ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Εθνικόν και Καποδιστριακόν Πανεπιστήμιον Αθηνών
ΙΔΡΥΘΕΝ ΤΟ 1837

ΝΟΜΙΚΗ ΣΧΟΛΗ

Π.Μ.Σ.: Ιστορία, Κοινωνιολογία και Φιλοσοφία του Δικαίου
ΕΙΔΙΚΕΥΣΗ: **Κοινωνιολογία του Δικαίου, Επιστήμη και Τεχνολογία**
ΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΕΤΟΣ: 2018 – 2019

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Νικόλαος Α. Καρανικόλας

Α.Μ.: 7340011718001

«Τεχνολογίες Βιομετρικής Ταυτοποίησης: Νομικοί & Βιοηθικοί Προβληματισμοί για την Προστασία των Προσωπικών Δεδομένων»

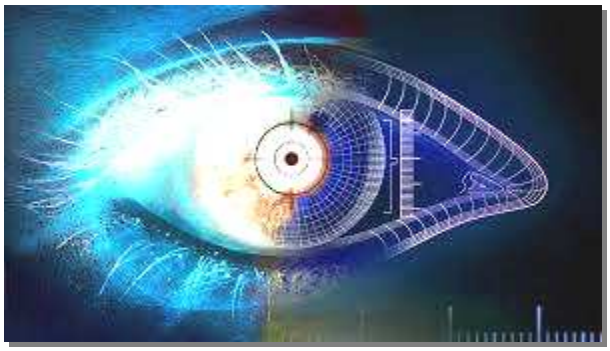
Επιβλέποντες:

α) Prof. Ελένη Ρεθυμιωτάκη

β) Prof. Γιώργος Γιαννόπουλος

γ) Prof. Β. Βουτσάκης

Αθήνα, Σεπτέμβριος 2019



«Το μέλλον είναι εδώ,

απλά δεν είναι ευρέως διαδεδομένο ακόμη.»

William Gibson,

Αμερικανός Συγγραφέας,

1948 -

Αντί Προλόγου

Η επιλογή της θεματικής των «*Τεχνολογιών Βιομετρικής Ταυτοποίησης*», θέτοντας στο επίκεντρο τους «*Νομικούς & Βιοηθικούς Προβληματισμούς για την Προστασία των Προσωπικών Δεδομένων*», πραγματοποιήθηκε για δύο βασικούς λόγους. Κατ' αρχάς, η προσωπική μου εμπλοκή σε θέματα ηλεκτρονικής διακυβέρνησης, στο πλαίσιο της εικοσαετούς θητείας μου στη δημόσια διοίκηση και κατά το μεγαλύτερο χρονικό διάστημα αυτής, σε θέσεις ευθύνης, μου έδωσε τη δυνατότητα να παρατηρήσω την συμβολή των ψηφιακών τεχνολογιών στην αντιμετώπιση της γραφειοκρατίας και στην επιτάχυνση των διοικητικών διαδικασιών

Επιπρόσθετα, η πρόσφατη τοποθέτηση μου στην νευραλγική θέση του Υπευθύνου Προστασίας Δεδομένων του Δήμου Αθηναίων (DPO), με ώθησε στην εντατικότερη μελέτη της βιβλιογραφίας που σχετίζεται με τη «Νομική Πληροφορική», ενός νέου σχετικά κλάδου της νομικής επιστήμης, στο πεδίο του οποίου, εντάσσεται και η εξεταζόμενη αντιμετώπιση των βιομετρικών δεδομένων ως υποσύνολο των προσωπικών δεδομένων.

Κριτήριο για την επιλογή των επιμέρους θεματικών ενοτήτων που πρόκειται να αναλυθούν στην παρούσα εργασία, αποτέλεσε η αναγκαιότητα να γίνει αναφορά στις πρόσφατες τεχνολογικές και βιομετρικές εξελίξεις, για τις οποίες ο νομικός επιστήμονας απαιτείται να είναι ενήμερος, χωρίς ωστόσο το ζητούμενο να είναι η απόκτηση εξειδικευμένων γνώσεων βιομετρικής τεχνολογίας αλλά μια ολιστική θεώρηση των σύγχρονων τεχνολογιών που επηρεάζουν είτε την ίδια την κοινωνιολογική επιστήμη, είτε την αντίληψή μας για την εξέλιξη του δικαίου.

Πιο συγκεκριμένα στο εισαγωγικό κεφάλαιο περιγράφεται σχηματικά η σταδιακή αύξηση της χρήσης των τεχνολογιών βιομετρικής αναγνώρισης σε διεθνικό επίπεδο, ως απότοκο της παγιωμένης ψηφιακής πραγματικότητας, ιδιαίτερα κατά τη διάρκεια της τελευταίας 20ετίας. Παράλληλα, εντοπίζεται και αναλύεται, η σημασιολογική συνεισφορά της προσθήκης «*βίο*» στην τεχνολογία στην πολιτική και στην ηθική.

Στο δεύτερο κεφάλαιο επιχειρείται μια ευρύτερη παρουσίαση του κανονιστικού και ρυθμιστικού πλαισίου των βιομετρικών δεδομένων σε εθνικό, ενωσιακό, διαμερικανικό και διεθνικό επίπεδο. και ταυτόχρονα παρουσιάζεται μια σύντομη συγκριτική ανάλυση των εννοιών των προσωπικών και βιομετρικών δεδομένων, αναδεικνύοντας τις ποιοτικές τους διαφορές.

Στο τρίτο κεφάλαιο προσδιορίζονται οι κοινωνιολογικοί και ηθικοί προβληματισμοί που προκύπτουν από την άκριτη εφαρμογή των τεχνολογιών βιομετρικής αναγνώρισης.

Abstract

"Biometric Identification Technologies: Legal & Bioethical Considerations for the Protection of Personal Data"

This work aims to identify the legal and ethical perspective of biometrics. Biometric systems have been developed in response to the growing demand for security currently in existence, and although some of them are highly reliable, no system is 100% effective, and these systems are also likely to be deceived. Different types of existing biometric systems for the recognition of an exclusive characteristic of a person. Showing the evolution of the biometric systems throughout history as well as their future trends are being explained in this paper. Throughout the last century there have been many companies that have concentrated their efforts on developing biometric systems to ensure their safety, as have the Defense Departments of several countries themselves. Therefore, laws and regulation initiated in order to protect personal data are also being discussed. Analysis of above-mentioned perspectives will be beneficial for the legal authorities to help and safeguard the personal data of population.

Ευχαριστίες

Αρχικά, θα ήθελα να εκφράσω την ειλικρινή ευγνωμοσύνη μου στην επιβλέπουσα καθηγήτρια της διπλωματικής μου εργασίας, Prof. Ελένη Ρεθυμιωτάκη, καθηγήτρια Κοινωνιολογίας του Δικαίου της Νομικής Σχολής του ΕΚΠΑ, για την ακαδημαϊκή υποστήριξη και καθοδήγηση, την μεταλαμπάδευση της πολύτιμης γνώσης της, αλλά και για την πνευματική έμπνευση και παροχή κινήτρων για την ολοκλήρωση του πονήματος. Η συμβολή της υπήρξε καταλυτική και αισθάνομαι ιδιαίτερη τιμή που είχα την τύχη να αποδεχθεί την επίβλεψη της παρούσας εργασίας. Δεν θα μπορούσα να έχω καλύτερο μέντορα.

Επίσης, θα ήθελα να ευχαριστήσω τον Prof. Γεώργιο Γιαννόπουλο, καθηγητή Δημοσίου Δικαίου, της Νομικής Σχολής, του ΕΚΠΑ, για τα διορατικά του σχόλια και την ισχυρή του ενθάρρυνσή, η οποία με παρότρυνε να διευρύνω την ανάλυση μου υπό την οπτική διαφόρων πεδίων της επιστήμης του Δικαίου.

Οι ειλικρινείς ευχαριστίες μου απευθύνονται επίσης στο τρίτο μέλος της τριμελούς επιτροπής επίβλεψης και αξιολόγησης της διπλωματικής μου εργασίας Prof. Β. Βουτσάκη, καθηγητή της Νομικής Σχολής του ΕΚΠΑ, για την υποστήριξη του.

Σας Ευχαριστώ

Πίνακας Περιεχομένων

1. ΚΕΦΑΛΑΙΟ ΠΡΩΤΟ

1.1. Εισαγωγή

Το 2001, οι βιομετρικές τεχνολογίες χαρακτηρίστηκαν από το έγκυρο MIT Technology Review, ως μια από τις αναδυόμενες τεχνολογίες που θα αλλάξουν τον κόσμο (Woodward et al. 2003: xxiii). Αμέσως μετά τα γεγονότα της 11ης Σεπτεμβρίου, η βιομετρική βιομηχανία τοποθετήθηκε στο διεθνές προσκήνιο από τις κυβερνήσεις πολλών κρατών οι οποίες δήλωσαν πρόθυμες να υιοθετήσουν βιομετρικές τεχνολογίες ως μέτρο ενίσχυσης της δημόσιας ασφάλειας.

Οι βιομετρικές τεχνολογίες, ως μέσο αυθεντικοποίησης και ταυτοποίησης του ατόμου αποκτούν ολοκληρωμένο νόημα μόνο εάν τις εντάξουμε στο πλαίσιο των εξουσιαστικών σχέσεων και των τεχνικών υπακοής οι οποίες εντοπίζουν και κατηγοριοποιούν τα υποκείμενα σε ένα περίπλοκο πολιτικά κοινωνικά και νομικά δίκτυο. Υπό αυτή την έννοια οι βιομετρικές τεχνολογίες σχετίζονται άμεσα με την βιοεξουσία.

Ο Μισέλ Φουκώ (2008: 34), παρατηρεί ότι η εμφάνιση του βιοπολιτικού κράτους σχετίζεται με την εγκαθίδρυση του ερωτήματος της αλήθειας στην καρδιά των εγκληματολογικών ερευνών. Το κλασσικό ερώτημα «τι έχεις κάνει» έχει πλέον αντικατασταθεί από το ερώτημα «ποιος είσαι» (Foucault 2008:34). Το κεντρικό ερώτημα που θέτουν οι βιομετρικές τεχνολογίες είναι ακριβώς αυτό, «ποιος είσαι». Με την ευρεία εφαρμογή των βιομετρικών τεχνολογιών το ερώτημα αυτό μετατράπηκε στο «τι είσαι».

Ωστόσο το ερώτημα «τι είσαι» συνδέεται άρρηκτα με το γεωπολιτικό status του υποκειμένου. Η απάντηση στο ερώτημα «τι είσαι», είσαι για παράδειγμα ένα έγχρωμο άτομο, ένα άτομο που αναζητά άσυλο, προσδιορίζει την απάντηση στο ποιος είσαι.

Στις σύγχρονες κοινωνίες λοιπόν, η κατακόρυφη αύξηση των προσδοκιών αναφορικά με την ασφάλεια έχει επηρεάσει καταλυτικά τις σχέσεις πολίτη και κράτους. Έχουμε ουσιαστικά επιστρέψει σε ένα είδος πρώιμου συνταγματισμού το οποίο προσδιορίζει τις εγγυήσεις για την ασφάλεια ως περισσότερο σημαντικές από τον σεβασμό των ελευθεριών και των ατομικών δικαιωμάτων[1].

Η θεώρηση της ασφαλείας ως το απόλυτο συλλογικό αγαθό που μονοπωλείται από το κράτος, δημιουργεί αναπόφευκτα μια ανασφάλεια για τις ατομικές ελευθερίες, την οποία το δίκαιο καλείται να αντιμετωπίσει και να περιορίσει. Σήμερα έχουμε να αντιμετωπίσουμε ένα κράτος το οποίο δρα είτε προληπτικά ή ως κράτος παιδαγωγός, εξομοιώνοντάς τον πολίτη με ένα δυνητικό παραβάτη. Ο πόλεμος ενάντια στην τρομοκρατία δημιούργησα το τέλειο πρόσχημα για την πολιτεία να υιοθετήσει ένα τεχνολογικό οπλοστάσιο το οποίο οδηγεί σε ένα καθολικό έλεγχο[2].

Η χρήση των βιομετρικών τεχνολογιών καθιστά το σώμα ένα αντικείμενο των μηχανισμών εξουσίας. Όπως αναφέρει ο Agamben (2007: 15), εφόσον η εξουσία ασκείται στο ίδιο το σώμα η χρήση των βιομετρικών τεχνολογιών αποτελούν μια μέθοδο ολοκληρωτικής κυριαρχίας. Πράγματι στις σημερινές κοινωνίες οι ραγδαίες εξελίξεις της βιοτεχνολογίας, η δημιουργία μεγάλων βάσεων δεδομένων με βιομετρικά στοιχεία, η συγκέντρωση και η αρχειοθέτηση ευαίσθητων πληροφοριών του ατόμου που σχετίζονται με τα βιομετρικά του δεδομένα, γεγονός που πολλές φορές συμβαίνει χωρίς τη συγκατάθεση του, αυξάνει κατακόρυφα τους κινδύνους για την προστασία της ιδιωτικότητας του ατόμου αλλά και εν τέλει για την δημοκρατική λειτουργία του ίδιου του πολιτεύματος[3].

[1]Βλ. Ν. Παρασκευόπουλο, *Ασφάλεια του κράτους και ανασφάλεια δικαίου, στον τόμο Τρομοκρατία και δικαιώματα*, Α. Μανιτάκης, Α. Τάκης (επιμ.), Σαββάλας, 2004, σ. 42 επ.
[2] Βλ. J. Derrida/ J. Habermas, *Le "concept" du 11 Septembre. Dialogues a New York avec G. Borradori*, Galile, 2003, σ. 57 επ, 87 επ.
[3] Βλ. G. Agamben, *Κατάσταση εξαίρεσης*, Πατάκης, 2007, σ. 15 επ.

Η σημαντικότητα των παραπάνω κινδύνων γίνεται περισσότερο κατανοητή στις περιπτώσεις που η συλλογή επεξεργασία και αρχειοθέτηση των βιομετρικών πληροφοριών του ατόμου σχετίζεται με την κατηγοριοποίηση των ατόμων σε συγκεκριμένα πρότυπα. Η κατάταξη αυτή δημιουργεί έναν ψηφιακό στιγματισμό του ατόμου, που οποίου η κοινωνική ταυτότητα προσδιορίζεται από αυτή τη διαδικασία και οδηγεί αναγκαστικά το άτομο σε συμμόρφωση με το προκαθορισμένο πρότυπο.

Τα όρια μεταξύ του ιδιωτικού και του δημόσιου χώρου του ατόμου γίνονται σαφώς δυσδιάκριτα καθώς η συγκέντρωση των βιομετρικών του δεδομένων και η χρήση για την ταυτοποίηση του, καταργούν την ανωνυμία του. Μέχρι πριν από 20 χρόνια η πρόσβαση στα βιομετρικά δεδομένα αποτελούσε αποκλειστικό προνόμιο των κρατικών υπηρεσιών. Σήμερα ωστόσο μπορεί οποιοσδήποτε με τη χρήση ενός smartphone να αποθηκεύσει βιομετρικά στοιχεία και να τα χρησιμοποιήσει στα κοινωνικά δίκτυα.

Αναλογιζόμενοι την κατάσταση όπως έχει διαμορφωθεί σήμερα θα μπορούσαμε να υιοθετήσουμε την άποψη του Agamben (1998: 72)[4], ο οποίος υποστηρίζει ότι στις σημερινές κοινωνίες όλα τα άτομα χωρίς εξαίρεση αποτελούν εν δυνάμει “Homines Sacri”[5], δηλαδή νοούνται ως πρόσωπα που τοποθετούνται στο περιθώριο, ως θύματα του κοινωνικού στιγματισμού. Σε παλαιότερες εποχές τα άτομα αυτά αποτελούσαν τις εξαιρέσεις, σήμερα ωστόσο λόγω της διαρκούς βιοτεχνολογικής παρέμβασης, ο άνθρωπος μετατρέπεται σε

[4] Agamben, Giorgio, Heller-Roazen, trans. *Homo Sacer: Sovereign Power and Bare Life Stanford,* California: Stanford University Press, 1 April 1998 σ.72.

[5] Ο Homo sacer (Λατινικός όρος για τον "ιερό άνθρωπο") είναι μια ορολογία του ρωμαϊκού δικαίου: πρόκειται για ένα πρόσωπο που μπορεί να σκοτωθεί από οποιονδήποτε, αλλά δεν μπορεί να θυσιαστεί σε θρησκευτικό τελετουργικό. Ο homo sacer θα μπορούσε επομένως να αναφέρεται στο άτομο που εξορίστηκε από την κοινωνία και στερείται όλων των δικαιωμάτων του, πολιτικών και θρησκευτικών. Ο Homo sacer ορίζεται με νομικούς όρους ως κάποιος που μπορεί να θανατωθεί χωρίς ο υπαίτιος να θεωρηθεί δολοφόνος και ταυτόχρονα είναι κάποιος που δεν μπορεί να θυσιασθεί. Ο «ιερός άνθρωπος» μπορεί με αυτή την έννοια να γίνει κατανοητός ως κάποιος που τοποθετείται έξω από το νόμο ή πέρα από αυτόν.

πειραματόζωο και αιχμάλωτο του κράτους με συνέπεια ο όρος homo sacri, να αφορά όχι σε μέρος αλλά στο σύνολο της μετανεωτερικής κοινωνίας[6].

1.2. Βιομετρικές τεχνολογίες ταυτοποίησης

Οι τεχνολογίες βιομετρικής ταυτοποίησης (biometrics) είναι ένα αυτοματοποιημένο σύστημα αναγνώρισης ανθρώπινων χαρακτηριστικών, που βασίζεται στα φυσικά χαρακτηριστικά και τη συμπεριφορά των ατόμων. Οι βιομετρικές τεχνολογίες διευκολύνουν τη απεικόνιση, αποθήκευση και επεξεργασία των βιομετρικών πληροφοριών των ανθρώπων, δηλαδή των βιολογικών, μορφολογικών και συμπεριφορικών χαρακτηριστικών τους. Αυτές οι πληροφορίες/χαρακτηριστικά ψηφιοποιούνται ώστε να μπορούν να αναγνωστούν από τους ηλεκτρονικούς υπολογιστές για να συγκριθούν με άλλες πληροφορίες, συνήθως του ίδιου τύπου (Zhang, Lu, & Zhang, 2018: 10).

Υπάρχουν πολλές εταιρείες τεχνολογίας σε όλο τον κόσμο που έχουν ήδη παρουσιάσει σύνθετα συστήματα ταυτοποίησης του ατόμου μέσω βιομετρικών στοιχείων, μια τεχνολογία που βασίζεται στα εγγενή χαρακτηριστικά κάθε υποκειμένου, όπως η αναγνώριση δακτυλικών αποτυπωμάτων ή η αναγνώριση προσώπου. Παρά το γεγονός ότι μέχρι και πριν από μερικά χρόνια συναντούσαμε αυτή την τεχνολογία μόνο σε αστυνομικές υποθέσεις, ή σε μεγάλης κλίμακας έρευνες ή σε ταινίες επιστημονικής φαντασίας, σήμερα είναι ολοένα και πιο συνηθισμένο να χρησιμοποιούνται βιομετρικά συστήματα ταυτοποίησης και σε άλλους τομείς, όπως σε ιδιωτικές εταιρείες, στις οποίες η χρήση της τεχνολογίας αυτής αποκτά ολοένα και μεγαλύτερο κομβικό ρόλο (Zuo, Saun, & Forrest, 2019: 1298e).

Η βιομετρική ταυτοποίηση αποτελείται από την αναγνώριση της ταυτότητας ενός ατόμου από το ίδιο του το σώμα, είτε μέσω της φωνής, είτε του αποτυπώματος είτε του

[6] Βλ. Φ. Τερζάκη, *Το αρχέτυπο του Νταχάου και του Γκουαντάναμο*, 2018, www.phorum.gr.

προσώπου. Σήμερα, το πιο δημοφιλές και το ασφαλέστερο σύστημα είναι η αναγνώριση μέσω δακτυλικών αποτυπωμάτων. Ωστόσο, στο άμεσο μέλλον θα επικρατήσει η αναγνώριση προσώπου. Αυτό το σύστημα δεν περικλείει μόνο τη φυσιογνωμία του ατόμου, αλλά είναι ικανό να συλλαμβάνει τα συναισθήματα στο πρόσωπό του, αναλύοντας τις κινήσεις ή τις εκφράσεις του.

Επί του παρόντος και αναφορικά με τον τρόπο ταυτοποίησης μας, καθημερινά στον ψηφιακό κόσμο, είμαστε υποχρεωμένοι να έχουμε κατά νου έναν μεγάλο αριθμό κωδικών πρόσβασης και ονομάτων χρηστών, τα οποία, σε πολλές περιπτώσεις, προκαλούν μεγαλύτερη ταλαιπωρία από τα πλεονεκτήματα που προσφέρουν, λόγω των προβλημάτων που προκύπτουν από την επιβράδυνση των διαδικασιών.

Η βιομετρική ταυτοποίηση όχι μόνο θα τερματίσει εντελώς τον μακρύ κατάλογο των κωδικών πρόσβασης και των ονομάτων χρηστών που θα πρέπει να ανακαλούμε στη μνήμη μας, αλλά θα τροποποιήσει επίσης την παραδοσιακή ταυτοποίηση μέσω φυσικών εγγράφων. Μπορείτε να φανταστείτε την αναγνώριση του εαυτού σας όταν φτάνετε σε ένα ξενοδοχείο, μόνο μέσω του προσώπου σας; Ή όταν επιβιβάζεστε σε ένα αεροπλάνο; Σε σύντομο χρονικό διάστημα, θα αποτελεί μέρος της καθημερινότητας μας (Zuo, Saun, & Forrest, 2019: 1300e).

Παρά την αυξανόμενη ανάπτυξη της τεχνολογίας αναγνώρισης προσώπου, υπάρχουν πολλοί τομείς στους οποίους το δακτυλικό αποτύπωμα φαίνεται να είναι η πρώτη επιλογή, όπως για παράδειγμα στις πληρωμές μέσω κινητών τηλεφώνων. Πρόσφατα, μια εταιρεία μεθόδων πληρωμών παρουσίασε την ανάλυση των ψηφιακών της πληρωμών για το 2017 , και μεταξύ 14.000 ευρωπαίων καταναλωτών, διαπιστώθηκε ότι η πλειονότητα ενδιαφέρεται για την ταυτοποίηση μέσω βιομετρικών συστημάτων, ιδίως όταν τα συστήματα αυτά ενσωματώνονται σε άλλα μέτρα ασφαλείας. Η βιομετρική ταυτοποίηση, μέσω της αναγνώρισης προσώπου ή μέσω της ψηφιακής ανάγνωσης του αποτυπώματος και άλλες

μέθοδοι που θα αναφερθούμε στη συνέχεια, δημιουργούν ένα πανόραμα από μεγάλες δυνατότητες που με τη συνδρομή των κατάλληλων και απαραίτητων συστημάτων ασφαλείας, θα αλλάξουν εντελώς τον τρόπο με τον οποίο σχετιζόμαστε με το ψηφιακό μας περιβάλλον (Smith, Mann, & Urbas, 2018: 25).

1.3. Το ανθρώπινο σώμα ως το ασφαλέστερο μέσο ταυτοποίησης

Στις 20 Σεπτεμβρίου 2013, το νέο iPhone 5S παρουσιάστηκε, προσφέροντας στο κοινό ένα διαφορετικό νέο χαρακτηριστικό: τη συσκευή ανάγνωσης δακτυλικών αποτυπωμάτων. Δεν ήταν το πρώτο τηλέφωνο που χρησιμοποίησε αυτή την τεχνολογία, αλλά δημιούργησε την πλειοψηφική τάση που καθιστά σήμερα τη συσκευή ανάγνωσης δακτυλικών αποτυπωμάτων, μια απαραίτητη απαίτηση για τα κινητά τηλέφωνα όλων των ειδών και ένας μεγάλο σύμμαχο για τις τράπεζες και τις εταιρείες που αναζητούν τη μεγαλύτερη ασφάλεια για τους πελάτες τους.

Η χρήση του ανθρώπινου σώματος ως σύστημα αυθεντικοποίησης είναι όλο και πιο συχνή, και εκτός από το δακτυλικό αποτύπωμα χρησιμοποιούνται, το πρόσωπο, η ίριδα του ματιού, η αναγνώριση φωνής, οι φλέβες, ακόμη και ο καρδιακός παλμός. Οι εταιρείες μπορούν να αναγνωρίζουν τους πελάτες τους ψηφιακά ανά πάσα στιγμή και από οπουδήποτε, πριν, κατά τη διάρκεια και μετά την όποια συναλλαγή. Σημαντική περίπτωση χρήσης της βιομετρικής τεχνολογίας είναι η δημιουργία τραπεζικών λογαριασμών, μέσω βιομετρικών διαδικασιών ταυτοποίησης και ηλεκτρονικής υπογραφής (Cabrera, Hernández, Niño, & Dasgupta, 2018: 35). Στην τράπεζα BBVA[7], για παράδειγμα, δημιούργησαν το

[7] Η Banco BilbaoVizcaya Argentaria (BBVA) είναι πολυεθνικός ισπανικός τραπεζικός όμιλος που ιδρύθηκε από τη συγχώνευση των Banco Bilbao Vizcaya και Argentaria το 1999 και είναι η δεύτερη μεγαλύτερη τράπεζα στην Ισπανία. Το 2007, η επιχείρηση ξεκίνησε μια πρωτοβουλία ψηφιακής μετατροπής της τράπεζας. Από το 2015, ο συνολικός αριθμός των ψηφιακών πελατών ανερχόταν σε 14,8 εκατομμύρια. Βλ. «Mentor Europe 5 Excellent Examples of Successful Transformation Programs». mentoreurope.com.

προηγούμενο έτος, μια νέα τεχνολογική μονάδα που ειδικεύεται στα βιομετρικά στοιχεία τα οποία επιτρέπουν την ψηφιακή πιστοποίηση της ταυτότητας μέσω προσώπου, φωνής ή ανάγνωσης δακτυλικών αποτυπωμάτων. Χάρη σε αυτό είναι δυνατό να δημιουργηθεί ένας λογαριασμός στην τράπεζα, χρησιμοποιώντας απλά μια selfie (Arslanian & Fischer, 2019: 113-121).

Ένα ακόμα σχετικό παράδειγμα αποτελεί η Caixa Bank[8], η οποία εφάρμοσε την τεχνολογία βιομετρικής αναγνώρισης σε όλο το δίκτυο των γραφείων της. Σήμερα, όλες οι διεργασίες υπογράφονται σε μια οθόνη αφής και με έναν εξοπλισμό βιομετρικής τεχνολογίας που επιτρέπει τη συλλογή βιομετρικών δεδομένων από τις υπογραφές των πελατών (πίεση, προσανατολισμό περιγράμματος) και αποθηκεύονται με ασφάλεια στην σύμβαση τράπεζας - πελάτη, η οποία εγγυάται έτσι τη νομική της ισχύ (Fraga, & De Souza, 2018: 110).

1.4. Το παράδειγμα της τράπεζας HSBC

Η HSBC[9] επιτρέπει στους πελάτες της να έχουν πρόσβαση σε όλες τις υπηρεσίες της με τη χρήση του δακτυλικού αποτυπώματος, μέσω των εφαρμογών των έξυπνων κινητών όπως το , fingerprint για το λογισμικό Android ή το Touch ID για το λογισμικό της Apple και ήταν η πρώτη τράπεζα στην ΕΕ που ενσωμάτωσε την τεχνολογία αναγνώρισης προσώπου «Face ID» του iPhone X , στις εφαρμογές που διαθέτει για τις έξυπνες κινητές συσκευές (smart phones, tablets, phablets).

Με αυτόν τον τρόπο, οι πελάτες της HSBC μπορούν να έχουν πρόσβαση στους λογαριασμούς τους χρησιμοποιώντας και αποθηκεύοντας το δακτυλικό αποτύπωμα ή την τρισδιάστατη αναγνώριση προσώπου και χωρίς να χρειάζεται να εισέλθουν σε ασφαλή

[8] https://www.caixabank.es/particular/holabank/online-banking.html

[9] Η HSBC Holdings plc είναι μια βρετανική πολυεθνική τράπεζα επενδύσεων και εταιρεία χρηματοπιστωτικών υπηρεσιών. Ήταν η 7η μεγαλύτερη τράπεζα στον κόσμο έως το 2018, και η μεγαλύτερη στην Ευρώπη, με συνολικό ενεργητικό 2.558 τρισεκατομμύρια δολάρια ΗΠΑ (από τον Δεκέμβριο του 2018). https://www.hsbc.co.uk/

σύνδεση με αριθμό ταυτοποίησης χρήστη, ή με τον κωδικό πρόσβασης. (Fraga, & De Souza, 2018: 110).

1.5. Η αποκλειστική χρήση βιομετρικών τεχνολογιών ταυτοποίησης: Το παράδειγμα της BBVA.

Η τράπεζα BBVA[10] έχει καταστήσει σαφές στους πελάτες της, ότι η χρήση βιομετρικών τεχνολογιών είναι απαραίτητη για την παροχή ορισμένων υπηρεσιών . Για παράδειγμα, η τράπεζα χρησιμοποιεί τη τεχνολογία DAS-Nano[11] η οποία σας επιτρέπει να δημιουργήσετε ένα λογαριασμό στην τράπεζα χρησιμοποιώντας μια «selfie» μέσω του «smartphone». Επιπλέον, ισχυρίζεται ότι είναι η πρώτη ευρωπαϊκή τράπεζα που προσφέρει στους πελάτες της την τεχνολογία του σαρωτή ίριδας της Samsung, Samsung Pass[12]. Αυτή η τεχνολογία επαληθεύει την ταυτότητα του χρήστη και του δίνει πρόσβαση στους λογαριασμούς του ενώ παράλληλα είναι μία από τις πιο ασφαλείς μεθόδους βιομετρικού ελέγχου ταυτότητας.

Επιπρόσθετα, η τράπεζα, χρησιμοποιεί τα βιομετρικά στοιχεία της φωνής μέσω του iPhone, και οι πελάτες της μπορούν να στείλουν χρήματα μέσω του Siri[13] μόνο με τη χρήση

[10]Το 2007, η επιχείρηση ξεκίνησε μια πρωτοβουλία για την ψηφιακή μετατροπή της τράπεζας. Μετά την εφαρμογή, παρατηρήθηκε αύξηση των νέων πελατών κατά 19% από έτος σε έτος. Από το 2015 ο συνολικός αριθμός των πελατών αυτών ανερχόταν σε 14,8 εκατομμύρια.
Το 2019, η BBVA αποφασίζει να ενοποιήσει το όνομά της παγκοσμίως και να εισαγάγει ένα νέο λογότυπο. Αυτό σήμαινε την εξαφάνιση των τοπικών ονομάτων στην Αργεντινή (Francés), στο Μεξικό (Bancomer), στο Περού (Continental) και στις Ηνωμένες Πολιτείες (Compass). Η Garanti Bank, το franchise του Ομίλου στην Τουρκία, άλλαξε το όνομά της στην Garanti BBVA

[11]Το Vali-Das είναι η σουίτα ελέγχου ταυτότητας λογισμικού που χρησιμοποιείται από κορυφαίες τράπεζες στον κόσμο για μη εξουσιοδοτημένη απομακρυσμένη πιστοποίηση ταυτότητας. Η αναγνώριση πελάτη χρησιμοποιεί τη βιομετρία προσώπου, τη βιομετρία φωνής κλπ.

