ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»

Ακαδημαϊκό έτος 2021-2022

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ
της Ειρήνης Ρήγα (Α.Μ.: ΜΔΙ 2039)

ΒΙΟΜΕΤΡΙΚΕΣ ΤΕΧΝΟΛΟΓΙΕΣ ΑΝΑΓΝΩΡΙΣΗΣ ΠΡΟΣΩΠΟΥ – Ο ΡΟΛΟΣ ΤΗΣ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ ΣΤΗΝ ΑΝΑΠΤΥΞΗ ΤΟΥΣ, ΕΝΙΣΧΥΣΗ ΒΙΝΤΕΟΕΠΙΤΗΡΗΣΗΣ ΚΑΙ ΑΝΑΚΥΠΤΟΝΤΑ ΖΗΤΗΜΑΤΑ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Επιβλέπουσα:

κ. Ευαγγελία (Λίλιαν) Μήτρου

Πειραιάς, Ιούνιος 2022

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΠΕΡΙΛΗΨΗ....4

ΕΙΣΑΓΩΓΗ....6

ΚΕΦΑΛΑΙΟ 1^{ο} : ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ- ΑΛΓΟΡΙΘΜΟΙ- ΒΙΟΜΕΤΡΙΚΕΣ ΜΕΘΟΔΟΙ/ΤΕΧΝΟΛΟΓΙΕΣ – ΒΙΝΤΕΟΕΠΙΤΗΡΗΣΗ....8

1.1. Εισαγωγή στην έννοια της Τεχνητής Νοημοσύνης – Σύντομη Ιστορική Αναδρομή - Κατηγοριοποίηση....**8**

1.1.1. Περιορισμένη ή αδύναμη (ή άλλως στενή ή ασθενής) Τεχνητή Νοημοσύνη....10

1.1.2. Γενική ή Ισχυρή Τεχνητή Νοημοσύνη....13

1.2.Αλγόριθμοι....**14**

1.2.1. Εννοιολογική προσέγγιση αλγορίθμων και Σύντομη μνεία στην ιστορική πορεία τους....15

1.2.2. Προγραμματισμός και Εκπαίδευση Αλγορίθμων....17

1.3. Εννοιολογική Οριοθέτηση και Σύντομη Ιστορική Αναδρομή των Βιομετρικών Τεχνολογιών και Βιομετρικών Συστημάτων – Χρήση αυτών μέσω Βιντεοεπιτήρησης.... **19**

ΚΕΦΑΛΑΙΟ 2^{ο} : ΠΤΥΧΕΣ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΩΣ ΘΕΜΕΛΙΩΔΟΥΣ ΑΝΘΡΩΠΙΝΟΥ ΔΙΚΑΙΩΜΑΤΟΣ – ΣΥΣΧΕΤΙΣΗ ΜΕ ΑΥΤΟ ΤΗΣ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ....28

2.1. Η εξέλιξη της έννοιας της ιδιωτικότητας βάσει ιστορικοκοινωνικού πλαισίου....**28**

2.2. Έννοια δεδομένων προσωπικού χαρακτήρα και Συνταγματική διάσταση αυτής σε συνδυασμό με την έννοια της ιδιωτικότητας.... **....31**

2.3. Νομοθετική πορεία και Ιστορική διαδρομή.... ....**35**

ΚΕΦΑΛΑΙΟ 3^{ο} : ΖΗΤΗΜΑΤΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΕ ΣΧΕΣΗ ΜΕ ΤΑ ΣΥΣΤΗΜΑΤΑ ΒΙΝΤΕΟΕΠΙΤΗΡΗΣΗΣ, ΣΧΕΔΙΟ ΚΑΝΟΝΙΣΜΟΥ Ε.Ε. ΓΙΑ ΤΗΝ ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ ΚΑΙ ΕΞΕΤΑΣΗ ΠΑΡΑΒΙΑΣΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΜΕΣΩ ΤΕΧΝΟΛΟΓΙΑΣ....40

3.1. Λειτουργία Συστημάτων Βιντεοεπιτήρησης, Επεξεργασία δεδομένων προσωπικού χαρακτήρα και Ιδιαιτερότητα Βιομετρικών δεδομένων....**40**

3.1.1.Νομιμότητα επεξεργασίας μέσω συστημάτων βιντεοεπιτήρησης....44

3.1.1.1. Βασικές Αρχές επεξεργασίας δεδομένων....44

3.1.1.2. Υποχρεώσεις Υπευθύνου Επεξεργασίας Δεδομένων προσωπικού χαρακτήρα και τήρηση εφαρμογής τους....48

3.1.1.3. Δικαιώματα υποκειμένου δεδομένων……52
3.1.1.4. Νομική Βάση επεξεργασίας δεδομένων βιντεοεπιτήρησης……55
3.1.2.Επεξεργασία Ειδικών Κατηγοριών Δεδομένων προσωπικού χαρακτήρα μέσω συστημάτων βιντεοεπιτήρησης……60
3.1.3. Ταυτότητα και Ιδιαιτερότητα Βιομετρικών Δεδομένων……62
3.2. Συστήματα Τεχνητής Νοημοσύνης και Προσέγγιση βάσει κινδύνου……**64**
3.2.1. Βασικά χαρακτηριστικά απαιτήσεων Λευκής Βίβλου για τις εφαρμογές Τεχνητής Νοημοσύνης ''υψηλού κινδύνου''……65
3.2.2. Σχέδιο Κανονισμού Ε.Ε. για την Τεχνητή Νοημοσύνη για τη δημιουργία νομικού πλαισίου στηριζόμενου στην προσέγγιση βάσει κινδύνου……68
3.2.3. Τα συστήματα απομακρυσμένης βιομετρικής αναγνώρισης φυσικών προσώπων για σκοπούς δίωξης του εγκλήματος βάσει Σχεδίου Κανονισμού Τεχνητής Νοημοσύνης……69
3.3. Τρεις αξιοσημείωτες περιπτώσεις καταστρατήγησης του δικαιώματος της ιδιωτικότητας μέσω εφαρμογής της τεχνολογίας……**71**
3.3.1. Το ''Σύνδρομο της Κίνας'' ως μορφή συστήματος αυτοματοποιημένου κοινωνικού ελέγχου……71
3.3.2. Κοινωνικά δίκτυα και Αναγνώριση προσώπου- Περίπτωση Βόρειας Καλιφόρνιας……74
3.3.3. Περίπτωση εταιρείας Clearview AI……76

ΕΠΙΛΟΓΟΣ - ΣΥΜΠΕΡΑΣΜΑΤΑ……79

ΒΙΒΛΙΟΓΡΑΦΙΑ……82

ΠΕΡΙΛΗΨΗ

Σε μια εποχή συνεχούς εξέλιξης και πολλαπλών τεχνολογικών προκλήσεων, ο πολίτης καλείται να πληροφορείται κατά το δυνατόν πληρέστερα τόσο για τον τρόπο λειτουργίας των συστημάτων αναγνώρισης προσώπου όσο και για τους κινδύνους που δύναται να επιφέρει η εκτός προβλεπόμενων νομίμων ορίων χρήση τους, σε ατομικό αλλά και σε συλλογικό επίπεδο, , παραβιάζοντας θεμελιώδη δικαιώματά του.

Στην παρούσα εργασία η ως άνω διαπίστωση αποτέλεσε το έναυσμα για τη μελέτη των βιομετρικών τεχνολογιών αναγνώρισης προσώπου, του ρόλου της τεχνητής νοημοσύνης στην ανάπτυξή τους, των διαστάσεων που λαμβάνουν λόγω της ενίσχυσης της βιντεοεπιτήρησης αλλά και των ζητημάτων προστασίας προσωπικών δεδομένων που ανακύπτουν εξ αυτής.

Στο πρώτο κεφάλαιο κρίθηκε ορθό να προσεγγιστούν οι κομβικές έννοιες της ‘’Τεχνητής Νοημοσύνης’’ και των ‘’Αλγορίθμων’’, καθώς αποτελούν τους θεμέλιους λίθους της σύλληψης και δημιουργίας συστημάτων αναγνώρισης προσώπου και η μελέτη τους συμβάλλει τα μέγιστα στην κατανόηση της λειτουργίας τους, των απεριόριστων δυνατοτήτων αλλά και των αστοχιών στις οποίες δύναται να οδηγήσει μια εσφαλμένη ταυτοποίηση. Επιχειρείται, λοιπόν, η εννοιολογική τους προσέγγιση και σύντομη μνεία στην ιστορική τους πορεία. Επιπλέον, στη μεν τεχνητή νοημοσύνη λαμβάνει χώρα η παρουσίαση των δύο κατηγοριών που τη συναποτελούν, ήτοι η ‘’περιορισμένη ή αδύναμη’’ και η ‘’γενική ή ισχυρή’’, στους δε αλγορίθμους η σημασία που πρέπει να δίδεται στην ποιότητα του προγραμματισμού τους και στην ορθή τους εκπαίδευση προκειμένου να χαρακτηρίζονται από ουδετερότητα και αντικειμενικότητα. Το εν λόγω κεφάλαιο ολοκληρώνεται με την αναφορά στην έννοια των ‘’Βιομετρικών Τεχνολογιών’’ και των ‘’Βιομετρικών Συστημάτων’’, τον ορισμό τους αλλά και τις προϋποθέσεις που πρέπει να πληρούνται προκειμένου να χρησιμοποιηθεί ένα ανθρώπινο χαρακτηριστικό της φυσιολογίας ή/και της συμπεριφοράς ως βιομετρικό χαρακτηριστικό, επισημαίνεται η χρήση αυτών μέσω της βιντεοεπιτήρησης και γίνεται σύντομη ιστορική αναδρομή.

Στο δεύτερο κεφάλαιο, παρουσιάζονται πτυχές της ιδιωτικότητας χάριν της σημασίας της ως θεμελιώδους δικαιώματος, το οποίο πρωτίστως παραβιάζεται λόγω της, κατά περίπτωση, υπερβολικής επεμβατικότητας των συστημάτων αναγνώρισης προσώπου στην ανθρώπινη ζωή. Γίνεται αναφορά στην εξέλιξη της έννοιας βάσει ιστορικοκοινωνικού πλαισίου, επισημαίνεται η έννοια των δεδομένων προσωπικού χαρακτήρα και η

συνταγματική τους διάσταση σε συνδυασμό με αυτή της ιδιωτικότητας και καταλήγει με τη μνεία στη νομοθετική πορεία και την ιστορική διαδρομή που διέγραψαν.

Στο τρίτο και τελευταίο κεφάλαιο, εκτίθενται αρχικώς τα ζητήματα προσωπικών δεδομένων που ανακύπτουν ως προς τη λειτουργία των συστημάτων βιντεοεπιτήρησης. Δίδεται έμφαση στη νομιμότητα της επεξεργασίας προσωπικών δεδομένων, βάσει του Γενικού Κανονισμού υπ' αριθμ. 2016/679 για την προστασία των Προσωπικών Δεδομένων (ΓΚΠΔ). Το ζήτημα της νομιμότητας της επεξεργασίας είναι κομβικό, διότι, προτού χρησιμοποιηθεί το υλικό, πρέπει να καθίσταται σαφής η παράθεση των σκοπών επεξεργασίας, να πληρούνται οι βασικές αρχές που τη διέπουν, να τηρούνται εμπράκτως οι υποχρεώσεις του υπευθύνου επεξεργασίας, όπως επίσης και τα δικαιώματα του υποκειμένου των δεδομένων. Ακολούθως, γίνεται αναφορά στην βαρύνουσα ιδιαιτερότητα των βιομετρικών δεδομένων και θίγεται η προσέγγιση των συστημάτων τεχνητής νοημοσύνης βάσει κινδύνου παρουσιάζοντας το Σχέδιο Κανονισμού της Ευρωπαϊκής Ένωσης για την Τεχνητή Νοημοσύνη. Η εν λόγω πραγματεία ολοκληρώνεται με την εξέταση τριών αξιοσημείωτων περιπτώσεων καταστρατήγησης του ως άνω αναφερθέντος θεμελιώδους δικαιώματος, της ιδιωτικότητας, μέσω της εφαρμογής της τεχνολογίας.

ΕΙΣΑΓΩΓΗ

Στη σημερινή εποχή η ανάπτυξη της τεχνολογίας λαμβάνει χώρα με ιδιαιτέρως ταχείς ρυθμούς και η παρείσφρηση εφαρμογών τεχνητής νοημοσύνης σε διαφόρους τομείς όπως του ιδιωτικού βίου, της οικονομίας, της υγείας, καλεί τους πολίτες να ευρίσκονται σε εγρήγορση ως προς την τεχνολογική τους κατάρτιση και συνεχή επιμόρφωση προκειμένου να ανταποκριθούν με υπευθυνότητα στη διαχείριση των νέων δεδομένων. Τα θετικά στοιχεία των εν λόγω εφαρμογών πλείστα όσα αλλά αντιστοίχως πολλές οι εσφαλμένες ταυτοποιήσεις των συστημάτων τεχνητής νοημοσύνης λόγω της αλγοριθμικής αδιαφάνειας.

Στην πορεία των ετών η διαμόρφωση των συστημάτων αναγνώρισης προσώπου, εκκινώντας ήδη από τη δεκαετία του 1960 και οδηγώντας στη σύγχρονη εποχή και τα σημερινά εξελιγμένα συστήματα, φανέρωσε την επιθυμία εντοπισμού και αναγνώρισης των ανθρωπίνων χαρακτηριστικών, αρχικώς με μη αυτοματοποιημένο τρόπο (περιπτώσεις ανάπτυξης τεχνικών ''eigenface'' και ''fisherfaces''[1]) και επακολούθως με αυτοματοποιημένες μεθόδους μέσω της χρήσης των χαρακτηριστικών της φυσιολογίας ή της συμπεριφοράς . Οι προβληματισμοί που εγείρονται ως προς τη χρήση των συγκεκριμένων συστημάτων εύλογοι, καθώς ιδιαιτέρως στην περίπτωση των βιομετρικών τεχνολογιών τα αντλούμενα δεδομένα υφίστανται ειδική τεχνική επεξεργασία και η χρήση τους αποσκοπεί στην αδιαμφισβήτητη ταυτοποίηση φυσικού προσώπου.
Με αυτό τον τρόπο, συνειδητοποιεί κανείς ότι οι τεχνολογίες παρακολούθησης δύνανται να οδηγήσουν σε περιορισμό θεμελιωδών ανθρωπίνων δικαιωμάτων, όπως αυτό της ιδιωτικότητας, αν δεν τηρούνται οι εγγυήσεις και συγκεκριμένες νομικές απαιτήσεις που θα διασφαλίζουν ότι το κανονιστικό πλαίσιο έχει προσμετρήσει τους άνω παράγοντες διαφυλάττοντας την ανθρώπινη αξιοπρέπεια και την ελεύθερη ανάπτυξη προσωπικότητας.

Προς αυτή την κατεύθυνση έχει συμβάλλει τα μέγιστα ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) μέσω των διατάξεων περί νομιμότητας επεξεργασίας κατά τη λειτουργία των συστημάτων βιντεοεπιτήρησης, επισημαίνοντας τη σαφήνεια και την επάρκεια της αιτιολόγησης από τις οποίες πρέπει να χαρακτηρίζεται ο σκοπός της εκάστοτε επεξεργασίας, το ότι πρέπει να πληρούνται οι βασικές αρχές που τη διέπουν – όπως επί παραδείγματι η αρχή νομιμότητας, αντικειμενικότητας και διαφάνειας - , ακόμη

[1] Βλ. Turk, M. και Pentland, A. (1991) 'Eigenfaces for Recognition', Journal of Cognitive Neuroscience, 3(1), σσ 71–86. Επίσης, βλ. Belhumeur, P.N., Hespanha, J.P., Kriegman, D.J. (1997) 'Eigenfaces vs. fisherfaces: Recognition using class specific linear projection', IEEE Transactions on Pattern Analysis and Machine Intelligence, 19(7), σελ. 711–720. doi:10.1109/34.598228.

να τηρούνται εμπράκτως οι υποχρεώσεις του υπευθύνου επεξεργασίας, όπως επίσης να δύνανται να ασκηθούν νομοτύπως τα δικαιώματα του υποκειμένου των δεδομένων. Τέλος, αποτελεί αδήριτη ανάγκη να λαμβάνεται υπόψη η ορθή νομική βάση στην οποία θα στηριχθεί η επεξεργασία των δεδομένων.

Αν τηρηθούν τα ανωτέρω και υφίσταται συνεχής επαγρύπνηση επί πιθανής μη ορθής χρήσης των συστημάτων αναγνώρισης προσώπου και των κινδύνων που αυτή συνεπάγεται – στην παρούσα μελέτη αναλύεται μάλιστα και το προταθέν Σχέδιο Κανονισμού Ε.Ε. για την Τεχνητή Νοημοσύνη για τη δημιουργία νομικού πλαισίου στηριζόμενου στην προσέγγιση βάσει κινδύνου- θα δίδεται η δυνατότητα αξιοποίησής τους προς εντοπισμό εγκληματικών, επί παραδείγματι, συμπεριφορών και έγκαιρη αντιμετώπισή τους αναδεικνύοντας την ουσία της δημιουργίας τους.

ΚΕΦΑΛΑΙΟ 1ο

ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ- ΑΛΓΟΡΙΘΜΟΙ- ΒΙΟΜΕΤΡΙΚΕΣ ΜΕΘΟΔΟΙ/ΤΕΧΝΟΛΟΓΙΕΣ – ΒΙΝΤΕΟΕΠΙΤΗΡΗΣΗ

1.1.Εισαγωγή στην έννοια της τεχνητής νοημοσύνης - Σύντομη Ιστορική Αναδρομή - Κατηγοριοποίηση

Η ανάπτυξη της τεχνητής νοημοσύνης λαμβάνει χώρα με ταχείς ρυθμούς. Καθίσταται εμφανές ότι η ψηφιακή τεχνολογία διαδραματίζει σημαίνοντα ρόλο σε κάθε πτυχή της ζωής και εξ αυτού του λόγου θα πρέπει να εμπνέει εμπιστοσύνη στους ανθρώπους , καθώς ο παράγοντας αυτός αποτελεί προϋπόθεση για την υιοθέτησή της.

Ως ‘’Τεχνητή Νοημοσύνη’’, κατά τους Negnevitsky, Βλαχάβα και Κεφαλά, δύναται να θεωρηθεί η ικανότητα μιας μηχανής, ηλεκτρονικού υπολογιστή ή ρομπότ που ελέγχεται από υπολογιστή, να εκτελεί εργασίες και καθήκοντα που συνδέονται με ευφυή, έμβια όντα.[2] Επιχειρώντας προσέγγιση των δύο συνθετικών του όρου, παρατηρεί κανείς ότι το πρώτο συνθετικό ‘’τεχνητή’’ απηχεί μια μη φυσική διεργασία, η οποία είναι κατασκευασμένη με τεχνικά μέσα. [3] Για το δεύτερο συνθετικό της, όμως, τη ‘’νοημοσύνη’’ δεν εντοπίζεται κοινώς παραδεκτός όρος στη βιβλιογραφία. Κατά ορισμένους συγγραφείς, όπως ο Ισραηλινός **Γιουβάλ Νώε Χαράρι, η επιστήμη γνωρίζει ελάχιστα για το νου και τη συνείδηση.**[4] Κατ’ επέκταση, αφού δεν είναι ακριβής η γνώση περί του τι είναι ο νους, ο άνθρωπος αδυνατεί να κατανοήσει τι είναι η τεχνητή νοημοσύνη παρότι ο ίδιος τη δημιούργησε. Ακόμη, **διατυπώνει την άποψη ότι σύντομα η τεχνητή νοημοσύνη θα έχει φτάσει σε τέτοια επίπεδα ώστε θα είναι σε θέση να γνωρίζει περισσότερα για τους ανθρώπους από ό, τι οι ίδιοι για τον εαυτό τους**. Διάφοροι ακόμη ορισμοί έχουν διατυπωθεί στην επιστημονική κοινότητα από τη δεκαετία του 1950 όταν η Τεχνητή Νοημοσύνη εμφανίστηκε για πρώτη φορά ως όρος. Ήταν τότε που ο **μαθηματικός Alan Turing** δημοσίευσε το περίφημο άρθρο του ‘’Computing Machinery and Intelligence’’, μέσω του οποίου **εισήγαγε μια διαδικασία** που φιλοδοξούσε να εξακριβώσει **αν μια μηχανή διαθέτει ευφυΐα.**[5] **Βασικό κριτήριο της διαδικασίας** ήταν ότι, **αν μια μηχανή επιτύχει**

[2] M. Negnevitsky, Artificial Intelligence: A Guide to Intelligence Systems (3rd Edition), Addison Wesley, 2020, Βλ. ομοίως Βλαχάβας, Κεφαλάς κ. ά., Τεχνητή Νοημοσύνη, Δ’ έκδοση, Εκδόσεις Πανεπιστημίου Μακεδονίας, Αύγουστος 2020, https:// aibook.csd.auth.gr/

[3] Λεωνίδας Ι. Κανέλλος, Εφαρμογές Τεχνητής Νοημοσύνης (στο δίκαιο και στη δικαστική πρακτική), Εκδ. Νομική Βιβλιοθήκη, 2020, σελ. 27

[4] Κανέλλος, 2020, σελ. 27

[5] Βόρρας Κ. Απόστολος, Μήτρου Λίλιαν, ‘’Τεχνητή Νοημοσύνη και προσωπικά δεδομένα, Μια θεώρηση υπό το πρίσμα του Ευρωπαϊκού Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 2016/679’’, ΔΙΤΕ(πρώην ΔΙΜΕΕ), Τεύχος 4/2018, Οκτώβριος- Νοέμβριος- Δεκέμβριος, σελ. 461

να ξεγελάσει τους ανθρώπους και να τους κάνει να πιστέψουν ότι είναι άνθρωπος, τότε πρέπει να είναι τουλάχιστον εξίσου έξυπνη με έναν άνθρωπο.[6] Την εν λόγω πρόταση του Turing, επακολούθησε η έκφραση της ανθρωπομορφικής ιδέας του John McCarthy[7] το 1956, ο οποίος ορίζει ως τεχνητή νοημοσύνη τον κλάδο που προσπαθεί να καταστήσει τις υπολογιστικές μηχανές ικανές να μιμηθούν τη συμπεριφορά του ανθρώπου αναφορικά με την κατανόηση του περιβάλλοντος και την επίλυση προβλημάτων. Η Τεχνητή Νοημοσύνη ως αντικείμενο έρευνας σε ποικίλους επιστημονικούς χώρους έχει εμπνεύσει και την έβδομη τέχνη.[8] Παρατηρείται, λοιπόν, ότι το πρίσμα και το περιβάλλον του κάθε ερευνητή είναι οι παράγοντες που καθορίζουν την ανά περιόδους εννοιολογική προσέγγιση του όρου. Κατά ένα μεγάλο ποσοστό οι ερευνητές ταυτίζονται με τον ορισμό που παρουσιάζουν οι **Barr και Feigenbaum**[9], ο οποίος συμφωνεί με αυτόν του McCarthy, παρουσιάζοντας την **''Τεχνητή Νοημοσύνη ως τομέα της επιστήμης των υπολογιστών που αποσκοπεί στη σχεδίαση και υλοποίηση προγραμμάτων, τα οποία δύνανται να μιμηθούν τις ανθρώπινες γνωστικές ικανότητες** με αποτέλεσμα να εμφανίζουν χαρακτηριστικά που προσιδιάζουν σε ανθρώπινη συμπεριφορά, όπως η **αντίληψη μέσω της όρασης, η μάθηση,** η εξαγωγή συμπερασμάτων και η κατανόηση της φυσικής γλώσσας''.

Στο σημείο αυτό, κρίνεται σκόπιμο να αναφερθεί κι ένας ακόμη ορισμός της Τεχνητής Νοημοσύνης, αυτός της υπ' αριθμόν COM (2018) 237 final ανακοίνωσης της Ευρωπαϊκής Επιτροπής με θέμα ''Τεχνητή Νοημοσύνη για την Ευρώπη'' κατά τον οποίο: ''η τεχνητή νοημοσύνη αναφέρεται σε συστήματα που χαρακτηρίζονται από ευφυή συμπεριφορά, αναλύοντας το περιβάλλον τους και ενεργώντας – με κάποιο βαθμό αυτονομίας- για την επίτευξη συγκεκριμένων στόχων. Τα συστήματα που λειτουργούν βάσει τεχνητής νοημοσύνης δύνανται να βασίζονται αποκλειστικά σε λογισμικό , ενεργώντας στον εικονικό κόσμο (π.χ. βοηθοί φωνής, λογισμικό ανάλυσης εικόνας, μηχανές αναζήτησης, συστήματα αναγνώρισης ομιλίας και προσώπου) ή η τεχνητή νοημοσύνη μπορεί να ενσωματωθεί σε συσκευές υλισμικού (π.χ. προηγμένα ρομπότ, αυτόνομα αυτοκίνητα, δρόμοι ή εφαρμογές του διαδικτύου των πραγμάτων).''.

Όσον αφορά στην **κατηγοριοποίηση της Τεχνητής Νοημοσύνης (ΤΝ**), κατά τους Τάσση και Κανέλλο, τις απόψεις των οποίων ασπάζεται και η Ανδρουλάκη[10], διακρίνεται σε δύο μεγάλες γενικές κατηγορίες που αναφέρονται κατά βάση **στην εξάρτηση της εφαρμογής της από τη συμμετοχή του ανθρώπινου παράγοντα.** Η Τεχνητή Νοημοσύνη διακρίνεται σε δύο μεγάλες –παγκοίνως παραδεκτές- γενικές κατηγορίες που αναφέρονται

---

[6] Turing Alan, Computing machinery and intelligence, Mind, 59, 1950, διαθέσιμο στο http://www.turing.org.uk/turing/scrapbook/test.html

[7] John McCarthy , What is AI? Basic Questions διαθέσιμο στο https://jmc.stanford.edu./atificial-intelligence/what-is-ai/index.html

[8] https://en.wikipedia.org/wiki/List_of_artificial_intelligence_films

[9] Avron Barr & Edward Feigenbaum, The Handbook of Artificial Intelligence, 1981, σελ. 21

[10] Τάσσης Σπύρος, Το δίκαιο στην εποχή της τεχνητής νοημοσύνης- Μια νέα οπτική στο δίκαιο και την ηθική, 2019 διαθέσιμο στο https://www.lawspot.gr/nomika-blogs/spiros_tassis/dikaio-stin-epohi-tis-tehnitis-noimosynis, Κανέλλος, 2020, σελ. 28 επ. και Ανδρουλάκη Ευαγγελία, Τεχνητή Νοημοσύνη και Προσωπικά Δεδομένα: η περίπτωση της εξ αποστάσεως βιομετρικής ταυτοποίησης, 2021, διαθέσιμο στο https://ejournals.lib.auth.gr/infolawj/

κυρίως στην εξάρτηση της εφαρμογής από τη συμμετοχή του ανθρώπινου παράγοντα, ήτοι την περιορισμένη ή αδύναμη (ή αλλιώς στενή ή ασθενής) ΤΝ και τη γενική ή ισχυρή ΤΝ, οι οποίες θα αναλυθούν στα δύο επόμενα επιμέρους κεφάλαια.

1.1.1. Περιορισμένη ή αδύναμη (ή αλλιώς στενή ή ασθενής) Τεχνητή Νοημοσύνη

Η εν λόγω κατηγορία ορίζεται ως η σημερινή ικανότητα ενός υπολογιστή να εκτελεί με εξαιρετική επιτυχία μια μεμονωμένη εργασία, επί παραδείγματι να διενεργεί πολύπλοκους μαθηματικούς υπολογισμούς, να εντοπίζει πληροφορίες ή να παίζει παιχνίδια (όπως σκάκι), αλλά διακρίνεται και σε ψηφιακές εφαρμογές των οποίων κάνουμε χρήση, όπως **εφαρμογή αναγνώρισης προσώπων**, εργαλείο φιλτραρίσματος ανεπιθύμητης αλληλογραφίας (spam) ή ακόμη και μια συνιστώμενη λίστα αναπαραγωγής από την υπηρεσία διαδικτυακής μουσικής Spotify ή ακόμη και ένα αυτοκίνητο χωρίς οδηγό. Αξίζει να διευκρινιστεί ότι όταν χρησιμοποιεί κανείς τον όρο ''αδύναμη ή ασθενής'', εννοεί ότι δε δύναται να αναπτύξει αυτόνομη γνώση αλλά στηρίζεται σε προγραμματισμό που εισάγει ο άνθρωπος, καθώς όλα τα συστήματα ΤΝ βρίσκουν έρεισμα στη γνώση και τον **αλγόριθμο** επιλογής της αντίδρασης που ορίζει ο άνθρωπος.[11] **Η πλειονότητα των σημερινών γνωστών εφαρμογών ανήκουν στην κατηγορία της στενής Τεχνητής Νοημοσύνης,** η οποία διήλθε διάφορα στάδια εξέλιξης που θεωρείται ορθό να θιγούν περαιτέρω σε συνάρτηση με μία εις έτι διάκριση, αυτή της στενής Τεχνητής Νοημοσύνης σε ''συμβολική ΤΝ'' και σε ''μηχανική μάθηση''. Τέλος, θα αναφερθούν και ορισμένα χαρακτηριστικά γνωρίσματα αυτής, προτού συνεχιστεί η μνεία στη ''γενική Τεχνητή Νοημοσύνη''.

Κατά τη δεκαετία του 1960 άρχεται το πρώτο κύμα εξέλιξης της ΤΝ και ολοκληρώνεται στο τέλος της δεκαετίας του 1980. Το χρονικό αυτό διάστημα έρχεται στο προσκήνιο η ''συμβολική τεχνητή νοημοσύνη'' , η οποία χαρακτηρίζεται από τα έμπειρα συστήματα.[12] Τα εν λόγω προγράμματα καθοδηγούν πιστά τον υπολογιστή ως προς την επίλυση προβλημάτων ενός επιστημονικού τομέα[13]. Η βάση τους εντοπίζεται σε ακριβείς κανόνες με δομή της μορφής ''εάν- τότε'', οι οποίοι είναι κωδικοποιημένοι από εμπειρογνώμονα (νομικό, γιατρό, μηχανικό, χημικό). Οι μεταβλητές της απόφασης δύνανται να έχουν μια ''τιμή αλήθειας'', η οποία κινείται βάσει πιθανοτήτων προκαθορισμένης κλίμακας, καθώς στην επιστήμη οι απόλυτες απαντήσεις που απαιτούνται από το σύστημα δεν είναι πάντα διαθέσιμες. Κατά το παράδειγμα που φέρει ο κ. Κανέλλος, σε συνέχεια των ανωτέρω επισημάνσεών του, ένα έμπειρο σύστημα ιατρικής διάγνωσης, κατόπιν ανάλυσης των συμπτωμάτων, δύναται να ενημερώσει τους ασθενείς για το βαθμό ή την πιθανότητα να

[11] Τάσσης, 2019

[12] Παράδειγμα ενός rule- based chatbox αποτελεί το πρόγραμμα ELIZA , το οποίο δημιουργήθηκε στο MIT μεταξύ 1964 και 1966 από τον Joseph Weizenbaum, το οποίο προσομοίωνε την επιφανειακή διενέργεια διαλόγου ανθρώπου- μηχανής στην αγγλική γλώσσα μέσω αναγνώρισης λεκτικών μοτίβων, Weizenbaum Joseph (January 1966). "ELIZA- A computer Program for the Study of Natural Language Communication Between Man and Machine'' http:// www.universelle-automation.de/1966_Boston.pdf

[13] Κανέλλος, 2020, σελ.29

έχουν κάποια ασθένεια. Κι αν συμπεριληφθούν πολλές μεταβλητές και τιμές, τα συστήματα είναι σε θέση να αντιμετωπίσουν οριακές τιμές παρά την ασάφειά τους.

Κατόπιν της αναφοράς στη συμβολική ΤΝ, η οποία επικράτησε για μια εικοσαετία, όπως εθίγη ανωτέρω, στις αρχές της δεκαετίας του 1990 και μέχρι το 2010 έλαβε χώρα ουσιώδης ώθηση για την έρευνα και την ανάπτυξη των τεχνολογιών ΤΝ μέσω της βελτίωσης της υπολογιστικής ισχύος και της χωρητικότητας μνήμης.[14] Τα στοιχεία αυτά συνετέλεσαν στο να μπορέσουν να εφαρμοστούν προσαρμοστικά στατιστικά μοντέλα σε μεγάλο όγκο δεδομένων αλλά και στη δυνατότητα να πραγματοποιηθούν προβλέψεις βάσει αυτών . Η σημαντική αυτή εξέλιξη ευνόησε την **ανάπτυξη της ''μηχανικής μάθησης'' (Machine learning), την οποία χρησιμοποιούν με παραγωγικό τρόπο τόσο δημόσιοι οργανισμοί όσο και ιδιωτικές εταιρείες.** Όλα αυτά τα στοιχεία, τα οποία παρατίθενται, καταδεικνύουν τη δυναμική της τεχνητής νοημοσύνης και την καταλυτική επίδραση που ασκούν τα συστήματά της σε πολλαπλούς τομείς τόσο της επιστήμης όσο και της καθημερινότητας. Τα τελευταία χρόνια, οι μηχανές διαφαίνεται εναργώς ότι έχουν ανεξαρτητοποιηθεί ως προς την εκμάθηση και τη διεύρυνση των γνώσεών τους καθώς επεξεργάζονται δεδομένα με σκοπό την παραγωγή νέων λύσεων. Σε αυτή την πρόοδο έχει συμβάλει η τεχνολογία της βαθιάς εκμάθησης (Deep Learning), η οποία αποτελεί υποπεδίο της μηχανικής μάθησης και την αναγνώρισή της οφείλει στο ότι ο τρόπος ανάπτυξής της ομοιάζει με τη δομή του εγκεφάλου του ανθρώπου.

Θεωρείται άξιο να σημειωθεί ότι ο συνδυασμός της ικανότητας ενός μηχανήματος να ''μαθαίνει'' (Machine learning, ως άνω), με την ύπαρξη και χρησιμοποίηση ''μεγάλων δεδομένων'' (big data) αποτελεί την κορύφωση της χρήσης της Τεχνητής Νοημοσύνης.[15] Ως **''μεγάλα δεδομένα''** ορίζονται οι βάσεις δεδομένων που δημιουργούνται από την εισροή τεράστιων ποσοτήτων από ετερόκλητα δεδομένα εξαγόμενα από διάφορες πηγές, συνήθως σε πραγματικό χρόνο και μεγάλη ταχύτητα.[16] Τα εν λόγω δεδομένα δημιουργούν εύφορο έδαφος ως προς την ανάλυσή τους καθώς εντοπίζονται επαναλαμβανόμενα μοτίβα ή/και συσχετισμοί μεταξύ αυτών και μπορούν εν συνεχεία να εξαχθούν συμπεράσματα βάσει αυτής της διαδικασίας. Όπως επισημαίνουν οι κ. Βόρρας και κ. Μήτρου, σε συνέχεια της πρότερης ανάλυσής τους, το χαρακτηριστικό στοιχείο διαφοροποίησης της Τεχνητής Νοημοσύνης και τω παραδοσιακών μοντέλων ανάλυσης δεδομένων είναι ότι στη δεύτερη περίπτωση χωρίς τον προγραμματιστή του συστήματος δεν είναι δυνατόν να προκαθοριστεί ο τρόπος με τον οποίο θα γίνει η συσχέτιση των δεδομένων, ενώ στην περίπτωση της Τεχνητής Νοημοσύνης μαθαίνει από τα δεδομένα που ''συναντά'', δίχως να υπάρχει συνεξάρτηση από τον ανθρώπινο παράγοντα.[17] Σχετικά με τη μηχανική μάθηση και την εξόρυξη δεδομένων χρησιμοποιούνται συχνά εναλλακτικά, αλλά παρά το γεγονός

[14] Κατά την ανάλυση του Κανέλλου(2020), δύο ορόσημα- ''σταθμοί'' της περιόδου αυτής αποτέλεσαν πρώτον , το 1996, η επικράτηση του σκακιστικού ρομπότ Deep Blue της IBM, επί του θρυλικού παγκόσμιου πρωταθλητή σκακιού Γκάρι Κασπάροφ, αλλά και, δεύτερον, το 2011, το σύστημα τεχνητής νοημοσύνης της IBM Watson το οποίο αντιμετώπισε και εκτόπισε όλους τους αντιπάλους του, νικώντας σε τηλεοπτικό παιχνίδι γνώσεων (Jeopardy)

[15] Βόρρας, Μήτρου, 2018, σελ. 461

[16] Laney, D., ''3-D Data Management: Controlling Data volume, Velocity and Variety, ''META Group Research Note, February 16 2001

[17] The Norwegian Data Protection Authority, Artificial Intelligence and Privacy, Report January 2018, page 5

αυτό θα μπορούσε να υποστηριχθεί ότι η **μηχανική μάθηση** επικεντρώνεται περισσότερο στην προσαρμοστική συμπεριφορά και τη λειτουργική χρήση, ενώ η **εξόρυξη δεδομένων** εστιάζει στο χειρισμό μεγάλων ποσοτήτων δεδομένων και στην ανακάλυψη προηγουμένων αγνώστων προτύπων (έμμεσες γνώσεις, κανονικότητες) στα δεδομένα.[18]

Η ως άνω ανάλυση είναι καίριας σημασίας, καθώς αποδίδεται η **διάσταση που καταλαμβάνει η τεχνητή νοημοσύνη μέσω των εφαρμογών της στη ζωή μας και γεννά έμπνευση και προσδοκίες για τις ευκαιρίες που συνεπάγεται η χρήση της.** Δεν μπορεί, όμως, να παραβλεφθεί κι ο **σκεπτικισμός που δημιουργείται σχετικά με τους κινδύνους που μπορεί να επιφέρει στους πολίτες,** οι οποίοι φοβούνται ότι δε θα έχουν τη δύναμη να υπερασπιστούν τα δικαιώματα και την ασφάλειά τους στις περιπτώσεις που καλούνται να αντιμετωπίσουν τις πληροφοριακές ασυμμετρίες της αλγοριθμικής λήψης αποφάσεων, όπως και οι επιχειρήσεις ανησυχούν λόγω των προβλημάτων ασφάλειας δικαίου.[19]

Καθώς η τεχνητή νοημοσύνη αναπτύσσεται, καθίσταται όλο και περισσότερη **επιτακτική η ανάγκη για διαφάνεια και λογοδοσία** μέσω της επεξήγησης των ανωτέρω αλγοριθμικά λαμβανομένων αποφάσεων έτσι ώστε να είναι κατανοητοί στο μέσο άνθρωπο. Οι δύο αυτές αρχές αποτελούν δύο εκ των σημαντικότερων εξ αυτών που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα και δύνανται κατά την Ανδρουλάκη[20] να οδηγήσουν στο μέλλον σε **''αλγοριθμική διαφάνεια''**, σε ό, τι αφορά στην τεχνητή νοημοσύνη.

