνώρισης προσώπου παρέχει έναν τρόπο ανίχνευσης όταν ένα συγκεκριμένο άτομο εισέρχεται σε μια συγκεκριμένη περιοχή επιτήρησης. Κάθε μεγάλο αεροδρόμιο και κάθε μεγάλο δημόσιο κτίριο μπορεί να έχει το δικό του ανεξάρτητο σύστημα επιτήρησης.

Τι θα γινόταν όμως αν όλα αυτά τα συστήματα ήταν δικτυωμένα μαζί; Για παράδειγμα, ένα άτομο το οποίο μπορεί να βρίσκεται στη λίστα παρακολούθησης για τη διέλευσή του από τον Καναδά στα σύνορα με τις Ηνωμένες Πολιτείες, θα μπορούσε να εντοπιστεί κατά τη διέλευση των συνόρων και η εικόνα του να προωθείται στη λίστα παρακολούθησης για τα διόδια του δρόμου της ταχείας κυκλοφορίας. Το άτομο θα μπορούσε να εντοπιστεί ξανά καθώς βγαίνει στην έξοδο προς το αεροδρόμιο, και η εικόνα του θα μπορούσε να προωθείται στη λίστα παρακολούθησης του συστήματος αεροδρομίου. Κάθε ένα από αυτά τα γεγονότα μπορούν επίσης να δίνουν αναφορά σε μια κεντρική τοποθεσία. Το αποτέλεσμα είναι μια συνεχής παρακολούθηση της τοποθεσίας του ατόμου. Ενώ μπορεί να πιστεύουμε ότι αυτό είναι καλό για έναν όχι και ΄΄τόσο καλό πολίτη΄΄ που είναι σε έναν α΄ κατάλογο των ύποπτων τρομοκρατών, εμείς θα το βλέπαμε ως παραβίαση της ιδιωτικής ζωής εάν γινόταν για ένα άτομο που έχει απλώς υπάρξει έντονος κριτικός σε κυβερνητικές πολιτικές. Αν αυτό γίνεται χωρίς επιτήρηση και αλόγιστα θα φτάσουμε σε ένα άλλο σημείο που θα το παρομοιάζαμε με το γνωστό τηλεοπτικό πρόγραμμα <<Big Brother>>. [17]

5.5 Πολιτικές για τη Βιομηχανία και την Κυβέρνηση από τις αρχές του 20ου αιώνα μέχρι τώρα.

Κατά τις αρχές 20ου αιώνα δεν υπήρχαν νομικές οδηγίες για το πού και πώς η τεχνολογία αναγνώρισης προσώπου μπορεί να χρησιμοποιηθεί σε δημόσιους χώρους [4]. Οι τοπικές αρχές παίρνουν αποφάσεις για την ανάπτυξη της τεχνολογίας αναγνώρισης προσώπου κατά περίπτωση και μερικές φορές χωρίς σαφή κατανόηση του τι εγκρίνουν. Υπάρχουν σημαντικά ερωτήματα ως προς τις πολιτικές που πρόκειται δρομολογηθούν για να ελέγξουν τον τρόπο που η κυβέρνηση κάνει χρήση αυτής της τεχνολογίας. Πώς θα έπρεπε να γίνει η εγκατάσταση του συστήματος αναγνώρισης προσώπου σε ένα συγκεκριμένο δημόσιο χώρο, ώστε να προταθεί, να εγκριθεί και να παρακολουθείται; Ποιες τεχνικές απαιτήσεις απόδοσης πρέπει να υπάρχουν για τέτοια συστήματα; Τι είδους ειδοποίηση πρέπει να δοθεί σχετικά με τη χρήση της τεχνολογίας σε άτομα μπαίνοντας στον δημόσιο χώρο; Τι κανόνες ελέγχου πρέπει να εφαρμόζονται για το ποιες εικόνες μπορούν να αποθηκεύονται στη βάση δεδομένων και για πόσο καιρό μπορεί να παραμένουν εκεί; Τις εικόνες που αποκτάμε από το σύστημα μπορούμε να τις διατηρούμε, και, αν ναι, για πόσο καιρό;

Οι επικριτές και υποστηρικτές της ιδιωτικής ζωής εξέφρασαν τις ανησυχίες τους για την απάτη ταυτότητας καθώς επίσης αναφέρθηκαν και στη παραβίαση της ιδιωτικής ζωής, με βάση των δεδομένων διαφωνιών που υπάρχουν γύρω από την ηθική της αναγνώρισης προσώπου.

Το απόρρητο είναι μία από τις ανησυχίες του ευρύτερου κοινού, κυρίως λόγω της έλλειψης διαφάνειας στον τρόπο αποθήκευσης και διαχείρισης των πληροφοριών. Η αναγνώριση προσώπου παραβιάζει το εγγενές δικαίωμα των πολιτών να βρίσκονται υπό συνεχή κρατική επιτήρηση και να διατηρούν τις εικόνες τους χωρίς συγκατάθεση. Το 2020, η Ευρωπαϊκή Επιτροπή απαγόρευσε την τεχνολογία αναγνώρισης προσώπου [12] σε δημόσιους χώρους για έως και πέντε χρόνια για να κάνει αλλαγές στο νομικό τους πλαίσιο και να συμπεριλάβει κατευθυντήριες γραμμές για το απόρρητο και την ηθική κατάχρηση.

Οι ανησυχίες περί απορρήτου σχετικά με την αναγνώριση προσώπου σχετίζονται με μη ασφαλείς πρακτικές αποθήκευσης δεδομένων που θα μπορούσαν να εκθέσουν δεδομένα αναγνώρισης προσώπου και άλλες πιθανές απειλές για την ασφάλεια. Οι περισσότεροι οργανισμοί συνεχίζουν να φιλοξενούν τα δεδομένα των προσώπων τους σε τοπικούς

διακομιστές, οδηγώντας τα σε τρωτά σημεία ασφαλείας, καθώς επίσης παρατηρείται και η έλλειψη επαγγελματιών ασφάλειας IT για τη διασφάλιση της ασφάλειας του δικτύου.

Οι τεχνολογίες αναγνώρισης προσώπου μπορούν να εξασφαλίσουν τη μέγιστη ασφάλεια δεδομένων όταν φιλοξενούνται στο cloud. Ωστόσο, η ακεραιότητα των δεδομένων μπορεί να διασφαλιστεί μόνο μέσω κατάλληλης κρυπτογράφησης. Η ανάπτυξη προσωπικού κυβερνοασφάλειας πληροφορικής είναι απαραίτητη για τη σωστή αποθήκευση δεδομένων, παρέχοντας παράλληλα τον έλεγχο των καταναλωτών για τη βελτίωση της λογοδοσίας και την πρόληψη της κακόβουλης κυκλοφορίας.

5.5.1 Από τη πλευρά της βιομηχανίας…

Τα καταναλωτικά προϊόντα εξοπλισμένα με τεχνολογίες αναγνώρισης προσώπου είναι λιγότερο αμφιλεγόμενα, δεδομένης της επιλογής απενεργοποίησης ή μη χρήσης της δυνατότητας αυτής. Ωστόσο, οι εταιρείες καταναλωτικών αγαθών εξακολουθούν να είναι θύματα απαγορεύσεων λόγω της διάβρωσης της ιδιωτικής ζωής. Ωστόσο, συνεχίζουν να προσφέρουν προϊόντα με τεχνολογία προσώπου, προωθώντας τα ως προηγμένο χαρακτηριστικό ασφαλείας.

Η αποφασιστικότητα να ακολουθήσει κάποιος τη νόμιμη οδό είναι ανοιχτή σε συσκευές που οι εταιρίες επιτρέπουν στον κάτοχο να ζητήσει οικονομική αποζημίωση για την παραβίαση της ιδιωτικής ζωής. Για παράδειγμα, ο γίγαντας των μέσων κοινωνικής δικτύωσης **Facebook** διευθέτησε μια αγωγή 650 εκατομμυρίων δολαρίων στο Ιλινόις για τη συλλογή φωτογραφιών που δεν ήταν δημόσια διαθέσιμες για αναγνώριση προσώπου [13].

5.5.2 Από τη πλευρά της Κυβέρνησης…

Όταν χρησιμοποιείται παράλληλα με τις πανταχού παρούσες κάμερες και τις αναλύσεις δεδομένων, η αναγνώριση προσώπου οδηγεί σε μαζική παρακολούθηση που θα μπορούσε να θέσει σε κίνδυνο την ελευθερία και τα δικαιώματα των πολιτών. Ενώ η τεχνολογία αναγνώρισης προσώπου βοηθά τις κυβερνήσεις με την επιβολή του νόμου εντοπίζοντας εγκληματίες, θέτει επίσης σε κίνδυνο τα θεμελιώδη δικαιώματα της ιδιωτικής ζωής των απλών και αθώων ανθρώπων.