[12]Το Samsung Pass είναι μια υπηρεσία διαχείρισης ταυτοτήτων, η οποία επιτρέπει την ασφαλή πρόσβαση μέσω βιομετρικού ελέγχου ταυτότητας.(Ιριδα · Δακτυλικό αποτύπωμα · Αναγνώριση προσώπου). Καθώς δεν απαιτείται πλέον εισαγωγή αναγνωριστικού και κωδικού πρόσβασης για τη σύνδεση σε τοποθεσίες web το Samsung Pass προσφέρει μια βελτιωμένη εμπειρία χρήστη, μέσω της ενσωμάτωσης προηγμένων βιομετρικών μεθόδων.Το Samsung Pass διαθέτει τεχνολογία FIDO (Fast Identity Online), η οποία διασφαλίζει την εγκυρότητα του ελέγχου ταυτότητας και προσφέρει απλές και ασφαλείς υπηρεσίες βιομετρικού ελέγχου ταυτότητας. https://www.samsung.com/gr/apps/samsung-pass/

[13]Το Siri είναι ένας εικονικός βοηθός που είναι μέρος των λειτουργικών συστημάτων iOS, της Apple Inc. Ο βοηθός χρησιμοποιεί φωνητικά ερωτήματα και έναν χρήστη φυσικής γλώσσας διεπαφής για να απαντήσει σε ερωτήσεις, να κάνει συστάσεις και να εκτελέσει ενέργειες μεταβιβάζοντας αιτήματα σε ένα σύνολο υπηρεσιών

της φωνής τους, που υποδεικνύει το όνομα της επαφής και το ποσό προς μεταφορά. (Arslanian, & Fischer, 2019: 113-121).

1.6. Βιομετρικά στοιχεία για την πρόληψη της απάτης

Αρκετές τράπεζες κάνουν χρήση της βιομετρικής τεχνολογίας για την πρόληψη της απάτης στον τομέα των πληρωμών. Τα βιομετρικά στοιχεία έχουν τη δυνατότητα να μεγιστοποιήσουν την ασφάλεια χάρη στον τρόπο με τον οποίο αποθηκεύονται τα βιολογικά δεδομένα, οπότε η χρήση τους είναι πολύ σημαντική για την προστασία των πελατών. Πολλές ευρωπαϊκές τράπεζες έχουν αρχίσει να χρησιμοποιούν στην τηλεφωνική εξυπηρέτηση πελατών, τα βιομετρικά στοιχεία της φωνής, ενώ οι πελάτες από την Ευρώπη έως τις ΗΠΑ, μπορούν να έχουν πρόσβαση στις τραπεζικές υπηρεσίες μέσω του αποτυπώματος τους, τη στιγμή που η αναγνώριση εικόνας χρησιμοποιείται στη διαδικασία εγγραφής σε τραπεζικές εφαρμογές έξυπνων συσκευών (Valkanov, 2019: 12-19).

1.7. Το τέλος της χρήσης κωδικών πρόσβασης

Στις καθημερινές μας ψηφιακές δραστηριότητες χρησιμοποιούμε σύνθετους κωδικούς προκειμένου να έχουμε πρόσβαση σε κάθε είδους λογαριασμό που διατηρούμε είτε πρόκειται για ηλεκτρονικό ταχυδρομείο είτε για τραπεζικό λογαριασμό. Ωστόσο, θα μπορούσαμε να ισχυριστούμε ότι το τέλος της χρήσης των σύνθετων και δύσχρηστων κωδικών πρόσβασης μπορεί να κρύβεται στις παρακάτω πέντε μεθόδους βιομετρικής ταυτοποίησης (Schwartz & Petrovic, 2019: 818).

Διαδικτύου. Το λογισμικό προσαρμόζεται στις προσωπικές γλωσσικές συνήθειες, τις αναζητήσεις και τις προτιμήσεις των χρηστών, με συνεχή χρήση.

1.7.1. **Σάρωση δακτυλικών αποτυπωμάτων**: είναι πιθανώς η τεχνολογία βιομετρικής επαλήθευσης την οποία έχουν συνηθίσει περισσότερο οι άνθρωποι. Η επαλήθευση δακτυλικών αποτυπωμάτων διαδραματίζει σημαντικό ρόλο στην αξιοποίηση των αστυνομικών αρχείων αλλά και στην ιατροδικαστική επιστήμη. Σήμερα πλέον κάνουμε χρήση της τεχνολογίας αυτής σε κινητά τηλέφωνα ή προκειμένου να αποκτήσουμε πρόσβαση σε κτίρια αντί να χρησιμοποιήσουμε κάρτες πρόσβασης ή κλειδιά. Όταν σαρωθεί ένα δακτυλικό αποτύπωμα, οι πληροφορίες της εικόνας επεξεργάζονται μέσω αλγορίθμων για τον εντοπισμό μοναδικών σημείων μέσα στο συγκεκριμένο δακτυλικό αποτύπωμα, ώστε να ταυτιστεί με ένα δακτυλικό αποτύπωμα που σαρώθηκε σε προηγούμενο χρόνο στην ίδια βάση δεδομένων.

1.7.2. **Η σάρωση της ίριδας**: πρόκειται για μια τεχνολογία που συναντούσαμε μόνο σε ταινίες κατασκόπων και επιστημονικής φαντασίας. Σήμερα είναι ένας ρεαλιστικός και εφαρμόσιμος τρόπος για την επαλήθευση της ταυτότητας. Αναγνωρίζοντας και ταυτοποιώντας τα μοτίβα της ίριδας, χρησιμοποιώντας μια βιομετρική βάση δεδομένων, οι σαρώσεις της ίριδας μπορούν να εκτελεστούν με μια απλή ματιά.

1.7.3. **Φωνητική επαλήθευση**: Ο τρόπος ομιλίας κάθε ατόμου είναι διαφορετικός, γεγονός που δίνει στη φωνή τη δυνατότητα να γίνει ένα ακόμα πολύτιμο στοιχείο αναγνώρισης. Το φωνητικό αποτύπωμα ενός ατόμου είναι μοναδικό, και υπάρχουν πάνω από εκατό στοιχεία που το διαφοροποιούν από κάθε άλλο. Επομένως, η βιομετρική ταυτοποίηση μέσω της φωνής θεωρείται μία από τις ασφαλέστερες μεθόδους. Επί του παρόντος, υπάρχουν περισσότεροι από 300.000.000 χρήστες που χρησιμοποιούν βιομετρικές εφαρμογές φωνής για να επαληθεύσουν την ταυτότητά τους (Dellwo, French, He, Frühholz, & Belin, 2018: 780). Ορισμένες από τις εταιρείες που χρησιμοποιούν ήδη αυτά τις βιομετρικές εφαρμογές είναι η τράπεζα HSBC και η γερμανική εταιρία τηλεπικοινωνιών Telecom. Αυτός ο τύπος

βιομετρικής τεχνολογίας λειτουργεί εντοπίζοντας ένα συγκεκριμένο φωνητικό αρχείο δεδομένων, γνωστό και ως "Φωνητικό αποτύπωμα". Με τη φωνητική επαλήθευση, ο χρήστης πρέπει μόνο να επαναλάβει μια συνθηματική φράση, η οποία στη συνέχεια συγκρίνεται με μια εγγραφή που είχε προηγουμένως παρασχεθεί από το χρήστη.

1.7.4. Βιομετρική αναγνώριση προσώπου: μέσω μιας κάμερας, το πρόσωπο ενός χρήστη σαρώνεται και έτσι χαρτογραφούνται οι διαστάσεις και οι θέσεις των χαρακτηριστικών του προσώπου. Συνοπτικά, αυτή η τεχνολογία αναλύει το πρόσωπό και στη συνέχεια το συγκρίνει με μια βάση δεδομένων εικόνων προσώπων για να ταυτοποιήσει ποιος ακριβώς είστε, δεδομένου ότι το συγκεκριμένο πρόσωπο έχει ήδη εγγραφεί στη συγκεκριμένη βάση δεδομένων. Η βιομετρική αναγνώριση προσώπου μπορεί να χρησιμοποιηθεί από τον έλεγχο ασφαλείας των αεροδρομίων για να εντοπίσει άτομα που βρίσκονται σε λίστα εξαίρεσης εξόδου από τη χώρα μέχρι στην καθημερινή χρήση του έξυπνου κινητού μας τηλεφώνου για να αποκτήσουμε πρόσβαση σε αυτό.

1.7.5. Αναγνώριση φλεβών[14]: Το γεγονός ότι το κυκλοφορικό σύστημα κάθε ατόμου είναι μοναδικό και ότι οι φλέβες βρίσκονται κάτω από το δέρμα καθιστά την αναγνώριση φλεβών μια μέθοδο βιομετρικής ταυτοποίησης η οποία είναι εξαιρετικά δύσκολο να παραβιαστεί κακόβουλα δηλαδή να χακαριστεί. Η τεχνολογία αναγνώρισης των φλεβών λειτουργεί γενικά αναλύοντας τα μοτίβα (σχήμα, πάχος, λεπτομέρειες) των φλεβών ενός δακτύλου, της παλάμης ,του χεριού ή του ματιού, και στη συνέχεια, φυσικά, εκτελείται η αναζήτηση αντίστοιχου μοτίβου σε μια βιομετρική βάση δεδομένων.

[14]το LG G8 ThinQ είναι το πρώτο smartphone στον κόσμο με σύστημα αναγνώρισης των φλεβών του χρήστη για ξεκλείδωμα της συσκευής, το οποίο ονομάζεται HandID. Ουσιαστικά, αναγνωρίζει το σχήμα, το πάχος και άλλες λεπτομέρειες των φλεβών στην παλάμη του χρήστη για να το ξεκλειδώσει. Επομένως, έχουμε τρεις τρόπους βιομετρικού ξεκλειδώματος: αναγνώριση αποτυπωμάτων, προσώπου και φλεβών.https://www.lg.com/us/lg-thinq

Κάθε είδος τεχνολογίας βιομετρικής ταυτοποίησης έχει τα ισχυρά και τα αδύνατα σημεία του, αλλά το σημαντικό είναι ότι προστατεύουν από την πλαστοπροσωπία ή από την πειρατεία ηλεκτρονικών λογαριασμών. Αυτό θα μπορούσε να σημαίνει ένα μέλλον χωρίς κωδικούς πρόσβασης και έναν συνδυασμό αρκετών βιομετρικών τεχνολογιών για να διασφαλιστεί η ταυτοποίηση μας.

1.8. Τεχνικά στάδια της βιομετρικής αναγνώρισης

Πριν από την υιοθέτηση ενός βιομετρικού συστήματος αναγνώρισης, είναι σημαντικό να εξετάσουμε την ισχύουσα νομοθεσία σε κάθε χώρα. Για παράδειγμα, η βιομετρική αναγνώριση είναι μια διαδικασία που απαιτεί την επεξεργασία προσωπικών δεδομένων που θεωρούνται "ευαίσθητα" για κάθε πολίτη της Ευρωπαϊκής Ένωσης, όπως προβλέπεται στον γενικό κανονισμό για την προστασία των δεδομένων (άρθρο 9) στον οποίο θα γίνει εκτενής αναφορά σε επόμενο κεφάλαιο.

Οπότε θα πρέπει να λαμβάνονται οι ακόλουθες προφυλάξεις:

- Διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων.
- Να δικαιολογείται επαρκώς η αναγκαιότητα για τη χρήση βιομετρικών στοιχείων
- Να αναφέρεται ρητά στο αρχείο δραστηριοτήτων της εταιρείας.
- Να υπάρχει επαρκής προηγούμενη ενημέρωση των υποκειμένων
- Να προτιμάται η χρήση ενός μοτίβου δακτυλικών αποτυπωμάτων που αποθηκεύεται σε κάρτες σε σχέση με μια μαζική αποθήκευση σε ένα διακομιστή.

1.9. Η λειτουργία της σάρωσης δακτυλικών αποτυπωμάτων

Πρώτον, ο χρήστης πρέπει να καταχωρήσει το αποτύπωμά του για μελλοντικούς ελέγχους (1:1) ή ταυτοποιήσεις (1: N). Ο χρήστης μπορεί να εγγραφεί τοποθετώντας το

δάχτυλό του σε μια συσκευή αναγνώρισης δακτυλικών αποτυπωμάτων , όπως ένα οπτικό ποντίκι με δακτυλικό αποτύπωμα ή μια συσκευή ελέγχου πρόσβασης. Ο αισθητήρας ψηφιοποιεί το δάχτυλο του χρήστη και συλλαμβάνει την τρισδιάστατη εικόνα του αποτυπώματος. Ο συγκεκριμένος αλγόριθμος εξάγει συγκεκριμένα σημεία από την εικόνα και μετατρέπει τις πληροφορίες σε ένα μοναδικό μαθηματικό μοντέλο, συγκρίσιμο με έναν κωδικό πρόσβασης με 60 ψηφία. Αυτό το μοναδικό μοντέλο κρυπτογραφείται και αρχειοθετείται για να εκπροσωπεί το χρήστη. Δεν αποθηκεύεται καμία συγκεκριμένη εικόνα του αποτυπώματος.

Στη συνέχεια, για την επαλήθευση, ένας εγγεγραμμένος χρήστης καθορίζει ποιος είναι (πληκτρολογεί ένα αναγνωριστικό χρήστη) και τοποθετώντας το δάχτυλό του στον αισθητήρα, καταγράφεται μια νέα εικόνα του αποτυπώματος του χρήστη. Συγκεκριμένα δεδομένα εξάγονται από το δακτυλικό αποτύπωμα και μετατρέπονται σε δείγμα. Το δείγμα αυτό συγκρίνεται με το προεγγεγραμμένο δείγμα χρήστη για να ελέγξει την συμβατότητα. Εάν το δείγμα αντιστοιχεί, ο χρήστης επαληθεύεται θετικά.

Για την ταυτοποίηση, ο χρήστης τοποθετεί το δάχτυλό του στον αισθητήρα χωρίς να ενημερώνει την ταυτότητά του (δεν εισάγει κανένα αναγνωριστικό χρήστη). Το νέο δείγμα που εξάγεται συγκρίνεται με τα ήδη υφιστάμενα δείγματα. Εάν εντοπιστεί συμβατότητα, ο χρήστης προσδιορίζεται ως ήδη εγγεγραμμένος.

1.10. Πρότυπο βιομετρικής διαδικασίας ταυτοποίησης σε δημόσιες υπηρεσίες

1. Επίδειξη ταυτότητας

2. Εξουσιοδότηση για την επεξεργασία των προσωπικών σας δεδομένων

3.Το έγγραφο ταυτότητάς σαρώνεται για να εξαγάγει το όνομα, το επώνυμο και τα δεδομένα του αριθμού ταυτοποίησης

5. Τα δακτυλικά αποτυπώματα καταγράφονται

6. Το αποτύπωμα ελέγχεται από τη βάση δεδομένων του εθνικού μητρώου

7.Υπογραφή του ηλεκτρονικού έγγραφου, χρησιμοποιώντας την οθόνη ψηφιοποίησης

8. Μετά την επικύρωση των πληροφοριών του εγγράφου, ο υπάλληλος θα εγκρίνει το έγγραφο με την ψηφιακή υπογραφή του.

1.11. Επιβεβαίωση της μοναδικότητας

Η κύρια λειτουργία των βιομετρικών τεχνολογιών είναι η καταχώριση του φυσικού χαρακτηριστικού του προσώπου που πρόκειται να χρησιμοποιηθεί σε διαφορετικές εφαρμογές ελέγχου πρόσβασης , όπου απαιτείται άδεια ή έλεγχος των ατόμων που εισέρχονται και εξέρχονται από μια ορισμένη περιοχή. Η βιομετρική τεχνολογία μέσω του ελέγχου πρόσβασης μπορεί επίσης να ελέγξει την παρουσία. Ανάλογα με τον τομέα στον οποίο εκτελείται ο έλεγχος πρόσβασης, τα βιομετρικά προγράμματα ανάγνωσης ενδέχεται να ποικίλλουν. Για παράδειγμα, η βιομετρία αναγνώρισης προσώπου είναι σκόπιμη για εκείνους τους τομείς όπου ή επαφή με άλλα προϊόντα αποτρέπουν την αναγνώριση δακτυλικών αποτυπωμάτων.

Η λειτουργία της βιομετρικής ως πεδίου τεχνητής νοημοσύνης είναι η ταυτοποίηση ενός ατόμου μέσω ορισμένων παραμέτρων του σώματός του, τα οποία είναι φυσικά και μη μεταβιβάσιμα, όπως η αναγνώριση δακτυλικών αποτυπωμάτων ή προσώπου (Douglas, Bailey, Leeney, & Curran, 2018:173).

Η ανάγκη για ασφάλεια έχει γίνει πιο επιτακτική με την αλματώδη άνοδο του διαδικτύου, τις ηλεκτρονικές αγορές, τις τραπεζικές συναλλαγές μέσω του διαδικτύου, και φυσικά μετά τις επιθέσεις της 11ης Σεπτεμβρίου στις ΗΠΑ. Οι τεχνολογίες βιομετρικής ταυτοποίησης αποτελούν το μέλλον των συστημάτων ασφαλείας και η ανάπτυξή τους τα τελευταία χρόνια έχει παρουσιάσει γεωμετρική πρόοδο σε σύγκριση με άλλες τεχνολογίες ασφαλείας. Η δυνητική υψηλή αποτελεσματικότητά τους, τις καθιστά ιδιαίτερα ελκυστικές

σε τομείς, όπου χρησιμοποιούνται ήδη βιομετρικά συστήματα (Ozuem, Howell, & Lancaster, 2018: 52).

1.11.1. Χρηματοπιστωτικά ιδρύματα: είναι ίσως ένας από τους τομείς που ιστορικά ανησυχεί ιδιαίτερα για την ασφάλεια, για την αποφυγή της απάτης και της απώλειας χρημάτων. Επομένως, ορισμένα χρηματοπιστωτικά ιδρύματα έχουν ήδη αρχίσει να επενδύουν σε μεγάλο βαθμό στα βιομετρικά συστήματα. Σε τράπεζες όπως η Bank of America και σε χρηματοπιστωτικά ιδρύματα, όπως η VISA ή η MasterCard, έχουν ήδη εφαρμοστεί συστήματα αναγνώρισης της ίριδας ή των φλεβών για την αντιμετώπιση των μεγάλων απωλειών που οφείλονται εν μέρει στην ανεπαρκή ασφάλεια των συστημάτων που χρησιμοποιήθηκαν μέχρι στιγμής.

1.11.2. Ηλεκτρονικό εμπόριο και ηλεκτρονικές τραπεζικές συναλλαγές. Αυτός είναι ένας από τους τομείς που εκτοξεύτηκε τα τελευταία χρόνια, και αυτός που επηρέασε περισσότερο την ανάπτυξη νέων συστημάτων ασφαλείας. Ο σχεδιασμός σε αυτόν τον τομέα αποσκοπεί στη μείωση των τιμών πώλησης των συσκευών βιομετρικής αναγνώριση σε βαθμό που αυτές να αποτελούν μέρος του υπολογιστή, ενσωματωμένο ακόμη και μέσα σε ένα ποντίκι ή πληκτρολόγιο, ή άλλο εξοπλισμό, όπως κινητά τηλέφωνα ή PDA. Ερευνάται επίσης η πιθανότητα της αναγνώρισης του αποτυπώματος, κατά της διάρκειας της πληκτρολόγησης από το χρήστη.

1.11.3. Τουρισμός και ταξίδια. Οι πρόσφατες συμφωνίες αρκετών κρατών σχετικά με τους κανονισμούς για την πρόσβαση στην ελεύθερη ζώνη διέλευσης των αερολιμένων έχει δημιουργήσει την ανάγκη να αναζητήσουμε άλλες μεθόδους ασφάλειας διαφορετικές από τις σημερινές. Αυτές οι εφαρμογές θα παρουσιαστούν λεπτομερώς αργότερα.

1.11.4. Ηλεκτρονική ταυτότητα. Θα ήταν αναμφίβολα η πλέον επαναστατική εφαρμογή της βιομετρικής τεχνολογίας: ένα βιομετρικό δελτίο ταυτότητας ή διαβατήριο θα

σηματοδοτούσε την εξάλειψη των καρτών, οι οποίες θα μπορούσαν να αντικατασταθούν για παράδειγμα από την ίριδα του κατόχου. Όπως αναφέρθηκε νωρίτερα, όσον αφορά την ασφάλεια των αερολιμένων, υπάρχουν ανάλογες εφαρμογές που ήδη λειτουργούν σε διάφορα αεροδρόμια του κόσμου.

1.11.5. Σάρωση του αμφιβληστροειδούς. Το βρετανικό αεροδρόμιο του Χίθροου επιλέχθηκε για την εφαρμογή ενός συστήματος αναγνώρισης ίριδας και επιτρέπει στους χρήστες να ταυτοποιούνται σε πραγματικό χρόνο μέσω μιας τράπεζας δεδομένων που έχουν ήδη συλλεχθεί. Το σύστημα βιομετρικών στοιχείων που εφαρμόζεται στην ταυτοποίηση βασίζεται τα ήδη αποθηκευμένα στοιχεία.

1.12. Case Studies σάρωσης ίριδας οφθαλμού

Η πλέον ενδιαφέρουσα εφαρμογή αναγνώρισης ίριδας έχει χρησιμοποιηθεί σε ATM για την επαλήθευση της ταυτότητας των πελατών μιας τράπεζας, όπως συμβαίνει για παράδειγμα με τα νέα ATM της Ancoria Bank[15] στην Κύπρο. Ο πελάτης πρέπει να τοποθετηθεί μπροστά από αυτό το ATM, έτσι ώστε το σύστημα αναγνώρισης ίριδας να τον αναγνωρίσει. Το σύστημα, επομένως, φωτογραφίζει το μάτι και μετατρέπει την εικόνα σε ψηφία. Μόλις μετατραπούν σε κώδικα, οι πληροφορίες αυτές αντιπαραβάλλονται με τα δεδομένα που είναι αποθηκευμένα στο database της τράπεζας, το οποίο επιβεβαιώνει αν ο χρήστης είναι ο πραγματικός κάτοχος της κάρτας. Έτσι, το σύστημα δημιουργεί μια ψηφιακή εικόνα της ίριδας του πελάτη η οποία καταγράφεται στη μαγνητική λωρίδα ή στο τσιπ της κάρτας με τη νέα ενσωματωμένη λειτουργικότητα. Με αυτόν τον τρόπο, επιτυγχάνεται μεγαλύτερη ασφάλεια όσον αφορά την πρόσβαση σε οικονομικά δεδομένα, δεδομένου ότι, εάν το

[15] Τα νέα ATM της Ancoria Bank ονομάζονται Self-Service Kiosks. Είναι βιομετρικά και δεν χρειάζεται ο πελάτης να έχει μαζί του την κάρτα του για να κάνει ανάληψη χρημάτων ή οποιαδήποτε άλλη τραπεζική συναλλαγή. https://www.ancoriabank.com/

αποτύπωμα της ίριδας του χρήστη δεν ταιριάζει με αυτό που έχει καταχωρηθεί στο database της τράπεζας, η εντολή απορρίπτεται.

Η Royal Bank of Canada[16] είναι μια ακόμη τράπεζα που χρησιμοποιεί ATM αυτού του τύπου, το οποίο δημιούργησε ο τεχνολογικός κολοσσός NCR[17]. Ονομάζεται Stella[18] και είναι σε θέση να αναγνωρίσει τον χρήστη, να τον χαιρετήσει με το όνομά του, να τον ακούσει, να του μιλήσει, να του παρουσιάσει ένα προσωπικό μενού με τις αγαπημένες του υπηρεσίες και λειτουργίες, και ακόμη και να του ευχηθεί για τα γενέθλιά του αν αποφασίσει να κάνει οποιαδήποτε οικονομική συναλλαγή την ημερομηνία αυτή. Οι νέες τεχνολογίες στις οποίες βασίζεται το ATM Stella περιλαμβάνουν το σύστημα αναγνώρισης ίριδας, την αναγνώριση φωνής -η οποία επιτρέπει τη συζήτηση με το τερματικό όπως με έναν υπάλληλο της Τράπεζας- και ένα ολοκληρωμένο σύστημα ικανό να επικοινωνεί με το κινητό τηλέφωνο του χρήστη και να μεταφορτώνει τις πληροφορίες των τελευταίων εργασιών που πραγματοποιήθηκαν στον προσωπικό ψηφιακό βοηθό (PDA) του χρήστη/πελάτη.

Ως εκ τούτου, οι δυνατότητες που προσφέρει αυτή η νέα τεχνολογία εκτιμώνται ιδιαίτερα από τους περισσότερους χρήστες της. Στην πραγματικότητα, η αποδοχή του συστήματος αναγνώρισης ίριδας στις δοκιμαστικές δοκιμές ATM που εγκατέστησε η NCR στην βρετανική τράπεζα British bank Nationwide Building Society[19] ήταν τεράστια. Σύμφωνα με μελέτη του ομίλου Pegram Walters[20], που διεξήχθη μεταξύ 1.000 πελατών, για

[16] Η Βασιλική Τράπεζα του Καναδά είναι μια καναδική πολυεθνική εταιρία χρηματοπιστωτικών υπηρεσιών και η μεγαλύτερη τράπεζα στον Καναδά σε κεφαλαιοποίηση της αγοράς. Η τράπεζα εξυπηρετεί πάνω από 16 εκατομμύρια πελάτες και έχει 80.000 υπαλλήλους παγκοσμίως. https://www.rbcroyalbank.com/personal.html

[17] Η NCR Corporation, γνωστή στο παρελθόν ως National Cash Register, και για μια σύντομη περίοδο γνωστή ως AT & T Global Information Solutions, είναι μια αμερικανική τεχνολογική εταιρεία που κατασκευάζει περίπτερα αυτοεξυπηρέτησης, τερματικά σημείων πώλησης, αυτοματοποιημένες ταμειακές μηχανές, σαρωτές γραμμωτού κώδικα και αναλώσιμα για επιχειρήσεις. https://www.ncr.com/

[18] Σχεδιασμένο από επιστήμονες και μηχανικούς στο εργαστήριο Advanced Solutions Concepts της NCR στο Νταντί της Σκωτίας, αυτό το "concept ATM" αλληλεπιδρά με τους πελάτες του κατά τη διάρκεια των συναλλαγών.Ο Rick Makos, αντιπρόεδρος οικονομικών για την NCR, δήλωσε ότι οι αντιδράσεις των καταναλωτών στην Stella ήταν κυρίως θετικές κατά τη διάρκεια της εβδομαδιαίας δοκιμαστικής περιόδου. https://www.atmmarketplace.com/articles/new-girl-in-town/

[19] Η Nationwide Building Society είναι βρετανικό χρηματοπιστωτικό ίδρυμα, το έβδομο μεγαλύτερο συνεταιριστικό χρηματοπιστωτικό ίδρυμα και η μεγαλύτερη οικοδομική εταιρεία στον κόσμο με περισσότερα από 15 εκατομμύρια μέλη.

[20] Βρετανική εταιρεία διεθνούς έρευνας αγοράς

διάστημα έξι μηνών, στο Ηνωμένο Βασίλειο, όλοι οι χρήστες του ATM θεωρούν ότι το σύστημα είναι αξιόπιστο και ασφαλές.

1.13. Συμπεριφορική Βιομετρία

Εκτός από την βιομετρική ταυτοποίηση και τη βιομετρική υπογραφή, αρκετές εταιρείες έχουν αρχίσει να αξιοποιούν τη αυμπεριφορική βιομετρία. Η συμπεριφορική βιομετρία είναι το πεδίο μελέτης που σχετίζεται με το μέτρο της μοναδικής αναγνώρισης των μετρήσιμων μοτίβων στις ανθρώπινες δραστηριότητες. Ο όρος έρχεται σε αντίθεση με τη φυσική βιομετρία, η οποία περιλαμβάνει εγγενή ανθρώπινα χαρακτηριστικά, όπως δακτυλικά αποτυπώματα ή μοτίβα ίριδας. Είναι φυσιολογικό να πας σε ένα μπαρ, και όταν ο σερβιτόρος σε δει και τσεκάρει τι ώρα είναι, να σου σερβίρει τον αγαπημένο σου καφέ. Αυτό επιτυγχάνεται με την ακόυσια χρήση της συμπεριφορικής βιομετρίας. Αν μεταξύ 3 και 5 κάθε μήνα, χρησιμοποιώ εφαρμογές ηλεκτρονικής τραπεζικής προκειμένου να κάνω μια συγκεκριμένη μεταφορά χρημάτων, η ενέργεια αυτή εμπίπτει στο πεδίο της συμπεριφορικής βιομετρίας. Διαθέτουμε στοιχεία για την τοποθεσία, δράση, χρονικό διάστημα, ενδιαφέρον ή επιθυμία. Αν λοιπόν ένας υπολογιστής αναγνωρίζει αυτό το προφίλ ή μοτίβο, θα μπορεί να αναγνωρίσει και αν αυτός που επιχειρεί να τον χρησιμοποιήσει είναι και πραγματικός κάτοχος του. Διάφορες εταιρείες σε όλο τον κόσμο όπως η Biocatch[21] στο Ισραήλ και η Behaviosec[22] στη Σουηδία που ειδικεύονται στην ανάπτυξη βιομετρικών συστημάτων ταυτοποίησης, εξετάζουν την πιθανότητα ανάπτυξης ενός τέτοιου συστήματος ασφαλείας. (Shrobe, Shrier, & Pentland, 2018: 365-377).

[21] https://www.biocatch.com/
[22] https://www.behaviosec.com

1.14. Εικόνες προσώπου ως βιομετρικά δεδομένα

Η αναγνώριση προσώπου είναι ένα σύστημα αναγνώρισης που μπορεί να ταυτοποιήσει ένα άτομο από τα χαρακτηριστικά του προσώπου του. Βασίζεται στη χρήση ενός αλγορίθμου που αναλύει τα χαρακτηριστικά του προσώπου του ατόμου και τα συγκρίνει με τα υπόλοιπα άτομα που περιλαμβάνονται στη βάση δεδομένων (Steiner, 2018: 735).

Το άτομο αναγνωρίζεται μέσω μιας εικόνας ή μιας φωτογραφίας και το πρόσωπο αναλύεται με ειδικά προγράμματα υπολογισμού ώστε να είναι σε θέση να κάνει τη σύγκριση με την εικόνα ή τη φωτογραφία που έχει ήδη ληφθεί. Σε αυτές τις περιπτώσεις, θα πρέπει να ληφθούν υπόψη οι αλλοιώσεις που προκαλεί η ηλικία στα πρόσωπα, αλλά και οι καθημερινές αλλαγές στην εμφάνιση ενός ατόμου όπως η χρήση φακών οράσεως, αλλαγή χτενίσματος κλπ.(Steiner, 2018: 736).

1.15. Προγράμματα αναγνώρισης προσώπου

Υπάρχει μια μεγάλη ποικιλία λογισμικών αναγνώρισης προσώπου. Οι εφαρμογές και τα προγράμματα που επιτρέπουν σε ένα άτομο να αναγνωριστεί από τα χαρακτηριστικά του προσώπου του πολλαπλασιάζονται μέρα με τη μέρα και κάποιες από αυτές τις εφαρμογές είναι δωρεάν (Hurst, 2018: 701-706).