Επιχειρώντας μια σύντομη προσέγγιση ορισμένων χαρακτηριστικών της στενής ΤΝ, κύριο στοιχείο αποτελεί η **αδυναμία μεταβιβαζόμενης μάθησης** από το έναν τομέα σε έναν άλλο[21], ήτοι για κάθε νέα εργασία που συντελείται πρέπει, κατά ένα μεγάλο βαθμό, να επαναλαμβάνεται από την αρχή η διαδικασία προγραμματισμού ενός συστήματος ή αλγοριθμικού μοντέλου, με διαφοροποίηση όμως των κινήσεων και της μηχανικής προσέγγισης. Κατά τον κ. Κανέλλο[22], ορισμένες βασικές αρχές που πρέπει να τηρούνται αναφορικά με την επιλογή των δεδομένων ενός αξιόπιστου και κοινωνικά δίκαιου αλγοριθμικού συστήματος, είναι η **αντικειμενικότητα, η αμεροληψία και η αποφυγή εισαγωγής διακρίσεων και μεροληψίας (algorithmic bias).** Είναι ευκρινής η διαπίστωση ότι η εν τοις πράγμασι πλήρωση των ως άνω αρχών αποσκοπεί στη διασφάλιση του ότι τα συμφέροντα μειονοτήτων και ευπαθών ομάδων αντιπροσωπεύονται με επάρκεια στα δεδομένα εκπαίδευσης και ότι ο αλγόριθμος λειτουργεί στην πράξη κατά το δυνατόν αντικειμενικά και δίκαια. Τέλος, αναφορικά με την **εκπαίδευση των αλγορίθμων** κρίνονται ως απαιτούμενα η μεγάλη υπολογιστική ισχύς και μεγάλος όγκος εκπαιδευτικών δεδομένων. Είναι στοιχεία που προϋποθέτουν τόσο οικονομικό υπόβαθρο

[18] Tomkos, I., Klonidis,D., Pikasis,E. and Theodoridis,S., 2020, Toward the 6G network era: Opportunities and Challenges, IT Professional , 22(1), pp.34-38

[19] Ευρωπαϊκή Επιτροπή, Λευκή Βίβλος, Τεχνητή Νοημοσύνη- Η ευρωπαϊκή προσέγγιση της αριστείας και της εμπιστοσύνης διαθέσιμο στο https://op.europa.eu/el/publication-detail/-/publication/ac957f13-53c6-11ea-aece-01aa75ed71a1

[20] Ανδρουλάκη, 2021, σελ. 16

[21] Ben Dickson, What is transfer learning?, 10th June 2019, διαθέσιμο στο https://bdtechtalks.com/2019/06/10/what-is-tranfer-learning

[22] Κανέλλος, 2020, σελ.54

αλλά και αξιοποίηση σε χρόνο και, προκειμένου να προσελκύσει το ενδιαφέρον των επενδυτών μια τέτοια ερευνητική απόπειρα τεχνητής νοημοσύνης, πρέπει να αφορά έναν καίριο τομέα δραστηριότητας.

Κατά τη μελέτη των πηγών της παρούσας εργασίας διαπίστωσα τον ιδιαίτερα σημαίνοντα ρόλο που διαδραματίζουν οι αλγόριθμοι στα συστήματα τεχνητής νοημοσύνης και δη αναγνώρισης προσώπου, καθώς **μετρήσεις από ατελείς αλγορίθμους δύνανται πολύ συχνά** να έχουν **ως αποτέλεσμα εσφαλμένη ταυτοποίηση φυσικών προσώπων**.

Εξ αυτού του λόγου, κατόπιν μιας σύντομης μνείας στην έτερη κατηγορία τεχνητής νοημοσύνης , τη ''γενική'' ή ''ισχυρή'', θα λάβει χώρα επισκόπηση ορισμένων στοιχείων της ιστορικής εξέλιξης και του προγραμματισμού αλλά και της εκπαίδευσης των αλγορίθμων.

1.1.2. Γενική ή Ισχυρή Τεχνητή Νοημοσύνη

Η συγκεκριμένη κατηγορία τεχνητής νοημοσύνης είναι ικανή να εμφανίζει **στοιχεία ανθρώπινης νοημοσύνης και κοινής λογικής** και έχει τη δυνατότητα να θέσει τους δικούς της στόχους και να αντιμετωπίσει κάθε γενικευμένο έργο που της ζητείται και να εκτελέσει επιτυχώς κάθε νοητική εργασία που απαιτείται, σχεδόν σα να ήταν άνθρωπος[23].

Τα στοιχεία αυτά παραμένουν **σε θεωρητικό υπόβαθρο**, καθώς η παρούσα περιγραφή τεχνητής νοημοσύνης αποτελεί τεχνολογικό ζητούμενο για τις επερχόμενες δεκαετίες. Διάφορα προηγμένα υπολογιστικά συστήματα που έχουν ανά περιόδους παρουσιαστεί, τα οποία έχουν αναπτύξει την ικανότητα λήψης αποφάσεων και σύνθεσης πληροφοριών βρίσκονται σε πρώιμο στάδιο, αδυνατώντας να προσομοιάσουν στις ανωτέρω ανθρώπινες ικανότητες μέσω συνδυασμού αυτών. [24] Δεν μπορεί, παρόλα αυτά, να παραγνωριστεί το γεγονός ότι ο τομέας της αναγνώρισης εικόνας αποτελεί εξαίρεση καθώς είναι μια επιτυχημένη εφαρμογή σε σχέση με άλλες απόπειρες που έχουν λάβει χώρα.

Οι επιστήμονες αξιολογούν την τεχνητή νοημοσύνη βασιζόμενοι σε **διάφορες δοκιμασίες** στις οποίες πρέπει να υποβληθεί και να φέρει εις πέρας με επιτυχία **η νοητική ικανότητα της μηχανής** ώστε να κριθεί **αν ομοιάζει ή όχι στην ανθρώπινη νοητική λειτουργία**. Ενδεικτικά και προς επίρρωση της νοητικής αλληλουχίας της ενότητας, θα επισημανθούν ορισμένες βασικές εξ αυτών δοκιμασίες που έχουν διατυπωθεί από την επιστημονική κοινότητα[25] προκειμένου να εξαχθούν συμπεράσματα. Πρώτη δοκιμασία αποτελεί το **Τεστ Turing**, το οποίο προβαίνει στον έλεγχο της ικανότητας της μηχανής να επιδείξει νοήμονα συμπεριφορά η οποία ισοδυναμεί με την αντίστοιχη του ανθρώπου ή είναι ακόμη και δυσδιάκριτη από αυτόν. Ακολουθούν ακόμη τέσσερις δοκιμασίες, αυτή του ''τεστ του

[23] Τάσσης, 2019 αλλά και σχετικές αναφορές διαθέσιμες στα https://medium.com/personified-systems-/structure-in-ai-law-ethics-the-world-and-the-mind-7e00c5e0ae2 και https://techcrunch.com/2017/01/28/artificial-intelligence-and-the-law/?guccounter

[24] Κανέλλος, 2020, σελ.35

[25] Turing Alan, Computing machinery and intelligence, Mind, 59, 1950, σελ. 433-460 διαθέσιμο στο http://www.turing.org.uk/turing/scrapbook/test.html , Russell & Peter Norvig, Τεχνητή Νοημοσύνη, μια σύγχρονη προσέγγιση, Εκδόσεις Κλειδάριθμος, 2021. Τα υπόλοιπα τεστ έχουν προταθεί από τους επιστήμονες Wozniak, Goertzel, Nillson κ.λπ.

καφέ'', το ''τεστ του μαθητή-ρομπότ'', το ''τεστ του εργαζομένου'' και το ''τεστ της συναρμολόγησης''. Τέλος, θα αναφερθούν ορισμένες **ικανότητες- δεξιότητες** που πρέπει να διαθέτει μια **νοήμων- ''έξυπνη'' μηχανή** προκειμένου να αντεπεξέλθει με επιτυχία στις δοκιμασίες που προαναφέρθηκαν. Αυτές είναι κατά πρώτον, η επεξεργασία της φυσικής γλώσσας, δεύτερον η αναπαράσταση και αποθήκευση της γνώσης , τρίτον η αυτοματοποιημένη συλλογιστική, τέταρτον, η μηχανική μάθηση –για την οποία έγινε εκτενής αναφορά ανωτέρω-, η μηχανική όραση και η μηχανική κίνηση.
Στο σημείο αυτό θα εκτεθεί η ενότητα που αφορά στους αλγορίθμους χάριν στον ιδιαίτερα σημαντικό ρόλο που διαδραματίζουν στα συστήματα Τεχνητής Νοημοσύνης.

1.2 Αλγόριθμοι

Σύμφωνα με τον **Άλβιν Τόφλερ,** διάσημο Αμερικανό συγγραφέα **''Οι αναλφάβητοι του 21ου αιώνα δε θα είναι εκείνοι που δεν ξέρουν γραφή και ανάγνωση, αλλά εκείνοι που δεν μπορούν να μάθουν, να ξεμάθουν και να ξαναμάθουν''.** Τονίζει με αυτό τον τρόπο τη σημασία του να προσαρμόζεται κανείς στις ανάγκες και στους ταχείς ρυθμούς εξέλιξης, να είναι τεχνολογικά ευέλικτος. Η μάθηση αποτελεί θεμελιώδη ιδιότητα της νοήμονος συμπεριφοράς του ανθρώπου[26]. Λόγω του ότι στόχο αποτελεί η προσπάθεια ανακάλυψης του βαθύτερου τρόπου λειτουργίας των αλγορίθμων, θεωρείται ορθό αυτό να πραγματοποιηθεί συγκριτικά με τις συνάψεις που λαμβάνουν χώρα στον ανθρώπινο εγκέφαλο. Όπως επισημαίνεται[27], η ακατάπαυστη ερευνητική δραστηριότητα της γνωστικής ψυχολογίας, αλλά και των κοινωνικών και ανθρωπιστικών επιστημών δεν έχει αποκρυπτογραφήσει σε απόλυτο βαθμό τη μαθησιακή διαδικασία. Δίδεται ως παράδειγμα αυτό ενός νεογέννητου μωρού με άπειρους νευρώνες οι οποίοι είναι υπεύθυνοι για τη δημιουργία συνάψεων στον εγκέφαλο αφού δοθούν τα κατάλληλα ερεθίσματα. Το ένστικτο είναι αυτό που ωθεί τα εγκεφαλικά κύτταρα να χρησιμοποιηθούν ορθώς, δίχως να έχει προηγηθεί εκπαίδευση μέσω ειδικού, παιδαγωγού ή κάποιας άλλης μορφής εκπαιδευτικού συστήματος. Αντιστοίχως, **στην επιστήμη των υπολογιστών, η οποία αναζητά την εύρεση αλγορίθμου που να μπορεί να συγκριθεί με τις νοητικές ικανότητες του ανθρώπινου εγκεφάλου,** ίσως να μην είναι εν τέλει πρωτευούσης σημασίας η ακριβής προσομοίωση **αλλά η κατεύθυνση της έρευνας προς ένα αυτόνομο μονοπάτι μηχανικής νοημοσύνης που θα διαφοροποιείται από τα πρότερα**.
Βάσει της προεκτεθείσας λογικής, θα αναφερθούν ορισμένα στοιχεία της ταυτότητας και της ιστορικής πορείας των αλγορίθμων, αλλά και του προγραμματισμού και της εκπαίδευσής τους**.**

[26] Σακκά Δ., Παιδαγωγική Ψυχολογία, Αθήνα, 1977, σελ. 404 κ.ε. και Κονιδιτσιώτου Β., Η Νεωτέρα Παιδαγωγική, Αθήνα, 1978, σελ.244
[27] Κανέλλος, 2020, σελ.49

1.2.1 Εννοιολογική προσέγγιση αλγορίθμων και σύντομη μνεία στην ιστορική πορεία τους

Επιχειρώντας τον ορισμό της έννοιας[28], **'' αλγόριθμος'' είναι ένα σύστημα σαφών κανόνων ή εντολών που δίδονται σε ένα πληροφοριακό σύστημα ή άλλη υπολογιστική μηχανή, με σκοπό αυτή να επιτελέσει μια ορισμένη σειρά επιμέρους ενεργειών,** οι οποίες είναι **αυστηρά καθορισμένες** και πρέπει να **εκτελεστούν σε πεπερασμένο χρόνο**.[29] Αξίζει να σημειωθεί ότι για να παραχθεί ένας αλγόριθμος είναι απαραίτητη η συνεργασία δύο ατόμων, του ''δημιουργού'' που αναλαμβάνει το σχεδιασμό μιας σειράς βημάτων και του ''εκτελεστή'' που βρίσκει τη λύση στο εκάστοτε πρόβλημα, καθώς μετρά τις αποστάσεις και καθορίζει τις κατάλληλες κινήσεις.[30]

Όσον αφορά στην ιστορική πορεία των αλγορίθμων, η ύπαρξή τους εκκινεί ήδη από την Εποχή του Λίθου, δηλαδή δεν προέκυψαν λόγω της ανάπτυξης της υπολογιστικής, όπως ενδεχομένως υπήρχε η εντύπωση. Η ιστορία τους είναι μακρά, ορισμένοι δε εξ αυτών έχουν ηλικία αιώνων. **Η ελληνική αρχαιότητα προσφέρει δύο χαρακτηριστικά παραδείγματα,** πρώτον **τον Αλγόριθμο του Ευκλείδη**[31] σχετικά με την εύρεση του μέγιστου κοινού διαιρέτη δύο αριθμών και δεύτερον, **το Κόσκινο του Ερατοσθένη**[32]**,** έναν πίνακα που λειτουργεί ως εργαλείο εύρεσης όλων των πρώτων αριθμών μέχρι ένα συγκεκριμένο ακέραιο. **Μέσω της απλής αυτής μεθόδου του Ερατοσθένη μπορούμε να**

---

[28] https://el.wikipedia.org/wiki/%CE%91%CE%BB%CE%B3%CF%8C%CF%81%CE%B9%CE%B8%CE%BC%CE%BF%CF%82 Η προέλευση του όρου ''αλγόριθμος'' εντοπίζεται στη λατινική λέξη Algorithmi (Αλγκορίτμι), η οποία μεταφέρθηκε στην ισπανική (guarismo) και στην πορτογαλική γλώσσα (algarismo), λέξεις οι οποίες σημαίνουν ψηφίο. Τη συναντάμε σε μία διατριβή του Πέρση μαθηματικού, αστρονόμου και λόγιου Μωχάμεντ ιμπν Μουζά αλ_Χουαρίζμι (780-846 μ. Χ.), από τον οίκο της Σοφίας στη Βαγδάτη. Η συγκεκριμένη διατριβή περιείχε συστηματικές τυποποιημένες λύσεις αλγεβρικών προβλημάτων και αποτελεί ίσως την πρώτη πλήρη πραγματεία περί άλγεβρας (al-jabr στα αραβικά)

[29] Στη βιβλιογραφία απαντώνται διάφοροι τρόποι αναπαράστασης ενός αλγορίθμου, όπως με ελεύθερο κείμενο (free text), διαγραμματικές τεχνικές (diagramming techniques) με πιο διαδεδομένο το διάγραμμα ροής (flow chart), φυσική γλώσσα (natural language) κατά βήματα, κωδικοποίηση (coding) δηλαδή με ένα πρόγραμμα γραμμένο είτε σε μία ψευδογλώσσα είτε σε κάποια γλώσσα προγραμματισμού η οποία εφόσον εκτελεστεί θα δώσει τα ίδια αποτελέσματα με τον αλγόριθμο. Οι εντολές αυτές είναι της μορφής ''διάβασε'', αν/τότε, ''διάλεξε'', ''σβήσε'', ''εκτύπωσε'', κ.λπ.

[30] Μ. Καρβούνης (2007) Αλγόριθμοι για υπολογιστές, ένας μικρός οδηγός, διαθέσιμο στο https://cgi.di.uoa.gr/~ip/Odigos.pdf

[31] Ουσιώδες να αναφερθούν ορισμένα στοιχεία για τον Ευκλείδη προκειμένου να του αποδοθεί η δέουσα σημασία στην πορεία ανάπτυξης των αλγορίθμων. Είναι γνωστός ως πατέρας της Γεωμετρίας (300 π.Χ.-270 π.Χ.), Έλληνας μαθηματικός καταγόμενος από την Αλεξάνδρεια της Αιγύπτου, όπου έζησε και δίδαξε περίπου κατά τη διάρκεια της βασιλείας του Πτολεμαίου. Κατέχει μια κρίσιμη θέση στην ιστορία της Λογικής και των Μαθηματικών, αφού είναι ο πρώτος που παράγει ένα αυστηρά δομημένο και συνεκτικό σύστημα προτάσεων (θεωρημάτων και πορισμάτων) βάσει ενός συνόλου ορισμών και πέντε μόνο αρχικές αναπόδεικτες προτάσεις (https://el.wikipedia.org/wiki/%CE%95%CF%85%CE%BA%CE%BB%CE%B5%CE%AF%CE%B4%CE%B7%CF%82)

[32] Ο Ερατοσθένης ο Κυρηναίος (Κυρήνη, 276 π.Χ. – Αλεξάνδρεια 194 π.Χ.) ήταν αρχαίος Έλληνας μαθηματικός, γεωγράφος, αστρονόμος, γεωδαίτης, μουσικός, ποιητής, ιστορικός- φιλόλογος και συγγραφέας. Θεωρείται ως ο πρώτος άνθρωπος στην ιστορία που υπολόγισε το μέγεθος της Γης κατασκευάζοντας ένα σύστημα συντεταγμένων με παράλληλους και μεσημβρινούς καθώς και ένα Χάρτη του κόσμου.

βρούμε όλους τους πρώτους αριθμούς μέχρι το 100 (ή μέχρι οποιονδήποτε δεδομένο αριθμό).

Από υπολογιστική άποψη ένα πρόγραμμα υπολογιστή αποτελεί την τεχνική υλοποίηση, ήτοι τη ''μετάφραση'' του αλγορίθμου σε μια γλώσσα προγραμματισμού[33]. Εξ αυτού κατανοεί κανείς ότι η δημιουργία αλγορίθμων αποτελεί κατά πρώτο λόγο μια μαθηματική και αναλυτική ικανότητα κι όχι δεξιότητα προγραμματισμού. Αυτό εν τοις πράγμασι σημαίνει ότι ακόμη κι ένας επαγγελματίας που δε διαθέτει γνώσεις προγραμματισμού αλλά έχει διεισδύσει ως προς την ουσία του προβλήματος που χρήζει επίλυσης, δύναται να επινοήσει αλγορίθμους. Η διαδικασία που θα ακολουθηθεί έγκειται στο ότι **ο ειδήμων, ο προγραμματιστής, θα μεταφέρει τη θεωρητική προσέγγιση σε μια γλώσσα προγραμματισμού που θα καθοδηγήσει τον υπολογιστή**.

Στη νεότερη εποχή, κατά τη δεκαετία του 1970, οι εφαρμογές έμπειρων συστημάτων (expert systems) λειτουργώντας με τα διαθέσιμα μέσα της εποχής, δηλαδή γλώσσες προγραμματισμού, όπως Prolog , LISP, στηρίζονταν στη συμβολική αναπαράσταση κανόνων και στην υπαγωγή σε αυτούς βιοτικών καταστάσεων προκειμένου να οδηγηθούν σε κάποια διαπίστωση. **Με το πέρας των ετών και τη συνεπαγόμενη εξέλιξη ,** παρατηρείται ότι η **ίδια ευρετική προσέγγιση στηρίζεται σε τεχνικές μηχανικής μάθησης υπό την υποστήριξη νεότερων προγραμματιστικών γλωσσών**. [34] Κι αυτό διότι οι επιστήμονες διαπίστωσαν ότι τα παρελθόντα νοήμονα συστήματα δε θα μπορούσαν να συντελέσουν στην **επίλυση σύνθετων προβλημάτων** κάτι το οποίο αναθέτουν **πλέον στους αλγόριθμους.** Καθήκον των αλγορίθμων[35], δρώντας στη θέση των ανθρώπων αποτελεί η οργάνωση των δεδομένων και η αλληλεπίδραση μαζί τους με αυτόνομο τρόπο. Παρατηρούνται διάφοροι τύποι αλγορίθμων τεχνητής νοημοσύνης[36] οι οποίοι δρουν αναλόγως με τον τύπο της μηχανικής μάθησης (επιβλεπόμενη ή μη, ενισχυτική μάθηση) που καλούνται να υποστηρίξουν και το είδος της εργασίας που πρέπει να επιτελέσουν (βελτιστοποίηση, αναγνώριση προτύπων, ανάλυση πιθανοτήτων).[37]

Η επίδραση των αποτελεσμάτων των αλγοριθμικών διαδικασιών είναι εμφανής και **έντονη στην καθημερινότητα πλείστων όσων ανθρώπων** κι αυτό διαφαίνεται και εμπράκτως μέσω μελετών που φανερώνουν **την εμπιστοσύνη μεγάλου ποσοστού του πληθυσμού στην αυθεντία των αλγορίθμων σε πολλούς τομείς, όπως** η **ιατρική διάγνωση,** η **αναγνώριση εικόνων,** η ανάλυση σύνθετων προβλημάτων**.**[38] **Παρά**, όμως, τη

[33] Κανέλλος, 2020, σελ.111

[34] Νεότερες προγραμματιστικές γλώσσες όπως Javascript, Python, R, Matlab, Weka, Julia, Go,Rust

[35] Είδη αλγορίθμων αποτελούν οι σειριακοί, παράλληλοι, επαναλαμβανόμενοι, γενετικοί κ.άλλοι, ''The 10 best machine learning algorithms for date science beginners'' (2019), διαθέσιμο στο https://www.dataquest.io/blog/top-10-machine-learning-algorithms-for-beginners/

[36] Τύποι συνήθων αλγορίθμων είναι οι ''ταξινόμησης'', ''οπισθοδρόμησης ή αποκλίσεων', ''ομαδοποίησης''κ.άλλοι ''Types of artificial intelligence Algorithms You Should know (A Complete Guide)''(2022) διαθέσιμο στο https://www.upgrad.com/blog/types-of-artificial-intelligence-algorithms/

[37] Κανέλλος, 2020, σελ.53

[38] Logg, J.M., Minson, J.A., & Moore,D.A. (2019). Algorithm Appreciation : People prefer algorithmic to human judgement. Organizational Behavior and Human Decision Processes, 151, 90-103, https://www.sciencedirect.com/science/article/abs/pii/S0749597818303388

βεβαιότητα που γεννάται στους ανθρώπους για την **αρτιότητα του συστήματος** των **αλγορίθμων**, είναι γεγονός, κοινός τόπος ότι **στερούνται ουδετερότητας και αντικειμενικότητας** και αυτό οφείλεται στην ποιότητα του προγραμματισμού και στην εκπαίδευσή τους, από την οποία έχουν άμεση εξάρτηση**.** Αποτέλεσμα αυτού να χαρακτηρίζονται από **μεροληψία και να δρουν αναλόγως αναπαράγοντας στερεότυπα**, τα οποία ενισχύουν διακρίσεις και περιθωριοποίηση εις βάρος ομάδων ανθρώπων με βάση το φύλο, το θρήσκευμα, τη σεξουαλικότητα κ.λπ. Τα στοιχεία αυτά που οφείλονται σε **εσφαλμένες πρακτικές κατά την σχεδίαση του συστήματος** αλλά και σε ανακριβείς μεθόδους κατά τη διαδικασία εκπαίδευσης των αλγορίθμων- η οποία θα αναπτυχθεί στην επόμενη υποενότητα- αποτελεί αδήριτη ανάγκη να τύχουν επιτακτικής πρόβλεψης-ρύθμισης προς αποτροπή παρόμοιων συμπεριφορών χρησιμοποιώντας κατάλληλες τεχνικές τόσο προληπτικά μέσω **μελέτης αντικτύπου** όσο και εκ των υστέρων με **μεθόδους ελέγχου.**

1.2.2 Προγραμματισμός και Εκπαίδευση Αλγορίθμων

Κομβικό παράγοντα για την ορθή λειτουργία του αλγορίθμου αποτελεί ο προγραμματισμός του. Όπως επισημαίνεται[39], στην περίπτωση των νευρωνικών δικτύων, η αλγοριθμική διαδικασία με την οποία επιτυγχάνεται **η μηχανική μάθηση δε στηρίζεται επί του παρόντος σε συλλογισμούς και έννοιες, αλλά η διαδικασία διαφοροποιείται**. Ο υπολογιστής χρησιμοποιώντας πολλά στρώματα νευρώνων, επιχειρεί να κατηγοριοποιήσει τα κοινά χαρακτηριστικά ενός ζητήματος και να εξαγάγει πρότυπα δεδομένων (data patterns), βασισμένα σε λέξεις κειμένου ή στοιχεία εικόνας. **Ως παράδειγμα δίδεται αυτό του συστήματος αναγνώρισης εικόνων,** το οποίο είναι βασισμένο σε φωτεινά εικονοστοιχεία (pixels) και ο υπολογιστικός αλγόριθμος επιχειρεί να αναλύσει τα εξωτερικά στοιχεία ο ρόλος των οποίων είναι καθοριστικός για την κάθε ομάδα. Η διαδικασία που περιγράφηκε αποσκοπεί – όπως υποστηρίζει ο συγγραφέας- στο να εκπαιδευτεί, να ‘’διδαχθεί’’ ο υπολογιστής από ένα σύνολο εικόνων που επεξεργάζεται ώστε να αποθηκεύσει τα στοιχεία στη μνήμη του και κατ’ επέκταση να τα αναγνωρίζει αυτόματα στον πραγματικό, εξωτερικό κόσμο, προβαίνοντας σε σύγκριση των χαρακτηριστικών τους. Αυτό έχει ως αποτέλεσμα να καθίσταται πιο εύκολο για τον **υπολογιστή να αντιληφθεί αν μια εικόνα που επεξεργάζεται, επί παραδείγματι μέσω κάμερας, αντιστοιχεί σε κάποιο ζώο, σε αυτοκίνητο ή σε άνθρωπο**. Στο σημείο αυτό έγκειται, όμως, και **η λεπτή γραμμή**, όπως υποστήριξε ο κ. Δασκαλάκης στη διάλεξή του[40],

---

και J. Logg, ‘’Do People Trust Algorithms More Than Companies Realize?’’ (2018), https://hbr.org/2018/10/do-people-trust-algorithms-more-than-companies-realize

[39] Κανέλλος, 2020, σελ. 55

[40] Διάλεξη του καθηγητή του MIT κ. Κωνσταντίνου Δασκαλάκη στο Ευγενίδειο ίδρυμα στις 14.1.2020 σε https://www.youtube.com/watch?v=NWGUjC8f7jQ

καθώς **αν παρατηρηθεί κάποιο διαφορετικό στοιχείο από αυτά που έχει ήδη αποθηκεύσει**, δηλαδή αν η εικόνα περιστραφεί ενδεικτικά κατά κάποιες μοίρες ή παρουσιαστεί ένα ζώο που όμως έχει διαφορετικά χαρακτηριστικά από αυτά που έχει στη μνήμη του, **ο υπολογιστής κάνει συχνά λάθη διότι εκλαμβάνει ότι πρόκειται για εντελώς άλλο αντικείμενο**! Αυτό αποτελεί **κομβικό σημείο και για την παρούσα εργασία,** καθώς **ο κίνδυνος σφαλμάτων των συστημάτων τεχνητής νοημοσύνης με βιομετρική ταυτοποίηση** που χρησιμοποιείται **για την αναγνώριση προσώπων** αποτελεί **το πιο συχνό ζήτημα αναφορικά με την παραβίαση θεμελιωδών δικαιωμάτων**!

Κρίνεται, λοιπόν, ουσιώδες να δίδεται έμφαση στην **εκπαίδευση των αλγορίθμων**. Κι αυτό διότι **προς εκπλήρωση του σκοπού της μηχανικής μάθησης, απαιτείται να τους χορηγείται μεγάλη ποσότητα και ποιότητα εκπαιδευτικών δεδομένων** (training data), αλλά και απλές υποθέσεις συσχετισμού μεταξύ τους. Κατ' αρχάς, όταν μεταδίδεται πρόσθετη γνώση, αυτή επιφέρει μεταβολές αυξομειώνοντας την ήδη υπάρχουσα, καταχωρημένη γνώση, με αποτέλεσμα την αλλαγή των χαρακτηριστικών της καθώς και την εσωτερική δομή των συστημάτων.[41] Οι **άνθρωποι** σε πρώτο στάδιο πρέπει να **καταχωρίσουν στη μηχανική μνήμη των υπολογιστικών συστημάτων τεχνητής νοημοσύνης πληροφορίες** και εμπειρικά δεδομένα, επί παραδείγματι κείμενα, φωτογραφίες, γραφήματα ή μουσικούς ήχους. Εν συνεχεία, **οι υπολογιστές μαθαίνουν να αναγνωρίζουν, μέσω αισθητήρων και καμερών υψηλής ευκρίνειας**, δεδομένα που ομοιάζουν με αυτά του πραγματικού κόσμου, όπως κείμενα, ήχους, γεωμετρικά σχήματα και περιβάλλοντα δράσης [42], προκειμένου να είναι ικανά να εκτελούν συγκεκριμένα καθήκοντα. Πρέπει, παρόλα αυτά, να τονιστεί ότι και παρά τη μελετημένη ανωτέρω διαδικασία, δεν μπορεί να αποκλειστεί η πιθανότητα λαθών και μάλιστα ακόμη και σε υψηλά επίπεδα αφού στην καθημερινή ζωή, στον πραγματικό κόσμο δεν εκλείπουν και οι αστάθμητοι, απρόβλεπτοι παράγοντες, όπως το να μην αναγνωρίσει ο αλγόριθμος ένα σήμα STOP, το οποίο δεν είναι στην κανονική του μορφή αλλά καλυμμένο με γκράφιτι ή αναποδογυρισμένο με φυσικό αποτέλεσμα το αυτοκίνητο να μη σταματήσει και να προκληθεί κίνδυνος ατυχήματος.

Κατόπιν της εκτενούς ανάλυσης περί του τρόπου λειτουργίας της τεχνητής νοημοσύνης αλλά και του ρόλου που διαδραματίζουν οι αλγόριθμοι σε σχέση με τον αντίκτυπο στον πραγματικό κόσμο, θα συγκεκριμενοποιηθεί η υπόστασή τους μέσω της εννοιολογικής οριοθέτησης και σύντομης ιστορικής αναδρομής των βιομετρικών τεχνολογιών και συστημάτων αλλά και της χρήσης αυτών μέσω της βιντεοεπιτήρησης.

[41] Κανέλλος, 2020, σελ.56

[42] Μαλακασιώτης, Πρ., ''Αναγνώριση μερών του λόγου σε ελληνικά κείμενα με τεχνικές ενεργητικής μάθησης'', Διπλ. εργασία, Π.Μ.Σ. στην Επιστήμη των υπολογιστών Οικονομικού Πανεπιστημίου Αθηνών, 2005

1.3. Εννοιολογική Οριοθέτηση και Σύντομη Ιστορική Αναδρομή των Βιομετρικών Τεχνολογιών και Βιομετρικών Συστημάτων – Χρήση αυτών μέσω Βιντεοεπιτήρησης

Στη σημερινή εποχή η χρήση τεχνολογιών που παρέχουν τη δυνατότητα ηλεκτρονικής ανάγνωσης και επεξεργασίας βιομετρικών δεδομένων εξαπλώνονται με ιλιγγιώδη ταχύτητα σε όλο το φάσμα της καθημερινής ζωής αλλά και του επαγγελματικού/εργασιακού βίου. Παράλληλα, οι τεχνολογίες αυτές είναι πλέον σε σημαντικό βαθμό οικονομικότερες και ταχύτερες σε σχέση με παρελθούσες περιόδους.[43] Επίσης, συντελούν στην επίλυση υποθέσεων τόσο στον ιατροδικαστικό τομέα (έρευνες πατρότητας και συγγένειας) όσο και στον εγκληματολογικό καθώς συνεισφέρουν σε υποθέσεις που αφορούν φόνους, βιασμούς, ληστείες[44]. Παρά τα θετικά στοιχεία τα οποία παρατηρούνται, το **ανακύπτον ζήτημα που προβληματίζει** είναι ότι **τα βιομετρικά δεδομένα μέσω της χρήσης βιομετρικών τεχνολογιών συνδέονται στενά με ορισμένα χαρακτηριστικά ενός ατόμου και κάποια από αυτά μπορούν να χρησιμοποιηθούν για την αποκάλυψη ευαίσθητων δεδομένων.**[45] Βέβαια **η νομική έννοια των βιομετρικών δεδομένων απέχει κατά πολύ από αυτή των βιομετρικών χαρακτηριστικών** που θα αναλυθούν στην εν λόγω ενότητα.

Αναφορικά με την ιστορική τους εξέλιξη, **η χρήση βιομετρικών χαρακτηριστικών** έλαβε χώρα **για πρώτη φορά, στα μέσα του 19ου αιώνα,** όταν **ο** Alphonse Bertillon, επικεφαλής του τμήματος εγκληματολογικής αναγνώρισης της αστυνομίας του Παρισιού χρησιμοποίησε **την ανθρωπομετρία ή τη χρήση των διαφορετικών μεγεθών του σώματος και των αναλογιών για τον εντοπισμό των εγκληματιών**. Η μέθοδος αυτή του Bertillon αντικαταστάθηκε στα τέλη του δεκάτου ενάτου αιώνα από τη χρήση των δακτυλικών αποτυπωμάτων[46], τα οποία απετέλεσαν ένα ανεκτίμητο εργαλείο στο πλαίσιο ποινικών ερευνών. Εν συνεχεία, θεωρείται ορθό να δοθούν ορισμένα στοιχεία σχετικά με τον ορισμό και τη διαμόρφωση των βιομετρικών συστημάτων-χαρακτηριστικών.