Πρόσφατα, η Ευρωπαϊκή Επιτροπή έλαβε μια ανοιχτή επιστολή από 51 οργανισμούς [17] που ζητούσαν την πλήρη απαγόρευση όλων των εργαλείων αναγνώρισης προσώπου για μαζική παρακολούθηση. Σε μια άλλη τροπή των γεγονότων, περισσότεροι από 43.000 Ευρωπαίοι πολίτες υπέγραψαν μια αναφορά **(**Reclaim Your Face) ζητώντας την απαγόρευση των πρακτικών βιομετρικής μαζικής επιτήρησης στην ΕΕ.

Η πρόσφατη σειρά γεγονότων έχει αμφισβητήσει την ηθική της τεχνολογίας αναγνώρισης προσώπου λόγω της απείθαρχης χρήσης της τεχνητής νοημοσύνης (AI) για χειραγώγηση και απειλή ανθρώπων, κυβερνητικών υπηρεσιών και συλλογικής δημοκρατίας. Η τεχνητή νοημοσύνη και η μηχανική μάθηση (ML) είναι τεχνολογίες που μπορούν να αξιοποιηθούν σε ασφαλείς τεχνολογίες αναγνώρισης προσώπου.

6 Τεχνητή νοημοσύνη και συστήματα αναγνώρισης προσώπου

6.1 Τι είναι η τεχνητή νοημοσύνη

Η τεχνητή νοημοσύνη (Artificial Intelligence – AI) είναι μια τεχνολογία που προσομοιώνει τις διαδικασίες της ανθρώπινης νοημοσύνης χρησιμοποιώντας μηχανές για τη λήψη γνωστικών αποφάσεων. Από την αναγνώριση προσώπων στην οθόνη κλειδώματος του κινητού μας μέχρι τα αυτοοδηγούμενα αυτοκίνητα, η τεχνητή νοημοσύνη απελευθέρωσε μια νέα σφαίρα μόχλευσης της τεχνολογίας.

Η τεχνητή νοημοσύνη είναι σε θέση να βοηθήσει τα συστήματα-μηχανές ώστε να κατανοήσουν καλύτερα το περιβάλλον τους. Επίσης είναι ικανή να τροφοδοτήσει με γνώσεις τα συστήματα αυτά ώστε να μπορούν να επιλύουν τα προβλήματα που μπορεί να εμφανιστούν και να δρουν προς την εύρεση της λύσης τους . Ο υπολογιστής δέχεται δεδομένα (ήδη έτοιμα ή συλλεγμένα μέσω αισθητήρων, π.χ. αισθητήρες απόστασης ,αισθητήρες θερμοκρασίας – υγρασίας ,αλλά και κάμερες), τα επεξεργάζεται και ανταποκρίνεται βάσει αυτών [26].

6.1.1 Πώς λειτουργεί η τεχνητή νοημοσύνη

Η τεχνητή νοημοσύνη χρησιμοποιεί ένα σύνολο μη δομημένων δεδομένων για να αναλύσει μοτίβα πληροφοριών χρησιμοποιώντας αλγορίθμους προκειμένου να συσχετίσει τις πληροφορίες για την παροχή αποτελεσμάτων. Έχοντας προγραμματιστεί να λαμβάνει γνωστικές αποφάσεις, η τεχνητή νοημοσύνη αυξάνει διάφορες μορφές αυτοματισμού αξιοποιώντας τα νευρωνικά δίκτυα, τη μηχανική μάθηση και τη βαθιά μάθηση για να καταλήξει σε μια απόφαση [10].

6.1.2 Πού χρησιμοποιείται η τεχνητή νοημοσύνη

Η Τεχνητή Νοημοσύνη είναι αναπόσπαστο μέρος διαφόρων εφαρμογών και λογισμικού SAS. Μερικές από τις ευρέως χρησιμοποιούμενες εφαρμογές περιλαμβάνουν την αναγνώριση εικόνας, την αναγνώριση ομιλίας, τη δημιουργία φυσικής γλώσσας, την

ανάλυση συναισθημάτων και τα chatbots (διαλογικό ρομπότ-πράκτορας). Η τεχνητή νοημοσύνη προσφέρει μια σειρά από χαρακτηριστικά που φαίνονται πολλά υποσχόμενα για τα προϊόντα του αύριο. Η τεχνητή νοημοσύνη μπορεί να αυτοματοποιήσει συχνές εργασίες μεγάλου όγκου μαθαίνοντας και ανακαλύπτοντας μέσω αξιοποίησης δεδομένων. Δεύτερον, προσθέτει ευφυΐα σε προϊόντα των τομέων του αυτοματισμού, των πλατφόρμων συνομιλίας, των έξυπνων μηχανών και των bots. Τρίτον, είναι σε θέση να αυτοεκπαιδεύεται μέσω αλγορίθμων. Στη συνέχεια, η τεχνητή νοημοσύνη εκτελεί μια βαθιά κατάδυση στο σύνολο των δεδομένων για να διευκολύνει τη λειτουργία πολύπλοκων ΄΄ενεργειών΄΄, όπως συστήματα ανίχνευσης απάτης. Επιπλέον, η τεχνητή νοημοσύνη χρησιμοποιεί βαθιά μάθηση για να εξασφαλίσει απίστευτη ακρίβεια αναλύοντας σταδιακά τις εισροές. Τέλος, βοηθά στη δημιουργία εσόδων από δεδομένα για τις επιχειρήσεις προκειμένου να παραμείνουν μπροστά από την καμπύλη ζήτησης [18].

6.2 Τα πλεονεκτήματα και τα μειονεκτήματα που φέρνει η τεχνητή νοημοσύνη για τον άνθρωπο.

6.2.1 Τα πλεονεκτήματα

- **Ελαχιστοποιεί την πιθανότητα σφάλματος**: Σχεδόν πλήρως, τα συστήματα τεχνητής νοημοσύνης εξαλείφουν την πιθανότητα σφάλματος, επειδή λειτουργούν με μεγαλύτερη ακρίβεια, κατά την επεξεργασία και τη σύγκριση μεγάλων όγκων μεταβλητών και δεδομένων.
- **Απλοποιεί την καθημερινή ζωή** : Ανιχνεύει και προβλέπει ανάγκες και γούστα των χρηστών.
- **Εκτελεί επαναλαμβανόμενες εργασίες που απαιτούν μεγάλο αριθμό πόρων και χρόνου**: Αύξηση αποτελεσματικότητας και καλύτερη λήψη αποφάσεων χωρίς τη παράμετρο των συναισθημάτων.
- **Αντικαθιστά τον άνθρωπο σε επίπονες εργασίες**: Με αυτή την ικανότητα, οι άνθρωποι θα μπορούν να επικεντρώνονται σε εργασίες που απαιτούν μεγαλύτερη ευθύνη.

- **Πρόοδος στην ιατρική**: Καλύτερη και ταχύτερη διάγνωση. Με τον όρο καλύτερη εννοούμε την ακρίβεια που προσφέρει η οποία είναι σημαντική και στην εφαρμογή των επεμβάσεων.
- **Αναλαμβάνει επικίνδυνες και πολύπλοκες εργασίες** : Σημαντικό εργαλείο για εργασίες που απαιτείται υπέρβαση των ανθρώπινων δυνατοτήτων.
- **Διαχειρίζεται και αναλύει δεδομένα σε ευαίσθητους τομείς** : έχει την ικανότητα να εντοπίζει απάτες και ανωμαλίες, καθώς και να οργανώνει το κεφάλαιο με τον καλύτερο τρόπο.
- **Δεν απαιτούν διαλείμματα**: Είναι μηχανές και δε χρειάζονται τροφή, ξεκούραση ή ανάπαυση ,έχουν σχεδιαστεί για να λειτουργούν μόνιμα.

(πηγή: https://www.informatique-mania.com/el/linformatique/intelligence-artificielle/)

6.2.2 Τα μειονεκτήματα

Όμως , οι εφαρμογές τεχνητής νοημοσύνης εχουν επίσης και κάποια αρνητικά αντίκτυπα στις ζωές των ανθρώπων. Παρακάτω αναφέρονται τα πιο σημαντικά από αυτα:

- **Υψηλό κόστος**: Όπως είναι φυσιολογικό μια τέτοια τεχνολογία με τόσες πολύπλοκες δυνατότητες θα είναι πολύ δαπανηρή.
- **Αύξηση ανεργίας** : Μπορεί να οδηγήσει στην αντικατάσταση των ανθρώπων με μηχανήματα.
- **Περιορισμένη προσαρμοστικότητα** : Οι μηχανές τεχνητής νοημοσύνης δεν είναι αποτελεσματικές στο να αντιμετωπίζουνε νέες καταστάσεις μονές τους εάν δεν υπάρχει τροποποίηση των λειτουργιών των μηχανών από τον άνθρωπο.
- **Έλλειψη δημιουργικότητας**: Δεν είναι ικανή να δημιουργήσει πρωτότυπες ιδέες.
- **Δεν βελτιώνεται με την εμπειρία**: Δεν εξελίσσεται όπως ο άνθρωπος όταν αποκτά εμπειρία πάνω σε ένα αντικείμενο.
- **Ευθύνη** : Η ευθύνη για τη σχεδίαση και την εφαρμογή της AI πιστώνεται στον άνθρωπο. Καθώς επίσης και οι κίνδυνοι που μπορεί να εμφανιστούν πιστώνονται στον άνθρωπο[24]. **(**πηγή: https://www.informatique-mania.com/el/linformatique/intelligence-artificielle/)

6.3 Τεχνητή νοημοσύνη και προστασία της ιδιωτικότητας

Μία από τις κύριες ανησυχίες σχετικά με την τεχνολογία αναγνώρισης προσώπου είναι η πιθανότητα μεροληψίας και διακρίσεων. Οι αλγόριθμοι αναγνώρισης προσώπου είναι τόσο ακριβείς και τόσο καλοί όσο και τα δεδομένα στα οποία εκπαιδεύονται. Εάν τα δεδομένα εκπαίδευσης είναι μεροληπτικά ή ελλιπή, ο αλγόριθμος θα αντανακλά αυτή την προκατάληψη, οδηγώντας σε ανακριβή ή μεροληπτικά αποτελέσματα. Αυτό έχει οδηγήσει σε εκκλήσεις για μεγαλύτερη διαφάνεια και εποπτεία στη χρήση της τεχνολογίας αναγνώρισης προσώπου.