1.15.1. Κοινωνικός χαρτογράφος (Social Mapper)

Το Social Mapper είναι μία εφαρμογή ανοιχτού κώδικα που αναζητά πληροφορίες προφίλ από ιστοτόπους κοινωνικής δικτύωσης, όπως το Facebook, το Instagram, το LinkedIn, το Google+, κλπ. Η εφαρμογή χρησιμοποιεί ως πηγή πληροφορίας ονόματα και φωτογραφίες και πραγματοποιεί σάρωση των προφίλ των κοινωνικών μέσων μαζικής

δικτύωσης του ορισμένου υποκειμένου. Χρειάζονται περίπου 60-70 δευτερόλεπτα για τη σάρωση ενός προφίλ βάσει των παρεχόμενων ονομάτων και φωτογραφιών[23].

Είναι μια εφαρμογή που λόγω των δυνατοτήτων της, θα μπορούσε να χρησιμοποιηθεί για phishing[24], αν και οι δημιουργοί της ισχυρίζονται ότι απευθύνεται σε ηθικούς και επαγγελματίες χάκερ[25] στον τομέα της ασφάλειας.

1.15.2. Open face

Το Open face είναι ένα πρόγραμμα αναγνώρισης προσώπου ανοιχτού κώδικα σχεδιασμένο από το Πανεπιστήμιο Carnegie Mellon της Πενσυλβάνια, το οποίο επιτρέπει την αναγνώριση ενός ατόμου μέσω φωτογραφιών. Τα smart κινητά τηλέφωνα έχουν ήδη ενσωματώσει αυτό το είδος τεχνολογίας, όπως το σύστημα αναγνώρισης προσώπου Xiaomi που χρησιμοποιεί η κινεζική εταιρεία στις συσκευές της (για παράδειγμα σε μοντέλα όπως το Mi Mix 2S ή το Mi 8)[26].

[23] Wilkin Jacob, 2018, *Mapping Social Media with Facial Recognition: A New Tool for Penetration Testers and Red Teamers*, https://www.trustwave.com

[24] Το Phishing είναι ενέργεια εξαπάτησης των χρηστών του διαδικτύου, κατά την οποία ο 'θύτης' υποδύεται μία αξιόπιστη οντότητα, καταχρώμενος την ελλιπή προστασία που παρέχουν τα ηλεκτρονικά εργαλεία, και την άγνοια του χρήστη-'θύματος', με σκοπό την αθέμιτη απόκτηση προσωπικών δεδομένων, όπως είναι ευαίσθητα ιδιωτικά στοιχεία και κωδικο

[25] Οι ηθικοί χάκερς είναι άνθρωποι της hacking κοινότητας που εισβάλλουν σε κάποιο σύστημα στα πλαίσια των ηθικών αρχών για να αναγνωρίσουν ποια είναι τα τρωτά σημεία, οι οποίοι είναι γνωστοί και ως white hat hackers. Οι white hats είναι οι hacker που χρησιμοποιούν την ικανότητά τους σαφώς κατά ηθικό τρόπο. Είναι παραδείγματος χάρη, οι υπάλληλοι εταιρειών, οι οποίοι έχουν άδεια να επιτίθενται στα δίκτυο και τα συστήματα της εταιρείας τους για τον καθορισμό των αδυναμιών. Επίσης white hats, είναι και οι πράκτορες της μυστικής υπηρεσίας που χρησιμοποιούν τις ικανότητές τους ή για τη διερεύνηση και την επίλυση διάφορων εγκλημάτων. Έχουν, δηλαδή, καθήκον να χρησιμοποιούν τις γνώσεις τους με τέτοιο τρόπο, ώστε να επωφεληθούν άλλοι άνθρωποι ή υπηρεσίες. http://www.infowar.com/hacker/99/HackerTaxonomy.

[26] https://findbiometrics.com/xiaomi-display-fingerprint-scanning-infrared-facial-recognition-505313/

1.15.3. Blippar

Το Blippar είναι μια εφαρμογή επαυξημένης πραγματικότητας και τεχνητής νοημοσύνης που επιτρέπει στον χρήστη να αναγνωρίζει όλα τα είδη των αντικειμένων, φυτών, ή και ζώων. Μεταξύ των λειτουργιών του είναι επίσης η αναγνώριση προσώπου[27].

1.15.4. Αναγνώριση προσώπου σε Online σύνδεση

Έχετε αναρωτηθεί ποτέ, πώς είναι δυνατόν το Facebook ή η Google να αναγνωρίζουν το πρόσωπό σας; Είναι επειδή χρησιμοποιούν όλο και πιο εξελιγμένες online εφαρμογές αναγνώρισης προσώπου. Στην πραγματικότητα, από το 2015, οι δύο εταιρείες βρίσκονται σε έναν σιωπηλό ψυχρό πόλεμο σε αυτόν τον τομέα με τις αντίστοιχες εφαρμογές τους. Πρώτο ήταν το Facebook που παρουσίασε την εφαρμογή DeepFace[28]. Η ομάδα έρευνας του Facebook δήλωσε ότι η μέθοδος DeepFace φτάνει σε ποσοστό ακρίβειας το 97,35% σε σύγκριση με το 85% που φτάνει το σύστημα αναγνώρισης δεύτερης γενιάς του FBI. Ωστόσο, η Google αντεπιτέθηκε με το FaceNet[29], ένα πρόγραμμα που επιτρέπει στον γίγαντα του διαδικτύου να αναγνωρίζει πρόσωπα με ποσοστό επιτυχίας 99,96%.

[27] Όπως αναφέρει η ίδια εταιρία «Μέσα από το βασίλειο της επαυξημένης πραγματικότητας και της τεχνητής νοημοσύνης, το Blippar σας βοηθάει να δείτε, να βιώσετε και να μάθετε περισσότερα από τον κόσμο. Καλώς ήλθατε στον κόσμο του μέλλοντος! Ξεκλειδώστε εμπειρίες επαυξημένης πραγματικότητας από καθημερινά αντικείμενα και μέρη με την εφαρμογή Blippar. Σαρώστε και δείτε τι μπορείτε να ανακαλύψετε. Μήπως έχετε δει μια διασημότητα αλλά δεν μπορείτε να την αναγνωρίσετε; ένα λογότυπο για το οποίο θέλετε να μάθετε περισσότερα ή αυτόν τον αξιαγάπητο σκύλο; Ή ποιος ζωγράφισε αυτό το καταπληκτικό έργο τέχνης; Σαρώστε τα με το blippar για να μάθετε περισσότερα.»
https://play.google.com/store/apps/details?id=com.blippar.ar.android&hl=el

[28] Το DeepFace είναι ένα σύστημα αναγνώρισης προσώπου μηχανικής μάθησης που δημιουργήθηκε από μια ερευνητική ομάδα στο Facebook. Χρησιμοποιεί ένα νευρωνικό δίχρωμο στρώμα με πάνω από 120 εκατομμύρια ζεύγη συνδέσεων, αντλώντας πληροφορίες απο τέσσερα εκατομμύρια εικόνες που έχουν ανεβάσει χρήστες του Facebook. Russell Brandom (July 7, 2014), "Why Facebook is beating the FBI at facial recognition", The Verge

[29] Το FaceNet είναι ένα σύστημα αναγνώρισης προσώπου που αναπτύχθηκε το 2015 από ερευνητές της Google. Το σύστημα FaceNet μπορεί να χρησιμοποιηθεί για την εξαγωγή χαρακτηριστικών υψηλής ποιότητας από πρόσωπα, που ονομάζονται εμπλουτισμοί προσώπου, τα οποία στη συνέχεια μπορούν να χρησιμοποιηθούν για την εκπαίδευση ενός συστήματος ταυτοποίησης προσώπου. https://machinelearningmastery.com

1.15.5. Αναζήτηση ατόμων μέσω φωτογραφιών

Το Social Mapper μπορεί να είναι το καλύτερο πρόγραμμα αναγνώρισης προσώπου αλλά δεν είναι το μόνο. Πολλές άλλες αντίστοιχες εφαρμογές διατίθενται, τόσο για υπολογιστές όσο και για κινητές συσκευές. Μία από αυτές τις ηλεκτρονικές εφαρμογές είναι η Tin Eye[30]. Σας επιτρέπει να ανεβάσετε τη φωτογραφία ενός ατόμου και να αναζητήσετε εικόνες παρόμοιες με την αρχική σε όλο το διαδίκτυο. Υπάρχουν επίσης εφαρμογές για την αναζήτηση ατόμων μέσω φωτογραφιών στα κοινωνικά δίκτυα. Ένα από αυτά είναι η Find-Face[31], μια εφαρμογή που δημιουργήθηκε από έναν Ρώσο προγραμματιστή σε συνεργασία με το Twitter, η οποία σας επιτρέπει να ανεβάσετε μια εικόνα ενός ατόμου και να εκτελέσετε μια αναζήτηση για αναγνώριση του μέσω των κοινωνικών δικτύων. Η τεχνολογία στον εν λόγω τομέα αναπτύσσεται με αλματώδεις ρυθμούς και αυτό καθιστά όλο και πιο δύσκολο τη διατήρηση της ανωνυμίας του ατόμου, ακόμη και εάν αυτή είναι η επιθυμία του (Ford, & Campbell, 2018: 135).

[30] Το TinEye είναι μια μηχανή αντίστροφης αναζήτησης εικόνας που αναπτύχθηκε από την Idée, Inc., μια εταιρεία που εδρεύει στο Τορόντο του Καναδά. Είναι η πρώτη μηχανή αναζήτησης εικόνων που χρησιμοποιεί τεχνολογία αναγνώρισης εικόνων και όχι λέξεις-κλειδιά, μεταδεδομένα ή υδατογραφήματα. Με την υποβολή μιας εικόνας, το TinEye δημιουργεί μια "μοναδική και συμπαγή ψηφιακή υπογραφή ή δακτυλικό αποτύπωμα" της εικόνας και την ταιριάζει με άλλες ευρετηριασμένες εικόνες. https://www.tineye.com/

[31] Η FindFace είναι μια τεχνολογία αναγνώρισης προσώπου που αναπτύχθηκε από τη ρωσική εταιρεία NtechLab που ειδικεύεται σε λύσεις νευρωνικών δικτύων.

2. ΚΕΦΑΛΑΙΟ ΔΕΥΤΕΡΟ –

Νομικό πλαίσιο της Βιομετρικής

2.1. Ιδιωτικότητα και το Δικαίωμα προστασίας του απορρήτου και των προσωπικών δεδομένων

Η βιομετρική ταυτοποίηση και επαλήθευση αποτελούν πλέον τεχνολογίες αιχμής, κομβικές για την απλοποίηση καθημερινών διαδικασιών και διαφαίνεται καθαρά ότι θα διαδραματίσουν πρωταγωνιστικό ρόλο στο άμεσο μέλλον όπου θα κυριαρχήσει η τεχνητή νοημοσύνη (AI) και το διαδίκτυο των πραγμάτων (IoT)[32]. Επί του παρόντος, η βιομετρική τεχνολογία εφαρμόζεται σε διάφορες περιπτώσεις και καταστάσεις με κύριο στόχο την απλούστευση των διαδικασιών αλλά και την ασφάλεια των συναλλαγών. Συναντούμε όλο και συχνότερα για παράδειγμα σαρωτές ίριδας στα σημεία ελέγχου ασφαλείας των αεροδρομίων, σαρωτές δακτυλικών αποτυπωμάτων για να αποκτήσουμε πρόσβαση σε ένα κτίριο γραφείων, τεχνολογία αναγνώρισης φωνής μέσα στα αυτοκίνητα ακόμη και σάρωση φλεβών για τη διαχείριση συναλλαγών και ευαίσθητων πληροφοριών μέσω έξυπνων συσκευών. Τα προσεχή έτη, θα αρχίσουμε να χρησιμοποιούμε όλο και περισσότερες τεχνολογίες βιομετρικής αναγνώρισης ως μέρος της καθημερινής μας ρουτίνας, γεγονός που προοιωνίζει την οριστική εξάλειψη των κωδικών πρόσβασης (Beaudet, Rieul, Fourre, & Chastel, 2019: 657).

[32] Το Ίντερνετ των πραγμάτων (IoT) είναι ένα σύστημα αλληλένδετων υπολογιστικών συσκευών, μηχανικών και ψηφιακών μηχανών, αντικειμένων, ζώων ή προσώπων που διαθέτουν μοναδικά αναγνωριστικά στοιχεία (UID) και τη δυνατότητα μεταφοράς δεδομένων μέσω δικτύου χωρίς να απαιτείται ανθρώπινη αλληλεπίδραση ή αλληλεπίδραση ανθρώπου με υπολογιστή. Rouse, Margaret (2019). "internet of things (IoT)". IOT Agenda.

Ωστόσο, η έως σήμερα προσέγγιση των δεδομένων προσωπικού χαρακτήρα στο κανονιστικό και ρυθμιστικό πλαίσιο των βιομετρικών δεδομένων είναι τουλάχιστον ανεπαρκής.

Παγκοσμίως ο ευαίσθητος τομέας της ιδιωτικής ζωής, του σεβασμού της ιδιωτικότητας και της διαχείρισης των προσωπικών πληροφοριών, δεν προστατεύεται απο ένα διεξοδικό και ισχυρό νομοθετικό πλαίσιο.

2.2. Η νομική αντιμετώπιση του ανθρώπινου σώματος ως αντικείμενο «ιδιοκτησίας»

Μια εναλλακτική λύση είναι να στραφούμε στη βιοηθική αναζητώντας μια απάντηση και να αναλύσουμε τις παραμέτρους κάτω από τις οποίες ρυθμίζεται κανονιστικά το πεδίο διαχείρισης του ανθρωπίνου σώματος και των ανθρωπίνων μελών και οργάνων. Στον τομέα της ιατρικής, συζητείται επίσης η εφαρμογή ενός ιδιοκτησιακού μοντέλου με βάση το εμπράγματο δίκαιο (το οποίο θα επέτρεπε στα άτομα να διατηρήσουν τον έλεγχο των τμημάτων του σώματός τους που έχουν αφαιρεθεί). Ένα τέτοιο μοντέλο, αν και μπορεί να προστατεύσει ένα άτομο από την πράξη της αφαίρεσης τμημάτων του σώματός του παρά τις επιθυμίες του, δεν παρέχει προστασία σε αυτά μόλις αφαιρεθούν (Herring & Chau, 2007: 34-61).

Η νομική έννοια της ιδιοκτησίας είναι ένα ισχυρό νομικό εργαλείο για τον έλεγχο ενός αγαθού, ωστόσο φέρει το σημασιολογικό βάρος του εμπορίου και της αγοράς. Ένα αγαθό που μπορεί να αποτελέσει αντικείμενο κτήσης και κυριότητας είναι ένα αγαθό που εμπίπτει στις αρχές του εμπορίου, και αυτό εγείρει μια ηθική σύγκρουση (De Witte & Ten Have, 1997: 55). Για μερικούς, είναι ασέβεια να αντιμετωπίζεται το ανθρώπινο σώμα ως ιδιοκτησία που μπορεί να ανταλλαγεί.

Μια τέτοια πρακτική θα μπορούσε να οδηγήσει στην εμπορευματοποίηση του σώματος, (το οποίο θεωρείται "ιερό"), και στην εξομοίωση του με ένα αυτοκίνητο ή μια τηλεόραση, ένα ταπεινωτικό δηλαδή όραμα για την ανθρωπότητα, το οποίο βρίσκεται πολύ κοντά στην έννοια της δουλείας (Herring & Chau, 2007: 34-61). Αυτή η προσέγγιση αποκαλύπτει ότι η έννοια της περιουσίας, για άλλη μια φορά, είναι ανεπαρκώς καθορισμένη. Δεν έχουμε σώμα, λέει ο Toombs (1999:73-94) αλλά είμαστε ένα σώμα, υπάρχουμε μέσα σε αυτό και εκπορευόμαστε από μέσα του. Το σώμα από μόνο του δεν μπορεί να συγκριθεί με οποιοδήποτε άλλο περιουσιακό μας στοιχείο. Η έννοια της ιδιοκτησίας απαιτεί διαχωρισμό μεταξύ του ιδιοκτήτη και του ενοίκου ενώ δεν υπάρχει σαφής διάκριση μεταξύ του «εαυτού» μας και του «σώματος μας» (Herring & Chau, 2007: 55).

Ωστόσο, η νομοθετική προσέγγιση για τη ρύθμιση του σώματος είναι μικτή, και θα ήταν εσφαλμένο να πούμε ότι όλα τα στοιχεία του σώματος τίθενται εκτός της εμπορικής δραστηριότητας. Ενώ η πώληση ενός οργάνου δεν είναι νόμιμη, η πώληση σπέρματος, μαλλιών ή αίματος επιτρέπεται στη συντριπτική πλειονότητα των νομικών συστημάτων (Rao, 2000: 359).

Ως εκ τούτου, ενδιαφερόμαστε πρωτίστως για τη διάκριση μεταξύ γενετικού υλικού και γενετικής πληροφορίας, διότι με αυτόν τον τρόπο μπορούμε να δημιουργήσουμε έναν παράλληλο συσχετισμό μεταξύ του βιομετρικού υλικού και των βιομετρικών δεδομένων όσον αφορά την ψηφιοποίηση του υλικού. Αν και γενικά θεωρείται ότι η έννοια της ιδιοκτησίας ισχύει για το γενετικό υλικό στο βαθμό που είναι μέρος του σώματος, το καθεστώς των γενετικών πληροφοριών παραμένει λιγότερο σαφές.

Πολλές χώρες απαγορεύουν την κυριότητα των γενετικών πληροφοριών για λόγους προστασίας της επιστημονικής προόδου. Ωστόσο στο πλαίσιο της επιστημονικής έρευνας, δεν υφίσταται διάκριση μεταξύ γενετικού υλικού και γενετικής πληροφορίας (De Witte & Ten Have, 1997: 55). Οι γενετικές πληροφορίες καθίστανται διαθέσιμες όταν το γενετικό

υλικό έχει αναλυθεί και τα αποτελέσματα έχουν αποθηκευτεί σε ένα αρχείο ή βάση δεδομένων. Κατά τον ίδιο τρόπο, τα βιομετρικά δεδομένα προκύπτουν από την ανάλυση του βιομετρικού χαρακτηριστικού και την αντιστοίχιση του σε ένα μοτίβο (Mordini & Massari, 2008: 488-498).

Οι νομοθετικές προσεγγίσεις που επιδιώκουν την προστασία των προσωπικών δεδομένων γενικά δεν ασχολούνται με την έννοια της ιδιοκτησίας, δεδομένου ότι είναι επικίνδυνο για την έννοια της ιδιωτικότητας, να παραδεχτούμε ότι τα άτομα μπορούν να εμπορεύονται τα προσωπικά τους στοιχεία. Ωστόσο, ενώ η μεταβίβαση κυριότητας φαίνεται να είναι το θεμελιώδες εμπόδιο για την εφαρμογή ενός ιδιοκτησιακού μοντέλου στα προσωπικά δεδομένα, η αλήθεια είναι ότι η αγορά των προσωπικών δεδομένων υπάρχει και αποκτά διαστάσεις πολλών εκατομμυρίων δολαρίων. Όπως ορίζεται επί του παρόντος, ο περιορισμός αναφορικά με την μεταβίβαση κυριότητας των προσωπικών δεδομένων υπάρχει μόνο για τους χρήστες από τους οποίους εξάγονται αυτά τα δεδομένα, αλλά όχι για τις εταιρείες που ασχολούνται με την εξόρυξη (Schwartz, 2003: 206).

Η προσέγγιση των δεδομένων προσωπικού χαρακτήρα ως προϊόν συναλλαγής με συγκεκριμένη οικονομική αξία δεν είναι κάτι καινούργιο: οι εταιρείες τείνουν να βλέπουν τα συσσωρευμένα δεδομένα ως περιουσιακό στοιχείο έχοντας επενδύσει στην εξόρυξη τους, χρησιμοποιώντας εξειδικευμένο λογισμικό.

Σε αυτό το πλαίσιο η έννοια της "αμοιβής" με την παροχή δωρεάν υπηρεσιών σε αντάλλαγμα με την παροχή πληροφοριών σχετικά με τις δραστηριότητες πλοήγησής μας, δεν είναι κάτι μη σύνηθες (Schwartz, 2003: 205). Παρά την προαναφερθείσα αντίσταση, σύμφωνα με τους Douilhet & Karanasiou (2016:100-105), η εισαγωγή της έννοιας των μεγάλων δεδομένων[33] προκαλεί μια ακαδημαϊκή κινητικότητα, η οποία μετακινείται από την

[33] Όταν μιλάμε για μεγάλα δεδομένα, αναφερόμαστε σε πολύ μεγάλες ποσότητες δεδομένων που συλλέγονται από διάφορες πηγές, όπως το διαδίκτυο, τα κοινωνικά δίκτυα, οι αισθητήρες αλλά και η αγορά ιστορικού. Οι εξελιγμένες αναλύσεις τα μετατρέπουν σε πληροφορίες που βοηθούν στη λήψη αποφάσεων σε πολλούς τομείς,

παραδοσιακή προσέγγιση της προστασίας της ιδιωτικής ζωής προς ένα καθεστώς ιδιοκτησίας ευρύτερα και σε κάθε περίπτωση, περισσότερο προστατευτικό.

2.3. Αποδόμηση της νομικής έννοιας των βιομετρικών δεδομένων

Είμαστε τα σώματά μας, ή τα σώματά μας είναι μέρος μας; Αν και αυτή η συζήτηση σχετίζεται περισσότερο με τον φιλοσοφικό τομέα, είναι αδύνατο να την αποφύγουμε αν προσπαθήσουμε να καθορίσουμε τη νομική προσέγγιση του σώματος και, κατά συνέπεια, την ψηφιοποίηση του. Η παραδοσιακή προσέγγιση των κανονισμών για τα προσωπικά δεδομένα στοχεύει στην αναγνώριση της σχέσης μας με τα δεδομένα στο πλαίσιο της προστασίας της ιδιωτικής μας ζωής και της πληροφοριακής μας αυτοδιάθεσης (Sanz Salguero, 2016: 360). Η προσέγγιση αυτή θα μπορούσε να χαρακτηριστεί ως προβληματική, δεδομένου ότι εάν προσεγγίσουμε τα δεδομένα προσωπικού χαρακτήρα με την έννοια της ιδιοκτησίας, αυτό συνεπάγεται την αποδοχή της ύπαρξης μιας αγοράς όπου τα δεδομένα προσωπικού χαρακτήρα μπορούν να ανταλλάσσονται και να πωλούνται (Schwartz, 2003: 205).

Όσον αφορά την ιδιωτικότητα σε σχέση με τις βιομετρικές τεχνολογίες, είναι σαφές ότι πρέπει να προϋπάρχει ένα νομοθετικό πλαίσιο για την προστασία των δεδομένων προσωπικού χαρακτήρα πριν από την εφαρμογή της βιομετρικής και η απουσία ενός τέτοιου πλαισίου έχει κοινωνικό και ηθικό αντίκτυπο στις ατομικές ελευθερίες (Privacy International, 2013).

Ωστόσο, ενώ η προσέγγιση αυτή είναι ορθή και λογική όσον αφορά τα δεδομένα προσωπικού χαρακτήρα, δεν επαρκεί για τη νομοθετική προσέγγιση των βιομετρικών

όπως το μάρκετινγκ και η διαφήμιση, Με βάση αυτά τα δεδομένα οι εταιρείες μπορούν να προσφέρουν τα προϊόντα τους μόνο σε εκείνους που τα χρειάζονται και μόνο όταν τα χρειάζονται.
https://www.lawspot.gr/nomika-nea/big-data-megala-dedomena

δεδομένων. Από τη στιγμή της συλλογής του, τα βιομετρικά δεδομένα μπορούν να προκαλέσουν μια σειρά ανησυχιών και προβληματισμών που σχετίζονται με πολιτισμικές νόρμες και συναφείς κοινωνικούς φόβους. Σε ορισμένες κουλτούρες ή θρησκείες, οι διαδικασίες συλλογής δακτυλικών αποτυπωμάτων ή η σάρωση της ίριδας του ματιού μπορεί να είναι επεμβατικές, δυσάρεστες ή ταπεινωτικές. Τα παιδιά αλλά και οι ενήλικες μπορεί να φοβούνται την επαφή των μηχανών με τα σώματά τους. Τα άτομα με αναπηρία ή τα άτομα της ΛΟΑΤΚΙ κοινότητας μπορεί να αποκλειστούν, να επηρεαστούν ή να υποστούν διακρίσεις μέσω της διαδικασίας κατάταξης και ταξινόμησης των βιομετρικών τους στοιχείων, λόγω της εφαρμογής παραμέτρων του τι ορίζεται ως "φυσιολογικός" (Wickins, 2007: 45-54).

Από την άλλη πλευρά, μολονότι η συλλογική εφαρμογή των βιομετρικών τεχνολογιών παρουσιάζεται συνήθως ως εργαλείο για την αύξηση της ασφάλειας και της «εμπιστοσύνης» στις σχέσεις με τις δομές ισχύος, συνήθως δημιουργεί το αντίθετο αποτέλεσμα στα άτομα που απευθύνονται (Zureik & Hindle , 2004: 113-137) προκαλώντας φόβο και δυσπιστία, καθώς και πιθανή άρνηση συμμετοχής από ολόκληρα τμήματα του πληθυσμού (Vagle, 2018:122).

Έτσι, ενώ η παραδοσιακή ιατρική δεοντολογία υποστηρίζει την έννοια της συναίνεσης κατόπιν ενημέρωσης βάσει του δικαιώματος αυτονομίας και αυτοδιάθεσης του ατόμου-σε σημείο που, για παράδειγμα, η λήψη δειγμάτων DNA από ένα πρόσωπο, συμπεριλαμβανομένου ενός κρατούμενου, τίθεται υπό αμφισβήτηση λόγω του δικαιώματος της προσωπικής ακεραιότητας - το δικαίωμα στα βιομετρικά δεδομένα προσεγγίστηκε αποκλειστικά με βάση το δικαίωμα στην ιδιωτικότητα και την προστασία των δεδομένων προσωπικού χαρακτήρα, ακόμη και όταν αναφερόμαστε σε περιπτώσεις συναίνεσης κατόπιν ενημέρωσης, παρόλο που ο αυτοματοποιημένος χαρακτήρας συλλογής των περισσότερων

βιομετρικών δεδομένων αποκλείει από μόνος του τη δυνατότητα προηγούμενης συγκατάθεσης (Bourcha, Deftou, & Koskina, 2017: 37-62).

Υπό αυτή την έννοια, η πράξη της συλλογής ενός αποτυπώματος ή της σάρωσης ενός προσώπου δεν θεωρείται παραβίαση της προσωπικής ακεραιότητας (Sutrop, 2010:102-114), αν και έχει ως συνέπεια σοβαρές επιπτώσεις αναφορικά με τον έλεγχο του σώματος μας.

Για τους For Van der Ploeg και άλλους (2007), η διαφοροποίηση αυτή απαιτεί τον επαναπροσδιορισμό αυτού που θεωρούμε ότι καλύπτεται από την έννοια της προσωπικής ακεραιότητας και ιδιαίτερα της σωματικής ακεραιότητας, επισημαίνοντας ότι κατά την εξαγωγή του DNA από ένα άτομο, η παραχώρηση μέρους της σωματικής ακεραιότητας δεν είναι η ίδια πράξη επαφής με το σώμα -ίσως δεν απαιτείται καν φυσική παρεμβολή, επειδή μια τρίχα που λαμβάνεται από τα ρούχα είναι αρκετή -αλλά οι πληροφορίες που παράγονται στο σώμα, οι αναλύσεις και οι διεργασίες που διεξάγονται σε αυτές τις πληροφορίες, και η γνώση σχετικά με το άτομο που καθίσταται εφικτή ως αποτέλεσμα της διαδικασίας αυτής.

Η μηχανοργάνωση του σώματος αναδομεί και μεταμορφώνει την ταυτότητα του ατόμου, καθώς η ανάγνωση του σώματος μέσω μηχανών και τεχνολογικών διεργασιών αποκαλύπτει πληροφορίες σχετικά με το άτομο που ήταν προηγουμένως άγνωστες, ακόμη και απο τον ίδιο του τον εαυτό.

Με αυτόν τον τρόπο, τα βιομετρικά στοιχεία "φιλτράρουν" το σώμα και τα αποτελέσματα γνωστοποιούνται σε φορέα της εξουσίας (Foessel & Garapon, 2006: 165-172). Το «άτομο» γίνεται «πρόσωπο» μόνο όταν έχει μια αναγνωρίσιμη ταυτότητα, όταν γίνεται μια αφηρημένη πραγματικότητα, ένα σημάδι.

Αναφερόμενος στα βιομετρικά δεδομένα, ο Anton Alterman (2003:139-150) επισημαίνει ότι η ιδιωτικότητα είναι ο έλεγχος για το πώς και πότε οι αναπαραστάσεις σχετικά με την ταυτότητά μας κοινοποιούνται σε άλλους, και ότι όταν το "κομμάτι μας" που χρησιμοποιείται για τη διαφύλαξη της ταυτότητάς μας είναι αυτό, που παραδίδεται στους

άλλους για έλεγχο ταυτότητας, η ιδιωτικότητα διαφεύγει από τον έλεγχό μας και ψηφιοποιείται με αποτέλεσμα να είναι δύσκολο να την επανακτήσουμε.

Προκειμένου να επιβεβαιωθεί ότι η χρήση των δεδομένων που εξάγονται από το σώμα επηρεάζει μόνο τις πληροφορίες και όχι το ίδιο το σώμα, θα πρέπει να αγνοήσουμε την αναπόσπαστη σχέση που υφίσταται μεταξύ αυτών των πληροφοριών και της αξίας του σώματος στο οποίο αναφέρονται. Ως εκ τούτου, η κατανόηση των βιομετρικών δεδομένων στον ίδιο βαθμό και νόημα με τα προσωπικά δεδομένα (όπως η διεύθυνση ή ο αριθμός τηλεφώνου ενός ατόμου) αγνοεί την κεντρική σημασία της προσωπικότητας όσον αφορά την ταυτότητα του ατόμου.

2.4. Τα βιομετρικά δεδομένα ως υποσύνολο των προσωπικών δεδομένων

Όσον αφορά την προστασία των δεδομένων προσωπικού χαρακτήρα, το 2015 θεωρείται το έτος κατά το οποίο υπήρξε μια κορύφωση του ενδιαφέροντος στη διεθνή αρένα, ιδίως απο την Ευρωπαϊκή Ένωσης και απο τις Ηνωμένες Πολιτείες της Αμερικής, η οποία επεσήμανε την ανάγκη για κοινά πρότυπα προστασίας μεταξύ των χωρών. Αυτή η τοποθέτηση άλλωστε προκύπτει από την απόφαση του Δικαστηρίου της Ευρωπαϊκής Ένωσης, η οποία κήρυξε άκυρη, μετά από 15 έτη εφαρμογής, τη λεγόμενη «Συμφωνία Ασφαλούς Λιμένα»[34].