Κατ' αρχάς, **τα βιομετρικά χαρακτηριστικά συνιστούν βιολογικές ιδιότητες, πτυχές συμπεριφοράς, φυσιολογικά χαρακτηριστικά, προσωπικά γνωρίσματα ή**

---

[43] Ομάδα Εργασίας του άρθρου 29, Γνώμη 3/2012 για την προστασία των δεδομένων σχετικά με τις εξελίξεις στις βιομετρικές τεχνολογίες, διαθέσιμη σε: https://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_el.pdf

[44] Φιτσιάλος Γεώργιος, Αποδεικτική αξία της γενετικής πληροφορίας, σε Μαρία Κανελλοπούλου-Μπότη/Φερενίκη Παναγοπούλου-Κουτνατζή (επιμ.), Ιατρική ευθύνη και Βιοηθική, Ιατρικές εκδόσεις Πασχαλίδη, Αθήνα 2014, σελ. 421 επ. (423-424)

[45] Παναγοπούλου-Κουτνατζή Φερενίκη, ''Βιομετρικές μέθοδοι και προστασία ιδιωτικότητας: Σκέψεις με αφορμή την απόφαση ΔΕΕ Michael Schwarz κατά κρατιδίου Bochum (C-291/2012), ΔΙΤΕ (π. ΔΙΜΕΕ), τεύχος 4/2013, Οκτώβριος- Νοέμβριος- Δεκέμβριος, σελ. 482

[46] Anil K. Jain/Salil Prabhakar/Arun Ross, An Introduction to Biometric Recognition, σε: 14 IEEE Transactions on Circuits and Systems for Video Technology: Special Issue on Image-and Video-based Biometrics 4, 2004, διαθέσιμο σε: http://biometrics.cse.msu.edu/JainRossPrabhakarCSVT_v15.pdf

επαναλαμβανόμενες κινήσεις. Τα γνωρίσματα όπως και οι κινήσεις είναι και τα δύο μοναδικά για το άτομο και δύνανται να μετρηθούν, ακόμη κι αν τα πρότυπα που χρησιμοποιούνται στην πράξη για την τεχνική μέτρησή τους εμπεριέχουν έναν ορισμένο βαθμό πιθανολόγησης [47]. Πρόκειται, δηλαδή, για μόνιμα γνωρίσματα ενός ανθρώπου, **μέσω των οποίων είναι δυνατή η αναγνώριση ή επαλήθευση της ταυτότητάς του**.[48] Στην ομάδα αυτή ανήκουν και τα γενετικά δεδομένα (DNA), τα σωματικά χαρακτηριστικά (π.χ. δακτυλικά αποτυπώματα, ίριδα ματιού, γεωμετρία προσώπου) ή ακόμα και στοιχεία συμπεριφοράς (π.χ. τρόπος βαδίσματος ή πληκτρολόγησης). Τα στοιχεία αυτά στο βαθμό που αποτελούν τμήμα της φυσιολογίας του ίδιου του ατόμου είναι αναλλοίωτα και ανά πάσα στιγμή διαθέσιμα[49].

Τα βιομετρικά συστήματα αναφέρονται στις αυτοματοποιημένες μεθόδους αναγνώρισης ενός προσώπου μέσω της χρήσης των χαρακτηριστικών της φυσιολογίας ή της συμπεριφοράς[50]. Ως προς τη διαδικασία, επί αυτού του πλαισίου, ένα βιομετρικό δείγμα συγκρίνεται με ένα βιομετρικό «πρότυπο», το οποίο αναφέρεται σε μια έκδοση ενός χαρακτηριστικού που κωδικοποιείται από έναν αλγόριθμο υπολογιστή, έτσι ώστε οι συγκρίσεις των καταχωρισμένων γνωρισμάτων να προσδιορίζουν με επάρκεια το συγκεκριμένο άτομο[51]. Ως προς τις τεχνικές των βιομετρικών χαρακτηριστικών, περιλαμβάνουν ορισμένες που χρησιμοποιούνται για τον εντοπισμό των ατόμων με βάση ένα συγκεκριμένο χαρακτηριστικό ή φυσικά χαρακτηριστικά μοναδικά για το άτομο[52]. **Κάθε ανθρώπινο χαρακτηριστικό** της φυσιολογίας ή/και της συμπεριφοράς μπορεί να χρησιμοποιηθεί ως **βιομετρικό χαρακτηριστικό,** αν πληρούνται οι ακόλουθες

---

[47]Ομάδα Εργασίας του άρθρου 29, Γνώμη 4/2007 σχετικά με την έννοια του όρου «δεδομένα προσωπικού χαρακτήρα», διαθέσιμη σε https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_el.pdf

[48] ''Η διαφορά μεταξύ επαλήθευσης (εξακρίβωσης) και αναγνώρισης της ταυτότητας ενός προσώπου είναι σημαντική. Η επαλήθευση απαντά στο ερώτημα: Είμαι πραγματικά αυτός που ισχυρίζομαι ότι είμαι; Το σύστημα πιστοποιεί την ταυτότητα του προσώπου προβαίνοντας στην επεξεργασία στοιχείων βιομετρίας που αναφέρονται στο πρόσωπο που υποβάλλει το ερώτημα και λαμβάνει μία απάντηση ''ναι/όχι'' (σύγκριση 1:1). Η αναγνώριση της ταυτότητας δίνει απάντηση στο ερώτημα: ποιος είμαι; Το σύστημα αναγνωρίζει το άτομο που υποβάλλει το ερώτημα διαχωρίζοντάς το από άλλα πρόσωπα, των οποίων τα βιομετρικά στοιχεία είναι επίσης αποθηκευμένα. Στην περίπτωση αυτή το σύστημα παίρνει μία απόφαση ''1 από ν'' και απαντά ότι το πρόσωπο που ερωτά είναι το Χ.'' , σύμφωνα με Βασιλοπούλου Ν. Ευαγγελία, ''Βιομετρικά και Γενετικά Δεδομένα'' σε Κοτσαλή Λ., Μενουδάκο Κ., *Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων (GDPR), Νομική Διάσταση και Πρακτική Εφαρμογή*, Αθήνα, Νομική Βιβλιοθήκη, 2018, σελ. 100 και Έγγραφο εργασίας WP80/2003 σχετικά με τα στοιχεία βιομετρίας, Ομάδα Εργασίας του άρθρου 29, διαθέσιμο σε https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_el.pdf

[49]Ιγγλεζάκης Ιωάννης, Ευαίσθητα Προσωπικά Δεδομένα, Εκδόσεις Σάκκουλα, Αθήνα-Θεσσαλονίκη 2004, σελ. 210.

[50]Francis Fungsang, Government Information Collection: U.S. E-Passports: ETA August 2006: Recent Changes Provide Additional Protection for Biometric Information Contained in U.S. Electronic Passports, 2 ISJLP 2006, σελ. 521 επ. (528).

[51] Int'l Civil Aviation Org. (ICAO), Technical Report: Development of a Logical Data Structure- (LDS) for Optional Capacity Expansion Technologies, Revision 1.7, 10-16 (18.5.2004) , διαθέσιμο σε: http:// www.icao.int/mrtd/download/documents/LDS-technical%20 report%202004.pdf

[52] Lisa Jane McGuire, Comment, Banking on Biometrics: Your Bank's New High-Tech Method of Identification May Mean Giving Up You Privacy, 33 AKRON L. REV. 2000, σελ. 441 επ. (444)

προϋποθέσεις : πρώτον, η καθολικότητα, δηλαδή κάθε άτομο πρέπει να έχει το χαρακτηριστικό, δεύτερον, ο διακριτικός χαρακτήρας, δηλαδή κάθε δύο άτομα θα πρέπει να είναι αρκετά διαφορετικά από την άποψη των χαρακτηριστικών, τρίτον η μονιμότητα, δηλαδή το χαρακτηριστικό θα πρέπει να είναι επαρκώς αμετάβλητο για ένα χρονικό διάστημα και τέταρτον, η μετρησιμότητα, δηλαδή το χαρακτηριστικό μπορεί να μετρηθεί ποσοτικά[53].

Ως προς την αξιολόγησή τους, τα βιομετρικά χαρακτηριστικά κρίνονται μέσα από μια ποικιλία παραγόντων, όπως η ακρίβεια της αναγνώρισης, η ταχύτητα, οι απαιτήσεις πόρων, οι επιπτώσεις για τους χρήστες (το σύστημα βιομετρικών στοιχείων θα πρέπει να είναι σχετικά ακίνδυνο), η αποδοχή τους από τον πληθυσμό και η αντίστασή τους σε διάφορες δόλιες μεθόδους εξαγωγής λανθασμένων συμπερασμάτων. Ακολούθως, **βαρύνουσας σημασίας κατηγοριοποίηση των βιομετρικών συστημάτων** αναφορικά με την κρίση περί νομιμότητας λειτουργίας τους είναι η **διάκριση σε αυτά που αφήνουν ίχνη και σε αυτά που δεν αφήνουν και, κατ' επέκταση, σε αυτά που συλλέγονται εν γνώσει του υποκειμένου των δεδομένων και σε αυτά που συλλέγονται εν αγνοία του**[54]. Εν αντιθέσει με το βιομετρικό δεδομένο της ίριδας του ματιού, η συλλογή δακτυλικών αποτυπωμάτων μπορεί να λάβει χώρα εν αγνοία του προσώπου, στο οποίο αυτά αναφέρονται. Όπως υποστηρίζεται[55], οι νέες κάμερες με υψηλή ανάλυση επιτρέπουν επί παραδείγματι με μια μόνο λήψη, την βιομετρική ανάλυση του προσώπου καθενός από τους χιλιάδες θεατές που ακολουθούν μια διαδήλωση ή βρίσκονται σε ένα στάδιο.

Στο πλαίσιο της εννοιολογικής προσέγγισης του όρου, κρίνεται καίριο να αναφερθούν τα συνηθέστερα βιομετρικά χαρακτηριστικά. **Το ευρύτερα χρησιμοποιούμενο βιομετρικό χαρακτηριστικό είναι η εικόνα του προσώπου**.[56] Μεγάλο ποσοστό ανθρώπων παρουσιάζουν μια φωτογραφία ταυτότητάς τους σχεδόν σε καθημερινή βάση για διαφορετικούς λόγους. Μέσω της χρήσης βιομετρικών συστημάτων είναι δυνατό το συγκεκριμένο άτομο να ταιριάζει με την εικόνα του. **Η δυσκολία του προσδιορισμού** εντοπίζεται όταν η εικόνα του προσώπου έχει ληφθεί από μία **παντελώς διαφορετική οπτική γωνία σε σχέση την αποθηκευμένη εικόνα.** Ένας ακόμη προβληματισμός που ανακύπτει είναι το κατά πόσον το πρόσωπο παρέχει επαρκή βάση για την αναγνώριση ενός μεγάλου αριθμού ταυτοτήτων, δεδομένου ότι υφίστανται φυσικές μεταβολές κατά τη διάρκεια της διαδικασίας της γήρανσης ή των τεχνητών μεταβολών που επέρχονται μέσω του μακιγιάζ ή της αλλαγής της κόμμωσης, του χτενίσματος [57].

Το **δεύτερο συχνότερο βιομετρικό χαρακτηριστικό αποτελεί η υπογραφή**. Είναι κοινώς αποδεκτό ότι η υπογραφή ενός ατόμου χαρακτηρίζει με μοναδικό τρόπο το άτομο. Τα βιομετρικά στοιχεία υπογραφής αποτελούν παράδειγμα νέων χρήσεων παραδοσιακών βιομετρικών τεχνολογιών[58]. Ωστόσο, οι υπογραφές συνιστούν έκφανση ανθρώπινης

[53] Anil K. Jain, Salil Prabhakar, & Arun Ross, 2004, σελ. 1-2
[54] Παναγοπούλου-Κουτνατζή Φερενίκη, 2013, σελ. 483
[55] www.gigapan.com
[56] Anil K. Jain, Salil Prabhakar, & Arun Ross, 2004, σελ. 8
[57] Παναγοπούλου-Κουτνατζή Φερενίκη, 2013, σελ. 484
[58] Ομάδα εργασίας του άρθρου 29, Γνώμη 3/2012, σελ.33

συμπεριφοράς και μπορούν να αλλάξουν κατά τη διάρκεια μιας χρονικής περιόδου, καθώς επίσης και να επηρεάζονται από φυσικές και συναισθηματικές αλλαγές στο πρόσωπο. Τα **βιομετρικά συστήματα είναι διόλου σπάνιο να ξεγελαστούν από επαγγελματίες πλαστογράφους παραχαράκτες** οι οποίοι είναι σε θέση να αναπαράγουν υπογραφές δυνάμενες να εξαπατήσουν τα βιομετρικά συστήματα.[59]

Ακολουθούν τα δακτυλικά αποτυπώματα, η αναγνώριση των οποίων συμπεριλαμβάνεται μεταξύ των παλαιότερων, ευρύτερα μελετημένων και εκτενέστερα ανεπτυγμένων βιομετρικών συστημάτων. Η χρήση των συστημάτων αναγνώρισης δακτυλικών αποτυπωμάτων είναι ιδιαίτερα συχνή, λόγω της ακρίβειάς τους αναφορικά με τον εντοπισμό ενός ατόμου. Αλλά και η μέθοδος της **σάρωσης δακτυλικών αποτυπωμάτων** είναι **πολύ εύχρηστη.** Παρόλα αυτά, στα αρνητικά των μεθόδων αναγνώρισης δακτυλικών αποτυπωμάτων συγκαταλέγεται ότι δεν είναι αλάνθαστες. Παρατηρούνται **γενετικοί παράγοντες, όπως η γήρανση**, το περιβάλλον ή επαγγελματικοί λόγοι (π.χ. όσοι εκπονούν χειρωνακτική εργασία συνήθως παρουσιάζουν πολλά κοψίματα και μώλωπες), οι οποίοι **δύνανται να μεταλλάσσουν συνεχώς τα δακτυλικά τους αποτυπώματα.**[60]

Τέταρτη και ειδική κατηγορία τέτοιων μοναδικών χαρακτηριστικών , άμεσα συνυφασμένων με το ανθρώπινο σώμα αποτελούν <u>τα γονίδια ενός ανθρώπου</u> (DNA - δεσοξυριβονουκλεϊκό οξύ), λόγω του αριθμού και του είδους των πληροφοριών που μπορεί να ανακύψουν κατά την ανάλυσή τους.[61] Το DNA βρίσκεται στον πυρήνα των κυττάρων του κάθε ατόμου. Είναι μοναδικό για κάθε άτομο, με την εξαίρεση των πανομοιότυπων διδύμων που μοιράζονται το ίδιο DNA. Παραμένει αναλλοίωτο και συνοδεύει τον άνθρωπο από τη στιγμή της γέννησής του μέχρι το θάνατό του[62]. Αντιθέτως τα δακτυλικά αποτυπώματα αλλοιώνονται ή και εξαφανίζονται λόγω της χειρωνακτικής εργασίας, των επεμβάσεων ή των ασθενειών. **Ένα εκ των σημαντικότερων ζητημάτων που σχετίζονται με τη δημιουργία βάσεων δεδομένων DNA, είναι το γεγονός ότι τα γενετικά δεδομένα που προέρχονται από δείγματα DNA** (γενετικούς τόπους) μπορούν **να αποκαλύψουν** - όχι άμεσα κατά τη φάση της συλλογής - **πληροφορίες σχετικά με την κατάσταση της υγείας, την προδιάθεση για ασθένειες ή την εθνοτική καταγωγή**[63].

---

[59] Anil K. Jain, Salil Prabhakar, & Arun Ross, 2004, σελ. 11

[60] Margaret Betzel, Biometrics: Privacy Year in Review: Recent Changes in the Law of Biometrics, 1 ISJLP 2005, σελ. 517 επ. (521).

[61] Βασιλοπούλου Ν. Ευαγγελία, 2018, σελ.102

[62] Πολλάτου Ιωάννα, Ανάλυση του DNA και νέοι ορίζοντες στη διερεύνηση του εγκλήματος, ΠοινΔικ 2001,1181

[63] Κρίνεται σκόπιμο να παρατεθεί στο σημείο αυτό προς επίρρωση των γραφομένων η ΑΠΔΠΧ, Απόφαση 29/2012, (διαθέσιμη σε: www.dpa.gr), με περαιτέρω ανάλυση των θεμάτων που άπτονται των βιομετρικών δεδομένων ως ειδικής κατηγορίας προσωπικών δεδομένων σε επόμενο κεφάλαιο. Στην εν λόγω απόφαση η Αρχή δέχεται ότι, ανεξαρτήτως του ειδικού χαρακτηρισμού των γενετικών τόπων STRs ως ευαίσθητα ή απλά προσωπικά δεδομένα, η δημοσίευσή τους σε ιστοσελίδα του διαδικτύου – ακόμα κι αν τα δεδομένα παραμείνουν δημοσιευμένα επί μικρό χρονικό διάστημα, ενόψει του ότι είναι δυνατόν να αποθηκευτούν και να τύχουν περαιτέρω επεξεργασίας και αναδημοσίευσης σε μεταγενέστερο χρόνο – ενέχει διακινδύνευση του δικαιώματος στην

Περαιτέρω, αξίζει να σημειωθεί ότι η πρώτη ύλη επί της οποίας γίνονται οι γενετικές αναλύσεις μπορεί εύκολα να διασπείρεται στο περιβάλλον χωρίς καν το άτομο να το αντιλαμβάνεται[64], και να μεταφέρεται στον τόπο του εγκλήματος με σκοπό τον αποπροσανατολισμό των ερευνών ή την ενοχοποίηση ή απενοχοποίηση συγκεκριμένων ατόμων[65]. Με τον τρόπο αυτό, οι γενετικές πληροφορίες μπορεί να οδηγήσουν στην αντιμετώπιση ατόμων ως μη ισοτίμων μελών της κοινωνίας βάσει γενετικών διακρίσεων και γενετικού στιγματισμού.[66]

Εξαιτίας των ανωτέρω, **η δημιουργία βάσεων δεδομένων DNA υποκρύπτει σοβαρό κίνδυνο για την ανθρώπινη αξιοπρέπεια και τα θεμελιώδη δικαιώματα[67].** Σύμφωνα με την κ. Μήτρου [68]**, η εξέταση του DNA συγκεκριμένου προσώπου, με στόχο να διακριβωθεί η συμμετοχή του σε συγκεκριμένες εγκληματικές πράξεις ή και η συγκρότηση ειδικής τράπεζας όπου θα καταχωρίζεται το γενετικό αποτύπωμα προσώπων που έχουν ήδη καταδικαστεί,** μπορεί να γίνουν αποδεκτά υπό την

ιδιωτικότητα του ατόμου και θα έπρεπε για το λόγο αυτό να είχε ληφθεί άδεια της Αρχής, σύμφωνα με τα οριζόμενα στη διάταξη του άρθρου 7 παρ. 2 του Ν 2472/1997. Αλλά λόγω του ότι υπάρχει αμφισβήτηση στην επιστημονική κοινότητα για την αξιοποίηση της πληροφοριακής αξίας των γενετικών τόπων STRs, η Αρχή δεν επέβαλε διοικητική κύρωση για τη μη λήψη άδειας από την Αρχή. Σημειώνεται ότι η για τυπικούς λόγους ανακληθείσα (με την απόφαση 73/2011 της Αρχής) απόφαση 44/2009 της ΑΠΔΠΧ (διαθέσιμες σε: www.dpa.gr) θεωρούσε ότι η γενετική ανάλυση τύπου STR θα πρέπει να θεωρηθεί ως ευαίσθητο προσωπικό δεδομένο που αφορά στην υγεία ή/και τη φυλετική ή εθνική καταγωγή ενός προσώπου, σύμφωνα με τα οριζόμενα στο άρθρο 2 στοιχ. β' του Νόμου 2472/1997. Σύμφωνα με τη Γνωμοδότηση 15/2011 του Εισαγγελέα του Αρείου Πάγου Αθανασίου Κονταξή (διαθέσιμη σε: https://eisap.gr/%CE%B3%CE%BD%CF%89%CE%BC%CE%BF%CE%B4%CF%8C%CF%84%CE%B7%CF%83%CE%B7-15-2011/), τα γενετικά δεδομένα συνιστούν ευαίσθητα προσωπικά δεδομένα.

Σαφής είναι η θέση του Ιωάννη Δ. Ιγγλεζάκη, (ό.π., 2004, σελ. 209), ο οποίος υποστηρίζει ότι τα γενετικά δεδομένα υπάγονται στην κατηγορία των ιατρικών δεδομένων, δηλαδή των ευαίσθητων (ήτοι, πλέον βάσει του Κανονισμού αριθ. 2016/679, των ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα).

[64] Ελισάβετ **Συμεωνίδου-Καστανίδου**, Ανάλυση DNA και ποινική δίκη: το ευρωπαϊκό θεσμικό πλαίσιο, σε: Σύνταγμα, Δημοκρατία και Πολιτειακοί Θεσμοί, Μνήμη Γιώργου Παπαδημητρίου ΙΙ, Εκδόσεις Σάκκουλα, Αθήνα-Θεσσαλονίκη 2013, σελ. 337 επ. (338)

[65] ΑΠΔΠΧ, Γνωμοδότηση 15/2001, σκ. 7, (διαθέσιμη σε: www.dpa.gr), σύμφωνα με την οποία η ταυτότητα των υπόπτων πρέπει να προκύπτει από άλλα στοιχεία, ενδείξεις ή αποδείξεις

[66] Ο ''γενετικός στιγματισμός'' μπορεί άλλωστε να απορρέει ήδη από την ένταξη σε μία πληθυσμιακή ή φυλετική ομάδα ως αποτέλεσμα των γενικών ερευνητικών αποτελεσμάτων που προκύπτουν από γενετικές ή ιατρικές έρευνες στην ομάδα αυτή., σύμφωνα με την κ. **Μήτρου** Λίλιαν, Βιοτράπεζες, Έρευνα και γενετικά δεδομένα, σε Γεώργιο Μανιάτη- Λίλιαν Μήτρου, Η προστασία των γενετικών δεδομένων, Εκδόσεις Σάκκουλα, Αθήνα- Θεσσαλονίκη, 2008, σελ.31.

Ακολούθως παρατίθεται ένα ενδιαφέρον παράδειγμα από την I. Schneider (Biobanken: Korpermaterial und Gendaten im Spannungsfeld von Gemeinwohl und privaer Aneignung στο έργο Nationaler Ethikrat. Biobanken:Chance fur den eissenschaftlichen Fortschritt oder Ausverkauf der ''Ressource Mensch? Tagungsdokumentation, 2002, σ.68 επ.), καθώς είχε πυροδοτήσει έντονη δημόσια συζήτηση αναφορικά με τις συνέπειες του γενετικού φυλετικού στιγματισμού : Το παράδειγμα των Εβραίων που προέρχονται από την Κεντρική Ευρώπη και ζουν στις ΗΠΑ, για τους οποίους ''διαπιστώθηκε'' ότι –συγκριτικά με άλλες πληθυσμιακές ομάδες- έχουν περισσότερες πιθανότητες να εκδηλώσουν την ασθένεια Tay-Sachs καθώς και καρκίνο του εντέρου και των ωοθηκών.

[67] Ομάδα Εργασίας του άρθρου 29, Γνώμη 3/2012, σελ. 31

[68] Μήτρου Λ., 2008, ό.π.. (υποσ.65), σελ.59

προϋπόθεση της ειδικής νομοθετικής ρυθμίσεως που προβλέπει μείζονες ουσιαστικές και διαδικαστικές εγγυήσεις.

Όπως επισημαίνεται[69], **η επεξεργασία του γενετικού υλικού** είναι ήδη αναγνωρισμένη από το **Ευρωπαϊκό Δικαστήριο Δικαιωμάτων του Ανθρώπου (ΕΔΔΑ)**[70] **ως ένας από τους θεμιτούς περιορισμούς της πληροφοριακής αυτοδιάθεσης του ατόμου**. Βάσει της Συνθήκης Prüm, γνωστής και ως "Schengen III", προβλέπεται η διακρατική συνεργασία για την άμεση πρόσβαση των κρατικών αρχών κάθε κράτους – μέλους σε όλες τις εθνικές βάσεις δεδομένων DNA και δακτυλικών αποτυπωμάτων με σκοπό τη διερεύνηση και καταστολή εγκλημάτων**. Ιδιαιτέρως σημαντική η Απόφαση 2008/615/ΔΕΥ του Συμβουλίου** της **Ευρωπαϊκής Ένωσης**[71], «σχετικά με την αναβάθμιση της διασυνοριακής συνεργασίας, ιδίως όσον αφορά την καταπολέμηση της τρομοκρατίας και του διασυνοριακού εγκλήματος», καθώς μέσω αυτής ολοκληρώθηκε η μεταφορά της Συνθήκης του Prüm στο κοινοτικό κεκτημένο και **τέθηκε η νομική βάση για τη δημιουργία του μεγαλύτερου πανευρωπαϊκού δικτύου βάσεων δεδομένων των αστυνομικών αρχών**. Πλέον κάθε κράτος μέλος όχι απλώς δικαιούται, αλλά <u>υποχρεούται</u> να δημιουργήσει αρχεία DNA για τη διεύρυνση αξιόποινων πράξεων, ενώ έχει επιπλέον την υποχρέωση να παρέχει πρόσβαση στα άλλα κράτη μέλη για την αυτοματοποιημένη αναζήτηση γενετικών αποτυπωμάτων. Όπως τονίζει η κ. Παναγοπούλου- Κουτνατζή, η συγκεκριμένη Απόφαση ώθησε την Ελλάδα να αναλάβει διεθνείς δεσμεύσεις περί της υποχρέωσης σύστασης εθνικών αυτοματοποιημένων αρχείων DNA και τη μέσω αυτής διευκόλυνση της διασυνοριακής ανταλλαγής πληροφοριών για την πρόληψη και διερεύνηση αξιόποινων πράξεων. Συγκεκριμένα, με βάση το άρθρο 2 παρ. 1 α΄ της Απόφασης, ανέλαβε να φέρει εις πέρας την υποχρέωση για την εντός τριών ετών σύσταση και τήρηση εθνικής βάσης DNA καθώς και για την ανταλλαγή δεδομένων με άλλες εθνικές βάσεις προς το σκοπό της διερεύνησης αξιόποινων πράξεων. Επιπλέον, βάσει του άρθρου 7 της ιδίας Απόφασης, η Ελλάδα υποχρεούται προς παροχή νομικής συνδρομής μέσω της συλλογής και εξέτασης κυτταρικού υλικού σχετικά με ορισμένο πρόσωπο το οποίο βρίσκεται επί του εδάφους της, υπό την προϋπόθεση ότι δεν υπάρχει ήδη διαθέσιμο το γενετικό του προφίλ στα εθνικά αρχεία.

Αξίζει, τέλος, να σημειωθεί ότι **βασικό προαπαιτούμενο περί του τρόπου λήψης του γενετικού υλικού είναι**[72] **ο ''έντιμος και νόμιμος τρόπος απόκτησης όλων των πληροφοριών''.** Επιπροσθέτως, η κ. Παναγοπούλου- Κουτνατζή συμπληρώνει ότι σύμφωνα με την αρχή 4 της Σύστασης R (92) 1, στις περιπτώσεις που το εθνικό δίκαιο επιτρέπει τη λήψη γενετικού υλικού , δύναται να γίνεται και παρά την αντίθετη βούληση του ατόμου, ελλείπει, όμως, η διευκρίνιση περί του αν είναι θεμιτή η χρήση βίας για τη

[69] Παναγοπούλου- Κουτνατζή Φ., 2013, Σελ. 485

[70] ΕΔΔΑ, Απόφαση S. και Marger κατά Ηνωμένου Βασιλείου (4.12.2008), σκ. 104-105

[71] ΕΕ L 210 της 6.8.2008, σελ. 1, η οποία διατηρήθηκε σε ισχύ και μετά την υιοθέτηση της Απόφασης-Πλαισίου 2008/977/ΔΕΥ «για την προστασία δεδομένων προσωπικού χαρακτήρα που τυγχάνουν επεξεργασίας στο πλαίσιο της αστυνομικής και δικαστικής συνεργασίας σε ποινικές υποθέσεις».

[72] Βάσει Επικαιροποίησης (5-6-2018) της Σύμβασης 108 του Συμβουλίου της Ευρώπης για την προστασία των φυσικών προσώπων από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, άρθρο 5

λήψη γενετικού υλικού ή αν απλώς μπορεί να χρησιμοποιείται γενετικό υλικό που το άτομο διασπείρει στο περιβάλλον[73]. Ο εν λόγω προβληματισμός θεωρείται κομβικός καθώς συνδέεται με την αρχή της αναλογικότητας, αφού όπως αναφέρεται στην παράγραφο 43 της αιτιολογικής έκθεσης της Σύστασης, κάθε κράτος θα αποφασίσει με αυτοτέλεια για το ζήτημα της λήψης.

Πέμπτη κατηγορία βιομετρικών χαρακτηριστικών αποτελεί <u>ο τρόπος πληκτρολόγησης</u>. Θα μπορούσε να είναι ενδεικτικός κατά μεγάλο ποσοστό σχετικά με τον προσδιορισμό της ταυτότητας του ατόμου, καθώς όπως καθίσταται γνωστό[74] κάθε άτομο χτυπάει τα πλήκτρα σε ένα πληκτρολόγιο με μοναδικό τρόπο. Παρόλα αυτά, από τη στιγμή που η συμπεριφορά του ατόμου μεταβάλλεται εν δυνάμει συν τω χρόνω και αυτό είναι ένα χαρακτηριστικό που συνδέεται με τη συμπεριφορά, θα μπορούσε επίσης να διαφοροποιηθεί.

Τελευταία μεγάλη κατηγορία βιομετρικών χαρακτηριστικών είναι η ίριδα του ματιού, δηλαδή η χρωματιστή περιοχή του ματιού. Όπως απορρέει από τη βιβλιογραφία[75], η οπτική της υφή διαμορφώνεται κατά τη διάρκεια της ανάπτυξής μας ως εμβρύων και καθίσταται μόνιμη και αμετάβλητη – εκτός περίπτωσης ενδεχόμενου τραυματισμού- από την ηλικία των δύο ετών. Καθένα από τα μάτια μας έχει τη δική του ίριδα με απολύτως μοναδικούς σχηματισμούς. Η ποικιλότητα και η πολυπλοκότητα αυτών των σχηματισμών συνδυαστικά με την τυχαία κατανομή τους σε ολόκληρο τον ανθρώπινο πληθυσμό συντελούν στη δυνατότητα της ίριδας να αξιοποιηθεί στην ανάπτυξη βιομετρικών συστημάτων. [76] **Η αναγνώριση της ίριδας χρησιμοποιείται ως βιομετρικό χαρακτηριστικό για εφαρμογές ελέγχου πρόσβασης τα τελευταία αρκετά χρόνια**.

---

[73] Σύμφωνα με την κ.Ελισάβετ Συμεωνίδου-Καστανίδου, [ό.π. (υποσ. 63), σελ. 346 επ], στο <u>άρθρο 201 Κώδικα Ποινικής Δικονομίας</u>- Ανάλυση DNA- (<u>κατόπιν πρόσφατης ενημέρωσής του με την ψήφιση του νόμου 4620/2019</u>) ορίζεται ότι όταν υπάρχουν σοβαρές ενδείξεις ότι ένα πρόσωπο έχει τελέσει κακούργημα ή πλημμέλημα που τιμωρείται με ποινή φυλάκισης τουλάχιστον ενός (1) έτους, οι διωκτικές αρχές λαμβάνουν υποχρεωτικά γενετικό υλικό για ανάλυση του DNA προκειμένου να διαπιστωθεί η ταυτότητα του δράστη του εγκλήματος αυτού. Τη λήψη γενετικού υλικού από τον ίδιο τον κατηγορούμενο διατάσσει ο αρμόδιος εισαγγελέας ή ανακριτής και πρέπει να διεξάγεται με απόλυτο σεβασμό στην αξιοπρέπειά του. Η ανάλυση περιορίζεται αποκλειστικά στα δεδομένα που είναι απολύτως αναγκαία για τη διαπίστωση αυτή και διεξάγεται σε κρατικό ή πανεπιστημιακό εργαστήριο. Την ανάλυση του DNA του κατηγορουμένου δικαιούται να ζητήσει και ο ίδιος για την υπεράσπισή του. Ακόμη, σύμφωνα με τη Γνωμοδότηση 15/2011, του Εισαγγελέα του Αρείου Πάγου Αθανασίου Κονταξή, (ό.π. υποσ. 62), η απόσπαση γενετικού υλικού από υπόπτους για ποινικά αδικήματα χωρίς τη συγκατάθεσή τους είναι επιτρεπτή. Επίσης, επισημαίνεται ότι βάσει της ΠορισμΑναφΕισΕφΘεσ 14.10.2013, (διαθέσιμη σε: http:// www.dsanet.gr/Epikairothta/Nomologia/poranafefthes2013.htm) το DNA λαμβάνεται νόμιμα και στο στάδιο της προκαταρκτικής εξέτασης από τις διωκτικές αρχές και χωρίς τη συγκατάθεση του φερομένου ως υπόπτου. (Βλ. και εκτενή κριτική από Αντώνιο Μπρούμα, ''Η Λήψη και Διατήρηση DNA στο Πλαίσιο της Ποινικής Διαδικασίας'', διαθέσιμο σε: http://lawandtech. eu/2011/11/18/dna/)

[74] Anil K. Jain, Salil Prabhakar, & Arun Ross, ό.π. υπ.45 , σελ. 8.

[75] Anil K. Jain, Salil Prabhakar, & Arun Ross, ό.π. υπ.45 , σελ. 10

[76] Νέες δυνατότητες αναγνώρισης εν κινήσει της ίριδας, 21-4-2015, διαθέσιμο στο https://securityreport.gr/archeio-periodikoy/2015/teychos-42/nees-dynatotites-anagnorisis-en-kinisei-tis-iridas/

Στο πλαίσιο της σύνδεσης με επόμενο κεφάλαιο, **καθίσταται πλέον σαφές για μεγάλο τμήμα του πληθυσμού, ότι θα ''παρέδιδαν'' την ιδιωτικότητά τους** μέσω των πλείστων όσων εφαρμογών –άμεσης ή έμμεσης- παρακολούθησης, αν υπήρχε κάποιο ''αντάλλαγμα'', όπως η άνεση και η καλύτερη εξυπηρέτησή τους. Στις ΗΠΑ αλλά και σε άλλες χώρες παρατηρείται προβληματισμός και καχυποψία για την διαπίστωση του εν λόγω φαινομένου. Είναι γεγονός ότι ευνοείται και επιταχύνεται η χρήση τέτοιου είδους συστημάτων βιομετρικών χαρακτηριστικών παγκοσμίως. [77] Παραδείγματα που θίγονται στο προαναφερθέν άρθρο, είναι αυτό της Βραζιλίας όπου αναγνωρίζονται με το συγκεκριμένο τρόπο ψηφοφόροι, αλλά και της Ινδίας όπου λαμβάνει χώρα παρακολούθηση δικαιούχων συνταξιοδοτικών προγραμμάτων.