Η τεχνητή νοημοσύνη έχει τη δυνατότητα να αντιμετωπίσει ορισμένα από τα ζητήματα που σχετίζονται με την τεχνολογία αναγνώρισης προσώπου. Οι αλγόριθμοι τεχνητής νοημοσύνης μπορούν να χρησιμοποιηθούν για τη βελτίωση της ακρίβειας και της αξιοπιστίας των συστημάτων αναγνώρισης προσώπου, ελαχιστοποιώντας παράλληλα το ενδεχόμενο μεροληψίας και διακρίσεων. Για παράδειγμα, η τεχνητή νοημοσύνη μπορεί να χρησιμοποιηθεί για τον εντοπισμό και τη διόρθωση των προκαταλήψεων στα δεδομένα εκπαίδευσης ή για τη βελτίωση της ακρίβειας της αναγνώρισης προσώπου σε εικόνες με χαμηλό φωτισμό ή χαμηλή ανάλυση.

Η τεχνητή νοημοσύνη έχει αλλάξει τα δεδομένα σε πολλούς κλάδους, από την υγειονομική περίθαλψη έως τη χρηματοδότηση, το μάρκετινγκ και πολλά άλλα. Ωστόσο, καθώς η τεχνολογία AI συνεχίζει να εξελίσσεται, η ένταση μεταξύ της AI και της προστασίας της ιδιωτικής ζωής έχει γίνει πιο εμφανής. Τα συστήματα AI βασίζονται σε τεράστιες ποσότητες δεδομένων για να λειτουργήσουν αποτελεσματικά και, ως εκ τούτου, συλλέγουν και επεξεργάζονται ευαίσθητες προσωπικές πληροφορίες, όπως δεδομένα υγείας, οικονομικές πληροφορίες και βιομετρικά δεδομένα. Αυτό εγείρει ανησυχίες σχετικά με το ενδεχόμενο παραβίασης της ιδιωτικής ζωής, παραβίασης δεδομένων και μη εξουσιοδοτημένης χρήσης προσωπικών πληροφοριών.

Η ένταση μεταξύ της AI και της προστασίας της ιδιωτικής ζωής επιδεινώνεται περαιτέρω από το γεγονός ότι τα συστήματα AI μπορούν να λαμβάνουν αποφάσεις με βάση δεδομένα που είναι μεροληπτικά ή ελλιπή. Αυτό θα μπορούσε να οδηγήσει σε διακρίσεις ή αποκλεισμό ορισμένων ομάδων ή ατόμων, γεγονός που αποτελεί παραβίαση των δικαιωμάτων τους στην ιδιωτική ζωή. Επιπλέον, η χρήση της AI σε εφαρμογές επιτήρησης και ασφάλειας, όπως η τεχνολογία αναγνώρισης προσώπου, εγείρει ανησυχίες για κυβερνητική ή εταιρική υπερβολή και πιθανή κατάχρηση εξουσίας.

Γι΄ αυτούς τους λόγους, υπάρχει μεγάλη ανάγκη για την ανάπτυξη ρυθμιστικών πλαισίων και δεοντολογικών κατευθυντήριων γραμμών που να διασφαλίζουν την υπεύθυνη χρήση της AI, προστατεύοντας παράλληλα τα δικαιώματα ιδιωτικότητας των ατόμων. Αυτό απαιτεί τη συνεργασία μεταξύ των φορέων χάραξης πολιτικής, των εταιρειών τεχνολογίας και της κοινωνίας των πολιτών για την επίτευξη της σωστής ισορροπίας μεταξύ της καινοτομίας και της προστασίας της ιδιωτικής ζωής. Το μέλλον της τεχνητής νοημοσύνης θα εξαρτηθεί από το πόσο καλά μπορούμε να αντιμετωπίσουμε αυτά τα πολύπλοκα ζητήματα και πώς μπορούμε να διασφαλίσουμε ότι τα οφέλη της τεχνητής νοημοσύνης θα αξιοποιηθούν χωρίς να διακυβεύονται η ιδιωτική ζωή των ατόμων και οι ατομικές ελευθερίες [24].

6.4 Πώς λειτουργεί η αναγνώριση προσώπου σε συνδυασμό με την τεχνητή νοημοσύνη

Ο βασικός τρόπος με τον οποίο λειτουργεί η τεχνητή νοημοσύνη στην αναγνώριση προσώπου είναι ότι ξεκινάει με ένα σύνολο χαρακτηριστικών με ΄΄ετικέτα΄΄. Ουσιαστικά, τα συστήματα αυτά ξεκινάνε με φωτογραφίες που έχουν υπάρχουσες, ταιριαστές συσχετίσεις με τα άτομα που εμπλέκονται. Πρέπει να υπάρχει μια αρχική, χειρωνακτική συσχέτιση μεταξύ του προσώπου ενός ατόμου και της υπόλοιπης ταυτότητάς του. Μόλις ξεκινήσει αυτό, γίνεται σταθερά πιο εύκολο να αναγνωριστούν πρόσωπα σε φωτογραφίες ανθρώπων «στην άγρια φύση» – ας πούμε έτσι, στις οποίες οι εικόνες που δεν είναι τόσο καθαρές αντιστοιχίζονται σε αυτό το σύνολο δεδομένων.

Και πώς ακριβώς μπορεί το AI να αναγνωρίσει πρόσωπα; Το πρόσωπο κάθε ατόμου χωρίζεται σε πολλά σημεία δεδομένων. Αυτά μπορεί να είναι η απόσταση μεταξύ των ματιών, το ύψος των ζυγωματικών, η απόσταση μεταξύ των ματιών και του στόματος, και ούτω καθεξής. Η αναγνώριση προσώπου AI αναζητά σε αυτά τα σημεία δεδομένων και προσπαθεί να λάβει υπόψη τις παραλλαγές (για παράδειγμα, απόσταση από την κάμερα και μικρές διακυμάνσεις στη γωνία του προσώπου).

Ωστόσο, ακόμη και τα καλά εκπαιδευμένα συστήματα αναγνώρισης προσώπου με τεχνητή νοημοσύνη δεν έχουν πραγματικό περιβάλλον και μπορούν να εξαπατηθούν. Αν κάποιος άνθρωπος δει έναν συνάδελφο που φοράει μάσκα προσώπου, γυαλιά ηλίου και καπέλο του μπέιζμπολ, μπορεί να τον αναγνωρίσει. Ένα σύστημα AI, ωστόσο, μπορεί να μην τα καταφέρει. Εξαρτάται από το επίπεδο εκπαίδευσης του νευρωνικού

δικτύου. Παρόλο που τα συστήματα αναγνώρισης προσώπου με τεχνητή νοημοσύνη είναι πιο επιφανειακά ακριβή, είναι επίσης πιο εύκολο για αυτά να κάνουν λάθος σε λιγότερο από ιδανικές συνθήκες.