[34] Οι αρχές για την προστασία της ιδιωτικής ζωής στο πλαίσιο της διεθνούς συμφωνίας ασφαλούς λιμένα ήταν οι αρχές που αναπτύχθηκαν μεταξύ του 1998 και του 2000, προκειμένου να αποφευχθεί τυχαία αποκάλυψη ή απώλεια προσωπικών πληροφοριών απο ιδιωτικούς οργανισμούς εντός της Ευρωπαϊκής Ένωσης και των Ηνωμένων Πολιτειών, οι οποίοι αποθήκευαν δεδομένα πελατών. Στο πλαίσιο μιας σειράς αποφάσεων σχετικά με την επάρκεια της προστασίας των δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν σε άλλες χώρες , η Ευρωπαϊκή Επιτροπή αποφάσισε το 2000 ότι οι αρχές των Ηνωμένων Πολιτειών συμμορφώθηκαν με την οδηγία της ΕΕ, παρουσιάζοντας τη λεγόμενη "συμφωνία ασφαλούς λιμένα". Οι αρχές αυτές ανατράπηκαν στις 6 Οκτωβρίου 2015 από το Ευρωπαϊκό Δικαστήριο, το οποίο επέτρεψε σε ορισμένες αμερικανικές εταιρείες να συμμορφωθούν με τους νόμους περί προστασίας της ιδιωτικής ζωής που προστατεύουν τους πολίτες της Ευρωπαϊκής Ένωσης και της Ελβετίας. Οι αμερικανικές εταιρείες που αποθηκεύουν δεδομένα πελατών θα μπορούσαν να πιστοποιήσουν μέσω της εφαρμογής 7 αρχών ότι συμμορφώθηκαν με τις απαιτήσεις της οδηγίας της ΕΕ για την προστασία των δεδομένων. "Judgment in Case C-362/14 Maximillian Schrems v Data Protection Commissioner: The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid" (press release) (Press release). Court of Justice of the European Union. 6 October 2015. p. 3.

Θα πρέπει να επισημανθεί ότι, μέσω της εν λόγω συμφωνίας, η Ευρωπαϊκή Επιτροπή επέτρεψε τη διαβίβαση δεδομένων προσωπικού χαρακτήρα μεταξύ εταιρειών της Ευρωπαϊκής Ένωσης και των Ηνωμένων Πολιτειών της Αμερικής, δεδομένου ότι η συμφωνία επέβαλε τη συμμόρφωση των οργανισμών με ένα επαρκές επίπεδο προστασίας δεδομένων.

2.5. Γενικές αρχές για την προστασία της ιδιωτικής ζωής και των δεδομένων

Ακολουθούν ορισμένες αρχές που πρέπει να λαμβάνονται υπόψη σε μια οργανωτική διαδικασία προστασίας των δεδομένων, όπως για παράδειγμα στη διαδικασία ανωνυμοποίησης δεδομένων[35]. Οι διαδικασίες ανωνυμοποίησης πρέπει να προσεγγίζονται υπό την έννοια της προστασίας των δεδομένων από το σχεδιασμό, πράγμα που σημαίνει ότι οι απαιτήσεις προστασίας της ιδιωτικής ζωής θα λαμβάνονται υπόψη από τα αρχικά στάδια του σχεδιασμού του συστήματος πληροφοριών ή του προϊόντος που χρησιμοποιείται για την διαδικασία ανωνυμοποίησης και καθόλη τη διάρκεια του κύκλου ζωής του εν λόγω συστήματος προϊόντων ή πληροφοριών. Η έννοια της προστασίας της ιδιωτικότητας και των δεδομένων από το σχεδιασμό (by design), όσον αφορά στις διαδικασίες ανωνυμοποίησης μπορεί να συνοψισθεί στην εφαρμογή των ακόλουθων αρχών (Briney, 2019:1):

2.5.1. **Προληπτική αρχή**. Η προστασία της ιδιωτικότητας είναι ο βασικός στόχος της εφαρμογής τεχνικών και οργανωτικών μέτρων όπως η ανωνυμοποίηση, και η διαχείρισή της πρέπει να διεξάγεται προληπτικά και όχι αντιδραστικά. Με άλλα λόγια

[35] Ως ανωνυμοποίηση ορίζεται η διαδικασία διαγραφής των αναγνωριστικών προσωπικού χαρακτήρα σε εγγραφές δεδομένων, έτσι ώστε να μην είναι πλέον εφικτό τα ανωνυμοποιημένα δεδομένα να συσχετιστούν με το υποκείμενο των δεδομένων14. Κατά συνέπεια από τους δύο αυτούς ορισμούς (δηλαδή αυτούς της ψευδωνυμοποίησης και της ανωνυμοποίησης) προκύπτει ότι η χρήση της ανωνυμοποίησης έχει ως αποτέλεσμα την αδυναμία προσδιορισμού του υποκειμένου των δεδομένων, ενώ η ψευδωνυμοποίηση αντικαθιστά την ταυτότητα του υποκειμένου των δεδομένων με τέτοιο τρόπο, ώστε να απαιτούνται πρόσθετες πληροφορίες για την εκ νέου αναγνώριση του υποκειμένου των δεδομένων. Βλ. Λουκάς Νικόλαος Η.,2017, *Τεχνικά μέτρα του Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR), Κρυπτογράφηση και Ψευδωνυμοποίηση*, Τμήμα Ψηφιακών Συστημάτων Πανεπιστημίου Πειραιά

η προστασία της ιδιωτικής ζωής δεν μπορεί να διασφαλιστεί εάν αντιμετωπίζεται ως το επιδιωκόμενο αποτέλεσμα της διόρθωσης των υφιστάμενων κενών που ευθύνονται για τυχόν ζημίες που έχουν ήδη προκληθεί. Επομένως είναι αναγκαίο να εξαλειφτεί η πιθανότητα επανασυσχετισμού των υποκειμένων των δεδομένων με τα ανωνυμοποιημένα δεδομένα (Sikdar, 2019: 1-2). Ένα σημαντικό μέτρο για το αρχικό στάδιο σχεδίασης του συστήματος πληροφοριών ή του προϊόντος που χρησιμοποιείται στις διαδικασίες ανωνυμοποίησης είναι η εκτέλεση μιας αρχικής ταξινόμησης των δεδομένων σε κλίμακα με βάση τη διαβάθμιση των ευαίσθητων δεδομένων. Αυτή η ταξινόμηση μπορεί να είναι ποιοτική ή ποσοτική και θα χρησιμεύσει ως σημείο αναφοράς στον οργανισμό. Για παράδειγμα, μπορεί να αναπτυχθεί ένα σύστημα ταξινόμησης που βασίζεται σε τουλάχιστον τρία επίπεδα ταυτοποίησης των προσώπων (μικροδεδομένα, έμμεσα δεδομένα ταυτοποίησης και ευαίσθητα δεδομένα - microdata, indirect identification data, and sensitive data). Η κλίμακα θα είναι γνωστή στο προσωπικό που εμπλέκεται στη διαδικασία ανωνυμοποίησης και θα αποτελεί το θεμελιώδες κλειδί που θα ληφθεί υπόψη στην ανάλυση κινδύνου ή στην εκτίμηση αντικτύπου σχετικά με την προστασία των προσωπικών δεδομένων (Bousdekis et al.: 2018: 177).

2.5.2. Αρχή της ιδιωτικότητας από τον σχεδιασμό. Η ουσιαστική προτεραιότητα στον στάδιο του σχεδιασμού ενός συστήματος πληροφοριών, είναι η διασφάλιση της εμπιστευτικότητας των εμπλεκόμενων υποκειμένων. Ως εκ τούτου, είναι προτιμότερο να διασφαλίζεται η ιδιωτικότητα στο αρχικό αυτό στάδιο, λαμβάνοντας υπόψη την κλιμακωτή διαβάθμιση που πρέπει να έχουν τα ανωνυμοποιημένα δεδομένα. Υπό αυτή την έννοια, η δημιουργία και η διατήρηση μιας ποιοτικής ή ποσοτικής κλίμακας με προκαθορισμένα κριτήρια υποδιαίρεσης, όπως αναφέρεται στη προηγούμενη

παράγραφο, είναι ένα εργαλείο αδιαμφισβήτητης χρησιμότητας για την εξάλειψη των όποιων μεταβλητών (Chaudhuri, & Cavoukian, 2018:8).

2.5.3. **Αρχή της αντικειμενικής ιδιωτικότητας**. Ως αποτέλεσμα της κλιμακωτής ταξινόμησης των δεδομένων, θα δημιουργηθεί ένας δείκτης καθορισμού του αποδεκτού ορίου κινδύνου για την ασφαλή επεξεργασία των δεδομένων. Αυτός ο δείκτης κινδύνου λαμβάνεται υπόψη κατά τον σχεδιασμό της διαδικασίας ανωνυμοποίησης ή της λήψης άλλων τεχνικών και οργανωτικών μέτρων διασφάλισης των δεδομένων και το κατώτατο όριο του δείκτη αποτελεί το αντικειμενικά αποδεκτό ορίου κινδύνου που θα καθορίζει τις περαιτέρω απαιτούμενες ενέργειες που θα πρέπει να ληφθούν στην περίπτωση υπέρβασης αυτού του ορίου.

2.5.4. **Αρχή της πλήρους λειτουργικότητας**. Από την αρχή του σχεδιασμού του συστήματος πληροφοριών, θα πρέπει να ληφθεί υπόψη η τελική χρησιμότητα των ανωνυμοποιημένων δεδομένων, εξασφαλίζοντας, στο μέτρο του δυνατού, την απουσία στρεβλώσεων σε σχέση με τα μη ανωνυμοποιημένα δεδομένα. Με αυτόν τον τρόπο, θα διασφαλιστεί η χρησιμότητα των ανωνυμοποιημένα δεδομένων. Σε ορισμένες περιπτώσεις, προκειμένου να διασφαλιστεί η ιδιωτικότητα των ατόμων, μπορεί να είναι απαραίτητο να χρησιμοποιηθούν στρεβλώσεις γεωγραφικού εύρους, όπως στην περίπτωση ατόμων με παθολογικά ευρήματα εξαιρετικά σπάνια. Σε αυτές τις περιπτώσεις, ο αποδέκτης των πληροφοριών θα ενημερωθεί για τον λόγο αλλοίωσης του γεωγραφικού εύρους ή οποιοδήποτε άλλο είδος διακυμάνσεων που χρησιμοποιήθηκαν κατά τη διαδικασία ανωνυμοποίησης (Patel, 2019: 6).

2.5.5. Αρχή της ιδιωτικότητας για όλον τον κύκλο ζωής των πληροφοριών. Τα μέτρα που εγγυώνται την Ιδιωτικότητα των ενδιαφερομένων μερών ισχύουν καθ' όλη τη διάρκεια του κύκλου ζωής των πληροφοριών που βασίζονται στα δεδομένα χωρίς ανωνυμοποίηση. Για παράδειγμα, κατά την έναρξη της διαδικασίας ανωνυμοποίησης, οι μεταβλητές ταυτοποίησης που δεν θεωρούνται απαραίτητες ή που δεν είναι δυνατόν να ανωνυμοποιηθούν εξαλείφονται και, όταν χρειαστεί η αξιοποίηση των ανωνυμοποιημένων πληροφοριών, θα εξακολουθήσουν να λαμβάνονται μέτρα για να εξασφαλισθεί η ιδιωτικότητα των ενδιαφερομένων μερών, όπως για παράδειγμα εσωτερικοί έλεγχοι για την επαλήθευση της ορθής χρήσης των πληροφοριών, τήρηση των διαδικασιών για την καταστροφή των πληροφοριών κ.λπ. (Romanou, 2018: 104).

2.5.6. Αρχή της ενημέρωσης και της κατάρτισης. Ένα από τα σημεία κλειδιά για τη διασφάλιση της ιδιωτικότητας των ενδιαφερομένων μερών είναι η εκπαίδευση και η σωστή ενημέρωση σχετικά με τα δεδομένα που διατίθενται στο προσωπικό που εμπλέκεται στη διαδικασία ανωνυμοποίησης αλλά και στην εκμετάλλευση των ανωνυμοποιημένων πληροφοριών. Κατά τη διάρκεια του κύκλου ζωής των πληροφοριών, όλο το προσωπικό με πρόσβαση σε ανώνυμα ή μη ανωνυμοποιημένα δεδομένα θα πρέπει να είναι ειδικά εκπαιδευμένο και ενημερωμένο για τις υποχρεώσεις του. Ο σχεδιασμός του συστήματος πληροφοριών ή του προϊόντος που χρησιμοποιείται για τη διαδικασία ανωνυμοποίησης, οφείλει να λάβει υπόψη του την ανάγκη αυτή από το αρχικό στάδιο, αξιολογώντας τα προφίλ και τις ανάγκες όλων όσοι εμπλέκονται στη διαδικασία ανωνυμοποίησης.

2.6. Η αργή αφομοίωση της έννοιας των βιομετρικών δεδομένων στο τομέα της ιδιωτικότητας

Το δικαίωμα στην ιδιωτική ζωή έχει κατοχυρωθεί ως ανθρώπινο δικαίωμα τόσο σε διεθνικό επίπεδο (Οργανισμός Ηνωμένων Εθνών)[36] όσο και σε περιφερειακό επίπεδο και ειδικότερα σε ενωσιακό και σε διααμερικανικό επίπεδο. Όσον αφορά στο διεθνικό επίπεδο, ισχύουν συμβάσεις παγκόσμιας εφαρμογής, όπως η Οικουμενική Διακήρυξη των ανθρωπίνων δικαιωμάτων του 1948 (άρθρο 12), το Διεθνές Σύμφωνο για τα ατομικά και πολιτικά δικαιώματα του 1966 (άρθρο 17), η διεθνής σύμβαση για την προστασία των δικαιωμάτων όλων των διακινούμενων εργαζομένων και των οικογενειών τους το 1990 (άρθρο 14) και η σύμβαση για τα δικαιώματα του παιδιού το 1989 (άρθρο 16), περιέχουν σχεδόν τους ίδιους όρους. Ομοίως, το δικαίωμα στην προστασία της ιδιωτικής ζωής χαίρει ρητής αναγνώρισης σε όλη την Αμερικανική ήπειρο, μέσω του άρθρου 11 της Αμερικανικής Σύμβασης για τα Ανθρώπινα Δικαιώματα[37] (Oussous, Benjelloun, Lahcen, & Belfkih, 2018: 431-448).

Στην αμερικανική ήπειρο, όπως και στο μεγαλύτερο μέρος του κόσμου, η χρήση βιομετρικών χαρακτηριστικών ως μηχανισμών ταυτοποίησης και εξακρίβωσης της

[36] Η Διεθνής Διακήρυξη των Ανθρωπίνων Δικαιωμάτων αναφέρεται σε μια συλλογή τριών διεθνών εγγράφων: την Οικουμενική Διακήρυξη των Ανθρωπίνων Δικαιωμάτων, το Διεθνές Σύμφωνο για τα Οικονομικά, Κοινωνικά και Πολιτιστικά Δικαιώματα και το Διεθνές Σύμφωνο για τα Ατομικά και Πολιτικά Δικαιώματα και τα δύο Προαιρετικά Πρωτόκολλά τους. Το 1948, η Γενική Συνέλευση των Ηνωμένων Εθνών ενέκρινε την Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου (UDHR), καθιερώνοντας το όραμα και τις αρχές που αναγνωρίζουν την αλληλεξάρτηση και το αδιαίρετο όλων των ανθρωπίνων δικαιωμάτων: ένα όραμα που εγγυάται την ανθρώπινη πολιτική και πολιτική ελευθερία καθώς και οικονομική και κοινωνική ευεξία. Το ESCR ενσωματώθηκε στο διεθνές δίκαιο των συνθηκών μέσω του Διεθνούς Συμφώνου για τα Οικονομικά, Κοινωνικά και Πολιτιστικά Δικαιώματα (ICESCR). Μέχρι σήμερα, περισσότερες από 150 χώρες έχουν επικυρώσει το ICESCR, αποδεχόμενοι την υποχρέωση να εκπληρώσουν τα οικονομικά, κοινωνικά και πολιτιστικά δικαιώματα των λαών τους. https://www.escr-net.org/resources/united-nations-human-rights-system-treaties-mechanisms-and-documents

[37] Η Αμερικανική Σύμβαση για τα Ανθρώπινα Δικαιώματα, γνωστή και ως Σύμφωνο του Σαν Χοσέ, είναι ένα διεθνές μέσο για τα ανθρώπινα δικαιώματα. Εγκρίθηκε από πολλές χώρες στο δυτικό ημισφαίριο στο Σαν Χοσέ της Κόστα Ρίκα στις 22 Νοεμβρίου 1969. Εφαρμόστηκε μετά την κατάθεση του ενδέκατου εγγράφου κύρωσης (της Γρενάδας) στις 18 Ιουλίου 1978.
Τα όργανα που είναι αρμόδια για την επίβλεψη της συμμόρφωσης με τη Σύμβαση είναι η Διαμερικανική Επιτροπή για τα Ανθρώπινα Δικαιώματα και το Διαμερικανικό Δικαστήριο Ανθρωπίνων Δικαιωμάτων, τα οποία είναι όργανα του Οργανισμού Αμερικανικών Κρατών (ΟΑΣ). http://www.oas.org/dil/treaties_B-32_American_Convention_on_Human_Rights_sign.htm

ταυτότητας έχει μακρά ιστορία. Παραδοσιακά, τα έγγραφα ταυτοποίησης περιέχουν φωτογραφίες του προσώπου και εκτυπώσεις των δακτυλικών αποτυπωμάτων (και σε κάποιες περιπτώσεις της παλάμης) ως ελάχιστα στοιχεία αναγνώρισης. Σύμφωνα με τους Berry & Stoney (2001:40), ένα από τα πρώτα συστήματα αναγνώρισης δακτυλικών αποτυπωμάτων χρονολογείται από το τέλος του 17^{ου} αιώνα στην Αργεντινή. Συγκεκριμένα όταν ο Δρ Ιβάν Βουκέτς εργαζόταν στη La Plata για να εγκαταστήσει ένα ανθρωπομετρικό σύστημα αναγνώρισης, ευρωπαϊκής προέλευσης, χρησιμοποίησε ένα σύνολο φυσικών χαρακτηριστικών ως μηχανισμό εξακρίβωσης της γνησιότητας και αφού έπεισε τις αρχές για τα πλεονεκτήματα του συστήματος, παρουσίασε το πρώτο στην ιστορία σύστημα αναγνώρισης μέσω δακτυλικών αποτυπωμάτων.

Η τεχνολογική επέκταση αυτών των χρήσεων, η οποία έχει αποκτήσει δυναμική ειδικά κατά τη διάρκεια της τελευταίας δεκαετίας, είναι το φυσικό επακόλουθο των πολιτικών ενίσχυσης της επιτήρησης, οι οποίες προωθούνται από τα κράτη με πρόσχημα την ασφάλεια των συναλλαγών και την διασφάλιση των προσωπικών δεδομένων των πολιτών. Ωστόσο, η εφαρμογή των συστημάτων αυτών χαρακτηρίζεται από την έλλειψη επαρκών νομικών πλαισίων για τη θέσπιση εγγυήσεων κατά την επεξεργασία των δεδομένων, καθώς και από την έλλειψη διαφάνειας κατά τη φάση λήψης αποφάσεων και εφαρμογής διαδικασιών (Association for Civil Rights, 2017a). Υπό αυτή την έννοια, οι ακόλουθες παράγραφοι δεν προορίζονται να χρησιμεύσουν ως μια εξαντλητική παρουσίαση περιπτώσεων χρήσης βιομετρικών τεχνολογιών, αλλά μόνο ως ανάλυση ορισμένων σχετικών παραδειγμάτων αναφορικά με τις συνέπειές που επέφεραν στον ευαίσθητο τομέα της προστασίας της ιδιωτικότητας του ατόμου.

2.7. Η νομική αντιμετώπιση των βιομετρικών δεδομένων στη Λατινική Αμερική

Η εφαρμογή συστημάτων βιομετρικού δελτίου ταυτότητας στις χώρες της Λατινικής Αμερικής, έχει συνδεθεί με τον δημόσιο διάλογο περί "εξάλειψης του αποκλεισμού". Έτσι, σε χώρες όπως η Αργεντινή, η χρήση βιομετρικών στοιχείων για την ταυτοποίηση έχει πολιτικοποιηθεί μέσω του εθνικού διαλόγου για τον εκσυγχρονισμό του κράτους (Association for Civil Rights, 2017b). Με ένα ιστορικό συχνών και σπασμωδικών δικτατορικών καθεστώτων, με την εκτίναξη του κοινωνικού και οικονομικού αποκλεισμού και με το φαινόμενο των ανεξιχνίαστων εξαφανίσεων, η Λατινική Αμερική παρουσιάζει ένα έντονο σκεπτικισμό αναφορικά με τη χρήση τεχνολογιών που στοχεύουν στην ενίσχυση της ασφάλειας της σχέσης πολίτη - κράτους (Ajana, 2013 : 586).

2.7.1. Αργεντινή

Στην περίπτωση της Αργεντινής, το ομοσπονδιακό σύστημα βιομετρικής ταυτοποίησης για την ασφάλεια (SIBIOS) εισήχθη το 2011 μέσω εκτελεστικού διατάγματος, με αιτιολόγηση την ασφάλεια των πολιτών και την καταπολέμηση του οργανωμένου εγκλήματος. Με αυτό το πρόσχημα, το κανονιστικό πλαίσιο για την εφαρμογή ενός προγράμματος εθνικής βιομετρικής ταυτοποίησης, δεν ακολούθησε τη συνήθη νομοθετική διαδικασία, παραλείποντας την κοινοβουλευτική συζήτηση και τη διαβούλευση με τους πολίτες, μια πάγια δηλαδή τακτική που συνοδεύει τέτοιου είδους κανονιστικές αποφάσεις.

Η SIBIOS[38] αποθηκεύει τα δακτυλικά αποτυπώματα, τις αποτυπώσεις παλάμης και τα βιομετρικά χαρακτηριστικά προσώπου όλων των πολιτών της Αργεντινής, καθώς και των

[38] Το Ομοσπονδιακό Σύστημα Βιομετρικής Ταυτοποίησης για την Ασφάλεια (SIBIOS) δημιουργήθηκε με το διάταγμα της εθνικής εκτελεστικής εξουσίας της Αργεντινής υπ. αριθ. 1766/11, που προωθήθηκε από το Υπουργείο Εθνικής Ασφάλειας. Κύριος στόχος του είναι να αποτελέσει το πλαίσιο για τη χρήση των βιομετρικών συστημάτων με στόχο την ενίσχυση της δημόσιας ασφάλειας και την πάταξη των εγκληματικών πράξεων. Οι οργανώσεις πολιτικής άμυνας στο Διαδίκτυο εκφράζουν αντιρρήσεις για την εφαρμογή του συστήματος λόγω των κινδύνων που ενέχει για την ιδιωτικότητα των πολιτών.
https://www.vialibre.org.ar/2012/01/10/biometria-en-argentina-la-vigilancia-masiva-como-politica-de-estado/

αλλοδαπών που εισέρχονται ή εξέρχονται από την Αργεντινή. Πρόκειται για τη σύλληψη και εφαρμογή ενός διαλειτουργικού και ολιστικού συστήματος επεξεργασίας δεδομένων, για τη χρήση του οποίου η ομοσπονδιακή αστυνομία, η επαρχιακή αστυνομία, το εθνικό μητρώο προσώπων, η εθνική διεύθυνση μετανάστευσης, καθώς και πολλοί άλλοι οργανισμοί που εξαρτώνται από την εκτελεστική, νομοθετική και δικαστική εθνική εξουσία, δεν είναι απαραίτητο να διαθέτει δικαστική άδεια για την πρόσβαση στα αποθηκευμένα δεδομένα, όπως είναι το σύνηθες.

Σύμφωνα με την αρχή προστασίας προσωπικών δεδομένων της Αργεντινής (Association for Civil Rights, 2017 b), οι παράμετροι χρήσης, φύλαξης και αποθήκευσης αυτών των πληροφοριών, καθώς και οι διαδικασίες για την απόκτηση και υιοθέτηση της τεχνολογίας που χρησιμοποιείται, δεν είναι διαφανείς και, ως εκ τούτου, εμποδίζεται η δημοκρατικά επιβεβλημένη άσκηση ελέγχου απο τον λαό σε αυτό. Επιπλέον, δεν υπάρχει νομοθετική πρόνοια στην Αργεντινή που να κατοχυρώνει τα βιομετρικά δεδομένα ως ιδιαίτερα ευαίσθητα προσωπικά δεδομένα, και αυτό το κενό θέτει σε κίνδυνο τη προστασία των δικαιωμάτων για την ιδιωτικότητα και την ακεραιότητα των πολιτών.

2.7.2. Βραζιλία

Η ιστορία των προσπαθειών της Βραζιλίας να υιοθετήσει ένα αυτοματοποιημένο σύστημα αναγνώρισης και ταυτοποίησης πολιτών ξεκινά από το 1997. Το 2004, το Υπουργείο Δικαιοσύνης παρουσίασε ένα μοντέλο βιομετρικής αναγνώρισης και ταυτοποίησης που εμπεριέχει το δακτυλικό αποτύπωμα, το μοτίβο ανίχνευσης προσώπου και την ίριδα των πολιτών, του οποίου η δυνητική εφαρμογή προκάλεσε ιδιαίτερη ανησυχία, δεδομένου ότι αυτές οι πληροφορίες θα αποθηκεύονται σε μια κεντρική βάση δεδομένων (Da Costa-Abreu & Smith, 2017:629-834).

Επιπρόσθετα, η Βραζιλία ξεκίνησε την εφαρμογή ενός ηλεκτρονικού συστήματος ψηφοφορίας το 2008, και υπάρχουν ενεργά σχέδια εφαρμογής βιομετρικών τεχνολογιών για την εξακρίβωση της ταυτότητας των ψηφοφόρων αλλά και για την επιτήρηση στο σύστημα μεταφορών, για την ταυτοποίηση στα σχολεία, σε τραπεζικούς φορείς και στα ATM. Οι δυνάμεις ασφαλείας, η αστυνομία και τα δικαστήρια συλλέγουν βιομετρικά δεδομένα (δακτυλικά αποτυπώματα) που αποθηκεύονται σε βάσεις δεδομένων των οποίων η νομική προστασία είναι σχεδόν ανύπαρκτη (Association for Civil Rights, 2017a).

Η εφαρμογή των βιομετρικών τεχνολογιών στη Βραζιλία παρουσιάζει μια σειρά ιδιαίτερων προκλήσεων σχετικά με την ιστορία, τη γεωγραφία και την κοινωνικοοικονομική της σύνθεση. Το κόστος της απόκτησης δεδομένων, το οποίο είναι ήδη υψηλό για την εφαρμογή οποιουδήποτε παγκόσμιου βιομετρικού συστήματος, είναι ακόμη πιο υψηλό δεδομένης της εδαφικής έκτασης της χώρας και του μεγάλου πληθυσμού της.

Εν προκειμένω, οι Da Costa-Abreu & Smith (2017) επισημαίνουν ότι, μολονότι οι τιμές μειώνονται, η τιμή μονάδας για τα εθνικά συστήματα αναγνώρισης εξακολουθεί να υπερβαίνει τα επίπεδα που μπορούν να διατεθούν από τις αναπτυσσόμενες χώρες, και ότι όταν μια τεχνολογία είναι δαπανηρή, το κόστος συνήθως μετακυλίεται στον πολίτη, θέτοντας έτσι και εμπόδια στην πρόσβαση. Στην περίπτωση της Βραζιλίας ειδικότερα, και γενικότερα της Λατινικής Αμερικής, όπου τα βιομετρικά συστήματα παρουσιάστηκαν ως λύση στα εμπόδια για την πρόσβαση σε αγαθά, υπηρεσίες και δικαιώματα από κοινωνικές ομάδες που έχουν υποστεί διακρίσεις, δεν έχει νόημα να επιδιωχθεί η επίλυση αυτού του χάσματος με δαπανηρές τεχνολογικές λύσεις.

2.7.3. Χιλή

Στη Χιλή, η χρήση βιομετρικών συστημάτων είναι διαδεδομένη και η χρήση του αποτυπώματος ως μηχανισμού ταυτοποίησης συναντάται από τις υπηρεσίες μετανάστευσης

μέχρι στο εθνικό σύστημα υγείας και στα τραπεζικά συστήματα. Επιπλέον, αυξάνεται η χρήση των συστημάτων αναγνώρισης προσώπου, ενός μηχανισμού που χρησιμοποιείται στις κάμερες επιτήρησης και στα μέσα μαζικών μεταφορών (Mouammine, & Collier, 2018: 1-10). Η περίπτωση αυτών των συστημάτων έχει ιδιαίτερο ενδιαφέρον, δεδομένου ότι αποτελούν πρωτοβουλίες δήμων, αρχών και θεσμών που ενεργούν ανεξάρτητα και χωρίς ένα προϋπάρχουν ρυθμιστικό πλαίσιο.

Ο οργανισμός ψηφιακών δικαιωμάτων[39] των πολιτών της Χιλής ανέφερε ότι δεν υπάρχουν στοιχεία σχετικά με την αποτελεσματικότητα αυτών των μηχανισμών για τους σκοπούς που επιδιώκουν, ιδίως, όσον αφορά την αύξηση της ασφάλειας των πολιτών και ότι αυτά έχουν υλοποιηθεί χωρίς προηγούμενες μελέτες , χωρίς την εφαρμογή της αρχής της αναλογικότητας, για να μην αναφέρουμε χωρίς διαφάνεια στη διαδικασία υποβολής οικονομικών προσφορών για την απόκτηση των εν λόγω τεχνολογιών.

2.7.4. Βενεζουέλα

Από την πλευρά της, η Βενεζουέλα εφάρμοσε για πρώτη φορά μηχανισμούς βιομετρικής αναγνώρισης στο εκλογικό της σύστημα μέσω του UPS (σύστημα ολοκληρωμένου ελέγχου ταυτότητας), το οποίο απαιτούσε έλεγχο ταυτότητας των ψηφοφόρων για την ενεργοποίηση των μηχανών ψηφοφορίας (Εθνικό Εκλογικό Συμβούλιο, s. f.) και η οποία χρησιμοποιήθηκε για πρώτη φορά στις εκλογές του 2012. Στη συνέχεια, εφαρμόστηκε το λεγόμενο βιομετρικό σύστημα για την επισιτιστική ασφάλεια, μέσω του οποίου οι πολίτες υποχρεούνται να επαληθεύουν την ταυτότητά τους με την χρήση ψηφιακών δακτυλικών αποτυπωμάτων όταν καλούνται να παραλάβουν προϊόντα "πρώτη ανάγκης" (τρόφιμα και φάρμακα).

[39] Η Derechos Digitales (Digital Rights) είναι μια οργάνωση λατινοαμερικανικής εμβέλειας, ανεξάρτητη και μη κερδοσκοπική, που ιδρύθηκε το 2005 και έχει θεμελιώδη στόχο την ανάπτυξη, υπεράσπιση και προώθηση των ανθρωπίνων δικαιωμάτων στο ψηφιακό περιβάλλον. https://www.derechosdigitales.org/

Στην περίπτωση της Βενεζουέλας, αν και το εθνικό δελτίο ταυτότητας δεν ενσωματώνει τις βιομετρικές τεχνολογίες, τα δεδομένα ενσωματώνονται στο εθνικό σύστημα ταυτοτήτων, καθώς τόσο το δημοτολόγιο όσο και το και εκλογικό μητρώο έχει διασυνδεθεί και τελεί υπό την εξουσία του εθνικού εκλογικού Συμβούλιου. Τα δεδομένα αυτά αποθηκεύονται σε μια βάση δεδομένων πολλαπλών προσβάσεων, συσχετίζονται με άλλες πληροφορίες, όπως η διεύθυνση κατοικείς του ατόμου, η ημερομηνία γέννησης και ο εθνικός αριθμός ταυτότητας (Zhang, 2018: 115), και στη συνέχεια χρησιμοποιούνται όχι μόνο απο τους κρατικούς φορείς, αλλά ακόμη και από σουπερμάρκετ και φαρμακεία, χωρίς προηγούμενη συγκατάθεση αλλά ούτε και ενημέρωση του υποκειμένου των δεδομένων.