Καταληκτικά, **ορισμένα ακόμη βιομετρικά χαρακτηριστικά** είναι η **δομή του προσώπου,** η **φωνή**[78]**,** αλλά και η **γεωμετρία των χεριών,** η **μορφή των φλεβών,** όπως και ο **ιδιαίτερος τρόπος βαδίσματος ή ομιλίας.**

Επιλογικά, βάσει της ανωτέρω ανάλυσης συνειδητοποιεί κανείς την **ευκολία** με την οποία μπορεί να **συλλεγούν κατά τη σημερινή εποχή βιομετρικά χαρακτηριστικά, ανεξαρτήτως του αν θα τύχουν επεξεργασίας ή όχι.** Εν τοις πράγμασι, παρατηρείται **αύξηση της βιντεοεπιτήρησης** μέσω της εφαρμογής της ευφυούς ανάλυσης βιντεολήψεων ακριβώς διότι **χρησιμοποιούνται σε πολύ μεγαλύτερο βαθμό οι βιομετρικές τεχνολογίες αναγνώρισης προσώπου και οι αλγόριθμοι τεχνητής νοημοσύνης**. **Πιο συγκεκριμένα,** προσεγγίζοντας τον **ορισμό της έννοιας της βιντεοεπιτήρησης**, σύμφωνα με το **άρθρο 4 της Οδηγίας 1/2011 ΑΠΔΠΧ** [79]**,** ως **''συστήματα βιντεοεπιτήρησης''**, στα οποία περιλαμβάνονται ιδίως τα κλειστά κυκλώματα τηλεόρασης, ορίζονται τα συστήματα που είναι μόνιμα εγκατεστημένα σε ένα χώρο, λειτουργούν συνεχώς ή σε τακτά χρονικά διαστήματα και έχουν τη δυνατότητα λήψης ή/και μετάδοσης σήματος εικόνας ή/και ήχου από το χώρο αυτό προς ένα

[77] Νέες δυνατότητες αναγνώρισης εν κινήσει της ίριδας, ό.π. υπ.75

[78] Ιδιαιτέρως για το βιομετρικό χαρακτηριστικό της φωνής θεωρείται ορθό να επισημανθεί ότι η Interpol εδώ και αρκετά χρόνια χρησιμοποιεί σε συνεργασία με τις εθνικές Αστυνομίες (όπως την Ιταλική τους Carabinieri, τη Μητροπολιτική Αστυνομία του Ηνωμένου Βασιλείου, τη Γερμανική Bundeskriminalamt και την Πορτογαλική Policia Judiciaria) διάφορα ''έξυπνα'' συστήματα αναγνώρισης φωνής υπόπτων και εγκληματιών (πρόκειται για συστήματα Mapping, Evidence, Respect , Smart κ.λπ., διαθέσιμο στο https://www.interpol.int/Who-we-are/Legal-framework/Information-communications-and-technology-ICT-law-projects/Completed-ICT-law-projects). Από το 2018 ολοκληρώθηκε ένα καινοτόμο πρόγραμμα αναγνώρισης φωνής, γνωστό ως SIIP (Speaker Identification Integrated Project, διαθέσιμο στο https://www.interpol.int/Who-we-are/Legal-framework/Information-communications-and-technology-ICT-law-projects/Speaker-Identification-Integrated-Project-SIIP) . Μέσω χρήσης βάσεων δεδομένων με πραγματικές ηχητικές καταγραφές, τέτοια συστήματα επιτρέπουν στις διωκτικές αρχές την ταυτοποίηση άγνωστων ομιλητών, οι οποίοι μιλούν διαφορετικές γλώσσες. Η προέλευση των δεδομένων είναι είτε από τα μέσα κοινωνικής δικτύωσης είτε από νόμιμες υποκλοπές επικοινωνιών με χρήση διάφορων τεχνικών (μικρόφωνα, θερμικές και βιομετρικές κάμερες, πίνακες με οθόνη αφής κ.λπ.). Η ταυτοποίηση πραγματοποιείται μέσω της χρήσης μιας μίξης δεικτών όπως ηλικία, φύλο, γλώσσα και προφορά. (βλ. Κανέλλο, 2020, σελ. 249). Τα ψηφιακά πρότυπα μετρήσεων χαρακτηριστικών των χρηστών φανερώνουν την ψυχική τους κατάσταση ανά πάσα στιγμή. Το βασικό πρόβλημα παρατηρείται κατά την ταυτοποίηση καθώς η τεχνολογία δε διαθέτει ιδιαίτερη ακρίβεια λόγω επίδρασης της χροιάς της φωνής από ποικίλους παράγοντες (εξωτερικός θόρυβος, ασθένειες, επεμβάσεις στο στόμα, πιθανοί τραυματισμοί).

[79] Οδηγία 1/2011 της Αρχής Προστασίας Προσωπικού Χαρακτήρα σχετικά με τη χρήση συστημάτων βιντεοεπιτήρησης για την προστασία προσώπων και αγαθών, 13-04-2011

περιορισμένο αριθμό οθονών προβολής ή/και μηχανημάτων καταγραφής (βλ. και Γνωμοδότηση υπ' αρ. 2/2010 ΑΠΔΠΧ, σκέψη 8). Η μετάδοση της εικόνας δύναται να γίνεται με απευθείας σύνδεση της κάμερας στην οθόνη προβολής ή/και στο μηχάνημα καταγραφής ή μέσω εσωτερικού δικτύου ή μέσω διαδικτύου αλλά για περιορισμένο αριθμό νομιμοποιούμενων προς τούτο αποδεκτών.

Ο βαθμός επέμβασης των νέων τεχνολογιών βιομετρικών συστημάτων στη ζωή του σύγχρονου ανθρώπου είναι συντριπτικός, περιορίζοντας τη δυνατότητά του να διατηρήσει την ανωνυμία του κατά την εκτέλεση των καθημερινών του δραστηριοτήτων. **Οι συνέπειες στην ιδιωτικότητα και τα προσωπικά δεδομένα** είναι **τεράστιες** όπως και οι κίνδυνοι για την καταπάτηση των ανθρωπίνων δικαιωμάτων**.**

Εξ αυτού του λόγου προτού αναλυθούν τα ζητήματα προστασίας προσωπικών δεδομένων που ανακύπτουν σε σχέση με τη βιντεοεπιτήρηση υπό το πρίσμα του Γενικού Κανονισμού για την Προστασία των Δεδομένων (ΓΚΠΔ), θεωρείται **σκόπιμο να προσεγγιστούν ακολούθως οι έννοιες της ιδιωτικότητας – και η εξέλιξή της - όπως και των προσωπικών δεδομένων μέσω της μνείας της συνταγματικής διάστασής τους αλλά και της νομοθετικής πορείας και της ιστορικής διαδρομής τους.**

ΚΕΦΑΛΑΙΟ 2ο

ΠΤΥΧΕΣ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΩΣ ΘΕΜΕΛΙΩΔΟΥΣ ΑΝΘΡΩΠΙΝΟΥ ΔΙΚΑΙΩΜΑΤΟΣ – ΣΥΣΧΕΤΙΣΗ ΜΕ ΑΥΤΟ ΤΗΣ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

2.1. Η εξέλιξη της έννοιας της ιδιωτικότητας βάσει ιστορικοκοινωνικού πλαισίου

Επιχειρώντας επισκόπηση της έννοιας της ιδιωτικότητας τόσο ιστορικά όσο και διαπολιτισμικά, διαπιστώνει κανείς ότι οι **μεγάλες επαναστάσεις του 18ου και 19ου αιώνα,** είχαν ως **απότοκο τη διασφάλιση των προσωπικών δικαιωμάτων** καθώς διαπλάστηκε **μια νέα κοινωνικοπολιτική δομή,** η οποία συνετέλεσε στην **έκφραση της ανάγκης για δικαίωμα στην ιδιωτικότητα**. Η **πρώτη έκφανση του αγαθού των ατομικών δικαιωμάτων και της ιδιωτικότητας,** υπό την οπτική της ελευθερίας και της ισότητας, εντοπίστηκε **για πρώτη φορά στην Αρχαία Ελλάδα** όπου άκμασε το πολίτευμα της δημοκρατίας. Ακόμη, **τα πρώτα δείγματα έκφρασης της ιδιωτικότητας** παρουσιάζονται **στη ''Γένεση''**, καθώς ο Θεός αντιστάθηκε στη δύναμη να εστιάσει το βλέμμα του στους γυμνούς πρωτόπλαστους (Αδάμ, Εύα)[80]. Κατά την ιστορική αναδρομή παρατηρείται ότι **η ιδιωτικότητα συνδέεται με την προστασία της οικίας (οίκος).** Κατά την περίοδο του Μεσαίωνα, εντοπίζεται διαφοροποίηση υπό την έννοια ότι η οικία παρουσιάζεται ως ένας δημόσιος χώρος που μπορεί να υποδεχτεί πέραν της οικογένειας, τους υπηρέτες αλλά και τους φιλοξενούμενους, μην αποτελώντας εν προκειμένω παράδειγμα ιδιωτικότητας[81]. Ακολούθως και **προ της εμφάνισης της Βιομηχανικής επανάστασης, η οικία** λειτουργούσε **ορισμένες φορές ως εργασιακό περιβάλλον**, στο οποίο κάθε οικογένεια περιεργαζόταν τα επαγγελματικά και δημόσια θέματα που την

[80] Μάνεσης, Α. (1978), Συνταγματικά Δικαιώματα, Πανεπιστημιακές Παραδόσεις, Εκδ. Οίκος Α. Σάκκουλα, Θεσ/νικη και **Μήτρου**, Λ. (2001), Προστασία Προσωπικών Δεδομένων: ένα νέο δικαίωμα; Στο έργο Δ. Τσάτσου - Ευ. Βενιζέλου - Ξ. Κοντιάδη (επιμ.), Το νέο Σύνταγμα - Πρακτικά συνεδρίου για το αναθεωρημένο Σύνταγμα του 1975/1986/2001, Αθήνα- Κομοτηνή και **Μήτρου**, Λ. ''Ιδιωτικότητα, προσωπικά δεδομένα και εργασιακές σχέσεις'', *Επιθεώρησις Εργατικού Δικαίου*, 2017, τόμος 76, τεύχος 2, σελ. 140-155

[81] Ariès, Ph. (1973). 'The Family and the City in the Old World and the New', στο V. Tutte & B. Meyerhoff,(επιμ.), Changing Images of the Family, Harmondsworth: Penguin, σελ.54

απασχολούσαν, χωρίς να έχει χρήση ως ιδιωτικός χώρος ενός και μόνου προσώπου[82] . Εξυπηρετούσε κυρίως θέματα εργασίας παρά την απόσυρση και ιδιώτευση των κατοίκων του[83] .

Όπως επισημαίνει ο Habermas[84] , η **πρώτη αλληλεπίδραση μεταξύ ιδιωτικότητας και κατοικίας οφείλεται** στο ότι **άλλαξε η αρχιτεκτονική στις κατοικίες και στις πόλεις,** σε συνδυασμό με την **ραγδαία ενίσχυση της δύναμης** που απέκτησε η **μεσαία αστική τάξη και** την **αύξηση του πληθυσμού στα αστικά κέντρα.** Εν συνεχεία, σύμφωνα με την αναφορά του Stone[85] , το 17ο αιώνα διαπλάθεται τμηματικά στην Αγγλία η έννοια της ιδιωτικότητας ανά κατοικία καθώς πραγματοποιείται ο διαχωρισμός των χώρων στο εσωτερικό περιβάλλον της οικίας σε δημόσιους και ιδιωτικούς[86]. Οι εν λόγω ενέργειες ευνόησαν τη δημιουργία κλίματος ιδιωτικής ζωής στο πλαίσιο της οικίας [87].

Όσον αφορά στα **νομοθετικά συστήματα** αρκετών κρατών**, παρατηρείται σύνδεση οίκου και ιδιωτικότητας. Εκκινώντας από την Ελλάδα στο άρθρο 9 παρ. 1 του Συντάγματος η κατοικία** αναφέρεται **ως άσυλο**. Όπως θίγει ο Solove[88], ο οίκος ως άσυλο προστατεύει τον κάθε άνθρωπο από οποιοδήποτε κίνδυνο. Επί παραδείγματι[89], στην υπόθεση Boyd (1882) εναντίον του κράτους των ΗΠΑ, το Ανώτατο Δικαστήριο δηλώνει εμφατικά τη φράση "ιερότητα του σπιτιού"[90]. Επί του θέματος αξίζει ακόμη να σημειωθεί η ρήση του συνταγματολόγου Ν. Ι. Σαριπόλου[91] : "Η δ' ασυλία του οίκου δεν σημαίνει απλώς το σωματικώς τρόπον τινά απαραβίασιον, αλλά και το σέβας και το ακαταζήτητον περί των όλων των κατά τον ιδιωτικόν βίον συμβαινόντων εντός του ιερού τούτου της οικογένειας ασύλου".

---

[82] Hareven, T.K. (1991). 'The Home and the Family in Historical Perspective', Social Research, 58, σελ. 256

[83] Rybczynski, W. (1987). Home: A short history of an idea. New York: Penguin, σελ. 11

[84] Habermas, J. (1991). The Structural Transformation of the Public Sphere: An Inquiry into the Category of Bourgeois Society. Cambridge: MIT Press

[85] Stone, L. (1991). 'The Public and Private Stately Homes of England, 1500-1990', Social Research, 58, σελ. 237.

[86] Meyer-Spacks, P. (2003). Privacy, Concealing the Eighteenth-Century Self. Chicago & London: The University of Chicago Press

[87]Zeldin, Th. (1996). An Intimate History of Humanity. London: Minerva

[88] Solove, D. (2002). 'Conceptualizing Privacy', California Law Review. 90:1087-1155.

[89] Λούντου Μαρία, ''Η προστασία των προσωπικών δεδομένων των εργαζομένων στο Δημόσιο και Ιδιωτικό τομέα υπό το πρίσμα των πρόσφατων νομοθετικών εξελίξεων (σύκριση-αντιπαραβολή και προοπτικές εξέλιξης)'', Διπλ. εργασία, Π.Μ.Σ. Δημόσια Διοίκηση- Δημόσιο Μάνατζμεντ, Τμ. Διοίκησης Επιχειρήσεων Πανεπιστημίου Δυτικής Αττικής, Αιγάλεω, 2021

[90] Ακριβοπούλου, Χ. (2010), Η ιδιωτικότητα του προσώπου μέσα από τη συνθετική αντίθεση δημόσιου-ιδιωτικού, *Επιστήμη και Κοινωνία (επιθεώρηση πολιτικής και ηθικής θεωρίας)*, τεύχος 26, σελ.10

[91] Σαρίπολος, ΝΤ. (1874). Πραγματεία του Συνταγματικού Δικαίου. Αθήνα: Τυπογραφείο Μιχαήλ Ν. Αγγελίδη, σελ. 192

Κατά τη μελέτη περί του όρου **''ιδιωτικότητα''** διαπιστώνεται **συχνά αντικατάσταση** του όρου **από** αυτόν **της "ιδιωτικής σφαίρας"**[92]. Σύμφωνα με την Γκίλη[93], ο όρος ''ιδιωτική σφαίρα'' συνήθως χρησιμοποιείται σε κράτη όπως η Γαλλία και η Γερμανία, όπου το δικαίωμα στην ιδιωτική ζωή ταυτίστηκε αρχικώς με το δικαίωμα στην προσωπικότητα και ακολούθως, σε δεύτερο χρόνο παρατηρήθηκε μετεξέλιξη του όρου σε μια πιο διευρυμένη έκδοση πέραν της προσωπικότητας, ήτοι την ''ιδιωτική σφαίρα''. Άλλες ερμηνείες του όρου λαμβάνουν χώρα κατά τη δεκαετία του 1960, όπως όταν αποδόθηκε ο ορισμός της ως "η αξίωση των ατόμων και των ιδρυμάτων να αποφασίζουν από μόνοι τους για το πότε, πώς και μέχρι ποιο σημείο οι πληροφορίες που αφορούν αυτούς, θα διαβιβάζονται σε άλλους" [94].

Στην Αγγλία, η αντιστοίχιση του όρου στο νομολογιακό δίκαιο είναι "**privacy**" προερχόμενη από το λατινικό ρήμα ''privo'' (το οποίο σημαίνει ''στερώ''). Έτσι, η έννοια "privatus" βρίσκει σημασιολογικό έρεισμα στην αρχαιοελληνική έννοια του "ιδιώτη", ενώ ο όρος "privacy" συνδέεται με την έννοια της "απομόνωσης" και της "αποχής" από τη δημόσια ζωή, χωρίς όμως παράλληλα να ταυτίζεται με το περιεχόμενο του δικαιώματος στην ιδιωτική ζωή. Παρόλα αυτά, φανερώνει τη βάση επί της οποίας τέθηκε ένα σύνολο δικαιωμάτων του ατόμου στην αυτονομία[95].

Παραθέτοντας **μία ακόμη προσέγγιση βάσει του τι ισχύει στο ελληνικό δίκαιο, η έννοια της ιδιωτικότητας** αφορά "**το χώρο που αυτοπροσδιορίζει κάθε άτομο** με **στόχο** να ασκεί μέσα σε αυτόν τις ατομικές και οικογενειακές δραστηριότητες χωρίς παρεμβάσεις και παρενοχλήσεις τρίτων. Ο χώρος αυτός εκτείνεται μεταξύ του ευρύτερου πλαισίου της κοινωνικής και επαγγελματικής ζωής ενός ατόμου και του απορρήτου του χώρου της αυστηρά προσωπικής ζωής του" [96]. Ακόμη, σύμφωνα με τις διατυπώσεις τριών μελετητών[97] η ιδιωτικότητα αφορά στη δυναμική της συγκρότησης ενός ατόμου ελεύθερου, αυτόνομου, αυτεξούσιου, ανεξάρτητου και αυτοπροσδιοριζόμενου.

Με το πέρας των ετών καθίσταται εμφανές ότι το δικαίωμα στην ιδιωτικότητα δεν παραμένει στάσιμο αλλά εμφανίζει εξελικτική ικανότητα και λόγω της ραγδαίας ανάπτυξης και διάδοσης των Τεχνολογιών Πληροφοριών και Επικοινωνιών και των μεταβολών που συνεπάγονται στην κοινωνία, η προστασία που παρέχεται στο άτομο μεταβάλλεται δυναμικά. Η αναγνώριση στην ιδιωτικότητα αποτελεί μια σύνθετη

---

[92] Δαγτόγλου, Π.Δ. (2005) Συνταγματικό Δίκαιο, Ατομικά Δικαιώματα Α', Εκδ. Α. Σάκκουλα, Αθήνα **και** Δημητρόπουλος, Α. (2005) Συνταγματικό Δίκαιο, Ειδικό μέρος. Παραδόσεις συνταγματικού δικαίου, τόμος ΙΙΙ, τεύχη ΙV επ. ια' έκδοση, Αθήνα.

[93] Ακριβοπούλου, Χ. (2012), Το δικαίωμα στην ιδιωτική ζωή (από τη γένεση, στη σύγχρονη διαμόρφωση και προστασία του), Εκδ. Α. Σάκκουλα, Αθήνα

[94] Solove, D. (2006) A Taxonomy of Privacy, University of Penn Law Review, Vol.154, No 3, pp. 479-564.

[95] ό.π. υποσ. 93

[96] Καρακώστας, Ι. (2012). Το δίκαιο της προσωπικότητας, Νομική Βιβλιοθήκη, Αθήνα, σελ. 35- 55

[97] Μαυριάς, Κ. (1982) Το συνταγματικό δίκαιο του ιδιωτικού βίου, Εκδ. Α. Σάκκουλα, Αθήνα και Βουτσάκη, Β. (2004), Το δικαίωμα στην ιδιωτική ζωή: υποκειμενικές και αντικειμενικές πτυχές, σε Γ. Παπαδημητρίου (επιμ.), Νέες Τεχνολογίες και συνταγματικά δικαιώματα, Αθήνα

συνάντηση μεταξύ δικαίου και κοινωνικής εξέλιξης. Όπως υποστηρίζεται[98], η σύγχρονη προστασία του ανθρώπου προσδιορίζεται από το συνδυασμό της πληροφοριακής έκρηξης και της τεχνολογικής προόδου, όπως και των διακινδυνεύσεων που αυτή εγκυμονεί για την ιδιωτική σφαίρα του προσώπου. Κατά τη διάρκεια αυτών των μεταβολών, η ιδιωτικότητα δε μένει ανεπηρέαστη αλλά υφίσταται μια διάκριση η οποία συνεχώς επαναπροσδιορίζεται. Αποτέλεσμα αυτού, πρακτικές που θεωρούνταν δημόσιες σε ένα συγκεκριμένο ιστορικό και κοινωνικό πλαίσιο, σήμερα θεωρούνται ως ιδιωτικές[99].

Επιπρόσθετα, δεν μπορεί να παραβλεφθεί η – κατά τη θεωρία και τη φιλοσοφία- αρνητική προσέγγιση της ιδιωτικότητας. Η φιλόσοφος Arendt αξιολογεί την ιδιωτικότητα του οίκου ως "στέρηση του λόγου, της έκφρασης και των δικαιωμάτων της πόλεως". Αντίστοιχα, ο Posner προσεγγίζει την ιδιωτικότητα ως "καταφύγιο" για απόκρυψη μη νόμιμων αλλά και αρνητικών δράσεων. Και στις δύο προσεγγίσεις παρουσιάζεται ως κοινό στοιχείο η ξεκάθαρη διάκριση δημόσιου - αρνητικού [100].

Έχοντας διατρέξει το **ιστορικοκοινωνικό πλαίσιο της ιδιωτικότητας**, συνειδητοποιεί κανείς τη **σύνδεση με το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα,** το οποίο είναι θεμελιώδες και η προάσπισή του διαδραματίζει σημαίνοντα ρόλο για την Ευρωπαϊκή Ένωση. Εξ αυτού του λόγου κρίνεται σκόπιμο να αναλυθεί η έννοια των προσωπικών δεδομένων, η συνταγματική διάσταση τόσο αυτών όσο και συνδυαστικά με την ιδιωτικότητα αλλά και η ιστορική διαδρομή και νομοθετική πορεία που διήλθε η έννοια**.**

2.2 Έννοια Δεδομένων Προσωπικού Χαρακτήρα και Συνταγματική διάσταση αυτής σε συνδυασμό με την έννοια της ιδιωτικότητας

Αρχικώς, θα πρέπει να αναφερθεί ότι **ο αναθεωρητικός νομοθέτης του 2001 εισήγαγε το ''δικαίωμα προστασίας προσωπικών δεδομένων'' στην ελληνική συνταγματική τάξη**. Επί της ουσίας τότε έλαβε χώρα η ρητή αποτύπωση, η τυποποίηση ενός δικαιώματος που είχε ήδη διαμορφωθεί από τον κοινό νομοθέτη σε εκπλήρωση των επιταγών του κοινοτικού δικαίου.[101] **Μέχρι εκείνη τη χρονική στιγμή,** όπως εξάγεται από τη νομολογία, **οι συνταγματικές βάσεις** της προστασίας προσωπικών δεδομένων εδράζονταν είτε στο ανωτέρω αναφερθέν **άρθρο 9 παρ. 1 του Συντάγματος** είτε στα **άρθρα 2 παρ.1 Σ και 5 παρ.1 Σ,** είτε στο **συνδυασμό αυτών,** ενώ **συχνά** γινόταν **συνδυασμός με την προστασία**

[98] Solove, 2002, σ. 1141

[99] Λούντου, 2021, σελ. 16

[100] Ακριβοπούλου, 2011, σελ. 1

[101] **Μήτρου** Λίλιαν, «Άρθρο 9Α » σε επιμέλεια των Καθηγητών Φ. Σπυρόπουλου, Ξ. Κοντιάδη, Χ. Ανθόπουλου και Γ. Γεραπετρίτη, Σύνταγμα, κατ' άρθρο Ερμηνεία, Εκδ. Σάκκουλα Αθήνα-Θεσσαλονίκη 2017, σελ. 215

της προσωπικότητας σύμφωνα με το άρθρο 57 ΑΚ.[102] Επιχειρώντας έναν ορισμό των ''δεδομένων'' (data), σύμφωνα με τους μελετητές,[103] είναι στοιχεία ή σύμβολα που περιέχουν κάποια πληροφορία. Στη σύγχρονη εποχή της επικράτησης των τεχνολογιών της πληροφορικής και των επικοινωνιών (ΤΠΕ), ως δεδομένο ορίζεται κάθε πληροφορία που έχει διαμορφωθεί έτσι ώστε να είναι αποτελεσματική η μεταφορά και η επεξεργασία της. Η αξιοποίηση της τεχνολογίας των υπολογιστών και του διαδικτύου οδήγησε στην εποχή των ψηφιακών δεδομένων και στις νέες δυνατότητες επεξεργασίας και ανάλυσής τους (π.χ. Big data analysis).

Πιο συγκεκριμένα**, τα προσωπικά δεδομένα αφορούν τα στοιχεία που συνδέονται με τα ίδια τα άτομα (φυσικά πρόσωπα) και είναι προσωπικού (ατομικού) χαρακτήρα.** Σύμφωνα με μια ευρύτερη ερμηνεία των προσωπικών δεδομένων, ορίζονται ως "αν αφορούν την ταυτότητα, τα χαρακτηριστικά ή τη συμπεριφορά του ατόμου ή αν οι πληροφορίες αυτές χρησιμοποιούνται για να διαπιστωθεί ή επηρεαστεί ο τρόπος που το άτομο αντιμετωπίζεται ή χαρακτηρίζεται" [104] . Ως προς τη φύση του περιεχόμενου της πληροφορίας, αυτή δύναται να προσδιορίζεται βάσει στοιχείων που διακρίνουν ένα άτομο, τα οποία είναι τόσο χαρακτηριστικά της φυσιολογίας του, όπως ύψος, χρώμα ματιών, όσο και υποκειμενικά στοιχεία, ήτοι απόψεις και δηλώσεις. Ακόμη, ο φορέας και το μέσο που περιλαμβάνουν την πληροφορία, μπορεί να είναι αλφαριθμητικοί χαρακτήρες, γραφικά, ακουστικά δεδομένα, σε έντυπη ή ψηφιακή μορφή [105].

Διατρέχοντας ουσιώδη σημεία της φύσης των προσωπικών δεδομένων, αντιλαμβάνεται κανείς τη σημασία της προστασίας τους. **Η συνταγματική θεμελίωση** αυτής συνδεόταν με την **αντίληψη για την ιδιωτικότητα και την έννοια και έκταση της προστασίας των προσωπικών πληροφοριών.** Σύμφωνα με τον Μαυριά[106], η συσχέτιση, αν όχι ταύτιση, με την προστασία του ιδιωτικού βίου (άρθρο 9 παρ. 1 Σ) ήταν καταρχήν εύλογη, διότι ο ιδιωτικός βίος περιλαμβάνει την πληροφοριακή ιδιωτικότητα, χωρίς όμως να εξαντλείται σε αυτήν. Άλλωστε, όπως τονίζεται, η ρητή προστασία του ιδιωτικού βίου αποτελούσε καινοτόμα και υψίστης συμβολικής αξίας επιλογή τόσο σε σχέση με την ελληνική συνταγματική ιστορία όσο και με άλλες εθνικές έννομες τάξεις, όπου – εξαιρουμένων των

---

[102] Ακριβοπούλου Χρ. (2011), Το δικαίωμα στην προστασία των προσωπικών δεδομένων μέσα από το φακό του δικαιώματος στην ιδιωτική ζωή, *ΘΠΔΔ* , τεύχος 7, σελ.679 επ.

[103] Πλατής, Ε. (2018), Προσωπικά Δεδομένα, προστασία GDPR, Εκδ. Παπαδόπουλος, Αθήνα, σελ.14 και **Sivarajah**, U., Kamal, M. M., Irani, Z., & Weerakkody, V. (2017), Critical analysis of big data challenges and analytical methods. Journal of Business Research, 70, 263–286 και **Lytras**, M., Raghavan, V., & Damiani, E. (2017). Cognitive computing and big data analytics research: From metaphors to value space for collective wisdom in human decision making and smart machines. International Journal on Semantic Web and Information Systems, 13(1), 1–10.

[104] Γνώμη 4/2007 σχετικά με την έννοια του όρου «δεδομένα προσωπικού χαρακτήρα», Ομάδα Εργασίας του άρθρου 29, διαθέσιμη σε https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_el.pdf

[105] Πλατής, 2018, σελ.14 και Κουκιάδης, Ι. Δ. (2019), Ο εργαζόμενος ως υποκείμενο προσωπικών δεδομένων, κατά το Γενικό Κανονισμό Προστασίας Δεδομένων, Εκδ. Σάκκουλα, Αθήνα.

[106] Μαυριάς, 1982

κατά τι μεταγενέστερων Συνταγμάτων Ισπανίας και Πορτογαλίας- δεν υπήρχε αντίστοιχη προστασία. Το δικαίωμα της προστασίας των προσωπικών πληροφοριών συνδέεται άμεσα με το δικαίωμα του άρθρου 5 παρ.1 Σ, ήτοι της ελεύθερης ανάπτυξης της προσωπικότητας του καθενός, και περιλαμβάνει την εγγύηση της αυτόνομης απόφασης του ατόμου για τη δημόσια και ιδιωτική παρουσίαση και εικόνα του . Η δυνατότητα αυτή δύναται να εκπληρωθεί μόνο υπό την προϋπόθεση να έχει το άτομο την ελευθερία να αποφασίζει αν και σε ποια έκταση οι πληροφορίες που σχετίζονται με αυτό θα γνωστοποιούνται στο περιβάλλον του.[107] **Το δικαίωμα προστασίας προσωπικών δεδομένων συνδέεται και με ένα ακόμη συνταγματικά κατοχυρωμένο δικαίωμα, αυτό της αξίας του ανθρώπου (άρθρο 2 παρ.1 Σ),** ο σεβασμός και η προστασία του οποίου αποτελούν πρωταρχική υποχρέωση της Πολιτείας**.** Η αξιοπρέπεια που χαρακτηρίζει τον άνθρωπο είναι ακριβώς η ελευθερία του, η οποία νοείται μεταξύ άλλων ως ελευθερία επιλογής μεταξύ πολλών δυνατοτήτων. Εξ αυτού του λόγου αποτελεί βαρύνουσας σημασίας επιταγή το **να μην καταγράφονται προσωπικές πληροφορίες που αποσκοπούν στον έλεγχο και τη χειραγώγηση αποφάσεων, καθώς θίγεται η ίδια η αξία του ανθρώπου** μέσω της άμεσης προσβολής της ελευθερίας του να μη διαδραματίζει κανένα ρόλο ο οποίος να προσδιορίζεται από τους άλλους.[108]

Πέραν του εθνικού πλαισίου, η υιοθέτηση του άρθρου 9Α Σ αντιστοιχούσε ταυτόχρονα στη διεθνή συνταγματική εξέλιξη, όπως αυτή εκφράστηκε σε συνταγματικό επίπεδο σε πολλές χώρες – όπως Ουγγαρία, Σλοβακία, Τσεχία, Κροατία, Λιθουανία, Πολωνία, Σλοβενία- να περιλαμβάνουν την προστασία των προσωπικών δεδομένων στα Συντάγματά τους.[109] Αλλά πέραν της ενσωμάτωσης, στη συνταγματική αναθεώρηση του 2001, της διάκρισης μεταξύ προστασίας ιδιωτικού βίου και προσωπικών δεδομένων, αυτή **αποτυπώθηκε στο Χάρτη Θεμελιωδών Δικαιωμάτων και Ελευθεριών της Ευρωπαϊκής Ένωσης, στον οποίο διαχωρίζεται το ''δικαίωμα κάθε προσώπου σε σεβασμό της ιδιωτικής και οικογενειακής ζωής, της κατοικίας και των επικοινωνιών του'' (άρθρο 7) από την προστασία των δεδομένων προσωπικού χαρακτήρα (άρθρο 8).**

Η ιδιαίτερη αξία του δικαιώματος κατοχυρώνεται μέσω της εισαγωγής της ειδικής συνταγματικής διάταξης, τονίζοντας τη σημασία που έχει η χρήση των προσωπικών δεδομένων για τις προϋποθέσεις προστασίας, ανάπτυξης και αυτόνομης δράσης ενός προσώπου μέσα σε μία κοινωνία, η οποία χαρακτηρίζεται για τη ραγδαία τεχνολογική της ανάπτυξη.[110] Όπως παρατηρούν οι μελετητές[111], πέραν του συμβολικού χαρακτήρα της εν λόγω ρύθμισης, μέσω της καταγραφής της αντίδρασης της συνταγματικής έννομης τάξης στο τεχνο-κοινωνικό περιβάλλον που συνεχώς μεταβάλλεται, δημιουργήθηκε από τον

[107] Μήτρου, Λ. (2001), σελ. 216 (ό.π. υποσ. 80)

[108] Haberle P., Έννοια και περιεχόμενο της ανθρώπινης αξιοπρέπειας κατά το γερμανικό και το ελληνικό Σύνταγμα

[109] Σωτηρόπουλος Α. Βασίλης., *Η συνταγματική προστασία των προσωπικών δεδομένων*, Αθήνα, Εκδ. Σάκκουλα, 2006

[110] Μήτρου Λ., Άρθρο 9Α (Βλ. υποσ.100), 2017, σελ. 217

[111] Κοντιάδης Ο νέος συνταγματισμός και τα θεμελιώδη δικαιώματα μετά την Αναθεώρηση του 2001, Εκδ. Αντ. Ν. Σάκκουλας, Αθήνα 2002, σελ. 196 και Βενιζέλος Ευάγγελος, Το αναθεωρητικό κεκτημένο, Εκδ. Αντ. Ν. Σάκκουλας, Αθήνα 2002, σελ. 159

αναθεωρητικό νομοθέτη μια βάση υποδοχής και ρύθμισης του φαινομένου της Κοινωνίας της Πληροφορίας.

Η νομοθετική οριοθέτηση των προσωπικών δεδομένων στον νόμο 2472/1997 ''για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα'' **είχε προηγηθεί της συνταγματικής διάταξης και συνέκλινε** με την απόδοση της έννοιας των προσωπικών δεδομένων κατά τον τρόπο που την είχε αποτυπώσει ο κοινοτικός νομοθέτης στην **Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία του ατόμου έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία δεδομένων.** Θεωρείται καίριο εν προκειμένω να αναφερθεί, ότι η προστατευτική εμβέλεια της συνταγματικής διάταξης καλύπτει κάθε δεδομένο και δε συναρτά την προστασία που προσφέρει το Σύνταγμα με την αναζήτηση του περιεχομένου του ιδιωτικού βίου και τη νύξη σχετικά με τα όρια της στενής ή της απόρρητης ιδιωτικής σφαίρας. [112]

Η επεξεργασία δεδομένων περιλαμβάνει τη συλλογή και χειρισμό των δεδομένων με σκοπό την εξαγωγή χρήσιμων πληροφοριών, χωρίς να είναι υποχρεωτικό να πραγματοποιηθούν και οι δύο. Μπορεί να υλοποιηθεί με παραδοσιακό (manual) ή ψηφιακό τρόπο (υπολογιστής, διαδίκτυο). Είναι μια αξιολογικά ουδέτερη διεργασία, όπου χωρίς αυτή δεν μπορεί να υπάρξει οργανωμένη λειτουργία των επιχειρήσεων και του κράτους. Από την άλλη, αποτελεί τη βάση κρίσιμων λειτουργιών έρευνας και διαχείρισης επιχειρήσεων και οργανισμών προς όφελος της κοινωνίας. Η διαδικασία επεξεργασίας περιλαμβάνει τα εξής στάδια[113]: 1.επαλήθευση,2.τακτοποίηση με κάποια σειρά, 3.ταξινόμηση, 4.περίληψη, 5.αναφορά, 6.ανάλυση και ερμηνεία.

Συνοψίζοντας, **η εκάστοτε πολιτική προστασίας προσωπικών δεδομένων** πρέπει να προσδιορίζει με σαφήνεια το **σκοπό επεξεργασίας** τους, αλλά και τον τρόπο που αυτή λαμβάνει χώρα ώστε να προσφέρει στα άτομα ως καταναλωτές, πολίτες, πελάτες, εργαζόμενους κ.ά., τη γνώση περί της δυνατότητας να διαθέτουν εκείνα τα μέσα για να ασκήσουν το δικαίωμα στην ιδιωτικότητα και στην προστασία της. Επίσης, να ενημερώνονται περί του τι μέσα διατίθενται σχετικά με την προστασία των ευαίσθητων (λεγόμενων ''ειδικών κατηγοριών'') προσωπικών τους δεδομένων από ενδεχόμενη κατάχρηση οποιουδήποτε είδους και έκτασης. Για να συμβούν όλα τα παραπάνω **θα πρέπει να αναπτυχθεί ειδική νομοθεσία που να ρυθμίζει και να ελέγχει όλη τη διαδικασία επεξεργασίας των προσωπικών δεδομένων** από φυσικά ή τεχνολογικά μέσα διαχείρισης και ανάλυσης, που μπορεί να πραγματοποιούν κυβερνήσεις, επιχειρήσεις ή οργανισμοί[114] . Κατόπιν της προσέγγισης των εννοιών των προσωπικών δεδομένων και της ιδιωτικότητας, θα ακολουθήσει η ανάπτυξη της νομοθετικής πορείας εκ παραλλήλου με την ιστορική διαδρομή των εννοιών.

[112] Μήτρου Λ., (Βλ. υποσ.110)

[113] Πλατής, 2018, σ.17

[114] Κυριαζόγλου, Ι. (2019), Προστασία Προσωπικών Δεδομένων, Εκδόσεις Φυλάτος, σελ.17

2.3.Νομοθετική πορεία και Ιστορική διαδρομή

Η ιστορική πορεία του δικαίου περί προστασίας των προσωπικών δεδομένων ξεκίνησε να διαγράφεται από τα τέλη του 19ου αιώνα, ήτοι διαρκεί περισσότερο από έναν αιώνα**. Το 1890,** τέθηκε για **πρώτη φορά η ανάγκη προστασίας της ιδιωτικότητας του ατόμου**, ως ενός νέου ατομικού δικαιώματος, όταν δύο διακεκριμένοι Αμερικανοί νομικοί (Warren, Brandeis) δημοσίευσαν ένα άρθρο με τίτλο "**The Right to Privacy"[115],** το οποίο αποτέλεσε τομή στην ιστορία της Αμερικανικής νομικής επιστήμης. Ειδικότερα, το εν λόγω άρθρο αξιολογείται ως κομβικό καθώς έθεσε την **πρώτη οριοθέτηση της "ιδιωτικής σφαίρας" ως βασικού στοιχείου της ατομικής ελευθερίας στην σύγχρονη εποχή, αναλογικά με τις εξελίξεις που λάμβαναν χώρα την τότε εποχή**- όπου συντελέστηκε η κορύφωση της 2ης Βιομηχανικής Επανάστασης- και της συνεχώς αυξανόμενης επιρροής του κράτους, των μέσων μαζικής ενημέρωσης, των επιχειρήσεων κ.α. Λόγω της έλλειψης που παρουσίασε η τότε κρατούσα νομοθεσία ως προς την επαρκή προστασία του πολίτη από "...τη διαρκώς αναπτυσσόμενη διείσδυση του Τύπου, των φωτογράφων, της επιχείρησης ή οποιασδήποτε μορφής ιδιοκτήτη κάθε είδους σύγχρονης συσκευής που δύναται να καταγράφει και να αναπαραγάγει περιεχόμενο εικόνας και ήχου...", η άποψη που διατύπωσαν ήταν η **ανάγκη για δημιουργία ενός νέου δικαίου που να ανταποκρίνεται στις τεχνολογικές εξελίξεις.** Δηλαδή εστιάζει στις νέες τεχνολογικές εφευρέσεις και διοικητικές πρακτικές και στην υποχρέωση να τεθούν σαφή όρια μεταξύ δημόσιου και ιδιωτικού βίου[116] .