	Τεχνητή Νοημοσύνη	***Ανθρώπινη νοημοσύνη***
Εμφάνιση	Η τεχνητή νοημοσύνη είναι μια πρόοδος που έγινε από τις ανθρώπινες ιδέες.	Από την άλλη πλευρά, τα ανθρώπινα πλάσματα είναι φτιαγμένα με την εγγενή ικανότητα να σκέφτονται, να συλλογίζονται, να αναθεωρούν κ.λπ.
Ρυθμός τεχνητής και ανθρώπινης νοημοσύνης	Σε σύγκριση με τους ανθρώπους, οι υπολογιστές μπορούν να χειριστούν περισσότερα δεδομένα με ταχύτερο ρυθμό. Στην περίπτωση που η ανθρώπινη διάνοια μπορεί να λύσει ένα μαθηματικό πρόβλημα σε 5 λεπτά, η τεχνητή νοημοσύνη μπορεί να λύσει 10 προβλήματα σε ένα λεπτό.	Όσον αφορά την ταχύτητα, ο άνθρωπος δεν μπορεί να νικήσει την ταχύτητα της τεχνητής νοημοσύνης ή των μηχανών.
Λήψη απόφασης	Η τεχνητή νοημοσύνη είναι βαθιά αντικειμενική στη λήψη επιλογών, επειδή αναλύει με βάση απολύτως συσσωρευμένα δεδομένα.	Οι επιλογές του ανθρώπου μπορεί να επηρεαστούν από υποκειμενικά στοιχεία που δεν βασίζονται μόνο σε αριθμούς.
Τελειότητα	Η τεχνητή νοημοσύνη συχνά παράγει ακριβή αποτελέσματα επειδή έχει ικανότητες με βάση ένα σύνολο τροποποιημένων κανόνων.	Για τις ανθρώπινες ιδέες, τις περισσότερες φορές υπάρχει χώρος για «ανθρώπινο λάθος», καθώς ορισμένα λεπτά στοιχεία μπορεί να παραλείπονται σε ένα σημείο .
Ευστροφία	Η τεχνητή νοημοσύνη μπορεί να εκτελεί εργασίες στον ίδιο χρόνο που ένα framework μπορεί να μαθαίνει μια εργασία τη φορά που του αναθέτουν	Οι δεξιότητες της ανθρώπινης κρίσης στηρίζουν το multitasking όπως αποδεικνύεται από διαφορετικούς και ταυτόχρονους ρόλους.
Τροποποίηση AI(τεχνητής	Η τεχνητή νοημοσύνη χρειάζεται πολύ περισσότερο χρόνο για να προσαρμοστεί στις νέες και ξένες αλλαγές.	Οι ανθρώπινες γνώσεις μπορούν να προσαρμόζονται ως αντίδραση στις αλλαγές στο περιβάλλον τους. Αυτό κάνει τα άτομα να μπορούν

νοημοσύνης) και Ανθρώπου		να απομνημονεύουν και να αποκτούν διαφορετικές δεξιότητες.
Κοινωνική δικτύωση	Η τεχνητή νοημοσύνη δεν έχει αποκτήσει την ικανότητα να επιλέξει σχετικά κοινωνικά και ενθουσιώδη στοιχεία.	Από την άλλη πλευρά, ως κοινωνικά πλάσματα, οι άνθρωποι είναι πολύ καλύτεροι στην κοινωνική αλληλεπίδραση, καθώς μπορούν να προετοιμάσουν θεωρητικά δεδομένα, να έχουν αυτογνωσία και να είναι ευαίσθητοι στα συναισθήματα των άλλων.

Πίνακας 2:Διαφορά μεταξύ τεχνητής νοημοσύνης και ανθρώπινης νοημοσύνης

6.5 Πού χρησιμοποιείται σήμερα η αναγνώριση προσώπου με τεχνητή νοημοσύνη

Η τεχνητή νοημοσύνη αναγνώρισης προσώπου εφαρμόζεται σε πολλές βιομηχανίες στις μέρες μας. Για παράδειγμα:

- Φροντίδα υγείας. Τα συστήματα αναγνώρισης προσώπου συνδυάζονται με την τεχνητή νοημοσύνη για την υποστήριξη των διαδικασιών διαχείρισης του πόνου και την παρακολούθηση της κατανάλωσης φαρμάκων από τον ασθενή.
- Ασφάλεια. Οι αλγόριθμοι βαθιάς μάθησης συμβάλλουν στη μείωση της ανάγκης για κανονικούς κωδικούς πρόσβασης σε κινητές συσκευές, στην αναγνώριση της ανίχνευσης απάτης και στη βελτίωση των δυνατοτήτων κατά της πλαστογράφησης.
- Επιβίβαση στο αεροδρόμιο: Κάθε χρόνο, πάνω από 100.000.000 άτομα περνούν από τα αεροδρόμια Orly και Charles de Gaulle του Παρισιού. Για να επιταχυνθούν τα πράγματα, τα αεροδρόμια άρχισαν να χρησιμοποιούν «έξυπνες πύλες», οι οποίες χρησιμοποιούν έναν συνδυασμό ελέγχων αναγνώρισης προσώπου και κινήσεων.
- Proctoring: Ορισμένες υπηρεσίες proctor χρησιμοποιούν λύσεις τεχνητής νοημοσύνης για τον εντοπισμό και την τεκμηρίωση ύποπτης συμπεριφοράς μέσω της παρακολούθησης κάμερας web. Οι ζωντανοί επόπτες μπορούν στη συνέχεια να αναλύσουν και να προσαρμόσουν αυτά τα γεγονότα [24].

6.6 Τεχνητή νοημοσύνη, συστήματα αναγνώρισης προσώπου και εφαρμογές

6.6.1 Μάρκετινγκ

Η τεχνητή νοημοσύνη και τα συστήματα αναγνώρισης προσώπου έχουν σημαντική σχέση με το μάρκετινγκ, καθώς προσφέρουν πολλές ευκαιρίες και εφαρμογές για τη εξέλιξη των στρατηγικών μάρκετινγκ και την παροχή προσαρμοσμένων εμπειριών στους καταναλωτές. Ας εξετάσουμε κάποιους τρόπους με τους οποίους συνδέονται η ΤΝ και η αναγνώριση προσώπου με το μάρκετινγκ:

Αναγνώριση προσώπου για αναγνώριση πελατών: Οι εταιρείες μπορούν να χρησιμοποιήσουν συστήματα αναγνώρισης προσώπου για να αναγνωρίζουν τους πελάτες τους και να παρέχουν εξατομικευμένες υπηρεσίες. Με τη χρήση της τεχνητής νοημοσύνης, μπορούν να συλλέγονται και να αναλύονται δεδομένα για τις προτιμήσεις, τις συνήθειες και τις ανάγκες των πελατών, προσφέροντας ένα εξατομικευμένο και προσαρμοσμένο πελατειακό περιβάλλον.

Διαφήμιση και προώθηση προϊόντων: Η ΤΝ μπορεί να χρησιμοποιηθεί για την ανάλυση μεγάλων όγκων δεδομένων πελατών και την αναγνώριση προτύπων αγοραστικής συμπεριφοράς. Αυτό μπορεί να βοηθήσει τις εταιρείες να προβλέψουν τις ανάγκες των πελατών τους, να προσφέρουν εξατομικευμένες προσφορές και να προωθήσουν τα προϊόντα τους με πιο αποτελεσματικό τρόπο.

Βελτιστοποίηση επικοινωνίας και εξυπηρέτησης πελατών: Η ΤΝ μπορεί να χρησιμοποιηθεί για την ανάπτυξη ευφυών συστημάτων εξυπηρέτησης πελατών, όπως οι εικονικοί βοηθοί ή τα chatbots. Αυτά τα συστήματα μπορούν να αναγνωρίζουν τον λόγο και την απόδοση των πελατών, να απαντούν σε ερωτήσεις και αιτήματα, και να παρέχουν προσαρμοσμένη εξυπηρέτηση.

Ανάλυση συναισθημάτων: Με τη χρήση της ΤΝ είναι δυνατή η ανάλυση συναισθημάτων από φωτογραφίες και βίντεο. Αυτό μπορεί να χρησιμοποιηθεί για να κατανοήσουμε τις αντιδράσεις των πελατών σε προϊόντα, διαφημίσεις ή καταστάσεις. Η ανάλυση των συναισθημάτων μπορεί να βοηθήσει τις εταιρείες να προσαρμόσουν τις στρατηγικές τους στις ανάγκες και τις προτιμήσεις των πελατών.

Αυτοί είναι μερικοί τρόποι με τους οποίους η τεχνητή νοημοσύνη και τα συστήματα αναγνώρισης προσώπου σχετίζονται με το μάρκετινγκ. Μπορούν να δημιουργήσουν προηγμένες εμπειρίες για τους καταναλωτές, να βελτιστοποιήσουν τις στρατηγικές

προώθησης και να προσφέρουν εξατομικευμένη εξυπηρέτηση, βοηθώντας έτσι τις εταιρείες να επιτύχουν τους στόχους τους στον τομέα του μάρκετινγκ [23].