Ελλείψει εθνικής νομοθεσίας σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα, και στο πλαίσιο ενός συστήματος που χρησιμοποιεί τις πληροφορίες των πολιτών του ως μηχανισμό πολιτικού ελέγχου, η χρήση βιομετρικών τεχνολογιών για την πρόσβαση σε βασικά αγαθά και υπηρεσίες αποτελεί χαρακτηριστικό παράδειγμα της ύπαρξης κοινωνικοπολιτικού χάσματος μεταξύ «νομιμότητας» και «παρανομίας».

Από τη στιγμή της εφαρμογής του προαναφερόμενου συστήματος βιομετρικής ταυτοποίησης, άρχισαν να παρουσιάζονται αναρίθμητες δυσλειτουργίες, όπως η αδυναμία απόκτησης βασικών αγαθών από ανήλικους, η μη εμφάνιση των αλλοδαπών στην εκλογική βάση δεδομένων (Miselem, 2014:200) και η άρνηση εξυπηρέτησης διαφυλικών ατόμων των οποίων η φυσική εμφάνιση δεν ταίριαζε με αυτή που αντικατοπτριζόταν στη βάση δεδομένων.

2.7.5. Παραγουάη

Η Παραγουάη είναι ακόμη μία χώρα που δεν διαθέτει νομοθεσία για τα προσωπικά δεδομένα. Ωστόσο, έχει σταδιακά εφαρμόσει συστήματα βιομετρικής αναγνώρισης. Στην περίπτωση αυτή, δεδομένου ότι δεν υπάρχει καθορισμένη δημόσια πολιτική, δεν υπάρχουν

και οδηγίες όσον αφορά τον χειρισμό των συλλεγόμενων πληροφοριών, την ίδια στιγμή που διάφοροι οργανισμοί απαιτούν την παροχή προσωπικών δεδομένων για την εκτέλεση συγκεκριμένων διαδικασιών (Association for Civil Rights, 2017a). Οι περιπτώσεις αυτές απεικονίζουν την μειονεκτική θέση των πολιτών απέναντι στο κράτος στην περίπτωση που τα δεδομένα τους απαιτούνται ως αντιπαροχή για ένα αγαθό ή μια υπηρεσία.

Στην Παραγουάη, υπήρξαν περιπτώσεις στις οποίες το ίδρυμα κοινωνικής ασφάλισης απαιτούσε τα δακτυλικά αποτυπώματα των ασθενών προκειμένου να τους επιτραπεί η συνταγογράφηση φαρμάκων (ABC Color, 2016), τη στιγμή που στη Βενεζουέλα, λόγω των ελλείψεων τροφίμων και των υψηλών ποσοστών πληθωρισμού, οι πολίτες αναγκάζονται να μπουν σε μια διαδικασία παροχής των δεδομένων τους, με αντάλλαγμα την αγορά τροφίμων (Meza, 2014).

2.8. Προϊσχύον, ισχύον & διαμορφούμενο νομικό πλαίσιο των προσωπικών δεδομένων

Μια πληροφορία προκειμένου να αποκτήσει την ιδιότητα του προσωπικού δεδομένου, και επομένως και τη νομική προστασία που αυτό απολαμβάνει, θα πρέπει να αναφέρεται σε ένα ορισμένο άτομο (το υποκείμενο των δεδομένων) και με αυτόν τον τρόπο να οδηγεί άμεσα ή και έμμεσα στην ταυτοποίηση του με ένα υπαρκτό φυσικό πρόσωπο.

Τα προσωπικά δεδομένα νοούνται ως πληροφορίες που περιέχουν αριθμητικά, ακουστικά, γραφικά, αλφαβητικά, φωτογραφικά ή οποιαδήποτε άλλα στοιχεία, μέσω των οποίων ένα άτομο μπορεί να αναγνωρισθεί και να προσδιοριστεί. Τόσο τα δακτυλικά αποτυπώματα όσο και τα χαρακτηριστικά του προσώπου αποτελούν αποκλειστικές πτυχές του κάθε ατόμου και επιτρέπουν στο συγκεκριμένο πρόσωπο να είναι αναγνωρίσιμο, και υπό αυτή την έννοια κατατάσσονται στα προσωπικά δεδομένα.

Ως εκ τούτου, τα βιομετρικά δεδομένα αντιμετωπίζονται νομικά ως προσωπικά δεδομένα και επομένως η τυχόν επεξεργασία τους θα πρέπει να είναι σύμφωνη με το ισχύον νομικό και κανονιστικό πλαίσιο της εκάστοτε εδαφικής αρμοδιότητας, εντός της οποίας λαμβάνει χώρο η επεξεργασία.

2.9. Ευρωπαϊκή Ένωση & ο νέος Γενικός Κανονισμός Προστασίας Δεδομένων

Στο νέο ενωσιακό κανονιστικό πλαίσιο τα βιομετρικά δεδομένα ορίζονται ως τα προσωπικά εκείνα δεδομένα, που προκύπτουν από ειδική τεχνική επεξεργασία συνδεόμενη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου και τα οποία επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου, όπως εικόνες προσώπου ή δακτυλοσκοπικά δεδομένα (άρθρα 4 § 14 του ΓΚΠΔ και 44 του Ν. 4624/2019).

Συγκεκριμένα, το άρθρο 9, του κανονισμού[40] 2016/679 συγκαταλέγει τα βιομετρικά δεδομένα στην ειδική κατηγορία δεδομένων προσωπικού χαρακτήρα, η επεξεργασία των οποίων, κατά γενικό κανόνα, απαγορεύεται, ιδίως, όταν αποσκοπεί στην αδιαμφισβήτητη ταυτοποίηση ενός φυσικού προσώπου.

Τα ευαίσθητα δεδομένα προσωπικού χαρακτήρα, αναφέρονται στο εν λόγω άρθρο ως δεδομένα ειδικών κατηγοριών και παρατίθενται εξαντλητικά ως εξής :

- δεδομένα που αποκαλύπτουν εθνοτική ή φυλετική καταγωγή,
- πολιτικές γνώμες,
- θρησκευτικές ή φιλοσοφικές πεποιθήσεις,

[40] Ο κανονισμός δεν αποτελεί το πρώτο νομικό κείμενο που αυτοτελώς πραγματεύεται την προστασία των προσωπικών δεδομένων. Αντίθετα, σε Ευρωπαϊκό επίπεδο, από το 1995 βρισκόταν σε ισχύ η Οδηγία 95/46/ΕΚ«για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών», η οποία ενσωματώθηκε στο εθνικό δίκαιο βάσει του Ν. 2472/1997 «για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα»

- συνδικαλιστική μεταχείριση,
- γενετικά δεδομένων και βιομετρικά δεδομένα,
- δεδομένα σχετικά με την υγεία
- δεδομένα που σχετίζονται με τη σεξουαλική ζωή ή τον σεξουαλικό προσανατολισμό

2.9.1. Επίδραση του νέου ΓΚΠΔ στην αντιμετώπιση των βιομετρικών δεδομένων

Στην προϋπάρχουσα σχετική νομοθεσία αρκετών ευρωπαϊκών χωρών, ίσχυε η κατηγοριοποίηση των προσωπικών δεδομένων σε επίπεδα ανάλογα με την επικινδυνότητα που θα μπορούσε να επιφέρει για την ασφάλεια τους, η πιθανή επεξεργασία τους. Ανάλογα με το επίπεδο του κινδύνου, καθοριζόταν απο τη νομοθεσία και το επίπεδο ειδικής προστασίας που απαιτούσε η επεξεργασία τους και επομένως και τα ελάχιστα απαιτούμενα μέτρα ασφαλείας.

Μέχρι σήμερα, τα βιομετρικά δεδομένα (σε όσα νομοθετικά κείμενα των κρατών της ένωσης γινόταν αναφορά)[41] είχαν ταξινομηθεί σε επίπεδο απλών προσωπικών δεδομένων και επομένως η τυχόν επεξεργασία τους δεν επέφερε υψηλό κίνδυνο για την ασφάλεια και την προστασία της ιδιωτικότητας των υποκειμένων τους (Thieme, Nanavati, & Mak, 2018: 904).

Ο νέος ΓΚΠΔ αφενός διευρύνει την κατηγορία των ευαίσθητων προσωπικών δεδομένων με την προσθήκη των γενετικών και βιομετρικών δεδομένων και αφετέρου ορίζει ρητώς ότι τα βιομετρικά δεδομένα ως δεδομένα ειδικής κατηγορίας που κατά προέκταση χρήζουν ειδικής προστασίας.

Σύμφωνα με τη γνωμοδότηση υπ. αριθ. 3/2007 σχετικά με την πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την τροποποίηση της κοινής

[41] Βλ. για παράδειγμα τον Ισπανικό οργανικό νόμο 15/1999, της 13ης Δεκεμβρίου, σχετικά με την προστασία των προσωπικών δεδομένων (LOPD), La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)

προξενικής εγκυκλίου σχετικά με τις θεωρήσεις διπλωματικών και προξενικών αρχών όσον αφορά την εισαγωγή βιομετρικών στοιχείων[42], τα βιομετρικά δεδομένα αποτελούν δεδομένα προσωπικού χαρακτήρα καθώς μπορούν να θεωρηθούν τόσο ως περιεχόμενο πληροφοριών που χαρακτηρίζει συγκεκριμένες βιολογικές ιδιότητες, φυσιολογικά χαρακτηριστικά ή/και προσωπικά γνωρίσματα που είναι μοναδικά για ένα άτομο, όσο και ως στοιχείο αντιστοίχισης μιας πληροφορίας με το άτομο αυτό. Κατά τον τρόπο αυτό τα βιομετρικά δεδομένα, λόγω του αποκλειστικού δεσμού τους με ένα συγκεκριμένο άτομο, μπορούν να λειτουργήσουν ως στοιχεία αναγνώρισης του εν λόγω ατόμου.

Στο ίδιο πνεύμα ο Ράσελ (2018) αναφέρει ότι η επεξεργασία των βιομετρικών δεδομένων που χρησιμοποιούνται για οποιονδήποτε σκοπό, συμπεριλαμβανομένου του ελέγχου της παρουσίας του ατόμου, απαιτεί τη λήψη ειδικών μέτρων προστασίας, δεδομένου ότι επιτρέπουν την ταυτοποίηση των ατόμων με αυτοματοποιημένο τρόπο (Ράσελ, 2018: 25).

Ως εκ τούτου, η όποια επεξεργασία βιομετρικών δεδομένων , καθότι αυτά έχουν πλέον ενταχθεί στην ειδική κατηγορία των ευαίσθητων δεδομένων θα μας αναγκάσει να λάβουμε πρόσθετα μέτρα για την προστασία αυτών των δεδομένων, χωρίς ωστόσο αυτά να διευκρινίζονται επαρκώς απο τον κανονισμό.

Το άρθρο 9 του ΓΚΠΔ υποδεικνύει μεν την απαγόρευση της χρήσης βιομετρικών δεδομένων, αλλά προβλέπει και αρκετές εξαιρέσεις όπως για παράδειγμα (παρ. 2, περ. η) είναι επιτρεπτή η χρήση βιομετρικών δεδομένων εάν η επεξεργασία είναι απαραίτητη για σκοπούς προληπτικής ή επαγγελματικής ιατρικής, εκτίμησης της ικανότητας προς εργασία του εργαζομένου, ιατρικής διάγνωσης, παροχής υγειονομικής ή κοινωνικής περίθαλψης ή θεραπείας ή διαχείρισης υγειονομικών και κοινωνικών συστημάτων και υπηρεσιών βάσει του

[42] Opinion N° 3/2007 on the Proposal for a Regulation of the European Parliament and of the Council amending the Common Consular Instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics, including provisions on the organisation of the reception and processing of visa applications COM(2006)269 final - WP 134. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp134_en.pdf

ενωσιακού δικαίου ή του δικαίου κράτους μέλους ή δυνάμει σύμβασης με επαγγελματία του τομέα της υγείας.

Το γεγονός ότι διαθέτουμε βιομετρικά δεδομένα δεν σημαίνει αυτομάτως ότι είμαστε υποχρεωμένοι να λάβουμε τα μέγιστα μέτρα ασφαλείας που διατίθενται σήμερα. Αυτό που συνεπάγεται, είναι ότι είναι απαραίτητο να ληφθούν πρόσθετα μέτρα προστασίας ανάλογα με τον όγκο των δεδομένων, και τον σκοπό για τον οποίο πρόκειται να χρησιμοποιηθούν.

Διαφορετικό κίνδυνο αντιμετωπίζει μια εταιρεία που διατηρεί τα βιομετρικά δεδομένα εκατοντάδων χιλιάδων ανθρώπων, και που χρησιμοποιεί αυτά τα δεδομένα για να ταυτοποιήσει τα άτομα μέσω φωτογραφιών τους στα μέσα κοινωνικής δικτύωσης για λόγους στοχευμένης διαφήμισης, και άλλου είδους κίνδυνο διατρέχει μια εταιρεία που διατηρεί τα βιομετρικά δεδομένα των εργαζομένων της απλά για τον έλεγχο παρουσιών. Ως εκ τούτου τα απαιτούμενα μέτρα δεν μπορεί να είναι τα ίδια, αλλά κατάλληλα κατά περίπτωση.

Θα πρέπει να επισημανθεί ότι ο ενωσιακός νομοθέτης στο άρθρο 9 παρ. 4 του ΓΚΠΔ, προνόησε ότι τα κράτη μέλη μπορούν να διατηρούν ή να θεσπίζουν περαιτέρω όρους, μεταξύ άλλων και περιορισμούς, όσον αφορά την επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων ή δεδομένων που αφορούν την υγεία. Έτσι, ο στόχος του περιορισμού της επεξεργασίας βιομετρικών δεδομένων δεν είναι άλλος από την προστασία της ιδιωτικής ζωής των πολιτών. Ως εκ τούτου, η επεξεργασία των βιομετρικών δεδομένων απαιτεί την έγκαιρη σύνταξη εκθέσεων που θα αξιολογούν τον ενδεχόμενο κίνδυνο και τον αντίκτυπο που θα έχει για τα υποκείμενα, μία τυχόν διαρροή βιομετρικών δεδομένων.

2.9.2. Διενέργεια Εκτίμησης Αντικτύπου (DPIA)

Για να εξακριβωθεί ότι τα ληφθέντα μέτρα είναι τα κατάλληλα, οι οργανισμοί που διατηρούν δεδομένα ειδικών κατηγοριών (ευαίσθητα) και εν προκειμένω βιομετρικά

δεδομένα, καλούνται να διενεργήσουν μια νέα διαδικασία που επέβαλε ο νέος κανονισμός και ονομάζεται εκτίμηση αντικτύπου (DPIA) .

Η υποχρέωση για τη διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) προβλέπεται στο άρθρο 35 παρ. 1 του ΓΚΠΔ. Η ΕΑΠΔ διενεργείται από τον υπεύθυνο επεξεργασίας όταν οι πράξεις επεξεργασίας ενδέχεται να επιφέρουν υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων ιδίως με τη χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας[43].

Η Ελληνική αρχή προστασίας δεδομένων, κατήρτισε, βάσει του άρθρου 35 παρ. 4 του ΓΚΠΔ, σχέδιο καταλόγου με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια ΕΑΠΔ. Πρόσφατα, δημοσιεύθηκε στην Εφημερίδα της Κυβερνήσεως[44] ο κατάλογος με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια εκτίμησης αντικτύπου βάσει του άρθρου 35 παρ. 4 του ΓΚΠΔ. Ο εν λόγω κατάλογος ομαδοποιεί και εξειδικεύει περαιτέρω τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια ΕΑΠΔ με παράθεση και ενδεικτικών παραδειγμάτων. Βασίζεται στο άρθρο 35 του ΓΚΠΔ και ιδίως στις παρ. 1 και 3 αυτού καθώς και στις εγκεκριμένες από το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων κατευθυντήριες γραμμές για την εκτίμηση αντικτύπου (WP248)45, τις οποίες συμπληρώνει και εξειδικεύει περαιτέρω.

Μια εκτίμηση αντικτύπου για την πιθανή επεξεργασία βιομετρικών δεδομένων πρέπει :

[43] https://www.dpa.gr/portal/page?_pageid=33,223264&_dad=portal&_schema=PORTAL
[44] ΦΕΚ Β΄ 1622/10-5-2019
[45] Για την παροχή συνεκτικής ερμηνείας των πράξεων επεξεργασίας στις οποίες απαιτείται η διενέργεια ΕΑΠΔ λόγω του υψηλού κινδύνου που ενέχουν, η Ομάδα Εργασίας του άρθρου 29 εξέδωσε τις «Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του κανονισμού 2016/679» (WP248), τις οποίες ενέκρινε το ΕΣΠΔ κατά την πρώτη ολομέλειά του. Σύμφωνα με τις ως άνω κατευθυντήριες γραμμές, στις περισσότερες περιπτώσεις μπορεί να θεωρηθεί ότι απαιτείται ΕΑΠΔ για επεξεργασία στην οποία πληρούνται δύο από τα κριτήρια που προσδιορίζονται σε αυτές. Σε ορισμένες περιπτώσεις, η διενέργεια ΕΑΠΔ απαιτείται όταν πληρούται ένα εκ των εν λόγω κριτηρίων.

- Να περιγράφει τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας.
- Να αξιολογεί την αναγκαιότητα, την αναλογικότητα και τα μέτρα συμμόρφωσης
- Να εντοπίζει και αξιολογεί τους κινδύνους για τα άτομα και
- Να προσδιορίσει τυχόν πρόσθετα μέτρα για τον μετριασμό των εν λόγω κινδύνων[46]

2.9.3. Προϋποθέσεις ορθής επεξεργασίας των βιομετρικών δεδομένων

Πρώτον, είναι απαραίτητο ο χρήστης να δώσει ρητή συγκατάθεση για τη επεξεργασία των βιομετρικών του δεδομένων. Επιπλέον, είναι απαραίτητη για την επεξεργασία η καταγραφή του αρχείου δραστηριοτήτων του οργανισμού, η οποία πρέπει να περιέχει τουλάχιστον τις ακόλουθες πληροφορίες (Shabani, & Borry, 2018:149):

- Εταιρική επωνυμία και στοιχεία επικοινωνίας του υπευθύνου, εκπροσώπου του υπεύθυνου, υπεύθυνου προστασίας δεδομένων και τυχόν συνυπεύθυνου.
- Οι στόχοι της εν λόγω επιχείρησης.
- Η Λεπτομερής περιγραφή των ενδιαφερομένων μερών και των δεδομένων προσωπικού χαρακτήρα.
- Οι αποδέκτες ανά κατηγορίες στις οποίες έχουν κοινοποιηθεί ή θα κοινοποιηθούν τα δεδομένα προσωπικού χαρακτήρα.

[46] Κυπριακό Γραφείο Επιτρόπου Προστασίας Δεδομένων
http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page2c_gr/page2c_gr?opendocument

- Οι προθεσμίες που καθορίστηκαν για την διαγραφή των διαφόρων κατηγοριών δεδομένων.

Ωστόσο, το άρθρο 9 θεσπίζει μια σειρά εξαιρέσεων για τις οποίες κάμπτεται ο απαγορευτικός χαρακτήρας της επεξεργασίας των βιομετρικών δεδομένων ως δεδομένα ειδικής κατηγορίας και συγκεκριμένα επιτρέπεται η επεξεργασία τους στις περιπτώσεις που :

α) το υποκείμενο των δεδομένων έχει παράσχει ρητή συγκατάθεση για την επεξεργασία αυτών των δεδομένων προσωπικού χαρακτήρα για έναν ή περισσότερους συγκεκριμένους σκοπούς, εκτός εάν το δίκαιο της Ένωσης ή κράτους μέλους προβλέπει ότι η απαγόρευση που αναφέρεται στην παράγραφο 1 δεν μπορεί να αρθεί από το υποκείμενο των δεδομένων,

β) η επεξεργασία είναι απαραίτητη για την εκτέλεση των υποχρεώσεων και την άσκηση συγκεκριμένων δικαιωμάτων του υπευθύνου επεξεργασίας ή του υποκειμένου των δεδομένων στον τομέα του εργατικού δικαίου και του δικαίου κοινωνικής ασφάλισης και κοινωνικής προστασίας, εφόσον επιτρέπεται από το δίκαιο της Ένωσης ή κράτους μέλους ή από συλλογική συμφωνία σύμφωνα με το εθνικό δίκαιο παρέχοντας κατάλληλες εγγυήσεις για τα θεμελιώδη δικαιώματα και τα συμφέροντα του υποκειμένου των δεδομένων,

γ) η επεξεργασία είναι απαραίτητη για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου, εάν το υποκείμενο των δεδομένων είναι σωματικά ή νομικά ανίκανο να συγκατατεθεί,

δ) η επεξεργασία διενεργείται, με κατάλληλες εγγυήσεις, στο πλαίσιο των νόμιμων δραστηριοτήτων ιδρύματος, οργάνωσης ή άλλου μη κερδοσκοπικού φορέα με πολιτικό, φιλοσοφικό, θρησκευτικό ή συνδικαλιστικό στόχο και υπό την προϋπόθεση ότι η

επεξεργασία αφορά αποκλειστικά τα μέλη ή τα πρώην μέλη του φορέα ή πρόσωπα τα οποία έχουν τακτική επικοινωνία μαζί του σε σχέση με τους σκοπούς του και ότι τα δεδομένα προσωπικού χαρακτήρα δεν κοινοποιούνται εκτός του συγκεκριμένου φορέα χωρίς τη συγκατάθεση των υποκειμένων των δεδομένων,

ε) η επεξεργασία αφορά δεδομένα προσωπικού χαρακτήρα τα οποία έχουν προδήλως δημοσιοποιηθεί από το υποκείμενο των δεδομένων,

στ) η επεξεργασία είναι απαραίτητη για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων ή όταν τα δικαστήρια ενεργούν υπό τη δικαιοδοτική τους ιδιότητα,

ζ) η επεξεργασία είναι απαραίτητη για λόγους ουσιαστικού δημόσιου συμφέροντος, βάσει του δικαίου της Ένωσης ή κράτους μέλους, το οποίο είναι ανάλογο προς τον επιδιωκόμενο στόχο, σέβεται την ουσία του δικαιώματος στην προστασία των δεδομένων και προβλέπει κατάλληλα και συγκεκριμένα μέτρα για τη διασφάλιση των θεμελιωδών δικαιωμάτων και των συμφερόντων του υποκειμένου των δεδομένων, η) η επεξεργασία είναι απαραίτητη για σκοπούς προληπτικής ή επαγγελματικής ιατρικής, εκτίμησης της ικανότητας προς εργασία του εργαζομένου, ιατρικής διάγνωσης, παροχής υγειονομικής ή κοινωνικής περίθαλψης ή θεραπείας ή διαχείρισης υγειονομικών και κοινωνικών συστημάτων και υπηρεσιών βάσει του ενωσιακού δικαίου ή του δικαίου κράτους μέλους ή δυνάμει σύμβασης με επαγγελματία του τομέα της υγείας και με την επιφύλαξη των προϋποθέσεων και των εγγυήσεων που αναφέρονται στην παράγραφο 3,

θ) η επεξεργασία είναι απαραίτητη για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας, όπως η προστασία έναντι σοβαρών διασυνοριακών απειλών κατά της υγείας ή η διασφάλιση υψηλών προτύπων ποιότητας και ασφάλειας της υγειονομικής περίθαλψης και των φαρμάκων ή των ιατροτεχνολογικών προϊόντων, βάσει του δικαίου

της Ένωσης ή του δικαίου κράτους μέλους, το οποίο προβλέπει κατάλληλα και συγκεκριμένα μέτρα για την προστασία των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων, ειδικότερα δε του επαγγελματικού απορρήτου, ή

ι) η επεξεργασία είναι απαραίτητη για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς σύμφωνα με το άρθρο 89 παράγραφος 1 βάσει του δικαίου της Ένωσης ή κράτους μέλους, οι οποίοι είναι ανάλογοι προς τον επιδιωκόμενο στόχο, σέβονται την ουσία του δικαιώματος στην προστασία των δεδομένων και προβλέπουν κατάλληλα και συγκεκριμένα μέτρα για τη διασφάλιση των θεμελιωδών δικαιωμάτων και των συμφερόντων του υποκειμένου των δεδομένων[47].

2.9.4. Αναβάθμιση των τεχνικών μέτρων ασφαλείας ως αποτέλεσμα του GDPR

Η αποθήκευση των βιομετρικών δεδομένων σε ένα σύστημα ή βάση δεδομένων γίνεται μέσω συγκεκριμένου αλγορίθμου, όπως για παράδειγμα του αλγορίθμου biokey[48] 10, ο οποίος είναι ένας από τους πιο εκτεταμένος σε χρήση αλγόριθμους παγκοσμίως.

Η εισροή των βιομετρικών δεδομένων στο σύστημα πραγματοποιείται μέσω ενός υψηλούς ποιότητας, συμπαγούς σαρωτή δακτυλικών αποτυπωμάτων USB. Η ίδια συσκευή USB λειτουργεί και ως αναγνώστης αναγνώρισης δακτυλικών αποτυπωμάτων. Το λογισμικό με τον ειδικό αλγόριθμο και το εν λόγω hardware καθιστούν την εγγραφή στο σύστημα ιδιαίτερη φιλική και γρήγορη για το χρήστη, ο οποίος άπαξ και καταχωρήσει τα βιομετρικά του δεδομένα στο σύστημα, μπορεί με τη χρήση οποιασδήποτε ανάλογης συσκευής να

[47] https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EL
[48] Το BIO-key είναι ένας συνεργάτης της Microsoft και ένας κορυφαίος κατασκευαστής βιομετρικών λύσεων ελέγχου ταυτότητας δακτυλικών αποτυπωμάτων

πραγματοποιήσει ένα γρήγορο και αξιόπιστο έλεγχο ταυτότητας ή να ενημερώσει για την παρουσία του τον οργανισμό, αντικαθιστώντας τη χρήση κωδικών πρόσβασης και χρησιμοποιώντας μια τεχνολογία που στηρίζεται στη δύναμη της αφής.

Το λογισμικό ελέγχου ταυτότητας αποθηκεύει τις βιομετρικές πληροφορίες στη βάση δεδομένων που βρίσκεται στον κεντρικό υπολογιστή, όχι με τη μορφή εικόνας, αλλά με αλφαριθμητικούς χαρακτήρες που επιτρέπουν συγκρίσεις μεταξύ τους, για να επιτευχθεί η ταύτιση μεταξύ δύο βιομετρικών δεδομένων και να αναγνωρισθεί το άτομο.

Με την έναρξη ισχύος του νέου κανονισμού οι μεγάλες εταιρίες διαχείρισης βιομετρικών δεδομένων βελτίωσαν το λογισμικό που χρησιμοποιούν προκειμένου να ενισχύσουν την ασφάλεια του συστήματος.

Ένα χαρακτηριστικό παράδειγμα αποτελεί η κρυπτογράφηση των βιομετρικών δεδομένων που περιέχονται στο σύστημα, βάσει καινοτόμων τεχνολογιών κωδικοποίησης/αποκωδικοποίησης των βιομετρικών σημάτων. Άλλα βελτιωμένα τεχνικά μέτρα προστασίας θα μπορούσαν να είναι η δημιουργία και λειτουργία μητρώου πρόσβασης στα βιομετρικά δεδομένα, η χρήση κωδικού πρόσβασης για την επικοινωνία μεταξύ του λογισμικού και των βιομετρικών τερματικών, ο διαχωρισμός συσχέτισης δεδομένων και τερματικών,[49] και τέλος η αυτόματη διαγραφή των αχρησιμοποίητων βιομετρικών δεδομένων.

Ειδικότερα η κρυπτογράφηση καθίσταται απαραίτητη για τις μεγάλες βάσεις δεδομένων, καθώς και για τα δεδομένα που επικοινωνούν μέσω δικτύων. Επιπροσθέτως, απαιτείται έλεγχος πρόσβασης, δηλαδή καταγραφή όλων των αποπειρών πρόσβασης που γίνονται στη συγκεκριμένη κατηγορία δεδομένων, με την ταυτόχρονη συλλογή των παρακάτω πληροφοριών

- Το πρόσωπο που αποπειράθηκε ή πέτυχε την πρόσβαση

[49] Με αυτόν τον τρόπο, εάν κάποιος που έχει πρόσβαση στις πληροφορίες ενός τερματικού, δεν θα μπορεί να γνωρίζει σε ποιον ανήκει το κάθε βιομετρικό στοιχείο.

- Την ακριβή ημερομηνία και ώρα πρόσβασης.
- Τα δεδομένα που ήταν προσβάσιμα.

2.10. Ο νέος εθνικός νόμος

Στη χώρα μας στις 30 Αυγούστου του τρέχοντος έτους, δημοσιεύθηκε στην Εφημερίδα της Κυβερνήσεως ο πολυαναμενόμενος νόμος για τα προσωπικά δεδομένα[50], με αριθμό 4624/2019 και τίτλο "Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις".

Ο νόμος αφορά:

α)στην αντικατάσταση του νομοθετικού πλαισίου που ρυθμίζει τη συγκρότηση και λειτουργία της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα,

β)στη λήψη μέτρων εφαρμογής του Κανονισμού 2016/679 (ΓΚΠΔ/GDPR)

γ)στην ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων.

Όσον αφορά στην αντιμετώπιση των βιομετρικών δεδομένων, ο εθνικός νομοθέτης κατά αναλογία με τον ενωσιακό, τα ενέταξε στις «ειδικές κατηγορίες δεδομένων προσωπικού

[50] Εκτελεστική και νομοθετική εξουσία κινήθηκαν εξαιρετικά γρήγορα, μετατρέποντας ένα σχέδιο νόμου υπό διαβούλευση σε Νόμο του Κράτους εντός μόλις 17 ημερών. Εν προκειμένω, η επίσπευση των διαδικασιών μπορεί, εν μέρει, να δικαιολογηθεί και από το γεγονός ότι η Ελλάδα έχει παραπεμφθεί στο Δικαστήριο της Ε.Ε. για την καθυστερημένη ενσωμάτωση της Οδηγίας 680/2016. Βλ. σχετικά https://europa.eu/rapid/press-release_IP-19-4261_en.htm

χαρακτήρα» του άρθρου 44, γεγονός που καθιστά αυστηρότερη την επεξεργασία τους. Το άρθρο 22 ωστόσο απαριθμεί τις περιπτώσεις που κατά παρέκκλιση από το άρθρο 9 παράγραφος 1 του ΓΚΠΔ η επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα με την έννοια του άρθρου 9 παράγραφος 1 του ΓΚΠΔ από δημόσιους και ιδιωτικούς φορείς, επιτρέπεται.