Μετά το Β΄ Παγκόσμιο πόλεμο τα περισσότερα κράτη, κατά κύριο λόγο ευρωπαϊκά, θέλησαν να προστατεύσουν τα προσωπικά δεδομένα των πολιτών τους. Αποτέλεσμα αυτού, να ενεργοποιηθεί το 1948 στον ΟΗΕ, μέσω ψηφοφορίας, η **Οικουμενική Διακήρυξη για τα Ανθρώπινα Δικαιώματα, στο άρθρο 12 της οποίας περιγράφεται ότι "κανείς δεν επιτρέπεται να υποστεί αυθαίρετες επεμβάσεις στην ιδιωτική του ζωή, την οικογένεια, την κατοικία ή την αλληλογραφία του, ούτε προσβολές της τιμής και της υπόληψής του.** Καθένας έχει το δικαίωμα να τον προστατεύουν οι νόμοι από επεμβάσεις και προσβολές, αυτού του είδους."[117] Ακολούθησαν και άλλες σχετικές πρωτοβουλίες από τον ΟΗΕ ως προς αναβαθμισμένη διαφύλαξη της ιδιωτικότητας, και ειδικότερα, αναφορικά με την προστασία των ατομικών δεδομένων, όπως οι "Guidelines for the Regulation of Computerized Personal Data Files" (το 1990) [118].

<u>Το κρίσιμο πρόβλημα στην επεξεργασία των προσωπικών δεδομένων παραμένει διαμέσου των ετών η προστασία τους ως προστασία της ιδιωτικότητας</u>. Τα δύο βασικά

---

[115] Warren, S.D. and Brandeis, L.D. (1890). The Right to Privacy, 5 (4) Harvard Law Review, p. 193

[116] Κουκιάδης, 2019, σ.21-22

[117] Οικουμενική Διακήρυξη για τα Ανθρώπινα Δικαιώματα, 10 Δεκεμβρίου 1948, διαθέσιμη σε https://unric.org/el/%CE%BF%CE%B9%CE%BA%CE%BF%CF%85%CE%BC%CE%B5%CE%BD%CE%B9%CE%BA%CE%B7-%CE%B4%CE%B9%CE%B1%CE%BA%CE%B7%CF%81%CF%85%CE%BE%CE%B7-%CE%B3%CE%B9%CE%B1-%CF%84%CE%B1-%CE%B1%CE%BD%CE%B8%CF%81%CF%89%CF%80%CE%B9-2/

[118] Κουκιάδης, 2019, σ.23

ζητήματα της μεταπολεμικής κοινωνίας του 20ού αιώνα, η γραφειοκρατία και η ανάπτυξη της τεχνολογίας ενέτειναν την ανάγκη της επάρκειας στην προστασία των προσωπικών δεδομένων και συνέδεσαν τις έννοιες των προσωπικών δεδομένων και της ιδιωτικότητας. Η κρατική παρέμβαση μέσω των σύνθετων δομών της σε συνάρτηση με το εκάστοτε κανονιστικό πλαίσιο δημιούργησαν τέτοιες προϋποθέσεις ώστε να είναι δυνατό να τεθεί υπό παρακολούθηση ο πολίτης κατά την καθημερινότητά του, έθεσαν έντονους προβληματισμούς στο κοινωνικό σύνολο και προκάλεσαν κατ' επέκταση ερωτηματικά ως προς τον τρόπο διαχείρισης και δικαιολόγησης από πλευράς του κράτους της επεξεργασίας δεδομένων για σκοπούς οι οποίοι ως επί το πλείστον δε φανερώνονται. Αντίστοιχα η τεχνολογική εξέλιξη με την έλευση των υπολογιστών, των βάσεων δεδομένων, της τεχνητής νοημοσύνης και εν γένει του διαδικτύου, διευκόλυναν την διαδικασία επεξεργασίας, δημιουργώντας θετικές επιδράσεις, αλλά ταυτοχρόνως κατέστη περισσότερο εύκολο το να λάβει χώρα παραβίαση του -εκάστοτε νομοθετικού πλαισίου- ελέγχου λόγω των ασύλληπτα, πλέον, πολλών δυνατοτήτων επεξεργασίας [119].

Αποτέλεσμα των ανωτέρω, η πρόκληση αναταραχής, **κατά τη μεταπολεμική εποχή,** σε αρκετά κράτη λόγω των κοινωνικών πιέσεων και του βαθμού επικινδυνότητας για **υποκλοπή των λεγόμενων ''ευαίσθητων'' προσωπικών δεδομένων από αθέμιτη ή μη νόμιμη επεξεργασία αυτών**. Ως απόρροια της διαμορφωθείσας κατάστασης, κάθε χώρα προσάρμοσε τις μεθόδους αντιμετώπισης/επίλυσης του ζητήματος σύμφωνα με την νομοθετική κουλτούρα της αλλά και σε υπερεθνικό επίπεδο (π.χ. ΕΟΚ-ΕΕ), ανάλογα με τους εκάστοτε συσχετισμούς. Πιο συγκεκριμένα, το 1950 το Συμβούλιο της Ευρώπης υπέγραψε την **Ευρωπαϊκή Σύμβαση των Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ), με έναρξη ισχύος από το 1953.** Η εν λόγω σύμβαση αποτελεί ένα **νομικά δεσμευτικό κείμενο για το Ευρωπαϊκό Δικαστήριο των Δικαιωμάτων του Ανθρώπου[120] , σκοπός** της είναι η προστασία των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών και στο πλαίσιο αυτό προσδιορίζει την επιβολή κυρώσεων λόγω παραβάσεων στις οποίες προβαίνουν τα κράτη.

Εν συνεχεία, η δεκαετία του '70 αποτέλεσε κομβική περίοδο για τη δημιουργία ενός θεσμικού πλαισίου προστασίας των πολιτών από την αθέμιτη επεξεργασία δεδομένων του κράτους ή των επιχειρήσεων. Κατά την εκτίμηση του Συμβουλίου της Ευρώπης οι τεχνολογικές εξελίξεις δεν λαμβάνονταν υπόψη από τις εθνικές νομοθεσίες, εξ αυτού του λόγου το **1968** δημοσίευσε **τη Σύσταση COM (1968) 509** σχετικά με τα προσωπικά δεδομένα και τις επιστημονικές τεχνολογικές εξελίξεις, εστιάζοντας στην προστασία δεδομένων και ιδιαιτέρως στις τράπεζες δεδομένων στο δημόσιο και ιδιωτικό τομέα. Το **πρώτο διεθνούς βεληνεκούς βήμα** πραγματοποιήθηκε **το 1970 στη Γερμανία, όπου στο ομόσπονδο κρατίδιό της, στην Έσση,** θεσπίστηκε **για πρώτη φορά, νομοθεσία αναφορικά με την προστασία των δεδομένων**. Η ενέργεια αυτή αποδόθηκε στην ευαισθητοποίηση που είχε δημιουργηθεί στην Γερμανική έννομη τάξη σχετικά με το Ναζιστικό καθεστώς (1933-1945) που είχε προβεί σε κατάφωρη παραβίαση των προσωπικών δεδομένων των πολιτών. **Ως**

[119] Martin Ev., 2018

[120] Κουκιάδης, 2019, Πλατής, 2018

προς τη θέσπιση αντίστοιχης νομοθεσίας έπονται η Σουηδία (1973) και η Γαλλία (1978), ενώ ακολούθως αρκετά ακόμη ευρωπαϊκά κράτη ενέταξαν με ρητή πρόβλεψη σε συνταγματικό επίπεδο την προστασία δεδομένων (Πορτογαλία, Ισπανία, Αυστρία)[121]**.**

Στα τέλη της δεκαετίας του '70, το Συμβούλιο της Ευρώπης **πρότεινε τη Σύμβαση 108 για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων,** τροποποιώντας το προηγούμενο κείμενό του, υπό τις επιταγές των τότε τεχνολογικών εξελίξεων (πληροφοριακά συστήματα, τράπεζες πληροφοριών κ.α.). Η συγκεκριμένη σύμβαση ήταν **επί μακρόν το βασικό κείμενο αναφορικά με την προστασία προσωπικών δεδομένων στον ευρωπαϊκό χώρο.** Άλλα αξιομνημόνευτα ευρωπαϊκά κείμενα είναι οι Κατευθυντήριες Αρχές για την προστασία της ιδιωτικότητας και τη διασυνοριακή αποστολή είκοσι (20) προσωπικών δικαιωμάτων, που εκδόθηκαν από τον Οργανισμό Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ) το 1980 μην έχοντας δεσμευτική ισχύ αλλά διαμορφώνοντας το πλαίσιο επί των αρχών που πρέπει να διέπουν την επεξεργασία δεδομένων.

Εν συνεχεία, το 1992 υπογράφηκε η Συνθήκη του Μάαστριχτ , η σημαντικότερη και ιστορικότερη συνθήκη της ευρωπαϊκής ηπείρου (γνωστή και ως Συνθήκη για την Ευρωπαϊκή Ένωση) που προσέδωσε πολιτική και κοινωνική διάσταση στην ευρωπαϊκή κανονιστική θεώρηση. Μετά το πέρας αρκετών ετών, υπεγράφη το 2007 και τέθηκε σε ισχύ το 2009 η Συνθήκη της Λισσαβόνας[122], όπου στο άρθρο 16 παρ.1 γίνεται μνεία για πρώτη φορά, σε επίπεδο πρωτογενούς Ευρωπαϊκού Δικαίου, στην ‘’προστασία των προσωπικών δεδομένων’’, με τη φράση ‘’Κάθε πρόσωπο έχει δικαίωμα προστασίας των δεδομένων προσωπικού χαρακτήρα που το αφορούν’’.

Μια **Οδηγία** που αποτελεί **το κείμενο αναφοράς σε ευρωπαϊκό επίπεδο στα θέματα προστασίας των δεδομένων προσωπικού χαρακτήρα** είναι **η 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου** (24η Οκτωβρίου 1995**).** Θεσπίζει ένα κανονιστικό πλαίσιο που έχει ως στόχο την επίτευξη και εδραίωση μιας ισορροπίας μεταξύ ενός υψηλού επιπέδου προστασίας της ιδιωτικής ζωής των προσώπων και της ελεύθερης κυκλοφορίας των δεδομένων προσωπικού χαρακτήρα ανά την Ευρωπαϊκή Ένωση[123].

Ακολούθως **άξιοι μνείας είναι οι νόμοι υπ’ αριθμ. 2472/1997, με αντικείμενο** τη θέσπιση προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα προς προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής, καταργηθείς πλέον, κι εν συνεχεία ο **υπ’ αριθμ. 3471/2006**, ο οποίος τροποποιεί τον προαναφερθέντα και θέτει **ως επιπλέον** των προγενεστέρων **σκοπό και τη διασφάλιση του απορρήτου των επικοινωνιών** στον τομέα των ηλεκτρονικών επικοινωνιών. Αυτή **θεμελιώνεται στην απαγόρευση της ακρόασης, υποκλοπής,**

---

[121] ό.π. υποσ. 119

[122] Συνθήκη Λισαβόνας για την ΕΕ 2012/c326/01 διαθέσιμο στο https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:326:FULL:EL:PDF

[123] Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, διαθέσιμη σε https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A31995L0046

αποθήκευσης ή οποιουδήποτε άλλου είδους παρακολούθησης ή επιτήρησης των ηλεκτρονικών επικοινωνιών και των συναφών δεδομένων κίνησης και θέσης, εκτός αν υπάρχει διαφορετική πρόβλεψη από το νόμο (άρθρο 4, παρ.2, παρεχόμενη προστασία απορρήτου επικοινωνιών). Στην περίπτωση καταγραφής συνδιαλέξεων και συναφών δεδομένων κίνησης, όταν πραγματοποιούνται κατά τη διάρκεια νόμιμης επαγγελματικής πρακτικής με σκοπό την παροχή αποδεικτικών στοιχείων εμπορικής συναλλαγής ή άλλης επικοινωνίας επαγγελματικού χαρακτήρα, αυτή είναι επιτρεπτή υπό την προϋπόθεση ότι και τα δύο μέρη παρέχουν τη συγκατάθεσή τους, κατόπιν προηγούμενης ενημέρωσης αυτών σχετικά με το σκοπό της καταγραφής (άρθρο 4, παρ.3). Ως προς τις ποινικές κυρώσεις, όποιος προβαίνει σε παράβαση των διατάξεων του νόμου τιμωρείται με φυλάκιση (ή κάθειρξη) και χρηματική ποινή.

Ακόμη, ένα **κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ** είναι ο **Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016** για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών **(Γενικός Κανονισμός για την Προστασία Δεδομένων),** ο οποίος καταργεί την οδηγία 95/46/ΕΚ. **Τέθηκε σε εφαρμογή στις 25 Μαΐου 2018.** Ο Κανονισμός είναι γενικής εφαρμογής, υποχρεωτικός και εφαρμόζεται άμεσα σε όλα τα κράτη μέλη, χωρίς να υπάρχει υποχρέωση για την ενσωμάτωσή του στην εθνική νομοθεσία του κάθε κράτους μέλους.

Ωστόσο, για κάποια ειδικότερα ζητήματα, όπως αυτό των εργασιακών σχέσεων, προβλέπεται η δημιουργία ρυθμίσεων από τις εθνικές νομοθεσίες.

Κατά την ίδια ημεροχρονολογία εκδόθηκε η **Οδηγία 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου** 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 και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και ταυτοχρόνως την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου. **Τόσο ο Γενικός Κανονισμός όσο και η Οδηγία ενσωματώθηκαν στην εθνική νομοθεσία με το νόμο 4624/2019 (ΦΕΚ 137/Α/29-8-2019),** σκοπό του οποίου πέραν της ενσωμάτωσης των δύο ως άνω νομοθετικών κειμένων και της λήψης μέτρων εφαρμογής του Γενικού Κανονισμού, αποτελεί και η αντικατάσταση του νομοθετικού πλαισίου που ρυθμίζει τη συγκρότηση και λειτουργία της **Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα** [(ΑΠΔΠΧ-συνταγματικά κατοχυρωμένη ανεξάρτητη δημόσια Αρχή, η οποία έχει ως αποστολή της την **εποπτεία** της εφαρμογής του Γενικού Κανονισμού Προστασίας Δεδομένων, του ν. 4624/2019, του ν. 3471/2006 και άλλων ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και την ενάσκηση των αρμοδιοτήτων που της ανατίθενται κάθε φορά. Δημιουργήθηκε στα πρότυπα της γαλλικής Commission Nationale de l' informatique et des liberteses (CNIL)][124].

Αξιοσημείωτο κείμενο, στο πλαίσιο της Ευρωπαϊκής Ένωσης, είναι και ο <u>Χάρτης Θεμελιωδών Δικαιωμάτων (ΧΘΔ) της ΕΕ</u>. Η Ευρωπαϊκή Ένωση συμβάλλει στη

[124] https://www.dpa.gr/ και https://www.cnil.fr/

διαφύλαξη και ανάπτυξη των κοινών αξιών της αξιοπρέπειας του ανθρώπου, της ελευθερίας, της ισότητας και της αλληλεγγύης, ενώ ταυτόχρονα σέβεται την πολυμορφία των πολιτισμών και των παραδόσεων των λαών της Ευρώπης. Με γνώμονα αυτή την κατεύθυνση, αποτελεί **αδήριτη ανάγκη η ενίσχυση της προστασίας των θεμελιωδών δικαιωμάτων, υπό την οπτική των κοινωνικών αλλαγών** που συντελούνται αλλά και **της εξέλιξης τόσο στον τομέα της επιστήμης όσο και της τεχνολογίας .**[125] Το ρόλο της πρακτικής νομοθετικής αποτύπωσης διαδραματίζει ο Χάρτης επιβεβαιώνοντας τα δικαιώματα που απορρέουν κατά κύριο λόγο από τις κοινές συνταγματικές παραδόσεις και τις διεθνείς υποχρεώσεις των κρατών-μελών - σεβόμενος τις αρμοδιότητες και τα καθήκοντα της Κοινότητας και της Ένωσης όπως και την αρχή της επικουρικότητας.

Στο άρθρο 8 παρ. 2 του ΧΘΔ της ΕΕ επισημαίνεται **η έννοια της προστασίας των προσωπικών δεδομένων και πιο συγκεκριμένα ότι η επεξεργασία τους πρέπει να γίνεται ''νομίμως, για καθορισμένους σκοπούς και με βάση τη συγκατάθεση του ενδιαφερομένου ή για άλλους θεμιτούς λόγους που προβλέπονται από το νόμο''.** Θέτει, λοιπόν, τις προϋποθέσεις – εγγυήσεις που θα πρέπει να τηρούνται. Αναφέρεται, όμως, και στα δικαιώματα του κάθε προσώπου, επισημαίνοντας ότι ''έχει δικαίωμα να έχει πρόσβαση στα συλλεγέντα δεδομένα που το αφορούν και να επιτυγχάνει τη διόρθωσή τους''. Εξίσου σημαντικό δικαίωμα είναι αυτό που διατυπώνεται στο άρθρο 11 του ΧΘΔ, αυτό της ελευθερίας της έκφρασης που περιλαμβάνει την ελευθερία γνώμης και την ελευθερία λήψης ή μετάδοσης πληροφοριών ή ιδεών, χωρίς την ανάμειξη δημοσίων αρχών και αδιακρίτως συνόρων (παρ.1).

Ο **Γενικός Κανονισμός για την Προστασία Δεδομένων** ευρίσκοντας έρεισμα στον Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ συμπληρώνει τις παραδοσιακές αρχές προστασίας της προσωπικότητας, προσθέτοντας νέα στοιχεία που συμβάλλουν στην εξειδίκευση των εν λόγω αρχών και στη διεύρυνση της προστασίας της προσωπικότητας. Ο άνθρωπος καθορίζει τους όρους προσβολής και παροχής αυτεξούσιας προστασίας συντελώντας στη δημιουργία ενός νέου συστήματος δικαίου που διατηρεί την αυτοτέλεια της προστασίας των προσωπικών δεδομένων. Με αυτό τον τρόπο **διευρύνεται το πλαίσιο προστασίας της ανθρώπινης προσωπικότητας συμπεριλαμβανομένης αυτής του υποκειμένου προσωπικών δεδομένων, τίθενται περιορισμοί** και διενεργείται **έλεγχος από τρίτο φορέα** (π.χ. από μια ανεξάρτητη αρχή).[126]

Καταληκτικά, δεν απαγορεύεται απαρέγκλιτα η επεξεργασία βάσει του προστατευτικού πεδίου που ορίζει ο κανονιστικός μηχανισμός προστασίας προσωπικών δεδομένων (GDPR), αλλά το ρυθμιστικό πλαίσιο στο οποίο αυτή υπόκειται αποσκοπεί στην επίτευξη ύπαρξης συμβιβαστικού πνεύματος μεταξύ του δικαιώματος της πληροφόρησης ή πληροφοριακής ελευθερίας και του δικαιώματος του πληροφοριακού αυτοπροσδιορισμού ή πληροφορικής αυτοδιάθεσης, με απώτερο στόχο τη διεύρυνση και ανανέωση της απόδοσης του όρου της προσωπικότητας και της προστασίας του ιδιωτικού βίου.

[125]Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (2000/C 364/01) διαθέσιμο στο https://www.europarl.europa.eu/charter/pdf/text_el.pdf

[126] Κουκιάδης, 2019, σ.36

ΚΕΦΑΛΑΙΟ 3ο

ΖΗΤΗΜΑΤΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΕ ΣΧΕΣΗ ΜΕ ΤΑ ΣΥΣΤΗΜΑΤΑ ΒΙΝΤΕΟΕΠΙΤΗΡΗΣΗΣ, ΣΧΕΔΙΟ ΚΑΝΟΝΙΣΜΟΥ Ε.Ε. ΓΙΑ ΤΗΝ ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ ΚΑΙ ΕΞΕΤΑΣΗ ΠΑΡΑΒΙΑΣΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΜΕΣΩ ΤΕΧΝΟΛΟΓΙΑΣ

3.1. Λειτουργία Συστημάτων Βιντεοεπιτήρησης, Επεξεργασία δεδομένων προσωπικού χαρακτήρα και Ιδιαιτερότητα Βιομετρικών δεδομένων

Κατόπιν της νομοθετικής διέλευσης των εννοιών της ιδιωτικότητας και των προσωπικών δεδομένων, αλλά και της ιστορικής πορείας που διέγραψαν οι εν λόγω έννοιες, θεωρείται καίριο προς την πληρότητα της παρούσας μελέτης να εξεταστούν τα ιδιαιτέρως ουσιώδη ζητήματα προσωπικών δεδομένων που ανακύπτουν βάσει του Γενικού Κανονισμού υπ' αριθμ. 2016/679 για την προστασία των Προσωπικών Δεδομένων (ΓΚΠΔ).

Εν αρχή, στη σημερινή εποχή του υπερκαταναλωτισμού, η εντατική χρήση συσκευών επιδρά αμεσότατα στη συμπεριφορά των πολιτών, καθιστώντας οικεία σε αυτούς την έννοια της βιντεοεπιτήρησης. Η χρήση συστημάτων βιντεοεπιτήρησης – ο ορισμός των οποίων δόθηκε στο πρώτο κεφάλαιο- είναι επιτρεπτή για συγκεκριμένους σκοπούς και η επεξεργασία τους πρέπει να διέπεται από ορισμένους κανόνες και να παρέχονται εγγυήσεις προς διασφάλιση ότι δε θα χρησιμοποιείται κατά τρόπο μη θεμιτό απέναντι στο εκάστοτε υποκείμενο των δεδομένων.

Ως προς <u>το πεδίο εφαρμογής</u> των εν λόγω συστημάτων, καθίσταται σαφές ότι **η αυτοματοποιημένη παρακολούθηση συγκεκριμένου χώρου με οπτικά ή οπτικοακουστικά μέσα διαδραματίζει ιδιαίτερο ρόλο, εξυπηρετώντας <u>διττό σκοπό</u>,** κατά πρώτον την προστασία προσώπων και αγαθών, ο οποίος δύναται να επιδιώκεται από πάσης φύσεως δημόσιους φορείς ή φυσικά ή νομικά πρόσωπα σε χώρους που διαχειρίζονται και κατά δεύτερον, την παροχή υπηρεσιών υγείας, ο οποίος ουσιαστικά αποτελεί ιδιαίτερη περίπτωση προστασίας προσώπων κι εν προκειμένω υπεύθυνοι επεξεργασίας μπορεί να είναι μόνο φυσικά ή νομικά πρόσωπα που δραστηριοποιούνται στο χώρο της υγείας και τους δεσμεύει το επαγγελματικό απόρρητο – π.χ. γιατροί, νοσηλευτικό προσωπικό.[127]

[127] Κατευθυντήριες Γραμμές 3/2019 σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω βιντεοσυσκευών (με τη σημείωση του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων ότι, εφόσον επιτρέπεται βάσει ΓΚΠΔ, ενδέχεται να ισχύουν ειδικές απαιτήσεις στην εθνική νομοθεσία) **και** Οδηγία 1/2011 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα σχετικά με τη χρήση συστημάτων βιντεοεπιτήρησης για την προστασία προσώπων και αγαθών, Αιτιολογική σκέψη 7

Κομβικό στοιχείο ως προς το πλαίσιο εφαρμογής του Γενικού Κανονισμού στην επεξεργασία των δεδομένων αποτελεί το να είναι δυνατή η άμεση ή έμμεση εξακρίβωση της ταυτότητας του ατόμου, επί τη βάσει της εξωτερικής τους εμφάνισης ή άλλων συγκεκριμένων στοιχείων, διότι όταν δε λαμβάνει χώρα σύνδεση με συγκεκριμένο πρόσωπο δεν εφαρμόζεται ο Γενικός Κανονισμός.

Ακόμη**, ο Γενικός Κανονισμός εμπίπτει στο πεδίο εφαρμογής της οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου** 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, συμπεριλαμβανομένης της προστασίας και πρόληψης έναντι κινδύνων που απειλούν τη δημόσια ασφάλεια, όπως και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.

Εν συνεχεία, **Γενική εξαίρεση από την εφαρμογή των διατάξεων προστασίας δεδομένων προσωπικού χαρακτήρα** αποτελεί η περίπτωση επεξεργασίας που διενεργείται από φυσικά πρόσωπα, στο πλαίσιο δραστηριοτήτων **αποκλειστικά προσωπικών ή οικιακών**[128], που μπορεί να περιλαμβάνει και επιγραμμική δραστηριότητα, **σύμφωνα με το άρθρο 2 παρ. 2 στοιχείο γ' του ΓΚΠΔ** και ισχύει σε περιπτώσεις λειτουργίας συστήματος βιντεοεπιτήρησης στο πλαίσιο οικιακής χρήσης[129], **υπό τον όρο** ότι χώροι εξωτερικοί της ιδιοκτησίας, δημόσιοι ή κοινόχρηστοι, δεν περιλαμβάνονται στο πεδίο ελέγχου της κάμερας. Ο περιορισμός της σημαντικής αυτής εξαίρεσης, γίνεται δεκτός κι από το Δικαστήριο της Ευρωπαϊκής Ένωσης. [130] Η **''οικιακή χρήση'' που εμπερικλείεται στην αποκαλούμενη ''εξαίρεση της οικιακής δραστηριότητας'' πρέπει να νοηθεί** κατά την υπό στενή εννοία ερμηνεία της, σύμφωνα με την κρίση του Ευρωπαϊκού Δικαστηρίου, **''ως αφορώσα αποκλειστικά τις δραστηριότητες οι οποίες εντάσσονται στο πλαίσιο της ιδιωτικής ή οικογενειακής ζωής των ιδιωτών,** πράγμα το οποίο προδήλως δεν ισχύει για την περίπτωση της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, η οποία συνίσταται στη δημοσίευσή τους στο Διαδίκτυο με συνέπεια να αποκτά πρόσβαση στα δεδομένα αυτά απροσδιόριστος αριθμός προσώπων''[131]**.**

Επιπλέον, στις Κατευθυντήριες γραμμές 3/2019, το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, θέτει **έναν ακόμη περιορισμό στην εξαίρεση της προσωπικής/οικιακής δραστηριότητας, αυτόν της συχνότητας της επιτήρησης,** που μπορεί να υποδηλώνει την ύπαρξη κάποιου είδους επαγγελματικής δραστηριότητας εκ μέρους του χρήστη του συστήματος, την τυχόν προσωπική του σχέση με το υποκείμενο των δεδομένων και τις πιθανές δυσμενείς επιπτώσεις της επεξεργασίας στο υποκείμενο των δεδομένων. Η συνδρομή ενός εξ αυτών των τριών στοιχείων, δεν υποδηλώνει απαραίτητα ότι δε θα

---

[128] Σκόνδρα Μαγδαληνή, ''Συστήματα Βιντεοεπιτήρησης, αναγνώριση προσώπου και προστασία προσωπικών δεδομένων'', *ΔΙΤΕ (πρώην ΔΙΜΕΕ)*, τεύχος 1/2020, Ιανουάριος-Φεβρουάριος- Μάρτιος, σελ. 46

[129] Περιπτώσεις, όπως η συγκεκριμένη, εξαιρούνται κι από το πεδίο εφαρμογής της Οδηγίας 1/2011, κατά τη ρητή πρόβλεψη του άρθρου 3 παρ, 2 β' αυτής

[130] Υπόθεση C-212/13, František Ryneš v Úřad pro ochranu osobních údajů, 11 December 2014, παρ. 33

[131] Ευρωπαϊκό Δικαστήριο, απόφαση στην υπόθεση C-101/01, υπόθεση Bodil Lindqvist, 6 Νοεμβρίου 2003, σκέψη 47.

πρόκειται για αποκλειστική προσωπική ή οικιακή δραστηριότητα, αλλά θα είναι απαραίτητο να γίνεται **μια συνολική ad hoc αξιολόγηση της συγκεκριμένης επεξεργασίας, προκειμένου να εξαχθεί ασφαλές συμπέρασμα, περί της εφαρμογής ή μη της εξαιρέσεως**. Παράδειγμα τέτοιων επεξεργασιών, μπορεί να είναι η λειτουργία συστήματος βιντεοεπιτήρησης εντός οικίας ή διαμερίσματος, όπου όμως καθημερινά απασχολείται προσωπικό, όπως οικιακή βοηθός, νοσοκόμα για περίθαλψη ασθενούς-ενοίκου της οικίας.[132] Στο σημείο αυτό κρίνεται σκόπιμο να παρατεθεί η **υπ' αριθμόν 10/2022 απόφαση της Αρχής Προστασίας Προσωπικών Δεδομένων (ΑΠΔΠΧ)** προκειμένου να αποσαφηνιστεί το πλαίσιο εφαρμογής ή μη της Γενικής εξαίρεσης από την εφαρμογή των διατάξεων προστασίας δεδομένων προσωπικού χαρακτήρα στο πλαίσιο δραστηριοτήτων αποκλειστικά προσωπικών ή οικιακών. [133]

Πιο συγκεκριμένα, με την εν λόγω απόφαση η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα εξέτασε καταγγελία αναφορικά με εγκατάσταση συστήματος βιντεοεπιτήρησης σε κατοικία. Σύμφωνα με την καταγγελία αυτή, ο καταγγελλόμενος, που διαμένει σε ισόγειο διπλοκατοικίας, έχει εγκαταστήσει κάμερες, τη μία εξ αυτών κάτω από το μπαλκόνι των καταγγελλόντων με τους οποίους είναι συνιδιοκτήτης του εν λόγω ακινήτου, οι οποίες (κάμερες) λαμβάνουν εικόνα και ήχο και συνδέονται με καταγραφικό μηχάνημα. Λαμβάνοντας, λοιπόν, υπόψη η Αρχή το δεδομένο της συνιδιοκτησίας, επισημαίνει στο σκεπτικό της ότι σε ένα σύστημα βιντεοεπιτήρησης το οποίο είναι εγκατεστημένο σε ιδιωτική οικία, **δε θεωρείται αποκλειστικά προσωπική ή οικιακή δραστηριότητα η λήψη και επεξεργασία εικόνας ή και ήχου, όταν το πεδίο ελέγχου της κάμερας περιλαμβάνει μη ιδιωτικούς χώρους** (δημόσιους, κοινόχρηστους ή χώρους που ανήκουν σε τρίτους). Αποτέλεσμα αυτού η συναφής επεξεργασία να εμπίπτει στο πεδίο εφαρμογής της νομοθεσίας για την προστασία των προσωπικών δεδομένων και να εξετάζεται η νομιμότητά της, συνδυαστικά προς την εφαρμογή των αρχών προστασίας δεδομένων προσωπικού χαρακτήρα.

Στις περιπτώσεις επεξεργασίας μέσω τέτοιων συστημάτων βιντεοεπιτήρησης, **η νομική βάση** που εφαρμόζεται είναι, ως επί το πλείστον, το άρθρο 6 παρ. 1 εδαφ. στ' του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων (ΓΚΠΔ). Ακόμη, ως προς την εξέταση της νομιμότητας της επεξεργασίας **βασική προϋπόθεση είναι η τήρηση της αρχής της αναλογικότητας,** η εφαρμογή της οποίας εξειδικεύεται στα άρθρα 6 και 7 της Οδηγίας 1/2011 της Αρχής, αλλά και στο Ειδικό Μέρος αυτής.

Ως προς την εξέταση από πλευράς της Αρχής του ειδικότερου ζητήματος της εγκατάστασης συστήματος βιντεοεπιτήρησης **σε συγκροτήματα κατοικιών**, διευκρινίζει ότι, όπως προβλέπεται στο άρθρο 15 του Ειδικού Μέρους της ανωτέρω Οδηγίας, η εγκατάσταση συστήματος βιντεοεπιτήρησης σε συγκροτήματα κατοικιών για την ασφάλεια κοινόχρηστων χώρων και των προσώπων που κυκλοφορούν σε αυτούς δύναται

[132] ό.π. υποσ 127

[133] Lawspot.gr, "Κάμερες σε κατοικία: Απαγόρευση χρήσης συστήματος βιντεοεπιτήρησης σε κοινόχρηστο χώρο (ΑΠΔΠΧ 10/2022) ", 15-3-2022, διαθέσιμο στο https://www.lawspot.gr/nomika-nea/kameres-se-katoikia-apagoreysi-hrisis-systimatos-vinteoepitirisis-se-koinohristo-horo

να πραγματοποιηθεί **μόνο με απόφαση του οργάνου που είναι υπεύθυνο για τη διαχείριση του συγκροτήματος** (π.χ. της Γενικής Συνέλευσης της πολυκατοικίας) σύμφωνα με τις διατάξεις του οικείου Κανονισμού, και όχι από κάποιον ένοικο μεμονωμένα, και τούτο υπό την προϋπόθεση ύπαρξης σύμφωνης γνώμης των δύο τρίτων (2/3) των ενοίκων της πολυκατοικίας.

Στην υπό εξέταση περίπτωση, σημαντικό να τονισθεί ότι **υπεύθυνος επεξεργασίας** του συστήματος βιντεοεπιτήρησης, δηλαδή αρμόδιος να αποφασίσει για το σκοπό και τον τρόπο χρήσης του συστήματος, είναι **η ένωση προσώπων των συνιδιοκτητών** που λειτουργεί μέσω της Γ.Σ. συνιδιοκτητών του συγκροτήματος και του σχετικού κανονισμού, όπου υφίσταται, **κι όχι μεμονωμένος ιδιοκτήτης**.

Βάσει των δοθέντων στοιχείων, κρίθηκε πως, καθώς οι χώροι είναι κοινόχρηστοι, θα έπρεπε η επιτήρηση, εφόσον υποτεθεί ότι είναι για την προστασία των κοινοχρήστων χώρων, να αποφασιστεί από τους συνιδιοκτήτες. **Λόγω μη ύπαρξης κανονισμού, θα έπρεπε τουλάχιστον, κατ' ανάλογη εφαρμογή, να υφίσταται πλειοψηφία 50%+1 με βάση τα ποσοστά ιδιοκτησίας.**

Ακόμη, αναφορικά με το **σκοπό της προστασίας προσώπων και αγαθών**, στην επίκληση του οποίου προβαίνει ο καταγγελλόμενος, η Αρχή έκρινε ότι αυτός είναι δυνατό να επιτευχθεί με άλλα μέσα (π.χ. φωτισμός, συναγερμός, τοποθέτηση κάμερας μόνο στην είσοδο του διαμερίσματός του και σε εσωτερικούς χώρους). Περαιτέρω, δεδομένου ότι ο επιτηρούμενος χώρος είναι κοινόχρηστος, δεν μπορεί να αποκλειστεί η χρήση του από τους λοιπούς ενοίκους, ιδίως καθώς τμήμα του επιτηρούμενου χώρου περιλαμβάνει την κοινή είσοδο των δύο διαμερισμάτων. Συνεπώς, κρίθηκε ότι λαμβάνει χώρα **<u>υπέρμετρη προσβολή</u> των δικαιωμάτων των προσώπων που διαμένουν στο άλλο διαμέρισμα του κτιρίου**, καθώς ενδέχεται να παρακολουθούνται σε δραστηριότητες στενά συνδεόμενες με την ιδιωτική τους ζωή.