6.6.2 Διάφορες εφαρμογές

Εκτός από το μάρκετινγκ, η τεχνητή νοημοσύνη και τα συστήματα αναγνώρισης προσώπου έχουν εφαρμογές και σε πολλούς άλλους τομείς. Ορισμένα παραδείγματα είναι:

1. Φροντίδα υγείας: Η τεχνητή νοημοσύνη και η αναγνώριση προσώπου χρησιμοποιούνται για την ανίχνευση και την παρακολούθηση ιατρικών καταστάσεων. Μπορούν να αναγνωρίσουν συμπτώματα ασθενειών στο πρόσωπο, να παρακολουθούν τον καρδιακό ρυθμό, τον παλμό και την κατάσταση του δέρματος, και να προσφέρουν εξατομικευμένη φροντίδα υγείας.
2. Παραγωγή και ρομποτική: Η τεχνητή νοημοσύνη και η αναγνώριση προσώπου χρησιμοποιούνται για την αυτοματοποίηση και τη βελτιστοποίηση της παραγωγής. Μπορούν να εντοπίζουν ανωμαλίες στην παραγωγική γραμμή, να διαχειρίζονται τον εφοδιασμό και την αποθήκευση, και να συνεργάζονται με ανθρώπους σε ασφαλή περιβάλλοντα.
3. Ασφάλεια και πρόληψη εγκλήματος: Οι τεχνολογίες αναγνώρισης προσώπου μπορούν να συνδυαστούν με την τεχνητή νοημοσύνη για την ενίσχυση της ασφάλειας και την πρόληψη του εγκλήματος. Αυτό μπορεί να εφαρμοστεί σε δημόσιους χώρους, όπως αεροδρόμια ή σταθμούς μετρό, για την ανίχνευση ανεπιθύμητων προσώπων ή την αναγνώριση εγκληματιών.
4. Προσωπική ασφάλεια και παρακολούθηση: Η τεχνητή νοημοσύνη και η αναγνώριση προσώπου μπορούν να χρησιμοποιηθούν για την παρακολούθηση και την ασφάλεια των ατόμων. Για παράδειγμα, συστήματα επιτήρησης μπορούν να αναγνωρίζουν τα πρόσωπα των ατόμων σε σπίτια ή επιχειρήσεις και να ειδοποιούν σε περίπτωση ύποπτων δραστηριοτήτων.
5. Επεξεργασία γλώσσας και αυτόματη απόκριση: Η τεχνητή νοημοσύνη και η αναγνώριση προσώπου μπορούν να χρησιμοποιηθούν για την επεξεργασία γλώσσας και την αυτόματη απόκριση. Αυτό μπορεί να εφαρμοστεί σε εικονικούς βοηθούς (chatbots) ή σε τηλεφωνικά συστήματα εξυπηρέτησης πελατών, όπου η αναγνώριση προσώπου μπορεί να βοηθήσει στην αυθεντικοποίηση των χρηστών και στην προσαρμογή των απαντήσεων στις ανάγκες τους.

6.7 Πώς εκπαιδεύεται η τεχνητή νοημοσύνη για τα συστήματα αναγνώρισης προσώπου

Η αναγνώριση προσώπου με τεχνητή νοημοσύνη πρέπει να εξασκηθεί σε μη αυτόματα επιλεγμένα σετ φωτογραφιών (δηλαδή πολλές φωτογραφίες από το ίδιο πρόσωπο, αλλά κάθε φωτογραφία από άλλη γωνιά λήψης, με άλλο φωτισμό, με επιλεγμένα σημεία του προσώπου να φαίνονται κ.λπ.). Ορισμένες εταιρείες το κάνουν πιο εύκολο για τους προγραμματιστές AI παρέχοντας δεδομένα εκπαίδευσης για συστήματα αναγνώρισης προσώπου. Τα μοντέλα αναγνώρισης προσώπου βλέπουν πολλούς υπολογισμούς αντί για ανθρώπινο πρόσωπο.

Για λόγους ασφαλείας και επιτήρησης, ένα μοντέλο μπορεί να συγκρίνει αυτούς τους υπολογισμούς με άλλους υπολογισμούς προσώπου που βρίσκονται σε μια βάση δεδομένων. Ωστόσο, ανεξάρτητα από την περίπτωση χρήσης, κάθε σύστημα αναγνώρισης προσώπου AI πρέπει να εκπαιδεύεται με πολλά δεδομένα εικόνας προσώπου. Τα μοντέλα τεχνητής νοημοσύνης πρέπει να εκπαιδεύονται με εικόνες προσώπου που ποικίλλουν ως προς την εθνικότητα, την ηλικία, τις γωνίες, τον φωτισμό και άλλους παράγοντες.

Μερικές φορές, για να δημιουργήσουν τα εκπαιδευτικά τους σύνολα δεδομένων, οι εταιρείες αναγνώρισης προσώπου παίρνουν δεδομένα από τον ανοιχτό ιστό, δηλαδή από τους δημόσιους δρόμους και τις κάμερες κυκλοφορίας, για να συγκεντρώσουν φωτογραφίες ατόμων χωρίς συναίνεση. Αυτό είναι εξαιρετικά αμφιλεγόμενο και η ηθική του τίθεται υπό αμφισβήτηση [20].

6.7.1 Βασικές διαδικασίες για την εκπαίδευση της τεχνητής νοημοσύνης για τα συστήματα αναγνώρισης προσώπου.

1) Συλλογή δεδομένων: Αρχικά, συλλέγονται μεγάλες ποσότητες δεδομένων που περιλαμβάνουν εικόνες προσώπων. Αυτές οι εικόνες μπορούν να προέρχονται από δημόσια σύνολα δεδομένων ή να συλλέγονται από συστήματα αναγνώρισης προσώπου σε πραγματικό χρόνο.

2) Προεπεξεργασία δεδομένων: Τα δεδομένα τυγχάνουν επεξεργασίας για να είναι κατάλληλα για την εκπαίδευση του μοντέλου. Αυτή η διαδικασία περιλαμβάνει την κανονικοποίηση των εικόνων, την ανίχνευση και την εξαγωγή των προσώπων από τις εικόνες, και την απομάκρυνση τυχόν παρεμβολών ή θορύβου.

3) Κατασκευή μοντέλου: Έπειτα, δημιουργείται ένα μοντέλο τεχνητής νοημοσύνης, συνήθως βασισμένο σε βαθιά νευρωνικά δίκτυα, το οποίο θα μάθει να αναγνωρίζει τα πρόσωπα από τα δεδομένα εκπαίδευσης. Αυτό το μοντέλο εκπαιδεύεται με τη χρήση των επεξεργασμένων δεδομένων και μεθόδων μάθησης, όπως η υπερεκπαίδευση (overfitting) ή η μάθηση με επίβλεψη.

4) Αξιολόγηση και βελτίωση: Το μοντέλο αξιολογείται χρησιμοποιώντας ένα σύνολο αξιολόγησης για να εκτιμηθεί η ακρίβειά του. Αν απαιτείται, πραγματοποιούνται βελτιστοποιήσεις στο μοντέλο μέσω της προσαρμογής των υπερπαραμέτρων, της επιπλέον εκπαίδευσης ή της χρήσης νέων δεδομένων.

Η διαδικασία εκπαίδευσης της τεχνητής νοημοσύνης για τα συστήματα αναγνώρισης προσώπου είναι επαναληπτική, και η ποιότητα των δεδομένων και η αποτελεσματικότητα της διαδικασίας επεξεργασίας δεδομένων έχουν σημαντική επίδραση στην απόδοση του συστήματος αναγνώρισης προσώπου [21] [22].

6.8 Το πρόβλημα με την αναγνώριση προσώπου, με τεχνητή νοημοσύνη

Υπάρχουν πολλές αμφισβητούμενες ηθικές αρχές που σχετίζονται με την ανάπτυξη της αναγνώρισης προσώπου AI (μέχρι το 2021 τουλάχιστον όπου υπάρχουν οι έρευνες και μελέτες με βάση τη συγγραφή αυτού του άρθρου). Για παράδειγμα, ερευνητές στο Πανεπιστήμιο Harrisburg της Pennsylvania ανέπτυξαν λογισμικό αναγνώρισης προσώπου με τεχνητή νοημοσύνη που, σύμφωνα με τα λεγόμενα τους, μπορούσε να προβλέψει εάν κάποιος επρόκειτο να γίνει εγκληματίας με ακρίβεια 80%. Υπήρξε ένα κύμα αρνητικών αντιδράσεων και το Πανεπιστήμιο κατέληξε να αφαιρέσει το δελτίο τύπου του για το θέμα αυτό και να μην δημοσιεύσει το έργο.

Ένα άλλο σημαντικό σημείο είναι η συλλογή δεδομένων χωρίς συναίνεση. Μέχρι τις αρχές της δεκαετίας του 2000, οι προγραμματιστές AI συνήθως έπαιρναν εθελοντές για να ποζάρουν για δεδομένα εκπαίδευσης. Σήμερα, όμως, η πλειονότητα των εικόνων των προσώπων συλλέγονται χωρίς άδεια. Για παράδειγμα, το 2016, ερευνητές από το Πανεπιστήμιο της Ουάσιγκτον του Σιάτλ δημοσίευσαν μια βάση δεδομένων που περιείχε 3,3 εκατομμύρια φωτογραφίες προσώπων που συλλέχθηκαν από το Flickr (είναι μια αμερικανική διαδικτυακή εφαρμογή διαχείρισης και κοινής χρήσης φωτογραφιών

στον κόσμο) χωρίς συγκατάθεση. Επί του παρόντος, δεν υπάρχουν σαφείς νομικές διασφαλίσεις σχετικά με τη συλλογή δεδομένων εκπαίδευσης για την αναγνώριση προσώπου, αλλά πρόσφατα, το Facebook κατέβαλε διακανονισμό 650 εκατομμυρίων δολαρίων για τη συλλογή δεδομένων προσώπου [8].

6.9 Μέτρα που πρέπει να λαμβάνονται για τη προστασία της ιδιωτικότητας από την εφαρμογή συστημάτων αναγνώρισης προσώπου με τη χρήση AI.