Στο άρθρο 23 «Επεξεργασία γενετικών δεδομένων» ο νομοθέτης προνοεί ότι Κατ' εφαρμογή της παραγράφου 4 του άρθρου 9 του ΓΚΠΔ[51] απαγορεύεται η επεξεργασία γενετικών δεδομένων για σκοπούς ασφάλισης υγείας και ζωής.

Ωστόσο, όπως αναφέρει ο Καρκατζούνης[52] (2019), ειδικά ερμηνευτικά ζητήματα ενδέχεται να δημιουργηθούν από την διατύπωση της παραγράφου 3 του άρθρου 27 αναφορικά με την επεξεργασία δεδομένων ειδικών κατηγοριών, (όπως βιομετρικά δεδομένα). Η παρ. 3 άρθρου 27 αναφέρει χαρακτηριστικά :

Κατά παρέκκλιση από το άρθρο 9 παράγραφος 1 του ΓΚΠΔ η επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα με την έννοια του άρθρου 9 παράγραφος 1 του ΓΚΠΔ για τους σκοπούς της σύμβασης εργασίας επιτρέπεται, εάν είναι απαραίτητη για την άσκηση των δικαιωμάτων ή την εκπλήρωση νόμιμων υποχρεώσεων που απορρέουν από το εργατικό δίκαιο, το δίκαιο της κοινωνικής ασφάλισης και της κοινωνικής προστασίας και δεν υπάρχει κανένας λόγος να θεωρηθεί ότι το έννομο συμφέρον του υποκειμένου των δεδομένων σε σχέση με την επεξεργασία υπερτερεί.

Στο σημείο αυτό ο νομοθέτης φαίνεται να “συγκεκριμενοποιεί” από το άρθρο 9, τις περ. 2α και 2β, ωστόσο η μη αναφορά στις υπόλοιπες βάσεις της εν λόγω παραγράφου του άρθρου 9 δημιουργεί ασάφεια ως προς τη δυνατότητα ισχύος τους στο πλαίσιο αυτό.

[51] Τα κράτη μέλη μπορούν να διατηρούν ή να θεσπίζουν περαιτέρω όρους, μεταξύ άλλων και περιορισμούς, όσον αφορά την επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων ή δεδομένων που αφορούν την υγεία.

[52] Καρκατζούνης Βασίλης, 2019, *Οι νέες διατάξεις για την προστασία προσωπικών δεδομένων των εργαζομένων (Νόμος 4624/2019)*, syntagmawatch.gr

2.11. Αποφάσεις της εθνικής Αρχής ΠΔΠΧ, σχετικά με τη βιομετρικά δεδομένα

Η Αρχή Προστασίας Δεδομένων έχει εκδώσει αρκετές αποφάσεις που αφορούν στη νομιμότητα επεξεργασίας δεδομένων από βιομετρικές εφαρμογές. Λόγω της διαφορετικότητας και πολυπλοκότητας της κάθε εφαρμογής η κάθε περίπτωση έχει κριθεί ξεχωριστά ώστε να επιτυγχάνεται στο μέγιστο βαθμό η προστασία του ατόμου από την επεξεργασία των προσωπικών του δεδομένων.

Κατ' εφαρμογή της αρχής της αναλογικότητας, η Αρχή έχει επιτρέψει τη χρήση βιομετρικών συστημάτων για τον έλεγχο πρόσβασης σε χώρους εργασίας αποκλειστικά και μόνο σε περιπτώσεις ιδιαίτερα κρίσιμων εγκαταστάσεων και με μοναδικό σκοπό την προστασία των προσώπων και των αγαθών εντός αυτών[53].

Η Αρχή με την 52/2003 απόφαση της απαγόρευσε την πιλοτική εφαρμογή βιομετρικού συστήματος στο αεροδρόμιο Ελευθέριος Βενιζέλος, το οποίο είχε σκοπό τη συλλογή και επεξεργασία δεδομένων δακτυλοσκόπησης και ίριδας του ματιού για την επαλήθευση της ταυτότητας των επιβατών που πρόκειται να ταξιδέψουν[54].

Σε παρόμοιο σκεπτικό, η Αρχή με την 59/2005 απόφαση της έκρινε ότι η εφαρμογή βιομετρικού συστήματος για την συλλογή και επεξεργασία δεδομένων δακτυλοσκόπησης με σκοπό τον έλεγχο πρόσβασης φιλάθλων και διαπιστευμένων ατόμων σε αθλητικές εγκαταστάσεις δεν είναι νόμιμη και συνεπώς δεν επιτρέπεται η εγκατάσταση πιλοτικού συστήματος δοκιμής τέτοιας επεξεργασίας, ακόμα και αν αυτό έχει καθαρά ερευνητικό χαρακτήρα. Αντίθετα, θεωρείται ότι η επίτευξη του εν λόγω ερευνητικού σκοπού μπορεί να πραγματοποιηθεί με άλλα ηπιότερα μέσα, όπως π.χ. δοκιμή του συστήματος σε εργαστηριακές συνθήκες[55].

[53] Βλ. «Το Νομικό Πλαίσιο της Επεξεργασίας Βιομετρικών Δεδομένων», 2019, https://lawandtech.eu/ , 9-9-19
[54] ΑΠΟΦΑΣΗ ΑΡ. 52/2003 - Απόφαση για την εφαρμογή συστήματος βιομετρικών μεθόδων στο αεροδρόμιο Ελευθέριος Βενιζέλος
[55] ΑΠΟΦΑΣΗ ΑΡ. 59/2005 - Απόρριψη αίτησης για εγκατάσταση πιλοτικού βιομετρικού συστήματος ελέγχου αθλητικών εγκαταστάσεων.

Στις παραπάνω αποφάσεις αναπτύσσεται η βασική θέση της αρχής ότι επεξεργασία βιομετρικών δεδομένων δεν είναι αναγκαία για την επίτευξη των συγκεκριμένων σκοπών . Ωστόσο δύναται να επιτραπεί η χρήση βιομετρικών τεχνολογιών για την πρόσβαση σε καταστάσεις υψηλής ασφαλείας πάντα όμως με την τήρηση αυστηρών προϋποθέσεων[56].

Ενδεικτική του πλαισίου της ως άνω «εξαίρεσης» αποτελεί η απόφαση 56/2009 της ΑΠΔΠΧ. Η ελληνική Αρχή με την 56/2009 απόφασή της αποδέχθηκε (και δεν έκρινε ως τελικά παράνομη) τη χρήση εξοπλισμού αναγνώρισης δακτυλικού αποτυπώματος επειδή αφορούσε σε συγκεκριμένους εργαζομένους που θα είχαν ειδική πρόσβαση σε ένα συγκεκριμένο χώρο, *«…όπου παράγονται και τηρούνται τα ιδιωτικά κλειδιά των Αρχών Πιστοποίησης τα οποία υπογράφουν τα Αναγνωρισμένα Πιστοποιητικά τελικών χρηστών»*. Ο συγκεκριμένος χώρος θα ήταν δυνατό να χαρακτηρισθεί ως υψίστης ασφαλείας και η δικαιολόγηση της επιλογής αυτής είναι η προστασία του δημοσίου συμφέροντος. Η συγκεκριμένη απόφαση μάλιστα, αφορά σε λόγους αρχής και ουσίας και όχι τεχνικούς. [Εκ περισσού να σημειωθεί ότι ο χρησιμοποιούμενος εξοπλισμός πληρούσε όλες τις αναγκαίες προδιαγραφές: (α) κρυπτογράφηση δεδομένων, (β) μη διατήρηση δεδομένων και (γ) τοπικό χαρακτήρα- μη σύνδεση με κεντρικό σύστημα[57]

2.12. ΗΠΑ: ο νόμος περί απορρήτου των βιομετρικών πληροφοριών (BIPA)

Στις Ηνωμένες πολιτείες η νομοθεσία για την επεξεργασία των βιομετρικών δεδομένων βρίσκεται στο στάδιο της εξέλιξης, καθώς όλο και περισσότερες πολιτείες επιδιώκουν να εισαγάγουν ένα σαφές ρυθμιστικό πλαίσιο σχετικά με τη συλλογή, τη χρήση και τη διατήρηση βιομετρικών δεδομένων. Επί του παρόντος, μόνο τρεις πολιτείες, το

56 Νάιδου Πετρινή , 2019, *GDPR: Η Επόμενη Μέρα. Βιομετρικά δεδομένα και εργασία*, Εφημερίδα ΜΑΚΕΔΟΝΙΑ, 24 Φεβρουαρίου 2019.

57 ΑΠΟΦΑΣΗ ΑΡ. 56/2009 - Εφαρμογή συστήματος δακτυλοσκόπησης για πρόσβαση εργαζομένων σε εγκαταστάσεις υψηλής ασφαλείας.

Illinois[58], το Τέξας[59] και η Ουάσιγκτον[60], έχουν θεσπίσει νόμους για την προστασία της ιδιωτικότητας των βιομετρικών δεδομένων, ενώ η California[61] πρόκειται να θέσει σε εφαρμογή την 1η Ιανουαρίου του 2020 το πρόσφατο νομοθέτημα Consumer Privacy Act (CCPA). Η Αριζόνα, η Φλόριντα και η Μασαχουσέτη έχουν επίσης προτείνει τη θέσπιση νομοθεσίας για την προστασία των βιομετρικών δεδομένων ενώ και άλλες πολιτείες εξετάζουν αυτό το ενδεχόμενο.

Ενώ τα πρόσφατα σχετικά νομοσχέδια αναγνωρίζουν την αναγκαιότητα ρύθμισης της συλλογής, διατήρησης και χρήσης των βιομετρικών δεδομένων, οι προσεγγίσεις τους διαφέρουν σημαντικά και υπογραμμίζουν τους διαφορετικούς τρόπους με τους οποίους οι πολιτείες προσπαθούν να συμβαδίσουν με την τεχνολογική πρόοδο.

Μια βασική διαφορά στις προσεγγίσεις των πολιτειών έγκειται στο εάν (α) επιτρέπεται μόνο ο γενικός εισαγγελέας της εκάστοτε πολιτείας να επιβάλει τον νόμο περί βιομετρικής ιδιωτικότητας, ή (β) στο να δημιουργηθεί ένα ιδιωτικό δικαίωμα δράσης, το οποίο θα επιτρέπει στα υποκείμενα των δεδομένων, να προσφεύγουν με ιδιωτική πρωτοβουλία στα πολιτικά δικαστήρια, διεκδικώντας αποζημιώσεις δεκάδων εκατομμυρίων, όπως αποδεικνύεται από τις εκατοντάδες των αγωγών αποζημίωσης που έχουν υποβληθεί για παραβιάσεις της σχετικής νομοθεσίας στο Illinois. Ειδικότερα, ο ψηφισμένος νόμος της California προνοεί περιορισμένο ιδιωτικό δικαίωμα δράσης σχετικά με την επεξεργασία των προσωπικών δεδομένων χωρίς να γίνεται ειδική αναφορά στις βιομετρικές πληροφορίες[62].

Άλλες διαφορές εντοπίζονται στον τρόπο με τον οποίο κάθε πολιτεία ορίζει τη βιομετρική πληροφορία ή βιομετρικό στοιχείο αναγνώρισης. Για παράδειγμα, οι βιομετρικές

[58] 740 ILCS 14/5
[59] TEX. BUS & COM. § 503.001.
[60] WASH. REV. CODE § 19.35
[61] CAL. CIV. CODE § 1798.100 et seq.
[62] CAL. CIV. CODE § 1798.150, limiting private right of action to personal information as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5.

πληροφορίες βάσει του CCPA στην California, ορίζονται με ένα ευρύ φάσμα ώστε να συμπεριλαμβάνουν φυσιολογικά, βιολογικά και συμπεριφορικά χαρακτηριστικά και περιλαμβάνουν όχι μόνο την παραδοσιακή ανίχνευση δακτυλικών αποτυπωμάτων και αμφιβληστροειδούς, αλλά και τα μοτίβα πληκτρολόγησης και βηματισμού καθώς και δεδομένα «ύπνου, υγείας και άσκησης» που περιέχουν στοιχεία αναγνώρισης του υποκειμένου.

Η Ουάσιγκτον χρησιμοποιεί έναν παρόμοιο επεκτατικό ορισμό, ο οποίος περιλαμβάνει τα δεδομένα που προκύπτουν από αυτόματες μετρήσεις των βιολογικών χαρακτηριστικών ενός ατόμου, όπως δακτυλικό αποτύπωμα, φωνητική αποτύπωση, αμφιβληστροειδείς ή άλλα μοναδικά βιολογικά χαρακτηριστικά που χρησιμοποιούνται για την αναγνώριση ατόμων. Ιλλινόις και Τέξας, από την άλλη πλευρά, περιορίζουν τον ορισμό του βιομετρικού στοιχείου αναγνώρισης σε συγκεκριμένους τύπους πληροφοριών, συμπεριλαμβανομένων δακτυλικών αποτυπωμάτων, σαρώσεων αμφιβληστροειδούς ή ίριδας, φωνητικών αποτυπωμάτων ή αρχείων πρόσωπο-γεωμετρίας.

Ωστόσο, ο νόμος του Illinois (BIPA) διευρύνει την έννοια της "βιομετρικής πληροφορίας", η οποία ορίζεται ως «οποιαδήποτε πληροφορία, ανεξάρτητα από τον τρόπο που συλλέγεται, μετατρέπεται, αποθηκεύεται ή διανέμεται, σχετίζεται με βιομετρικό στοιχείο ενός ατόμου και χρησιμοποιείται για την αναγνώριση του ατόμου».

Καθώς όλο και περισσότερες πολιτείες εξετάζουν ή πρόκειται σύντομα να εφαρμόσουν ειδική νομοθεσία για την προστασία των βιομετρικών δεδομένων, καθίσταται όλο και πιο σημαντικό για τις εταιρείες και τους οργανισμούς να διασφαλίζουν ότι είναι προετοιμασμένοι και ότι βρίσκονται σε συμμόρφωση με τους ισχύοντες και εν δυνάμει εφαρμοστέους βιομετρικούς νόμους περί ιδιωτικότητας.

2.12.1. Ιλινόις

Στην πολιτεία του Ιλινόις ο νόμος για την ιδιωτικότητα των βιομετρικών πληροφοριών, ο γνωστός Biometric Information Privacy Act (BIPA)[63] ψηφίστηκε και τέθηκε άμεσα σε ισχύ, στις 3 Οκτωβρίου 2008. Ο BIPA[64] προστατεύει απο την παράνομη συλλογή και αποθήκευση βιομετρικών πληροφοριών. Όταν το Ιλινόις εισήγαγε το συγκεκριμένο νόμο το 2008, έγινε η πρώτη πολιτεία των ΗΠΑ που εφάρμοσε ένα κανονιστικό πλαίσιο εξειδικευμένο στη συλλογή βιομετρικών πληροφοριών.

Ο BIPA παραμένει μέχρι σήμερα ο μοναδικός βιομετρικός νόμος στις ΗΠΑ, που επιτρέπει στους ιδιώτες να καταθέτουν αγωγή για ζημίες που προκύπτουν από παραβίαση των διατάξεων του. Ο νόμος προβλέπει επίσης καταβολή αποζημίωσης ύψους 1,000 δολαρίων ανά παράβαση και 5,000 δολαρίων ανά παράβαση εάν συντρέχει δόλος αλλά και βαριά αμέλεια. Λόγω αυτής της πρόνοιας για αστικές αποζημιώσεις, ο BIPA έχει προκαλέσει σωρεία αγωγών προς ιδιώτες.

Ο BIPA απαιτεί από τις εταιρείες που δραστηριοποιούνται στο Ιλινόις να συμμορφώνονται με συγκεκριμένες απαιτήσεις σχετικά με τη συλλογή και αποθήκευση βιομετρικών πληροφοριών. Αυτές περιλαμβάνουν :

- Την λήψη της προηγούμενης συγκατάθεσης των υποκειμένων, εάν η εταιρεία σκοπεύει να συλλέξει ή να γνωστοποιήσει τα προσωπικά βιομετρικά τους αναγνωριστικά στοιχεία.

[63] "Public Act 0994 95TH GENERAL ASSEMBLY". www.ilga.gov.

[64] Το Senate Bill 2400, το οποίο τελικά έγινε ο βιομετρικός νόμος για την προστασία της ιδιωτικής ζωής, εισήχθη από τον κρατικό γερουσιαστή Terry Link στις 14 Φεβρουαρίου 2008. πέρασε και τα δύο Σπίτια της Γενικής Συνέλευσης του Ιλινόις στις 10 Ιουλίου 2008 και εγκρίθηκε από τον τότε κυβερνήτη Rod Blagojevich στις 3 Οκτωβρίου 2008. Σκοπός του νόμου ήταν η θέσπιση κανόνων συμπεριφοράς για τις ιδιωτικές επιχειρήσεις που συλλέγουν ή κατέχουν βιομετρικά στοιχεία. Το 2016, ο Senator Link πρότεινε και στη συνέχεια απέσυρε μια τροποποίηση του νόμου που θα περιόριζε την εφαρμογή του νόμου σε βιομετρικά δεδομένα που συλλέχθηκαν από το κοινό.

- Την καταστροφή των βιομετρικών δεδομένων μετά απο ορισμένο χρονικό διάστημα. Με την πάροδο τριών ετών απο την τελευταία αλληλεπίδραση του ατόμου με τον φορέα διατήρησης της πληροφορίας ή άμεσα εάν αλλάξει ο αρχικός σκοπός της συλλογής ή της απόκτησης αυτών των βιομετρικών δεδομένων.

- Την ασφαλή αποθήκευση των βιομετρικών αναγνωριστικών στοιχείων.

Επιπρόσθετα, στο Ιλινόις, ο νόμος για την προστασία των βιομετρικών πληροφοριών επιτρέπει στους εργαζόμενους να μηνύσουν τους εργοδότες τους, για την κακόβουλη χρήση των βιομετρικών τους δεδομένων. Σύμφωνα με το περιοδικό Cook County, στο Ιλινόις, τόσο η εταιρεία σούπερ μάρκετ Mariano όσο και το Intercontinental Hotel Group έχουν δεχθεί αγωγές αποζημίωσης απο εργαζόμενους που υποστηρίζουν ότι οι συγκεκριμένες εταιρίες συλλέγουν και αποθηκεύουν τα δακτυλικά αποτυπώματα και άλλα βιομετρικά τους δεδομένα, χωρίς τη συγκατάθεση τους[65].

Ο νόμος έχει επίσης αποτελέσει σημείο σύγκρουσης μεταξύ εταιριών τεχνολογίας που χρησιμοποιούν την αναγνώριση προσώπου ως εργαλείο ταξινόμησης φωτογραφιών, όπως το Facebook και το Google και των χρηστών των μέσων κοινωνικής δικτύωσης στο Ιλινόις. Οι ενάγοντες ισχυρίζονται ότι το Facebook συγκέντρωσε τα βιομετρικά δεδομένα των χρηστών κρυφά και χωρίς συγκατάθεση. Συγκεκριμένα, ισχυρίζονται ότι το πρόγραμμα Suggestions Tag[66] παραβίασε τον BIPA επειδή το Facebook δεν πληροφόρησε τους

[65] Minnis, Glenn (2018-03-02). "Employers facing surge in class action suits over storage, use of employee fingerprints, other biometrics". Cook County Record. https://cookcountyrecord.com/stories/511172229-employers-facing-surge-in-class-action-suits-over-storage-use-of-employee-fingerprints-other-biometrics

[66] Η περίπτωση αυτή σχετίζεται με την εφαρμογή "Suggestions Tag" του Facebook, η οποία τέθηκε σε εφαρμογή το 2010. Το πρόγραμμα λειτουργεί με σάρωση των μεταφορτωμένων φωτογραφιών και στη συνέχεια εντοπίζει πρόσωπα που εμφανίζονται σε αυτές. Εάν το πρόγραμμα αναγνωρίσει και προσδιορίσει ένα από τα πρόσωπα που εμφανίζονται στη φωτογραφία, το Facebook θα προτείνει το όνομα του ατόμου μέσω της αυτόματης επισήμανσης του. Στην πραγματικότητα, το πρόγραμμα παρουσιάζει τα ονόματα των προσώπων στις φωτογραφίες και προτρέπει τους χρήστες να επισημάνουν αυτά τα άτομα με Tag. Το Facebook χρησιμοποιεί την τεχνολογία αναγνώρισης προσώπου "state-of-the-art" για την εξαγωγή βιομετρικών αναγνωριστικών από τις φωτογραφίες που μεταφορτώνουν οι χρήστες. Στη συνέχεια δημιουργεί και αποθηκεύει ψηφιακές αναπαραστάσεις (γνωστές ως "πρότυπα") των προσώπων των χρηστών, βάσει της γεωμετρικής

ενάγοντες γραπτώς ότι τα βιομετρικά τους αναγνωριστικά στοιχεία (γεωμετρία προσώπου) παράγονται, συλλέγονται και αποθηκεύονται[67].

Στη συνέχεια το Facebook υπέβαλε αίτηση για απόρριψη της αγωγής. Η πρόταση προέβαλε δύο επιχειρήματα: (1) "οι ενάγοντες δεν μπορούν να διεκδικήσουν αξιώσεις στηριζόμενοι στο νόμο BIPA του Ιλινόις επειδή έχουν ήδη δεχθεί ότι για τις διαφωνίες τους με το Facebook εφαρμόζονται οι νόμοι της πολιτείας της Καλιφόρνια " και (2) ο νόμος "BIPA του Ιλινόις δεν έχει πεδίο εφαρμογής σε τέτοιου είδους υπηρεσίες". Οι ενάγοντες αρνήθηκαν ότι συμφώνησαν σε οτιδήποτε με το Facebook, συμπεριλαμβανομένης της διάταξης περί επιλογής του νόμου. Μετά από πρόσθετη ενημέρωση και από τις δύο πλευρές, το Δικαστήριο έκρινε ότι είναι εφαρμοστέο το δίκαιο του Ιλινόις και ότι οι ενάγοντες έχουν προβεί σε αξίωση που εμπίπτει πεδίο εφαρμογής του BIPA. Το Facebook έχει προωθήσει νομοθετικές αναθεωρήσεις στο νόμο σε αρκετές περιπτώσεις, αλλά μέχρι στιγμής χωρίς επιτυχία.

Η πιο πρόσφατη δικαστική υπόθεση που σχετίζεται με την εφαρμογή του BIPA και δέχθηκε αρκετές κριτικές είναι η Rosenbach v. Six Flags Entertainment Corp[68]. Στις 25 Ιανουαρίου 2019, το Ανώτατο Δικαστήριο του Ιλινόις έκρινε ότι ένα πρόσωπο μπορεί να απαιτήσει αποζημίωση κατόπιν παραβίασης του νόμου για την προστασία της ιδιωτικής ζωής στον τομέα των βιομετρικών πληροφοριών του Ιλινόις (BIPA), ακόμη και αν το πρόσωπο αυτό δεν υπέστη πραγματική ζημία από την παραβίαση.

σχέσης των χαρακτηριστικών του προσώπου που είναι μοναδικά σε κάθε άτομο όπως η απόσταση μεταξύ των ματιών, της μύτης και των αυτιών κλπ.

[67] Case No. 15-cv-03747-JD, IN RE FACEBOOK BIOMETRIC INFORMATION PRIVACY LITIGATION,United States District Court, N.D. California, Signed May 5, 2016.

[68] Rosenbach v. Six Flags Entertainment Corp., 2019 IL 123186, https://courts.illinois.gov/Opinions/SupremeCourt/2019/123186.pdf

2.12.2. Αριζόνα

Στις 28 Ιανουαρίου 2019 ψηφίστηκε το νομοσχέδιο 2478 της Αριζόνα ("HB 2478"), το οποίο, το οποίο απαγορεύει στις εταιρίες να συλλέγουν, να επεξεργάζονται ή να αποθηκεύουν τα βιομετρικά αναγνωριστικά στοιχεία ενός ατόμου, για εμπορικούς σκοπούς, δημιουργώντας έτσι έναν μηχανισμό για την αποτροπή της επακόλουθης χρήσης βιομετρικών δεδομένων για σκοπούς αυτού του είδους.

Ο HB 2478 ενσωματώνει τις ανάλογες διατάξεις του δίκαιου περί προστασίας της ιδιωτικής ζωής και των βιομετρικών δεδομένων της πολιτείας της Ουάσινγκτον και κατά αναλογία με το νόμο της Καλιφόρνια και της Ουάσινγκτον, ο νόμος της Αριζόνα, διευρύνει την έννοια του "βιομετρικό αναγνωριστικού στοιχείου" ώστε να περιλαμβάνει εκτός απο το δακτυλικό αποτύπωμα, τον αμφιβληστροειδή και την πρόσωπο-γεωμετρία, οποιοδήποτε άλλο "μοναδικό βιολογικό χαρακτηριστικό που χρησιμοποιείται για τον προσδιορισμό συγκεκριμένου ατόμου.

2.12.3. Μασαχουσέτη

Τον Ιανουάριο του τρέχοντος έτους (2019), η πολιτεία της Μασαχουσέτης ψήφισε νόμο με τίτλο "Νομοθετική Πράξη σχετικά με την Ιδιωτικότητα των δεδομένων των καταναλωτών" ("S.120"). Η βιομετρική πληροφορία ορίζεται επίσης ευρέως και περιλαμβάνει όχι μόνο σαρώσεις αμφιβληστροειδούς, δακτυλικά αποτυπώματα και αποτυπώσεις παλάμης, αλλά και «στυλ» ή ρυθμούς πληκτρολόγησης, ρυθμούς βάδισης , ακόμα και μοτίβο ύπνου ή άσκησης. Οι φορείς συλλογής πληροφοριών που εμπίπτουν στο πεδίο εφαρμογής του S.120 υποχρεούνται να ενημερώνουν εκ των προτέρων τους καταναλωτές σχετικά με τις διάφορες κατηγορίες προσωπικών πληροφοριών που συλλέγονται, τον επιχειρησιακό σκοπό αυτής της συλλογής και την τυχόν κοινοποίηση τους

σε τρίτους. Εκτός από τις απαιτήσεις προειδοποίησης, ο S.120 επιτρέπει στους καταναλωτές να αποκτήσουν αντίγραφο των προσωπικών τους πληροφοριών που συλλέχθηκαν αλλά και να ζητήσουν τη διαγραφή τους. Ο S.120 περιλαμβάνει επίσης μια διάταξη που απαγορεύει τις διακρίσεις. Η διάταξη απαγορεύει στις επιχειρήσεις να αντιμετωπίζουν με διαφορετικό τρόπο τους καταναλωτές οι οποίοι ασκούν τα δικαιώματά.

2.12.4. Φλόριντα

Στα τέλη Φεβρουαρίου του 2019, η πολιτεία της Φλόριντα ψήφισε και έθεσε σε εφαρμογή τον δικό της νόμο για τα βιομετρικά δεδομένα, το επονομαζόμενο "Biometric Information Privacy Act" (πανομοιότυπος με τον BIPA του Ιλινόις). Βάσει του εν λόγω νόμου, κάθε οργανισμός ή εταιρία που διατηρεί βιομετρικές πληροφορίες θα πρέπει να συντάξει και να εφαρμόσει μια δημόσια διαθέσιμη πολιτική σχετικά με τις διαδικασίες αποθήκευσης και καταστροφής των βιομετρικών πληροφοριών.

Επίσης ο νόμος απαγορεύει την πώληση, τη μίσθωση, το εμπόριο ή το κέρδος από τις βιομετρικές πληροφορίες ενός ατόμου και απαιτούν προηγούμενη εξουσιοδότηση απο το υποκείμενο των δεδομένων πριν αυτά γνωστοποιηθούν σε τρίτους. Ο νέος νόμος της Φλόριντα πρόκειται να τεθεί σε ισχύ τον Οκτώβριο του 2019.

Αν και το περιεχόμενο των προτεινόμενων αλλά και τον ισχυόντων νομοθετικών ρυθμίσεων που έχουν εισαχθεί απο την κάθε πολιτεία μεμονωμένα, είναι ανομοιογενές, οι εταιρείες και οι οργανισμοί που ενδεχομένως συλλέγουν, αποθηκεύουν ή χρησιμοποιούν βιομετρικές πληροφορίες στις ΗΠΑ θα πρέπει να συνεχίσουν να παρακολουθούν τις εξελίξεις του πολιτειακού και του ομοσπονδιακού δικαίου για να εξασφαλίσουν τη συμμόρφωση τους με τις νέες διατάξεις. Υπό το φως της σαφούς τάσης όλων των πολιτειών να εφαρμόσουν άμεσα ένα κανονιστικό πλαίσιο για την προστασία των βιομετρικών

δεδομένων και της ταχύτητας με την οποία προτείνονται και ψηφίζονται οι νέοι σχετικοί νόμοι, οι ενδιαφερόμενοι δέον θα ήταν να σχεδιάσουν και εφαρμόσουν πολιτικές και διαδικασίες για την προστασία των βιομετρικών πληροφοριών που είναι σε συμμόρφωση με τις υφιστάμενες νομοθετικές διατάξεις, όπως αυτές ήδη ισχύουν στις προαναφερθείσες πρωτοπόρες στον τομέα αυτό πολιτείες.

2.12.5. Καλιφόρνια

Το διάταγμα περί επιτήρησης και προστασίας της ιδιωτικότητας που υπεγράφη στις 6 Μαΐου 2019 από το συμβούλιο Εποπτικών Αρχών του Σαν Φρανσίσκο[69] απαγορεύει ρητά την χρήση τεχνολογιών βιομετρικής αναγνώρισης προσώπων σε όλους τους δημόσιους χώρους της πόλης του Σαν Φρανσίσκο. Με το εν λόγω νομοθέτημα πραγματοποιήθηκε, παγκοσμίως, η πρώτη απαγόρευση χρήσης της τεχνολογίας αναγνώρισης προσώπων σε μιας μεγάλη πόλη. Το διάταγμα απαγορεύει στην κυβέρνησή τη χρήση του face recognition, συμπεριλαμβανομένης και της αστυνομίας (San Francisco Police Department)[70].

2.13. Ηνωμένο Βασίλειο

Στο Ηνωμένο Βασίλειο, ο νόμος περί προστασίας δεδομένων του 2018 (c 12)[71] , οποίος μετα την ψήφιση του υπεγράφη απο την βασίλισσα στις 23 Μαΐου, 2018, είναι ο ισχύων νόμος ο οποίος επικαιροποίησε τους νόμους περί προστασίας δεδομένων στο Ηνωμένο Βασίλειο. Πρόκειται για έναν εθνικό νόμο ο οποίος συμπληρώνει τον κανονισμό

[69] Το Συμβούλιο Εποπτικών Αρχών του Σαν Φρανσίσκο είναι το νομοθετικό όργανο της κυβέρνησης της Πόλης και της επαρχίας του Σαν Φρανσίσκο, Καλιφόρνια, Ηνωμένες Πολιτείες. https://sfbos.org/

[70] Conger Kate, 2019, Tech-Savvy City Bans a Crime-Fighting Tool: Facial Recognition, New York Times, May 15, Page 1,

[71] Data Protection Act 2018, UK Public General Acts2018 c. 12

για την προστασία γενικών δεδομένων της Ευρωπαϊκής Ένωσης (GDPR) και επικαιροποιεί τον νόμο περί προστασίας δεδομένων του 1998.