Καίρια επιπλέον η **επισήμανση της Αρχής, ως προς τον υπεύθυνο επεξεργασίας, ως ένοικο διαμερίσματος,** ότι έχει **ευθεία εφαρμογή η γνωμοδότηση 5/2017** διατυπωθείσα από την ίδια. Συνεπώς, ο **καταγγελλόμενος θα μπορούσε να επιτηρεί μόνο ιδιωτικούς του χώρους και μικρό τμήμα της εισόδου του διαμερίσματός του <u>αλλά όχι</u> την κεντρική είσοδο, χωρίς να έχει προηγηθεί συμφωνία με τους λοιπούς ενοίκους.**

Συμπερασματικά **, η Αρχή**, λαμβάνοντας υπόψη τη φύση και το σκοπό της επεξεργασίας, την επί χρόνια υπάρχουσα διαφωνία των δύο πλευρών, τη συγγενική τους σχέση και το γεγονός ότι η επεξεργασία ενδέχεται να έχει συνέπειες για συγκεκριμένα ολιγάριθμα φυσικά πρόσωπα, **επέβαλε ως καταλληλότερο μέτρο αυτό της απαγόρευσης της λειτουργίας συστήματος βιντεοεπιτήρησης,** το οποίο λαμβάνει εικόνα από κοινόχρηστους χώρους.

Η παράθεση και ανάλυση της ως άνω απόφασης της Αρχής αποτελεί το δίαυλο προκειμένου να εξεταστεί το ουσιωδέστατο **ζήτημα της νομιμότητας της επεξεργασίας** προσωπικών δεδομένων μέσω συστημάτων βιντεοεπιτήρησης, καθώς προτού χρησιμοποιηθεί το υλικό πρέπει να καθίσταται σαφής η παράθεση των σκοπών επεξεργασίας, να πληρούνται οι βασικές αρχές που τη διέπουν, να τηρούνται εν τη πράξει

οι υποχρεώσεις του υπευθύνου επεξεργασίας, όπως επίσης και τα δικαιώματα του υποκειμένου των δεδομένων (απαραίτητες προϋποθέσεις).

3.1.1. Νομιμότητα επεξεργασίας μέσω συστημάτων βιντεοεπιτήρησης

3.1.1.1. Βασικές Αρχές επεξεργασίας δεδομένων

Σύμφωνα με το άρθρο 5 ΓΚΠΔ[134], για να είναι νόμιμη η επεξεργασία προσωπικών δεδομένων (απλών και ειδικών κατηγοριών) πρέπει να διέπεται από ορισμένες αρχές :

i)Η αρχή της νομιμότητας, αντικειμενικότητας και διαφάνειας (άρ. 5, παρ.1, στοιχ. α')

Σύμφωνα με τη συγκεκριμένη αρχή, τα δεδομένα πρέπει να υποβάλλονται σε σύννομη και θεμιτή επεξεργασία, με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων. Η διαφάνεια απαιτεί η ενημέρωση του υποκειμένου να είναι συνοπτική, εύκολα προσβάσιμη, κατανοητή, με σαφή και απλή διατύπωση.
Η εν λόγω αρχή διαδραματίζει ιδιαιτέρως σημαίνοντα ρόλο και στην υπό εξέταση θεματική των συστημάτων αναγνώρισης προσώπου, καθώς όταν οι πολίτες, τα υποκείμενα, ευρίσκονται σε οποιοδήποτε δημόσιο χώρο, η συλλογή και επεξεργασία των εικόνων προσώπου λαμβάνει χώρα απουσία διαφάνειας αφού τα υποκείμενα δεν έχουν γνώση περί αυτής. Αποτέλεσμα αυτού να μην τους παρέχεται εξ αρχής η δυνατότητα να ασκήσουν τα δικαιώματά τους. Αντιθέτως, ο διαφανής, κατά τον Γενικό Κανονισμό (αιτιολογική σκέψη 39), τρόπος θα πρέπει να συνίσταται στην επάρκεια των πληροφοριών που παρέχονται σε περίπτωση επεξεργασίας δεδομένων προσωπικού χαρακτήρα (τόσο στην περίπτωση της απευθείας συλλογής από τα ίδια όσο και από τρίτα πρόσωπα). Επιπλέον, ως προς την εξέταση των **περιορισμών του δικαιώματος ενημέρωσης** βάσει του Γενικού Κανονισμού, αυτός λαμβάνει χώρα όταν τα υποκείμενα των δεδομένων διαθέτουν ήδη τις πληροφορίες, είτε η συλλογή γίνεται απευθείας από τα ίδια είτε από άλλες πηγές. Στη δεύτερη περίπτωση (όταν συλλέγονται δεδομένα από άλλες πηγές) τα υποκείμενα των δεδομένων δεν έχουν το δικαίωμα ενημέρωσης, όταν: α) η παροχή των πληροφοριών αποδεικνύεται αδύνατη ή συνεπάγεται δυσανάλογη προσπάθεια για τον υπεύθυνο επεξεργασίας, β) η απόκτηση ή η κοινολόγηση προβλέπεται ρητώς από το δίκαιο της Ένωσης ή του κράτους μέλους, και γ) τα δεδομένα πρέπει να παραμείνουν εμπιστευτικά δυνάμει υποχρέωσης επαγγελματικού απορρήτου που ρυθμίζεται από το δίκαιο της Ένωσης ή κράτους μέλους.

[134] Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων - **ΓΚΠΔ)** διαθέσιμος σε https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679&from=HR

ii) **Αρχή Περιορισμού του σκοπού (άρ.5, παρ.1, στοιχ. β')**

Σύμφωνα με την εν λόγω αρχή του Γενικού Κανονισμού, τα δεδομένα προσωπικού χαρακτήρα συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς· η περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς δεν θεωρείται ασύμβατη με τους αρχικούς σκοπούς σύμφωνα με το άρθρο 89 παράγραφος 1.
Η **έννοια του περιορισμού** έγκειται στο ότι ο **σκοπός** πρέπει να είναι **σαφής** και εξ αρχής **λεπτομερώς καθορισμένος**. Προσδιορισμός του σκοπού κατά τρόπο γενικό και αόριστο δεν είναι σύμφωνος με την αρχή αυτή.[135]

iii) Αρχή Ελαχιστοποίησης των δεδομένων (άρ.5, παρ.1, στοιχ. γ')

Κατά την εν λόγω αρχή, τα δεδομένα προσωπικού χαρακτήρα είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία. Με γνώμονα την αρχή της ελαχιστοποίησης δεδομένων[136], οι υπεύθυνοι επεξεργασίας πρέπει να διασφαλίζουν ότι τα εξαγόμενα από την ψηφιακή εικόνα δεδομένα για τη δημιουργία προτύπου **δε θα είναι υπερβολικά** και θα περιέχουν **μόνο** τις **πληροφορίες που απαιτούνται για τον συγκεκριμένο σκοπό**, αποτρέποντας επομένως κάθε πιθανή περαιτέρω επεξεργασία. Θα πρέπει να ληφθούν μέτρα προκειμένου να διασφαλίζεται ότι θα είναι αδύνατη η διαβίβαση προτύπων μεταξύ βιομετρικών συστημάτων.

iv) Αρχή Ακρίβειας (άρ.5, παρ.1, στοιχ.δ')

Σύμφωνα με την τέταρτη αρχή που διέπει την επεξεργασία προσωπικών δεδομένων, αυτά πρέπει να είναι **ακριβή** και, όταν κριθεί αναγκαίο, **να επικαιροποιούνται**· ακόμη, πρέπει να λαμβάνονται όλα τα εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση δεδομένων προσωπικού χαρακτήρα τα οποία είναι ανακριβή, σε σχέση με τους σκοπούς της επεξεργασίας.

v) Αρχή Περιορισμού της περιόδου αποθήκευσης (άρ.5, παρ.1, στοιχ. ε')

Σύμφωνα με την ιδιαιτέρως σημαντική αυτή αρχή που διατυπώνεται στο Γενικό

[135] Σκόνδρα, 2020, σελ. 47
[136] Κατευθυντήριες Γραμμές 3/2019 σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω βιντεοσυσκευών, σελ. 24

Κανονισμό, τα δεδομένα προσωπικού χαρακτήρα πρέπει να διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα[137] που απαιτείται για τους σκοπούς της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα· τα δεδομένα προσωπικού χαρακτήρα μπορούν να αποθηκεύονται για μεγαλύτερα διαστήματα, εφόσον αυτά θα υποβάλλονται σε επεξεργασία μόνο για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς, σύμφωνα με το άρθρο 89 παράγραφος 1 και εφόσον εφαρμόζονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα που απαιτεί ο παρών κανονισμός για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων.

vi) Αρχές Ακεραιότητας και εμπιστευτικότητας (άρ.5, παρ.1, στοιχ.στ')

Τέλος, μέσω της **λήψης κατάλληλων τεχνικών και οργανωτικών μέτρων** εδραιώνονται οι αρχές της ακεραιότητας και της εμπιστευτικότητας καθώς τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια αυτών, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά.

vii) Αρχή Λογοδοσίας (άρ.5, παρ.2)

Σύμφωνα με την παράγραφο 2 του θεμελιώδους αυτού άρθρου του Γενικού Κανονισμού, ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και πρέπει να είναι σε θέση να αποδείξει τη συμμόρφωση με τα οριζόμενα στην πρώτη παράγραφο.

Προτού λάβει χώρα η ανάλυση των υποχρεώσεων του υπευθύνου επεξεργασίας ως προς την τήρηση της εφαρμογής τους, κρίνεται ορθό να οριοθετηθεί η εννοιολογική υπόσταση της ''λογοδοσίας''. Σύμφωνα με την κα Μήτρου[138], η πρωταρχική σημασία της λογοδοσίας σχετίζεται με την ύπαρξη της υποχρέωσης να εξηγεί, να αιτιολογεί κανείς τη συμπεριφορά ή τις ενέργειές του. Η έννοια της λογοδοσίας, όπως παρατηρείται, συνδέεται στενά με την αντίληψη περί επίτευξης συμμόρφωσης μέσω κατάλληλου ελέγχου. Ως προς την

[137] Σύμφωνα με τα γραφόμενα στο άρθρο 8 της Οδηγίας 1/2011 της ΑΠΔΠΧ, εφόσον από τη λήψη εικόνων που αποθηκεύονται ή τη λήψη που γίνεται σε πραγματικό χρόνο δεν προκύπτει επέλευση συμβάντος που εμπίπτει στον επιδιωκόμενο σκοπό, τα δεδομένα πρέπει να καταστρέφονται το αργότερο μέσα σε δεκαπέντε (15) εργάσιμες ημέρες, με την επιφύλαξη ειδικότερων διατάξεων της κείμενης νομοθεσίας που ισχύουν για συγκεκριμένες κατηγορίες υπεύθυνων επεξεργασίας (π.χ. καζίνο) ή αν στην παρούσα Οδηγία ορίζεται διαφορετικά.

[138] Μήτρου Λίλιαν, ''Η αρχή της λογοδοσίας'' (ως υποκεφάλαιο ενότητας ''Υποχρεώσεις του υπευθύνου επεξεργασίας''- Γιώργος Ν. Γιαννόπουλος, Λίλιαν Μήτρου, Γρηγόρης Τσόλιας) σε Κοτσαλή Λ., Μενουδάκο Κ., *Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων (GDPR), Νομική Διάσταση και Πρακτική Εφαρμογή*, Αθήνα, Νομική Βιβλιοθήκη, 2018, σελ. 170

''προβλεπτική ικανότητα'' της Ομάδας Εργασίας του άρθρου 29, διέκριναν στην έννοια της λογοδοσίας τη σύζευξη των νέων μηχανισμών που θα εξασφάλιζαν την **αποτελεσματική προστασία των προσωπικών δεδομένων στην πράξη**.[139] Οι ευρωπαϊκές αρχές εξέλαβαν τη λογοδοσία ως ''όρο που δηλώνει τον τρόπο με τον οποίο ασκείται η υπευθυνότητα και η σχετική επαλήθευση''. Στην υπό εξέταση μελέτη η ''λογοδοσία'' προσδιορίζεται εννοιολογικά ως **μηχανισμός εγγύησης της τήρησης των αρχών** που διέπουν την **επεξεργασία των προσωπικών δεδομένων** βάσει του Γενικού Κανονισμού για την προστασία των δεδομένων. Η ξεχωριστή μνεία στην εν λόγω αρχή οφείλεται στη λειτουργία της θέτοντας ως προϋπόθεση τη θεμελίωση κανόνων βάσει των οποίων θα κριθεί η συμπεριφορά του υπόχρεου σε λογοδοσία (και δίδεται έμφαση τόσο στον παρόντα ΓΚΠΔ, όσο και στον προγενέστερο νόμο υπ' αριθμ. 2472/97 αναφορικά με την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα).

Ουσιώδες για τον υπεύθυνο επεξεργασίας, στο πλαίσιο πρακτικής αποτύπωσης της ευθύνης του, να διαμορφώνει ένα πρόγραμμα διαχείρισης ιδιωτικότητας που θα εφαρμόζει τις κατευθυντήριες αρχές, έχοντας προσμετρήσει τις σχετικές παραμέτρους.

Τέλος, δεν πρέπει να επαφίεται σε ήδη ειλημμένα μέτρα, τεχνικού και οργανωτικού χαρακτήρα, αλλά να προβαίνει σε επικαιροποίηση αυτών σε τακτά χρονικά διαστήματα. Ως προτεινόμενα **μέτρα λογοδοσίας** σημειώνονται τα κάτωθι[140] :

- έγκαιρη χαρτογράφηση εργασιών και διαδικασιών επεξεργασίας
- θέσπιση εσωτερικών (γραπτών , δεσμευτικών και διαφανών ως προς τα υποκείμενα) πολιτικών προστασίας δεδομένων
- υιοθέτηση κατάλληλων και αποτελεσματικών διαδικασιών και εργαλείων εφαρμογής των πολιτικών
- έλεγχος και (επαν-) αξιολόγηση της αποτελεσματικότητάς τους, όπως και πρόβλεψη διαδικασιών για την αντιμετώπιση ελλιπούς συμμόρφωσης και παραβίασης δεδομένων
- θέσπιση διαδικασιών για την ανταπόκριση στα αιτήματα ενημέρωσης, πρόσβασης, διόρθωσης, διαγραφής και περιορισμού της επεξεργασίας, όπως και
- συνολική οργάνωση εσωτερικού μηχανισμού χειρισμού καταγγελιών

Τα ως άνω μέτρα σε συνδυασμό με την ορθή ενημέρωση και τον εποικοδομητικό προβληματισμό των ατόμων που ασχολούνται με την επεξεργασία δεδομένων προσωπικού χαρακτήρα θα συντελέσουν μακροπρόθεσμα στο να εδραιωθεί η ούτως λεγόμενη ''κουλτούρα περί της προστασίας δεδομένων προσωπικού χαρακτήρα''.

---

[139] Γνώμη 3/2010 σχετικά με την αρχή της λογοδοσίας, Ομάδα εργασίας του Άρθρου 29 για την Προστασία των δεδομένων, σελ.3, διαθέσιμη σε https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_el.pdf

[140] Μήτρου (ό.π. υποσ.138), 2018, σελ. 175

3.1.1.2.Υποχρεώσεις Υπευθύνου Επεξεργασίας Δεδομένων προσωπικού χαρακτήρα και τήρηση εφαρμογής τους

Σύμφωνα με τα άρθρα 13 και 14 ΓΚΠΔ, ο υπεύθυνος επεξεργασίας οφείλει να προβαίνει σε **ενημέρωση προς τα υποκείμενα αναφορικά με την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων**, στην οποία συμπεριλαμβάνεται και η κατάρτιση προφίλ, και, τουλάχιστον στις περιπτώσεις αυτές, παρέχονται σημαντικές πληροφορίες σχετικά με τη λογική που ακολουθείται, καθώς και τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων. Επιπροσθέτως, στην αιτιολογική σκέψη 71 του ΓΚΠΔ, αναφέρεται το δικαίωμα του υποκειμένου να λάβει αιτιολόγηση της απόφασης που ελήφθη στο πλαίσιο μίας αυτοματοποιημένης επεξεργασίας, ήτοι να ενημερωθεί πώς το σύστημα στάθμισε και αξιολόγησε τα δεδομένα του σε μία συγκεκριμένη περίπτωση.[141] Τα εν λόγω άρθρα συνδέονται άμεσα με την κατ' άρθρο 5 παρ.1 στοιχ. α΄ ΓΚΠΔ αρχή επεξεργασίας δεδομένων, αυτή της διαφάνειας. Οι πληροφορίες διακρίνονται σε αυτές που παρέχονται εάν τα δεδομένα προσωπικού χαρακτήρα **συλλέγονται από το υποκείμενο των δεδομένων** (**κατ' άρθρο 13 ΓΚΠΔ**) και σε αυτές που παρέχονται αν τα δεδομένα **δεν έχουν συλλεγεί από το υποκείμενο των δεδομένων (κατ'άρθρο 14 ΓΚΠΔ).**

Στην πρώτη περίπτωση, ο υπεύθυνος επεξεργασίας παρέχει στο υποκείμενο των δεδομένων τις ακόλουθες πληροφορίες (ως εκ του άρθρου εξάγονται):

α) την ταυτότητα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας και, κατά περίπτωση, του εκπροσώπου του υπευθύνου επεξεργασίας,

β) τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων, κατά περίπτωση,

γ) τους σκοπούς της επεξεργασίας για τους οποίους προορίζονται τα δεδομένα προσωπικού χαρακτήρα, καθώς και τη νομική βάση για την επεξεργασία,

δ) εάν η επεξεργασία βασίζεται στο άρθρο 6 παράγραφος 1 στοιχείο στ), τα έννομα συμφέροντα που επιδιώκονται από τον υπεύθυνο επεξεργασίας ή από τρίτο,

ε) τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων προσωπικού χαρακτήρα, εάν υπάρχουν,

σ κατά περίπτωση, την πρόθεση του υπευθύνου επεξεργασίας να διαβιβάσει δεδομένα

τ) προσωπικού χαρακτήρα σε τρίτη χώρα ή διεθνή οργανισμό και την ύπαρξη ή την απουσία απόφασης επάρκειας της Επιτροπής ή, όταν πρόκειται για τις διαβιβάσεις που αναφέρονται στο άρθρο 46 ή 47 ή στο άρθρο 49 παράγραφος 1 δεύτερο εδάφιο, αναφορά στις ενδεδειγμένες ή κατάλληλες εγγυήσεις και τα μέσα για να αποκτηθεί αντίγραφό τους ή στο πού διατέθηκαν.

Ουσιώδεις, επιπλέον, κρίνονται προς παράθεση ορισμένες επιπρόσθετες πληροφορίες

[141] Βόρρας Κ. Απόστολος, Μήτρου Λίλιαν (2018) ''Τεχνητή Νοημοσύνη και Προσωπικά Δεδομένα- Μια θεώρηση υπό το πρίσμα του Ευρωπαϊκού Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 2016/679'', *ΔΙΤΕ (πρ. ΔΙΜΕΕ), 4/2018*, Οκτώβριος- Νοέμβριος- Δεκέμβριος, *σελ. 460*

που θίγονται στην παρ.2 του άρθρου 13 ΓΚΠΔ και σχετίζονται με την αναγκαιότητα εξασφάλισης θεμιτής και διαφανούς επεξεργασίας ήτοι:

α)το χρονικό διάστημα για το οποίο θα αποθηκευτούν τα δεδομένα προσωπικού χαρακτήρα ή, όταν αυτό είναι αδύνατο, τα κριτήρια που καθορίζουν το εν λόγω διάστημα,

β)την ύπαρξη δικαιώματος υποβολής αιτήματος στον υπεύθυνο επεξεργασίας για πρόσβαση και διόρθωση ή διαγραφή των δεδομένων προσωπικού χαρακτήρα ή περιορισμό της επεξεργασίας που αφορούν το υποκείμενο των δεδομένων ή δικαιώματος αντίταξης στην επεξεργασία, καθώς και δικαιώματος στη φορητότητα των δεδομένων,

γ)όταν η επεξεργασία βασίζεται στο άρθρο 6 παράγραφος 1 στοιχείο α) ή στο άρθρο 9 παράγραφος 2 στοιχείο α), την ύπαρξη του δικαιώματος να ανακαλέσει τη συγκατάθεσή του οποτεδήποτε, χωρίς να θιγεί η νομιμότητα της επεξεργασίας που βασίστηκε στη συγκατάθεση πριν από την ανάκλησή της,

δ) το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή,

ε)κατά πόσο η παροχή δεδομένων προσωπικού χαρακτήρα αποτελεί νομική ή συμβατική υποχρέωση ή απαίτηση για τη σύναψη σύμβασης, καθώς και κατά πόσο το υποκείμενο των δεδομένων υποχρεούται να παρέχει τα δεδομένα προσωπικού χαρακτήρα και ποιες ενδεχόμενες συνέπειες θα είχε η μη παροχή των δεδομένων αυτών,

σ την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της

τ) κατάρτισης προφίλ, που αναφέρεται στο άρθρο 22 παράγραφοι 1 και 4 και, τουλάχιστον στις περιπτώσεις αυτές, σημαντικές πληροφορίες σχετικά με τη λογική που ακολουθείται, καθώς και τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων.

Ως προς τη συσχέτιση του άρθρου 13 με τη λειτουργία των συστημάτων βιντεοεπιτήρησης, κατά την κρίση του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων (ΕΣΠΔ), αποτελεί υποχρέωση των κρατών -μελών η ενημέρωση των ατόμων για τη χρήση των συστημάτων σε δημόσιους χώρους. **Ως βέλτιστη πρακτική, το ΕΣΠΔ συστήνει την παροχή διπλού επιπέδου ενημέρωσης[142],** ήτοι: Σε πρώτο επίπεδο, οι βασικές πληροφορίες δίδονται με τη χρήση προειδοποιητικών πινακίδων σε εύλογη απόσταση από τα σημεία που παρακολουθούνται και χωρίς να απαιτείται το άτομο να εισέλθει στον επιτηρούμενο χώρο. Οι πληροφορίες αυτές περιλαμβάνουν- ως άνω επισημάνθηκε- την ταυτότητα του υπευθύνου επεξεργασίας, το σκοπό της επεξεργασίας, τα δικαιώματα των υποκειμένων, την περίοδο διατήρησης και αποθήκευσης των δεδομένων, τις συνέπειες επεξεργασίας και κάθε άλλη πληροφορία που δεν αναμένει ευλόγως το υποκείμενο. Σε δεύτερο επίπεδο, η παροχή περαιτέρω ενημέρωσης πραγματοποιείται με τη χρήση ενημερωτικών εντύπων (π.χ. μία αφίσα) ή μέσω δηλώσεων του υπευθύνου επεξεργασίας ηλεκτρονικά ανηρτημένων που θα

[142] Σκόνδρα, 2020, σελ. 47

περιλαμβάνουν τις υπόλοιπες παρεχόμενες πληροφορίες κατά τη διαδικασία συλλογής δεδομένων προσωπικού χαρακτήρα από το ίδιο το υποκείμενο των δεδομένων το οποίο θα πρέπει να αναφέρεται σαφώς στην προειδοποιητική πινακίδα (π.χ. να αναγράφεται το QR code ή η διεύθυνση ιστοτόπου).

Εν συνεχεία, μία ακόμη σημαντική υποχρέωση του Υπευθύνου επεξεργασίας είναι η **υιοθέτηση τεχνικών και οργανωτικών μέτρων ασφάλειας της επεξεργασίας σε κάθε επίπεδό της (συλλογή, μετάδοση, αποθήκευση),** καθώς και σε όλες τις συσκευές και τους **κόμβους** μετάδοσης (κάμερες, μηχάνημα καταγραφής, ασύρματη ή ενσύρματη μετάδοση, δικτυακή ή διαδικτυακή σύνδεση, εφαρμογή διαχείρισης δεδομένων κλπ), που συναποτελούν το σύστημα της βιντεοεπιτήρησης [κατ' εφαρμογή των αρχών προστασίας εκ του σχεδιασμού (privacy by design, σύμφωνα με το άρθ. **25 ΓΚΠΔ**) και ασφάλειας της επεξεργασίας (σύμφωνα με το άρθ. **32 ΓΚΠΔ**)].

Ειδικότερα, σύμφωνα με τις Κατευθυντήριες Γραμμές 3/2019 σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω βιντεοσυσκευών[143], προκειμένου να επιτευχθεί επαρκής διασφάλιση της επεξεργασίας, ο υπεύθυνος επεξεργασίας αλλά και ο εκτελών πρέπει να μεριμνούν ώστε τα μέτρα που εφαρμόζονται να είναι ανάλογα προς τους κινδύνους για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων . Η εφαρμογή τους πρέπει να ξεκινά – σύμφωνα με το άρθρο 25 ΓΚΠΔ- ήδη από τη στιγμή που προγραμματίζουν τη βιντεοεπιτήρηση, δηλ. <u>προτού</u> ξεκινήσουν τη συλλογή και επεξεργασία βιντεοσκοπημένου υλικού (<u>privacy be design</u>). Όταν προβαίνουν στις εν λόγω οργανωτικές πρακτικές, θα πρέπει να είναι σύμφωνες με τις οριζόμενες, στο άρθρο 5 ΓΚΠΔ, αρχές που εθίγησαν ανωτέρω. Εν τοις πράγμασι κατά τη διάρκεια δημιουργίας τω δικών τους πολιτικών και διαδικασιών βιντεοεπιτήρησης, λαμβάνουν τα επόμενα <u>οργανωτικά μέτρα</u>[144]:

i) Ποιος είναι υπεύθυνος για τη διαχείριση και τον χειρισμό του συστήματος βιντεοεπιτήρησης.
ii) Σκοπός και πεδίο εφαρμογής του σχεδίου βιντεοεπιτήρησης
iii) Ενδεδειγμένη και απαγορευμένη χρήση
(πότε και πού είναι επιτρεπτή η βιντεοεπιτήρηση αλλά και πότε και πού όχι, π.χ. χρήση κρυφών καμερών και ήχου επιπλέον της βιντεοσκόπησης)
iv) Μέτρα διαφάνειας (Υποχρεώσεις ως προς την επίτευξή της)
v) Τρόπος μέσω του οποίου πραγματοποιείται η βιντεοσκόπηση και για πόση διάρκεια –συμπεριλαμβάνεται εν προκειμένω η αποθήκευση σε αρχείο βιντεοσκοπημένου υλικού που αφορά συμβάντα ασφάλειας)
vi) Ζήτημα περί του ποιος πρέπει να λάβει σχετική κατάρτιση και πότε
vii) Ταυτότητα αυτού που έχει πρόσβαση στο βιντεοσκοπημένο υλικό και για ποιο

[143] σελ.34-36 των Κατευθυντηρίων
[144] Κατευθυντήριες Γραμμές 3/2019 σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω βιντεοσυσκευών, σελ.38

σκοπό

Viii)Επιχειρησιακές διαδικασίες (π.χ. από ποιον και από πού παρακολουθείται η βιντεοεπιτήρηση, ενέργειες σε περίπτωση παραβίασης δεδομένων).

Πέραν, όμως των οργανωτικών, λαμβάνονται και τα τεχνικά μέτρα, δηλαδή μέτρα που προστατεύουν από σκόπιμη ή ακούσια παρεμβολή στις συνήθεις λειτουργίες του συστήματος (''ασφάλεια συστήματος και δεδομένων'' [145]):

Πρώτον, η προστασία ολόκληρης της υποδομής του συστήματος VSS (συμπεριλαμβανομένων των καμερών με απομακρυσμένη σύνδεση, των καλωδιώσεων και της τροφοδοσίας) από φυσική παραβίαση και κλοπή.

Δεύτερον, η προστασία της διαβίβασης οπτικοακουστικού υλικού με ασφαλείς διαύλους επικοινωνίας ενάντια σε υποκλοπή

Τρίτον, η κρυπτογράφηση δεδομένων

Τέταρτον, η χρήση λύσεων βασισμένων στο υλικό και το λογισμικό όπως τείχη προστασίας, συστήματα καταπολέμησης ιών ή ανίχνευσης εισβολών για την προστασία από κυβερνοεπιθέσεις

Πέμπτον, ανίχνευση δυσλειτουργιών των εξαρτημάτων, του λογισμικού και των διασυνδέσεων του συστήματος

Τέλος, ιδιαίτερη μνεία ως προς τις καίριες υποχρεώσεις του υπευθύνου επεξεργασίας αποτελεί **η κατ' άρθρο 35 ΓΚΠΔ εκτίμηση αντικτύπου στην προστασία των προσωπικών δεδομένων (ΕΑΠΔ).**

Σύμφωνα με την παρ. 1 του άρθρου, όταν ένα είδος επεξεργασίας ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας είναι απαραίτητο να διενεργεί εκτίμηση των επιπτώσεων για την προστασία δεδομένων.[146] Προσέτι, άξια αναφοράς η παράγραφος 3 στοιχείο γ) του ΓΚΠΔ που ορίζει ότι οι υπεύθυνοι επεξεργασίας υποχρεούνται να διενεργούν εκτιμήσεις αντικτύπου σχετικά με την προστασία δεδομένων εάν η επεξεργασία αποτελεί συστηματική παρακολούθηση δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα. Εν συνεχεία, κατά την παρ. 4 του άρθρου επισημαίνεται ότι κάθε εποπτική αρχή πρέπει να καταρτίζει κατάλογο με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια εκτίμησης αντικτύπου σχετικά με την

[145] Βάσει των Κατευθυντηρίων Γραμμών 3/2019, σελ. 38, **Ασφάλεια συστήματος** σημαίνει φυσική ασφάλεια όλων των εξαρτημάτων του συστήματος και ακεραιότητα συστήματος, δηλαδή προστασία και ανθεκτικότητα σε περίπτωση σκόπιμης ή ακούσιας παρεμπόδισης των κανονικών λειτουργιών και ελέγχου της πρόσβασης. Επίσης, Ασφάλεια δεδομένων ορίζεται ως το σύνολο των τριών εννοιών που ακολουθούν, ήτοι εμπιστευτικότητα (τα δεδομένα είναι προσπελάσιμα μόνο σε όσους έχει παραχωρηθεί πρόσβαση), ακεραιότητα (προλαμβάνεται η απώλεια ή η παραποίηση δεδομένων) και διαθεσιμότητα (τα δεδομένα είναι προσπελάσιμα όταν απαιτείται).

[146] Σκόνδρα, 2020, σελ. 47 **και** Κατευθυντήριες Γραμμές 3/2019, σελ. 40

προστασία δεδομένων εντός της οικείας χώρας. Εκ των ως άνω συνάγεται ότι στην περίπτωση της βιντεοεπιτήρησης είναι υποχρεωτική η διενέργεια εκτίμησης αντικτύπου, καθώς μέσω αυτής εξυπηρετούνται συγκεκριμένοι σκοποί (απαιτείται ιδίως στη μεγάλης κλίμακας επεξεργασία των ειδικών κατηγοριών δεδομένων, στα οποία συμπεριλαμβάνονται και τα υπό εξέταση βιομετρικά – αρ.35 , παρ. 3 περ.β) και άρ.9 παρ.1 ΓΚΠΔ)

Συμπληρωματική της μελέτης αντικτύπου για την ιδιωτικότητα, είναι **η αλγοριθμική μελέτη αντικτύπου** που δεν είναι άμεσα επιβεβλημένη νομοθετικά και αποτελεί διαδικασία ευρύτερη της ήδη αναλυθείσας. Διενεργείται για τυχόν ύπαρξη προκαταλήψεων τόσο σε εκπαιδευτικά όσο και σε επιχειρησιακά δεδομένα και την αναγκαιότητα της συγκεκριμένης μελέτης αντικτύπου περί αλγορίθμων τονίζει και ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων (Γνώμη 4/2020 για τη Λευκή Βίβλο της Ευρωπαϊκής Επιτροπής για την Τεχνητή Νοημοσύνη).[147]

3.1.1.3. Δικαιώματα υποκειμένου δεδομένων

Στην παρούσα υποενότητα και προς την πληρότητα της προσέγγισης των διαφόρων πτυχών των προϋποθέσεων που πρέπει να συντρέχουν προκειμένου να είναι η νόμιμη επεξεργασία, θα αναφερθούν τα δικαιώματα του υποκειμένου των δεδομένων σύμφωνα με τον ΓΚΠΔ, εστιάζοντας σε αυτά της πρόσβασης και της διαγραφής.

- Σύμφωνα με το <u>άρθρο 12 ΓΚΠΔ</u>, το οποίο θεμελιώνει <u>το δικαίωμα ενημέρωσης</u> του υποκειμένου και συνδυαστικά με τα άρθρα 13 και 14 ΓΚΠΔ που ορίζουν την αρχή της διαφάνειας, τα φυσικά πρόσωπα έχουν δικαίωμα να ενημερώνονται με ακρίβεια και σαφήνεια για τη συλλογή και τη χρήση (επεξεργασία) των προσωπικών τους δεδομένων.

- Σύμφωνα με <u>το άρθρο 15ΓΚΠΔ (''δικαίωμα πρόσβασης του υποκειμένου των δεδομένων'')</u>, το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητεί <u>επιβεβαίωση</u> από τον υπεύθυνο επεξεργασίας ως προς το αν τα δεδομένα προσωπικού χαρακτήρα που το αφορούν υποβάλλονται σε επεξεργασία. **<u>Όσον αφορά στη βιντεοεπιτήρηση</u>**, αυτό σημαίνει[148] ότι εάν δεν γίνει αποθήκευση ή διαβίβαση με κανέναν τρόπο των δεδομένων, τότε από τη στιγμή που θα λάβει χώρα και θα ολοκληρωθεί η παρακολούθηση σε πραγματικό χρόνο (''ζωντανή παρακολούθηση'') ο υπεύθυνος επεξεργασίας δύναται μόνο να μεταδώσει την πληροφορία ότι κανένα δεδομένο προσωπικού χαρακτήρα δεν υποβάλλεται πλέον σε επεξεργασία (πέραν των γενικών κατά το άρθρο 13 ΓΚΠΔ υποχρεώσεων διαφάνειας και πληροφόρησης). Αν παρόλα αυτά

[147] Κανέλλος, 2020, σελ. 289-290

[148] όπως επισημαίνεται στην ερμηνεία βάσει των Κατευθυντήριων γραμμών 3/2019

συνεχίζεται να πραγματοποιείται επεξεργασία δεδομένων τη στιγμή του αιτήματος (δηλ. αν τα δεδομένα αποθηκεύονται ή υποβάλλονται σε συνεχή επεξεργασία με οποιονδήποτε άλλον τρόπο), το υποκείμενο των δεδομένων θα πρέπει να λάβει πρόσβαση και πληροφόρηση σύμφωνα με το άρθρο 15.

Όπως σημειώνει η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), [149] δικαιώματα των υποκειμένων των δεδομένων είναι δυνατό να υπόκεινται σε νόμιμους περιορισμούς μέσω νομοθετικών μέτρων, με την προϋπόθεση να μην παραβιάζουν τον πυρήνα του εκάστοτε δικαιώματος, αφορούν σε αναγκαία και αναλογικά μέτρα που οφείλει να λαμβάνει μια δημοκρατική κοινωνία, εξυπηρετούν κάποιον από τους σκοπούς που αναφέρονται περιοριστικά στο άρθρο 23 παρ. 1 στοιχ. α'- ι' ΓΚΠΔ και καλύπτουν τις προϋποθέσεις του άρθρου 23 παρ. 2 αναφορικά με το ελάχιστο περιεχόμενό τους.

Επίσης, στο πλαίσιο της παρ.3 του άρθρου, ο υπεύθυνος επεξεργασίας θα πρέπει να λάβει τα κατάλληλα μέτρα προκειμένου να αποτρέψει τη λήψη αντιγράφου του βιντεοσκοπημένου υλικού του υποκειμένου των δεδομένων, διότι θα μπορούσαν να προσβληθούν τα δικαιώματα και οι ελευθερίες άλλων υποκειμένων των δεδομένων. Ένα ενδεικτικό μέτρο είναι το να ''θολώσει'' μέσω τεχνικής επεξεργασίας τα πρόσωπά τους (μέθοδοι απόκρυψης ή αλλοίωσης).

- Έπειτα, κατά το άρθρο 16 ΓΚΠΔ (''Δικαίωμα διόρθωσης''), το υποκείμενο έχει το δικαίωμα, σύμφωνα με το περιεχόμενο του άρθρου, να απαιτήσει από τον υπεύθυνο επεξεργασίας, χωρίς αδικαιολόγητη καθυστέρηση, τη διόρθωση ανακριβών δεδομένων προσωπικού χαρακτήρα που το αφορούν (σε περίπτωση ελλιπούς καταχώρισης δεδομένων δύναται να απαιτήσει συμπληρωματική δήλωση).