Η προστασία της ιδιωτικής ζωής κατά τη χρήση συστημάτων προσωπικής ταυτοποίησης που λειτουργούν με τεχνητή νοημοσύνη είναι ζωτικής σημασίας. Ακολουθούν ορισμένα μέτρα που οι άνθρωποι μπορούν να λάβουν για την προστασία της ιδιωτικής τους ζωής:

- Ελαχιστοποίηση των δεδομένων: ελαχιστοποιείται η συλλογή και η αποθήκευση προσωπικών δεδομένων σε ό,τι είναι απαραίτητο για τη διαδικασία ταυτοποίησης. Αποφεύγετε την αποθήκευση ευαίσθητων πληροφοριών που δεν σχετίζονται άμεσα με τον σκοπό του συστήματος.
- Συναίνεση μετά από ενημέρωση: διασφαλίζεται ότι τα άτομα είναι πλήρως ενημερωμένα σχετικά με τον σκοπό, το πεδίο εφαρμογής και τους πιθανούς κινδύνους που συνδέονται με το σύστημα προσωπικής ταυτοποίησης. Λαμβάνετε η ρητή συγκατάθεση των χρηστών πριν από τη συλλογή και επεξεργασία των προσωπικών τους δεδομένων.
- Ανωνυμοποίηση και ψευδωνυμοποίηση: Εφαρμόζονται τεχνικές όπως η ανωνυμοποίηση και η ψευδωνυμοποίηση για την προστασία των προσωπικών δεδομένων. Η ανωνυμοποίηση αφαιρεί τις προσωπικά αναγνωρίσιμες πληροφορίες, ενώ η ψευδωνυμοποίηση αντικαθιστά τα αναγνωρίσιμα δεδομένα με τεχνητά αναγνωριστικά στοιχεία για τη μείωση του κινδύνου εκ νέου ταυτοποίησης.
- Ισχυρά μέτρα ασφαλείας: Εφαρμόζονται ισχυρά μέτρα ασφαλείας για την προστασία των δεδομένων του συστήματος προσωπικής ταυτοποίησης από μη εξουσιοδοτημένη πρόσβαση, συμπεριλαμβανομένης της κρυπτογράφησης, της ασφαλούς αποθήκευσης και των τακτικών ελέγχων ασφαλείας. Ακολουθούνται

τις βέλτιστες πρακτικές για ασφαλή κωδικοποίηση και αρχιτεκτονική του συστήματος.

- Περιορισμός σκοπού: Διασφάλιση ότι τα προσωπικά δεδομένα που συλλέγονται για σκοπούς ταυτοποίησης χρησιμοποιούνται μόνο για τον προβλεπόμενο σκοπό και δεν κοινοποιούνται ή επαναχρησιμοποιούνται χωρίς τη ρητή συγκατάθεση των ατόμων.
- Διαφάνεια και επεξηγηματική δύναμη: Σχεδιάζονται συστήματα προσωπικής ταυτοποίησης που είναι διαφανή και επεξηγήσιμα. Οι χρήστες θα πρέπει να κατανοούν σαφώς τον τρόπο επεξεργασίας των δεδομένων τους, τους εμπλεκόμενους αλγορίθμους και τις πιθανές επιπτώσεις στην ιδιωτική τους ζωή.
- Έλεγχος των χρηστών και δικαιώματα πρόσβασης. Να τους επιτρέπετε να έχουν πρόσβαση, να αναθεωρούν, να διορθώνουν και να διαγράφουν τις πληροφορίες τους, ανάλογα με τις ανάγκες. Εφαρμογή φιλικών προς τον χρήστη ρυθμίσεων και προτιμήσεων απορρήτου.
- Τακτικοί έλεγχοι δεδομένων: Διενέργεια τακτικών ελέγχων για τον έλεγχο και την αξιολόγηση των δεδομένων που είναι αποθηκευμένα στο σύστημα προσωπικής ταυτοποίησης. Αφαιρούνται τα περιττά ή ξεπερασμένα δεδομένα για να ελαχιστοποιούνται οι κίνδυνοι της προστασίας της ιδιωτικής ζωής.
- Προστασία της ιδιωτικής ζωής μέσω του σχεδιασμού: Ενσωματώνονται από την αρχή οι εκτιμήσεις για την προστασία της ιδιωτικής ζωής στο σχεδιασμό και της ανάπτυξης των συστημάτων προσωπικής ταυτοποίησης. Ακολουθούνται οι αρχές της προστασίας της ιδιωτικής ζωής μέσω σχεδιασμού για να διασφαλίζεται ότι η προστασία της ιδιωτικής ζωής αποτελεί αναπόσπαστο μέρος της αρχιτεκτονικής και της λειτουργικότητας του συστήματος [19].

6.10 Περί νομοθεσιών της ευρωπαϊκής ένωσης για τη χρήση της τεχνητής νοημοσύνης

Η ευρωπαϊκή ένωση έχει εγκαθιδρύσει από τη μεριά της ένα σύνολο από νόμους και κανόνες όπου στοχεύον στη προστασία των δικαιωμάτων και των προσωπικών δεδομενων των ανθρώπων από τη χρήση των συστημάτων τεχνητής νοημοσύνης .

Συγκεκριμένα η ΕΕ έχει χωρίσει τους νόμους των συστημάτων τεχνητής νοημοσύνης σε κατηγορίες ανάλογα με το βαθμό κινδύνου που εγκυμονείτε:

- Unacceptable risk: Στη κατηγορία αυτή των νόμων χαρακτηρίζονται εκείνες οι χρήσεις των συστημάτων τεχνητής νοημοσύνης τα οποία θίγουν ευάλωτες κοινωνικές ομάδες και εχουν τάσεις ανάπτυξης χειραγωγικών τεχνικών.
- High risk: Εδώ έχουμε τους νόμους που αναφέρονται σε δυσμενείς επιπτώσεις ,στην ασφάλεια των ανθρώπων ή στα θεμελιώδη δικαιώματά τους από τη χρήση της τεχνητής νοημοσύνης στη Βιομετρική αναγνώριση και κατηγοριοποίηση φυσικών προσώπων.
- Limited risk : Στη κατηγορία αυτή περιλαμβάνονται τα βιομετρικά συστήματα κατηγοριοποίησης και τα συστήματα τεχνητής νοημοσύνης που παράγουν ή χειραγωγούν περιεχόμενο εικόνας, ήχου ή βίντεο.
- Low or minimal risk: Στην τελευταία κατηγορία εντάσσονται εκείνα τα συστήματα τεχνητής νοημοσύνης τα οποία θα μπορούσαν να αναπτυχθούν και να χρησιμοποιηθούν στην ΕΕ χωρίς να συμμορφώνονται με πρόσθετες νομικές υποχρεώσεις. [30]

6.11 Το συμπέρασμα της σχέσης μεταξύ AI και βιομετρικών στοιχείων

Τα συστήματα αναγνώρισης προσώπου είναι ένας τύπος βιομετρικής τεχνολογίας που χρησιμοποιούν τεχνητή νοημοσύνη για την αναγνώριση και την επαλήθευση της ταυτότητας ατόμων με βάση τα χαρακτηριστικά του προσώπου τους. Συνήθως λειτουργούν με τη λήψη μιας εικόνας ή ενός βίντεο του προσώπου ενός ατόμου και στη συνέχεια με τη χρήση εξελιγμένων αλγορίθμων για τη σύγκρισή τους με μια βάση δεδομένων γνωστών προσώπων για την εύρεση μιας αντιστοιχίας.

Η τεχνητή νοημοσύνη διαδραματίζει κρίσιμο ρόλο στα συστήματα αναγνώρισης προσώπων επειδή τους επιτρέπει να εκτελούν πολύπλοκους υπολογισμούς και εργασίες αναγνώρισης προτύπων με ταχύτητα και ακρίβεια που θα ήταν αδύνατο να επιτύχει ο άνθρωπος. Τα συστήματα αναγνώρισης προσώπου με τεχνητή νοημοσύνη μπορούν να ανιχνεύουν λεπτές παραλλαγές στα χαρακτηριστικά του προσώπου, όπως η απόσταση μεταξύ των ματιών, το σχήμα της μύτης και το περίγραμμα της γνάθου, γεγονός που καθιστά δυνατή την αναγνώριση ατόμων με μεγάλη ακρίβεια.

Υπάρχουν πολλές διαφορετικές εφαρμογές των συστημάτων αναγνώρισης προσώπου και της τεχνητής νοημοσύνης, όπως η ασφάλεια και η επιτήρηση, ο βιομετρικός έλεγχος ταυτότητας και το μάρκετινγκ και η διαφήμιση. Για παράδειγμα, οι υπηρεσίες επιβολής του νόμου χρησιμοποιούν την τεχνολογία αναγνώρισης προσώπου για τον εντοπισμό εγκληματιών και την ταυτοποίηση υπόπτων, ενώ οι επιχειρήσεις μπορούν να τη χρησιμοποιήσουν για την αυθεντικοποίηση πελατών για ηλεκτρονικές συναλλαγές ή για την προσαρμογή των μηνυμάτων μάρκετινγκ με βάση την προσωπικότητα ενός πελάτη.