Ο νόμος εισάγει νέα αδικήματα όπως την απο πρόθεση ή απο αμέλεια αποκάλυψη προσωπικών δεδομένων χωρίς τη συγκατάθεση του υποκειμένου, την πώληση ή την προσφορά προς πώληση προσωπικών δεδομένων που ελήφθησαν με διαφορετικό προς χρήση σκοπό.

Ουσιαστικά, ο νόμος εφαρμόζει εκείνα τα μέρη του GDPR που «καθορίζονται από το δίκαιο των κρατών μελών» και δημιουργεί ένα πλαίσιο παρόμοιο με το GDPR για την επεξεργασία προσωπικών δεδομένων. Αυτό περιλαμβάνει και την επεξεργασία προσωπικών δεδομένων μέσω των υπηρεσιών πληροφοριών, των υπηρεσιών μετανάστευσης και γενικά όλων των δημοσίων αρχών.

Η βρετανική κυβέρνηση δήλωσε ότι ο νέος νόμος για την προστασία των δεδομένων καθιστά το κανονιστικό πλαίσιο προστασίας δεδομένων κατάλληλο για την ψηφιακή εποχή στην οποία γίνεται επεξεργασία όλο και μεγαλύτερης ποσότητας δεδομένων ,επιτρέπει στα άτομα να αναλάβουν τον έλεγχο των δεδομένων τους, υποστηρίζει τις επιχειρήσεις και τους οργανισμούς του Ηνωμένου Βασιλείου και εγγυάται ότι το Ηνωμένο Βασίλειο είναι προετοιμασμένο, ως προς αυτό τον τομέα για το επερχόμενο Brexit. Άλλωστε ο ίδιος ο νόμος για την απόσυρση του H.B. από την E.E. European Union (Withdrawal) Act 2018, αναφέρει ότι ο κανονισμός θα ενσωματωθεί άμεσα στο εθνικό δίκαιο αμέσως μετά την έξοδο του Ηνωμένου Βασιλείου από την Ευρωπαϊκή Ένωση[72].

Αυτό που καθιστά το βρετανικό νόμο για την προστασία δεδομένων ιδιαίτερο, είναι ότι επεκτείνει το GDPR και σε άλλα πεδία αρμοδιότητας. Το Ηνωμένο Βασίλειο αποφάσισε

[72] Incorporation of direct EU legislation, http://www.legislation.gov.uk/ukpga/2018/16/section/3/enacted

στην πραγματικότητα να διευρύνει το πεδίο εφαρμογής του GDPR και να τον εφαρμόσει και περιπτώσεις όπως η μεταναστευτική πολιτική ή οι ποινικές καταδίκες.

2.14. Η αναπτυσσόμενη παγκόσμια συναίνεση για την προστασία των βιομετρικών δεδομένων

Περισσότερες από 120 χώρες έχουν ήδη ψηφίσει και εφαρμόσει νομοθεσία για την προστασία των προσωπικών δεδομένων (στην έννοια των οποίων εμπίπτουν και τα βιομετρικά δεδομένα), ενώ άλλες 30 βρίσκονται στην διαδικασία διαβούλευσης για την εισαγωγή παρόμοιων νομοθετημάτων[73]. Ωστόσο η νομοθεσία που είναι σχετική με τη προστασία των βιομετρικών δεδομένων δεν είναι ιδιαίτερα διαδεδομένη παγκοσμίως και το γεγονός αυτό οδηγεί σε αποκλίσεις όσον αφορά στις νομοθετικές προσεγγίσεις.

Η Γερμανία για παράδειγμα είναι γνωστή για την εφαρμογή αυστηρής νομοθεσίας για τα προσωπικά δεδομένα και την ιδιωτικότητα αλλά την ίδια στιγμή επιτρέπει τη λειτουργία τεχνολογίας αναγνώρισης προσώπου στους σιδηροδρομικούς σταθμούς.

Για την προστασία του δικαιώματος της ιδιωτικότητας υπάρχουν διεθνώς αρκετά νομοθετικά κείμενα και χωρίς να προσπαθήσουμε να παρουσιάσουμε έναν εξαντλητικό κατάλογο αυτών αξίζει να αναφερθούμε στη «Συνθήκη για την προστασία του ατόμου σε σχέση με την αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων» της 28ης Ιανουαρίου 1981 του Συμβουλίου της Ευρώπης. (Convention for the protection of individuals with regard to automatic processing of personal data)[74]. Το κείμενο αυτό έθεσε τις θεμελιώδεις υποχρεώσεις των κρατών-μελών του Συμβουλίου της Ευρώπης για την προστασία των

[73] https://www.wired.com/story/hackers-say-broke-face-id-security/

[74] Όλα τα μέλη του Συμβουλίου της Ευρώπης έχουν επικυρώσει τη συνθήκη, αλλά και κράτη εκτός του Συμβουλίου της Ευρώπης, το Cabo Verde, ο Μαυρίκιος, το Μεξικό, η Σενεγάλη, η Τυνησία και η Ουρουγουάη έχουν προσχωρήσει στη συνθήκη.

προσωπικών δεδομένων του ατόμου, λαμβάνοντας υπόψη την αυξανόμενη διασυνοριακής ροή δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε αυτόματη επεξεργασία[75].

Στις 28 Ιανουαρίου 2019, με την ευκαιρία της Διεθνούς Ημέρας Προστασίας Δεδομένων, η Συμβουλευτική Επιτροπή της Σύμβασης για την Προστασία των Προσώπων σε σχέση με την Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα (Σύμβαση 108) δημοσίευσε τις Οδηγίες για την Τεχνητή Νοημοσύνη και την Προστασία των Δεδομένων (New Guidelines on Artificial Intelligence and Data Protection).

Οι κατευθυντήριες γραμμές στοχεύουν να βοηθήσουν τους κατασκευαστές και τους υπεύθυνους για τη χάραξη πολιτικής τεχνητής νοημοσύνης (AI), να διασφαλίσουν ότι οι εφαρμογές τους δεν υπονομεύουν το δικαίωμα προστασίας των δεδομένων. Όπως ανέφερε η Επιτροπή σε έκθεση[76] που συνέταξε ο Mantelero (2019), "τα προσωπικά δεδομένα αποτελούν με αυξανόμενους ρυθμούς τόσο την πηγή όσο και τον στόχο των εφαρμογών τεχνητής νοημοσύνης. Επιπρόσθετα οι τελευταίες δεν υπόκεινται σε κάποιο κανονιστικό πλαίσιο και συχνά παραβλέπουν θεμελιώδη δικαιώματα του ατόμου.

Η υιοθέτηση ενός νομικού πλαισίου από το συμβούλιο της Ευρώπης, στοχεύει στην ανάπτυξη εφαρμογών τεχνητής νοημοσύνης που θα σέβονται τα ατομικά δικαιώματα και οι όποιες δεν θα αποτελούν προϊόν αλόγιστης βούλησης των τεχνολογικών κολοσσών που πιέζονται από τον ανταγωνισμό της συγκεκριμένης αγοράς.

Το συμβούλιο της Ευρώπης υπογραμμίζει ότι η προστασία των ανθρωπίνων δικαιωμάτων συμπεριλαμβανομένου του δικαιώματος προστασίας των προσωπικών δεδομένων θα πρέπει να αποτελεί το βασικό ζητούμενο κατά τη διάρκεια κατασκευής μιας

75 Treaty No.108, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

76 Mantelero Alessandro, 2019, *Report on Artificial Intelligence Artificial Intelligence and Data Protection: Challenges and Possible Remedies*, Council of Europe, Strasbourg, 25 January 2019

εφαρμογής τεχνητής νοημοσύνης ειδικά όταν αυτή χρησιμοποιείται στην διαδικασία λήψης αυτοματοποιημένων αποφάσεων και να λαμβάνονται υπ' όψη οι αρχές της επικαιροποιημένης συνθήκης προσωπικών δεδομένων (Συνθήκη 108+)[77] του Οκτωβρίου 2018.

Επιπρόσθετα κάθε καινοτομία στο πεδίο της τεχνητής νοημοσύνης θα πρέπει να είναι σχεδιασμένη με τρόπο που θα ελαχιστοποιεί τον κίνδυνο για τα προσωπικά δεδομένα και που θα επιτρέπει στα υποκείμενα των δεδομένων να διατηρούν τον έλεγχο στα δεδομένα τους και στα αποτελέσματα που αυτά παράγουν από τυχόν επεξεργασία.

Οι συγκεκριμένες κατευθυντήριες οδηγίες σχετικά με την τεχνητή νοημοσύνη αντιμετώπισαν πολύ σοβαρά ζητήματα ιδιαίτερα σ' ένα κόσμο που πρωταγωνιστούν πλέον τα μεγάλα δεδομένα. Η αναγκαιότητα για την προστασία της προσωπικής αυτονομίας που βασίζεται στο δικαίωμα του ατόμου να διατηρεί τον έλεγχο των προσωπικών του δεδομένων και της τυχόν επεξεργασία τους, καθιστά την εφαρμογή των εν λόγω οδηγιών, πιο επιτακτική από ποτέ.

Η αναγκαιότητα αλλά και η απαίτηση εφαρμογής τέτοιου είδους εγγυήσεων καταδεικνύει ξεκάθαρα την παγιωμένη στάση της Ευρώπης σχετικά με την προστασία των ανθρωπίνων δικαιωμάτων και εν προκειμένω την προστασία των προσωπικών δεδομένων. Ωστόσο η ολική ή μερική απουσία της εφαρμογής τέτοιου είδους εγγυήσεων, οφείλεται τόσο στην δυσκολία των αρχών να διασφαλίσουν την εφαρμογή της υφιστάμενης νομοθεσίας, όσο και στην έλλειψη πρόθεσης από τους ίδιους τους οργανισμούς να εφαρμόσουν το κανονιστικό πλαίσιο ή ακόμα και να προβούν σε αυτορρύθμιση, υποδεικνύει την αδυναμία

[77] Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data. Amending protocol to the Convention for the Protection of Individuals with Regard to the Processing of Personal Data, adopted by the Committee of Ministers at its 128th Session in Elsinore on 18 May 2018. https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

παροχής ενός ελάχιστου επιπέδου προστασίας κυρίως για αυτούς που το χρειάζονται περισσότερο.

Στην άλλη πλευρά του Ατλαντικού έχουμε να αντιμετωπίσουμε ένα διαφορετικό ζήτημα. Αν και υπάρχει μακρά παράδοση στο σεβασμό της ιδιωτικότητας του ατόμου η οποία προστατεύεται νομοθετικά, η προστασία των προσωπικών δεδομένων και ειδικότερα των βιομετρικών δεδομένων, ακόμη υστερεί κυρίως σε κανονιστικό πλαίσιο παρά τις προσπάθειες που έχουν καταβληθεί από οργανισμούς όπως από τον Οργανισμό Αμερικανικών Κρατών (Organization of American States)[78] και το Ιβηρο-Αμερικανικό Δίκτυο Προστασίας Δεδομένων (Ibero-American Data Protection Network) (RIDP)[79].

Οι σύγχρονες τεχνολογίες βιομετρικής αναγνώρισης αντιμετωπίζονται με σκεπτικισμό τόσο με θετικό όσο και με αρνητικό πρόσημο. Από τη μία πλευρά δεν είναι ιδιαίτερα ευχάριστο να γνωρίζεις ότι οι κυβερνητικές υπηρεσίες πληροφοριών είναι σε θέση να γνωρίζουν την ακριβή τοποθεσία του κάθε ατόμου αλλά και να εξακριβώνουν την ταυτότητα του μέσω καμερών ασφαλείας που χρησιμοποιούν βιομετρική τεχνολογία γεωμετρίας προσώπου.

Επίσης είναι απόλυτα φυσιολογικό να ενοχλούμαστε από το γεγονός ότι ο οποιοσδήποτε με τη χρήση ενός απλού smartphone μπορεί μέσω της λήψης φωτογραφιών να συλλέξει ευαίσθητα προσωπικά μας δεδομένα, βιομετρικά μας στοιχεία που οδηγούν στην

[78] Ο Οργανισμός Αμερικανικών Κρατών (Organization of American States) είναι ένας ηπειρωτικός οργανισμός που ιδρύθηκε στις 30 Απριλίου 1948 για τους σκοπούς της περιφερειακής αλληλεγγύης και της συνεργασίας μεταξύ των κρατών μελών της. Με έδρα την πρωτεύουσα των Ηνωμένων Πολιτειών Ουάσιγκτον, D.C., τα μέλη του ΟΑΣ είναι τα 35 ανεξάρτητα κράτη της Αμερικής. http://www.oas.org/en/

79 Το Ιβηρο-Αμερικανικό Δίκτυο Προστασίας Δεδομένων (Ibero-American Data Protection Network) (RIDP) αποτελείται από 22 αρχές προστασίας δεδομένων (DPA) από την Ισπανία, την Πορτογαλία, το Μεξικό και άλλες χώρες της Κεντρικής και Νότιας Αμερικής και της Καραϊβικής. Κατά την τελευταία δεκαετία, ο οργανισμός προώθησε την ανάπτυξη συνολικής νομοθεσίας για την προστασία των δεδομένων και την εισαγωγή αρχών προστασίας δεδομένων σε ολόκληρη τη Λατινική Αμερική. http://www.redipd.org/index-iden-idphp.php

αποκάλυψη της ταυτότητας μας. Μια τέτοια προοπτική όχι μόνο μας προκαλεί ανησυχίες άλλα αλλοιώνει την συλλογική αντίληψη αρκετών γενεών για την έννοια της ιδιωτικότητας.

Από την άλλη πλευρά είναι γεγονός ότι οι βιομετρικές τεχνολογίες έχουν εξελιχθεί με τέτοιο τρόπο ώστε να χρησιμοποιούνται σε καθημερινή βάση κι από το μεγαλύτερο μέρος του πληθυσμού. Το γεγονός ότι περισσότεροι άνθρωποι κυκλοφορούν με ένα smartphone το οποίο διαθέτει κάμερα υψηλής τεχνολογίας και τεχνητής νοημοσύνης αποδεικνύει αυτή την πραγματικότητα. Ο εντοπισμός ύποπτων συμπεριφορών μέσω της βίντεο-επιτήρησης, ο έλεγχος πρόσβασης σε κτίρια ή σε περιορισμένες περιοχές αλλά και η δημογραφική ανάλυση του πληθυσμού σε σχέση με το γένος και την ηλικία αποτελούν κάποιες από τις εφαρμογές της βιομετρικής τεχνολογίας αναγνώρισης που δεν ενοχοποιούνται ιδιαίτερα.

3. ΚΕΦΑΛΑΙΟ ΤΡΙΤΟ – Ηθική και Βιομετρία

3.1. Η τεχνολογία ως το νέο «μάντρα» της εποχής

Ζούμε σε μια εποχή όπου οι νόμοι και κανονισμοί δεν είναι σε θέση να ακολουθήσουν την αλματώδη ταχύτητα των τεχνολογικών και ψηφιακών μετασχηματισμών καθώς και των κοινωνικών επιπτώσεων που προκύπτουν από την εφαρμογή τους.

Έχει επικρατήσει παγκοσμίως μια τάση εξιδανίκευσης της τεχνολογίας και των λύσεων που αυτή προσφέρει, βελτιώνοντας πράγματι σε πολλές περιπτώσεις την ποιότητα ζωής όλων μας. Ωστόσο αυτή η ανάλυση της τεχνολογικής εξέλιξης θέτει στο απυρόβλητο την τεχνολογία και τις εφαρμογές της, παρουσιάζοντας μια μονόπλευρη θεώρηση, υπερτονίζοντας τα θετικά σημεία της τεχνολογικής προόδου, ενώ υποκρύπτει ή στην καλύτερη περίπτωση αγνοεί ηθελημένα τα αρνητικά της σημεία.

Η τεχνολογία έχει αναχθεί στο «μάντρα» της εποχής, δημιουργώντας την πεποίθηση ότι κάθε είδους πρόβλημα μπορεί να επιλυθεί με την εφαρμογή τεχνολογικών παρεμβάσεων. Ο Μορόζοφ (2013) υποστηρίζει ότι ζούμε σε ένα καθεστώς τεχνολογικής παντοκρατορίας το οποίο έχει προωθηθεί από τους ηγέτες της Σίλικον Βάλεϋ προβάλλοντας τις ψηφιακές παρεμβάσεις ως στην απόλυτη λύση στα πάντα, ονοματίζοντάς αυτή την τάση *solutionism*[80]. Η τεχνολογία λειτουργεί δηλαδή ως ένα τεκμήριο λύσης των προβλημάτων.

Η τεχνολογία και ιδιαίτερα η ψηφιακή μπορούν πράγματι να αποτελέσουν τη λύση σε πολλά προβλήματα όπως για παράδειγμα στη γραφειοκρατία και στην κρατική ανεπάρκεια εξυπηρέτησης των πολιτών. Ωστόσο η θεώρηση της τεχνολογίας ως πανάκεια, ενέχει

80 Morozov Evgeny, 2019, *Save Everything, Click Here. The Folly of Technological Solutionism*, public affairs books.

κινδύνους καθώς αγνοεί την τεχνολογική δεοντολογία. Το Μάρτιο του 2017 Ο υπουργός εργασίας και κοινωνικής πολιτικής της αυτόνομης κοινότητας των Βάσκων στην Ισπανία ανακοίνωσε την λήψη μέτρων για τη βελτίωση της λειτουργίας των υπηρεσιών. Ένα από αυτά τα μέτρα ήταν η εφαρμογή ηλεκτρονικού συστήματος ταυτοποίησης των χρηστών της ψηφιακής πλατφόρμας του υπουργείου. Οι χρήστες ωφελούμενοι των κοινωνικών προγραμμάτων θα έπρεπε να καταχωρήσουν τα βιομετρικά τους στοιχεία στην εφαρμογή προκειμένου να εγγραφούν στην υπηρεσία. Με αυτό τον τρόπο μόνο θα είχαν πρόσβαση στην οικονομική βοήθεια του ελάχιστου εγγυημένου εισοδήματος το οποίο παρέχει η Βασκική κυβέρνηση στους πολίτες που το μηνιαίο εισόδημα τους είναι κάτω από 650 ευρώ.

Με την χρήση των βιομετρικών στοιχείων θα μπορούσε να αποφευχθεί η απάτη και η πλαστοπροσωπία. Αυτό το παράδειγμα ανάμεσα σε πολλά άλλα παρουσιάζει τη χρήση των τεχνολογιών βιομετρικής αναγνώρισης ως μία ιδανική λύση για προβλήματα που αντιμετωπίζει η δημόσια διοίκηση. Ωστόσο αυτές οι προσεγγίσεις δεν θα πρέπει να υιοθετούνται άκριτα. Η χρήση τεχνολογιών βιομετρικής αναγνώρισης δεν αποτελεί πανάκεια.

3.2. Τεχνολογικός σκεπτικισμός & Βιοηθικοί προβληματισμοί

Υπάρχουν αρκετοί ηθικοί προβληματισμοί αναφορικά με τη χρήση των βιομετρικών στοιχείων του ατόμου καθώς αυτή ενέχει κινδύνους τόσο για την ιδιωτικότητα όσο και για τον κοινωνικό αποκλεισμό. Η έρευνα, μας έχει δείξει ότι θα υπάρχουν πάντα άτομα ή ομάδες ατόμων των οποίων τα βιομετρικά χαρακτηριστικά δεν μπορούν να ταυτοποιηθούν αξιόπιστα. Οι κωδικοί που χρησιμοποιούμε για την αυθεντικοποίηση μας κατά την διαδικασία εισόδου στους λογαριασμούς μας ηλεκτρονικού ταχυδρομείου ή στα κοινωνικά δίκτυα μπορούν να επιφέρουν δύο μόνο αποτελέσματα. Να ταιριάζουν ή να μην ταιριάζουν και αναλόγως το άτομο να συνδεθεί ή να μη μπορεί να συνδεθεί.

Αντιθέτως η ταυτοποίηση μέσω βιομετρικών στοιχείων δεν επιφέρει πάντα απόλυτο αποτέλεσμα. Υπάρχουν επίπεδα αξιοπιστίας του αποτελέσματος που σχετίζεται με το τρόπο συλλογής του δείγματος και την αλλοίωση των στοιχείων. Πάντοτε θα υπάρχουν παράγοντες που μπορούν να επιφέρουν αλλαγές μεταξύ του δείγματος που έχει συλλεχθεί και των πραγματικών βιομετρικών στοιχείων του ατόμου όπως για παράδειγμα η αλλαγή των χαρακτηριστικών του προσώπου λόγω ηλικίας ή εξαιτίας κάποιου τραυματισμού αλλά και τεχνολογικές αστοχίες που καταλήγουν σε μερική και όχι απόλυτη αναγνώριση. Αυτή είναι μια περίπτωση κοινωνικού αποκλεισμού, το γεγονός δηλαδή ότι κάποιο ποσοστό των ατόμων θα απορριφθούν ή δεν θα μπορούν να αναγνωριστούν από το βιομετρικό σύστημα.

Υπάρχει ωστόσο και ένα άλλο είδος κοινωνικού αποκλεισμού. Οι διακρίσεις και ο στιγματισμός. Η χρήση των βιομετρικών τεχνολογιών σε συγκεκριμένες εφαρμογές μπορεί να αποτελούν πλεονέκτημα όπως για παράδειγμα η πρόσβαση σε χώρους, ή η είσοδος σε προγράμματα υπολογιστών κλπ. Κυρίως όμως λειτουργεί συνειρμικά και εμπεριέχει την υπόνοια εγκλήματος. Η καταγραφή δακτυλικών αποτυπωμάτων αποτελεί τη διαδικασία την οποία χρησιμοποιεί η αστυνομία και οι δυνάμεις ασφαλείας σε πολλές χώρες προκειμένου να καταχωρήσουν τους εγκληματίες σε αρχεία και εάν δεν υπήρχε υποχρεωτικότητα για την παροχή αυτών το στοιχείων είναι σίγουρο ότι δεν θα καταχωρούσαν όλοι οι πολίτες εθελοντικά τα δακτυλικά τους αποτυπώματα, λόγω του συσχετισμού αυτής της διαδικασίας με το έγκλημα.

Υπάρχουν ακόμη συνειδησιακοί ή θρησκευτικοί λόγοι που ενδέχεται να αποκλείσουν συγκεκριμένες κοινωνικές ομάδες από τη χρήση αυτών των τεχνολογιών. Για παράδειγμα τα μέλη αρκετών θρησκευτικών οργανώσεων στις Ηνωμένες Πολιτείες αρνούνται να εγγραφούν σε βιομετρικά προγράμματα καθώς θεωρούν ότι αυτά φέρνουν «το σημάδι του θηρίου» (Αποκάλυψη 13: 16-18).

Στον ψηφιακό κόσμο η κυβερνοασφάλεια είναι ένα ζητούμενο κομβικής σημασίας. Οι συχνές ειδήσεις για τις διαρροές δεδομένων από τεχνολογικές εταιρίες προβληματίζουν και δημιουργούν αισθήματα ανασφάλειας. Οι υπεύθυνοι επεξεργασίας των βιομετρικών δεδομένων θα πρέπει να διαβεβαιώνουν ότι η τεχνολογία είναι ασφαλής κι αυτό δεν είναι πάντοτε δυνατό. Η πρακτική αδυναμία εξασφάλισης 100% προστασίας έχει σοβαρές οικονομικές, κοινωνικές, ηθικές και νομικές συνέπειες. Δεν είναι δυνατό να παραχωρούμε βιομετρικά δεδομένα σε αρχές που δεν λαμβάνουν υπόψη τα ατομικά δικαιώματα. Πρέπει να απαιτείται απόλυτη διαφάνεια και υπευθυνότητα όσον αφορά στη χρήση βιομετρικής τεχνολογίας από τους οργανισμούς.

Το Βιομετρικό Ινστιτούτο[81] έχει δημοσιεύσει τις επτά ηθικές αρχές πάνω στις οποίες θα πρέπει να εφαρμόζονται οι βιομετρικές τεχνολογίες σε τομείς όπως η ασφάλεια η εργασία και η λήψη αυτοματοποιημένων αποφάσεων. Αυτός ο κατάλογος των αρχών δίνει ιδιαίτερη έμφαση στην ηθική συμπεριφορά και περιλαμβάνει όλες τις πτυχές που σχετίζονται με την κατοχή βιομετρικών στοιχείων ως εργαλείο που θα πρέπει να υπηρετεί τον άνθρωπο με δικαιοσύνη και υπευθυνότητα διασφαλίζοντας την ιδιωτικότητα και την αξιοπρέπεια του ατόμου. Η έκδοση των συγκεκριμένων αρχών για τα βιομετρικά δεδομένα πραγματοποιήθηκε κατόπιν απαίτησης τεχνολογικών εταιρειών οι οποίες άσκησαν πιέσεις στις κυβερνήσεις για την εφαρμογή ενός ρυθμιστικού πλαισίου όσον αφορά στη διακίνηση βιομετρικών δεδομένων που χρησιμοποιούν εφαρμογές τεχνητής νοημοσύνης με ιδιαίτερη έμφαση στις εφαρμογές αναγνώρισης προσώπου (Olimid & Rogozea, 2018: 63)

81 Το Ινστιτούτο Βιομετρίας ιδρύθηκε το 2001 και αντιπροσωπεύει μια κοινότητα με πολλούς φορείς που διαδίδεται σε όλο τον κόσμο. Η αποστολή του Ινστιτούτου είναι να προωθήσει την υπεύθυνη και ηθική χρήση της βιομετρικής ανάλυσης ως ανεξάρτητο και αμερόληπτο διεθνές φόρουμ για τους βιομετρικούς χρήστες και άλλα ενδιαφερόμενα μέρη. Για την επίτευξη αυτής της αποστολής, οι στόχοι του Ινστιτούτου Βιομετρίας είναι:
Να αναπτύξει ηγετική σκέψη και καθοδήγηση για την υπεύθυνη χρήση της βιομετρίας, χρησιμοποιώντας τη συμβολή των εμπειρογνωμόνων,
Να διευκολύνει τη μεταφορά γνώσης στα μέλη, στους βασικούς ενδιαφερόμενους και στο κοινό
Να ενεργεί ως σύνδεσμος για την παγκόσμια βιομετρική βιομηχανία, συμπεριλαμβανομένων των χρηστών, των προμηθευτών, των ακαδημαϊκών, των ρυθμιστικών αρχών και των υπερασπιστών της ιδιωτικότητας. https://www.biometricsinstitute.org/about/

Η βιομετρική τεχνολογία έχει πάρει ανεξέλεγκτες διαστάσεις τα τελευταία χρόνια και αυτό καθιστά ιδιαίτερα δύσκολη την πρόβλεψη των εμπορικών εφαρμογών ή των εφαρμογών επιτήρησης που επηρεάζουν την καθημερινότητά μας.

3.3. Κίνδυνοι που σχετίζονται με τη χρήση βιομετρικών δεδομένων

Η κατοχή, η χρήση και επεξεργασία βιομετρικών στοιχείων από οργανισμούς που διατηρούν μεγάλες βάσεις δεδομένων, εγείρει αρκετές ανησυχίες καθώς τα δεδομένα δεν βρίσκονται πλέον υπό τον έλεγχο του υποκειμένου (Kindt, 2007: 167)

Οι τεχνολογίες βιομετρικής αναγνώρισης αυξάνουν επίσης τους κινδύνους λανθασμένης ταυτοποίησης σε σύγκριση με τους κινδύνους που αντιμετωπίζουν παραδοσιακά συστήματα ταυτοποίησης όπως η χρήση προσωπικής κάρτας. Από τη στιγμή που τα βιομετρικά δεδομένα είναι μοναδικά και αναντικατάστατα η πιθανότητα απώλειας ή κλοπής αυτών σημαίνει ότι εξαφανίζεται και η νομική ταυτότητα του ατόμου που σχετίζεται με αυτά και η οποία δεν μπορεί να επανακτηθεί εάν δεν προσκομιστούν νέα βιομετρικά δεδομένα. Εάν δεν υπάρχει λοιπόν το κατάλληλο νομικό πλαίσιο το άτομο κινδυνεύει να χάσει τη δυνατότητα ταυτοποίησης του χωρίς να είναι σε θέση να διεκδικήσει αποζημίωση (Friedland, &Tschantz, 2019: 659-704).

Επιπρόσθετα υπάρχουν έρευνες που αποδεικνύουν ότι σχεδόν όλα τα βιωματικά δεδομένα περιέχουν ένα σημαντικό αριθμό επιπρόσθετων πληροφοριών η οποίες δεν είναι απαραίτητες για το σκοπό τον οποίο συλλέχθηκαν και οι οποίες σχετίζονται με την υγεία του υποκείμενου. Αν και θεωρητικά αυτές οι πληροφορίες θα έπρεπε να καταστραφούν με την ολοκλήρωση της δημιουργίας της εφαρμογής η απουσία ενός ξεκάθαρου κανονιστικού πλαισίου αναφορικά με τη διαδικασία επεξεργασίας αυτών των δεδομένων μπορεί να οδηγήσει στον πολλαπλασιασμό της ποσότητας των βιομετρικών δεδομένων που διατηρούνται σε μια βάση (Kindt, 2007: 168).

3.4. Ατομικά Δικαιώματα ή Ασφάλεια

Η μέχρι σήμερα χρήση των βιομετρικών τεχνολογιών σε πολλά κράτη σχετίζεται με την έννοια της ταυτότητας. Ωστόσο αντί αυτό να αποτελεί ένα παγιωμένο δικαίωμα του ατόμου έναντι του κράτους (το δικαίωμα να αναγνωρίζεσαι ως ένα υποκείμενο δικαιωμάτων σε ένα κοινωνικό σύστημα) φαίνεται να αποτελεί ένα δικαίωμα του κράτους έναντι του ατόμου, να λειτουργεί δηλαδή αντίστροφα (η δύναμη της κατοχής της χρήσης των στοιχείων που αποτελούν την ταυτότητα του υποκειμένου, προκειμένου να χρησιμοποιηθούν για διάφορους πολιτικούς σκοπούς). Πρόκειται για ένα παιχνίδι εξουσίας πού υποβιβάζει τα ατομικά δικαιώματα έναντι της εξουσίας που φέρει το κράτος (Rahman, Verhaert, &Nyst, 2018: 8).

Η τάση που επικρατεί παγκοσμίως και που θεμελιώθηκε κυρίως μετά την 11^{η} Σεπτεμβρίου σχετίζεται με τη ρητορική της ενίσχυσης της ασφάλειας. Ο στόχος αυτός χρησιμοποιείται ως το επιχείρημα που θα δικαιολογήσει την αυξανόμενη εισχώρηση στην ιδιωτική ζωή των ατόμων εντελώς προσχηματικά. Ωστόσο όπως είναι γνωστό τα ατομικά δικαιώματα σχετίζονται εξ ορισμού με την προσωπικότητα του ατόμου και οποιαδήποτε προσπάθεια διαπραγμάτευσης για την έκπτωση αυτών, θα ήταν ιδιαίτερα επιβλαβής για την ίδια την αξιοπρέπεια του ατόμου.