- Ακολουθεί το ''δικαίωμα διαγραφής ή δικαίωμα στη λήθη'' (κατ' άρθρο 17 ΓΚΠΔ). Σύμφωνα με τα οριζόμενα στο άρθρο, το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητήσει από τον υπεύθυνο επεξεργασίας τη διαγραφή δεδομένων προσωπικού χαρακτήρα που το αφορούν χωρίς αδικαιολόγητη καθυστέρηση και ο υπεύθυνος επεξεργασίας έχει την υποχρέωση να διαγράψει δεδομένα προσωπικού χαρακτήρα χωρίς αδικαιολόγητη καθυστέρηση, εάν ισχύει ένας από τους λόγους που θίγονται στην παράγραφο 1 (και *ταυτοχρόνως δεν εφαρμόζεται κάποια από τις εξαιρέσεις της παραγράφου 3* του άρθρου). Οι λόγοι διακρίνονται , βάσει των Κατευθυντηρίων γραμμών 3/2019 του Ευρωπαϊκού Συμβουλίου Προστασίας δεδομένων , σε αυτούς της συγκατάθεσης, δηλ. τα δεδομένα θα πρέπει απαραιτήτως να διαγράφονται

[149] Αρχή Προστασίας Δεδομένων, Τα δικαιώματά μου στο πλαίσιο του ΓΚΠΔ - Δικαίωμα πρόσβασης του υποκειμένου των δεδομένων σε https://dpa.gr/index.php/el/polites/gkpd/dikaiwma_prosvasis_upokeimenou

όταν ανακαλείται η συγκατάθεση (και ταυτοχρόνως δεν εγείρεται άλλη νομική βάση σχετικά με την επεξεργασία), αλλά και του εννόμου συμφέροντος, όταν το υποκείμενο των δεδομένων ασκεί το δικαίωμα εναντίωσης και δεν υπερισχύουν άλλοι επιτακτικοί και νόμιμοι λόγοι για την επεξεργασία αλλά και στην περίπτωση της άμεσης εμπορικής προώθησης (στην οποία συμπεριλαμβάνεται και η κατάρτιση προφίλ, όταν το υποκείμενο των δεδομένων είναι αντίθετο στην επεξεργασία. Εν συνεχεία, ουσιώδες να αναφερθεί ότι όταν ο υπεύθυνος επεξεργασίας έχει δημοσιοποιήσει το βιντεοσκοπημένο υλικό (π.χ. ραδιοτηλεοπτική μετάδοση ή διαδικτυακή μετάδοση συνεχούς ροής), πρέπει να ληφθούν εύλογα μέτρα προκειμένου να ενημερωθούν άλλοι υπεύθυνοι επεξεργασίας (που επίσης επεξεργάζονται τα συγκεκριμένα δεδομένα προσωπικού χαρακτήρα) για το αίτημα σύμφωνα με την παράγραφο 2 του άρθρου. Ως προς το περιεχόμενό τους, θα πρέπει να περιλαμβάνουν τεχνικά μέτρα ενώ πρέπει να λαμβάνεται υπόψη η διαθέσιμη τεχνολογία και το κόστος εφαρμογής. Τέλος, στην περίπτωση θόλωσης εικόνας – ως προς τη βιντεοεπιτήρηση- και στη συνέχεια μη δυνατότητας ανάκτησης των προσωπικών δεδομένων που αυτή περιείχε, τα δεδομένα εκλαμβάνονται ως διαγεγραμμένα, σύμφωνα με τον ΓΚΠΔ.

- Ακόμη, πέραν της υποχρέωσης του υπευθύνου επεξεργασίας προς διαγραφή προσωπικών δεδομένων κατόπιν αιτήματος του υποκειμένου αυτών, αυτός υποχρεούται, τηρώντας τις αρχές του ΓΚΠΔ να περιορίσει τα αποθηκευμένα δεδομένα προσωπικού χαρακτήρα (''Δικαίωμα περιορισμού της επεξεργασίας'', κατ' άρθρο 18 ΓΚΠΔ). Πιο συγκεκριμένα, το υποκείμενο δικαιούται να εξασφαλίζει το συγκεκριμένο δικαίωμα όταν πληρούνται οι προϋποθέσεις που ορίζονται στην παράγραφο 1 του άρθρου.

- Ένα ακόμη δικαίωμα του υποκειμένου που θίγει ο Γενικός Κανονισμός είναι αυτό της ''Φορητότητας των δεδομένων''. Σύμφωνα με το άρθρο 20 ΓΚΠΔ, το υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει τα δεδομένα προσωπικού χαρακτήρα που το αφορούν, και τα οποία έχει παράσχει σε υπεύθυνο επεξεργασίας, σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο, καθώς και το δικαίωμα να προβαίνει σε διαβίβαση των εν λόγω δεδομένων σε άλλον υπεύθυνο επεξεργασίας χωρίς αντίρρηση από τον υπεύθυνο επεξεργασίας στον οποίο παρασχέθηκαν τα δεδομένα προσωπικού χαρακτήρα, υπό τις ακόλουθες προϋποθέσεις:

- ✓ η επεξεργασία βασίζεται σε συγκατάθεση σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο α) ΓΚΠΔ ή το άρθρο 9 παράγραφος 2 στοιχείο α) ΓΚΠΔ ή σε σύμβαση σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο β) ΓΚΠΔ και
- ✓ η επεξεργασία διενεργείται με αυτοματοποιημένα μέσα.

- Καταληκτικά, βαρύνουσας σημασίας αποτελεί η αναφορά στο ''Δικαίωμα εναντίωσης'', που θεμελιώνεται στο άρθρο 21 ΓΚΠΔ.

  Όσον αφορά στις νομικές βάσεις επεξεργασίας για το υπό εξέταση δικαίωμα – εν συνόλω θα αναλυθούν στο επόμενο κεφάλαιο- , εφαρμόζεται όταν η βιντεοεπιτήρηση βρίσκει έρεισμα είτε στο έννομο συμφέρον (άρ.6 παρ.1 στοιχ.στ) ΓΚΠΔ) είτε στην εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον (άρ.6 παρ.1 στοιχ.ε) ΓΚΠΔ). Στην περίπτωση επίκλησης ενός εκ των δύο νομικών βάσεων από πλευράς του υποκειμένου, ο υπεύθυνος επεξεργασίας δε συνεχίζει να υποβάλλει πλέον τα δεδομένα προσωπικού χαρακτήρα σε επεξεργασία, εκτός αν αποδείξει ότι συντρέχουν επιτακτικοί και νόμιμοι λόγοι που υπερισχύουν των δικαιωμάτων και των συμφερόντων των υποκειμένων. Στην περίπτωση βιντεοεπιτηρούμενης περιοχής, μη δημοσίως προσβάσιμης και κατά τέτοιο τρόπο περιορισμένης, η αντίρρηση του υποκειμένου θα μπορούσε να διατυπωθεί κατά την είσοδο στον παρακολουθούμενο χώρο, κατά την παραμονή σε αυτόν ή κατόπιν της αποχώρησης από αυτόν[150]. Επομένως, η **νομιμότητα της παρακολούθησης από πλευράς του υπευθύνου θεμελιώνεται (α)** αν σταματήσει, αμέσως μόλις λάβει σχετικό αίτημα, τη λειτουργία της κάμερας από την επεξεργασία προσωπικών δεδομένων και **(β)** αν τα μέτρα ελέγχου για την πρόσβαση στον παρακολουθούμενο χώρο είναι πολύ αυστηρά, ώστε ο υπεύθυνος να μπορεί να διασφαλίσει την προηγούμενη έγκριση του υποκειμένου, δηλαδή αν μπορεί να εισέλθει στο χώρο και εφόσον δεν αφορά σημείο στο οποίο μπορεί να έχει πρόσβαση ως πολίτης.

3.1.1.4.Νομική Βάση επεξεργασίας δεδομένων Βιντεοεπιτήρησης

Ως νομική βάση επεξεργασίας νοείται κάθε βάση που εμπίπτει στο **άρθρο 6 παρ.1 ΓΚΠΔ**.

Εξετάζοντας, λοιπόν, τη νομιμότητα της επεξεργασίας, υπό το πρίσμα της νομικής βάσης, η πρώτη περίπτωση που μελετά κανείς είναι η υπό **στοιχ. α),** ήτοι η **συγκατάθεση** του υποκειμένου των δεδομένων. Σύμφωνα με το άρθρο 4 περ.11 ΓΚΠΔ, το άρθρο 7 ΓΚΠΔ αλλά και τις σχετικές Κατευθυντήριες Γραμμές[151] πρέπει να είναι ελεύθερη, συγκεκριμένη, ρητή και να παρέχεται με πλήρη επίγνωση (βασικές προϋποθέσεις). Ως προς τη συστηματική παρακολούθηση, η συγκατάθεση δύναται να νοηθεί μόνο ως εξαιρετική νομική βάση, διότι η παρακολούθηση απροσδιόριστου

[150] Σκόνδρα, 2020, σελ. 48 **και** Κατευθυντήριες Γραμμές 3/2019, σελ.29

[151] Ομάδα εργασίας του άρθρου 29, Κατευθυντήριες γραμμές σχετικά με τη συγκατάθεση βάσει του κανονισμού 2016/679 (W P 259 αναθ. 01) (Εκδόθηκαν στις 28 Νοεμβρίου 2017 - τελικώς αναθεωρήθηκαν και εκδόθηκαν στις 10 Απριλίου 2018)

αριθμού ανθρώπων αποτελεί εγγενές χαρακτηριστικό της τεχνολογίας της βιντεοεπιτήρησης. Εν τοις πράγμασι, ο υπεύθυνος επεξεργασίας σπανίως δύναται να αποδείξει ότι το υποκείμενο των δεδομένων συγκατατέθηκε εκ των προτέρων για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν (άρ. 7 παρ. 1). Σύμφωνα με την παρ.3 του άρ.7, το υποκείμενο των δεδομένων έχει το δικαίωμα ανάκλησης της συγκατάθεσής του ανά πάσα στιγμή. Το ουσιώδες είναι ότι στην περίπτωση αυτή, δε θίγεται η νομιμότητα της επεξεργασίας που είχε ως νομικό έρεισμα αυτό της συγκατάθεσης μέχρι το χρονικό σημείο της ανάκλησης και το πρότερο αυτού.

Τέλος, θεωρείται καίριο να σημειωθούν δύο ακόμη σημεία. Το πρώτο, έγκειται στο ότι το γεγονός απλώς και μόνο ότι ένα άτομο εισέρχεται σε σηματοδοτημένο παρακολουθούμενο χώρο δε συνεπάγεται αυτομάτως δήλωση ή σαφή θετική ενέργεια από πλευράς του , όπως αυτή τεκμηριώνεται βάσει συγκατάθεσης, παρά μόνο στην περίπτωση που τυγχάνει να πληρούν κι αυτές τις προϋποθέσεις που τίθενται με βάση τα άρθρα 4 και 7 ΓΚΠΔ. [152] Το δεύτερο σημείο σχετίζεται με την ανισορροπία που παρατηρείται μεταξύ εργοδοτών και εργαζομένων καθώς στις πλείστες περιπτώσεις οι εργοδότες δε θα πρέπει να στηρίζονται στη συγκατάθεση των εργαζομένων όταν προβαίνουν σε επεξεργασία δεδομένων προσωπικού χαρακτήρα, αφού αυτή πιθανότατα δε θα έχει δοθεί ελεύθερα. Στη συγκεκριμένη περίπτωση προτιμητέο είναι να λαμβάνονται υπόψη οι Κατευθυντήριες Γραμμές σχετικά με τη συγκατάθεση.[153]

Εν συνεχεία, **η δεύτερη νομική βάση είναι η εκτέλεση σύμβασης** (''η *επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης*'', σύμφωνα με το **στοιχ.β'** της **παρ.1** του **άρ.6 ΓΚΠΔ**).

Κατά την άποψη που διατυπώνει η κ. Σκόνδρα [154], συγκεκριμενοποιείται το πλαίσιο σύμφωνα με το οποίο η σύμβαση λογίζεται ως νομική βάση, κι αυτό λαμβάνει χώρα όταν η επεξεργασία αυτή καθαυτή, εν όλω ή εν μέρει, δομεί το κύριο αντικείμενο της σύμβασης . Επί μία εις έτι φορά θα αναφερθεί η περίπτωση συμβατικής σχέσης μεταξύ εργοδότη- εργαζομένου, καθώς λανθάνει το ενδεχόμενο ύπαρξης μη έγκυρης συγκατάθεσης του υποκειμένου των δεδομένων υπό το ''μανδύα'' της σύμβασης. Λόγω αυτού η θεμελίωση της πραγματικής συμβατικής ελευθερίας ως απαραίτητης προϋπόθεσης για την εγκυρότητα της σύμβασης διαδραματίζει ιδιαιτέρως σημαίνοντα ρόλο.

Επιπροσθέτως, **τρίτη κατά σειρά νομική βάση επεξεργασίας** είναι αυτή της **εκ του νόμου υποχρέωσης του υπευθύνου επεξεργασίας (στοιχ. γ**).

[152] ό.π. υποσημ. 150, θα πρέπει να λαμβάνονται υπόψη και στην εν λόγω περίπτωση

[153] Κατευθυντήριες γραμμές 3/2019, σελ. 16

[154] Σκόνδρα, 2020, 48

Εν τοιαύτη βάσει, αναλόγως του εθνικού δικαίου των κρατών - μελών[155], παρατηρούνται ενδεχόμενες περιπτώσεις κατά τις οποίες ο υπεύθυνος επεξεργασίας υποχρεούται να ενεργοποιεί τη λειτουργία συστήματος βιντεοεπιτήρησης.

Τέταρτη νομική βάση επεξεργασίας, κατά το Γενικό Κανονισμό, είναι η υπό **στοιχ.δ**), **διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου.**

Αποτελεί μία ακόμη εξαιρετική περίπτωση, καθώς απαιτεί την ύπαρξη μιας όλως επείγουσας κατάστασης προκειμένου να μπορεί να εγερθεί ως νομική βάση, η οποία δε θα μπορούσε να ευσταθεί σε σύστημα βιντεοεπιτήρησης (λόγω της απαιτούμενης προεργασίας στην τοποθέτηση και εγκατάστασή του), παρά μόνο αν λάμβανε χώρα περαιτέρω διαβίβαση και χρήση του βιντεοληπτικού υλικού.

Ακολούθως, **μια ιδιαίτερα σημαντική νομική βάση** είναι αυτή της επεξεργασίας που είναι απαραίτητη για την **εκπλήρωση καθήκοντος** που **εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας** που έχει ανατεθεί στον υπεύθυνο επεξεργασίας (**άρ.6 παρ.1 στοιχ. ε) ΓΚΠΔ**).

Η εν λόγω νομική βάση συμπεριλαμβάνεται στις κατ' εξαίρεση εφαρμοζόμενες καθώς απαραίτητο στοιχείο- απαιτούμενη προϋπόθεση αποτελεί η θεμελίωση του στοιχείου της αναγκαιότητας της επεξεργασίας προς εκπλήρωση ορισμένου καθήκοντος δημοσίου πλαισίου. Αυτονοήτως και σε συνάρτηση τόσο με τις βασικές αρχές όσο και με τα δικαιώματα του υποκειμένου που προεκτέθηκαν, συνειδητοποιεί κανείς τη σημασία της προτέρας αξιολόγησης της εκάστοτε κατάστασης ως προς το βαθμό επικινδυνότητας αλλά και την ενδεχόμενη απαίτηση εκπόνησης μελέτης εκτίμησης αντικτύπου κατά το άρθρο 35 ΓΚΠΔ.

Ολοκληρώνοντας την παράθεση των νομικών βάσεων – προϋποθέσεων νομιμότητας επεξεργασίας δεδομένων βιντεοεπιτήρησης, η καταλληλότερη και ευρύτερα χρησιμοποιούμενη στην πράξη είναι η **ύπαρξη εννόμων συμφερόντων** (**άρ.6 παρ.1 στοιχ.στ**) **ΓΚΠΔ**) . Κατά το λεκτικό του άρθρου, η βιντεοεπιτήρηση είναι νόμιμη εάν είναι απαραίτητη για την επίτευξη του σκοπού του εννόμου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, **εκτός εάν** έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων.

Επιχειρώντας την κατά το δυνατόν σαφέστερη παρουσίαση της διάστασης και των κριτηρίων της συγκεκριμένης νόμιμης βάσης, θεωρείται ορθό να αναφερθεί ότι ο υπεύθυνος επεξεργασίας υποχρεούται – τηρώντας τη βασική αρχή της λογοδοσίας- να

[155] Στο ελληνικό δίκαιο αντίστοιχες περιπτώσεις αποτελούν, επί παραδείγματι, ο Κανονισμός Ασφάλειας των Καταστημάτων Κράτησης (Αριθμ. 104356 , ΦΕΚ Β΄ 3581/31.12.2014) και ο Γενικός Κανονισμός Λειτουργίας Κέντρων Υποδοχής και Ταυτοποίησης και Κινητών Μονάδων Υποδοχής και Ταυτοποίησης για τα κέντρα υποδοχής προσφύγων (Αριθμ. 1/7433, ΦΕΚ Β΄ 2219/10.06.2019),

πραγματοποιήσει μια ad hoc στάθμιση μεταξύ τόσο των δικών του εννόμων συμφερόντων ως προς την υλοποίηση της επεξεργασίας όσο και των προσβαλλόμενων δικαιωμάτων και ελευθεριών των υποκειμένων των δεδομένων (των εν γένει δικαιωμάτων κι όχι αποκλειστικά του δικαιώματος στην προστασία των προσωπικών του δεδομένων).

Στο πλαίσιο αυτό, οι επιμέρους προϋποθέσεις της νομικής βάσης του άρθρου 6 παρ.1 στοιχ. στ) ΓΚΠΔ, είναι οι κάτωθι: 1) η επεξεργασία να είναι απαραίτητη για την επίτευξη του σκοπού της, 2) ο σκοπός της να συνίσταται σε έννομο συμφέρον του υπευθύνου επεξεργασίας ή τρίτου και 3) τα δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων να μην υπερέχουν έναντι του εννόμου συμφέροντος χάριν του οποίου διενεργείται η επεξεργασία.

Η απόφαση, επομένως, του υπευθύνου πρέπει να λαμβάνεται κατά περίπτωση, καθώς απλοί συσχετισμοί αφηρημένων καταστάσεων ή προσπάθεια σύγκρισης παρεμφερών περιπτώσεων δεν επαρκούν[156]. Καθήκον του είναι η αξιολόγηση των κινδύνων παραβίασης των δικαιωμάτων των υποκειμένων και κομβικό κριτήριο ως προς την επιτυχή ολοκλήρωση αυτής είναι η λήψη υπόψη της έντασης[157] της παρέμβασης στα ατομικά δικαιώματα και ελευθερίες.

Το έννομο συμφέρον πρέπει να διαθέτει ορισμένα χαρακτηριστικά, όπως να υφίσταται *πραγματικά* και να αφορά *παρόν* ζήτημα [158]. Και τούτο διότι, προτού εκκινήσει η βιντεοεπιτήρηση, ο υπεύθυνος οφείλει να είναι βέβαιος ότι λαμβάνει χώρα *πραγματική* (*όχι πλασματική ή υποθετική*) κατάσταση κινδύνου ώστε να μην προχωρήσει σε λανθασμένες ενέργειες. Η πρότερη καταγραφή συναφών συμβάντων – και των αντιστοίχων διενεργηθεισών ποινικών διώξεων- δύναται να λειτουργήσει βοηθητικά, ως ισχυρής αξίας τεκμήριο, εν σχέσει με την ύπαρξη εννόμου συμφέροντος. Δε θα ήταν ορθό, ακόμη, να παραβλέψει στο πλαίσιο αυτό, να εκτιμήσει τις εύλογες προσδοκίες του υποκειμένου των δεδομένων περί παρακολούθησής του τόσο κατά τη στιγμή που πραγματοποιείται όσο και κατά την επεξεργασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν.[159]

Αναφορικά με τη διαδικασία της στάθμισης, ουσιώδης προς επισήμανση εφαρμοστέα αρχή είναι αυτή της **αναλογικότητας,** η οποία σύμφωνα με το **άρθρο 5 της Οδηγίας 1/2011 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ),** εξετάζεται ως προς **τρεις βασικές παραμέτρους: πρώτον, την αναγκαιότητα της επεξεργασίας** μέσω βιντεοεπιτήρησης για την επίτευξη του σκοπού, χωρίς να γίνεται υπέρβαση του αναγκαίου μέτρου**, δεύτερον, το κατά πόσο η επεξεργασία είναι**

[156] Κατευθυντήριες γραμμές 3/2019, σελ.13

[157] Η ένταση εξαρτάται, μεταξύ άλλων, από το είδος των πληροφοριών που συγκεντρώνονται (περιεχόμενο των πληροφοριών), το πεδίο κάλυψης (πυκνότητα πληροφοριών, χωρική και γεωγραφική έκταση), τον αριθμό των ενδιαφερόμενων υποκειμένων των δεδομένων –είτε ως συγκεκριμένος αριθμός είτε ως αναλογία του σχετικού πληθυσμού– την υπό εξέταση κατάσταση, τα πραγματικά συμφέροντα της ομάδας των υποκειμένων των δεδομένων, τα εναλλακτικά μέσα, καθώς και τη φύση και το πεδίο εφαρμογής της αξιολόγησης των δεδομένων.

[158] Γνώμη 06/2014 σχετικά με την έννοια των εννόμων συμφερόντων του υπευθύνου επεξεργασίας, σύμφωνα με το άρθρο 7 της οδηγίας 95/46/ΕΚ (WP217), Ομάδα εργασίας του άρθρου 29, σ. 24 και επ. και Υπόθεση ΕΔ C-708/18, σ. 44

[159] Αιτιολογική σκέψη 47 του ΓΚΠΔ

πρόσφορη και κατάλληλη ώστε να επιτευχθεί ο επιδιωκόμενος σκοπός **με τα –κατά το δυνατόν- ηπιότερα μέσα** (άρ.4 ν.2472/1997**)** και **τρίτον, την εν στενή εννοία αναλογικότητα,** σύμφωνα με την οποία πρέπει να ελέγχεται αν η προσβολή των δικαιωμάτων και ελευθεριών είναι δυσανάλογη σε σχέση με τα πλεονεκτήματα της επεξεργασίας.

Τις τρεις ως άνω παραμέτρους οφείλει να λαμβάνει πάντα υπόψη ο υπεύθυνος επεξεργασίας και να τις μελετά προσεκτικά προτού ενεργήσει. Τα μέτρα βιντεοεπιτήρησης, σύμφωνα με τις Κατευθυντήριες Γραμμές 3/2019, θα πρέπει να επιλέγονται μόνο εάν ο σκοπός της επεξεργασίας δε θα μπορούσε εύλογα να εκπληρωθεί με άλλα μέσα, τα οποία θίγουν σε μικρότερο βαθμό τα θεμελιώδη δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων, δηλαδή θα είναι εξίσου αποτελεσματικά αλλά λιγότερο επαχθή για το άτομο. Επί παραδείγματι, αντί να προβεί σε εγκατάσταση συστημάτων βιντεοεπιτήρησης, θα εδύνατο να λάβει εναλλακτικά μέτρα ασφαλείας, όπως περίφραξη της ιδιοκτησίας του, ανάθεση σε προσωπικό ασφαλείας τακτικότερων ελέγχων του χώρου, πρόσληψη φυλάκων, τοποθέτηση καλύτερου φωτισμού αλλά και κλειδαριών ασφαλείας, απαραβίαστων παραθύρων και πορτών. Επιπροσθέτως, αναφορικά με την πρώτη παράμετρο της αναλογικότητας, τα σημεία όπου εγκαθίστανται οι κάμερες και ο τρόπος που λαμβάνονται τα συλλεγόμενα δεδομένα πρέπει να προσδιορίζονται έτσι ώστε τούτα να μην είναι περισσότερα από όσα είναι απολύτως αναγκαία για την εκπλήρωση του σκοπού της επεξεργασίας (συσχέτιση με ‘’αρχή ελαχιστοποίησης’’- άρ.5 παρ.1.στοιχ. γ) ΓΚΠΔ).

Το στοιχείο της χρησιμοποίησης ηπιότερων μέσων προς επίτευξη ίδιων σκοπών αναδεικνύει η ΑΠΔΠΧ μέσω της νομολογίας της. Πιο συγκεκριμένα**, με την υπ’ αριθ. 137/2013 *απόφασή της, χαρακτηριστική πλέον ως προς τη συσχέτισή της με την ‘’αρχή της αναλογικότητας’’*** , έκρινε ως αναλογική και αναγκαία την εγκατάσταση καμερών εξωτερικά των συρμών του Μετρό, για έλεγχο των θυρών, αφού δεν υπάρχει άλλο ηπιότερο και πρόσφορο μέσο. Αντίθετα, στην ίδια απόφαση, η ΑΠΔΠΧ έκρινε ως μη αναγκαία την ύπαρξη καμερών εντός των συρμών [160], αφού η ΣΤΑΣΥ θα μπορούσε να επιτύχει τους ίδιους σκοπούς (ασφάλειας έναντι κακόβουλων ενεργειών (security) ή/και ατυχημάτων (safety), χρησιμοποιώντας ηπιότερα μέσα, όπως η επιτήρηση των εσωτερικών χώρων των συρμών από προσωπικό ασφαλείας ή στην περαιτέρω αξιοποίηση των δυνατοτήτων των ήδη εγκατεστημένων καμερών ασφαλείας στους σταθμούς και στις αποβάθρες του μετρό.

Καταληκτικά, προτού αναλυθεί η βιντεοεπιτήρηση και επεξεργασία των ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα, αξίζει να σημειωθούν ορισμένα ενδεικτικά σημεία των άρθρων 6 και 7 της Οδηγίας 1/2011 ΑΠΔΠΧ, ως προς την εξειδίκευση της αρχής της αναλογικότητας και την απαγόρευση επιτήρησης στους χώρους εργασίας αντιστοίχως.

Σύμφωνα με το άρθρο 6, παρατηρούνται **ειδικές περιπτώσεις εφαρμογής της**

[160] όπως επισημαίνει και η κ.Σκόνδρα, 2020, σελ. 50

αρχής της αναλογικότητας, επί των οποίων ο κανόνας είναι η απαγόρευση λήψης εικόνας μέσω βιντεοεπιτήρησης, αλλά κατ᾽εξαίρεση, σε ορισμένες εξ αυτών, αυτή δύναται να επιτραπεί **εφόσον** πληρούνται ορισμένες προϋποθέσεις. Οι ειδικές αυτές περιπτώσεις είναι: 1) λήψη εικόνας από παράπλευρες οδούς και πεζοδρόμια, 2) λήψη εικόνας από εισόδους ή εσωτερικό γειτονικών κατοικιών, κτιρίων ή άλλων χώρων, 3) χώροι στους οποίους η εγκατάσταση συστημάτων βιντεοεπιτήρησης απαγορεύεται, λόγω προσβολής του σκληρού πυρήνα του δικαιώματος στην προστασία της ιδιωτικής ζωής (όπως χώροι και προθάλαμοι τουαλετών ανεξαρτήτως του είδους της επιχείρησης ή του φορέα που βρίσκονται οι χώροι αυτοί, όπως και αποδυτήρια και λουτρά προσωπικού ή πελατών), 4) κάμερες με δυνατότητα στρέψης και εστίασης, 5) δεδομένα ήχου και 6) ελαχιστοποίηση δεδομένων με βάση την επιλογή συγκεκριμένων τεχνολογιών (privacy by design) - επιλογή εκ μέρους του υπευθύνου επεξεργασίας τεχνολογιών όσο το δυνατόν πιο "φιλικών" προς την ιδιωτικότητα (π.χ. συστήματα με δυνατότητα κρυπτογράφησης των αποθηκευμένων εικόνων ή/και δυνατότητα "θόλωσης").

Τέλος, σύμφωνα με το άρθρο 7 , στις περιπτώσεις λειτουργίας συστημάτων βιντεοεπιτήρησης σε χώρους εργασίας η εφαρμογή της αρχής της αναλογικότητας διαδραματίζει σημαίνοντα ρόλο. Ο **κανόνας** βασίζεται στο ότι ''*δε θα πρέπει να χρησιμοποιείται για την επιτήρηση των εργαζομένων εντός των χώρων αυτών, εκτός από* ***ειδικές εξαιρετικές περιπτώσεις*** *όπου αυτό δικαιολογείται από τη φύση και τις συνθήκες εργασίας και είναι απαραίτητο για την προστασία της υγείας και της ασφάλειας των εργαζομένων ή την προστασία κρίσιμων χώρων εργασίας (π.χ. στρατιωτικά εργοστάσια, τράπεζες, εγκαταστάσεις υψηλού κινδύνου)*''. Είναι ορθό, λοιπόν, να λαμβάνει χώρα πάντα στάθμιση από πλευράς του υπευθύνου επεξεργασίας και να μην επιτραπεί, σε καμία περίπτωση, τα δεδομένα που συλλέγονται μέσω συστήματος βιντεοεπιτήρησης να χρησιμοποιηθούν ως αποκλειστικά κριτήρια για την αξιολόγηση της συμπεριφοράς και της αποδοτικότητας των εργαζομένων (επίσης, Οδηγία υπ' αρ. 115/2001 για την επεξεργασία των προσωπικών δεδομένων των εργαζομένων, τμήμα Ε', παρ. 6 – 8).

3.1.2.Επεξεργασία Ειδικών Κατηγοριών Δεδομένων προσωπικού χαρακτήρα μέσω συστημάτων βιντεοεπιτήρησης

Στη σημερινή εποχή που τα συστήματα βιντεοεπιτήρησης έχουν διευρύνει κατά πολύ το πεδίο τους, συλλέγοντας πολύ μεγάλο όγκο δεδομένων, μεταξύ αυτών και εικόνες που απαθανατίζουν στοιχεία ιδιαιτέρως προσωπικά, θα μπορούσε κάποιος να διερωτηθεί αν και υπό ποιες προϋποθέσεις η βιντεοεπιτήρηση συνιστά επεξεργασία δεδομένων ειδικών κατηγοριών.

Το **κομβικό στοιχείο** που διαφωτίζει ως προς τον ανωτέρω προβληματισμό είναι το κριτήριο του **σκοπού.** Όπως επισημαίνεται από το Ευρωπαϊκό Συμβούλιο Προστασίας

Δεδομένων, μέσω των Κατευθυντήριων Γραμμών του 3/2019, το τι αντιμετώπισης θα τύχουν τα δεδομένα έγκειται στον υπεύθυνο επεξεργασίας καθώς διαφέρει το να συλλεγούν και τέτοιου είδους δεδομένα παρεμπιπτόντως μεταξύ άλλων, από το να γίνει συλλογή αυτών επί τούτου. Στη δεύτερη περίπτωση , αν το υλικό αυτό υποβληθεί σε επεξεργασία με σκοπό την εξαγωγή συμπερασμάτων για ειδικές κατηγορίες δεδομένων, τότε εφαρμόζεται, κατ' αρχήν, **η παρ. 1** του **άρθρου 9 ΓΚΠΔ**, που αποτελεί τον **κανόνα περί απαγόρευσης** της **επεξεργασίας δεδομένων προσωπικού χαρακτήρα** που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και της επεξεργασίας γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό.

Εν συνεχεία, όμως, θα πρέπει να εξεταστεί αν μία ή περισσότερες εκ των περιπτώσεων απαγόρευσης εμπίπτουν στην **παρ. 2 του άρ.9 ΓΚΠΔ**, σύμφωνα με την οποία, παρατηρούνται **''εξαιρέσεις'' της γενικής απαγόρευσης, δηλαδή περιπτώσεις επιτρεπτής επεξεργασίας**.

Αυτές, σύμφωνα με το Γενικό Κανονισμό, είναι οι ακόλουθες. **Πρώτον,** η περίπτωση της ρητής συγκατάθεσης εκ του υποκειμένου των δεδομένων για την επεξεργασία των δεδομένων του για έναν ή περισσότερους συγκεκριμένους σκοπούς. Η θιγόμενη περίπτωση είναι ιδιάζουσα, καθώς προβλέπει την εξαίρεση της εξαίρεσης, δηλαδή την επαναφορά στον κανόνα της απαγόρευσης της επεξεργασίας, ορίζοντας ότι το δίκαιο της Ένωσης ή του κράτους- μέλους δύνανται να προβλέπουν ότι η απαγόρευση της επεξεργασίας δεν μπορεί να αρθεί από το υποκείμενο των δεδομένων.[161] Δεύτερον, 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 με το εθνικό δίκαιο με την παροχή κατάλληλων εγγυήσεων για τα θεμελιώδη δικαιώματα και τα συμφέροντα του υποκειμένου των δεδομένων (άρ.9 παρ. 2 στοιχ.β) ΓΚΠΔ). **Τρίτον,** η επεξεργασία είναι απαραίτητη για την προστασία ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου, αν το υποκείμενο είναι σωματικό ή νομικά ανίκανο προς συγκατάθεση (στοιχ.γ). **Τέταρτον,** η επεξεργασία διενεργείται στο πλαίσιο νόμιμων δραστηριοτήτων ιδρύματος, οργάνωσης ή άλλου μη κερδοσκοπικού φορέα με πολιτικό, φιλοσοφικό, θρησκευτικό ή συνδικαλιστικό στόχο και αφορά αποκλειστικά στα νυν ή πρώην μέλη ή τα πρόσωπα με τα οποία έχει τακτική επικοινωνία εν όψει των σκοπών

[161] Η συγκατάθεση δεν μπορεί να αποτελέσει αυτοτελή νομική βάση επεξεργασίας στο πλαίσιο ειδικών περιπτώσεων στις οποίες υπάρχει εμφανής ανισορροπία μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας κι εξ αυτού του λόγου καθίσταται απίθανο να πρόκειται για ελεύθερη συγκατάθεση υπό τις συγκεκριμένες περιστάσεις σε Βασιλοπούλου Ν. Ευαγγελία, 2018, σελ. 107

του (στοιχ. δ). **Πέμπτον,** η επεξεργασία αφορά σε δεδομένα που έχει προδήλως δημοσιοποιήσει το υποκείμενο (στοιχ. ε). **Έκτον,** η επεξεργασία είναι απαραίτητη για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων είτε σε δικαστική διαδικασία, είτε σε διοικητική είτε σε τυχόν εξωδικαστική διαδικασία ή όταν τα δικαστήρια ενεργούν υπό τη δικαιοδοτική τους ιδιότητα (στοιχ. στ). **Έβδομον,** η επεξεργασία είναι απαραίτητη για λόγους ουσιαστικού δημοσίου συμφέροντος, βάσει του δικαίου της Ένωσης ή κράτους μέλους (στοιχ.ζ). **Όγδοον,** η επεξεργασία είναι απαραίτητη για σκοπούς προληπτικής ή επαγγελματικής ιατρικής, εκτίμησης της ικανότητας προς εργασία, ιατρικής διάγνωσης, παροχής υγειονομικής ή κοινωνικής περίθαλψης ή θεραπείας ή διαχείρισης υγειονομικών και κοινωνικών συστημάτων και υπηρεσιών βάσει του δικαίου της Ένωσης ή του κράτους μέλους ή δυνάμει της σύμβασης με επαγγελματία του τομέα της υγείας και με την επιφύλαξη της διάταξης της παρ. 3, ήτοι υπό την προϋπόθεση ότι η επεξεργασία γίνεται από ή υπό τη ευθύνη επαγγελματία που υπόκειται στην υποχρέωση τήρησης του επαγγελματικού απορρήτου ή από πρόσωπο που υπέχει επίσης υποχρέωση τήρησης απορρήτου (στοιχ. η). **Ένατον**, η επεξεργασία είναι απαραίτητη για λόγους δημοσίου συμφέροντος στον τομέα της δημόσιας υγείας (στοιχ. θ) και **δέκατον**, η επεξεργασία είναι απαραίτητη για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς (στοιχ. ι).