Ωστόσο, υπάρχουν επίσης ανησυχίες σχετικά με την πιθανή κατάχρηση των συστημάτων αναγνώρισης προσώπου και τον αντίκτυπο που θα μπορούσαν να έχουν στην ιδιωτική ζωή και τις πολιτικές ελευθερίες. Ορισμένοι ανησυχούν ότι τα συστήματα αυτά θα μπορούσαν να χρησιμοποιηθούν για την παρακολούθηση ατόμων χωρίς τη γνώση ή τη συγκατάθεσή τους ή ότι θα μπορούσαν να χρησιμοποιηθούν για τη διάκριση ορισμένων ομάδων με βάση την εμφάνισή τους. Οι αλγόριθμοι ΤΝ μπορεί να καταλήξουν σε λανθασμένα αποτελέσματα, αν εκπαιδευτούν με δεδομένα που περιέχουν προκαταλήψεις ή ανακρίβειες. Υπάρχει ο κίνδυνος να υπάρχουν ανισότητες στην επεξεργασία και ανάλυση δεδομένων, με ανυπόληπτα αποτελέσματα για διάφορες ομάδες του πληθυσμού, αν οι αλγόριθμοι είναι εκπαιδευμένοι με δεδομένα που αντικατοπτρίζουν υφιστάμενες κοινωνικές ανισότητες, μπορεί να ενισχύσουν αυτές τις ανισότητες.

Η αυτοματοποίηση που προκαλείται από την χρήση της ΤΝ μπορεί να οδηγήσει σε απώλεια θέσεων εργασίας, κυρίως σε επαγγέλματα που μπορούν να αντικατασταθούν εύκολα από μηχανές.

Όπως συμβαίνει με κάθε τεχνολογία, είναι σημαντικό να σταθμίζονται τα πιθανά οφέλη και οι κίνδυνοι των συστημάτων αναγνώρισης προσώπου και της τεχνητής νοημοσύνης και να εφαρμόζονται οι κατάλληλες διασφαλίσεις για την προστασία από την κακή χρήση. Είναι σημαντικό να ληφθούν μέτρα προφύλαξης και ρύθμισης προκειμένου να

διασφαλιστεί η δίκαιη, ασφαλής και διαφανής χρήση της τεχνητής νοημοσύνης και των βιομετρικών στοιχείων.

7 Συμπεράσματα

Αυτή η εργασία κάνει μια εκτενή ανασκόπηση κυρίως στα βιομετρικά συστήματα και το πως αυτά έρχονται αντιμέτωπα με τις προστασία της ιδιωτικότητας. Σε δεύτερη φάση αναλύεται πιο ειδικά η χρήση συστημάτων αναγνώρισης προσώπου και πώς αυτά συνδέονται με τη χρήση της τεχνητής νοημοσύνης.

Μέσα από τη βιβλιογραφική έρευνα παρατηρήσαμε ότι αν και η ακρίβεια αναγνώρισης έχει βελτιωθεί, η απόδοση αντιστοίχισης μπορεί να είναι ακόμα ανεπαρκής μετά από ορισμένες μη ιδανικές συνθήκες ή όταν το επίπεδο ασφάλειας του βιομετρικού συστήματος είναι ισχυρό. Από το γεγονός αυτό γίνεται σαφές ότι κατά τη σχεδίαση του βιομετρικού συστήματος ο σχεδιαστής πρέπει να λάβει υπόψη , να διατηρήσει μια προσεκτική ισορροπία μεταξύ της ακρίβειας αναγνώρισης του συστήματος και της ασφάλειας.

Στο δεύτερο μέρος της εργασίας όπου αναλύσαμε τα συστήματα αναγνώρισης προσώπου, ήρθαμε αντιμέτωποι με πρακτικά ερωτήματα ως προς τη χρήση των συστημάτων αυτών. Δηλαδή υπάρχει κάποιο όριο που ξεπερνιέται κατά τη συλλογή δεδομένων; Κατά πόσο μπορεί να θεωρηθεί ένα τέτοιο σύστημα αξιόπιστο όταν πρέπει να χρησιμοποιηθεί ως απόδειξη στις δικαστικές αίθουσες; Να σημειώσουμε πως εδώ πως πολλές ανησυχίες ως προς τη νομοθεσία έχουν ήδη απαντηθεί από τους νομοθέτες, αυτές κυρίως αναφέρονται για τα πρώτα χρόνια της εμφάνισης των συστημάτων αναγνώρισης προσώπου, όπου σταδιακά πάρθηκαν σημαντικές αποφάσεις και νόμοι.

Ένα σύστημα που μπορεί να προσδιορίσει τέλεια κάθε άτομο θα ήταν πολύ χειρότερο, καθώς θα μπορούσε να σημάνει το τέλος της ιδιωτικής ζωής. Αυτός είναι ο λόγος για τον οποίο όλο και περισσότεροι άνθρωποι ζητούν να τεθούν κυβερνητικά όρια για το πότε και πώς μπορεί να χρησιμοποιηθεί μια τέτοια τεχνολογία.

Ο κόσμος δεν έχει αποφασίσει ακριβώς τι θέλει ή μπορεί να μη γνωρίζει. Δηλαδή, όλοι εν έτη 2023 θέλουμε το κινητό μας ή ο υπολογιστής μας να ξεκλειδώνει με την αναγνώριση προσώπου και το θεωρούμε πολύ ενδιαφέρον, ωραίο και διασκεδαστικό. Σπάνια κάποιος θα κάνει παράπονα για την αναγνώριση προσώπου στο κινητό. Αντίθετα, όταν ακούσουμε την ίδια τεχνολογία σε δρόμους, τράπεζες και αεροδρόμια αλλάζει όλη η στάση μας και γινόμαστε κατά αυτής της τεχνολογίας. Είναι ένα ερώτημα που δε μπορεί να απαντηθεί ή μπορεί και να απαντηθεί;

Εν κατακλείδι, η ενσωμάτωση των συστημάτων αναγνώρισης προσώπου με την ΤΝ υπόσχεται πολλά και έχει σημαντικές δυνατότητες σε διάφορους τομείς. Ο συνδυασμός αλγορίθμων ΤΝ και τεχνολογίας αναγνώρισης προσώπου προσφέρει πολυάριθμα οφέλη, όπως ενισχυμένη ασφάλεια, βελτιωμένη αποδοτικότητα, εξατομικευμένες εμπειρίες, προηγμένη αλληλεπίδραση ανθρώπου-υπολογιστή, υποστήριξη της επιβολής του νόμου και ιατρικές εφαρμογές.

Αυτοματοποιώντας τις διαδικασίες επαλήθευσης ταυτότητας, τα συστήματα αναγνώρισης προσώπου με AI μπορούν να ενισχύσουν τα μέτρα ασφαλείας και να εξορθολογήσουν τις λειτουργίες. Παρέχουν μια αξιόπιστη και αποτελεσματική μέθοδο για την ταυτοποίηση ατόμων, τη χορήγηση πρόσβασης και την αποτροπή μη εξουσιοδοτημένης εισόδου. Η τεχνολογία αυτή έχει τη δυνατότητα να φέρει επανάσταση στα συστήματα ασφαλείας σε διάφορους κλάδους, όπως οι μεταφορές, οι τράπεζες και οι κυβερνητικοί τομείς.

Επιπλέον, τα συστήματα αναγνώρισης προσώπου με τεχνητή νοημοσύνη επιτρέπουν την εξατομίκευση και την προσαρμογή σε διάφορους τομείς. Αναγνωρίζοντας τα άτομα, τα συστήματα αυτά μπορούν να προσαρμόζουν τις εμπειρίες και τις υπηρεσίες σύμφωνα με τις προτιμήσεις τους, οδηγώντας σε βελτιωμένη ικανοποίηση και δέσμευση των πελατών. Στο λιανικό εμπόριο, για παράδειγμα, μπορούν να προσφέρονται εξατομικευμένες συστάσεις, ενώ στα έξυπνα σπίτια, οι ρυθμίσεις μπορούν να προσαρμόζονται με βάση τις προτιμήσεις των αναγνωρισμένων ατόμων.

Η ενσωμάτωση της τεχνολογίας αναγνώρισης προσώπου με την τεχνητή νοημοσύνη συμβάλλει επίσης στην προηγμένη αλληλεπίδραση ανθρώπου-υπολογιστή. Χρησιμοποιώντας την αναγνώριση προσώπου ως βιομετρικό αναγνωριστικό, οι χρήστες μπορούν να έχουν αβίαστα πρόσβαση σε συσκευές, να πραγματοποιούν ασφαλείς πληρωμές και να έχουν πρόσβαση σε εξατομικευμένο περιεχόμενο. Αυτή η απρόσκοπτη αλληλεπίδραση βελτιώνει την ευκολία και την εμπειρία του χρήστη.