Δίχως αμφιβολία η εφαρμογή αυτών των τεχνολογιών προκειμένου να είναι σύμφωνη με το σεβασμό των ατομικών δικαιωμάτων θα πρέπει πρώτα απ' όλα να διασφαλίζει ένα υψηλό επίπεδο διαφάνειας. Η θέσπιση κανόνων που θα διασφαλίζουν αυτή τη διαφάνεια είναι επιτακτική καθώς η μοναδικότητα που έχουν από τη φύση τους τα βιομετρικά δεδομένα τα καθιστά ιδιαίτερα ευάλωτα σε ενδεχόμενη κακή χρήση η οποία θα επέφερε μη αναστρέψιμα αποτελέσματα για την διασφάλιση των ατομικών δικαιωμάτων (Pugliese, 2010:17)[82].

[82] Pugliese J., 2010, Biometrics : Bodies Technologies, Biopolitics, Routledge

3.5. Case Study - Μέξικο Σίτυ

Μεταξύ του 2009 και το 2011 το Μέξικο Σίτυ χρησιμοποίησε ένα συνδυασμό αναγνώρισης προσώπου και ανάλυσης βιομετρικών στοιχείων, προκειμένου να σκανάρει τα πρόσωπα 22 εκατομμυρίων ανθρώπων μέσω 15.000 καμερών. Η χρήση αυτής της βιομετρικής εφαρμογής σε συνδυασμό με την υψηλή τεχνολογία των καμερών οι οποίες διέθεταν αισθητήρες ήχου ώστε να κινούνται προς την πλευρά του ήχου των πυροβολισμών, συνετέλεσαν στην μείωση της εγκληματικότητας κατά 33% και κατά 50% στην κλοπή αυτοκινήτων. Ο χρόνος ανταπόκρισης της αστυνομίας είναι πολύ μικρότερος σε σχέση με το μέσο χρόνο ανταπόκρισης των προηγούμενων ετών και ο δήμος του Μέξικο Σίτυ δίνει εύσημα στις βιομετρικές τεχνολογίες οι οποία συνετέλεσαν κομβικό ρόλο στην εφαρμογή ενός από τα πλέον φιλόδοξα προγράμματα αστικής ασφαλείας στον κόσμο[83].

3.6. Εξισορρόπηση της ασφάλειας με την ιδιωτικότητα και την προστασία των δεδομένων

Η απουσία κοινών διεθνών κριτηρίων σχετικά με την προστασία των προσωπικών δεδομένων καταδεικνύει τις διαφορετικές προσεγγίσεις των κυβερνήσεων παγκοσμίως στο μείζον θέμα των ανθρωπίνων δικαιωμάτων. Η έλλειψη αυτής της κοινής προσέγγισης μεταξύ των εθνών υπονομεύει την πραγματοποίηση συγκεκριμένων σημαντικών στόχων όπως είναι η οικονομική και η κοινωνική ανάπτυξη, η εξάλειψη των περιορισμών στην ελεύθερη κίνηση δεδομένων και η υλοποίηση πολιτικών προστασίας της ιδιωτικότητας του ατόμου (Toch et al., 2018: 36).

[83] Perala A., 2019, *Smart Lighting, Biometric Surveillance Specialists Team Up to Deliver Security Solution in Mexico City*, findbiometrics.com

Επιπρόσθετα δεν πρέπει να λησμονούμε ότι η προστασία του ατόμου σχετικά με την επεξεργασία των προσωπικών δεδομένων αποτελεί ένα αναγκαίο εργαλείο το οποίο εγγυάται την προστασία του έναντι άλλων ανθρωπίνων δικαιωμάτων και θεμελιωδών ελευθεριών καθώς σε τελική ανάλυση σχετίζεται με την ίδια την αξιοπρέπεια του ατόμου. Σχετίζεται επίσης με δικαιώματα όπως ισότητα και η απαγόρευση διακρίσεων καθώς η αποκάλυψη ευαίσθητων πληροφοριών μπορεί να οδηγήσει στην απομόνωση του ατόμου ή ακόμα και με την εκδήλωση ρατσιστικών συμπεριφορών εις βάρος του.

Ένα επιπλέον θέμα το οποίο ενισχύει την ανάγκη για τη δημιουργία ομογενοποιημένων πολιτικών σε παγκόσμιο επίπεδο είναι η επίπτωση που θα είχε στην ενίσχυση της εμπιστοσύνης των χρηστών και των καταναλωτών απέναντι στις τεχνολογίες βιομετρικής αναγνώρισης. Η αποτελεσματική, νομοθετικά θεσπισμένη, προστασία της ιδιωτικότητας, η λειτουργία ανεξάρτητων διοικητικών αρχών, διαδικασιών και κανόνων εξυγίανσης αποτελούν τη βάση για την δημιουργία αυτής της εμπιστοσύνης η οποία είναι απαραίτητη σε όλες τις περιπτώσεις, είτε στις σχέσεις πολιτών και δημόσιας διοίκησης είτε στις σχέσεις μεταξύ καταναλωτών και παρόχων υπηρεσιών.

3.7. Η εφαρμογή της αρχής της αναλογικότητας

Ωστόσο, η ανησυχία σχετικά με τη χρήση των βιομετρικών βάσεων δεδομένων είναι εύλογη και δικαιολογημένη. Η πρόκληση που καλούνται να αντιμετωπίσουν οι αρχές έγκειται στη διασφάλιση της εξισορρόπησης μεταξύ των δικαιωμάτων του υποκειμένου και του ευρύτερου δημοσίου συμφέροντος ή του νόμιμου εμπορικού συμφέροντος.

Η πληροφορία αποτελεί ένα πολύτιμο πόρο στις σημερινές κοινωνίες καθώς η επεξεργασία αυτών καθορίζει την λήψη αποφάσεων σε πολλούς κοινωνικούς τομείς. Η επεξεργασία και η εξόρυξη μεγάλων ποσοτήτων πληροφοριών μπορούν να επιφέρουν

πολλαπλά οφέλη για την κοινωνία με την προϋπόθεση ότι σέβονται δικαιώματα των ανθρώπων την ιδιωτικότητα τους και εξασφαλίζουν την προστασία των προσωπικών τους δεδομένων. Σε αυτό το πλαίσιο η λήψη συγκεκριμένων τεχνικών μέτρων όπως είναι η ανωνυμοποίηση των πληροφοριών, μπορεί να εγγυηθεί τα πλεονεκτήματα που προσφέρει η κοινωνία της πληροφορίας χωρίς να γίνει κανένα είδους έκπτωση στον τομέα της προστασίας των δεδομένων (Deliversky, & Deliverska, 2018: 25). Προκειμένου να επιτευχθεί αυτός ο στόχος είναι απαραίτητη η εξασφάλιση της μη αναστρεψιμότητας της ανωνυμοποίησης τον δεδομένων.

Επιπλέον, τα βιομετρικά δεδομένα πρέπει να είναι επαρκή, και όχι υπερβολικά σε σχέση με τους σκοπούς για τους οποίους συλλέγονται. Ο σεβασμός αυτής της αρχής συνεπάγεται, σαφή καθορισμό του σκοπού για τον οποίο τα βιομετρικά δεδομένα συλλέγονται και υποβάλλονται σε επεξεργασία. Η αξιολόγηση των μέτρων με βάση την αναλογικότητα τους πραγματοποιείται με το απλό ερώτημα: Μπορεί ο επιδιωκόμενος σκοπός να επιτευχθεί με λιγότερο παρεμβατικό τρόπο. Η αναλογικότητα αποτέλεσε το κύριο κριτήριο σε όλες σχεδόν τις αποφάσεις που ελήφθησαν μέχρι σήμερα από τις αρχές προστασίας δεδομένων σε πανευρωπαϊκό επίπεδο.

Η Γαλλική αρχή προστασίας δεδομένων δεν επέτρεψε τη χρήση δακτυλικών αποτυπωμάτων για την πρόσβαση παιδιών σε σχολικό εστιατόριο αλλά δέχτηκε για τον ίδιο σκοπό την χρήση του μοτίβου της παλάμης του χεριού[84].

Η Γερμανική αρχή προστασίας δεδομένων επέτρεψε την εισαγωγή βιομετρικών στοιχείων στις ταυτότητες προκειμένου να αποτρέψει την δημιουργία πλαστών υπό την προϋπόθεση ότι τα δεδομένα αποθηκεύονται στο μικροτσίπ της κάρτας και όχι σε βάσεις

[84] Working document on biometrics , 2003,THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA set up by Directive 95/46/EC of the European Parliament and of the Council, http://www.europa.eu.int/comm/privacy

δεδομένων στις οποίες μπορεί να γίνει σύγκριση μεταβατικά από τυπώματα του υποκειμένου[85].

Στο Ηνωμένο Βασίλειο το νομοσχέδιο για την εισαγωγή των βιομετρικών ταυτοτήτων αποτέλεσε αντικείμενο αντιπαράθεσης για μεγάλο χρονικό διάστημα, έφτασε μέχρι το πρώτο πιλοτικό πεδίο εφαρμογής και εγκαταλείφθηκε οριστικά το 2010[86].

Η Ινδία έχει εισαγάγει ένα σύστημα εικονικής βιομετρικής ταυτότητας με πάνω από 1 δισεκατομμύριο ανθρώπους εγγεγραμμένους. Ωστόσο αμφισβητείται η συνταγματικότητα του μέτρου καθώς έρχεται σε σύγκρουση με το δικαίωμα της ιδιωτικότητας και η υπόθεση εξετάζεται από τα δικαστήρια της χώρας[87].

3.8. Επίμετρο

Αυτή η εργασία ξεκίνησε αναγνωρίζοντας τις κοινωνικές ανησυχίες που εγείρονται από την πιθανότητα κακής χρήσης των βιομετρικών δεδομένων που συλλέγονται και χρησιμοποιούνται.

Οι ανησυχίες αυτές έθεσαν τη βάση λήψης κανονιστικών μέτρων για τον έλεγχο της επεξεργασίας βιομετρικών δεδομένων και την ενίσχυση του ατομικού δικαιώματος της ιδιωτικότητας και της προστασίας των προσωπικών δεδομένων.

Αρχικά κατέστη σαφές τί εννοούμε με την έννοια βιομετρικά δεδομένα αλλά και πώς αυτά θα πρέπει να αντιμετωπιστούν από νομικής πλευράς. Η αποτελεσματική θεσμική προστασία των βιομετρικών δεδομένων θα πρέπει να διασφαλίζει την ακρίβεια για την ασφάλεια των δεδομένων που αποθηκεύονται με σκοπό να χρησιμοποιηθούν για την

[85] Ο.π.
[86] Βλ. Vallance Patrick, 2018, *Biometrics: a guide*, UK government office of science.
[87] www.thehindu.com

ταυτοποίηση του ατόμου, να δικαιολογεί επαρκώς την επιλογή εφαρμογής αυτού του μέτρου σε σχέση με κάποιο ηπιότερο, εφαρμόζοντας την αρχή της αναλογικότητας. Τα θέματα ιδιωτικότητας που σχετίζονται με τα βιομετρικά δεδομένα αφορούν κυρίως στις κατηγορίες δημόσιου ελέγχου πρόσβασης σε κτίρια, online τραπεζικές συναλλαγές και άλλες παρόμοιες δραστηριότητες.

Οι νομοθετικές πρωτοβουλίες για την προστασία των βιομετρικών δεδομένων βρίσκονται σε εξέλιξη παγκοσμίως με την Ευρώπη να πρωτοπορεί στον τομέα αυτό προβλέποντας στο γενικό κανονισμό για την προστασία δεδομένων αυστηρές προϋποθέσεις για τη συλλογή και επεξεργασία βιομετρικών δεδομένων. Η ευρωπαϊκή νομοθεσία αναμφισβήτητα αυξάνει σημαντικά την προστασία της ιδιωτικότητας του ατόμου. Οι βιομετρικές τεχνολογίες αναγνώρισης εάν είναι σωστά σχεδιασμένες, λαμβάνοντας υπόψη την ισχύουσα νομοθεσία μπορούν θεωρητικά να επιλύσουν αρκετά προβλήματα δημόσιας πολιτικής, εμπορικής δραστηριότητας αλλά και να διευκολύνουν το άτομο σε καθημερινές προσωπικές ενασχολήσεις.

Ωστόσο, ευλόγως μας είναι αρκετά δύσκολο να υπερεκτιμήσουμε την σημασία των βιομετρικών τεχνολογιών στην κοινωνική λειτουργία. Η έμφυτη και αρχέτυπη αναγκαιότητα για την ανάπτυξη της προσωπικότητάς και της ατομικής ταυτότητας είναι ιδιαίτερα ισχυρή, κομβικής σημασίας για τον αυτοπροσδιορισμό του ατόμου και σχετίζεται άμεσα με τη διαφορετικότητα. Η άκριτη και αλόγιστη υιοθέτηση βιομετρικών τεχνολογιών ενέχει τον κίνδυνο της ολοκληρωτικής παράδοσης της εξουσίας που έχουμε πάνω στο σώμα μας, σε τρίτες οντότητες, με αμφιλεγόμενο σκοπό δράσης.

Το Μάρτιο του 2004 ο γνωστός Ιταλός φιλόσοφος Giorgio Agamben προσκλήθηκε από το πανεπιστήμιο της Νέας Υόρκης προκειμένου να παραδώσει μια σειρά διαλέξεων, ωστόσο ο ίδιος αρνήθηκε να παραστεί καθώς αντιτίθεται στη παραχώρηση βιομετρικών

στοιχειών όπως τα δακτυλικά του αποτυπώματα, το οποίο αποτελεί αναγκαία προϋπόθεση για τον έλεγχο της εισόδου των ταξιδιωτών στις Ηνωμένες Πολιτείες. Μετά την άρνηση τις πρόσκλησης έγραψε ένα σύντομο σημείωμα εξηγώντας τους λόγους της απόφασης του. «Δεν υφίσταται πλέον όριο στις τεχνολογίες ελέγχου του σώματος μας και η παραβίαση αυτή σηματοδοτεί μια νέα παγκόσμια κατάσταση… Η ηλεκτρονική καταχώρηση των βιομετρικών μας δεδομένων θα πρέπει να αποτελεί αυτό το όριο.…Αυτό που βιώνουμε σήμερα δε σχετίζεται πλέον με την ελεύθερη και ενεργή συμμετοχή μας στο πολιτικό γίγνεσθαι αλλά αποτελεί την υφαρπαγή και την καταγραφή των πιο ιδιωτικών και απροστάτευτων στοιχείων μας που σχετίζονται με την ίδια την βιολογική μας ζωή»[88.]

Η κοινωνική ιστορία μας έχει διδάξει ότι τέτοιου είδους μέθοδοι καταναγκαστικού χαρακτήρα, χρησιμοποιήθηκαν στο πλαίσιο της αποικιοκρατίας, ή οδήγησαν στον κοινωνικό στιγματισμό, στο ρατσισμό, στο σεξισμό, στην ομοφοβία. Με παράδοξο τρόπο ο πολίτης μετατρέπεται σε έναν εν δυνάμει ύποπτο καθώς γίνεται αντικείμενο τεχνολογικών εφαρμογών και πρακτικών που μέχρι σήμερα χρησιμοποιούνταν μόνο για τα πιο επικίνδυνα άτομα. Η καθολικότητα στη χρήση των βιομετρικών τεχνολογιών αναγνώρισης οδηγεί αναπόφευκτα στο εξής παράδοξο: Το ανθρώπινο είδος ανακηρύσσεται και επίσημα το πλέον επικίνδυνο από όλα τα είδη.

Words count: 19.960

[88] Βλ. Agamben G., 2004, *Bodies without Words*, German Law Journal 5

Βιβλιογραφία

- Agamben G., (2004), Bodies without Words, German Law Journal 5
- Agamben G., (2007), Κατάσταση εξαίρεσης, Πατάκης, σ. 15 επ
- Agamben G., (1998), Heller-Roazen, trans. Homo Sacer: Sovereign Power and Bare Life Stanford, California: Stanford University Press, 1 April. 72.
- Ajana, B., (2013). Asylum, identity management and biometric control. Journal of Refugee Studies, 26(4), 576-595.
- Alterman, A. (2003). ``A piece of yourself'': Ethical issues in biometric identification. Ethics and information technology, 5(3), 139-150.
- Arslanian, H., & Fischer, F. (2019). Blockchain As an Enabling Technology. In The Future of Finance (pp. 113-121). Palgrave Macmillan, Cham.
- Beaudet, J., Rieul, F., Fourre, J. Y., &Chastel, P. (2019). U.S. Patent Application No. 16/057,657.
- Berry, J., & Stoney, D. A. (2001). The history and development of fingerprinting. Advances in fingerprint Technology, 2, 13-52.
- Bourcha, C., Deftou, M. L., &Koskina, A. (2017). Data mining of biometric data: revisting the concept of private life?. Ius et Scientia, 3 (2), 37-62.
- Bousdekis, A., Papageorgiou, N., Magoutas, B., Apostolou, D., &Mentzas, G. (2018). Enabling condition-based maintenance decisions with proactive event-driven computing. Computers in Industry, 100, 173-183.
- Briney, K. (2019). Data Management Practices in Academic Library Learning Analytics: A Critical Review. Journal of Librarianship and Scholarly Communication, 7(1), 1.
- Cabrera, C., Hernández, G., Niño, L. F., & Dasgupta, D. (2018, October). Thermal Vein Signatures, DNA and EEG Brainprint in Biometric User Authentication. In Workshop on Engineering Applications (pp. 30-41). Springer, Cham.
- Chaudhuri, A., &Cavoukian, A. (2018). The Proactive and Preventive Privacy (3P) Framework for IoT Privacy by Design. EDPACS, 57(1), 1-16.
- Conger Kate, 2019, Tech-Savvy City Bans a Crime-Fighting Tool: Facial Recognition, New York Times, May 15, Page 1,
- Crutzen, R., Ygram Peters, G. J., & Mondschein, C. (2019). Why and how we should care about the General Data Protection Regulation. Psychology & health, 1-11.

- Da Costa-Abreu, M., & Smith, S. (2017). Using biometric-based identification systems in Brazil: A review on low cost fingerprint techniques on-the-go. Computer law & security review, 33(5), 629-634.
- De Witte, J. I., & Ten Have, H. (1997). Ownership of genetic material and information. Social Science & Medicine, 45(1), 51-60.
- Deliversky, J., &Deliverska, M. (2018). Ethical and Legal Considerations in Biometric Data Usage—Bulgarian Perspective. Frontiers in public health, 6, 25.
- Dellwo, V., French, P., He, L., Frühholz, S., & Belin, P. (2018). Voice Biometrics for Forensic Speaker Recognition Applications. 777-798.
- Derrida J. / J. Habermas, (2003), Le "concept" du 11 Septembre. Dialogues a NewYork avec G. Borradori, Galile, σ. 57 επ, 87 επ.
- Douglas, M., Bailey, K., Leeney, M., & Curran, K. (2018). An overview of steganography techniques applied to the protection of biometric data. Multimedia Tools and Applications, 77(13), 17333-17373.
- Foessel, M., &Garapon, A. (2006). Biometrics: the new forms of identity. Spirit , (8), 165-172.
- Ford, K., & Campbell, S. (2018). Being Participatory Through Photo-Based Images. In Being Participatory: Researching with Children and Young People (pp. 127-146). Springer, Cham.
- Fraga, A., & De Souza, M. C. M. (2018). Chapter Six Corporate Governance In A Brazilian State-Owned Bank Marcelo Amaral, Arlindo Freitas. Governing Turbulence, Risk and Opportunities in the Complexity Age, 110.
- Friedland, G., &Tschantz, M. C. (2019, July). Privacy concerns of multimodal sensor systems. In The Handbook of Multimodal-Multisensor Interfaces (pp. 659-704). Association for Computing Machinery and Morgan & Claypool.
- Herring, J., & Chau, P. L. (2007). My body, your body, our bodies. Medical Law Review, 15(1), 34-61.
- Hurst, A. C. (2018). Facial recognition software in clinical dysmorphology. Current opinion in pediatrics, 30(6), 701-706.
- Karanasiou, A. P., &Douilhet, E. (2016, April). Never mind the data: The legal quest over control of information & the networked self. In 2016 IEEE International Conference on Cloud Engineering Workshop (IC2EW) (pp. 100-105). IEEE.

- Kindt, E. (2007). Biometric applications and the data protection legislation. Datenschutz und Datensicherheit-DuD, 31(3), 166-170.
- Mantelero Alessandro, (2019), Report on Artificial IntelligenceArtificial Intelligence and Data Protection: Challenges and Possible Remedies, Council of Europe, Strasbourg, 25 January 2019
- Miselem, N. C. (2014). History and Analysis of French Contributions to Space Exploration.
- Mordini, E., &Massari, S. (2008). Body, biometrics and identity. Bioethics, 22(9), 488-498.
- Morozov Evgeny, (2019), Save Everything, Click Here. The Folly of Technological Solutionism, public affairs books.
- Mouammine, A., & Collier, J. (2018). The impact of DNA methylation in Alphaproteobacteria. Molecular microbiology, 110(1), 1-10.
- Nagasundaram, S., &Aissi, S. (2019). U.S. Patent Application No. 16/232,767.
- North-Samardzic, A. (2019). Biometric Technology and Ethics: Beyond Security Applications. Journal of Business Ethics, 1-18.
- Nowak, A., &Latané, B. (2018). Simulating the emergence of social order from individual behaviour. In Simulating societies(pp. 63-84). Routledge.
- Olimid, A. P., Rogozea, L. M., &Olimid, D. A. (2018). Ethical approach to the genetic, biometric and health data protection and processing in the new EU General Data Protection Regulation (2018). Romanian journal of morphology and embryology= Revue roumaine de morphologie et embryologie, 59(2), 631-636.
- Oussous, A., Benjelloun, F. Z., Lahcen, A. A., &Belfkih, S. (2018). Big Data technologies: A survey. Journal of King Saud University-Computer and Information Sciences, 30(4), 431-448.
- Ozuem, W., Howell, K. E., & Lancaster, G. (2018). Developing technologically induced environments: the case of the Nigerian banking sector. Journal of Financial Services Marketing, 23(1), 50-61.
- Patel, Y. (2019). The state of play–traditional versus behavioural biometrics. Biometric Technology Today, 2019(2), 5-7.
- Perala A., (2019), Smart Lighting, Biometric Surveillance Specialists Team Up to Deliver Security Solution in Mexico City, findbiometrics.com
- Pugliese J., (2010), Biometrics : Bodies Technologies, Biopolitics, Routledge

- Quirin, M., Tops, M., & Kuhl, J. (2019). Autonomous Motivation, Internalization. The Oxford Handbook of Human Motivation, 393.
- Rahman, Z., Verhaert, P., &Nyst, C. (2018). Biometrics in the Humanitarian Sector. 1-22.
- Rao, R. (2000). Property, privacy, and the human body. BUL rev., 80, 359.
- Romanou, A. (2018). The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise. Computer law & security review, 34(1), 99-110.
- Rouse, Margaret, (2019), "internet of things (IoT)". IOT Agenda.
- Russell Brandom, (2014), "Why Facebook is beating the FBI at facial recognition", The Verge
- Russell, S. (2018). EU General Data Protection Regulation (GDPR).
- Sanz Salguero, FJ (2016). Relationship between the protection of personal data and the right of access to public information within the framework of comparative law. Ius et Praxis , 22 (1), 323-376.
- Schwartz, A. L., &Petrovic, V. (2019). U.S. Patent Application No. 16/169,818.
- Schwartz, P. M. (2003). Property, privacy, and personal data. Harv. L. Rev., 117, 2056.
- Shabani, M., &Borry, P. (2018). Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation. European Journal of Human Genetics, 26(2), 149.
- Shrobe, H., Shrier, D. L., & Pentland, A. (2018). Behavioral Biometrics. 365-377.
- Sikdar, S. (2019). Environmental protection: reactive and proactive approaches. 1-2.
- Smith, M., Mann, M., &Urbas, G. (2018). Biometrics, crime and security. Routledge. 5-35
- Steiner, M. S. (2018). U.S. Patent No. 9,996,735. Washington, DC: U.S. Patent and Trademark Office.
- Sutrop, M. (2010, January). Ethical issues in governing biometric technologies. In International Conference on Ethics and Policy of Biometrics (pp. 102-114). Springer, Berlin, Heidelberg.
- Thieme, M., Nanavati, S., Nanavati, R., &Mak, M. (2018). U.S. Patent Application No. 15/848,904.

- Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review, 34(1), 134-153.
- Toch, E., Bettini, C., Shmueli, E., Radaelli, L., Lanzi, A., Riboni, D., &Lepri, B. (2018). The privacy implications of cyber security systems: A technological survey. ACM Computing Surveys (CSUR), 51(2), 36.
- Toombs, S. K. (1999). What does it mean to be somebody? Phenomenological reflections and ethical quandaries. In Persons and their bodies: Rights, responsibilities, relationships (pp. 73-94). Springer, Dordrecht.
- Vagle, M. D. (2018). Crafting phenomenological research. Routledge.
- Valkanov, N. (2019). Smart Compliance or How New Technologies Change Customer Identification Mechanisms in Banking. Economics and computer science, (2), 12-19.
- Vallance Patrick, (2018), Biometrics : a guide, UK government office of science.
- Van der Ploeg, S. H. W., Izmalkov, A., van den Brink, A. M., Hübner, U., Grajcar, M., Il'Ichev, E., ... &Zagoskin, A. M. (2007). Controllable coupling of superconducting flux qubits. Physical review letters, 98(5), 057004.
- Wickins, J. (2007). The ethics of biometrics: the risk of social exclusion from the widespread use of electronic identification. Science and Engineering Ethics, 13(1), 45-54.
- Wilkin Jacob, (2018), Mapping Social Media with Facial Recognition: A New Tool for Penetration Testers and Red Teamers, https://www.trustwave.com
- Wortham, R. H., Gaudl, S. E., & Bryson, J. J. (2019). Instinct: A biologically inspired reactive planner for intelligent embedded systems. Cognitive Systems Research, 57, 207-215.
- Zhang, D. (2018, October). Big data security and privacy protection. In 8th International Conference on Management and Computer Science (ICMCS 2018). Atlantis Press. 113
- Zhang, D., Lu, G., & Zhang, L. (2018). Advanced biometrics. Springer International Publishing. 10.
- Zuo, K. J., Saun, T. J., & Forrest, C. R. (2019). Facial Recognition Technology: A Primer for Plastic Surgeons. Plastic and reconstructive surgery, 143(6), 1298e-1306e.

- Zureik, E., &Hindle, K. (2004). Governance, security and technology: The case of biometrics. Studies in PoliticalEconomy, 73(1), 113-137.

- Καρκατζούνης Βασίλης, (2019), Οι νέες διατάξεις για την προστασία προσωπικών δεδομένων των εργαζομένων (Νόμος 4624/2019), syntagmawatch.gr
- Λουκάς Νικόλαος Η., (2017), Τεχνικά μέτρα του Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR),
- Νάιδου Πετρινή , (2019), GDPR: Η Επόμενη Μέρα. Βιομετρικά δεδομένα και εργασία, Εφημερίδα ΜΑΚΕΔΟΝΙΑ, 24 Φεβρουαρίου 2019.
- Παρασκευόπουλος Ν., (2004), Ασφάλεια του κράτους και ανασφάλεια δικαίου, στον τόμο Τρομοκρατία και δικαιώματα, Α. Μανιτάκης, Α. Τάκης (επιμ.), Σαββάλας, , σ. 42 επ
- Τερζάκη Φ., (2018), Το αρχέτυπο του Νταχάου και του Γκουαντάναμο, www.phorum.gr.

Δήλωση περί μη προσβολής δικαιωμάτων πνευματικής ιδιοκτησίας

Δηλώνω υπεύθυνα ότι η διπλωματική εργασία, την οποία υποβάλλω, δεν περιλαμβάνει στοιχεία προσβολής δικαιωμάτων πνευματικής ιδιοκτησίας σύμφωνα με τους ακόλουθους όρους τους οποίους διάβασα και αποδέχομαι:

Η διπλωματική εργασία πρέπει να αποτελεί έργο του υποβάλλοντος αυτήν υποψήφιου διπλωματούχου.

Η αντιγραφή ή η παράφραση έργου τρίτου προσώπου αποτελεί προσβολή δικαιώματος πνευματικής ιδιοκτησίας και συνιστά σοβαρό αδίκημα, ισοδύναμο σε βαρύτητα με την αντιγραφή κατά τη διάρκεια της εξέτασης. Στο αδίκημα αυτό περιλαμβάνεται τόσο η προσβολή δικαιώματος πνευματικής ιδιοκτησίας άλλου υποψήφιου διπλωματούχου όσο και η αντιγραφή από δημοσιευμένες πηγές, όπως βιβλία, εισηγήσεις ή επιστημονικά άρθρα. Το υλικό που συνιστά αντικείμενο λογοκλοπής μπορεί να προέρχεται από οποιαδήποτε πηγή.

Η αντιγραφή ή χρήση υλικού προερχόμενου από το διαδίκτυο ή από ηλεκτρονική εγκυκλοπαίδεια επιφέρει τις ίδιες δυσμενείς έννομες συνέπειες με τη χρήση υλικού προερχόμενου από τυπωμένη πηγή ή βάση δεδομένων.

Η χρήση αποσπασμάτων από το έργο τρίτων είναι αποδεκτή εφόσον, αναφέρεται η πηγή του σχετικού αποσπάσματος. Σε περίπτωση επί λέξει μεταφοράς αποσπάσματος από το έργο άλλου, η χρήση εισαγωγικών ή σχετικής υποσημείωσης είναι απαραίτητη, ούτως ώστε η πηγή του αποσπάσματος να αναγνωρίζεται.

Η παράφραση κειμένου, αποτελεί προσβολή δικαιώματος πνευματικής ιδιοκτησίας. Οι πηγές των αποσπασμάτων που χρησιμοποιούνται θα πρέπει να καταγράφονται πλήρως σε πίνακα βιβλιογραφίας στο τέλος της διπλωματικής εργασίας .

Η προσβολή δικαιωμάτων πνευματικής ιδιοκτησίας επισύρει την επιβολή κυρώσεων. Για την επιβολή των ενδεδειγμένων κυρώσεων, τα αρμόδια όργανα της Σχολής θα λαμβάνουν υπόψη παράγοντες όπως το εύρος και το μέγεθος του τμήματος της διπλωματικής εργασίας που συνιστά προσβολή δικαιωμάτων πνευματικής ιδιοκτησίας.

Οι κυρώσεις θα επιβάλλονται, ύστερα από γνώμη της τριμελούς εξεταστικής επιτροπής με απόφαση της Συνέλευσης της Σχολής, και μπορούν να συνίστανται στον μηδενισμό της διπλωματικής εργασίας (με ή χωρίς δυνατότητα επανυποβολής), τη διαγραφή από τα Μητρώα των μεταπτυχιακών φοιτητών , καθώς και την επιβολή πειθαρχικών ποινών, όπως η αναστολή της φοιτητικής ιδιότητας του υποψήφιου διπλωματούχου.

Επιπλέον, παρέχω τη συναίνεσή μου, ώστε ένα ηλεκτρονικό αντίγραφο της διπλωματικής εργασίας μου να υποβληθεί σε ηλεκτρονικό έλεγχο για τον εντοπισμό τυχόν στοιχείων προσβολής δικαιωμάτων πνευματικής ιδιοκτησίας.

Ημερομηνία	Υπογραφή Υποψηφίου
30/9/2019	*Νικόλαος Α. Καρανικόλας*

NIKOLAOS KARANIKOLAS
2019.12.18 11:06:22
+02'00'