Επιπλέον, τα συστήματα αναγνώρισης προσώπου με τεχνητή νοημοσύνη έχουν πολύτιμες εφαρμογές στην επιβολή του νόμου και τη δημόσια ασφάλεια. Μπορούν να βοηθήσουν στον εντοπισμό και την παρακολούθηση εγκληματιών ή υπόπτων με την αντιστοίχιση των προσώπων με τις υπάρχουσες βάσεις δεδομένων. Η τεχνολογία αυτή μπορεί να βοηθήσει τις έρευνες και να συμβάλει στη συνολική ασφάλεια των κοινοτήτων.

Στον ιατρικό τομέα, η τεχνολογία αναγνώρισης προσώπου έχει τη δυνατότητα να παρακολουθεί ασθενείς, να αναλύει τις εκφράσεις του προσώπου για την ανίχνευση συναισθημάτων και να βοηθά στη διάγνωση ορισμένων ιατρικών καταστάσεων με βάση τα στοιχεία του προσώπου. Μπορεί να συμβάλει σε πιο ακριβείς αξιολογήσεις και εξατομικευμένη φροντίδα.

Η τεχνητή νοημοσύνη και τα συστήματα αναγνώρισης προσώπου προσφέρουν πολλές εφαρμογές και οφέλη στον τομέα του μάρκετινγκ και όχι μόνο. Μέσω της αναγνώρισης προσώπου, μπορεί να δημιουργηθεί εξατομικευμένη εμπειρία πελάτη, προσαρμοσμένη στις προτιμήσεις του κάθε ατόμου, βελτιώνοντας έτσι την ικανοποίηση και την πιστοποίηση του πελάτη. Επιπλέον, η αναγνώριση προσώπου σε συνδυασμό με την τεχνητή νοημοσύνη μπορεί να βελτιώσει την ασφάλεια και την πρόληψη εγκλημάτων, επιτρέποντας την ανίχνευση ανεπιθύμητων προσώπων ή την αναγνώριση εγκληματικών δραστηριοτήτων. Επίσης, μπορεί να χρησιμοποιηθεί για προσωπική ασφάλεια και παρακολούθηση, ενώ επιτρέπει επίσης την επεξεργασία γλώσσας και την αυτόματη απόκριση.

Ενώ τα συστήματα αναγνώρισης προσώπου με τεχνητή νοημοσύνη προσφέρουν πολυάριθμα οφέλη, είναι ζωτικής σημασίας να αντιμετωπιστούν οι ηθικές ανησυχίες και τα ζητήματα προστασίας της ιδιωτικής ζωής. Η εξεύρεση ισορροπίας μεταξύ ασφάλειας και ιδιωτικότητας, η εφαρμογή αυστηρών μέτρων προστασίας δεδομένων και η διασφάλιση της διαφάνειας στη χρήση και την αποθήκευση των δεδομένων προσώπου είναι ουσιώδους σημασίας για την υπεύθυνη ανάπτυξη και αποδοχή αυτής της τεχνολογίας.

Συμπερασματικά, η ενσωμάτωση των συστημάτων αναγνώρισης προσώπου με την ΤΝ έχει τη δυνατότητα να φέρει επανάσταση στην ασφάλεια, την αποτελεσματικότητα, την εξατομίκευση και την αλληλεπίδραση ανθρώπου-υπολογιστή σε διάφορους τομείς. Ωστόσο, πρέπει να δοθεί προτεραιότητα σε δεοντολογικά ζητήματα και σε εγγυήσεις προστασίας της ιδιωτικής ζωής, ώστε να διασφαλιστεί η υπεύθυνη και επωφελής χρήση αυτής της τεχνολογίας.

Βιβλιογραφία

1) By Recfaces, 7 December 2020 | ABOUT BIOMETRICS.The History of Biometrics

2) Geng, S., Giannopoulou, G. and Kabir-Querrec, M., 2019, November. Privacy Protection in Distributed Fingerprint-based Authentication. In Proceedings of the 18th ACM Workshop on Privacy in the Electronic Society (pp. 125-129).

3) Zorkadis, V. and Donos, P., 2004. On biometrics-based authentication and identification from a privacy-protection perspective: Deriving privacy-enhancing requirements. *Information Management & Computer Security*, *12*(1), pp.125-137.

4) Bowyer, K.W. (2004). Face recognition technology: security versus privacy. *IEEE Technology and Society Magazine*, 23(1), pp.9–19. doi:https://doi.org/10.1109/mtas.2004.1273467.

5) Lofred Madzou, John Riemen, Sébastien Louradour, Luc Garcia, Odhran McCarthy, Maria Eira, 05 Oct 2021. This is best practice for using facial recognition in law enforcement

6) By RECFACES, NOVEMBER 2020 | TECHNOLOGIES.What is Facial Recognition Used For?

7) Κωνσταντίνος Ζουμπουλάκης και Κωνσταντίνος Κακαβούλης 14 Σεπτεμβρίου, 2020, Facial recognition και αντεγκληματική πολιτική: Μια βεβιασμένη συνύπαρξη

8) RecFaces, 30 Juny 2021. What Is AI Facial Recognition Tech and How does It Work?

9) Deutsche Welle, Καρίν Σενζ, ARD Κων/Πολη. 02.01.2021. Τι σχέση έχουν η Κίνα, οι Ουιγούροι και η Τουρκία;

10) D. Alayon. Understanding Artificial Intelligence. Accessed: 2018. [Online]. Available: https://medium.com/future-today/understandingartificial-intelligence-f800b51c767f

11) McMahan, B., Moore, E., Ramage, D., Hampson, S. and Arcas, B.A. y (2017). Communication-Efficient Learning of Deep Networks from Decehttps://1drv.ms/w/s!AvU3KbjzAbOQlAEPoFRjCYGb0ved?e=48urlentralizedData. *PMLR*.[online].Available:http://proceedings.mlr.press/v54/mcmahan17a?ref=https://githubhelp.com

12) MADIEGA, T. & MILDEBRATH, H., 2021. Regulating facial recognition in the EU, EPRS: European Parliamentary Research Service. Retrieved from https://policycommons.net/artifacts/1815279/regulating-facial-recognition-in-the-eu/2551619/ on 02 Jun 2022. CID: 20.500.12592/4292px.

13) Barnette, W.P., 2021. There Is No Conservative Case for Class Actions.

14) http://ebooks.edu.gr/ebooks/v/html/8547/4722/Arches-Oikonomikis-Theorias_G-Lykeiou-SpOikPlir_html-apli/index2.html

15) Έγγραφο WP80 εργασίες σχετικά με τα στοιχεία βιομετρίας , Αύγουστος 2003.

16) Sarkar, Arpita, and Binod K. Singh. "A review on performance, security and various biometric template protection schemes for biometric authentication systems." Multimedia Tools and Applications 79, no. 37 (2020): 27721-27776.

17) Daphne Leprince-Ringuet on April 6, 2021 Facial recognition tech is supporting mass surveillance. It's time for a ban, say privacy campaigners

18) Suneratech : What Is AI, ML & How They Are Applied to Facial Recognition Technology
OCTOBER 22, 2021

19) Ευρωπαϊκή επιτροπή, Βρυξέλλες ,21/4/21, Κανονισμός του ευρωπαϊκού κοινοβουλίου και του συμβουλίου(Πράξη για τη τεχνητή νοημοσύνη).

20) Agarwal, M., Jain, N., Kumar, M. M., & Agrawal, H. (2010). Face recognition using eigen faces and artificial neural network. International Journal of Computer Theory and Engineering, 2(4), 624.

21) Hung, C. V., Vladimirovich, A. S., Van Giang, N., Hoan, N. T., City, T. D. M., Province, B. D., ... & Tham, P. N. BINH DUONG UNIVERSITY JOURNAL OF SCIENCE AND TECHNOLOGY.

22) Taigman, Y., Yang, M., Ranzato, M. A., & Wolf, L. (2014). Deepface: Closing the gap to human-level performance in face verification. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 1701-1708).

23) Srivastava, G., & Bag, S. (2023). Modern-day marketing concepts based on face recognition and neuro-marketing: a review and future research directions. Benchmarking: An International Journal.

24) Shrestha, A. and Mahmood, A. (2019). Review of Deep Learning Algorithms and Architectures. *IEEE Access*, 7, pp.53040–53065. doi:https://doi.org/10.1109/access.2019.2912200.

25) December 13, 2021. S.Korea to test AI-powered facial recognition to track COVID-19 cases,By Sangmi Cha

26) R. Chu. What is AI? A Brief Explanation for Layman. Accessed: 2018. [Online]. Available: https://medium.com/datadriveninvestor/what-is-aia-brief-explanation-for-layman-f79f368702ea

27) Ng, A., 2020. How China uses facial recognition to control human behavior. CNET.

28) J. Soria-Comas, J. Domingo-Ferrer, D. Sanchez, and D. Megias, ‘‘Individual differential privacy: A utility-preserving formulation of differential privacy guarantees,’’ IEEE Trans. Inf. Forensics Security, vol. 12, no. 6, pp. 1418–1429, Jun. 2017.

29) REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016

30) MADIEGA, Tambiama. Artificial intelligence act. European Parliament: European Parliamentary Research Service, 2020

31) Lawspot , Αναγνώριση προσώπου (Face recognition) και προσωπικά δεδομένα , Μαγδαληνή Σκόνδρα , 21/01/20