Υποχρέωση του υπευθύνου επεξεργασίας, αν το σύστημα βιντεοεπιτήρησης χρησιμοποιείται για να γίνει επεξεργασία ειδικών κατηγοριών δεδομένων, αποτελεί ο προσδιορισμός **τόσο** μίας εκ των ως άνω περιοριστικά απαριθμούμενων στην παρ.2 περιπτώσεων **όσο** και μίας εκ των νομικών βάσεων του άρθρου 6 ΓΚΠΔ. Επιπλέον, κρίνεται ιδιαιτέρως σημαντικό στην επεξεργασία των εν λόγω κατηγοριών δεδομένων να πραγματοποιούνται <u>υψηλού επιπέδου εκτιμήσεις αντικτύπου (άρ. 35 παρ.1 και 2 στοιχ.β) ΓΚΠΔ)</u>, δηλαδή εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας ως προς την ασφάλεια και την προστασία των δεδομένων[162], καθώς η εξειδίκευση αυτή της νομοθετικής απαίτησης καταδεικνύει ότι τα ειδικών κατηγοριών δεδομένα, ανεξαρτήτως της επεξεργασίας που μπορεί να τεθούν - κυρίως δε τα βιομετρικά και τα γενετικά, για τη διαχείριση των οποίων είναι περισσότερο αυξημένες οι τεχνολογικές απαιτήσεις- επιφέρουν υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων σε βαθμό που η αυστηροποίηση της προστασίας τους να θεωρείται επιβεβλημένη, χωρίς αυτό να σημαίνει ότι δε δύνανται να τύχουν νόμιμης επεξεργασίας.[163]

3.1.3.Ταυτότητα και Ιδιαιτερότητα Βιομετρικών Δεδομένων

Σύμφωνα με το άρθρο 4 παρ. 14 ΓΚΠΔ και τη σκέψη 51 εδάφιο γ' ΓΚΠΔ, ως

[162] Κατευθυντήριες Γραμμές 3/2019, σελ.20

[163] Βασιλοπούλου Ν. Ευαγγελία, 2018, σελ. 109

''Βιομετρικά Δεδομένα νοούνται αυτά οποία 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''. Από τον προηγηθέντα ορισμό προκύπτουν **τρία βασικά στοιχεία- κριτήρια** που χαρακτηρίζουν τα βιομετρικά δεδομένα : **πρώτον**, το ότι έχουν ως αντικείμενο το άτομο και ιδιαιτέρως τα φυσικά, βιολογικά και συμπεριφορικά χαρακτηριστικά του (φύση των δεδομένων), **δεύτερον**, ότι είναι προϊόν ''ειδικής τεχνικής επεξεργασίας'' (μέσα και τρόπος επεξεργασίας) και **τρίτον,** ότι η χρήση τους αποσκοπεί στην αδιαμφισβήτητη ταυτοποίηση φυσικού προσώπου (σκοπός επεξεργασίας). Αναφορικά με τις εικόνες προσώπου, ουσιώδες να επισημανθεί βάσει της αιτιολογικής σκέψης 51 ΓΚΠΔ, ότι η επεξεργασία φωτογραφιών δε θεωρείται ότι αποτελεί σε κάθε περίπτωση επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων. Και τούτο διότι αυτές συνδέονται με τον ορισμό των βιομετρικών δεδομένων μόνο αν η επεξεργασία τους πραγματοποιήθηκε με τα συγκεκριμένα ''ειδικά τεχνικά μέσα'' που επιτρέπουν την άμεση σύνδεση με το άτομο, την αδιαμφισβήτητη ταυτοποίησή του.

Εξ αυτού του σημείου απορρέει και η **ιδιαιτερότητα των βιομετρικών δεδομένων**, καθώς είναι ιδιαιτέρως λεπτή η γραμμή που διαχωρίζει εν τοις πράγμασι τα ''ευαίσθητα''- ειδικών κατηγοριών προσωπικά δεδομένα και τον τρόπο και σκοπό επεξεργασίας τους σε σχέση με τα απλά. Και τούτο διότι στην εποχή της υπερπληροφόρησης και των υπερβολικά πολλών δυνατοτήτων, εγείρονται σοβαρές ανησυχίες από τη χρήση των βιομετρικών δεδομένων στον τομέα της ιδιωτικής ζωής και της προστασίας δεδομένων, λόγω των αυξημένων κινδύνων για τα δικαιώματα των υποκειμένων των δεδομένων. Ο κίνδυνος έγκειται στο ότι είναι δυνατόν να συλλέγονται, επί παραδείγματι, μέσω προφίλ φωτογραφιών στα μέσα κοινωνικής δικτύωσης, βιομετρικά δεδομένα εν αγνοία του προσώπου στο οποίο αναφέρονται λόγω του ότι αυτό αφήνει ίχνη ακουσίως, χωρίς να το γνωρίζει.[164] Τέτοιου είδους **συγκεκαλυμμένες τεχνικές συλλογής και αποθήκευσης/ επεξεργασίας υλικού**[165] που επιτρέπουν την **ταυτοποίηση του ατόμου** με αυτό τον τρόπο, **διαρρηγνύουν τη σφαίρα της ιδιωτικότητας**, καθώς η πρακτική χρήση των βιομετρικών δεδομένων υπερβαίνει τον αρχικό σκοπό και σταδιακά οδηγεί σε απώλεια του δικαιώματος πληροφοριακού αυτοπροσδιορισμού. Αντιθέτως, τα τεχνολογικά μέσα αναγνώρισης προσώπου οφείλουν να χρησιμοποιούνται με γνώμονα τις πρωτεύουσες αρχές της νομιμότητας, της αναγκαιότητας, της αναλογικότητας και της ελαχιστοποίησης, σύμφωνα με τα οριζόμενα στον ΓΚΠΔ (ως άνω αναλύθηκαν).

Εστιάζοντας στη μελέτη των εν λόγω βιομετρικών τεχνολογιών, συνειδητοποιεί κανείς

[164] ό.π. υποσημ. 162, σελ.104

[165] Παρατηρούνται ακόμη και συστήματα που συλλέγουν κρυφά πληροφορίες σχετικά με χαρακτηριστικά των ατόμων που αφορούν το συναισθηματικό τους κόσμο ή τη σωματική τους διάπλαση, αλλά και δεδομένα σχετικά με την υγεία τους (απουσία αναλογικότητας και επεξεργασία ευαίσθητων ''ευαίσθητων'' δεδομένων) σε Παναγοπούλου-Φερενίκη Κουτνατζή, 2013, σελ. 486

ότι τα λογισμικά συχνά βαρύνονται τόσο με εσφαλμένα αποτελέσματα ταυτοποίησης προσώπων όσο και με λανθασμένες διαπιστώσεις πρόβλεψης συμπεριφορών ως απόρροια της υποβαθμισμένης ποιότητας των δεδομένων κατά την επεξεργασία αλλά και του τρόπου εκπαίδευσης των αλγορίθμων – σε συνάρτηση με τα αναλυθέντα σε πρότερο κεφάλαιο. Εξ αιτίας αυτών των παραμέτρων, επέρχεται η παραβίαση της αρχής της ακρίβειας που αποτελεί μία εκ των σημαντικότερων αρχών επεξεργασίας των προσωπικών δεδομένων, αλλά διαπιστώνονται και πλείστες όσες διακρίσεις φυλετικές κι άλλες. Εκ των ως άνω συνάγεται ότι ο ''κίνδυνος'' ως έννοια διαδραματίζει σημαντικό ρόλο ως προς την επίδραση στην επεξεργασία των προσωπικών δεδομένων σε συνάρτηση με την εφαρμογή βασικών αρχών όπως της ελαχιστοποίησης (που αποτελεί κι απώτατο όριο για τους αλγορίθμους), της λογοδοσίας και της διαφάνειας.

Για τούτο το λόγο, κρίνεται σκόπιμο να γίνει αναφορά στο επόμενο κεφάλαιο στο προτεινόμενο από την Ευρωπαϊκή Επιτροπή σχέδιο Κανονισμού Τεχνητής Νοημοσύνης για τη δημιουργία σχετικού νομικού πλαισίου στηριζόμενου στην προσέγγιση βάσει κινδύνου αλλά και στην περίπτωση συστημάτων απομακρυσμένης βιομετρικής αναγνώρισης φυσικών προσώπων για σκοπούς δίωξης του εγκλήματος.

3.2.Συστήματα Τεχνητής Νοημοσύνης και Προσέγγιση βάσει κινδύνου

Επιχειρώντας την προσέγγιση του προς εξέταση ζητήματος, θεωρείται ορθό να αναφερθεί ότι η **ανάπτυξη της τεχνητής νοημοσύνης** και ο τρόπος με τον οποίο έχει ενσωματωθεί στους τομείς της οικονομίας, της υγείας, των εργασιακών σχέσεων, του ιδιωτικού βίου, της ηθικής, καθιστά απαραίτητο τόσο να διαχειριστεί κανείς με διαφορετικό τρόπο την παραδοσιακή έννοια του ''δικαίου'' όσο και να ενισχυθεί θεσμικά το ισχύον νομοθετικό πλαίσιο που την καλύπτει, προκειμένου η περαιτέρω εξέλιξή της να κάμψει κατά το δυνατόν τους προβληματισμούς που ανεγείρονται από την εφαρμογή της.[166]

Ως προς το κριτήριο διάκρισης εφαρμογών τεχνητής νοημοσύνης, σύμφωνα με την Ευρωπαϊκή Επιτροπή, έγκειται στο κατά πόσο είναι ή όχι «υψηλού κινδύνου». Τούτο πηγάζει από το εάν ο τομέας στον οποίο χρησιμοποιούνται οι εφαρμογές και η χρήση για την οποία προορίζονται, ενέχουν σημαντικούς κινδύνους, ιδίως από την άποψη

[166] Σύμφωνα με την υπ' αρ. 2017/C 288/01 Γνωμοδότηση της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής με θέμα «Η τεχνητή νοημοσύνη — Η επίδραση της τεχνητής νοημοσύνης στην (ψηφιακή) ενιαία αγορά, στην παραγωγή, στην κατανάλωση, στην απασχόληση και στην κοινωνία» της 31.8.2017, όπου γίνεται αναφορά στο ότι πρέπει να αναπτυχθούν νέες διαδικασίες τυποποίησης για την επαλήθευση και την επικύρωση των συστημάτων τεχνητής νοημοσύνης, οι οποίες θα πρέπει να βασίζονται σε μεγάλο φάσμα κανόνων, έτσι ώστε να καθίσταται δυνατή η αξιολόγηση και ο έλεγχος της ασφάλειας, της διαφάνειας, της αναγνωσιμότητας, της δυνατότητας λογοδοσίας και της ηθικής υπευθυνότητας των συστημάτων τεχνητής νοημοσύνης, διαθέσιμο σε https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A52016IE5369

προστασίας της ασφάλειας, των δικαιωμάτων των καταναλωτών και των θεμελιωδών δικαιωμάτων[167]. Τα κριτήρια αυτά πρέπει να συντρέχουν σωρευτικά για να θεωρηθεί μία εφαρμογή τεχνητής νοημοσύνης «υψηλού κινδύνου» και ως εκ τούτου κατά τον σχεδιασμό κανονιστικού πλαισίου για την τεχνητή νοημοσύνη πρέπει να τηρούνται συγκεκριμένες υποχρεωτικές νομικές απαιτήσεις. Οι νομικές αυτές απαιτήσεις αναλύονται από την **Ευρωπαϊκή Επιτροπή στη Λευκή Βίβλο για την Τεχνητή Νοημοσύνη**[168] και διαθέτουν **ορισμένα βασικά χαρακτηριστικά**, η διάσταση των οποίων θα ήταν ορθό να αποδοθεί εν συντομία.

3.2.1 Βασικά χαρακτηριστικά απαιτήσεων Λευκής Βίβλου για τις εφαρμογές Τεχνητής Νοημοσύνης ''υψηλού κινδύνου''

Πρώτο εκ των βασικών χαρακτηριστικών της Λευκής Βίβλου αναφορικά με τις **εφαρμογές Τεχνητής Νοημοσύνης ''υψηλού κινδύνου''** αποτελούν **τα δεδομένα εκπαίδευσης.** Η λειτουργία πολλών συστημάτων Τεχνητής Νοημοσύνης (ΤΝ), καθώς και οι δράσεις και οι αποφάσεις στις οποίες μπορούν να οδηγήσουν, εξαρτώνται σε μεγάλο βαθμό από το σύνολο των δεδομένων βάσει του οποίου έχουν εκπαιδευτεί τα συστήματα. Οι απαιτήσεις τις οποίες θα έπρεπε να πληρούν, αποσκοπούν τόσο στην παροχή εύλογων εγγυήσεων ότι η μεταγενέστερη χρήση των προϊόντων ή υπηρεσιών είναι ασφαλής και συμμορφούμενη με τις επιταγές των κανόνων της ΕΕ όσο και στη λήψη εύλογων μέτρων που θα εγγυώνται ότι η επακόλουθη χρήση των συστημάτων ΤΝ δε συντελεί στη δημιουργία διακρίσεων. Ακόμη, αποσκοπούν στη διασφάλιση της επαρκούς προστασίας της ιδιωτικότητας και των δεδομένων προσωπικού χαρακτήρα κατά τη χρήση προϊόντων και υπηρεσιών που βασίζονται στην ΤΝ. **Δεύτερο χαρακτηριστικό των απαιτήσεων** αποτελεί η **τήρηση αρχείων** σχετικά με τον **προγραμματισμό του αλγορίθμου** όπως και δεδομένων που χρησιμοποιούνται για την εκπαίδευση των συστημάτων ΤΝ ''υψηλού κινδύνου''. Και τούτο καθίσταται απαραίτητο λόγω της πολυπλοκότητας και της αδιαφάνειας πολλών συστημάτων ΤΝ αλλά και της συνεπαγόμενης δυσκολίας για την αποτελεσματική επαλήθευση της συμμόρφωσης με τους ισχύοντες κανόνες και την επιβολή τους. Το χρονικό διάστημα φύλαξης των αρχείων και του συνόλου των δεδομένων πρέπει να είναι περιορισμένο, εύλογο ώστε να διασφαλιστεί η αποτελεσματική εφαρμογή της σχετικής νομοθεσίας.

Επιπροσθέτως, προς επίτευξη της διαφάνειας, είναι ουσιώδης η **παροχή επαρκών πληροφοριών** σχετικά με τη χρήση συστημάτων ΤΝ ''υψηλού κινδύνου''. Πρέπει να δίδεται έμφαση στο σκοπό για τον οποίο προορίζονται τα συστήματα αλά και στην σαφή και τεκμηριωμένη ενημέρωση των πολιτών όταν βρίσκονται σε αλληλεπίδραση

[167] Ανδρουλάκη Ευαγγελία, ''Τεχνητή νοημοσύνη και προσωπικά δεδομένα: η περίπτωση της εξ αποστάσεως βιομετρικής ταυτοποίησης'', *Επιθεώρηση Δικαίου Πληροφορικής*, Τομ.1, αρ.1 (2021), σελ.6, διαθέσιμο σε https://ejournals.lib.auth.gr/infolawj/article/view/8236

[168] Λευκή Βίβλος -- Τεχνητή νοημοσύνη - Η ευρωπαϊκή προσέγγιση της αριστείας και της εμπιστοσύνης, της Ευρωπαϊκής Επιτροπής, COM (2020) 65 final της 19.2.2020, σελ. 23-27, διαθέσιμο σε https://op.europa.eu/el/publication-detail/-/publication/ac957f13-53c6-11ea-aece-01aa75ed71a1

με σύστημα ΤΝ. **Μία ακόμη απαίτηση**, σύμφωνα με τη Λευκή βίβλο, είναι αυτή της **στιβαρότητας** και της **ακρίβειας** από την οποία θα πρέπει να διέπονται τα συστήματα ΤΝ. Τα δύο αυτά στοιχεία προσδίδουν αξιοπιστία και αποτελούν θεμελιώδεις προϋποθέσεις λήψης όλων των εύλογων μέτρων για την ελαχιστοποίηση του κινδύνου πρόκλησης βλάβης. **Η πέμπτη απαίτηση** αφορά στην **ανθρώπινη εποπτεία**. Η ύπαρξη και ανάδειξη του στοιχείου αυτού αποτελεί κομβικό παράγοντα για την επίτευξη μιας αξιόπιστης, ηθικής και ανθρωποκεντρικής ΤΝ, καθώς διασφαλίζεται η ανθρώπινη συμμετοχή και συνεισφορά με τον κατάλληλο τρόπο και τα ενδεικνυόμενα μέσα στις εφαρμογές ΤΝ ''υψηλού κινδύνου''. Ταυτοχρόνως, όπως επισημαίνεται στη Λευκή Βίβλο, δε θίγονται τα νόμιμα δικαιώματα που κατοχυρώνονται στο Γενικό Κανονισμό, όταν ένα σύστημα ΤΝ επεξεργάζεται δεδομένα προσωπικού χαρακτήρα κι επιπλέον θα μπορούσε να παρέχεται κι η δυνατότητα παρακολούθησης του συστήματος ΤΝ , στο πλαίσιο της εποπτείας, ενώ αυτό βρίσκεται σε λειτουργία και να λάβει χώρα παρέμβαση σε πραγματικό χρόνο και πιθανή απενεργοποίησή του, αν αυτό κριθεί αναγκαίο.

Τέλος, αποτελεί αδήριτη ανάγκη να επισημανθούν οι **ειδικές απαιτήσεις για την εξ αποστάσεως βιομετρική ταυτοποίηση.** Η εξ αποστάσεως βιομετρική ταυτοποίηση είναι η ταυτοποίηση που γίνεται όταν προσδιορίζεται εξ αποστάσεως η ταυτότητα πολλών ατόμων με τη χρήση βιομετρικών αναγνωριστικών στοιχείων, όπως για παράδειγμα των δακτυλικών αποτυπωμάτων, της εικόνας προσώπου, της ίριδας των ματιών κ.λπ., σε δημόσιο χώρο, συνεχώς ή εξακολουθητικά, μέσω της αντιπαραβολής τους με δεδομένα που ήδη υπάρχουν σε συγκεκριμένες βάσεις δεδομένων.[169] Από αυτή τη διαδικασία προκύπτει αν το υπόδειγμα των βιομετρικών δεδομένων συγκεκριμένου προσώπου είναι αποθηκευμένο σε βάση δεδομένων, στην οποία συμπεριλαμβάνονται πολλά υποδείγματα.[170]

Η τεχνολογία αναγνώρισης προσώπου που χρησιμοποιείται από τις εφαρμογές τεχνητής νοημοσύνης είναι αυτή που συντελεί στο να πραγματοποιηθεί η σύγκριση πολλών ψηφιακών εικόνων προσώπου ώστε να διαπιστωθεί αν ανήκουν στο ίδιο φυσικό πρόσωπο, επιτρέποντας την αυτόματη ταυτοποίηση ενός ατόμου κατόπιν αντιστοίχισης δύο ή περισσότερων προσώπων από ψηφιακές εικόνες. Ενδιαφέρον παρουσιάζει το πώς επιτυγχάνεται αυτό το αποτέλεσμα, καθώς ανιχνεύονται και μετρώνται διάφορα χαρακτηριστικά του προσώπου τα οποία η συγκεκριμένη τεχνολογία εξάγει από την εικόνα κι εν συνεχεία τα συγκρίνει με χαρακτηριστικά που λαμβάνει από άλλα πρόσωπα.[171]

Τα βιομετρικά δεδομένα, όπως έχει καταστεί σαφές, αποτελούν ειδική κατηγορία δεδομένων προσωπικού χαρακτήρα, γεγονός που έχει ως αποτέλεσμα την πρόκληση

[169] E. Syta, M. J. Fischer, D. Wolinsky, A. Silberschatz, G. Gallegos-Garcia and B. Ford, Private Eyes: Secure Remote Biometric Authentication (2015), διαθέσιμο σε https://dedis.cs.yale.edu/dissent/papers/secrypt15-biometric.pdf

[170] Ανδρουλάκη Ευ., 2021, σελ.7

[171] L. Introna and H. Nissenbaum, Facial Recognition Technology: A Survey of Policy and Implementation Issues, Lancaster University Management School Working Paper 2010/030

κινδύνων για θεμελιώδη δικαιώματα στην περίπτωση συλλογής και χρήσης τους από εφαρμογές τεχνητής νοημοσύνης με σκοπό την εξ αποστάσεως βιομετρική ταυτοποίηση και για αυτό το λόγο θα πρέπει να τυγχάνουν ειδικής προστασίας. Καθώς υπάγονται στην παράγραφο 2 του άρθρου 9 ΓΚΠΔ, η **επεξεργασία** τους είναι δυνατή κατ' εξαίρεση, ήτοι **μόνο για συγκεκριμένους λόγους**, με τη ύπαρξη του **ουσιαστικού δημοσίου συμφέροντος** να αποτελεί **τον σημαντικότερο εξ αυτών.**

Καταλυτική στην περίπτωση της εν λόγω επεξεργασίας, η οποία πραγματοποιείται βάσει του δικαίου της ΕΕ ή των κρατών μελών, είναι η τήρηση των απαιτήσεων αναλογικότητας, η ύπαρξη σεβασμού του δικαιώματος στην προστασία των δεδομένων, των κατάλληλων και επαρκών εγγυήσεων και της πλήρους αιτιολογίας για τη συγκεκριμένη επεξεργασία, όταν υφίσταται αυστηρή ανάγκη.

Στο πλαίσιο των απαιτήσεων της αναλογικότητας, ιδιαιτέρως σημαντική πτυχή της αξιολόγησης επάρκειας ενός συστήματος τεχνητής νοημοσύνης που χρησιμοποιεί βιομετρικά δεδομένα είναι η επισκόπηση της δυνατότητας επίτευξης του επιδιωκόμενου σκοπού με τις λιγότερες επιπτώσεις σε βάρος της ιδιωτικότητας.[172]

Ως προς τις επιπτώσεις στα θεμελιώδη δικαιώματα από τη χρήση συστημάτων Τεχνητής Νοημοσύνης για την εξ αποστάσεως βιομετρική ταυτοποίηση, δύναται να διαφέρουν σε σημαντικό βαθμό αναλόγως του σκοπού, του πλαισίου και του πεδίου εφαρμογής της χρήσης.[173]

Το συνηθέστερο ζήτημα που προκύπτει ως προς την παραβίαση των θεμελιωδών δικαιωμάτων είναι ο κίνδυνος σφαλμάτων των εν λόγω συστημάτων τεχνητής νοημοσύνης στην αντιστοίχιση προσώπων, με ενδεχόμενη απορρέουσα παραβίαση του δικαιώματος στην ανθρώπινη αξιοπρέπεια, των δικαιωμάτων στο σεβασμό της ιδιωτικής ζωής και στον πληροφοριακό αυτοκαθορισμό, όπως και διαπίστωση περί διακρίσεων εις βάρος ειδικών ομάδων όπως τα παιδιά, οι ηλικιωμένοι και τα άτομα με αναπηρία.[174]

Η επέκταση του κινδύνου εν δυνάμει λαμβάνει χώρα και στην επίδραση λειτουργίας του δημοκρατικού πολιτεύματος λόγω του συνεχούς περιορισμού της ιδιωτικής ζωής. Όπως επισημαίνεται στην Ετήσια Έκθεση του Βρετανού Επιτρόπου Βιομετρικών Στοιχείων, παρατηρείται κίνδυνος για εσφαλμένα αποτελέσματα λόγω ατελών αλγορίθμων στην τεχνολογία αναγνώρισης προσώπου που χρησιμοποιείται από την Αστυνομία του Ηνωμένου Βασιλείου προβαίνοντας σε διακρίσεις ως προς εσφαλμένη αναγνώριση κυρίως γυναικών και έγχρωμων ατόμων.[175]

---

[172] Φ. Παναγοπούλου-Κουτνατζή, Βιομετρικές μέθοδοι και προστασία ιδιωτικότητας: Σκέψεις με αφορμή την απόφαση ΔΕΕ Michael Schwarz κατά κρατιδίου Bochum (C-291/2012), *ΔΙΤΕ (π. ΔΙΜΕΕ)*, τεύχος 4/2013, Οκτώβριος- Νοέμβριος- Δεκέμβριο, σελ. 488

[173] ό.π. υποσ 168, σελ.27 (Ευρωπαϊκή Επιτροπή, Λευκή Βίβλος για την Τεχνητή Νοημοσύνη)

[174] ό.π.υποσ 167, σελ.14 (Ανδρουλάκη Ευ.)

[175] ό.π.υποσ 167, σελ.15

Εκ των ανωτέρω συνάγεται η σπουδαιότητα της δεόντως αιτιολογημένης και αναλογικής χρήσης της ΤΝ σχετικά με την εξ αποστάσεως βιομετρική ταυτοποίηση αλλά και της παροχής επαρκών εγγυήσεων.

3.2.2. Σχέδιο Κανονισμού Ε.Ε. για την Τεχνητή Νοημοσύνη για τη δημιουργία νομικού πλαισίου στηριζόμενου στην προσέγγιση βάσει κινδύνου

Λαμβάνοντας υπόψιν το εύρος του κινδύνου σε σχέση με την επίδραση που ασκεί στην ασφάλεια και τα θεμελιώδη ατομικά δικαιώματα πολιτών και επιχειρήσεων, η Ευρωπαϊκή Επιτροπή προτείνει τη δημιουργία σχετικού νομικού πλαισίου εστιάζοντας στη διαβάθμιση του επιπέδου κινδύνου και στην αντίστοιχη κατηγοριοποίηση των συστημάτων Τεχνητής Νοημοσύνης βάσει αυτού. Ως εκ τούτου, θεωρείται ορθό να παρατεθεί **η διάκριση** σε : **α)** ***«μη αποδεκτού κινδύνου»***, που απαγορεύονται πλήρως, **β) «*υψηλού κινδύνου*»,** των οποίων η κατασκευή και χρήση υπόκειται σε αυστηρές υποχρεώσεις προτού επιτραπεί η διάθεση και η κυκλοφορία τους στην αγορά**, γ) «*περιορισμένου κινδύνου*»**, των οποίων η χρήση επιτρέπεται υπό συγκεκριμένες υποχρεώσεις διαφάνειας και **δ) «*ελαχίστου κινδύνου*»,** των οποίων η χρήση επιτρέπεται χωρίς την επιβολή υποχρεώσεων με βάση την πρόταση σχεδίου Κανονισμού ΤΝ. [176]

Ως προς τη δεύτερη κατά σειρά περίπτωση των **συστημάτων ΤΝ «*υψηλού κινδύνου*»,** είναι απαραίτητο να αξιολογηθούν ως προς τη συμμόρφωση προς τις απαιτήσεις του Κανονισμού ΤΝ, προτού τεθούν σε κυκλοφορία στην αγορά και αξιολογηθούν. Οι εν λόγω **απαιτήσεις** προσδιορίζονται στις κάτωθι: *πρώτον*, εγκατάσταση και λειτουργία συστήματος εποπτείας και διαχείρισης κινδύνου καθ' όλο τον κύκλο ζωής του ελεγχόμενου συστήματος ΤΝ, *δεύτερον*, τήρηση κανόνων για τη χρήση δεδομένων αναγκαίων για την εκπαίδευση των αλγοριθμικών συστημάτων, *τρίτον*, τεχνική τεκμηρίωση του συστήματος ΤΝ προ της θέσης σε κυκλοφορία στην αγορά, *τέταρτον*, σχεδιασμό και ανάπτυξη του συστήματος ΤΝ κατά τρόπο ώστε να διατηρεί αυτόματες καταγραφές συμβάντων (logs) με περαιτέρω δυνατότητα αναγνώρισης προτύπων ή κοινά αποδεκτών χαρακτηριστικών που θα καθιστούν εφικτή την ιχνηλάτηση του συστήματος, *πέμπτον*, υποχρεώσεις διαφάνειας ώστε οι χρήστες των συστημάτων ΤΝ να μπορούν να ερμηνεύουν το εξαγόμενο αποτέλεσμα του συστήματος και να το χρησιμοποιούν συναφώς και υποχρέωση ανθρώπινης επίβλεψης κατά τη λειτουργία του συστήματος και σχεδιασμός του συστήματος ώστε να επιτυγχάνεται το κατάλληλο επίπεδο ακρίβειας, διαθεσιμότητας και κυβερνοασφάλειας (άρθρα 8-15 σχεδίου Καν ΤΝ και περαιτέρω εξειδίκευση τους στα

[176] Τσόλιας Γρηγόρης, ''Η αναγνώριση και ταυτοποίηση προσώπων για σκοπούς δίωξης του εγκλήματος σύμφωνα με το Σχέδιο Κανονισμού Ε.Ε. για την Τεχνητή Νοημοσύνη'', 13/05/2021, διαθέσιμο σε https://www.lawspot.gr/nomika-nea/i-anagnorisi-kai-taytopoiisi-prosopon-gia-skopoys-dioxis-toy-egklimatos-symfona-me-shedio (Το κείμενο αποδίδει εμπλουτισμένη προφορική εισήγηση στην εκδήλωση του IAPP Knowledge Net Chapter Greece της 06.5.2021)

άρθρα 16-29 σχεδίου Καν ΤΝ).

Αναφορικά με τον έλεγχο πλήρωσης των απαιτούμενων υποχρεώσεων ανατίθεται σε ειδικές ελεγκτικές αρχές οι οποίες θα προβαίνουν στην σχετική επιβεβαίωση και η οποία μπορεί να συνίσταται και στην έκδοση πιστοποιητικών συμβατότητας (άρ. 44 σχ. Καν. ΤΝ) ή δήλωση συμμόρφωσης της ΕΕ με σήμανση CE (άρ. 48-49 σχ. Καν. ΤΝ). Προτού κυκλοφορήσει στην αγορά, το σύστημα ΤΝ υψηλού κινδύνου, εφόσον έχει διέλθει επιτυχώς των προηγούμενων ελέγχων, καταχωρείται σε ειδική βάση δεδομένων της Ε.Ε. (άρ. 51 και 60 σχ. Καν ΤΝ). Μετά την κυκλοφορία του συστήματος ΤΝ υψηλού κινδύνου στην αγορά, το σχ. Καν ΤΝ περιλαμβάνει ένα δεύτερο στάδιο υποχρεώσεων συμμόρφωσης που περιλαμβάνουν την εγκατάσταση και λειτουργία συστήματος παρακολούθησης του συστήματος ΤΝ, την υποχρεωτική υποβολή αναφοράς σοβαρού συμβάντος ή δυσλειτουργίας τους συστήματος ΤΝ που οδηγεί σε παραβίαση υποχρεώσεων του δικαίου της Ε.Ε. για την προστασία ατομικών και θεμελιωδών δικαιωμάτων.[177]

3.2.3. Τα συστήματα απομακρυσμένης βιομετρικής αναγνώρισης φυσικών προσώπων για σκοπούς δίωξης του εγκλήματος βάσει Σχεδίου Κανονισμού Τεχνητής Νοημοσύνης

Στο σημείο αυτό αξίζει να σημειωθεί το τι προβλέπεται στο Σχέδιο Κανονισμού ΤΝ αναφορικά με την περίπτωση των συστημάτων απομακρυσμένης βιομετρικής αναγνώρισης και ταυτοποίησης φυσικών προσώπων για σκοπούς δίωξης του εγκλήματος.

Σε συνάρτηση με τα όσα ως άνω αναλύθηκαν, στο άρθρο 4 περ.36 του σχ. Καν. ΤΝ υπογραμμίζεται το ότι στα βιομετρικά δεδομένα προσώπου που τίθενται προς σύγκριση σε σχέση με αυτά που περιλαμβάνονται σε μια βάση δεδομένων αναφοράς, δεν είναι δυνατό να υπάρχει πρότερη γνώση του χειριστή του συστήματος (π.χ. Αστυνομία) αν το πρόσωπο που διερευνάται θα είναι παρόν και είναι δυνατόν να γίνει ταυτοποίησή του κατά τη λειτουργία του συστήματος.

Επιπλέον, **στο άρθρο 3** περιπτώσεις 37 και 38 του σχ. Καν. ΤΝ, λαμβάνει χώρα διάκριση μεταξύ μεταξύ συστήματος απομακρυσμένης βιομετρικής αναγνώρισης/ταυτοποίησης που λειτουργεί σε **πραγματικό χρόνο** (real-time RBI) και προβαίνει σε άμεση ή με ελάχιστη καθυστέρηση, ταυτοποίηση (**περ. 37**) και συστήματος που λειτουργεί **ετεροχρονισμένα** (post RBI) και προβαίνει σε ταυτοποίηση όχι σε πραγματικό χρόνο αλλά μεταγενέστερα (**περ. 38**), όπως επίσης διακρίνονται και σε ταυτοποιούμενα σε δημοσίως προσβάσιμους χώρους και μη (περ.39).

Επιχειρώντας σύνδεση με την ενότητα διαβάθμισης του κινδύνου, αποτελεί αδήριτη

[177] ό.π. υποσ 176

ανάγκη να αναφερθεί ότι **τα συστήματα απομακρυσμένης βιομετρικής αναγνώρισης /ταυτοποίησης** συμπεριλαμβάνονται στην **κατηγορία συστημάτων ΤΝ υψηλού κινδύνου** που λειτουργούν **είτε** σε πραγματικό χρόνο (real-time RBI) **είτε** ετεροχρονισμένα **είτε** χρησιμοποιούνται από ιδιώτες, **είτε** από αρμόδιες δημόσιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης και δίωξης ποινικών αδικημάτων (άρθρο 6 σε συνδυασμό με το Παράρτημα ΙΙΙ περ. 1 α' και περ. 6' του σχ. Καν ΤΝ).

Αντιθέτως όταν συντρέχουν σωρευτικά τα κάτωθι στοιχεία i) λειτουργία σε πραγματικό χρόνο, ii) σε δημοσίως προσβάσιμους χώρους και iii) για σκοπούς επιβολής του νόμου, η χρήση συστήματος ΤΝ απαγορεύεται, καθώς εμπίπτουν στην κατηγορία του ''μη αποδεκτού κινδύνου'' (άρ. 5 παρ. 1 περ. δ'). Κατ' εξαίρεσιν είναι επιτρεπτή και αυστηρώς αναγκαία αν πρόκειται για τους επόμενους τρεις σκοπούς:

α. τη στοχευμένη αναζήτηση πιθανών θυμάτων εγκλημάτων, περιλαμβανομένων εξαφανισμένων παιδιών

β. την πρόληψη επέλευσης συγκεκριμένης, σοβαρής και άμεσης απειλής για τη ζωή ή τη φυσική ασφάλεια φυσικών προσώπων ή τρομοκρατικών επιθέσεων

γ. την ανίχνευση, εντοπισμό, αναγνώριση και δίωξη δράστη εγκλήματος ή υπόπτου ενός εκ των 32 ποινικών αδικημάτων που περιλαμβάνονται στον κατάλογο της ''Απόφασης - Πλαίσιο'' για το ευρωπαϊκό ένταλμα σύλληψης και εφόσον τιμωρείται και κατά το δίκαιο του κράτους-μέλους που αφορά με ποινή με ανώτατο όριο τουλάχιστον τα 3 έτη στέρησης της ελευθερίας.

Κατά την εξέταση και της παρούσας πτυχής, διαπιστώνεται η απαίτηση να συμφωνεί η χρήση των συστημάτων ΤΝ προς τις απαραίτητες και ανάλογες **εγγυήσεις** *σε συνάρτηση με* περιορισμούς τόσο χρονικούς και γεωγραφικούς όσο και προσωπικούς. Τη σπουδαιότερη εκ των εγγυήσεων αποτελεί η υποχρέωση προηγούμενης αδειοδότησης της λειτουργίας των συστημάτων σε πραγματικό χρόνο σε δημοσίως προσβάσιμους χώρους και παρεχόμενη από ανεξάρτητη και αμερόληπτη δικαστική/διοικητική αρχή. Επίσης το αίτημα της Αρχής πρέπει να είναι αιτιολογημένο, συνοδευόμενο από αντικειμενικές αποδείξεις ή εναργείς ενδείξεις στο πλαίσιο της αναλογικότητας σε σχέση με τους επιδιωκόμενους σκοπούς .

Στο πλαίσιο αυτό πρέπει να πληρούνται τα κριτήρια που προβλέπονται στο άρ. 5 (παρ.2) σχετικά με τη λήψη και το μεταγενέστερο έλεγχο νομιμότητας της απόφασης για τη χρήση του συστήματος και να προκύπτουν βάσει εναργών και αναλυτικών ρυθμίσεων περιλαμβανομένων σε διατάξεις της εθνικής νομοθεσίας, αποδεικνύοντας με αυτό τον τρόπο την εναρμόνιση με τις απαιτήσεις συμβατότητας προς τις διατάξεις του ΧΘΔΕΕ και ΕΣΔΑ καθώς και τη σχετική νομολογία τόσο του ΕΔΔΑ όσο κυρίως του Δικαστηρίου της ΕΕ.

Εν κατακλείδι, το ενδεχόμενο χρήσης των συστημάτων απομακρυσμένης βιομετρικής ταυτοποίησης σε δημοσίως προσβάσιμους χώρους σε πραγματικό χρόνο (real time RBI) έγκειται στη διακριτική ευχέρεια του κάθε κράτους μέλους σχετικά με το αν αυτή θα επιτραπεί ή όχι (άρ. 5 παρ. 4, αιτ. σκ. 22), αλλά με τους όρους και τις

εγγυήσεις που αναφέρονται στις προηγούμενες παραγράφους που θα ενσωματωθούν στον εθνικό νόμο και πλέον αυτού θα γίνεται προσδιορισμός της αρμόδιας αρχής που θα παρέχει την άδεια για τη χρήση των συστημάτων αυτών για λόγους επιβολής του νόμου. [178]

3.3. Τρεις αξιοσημείωτες περιπτώσεις καταστρατήγησης του δικαιώματος της ιδιωτικότητας μέσω εφαρμογής της τεχνολογίας

Κατόπιν της εκτενούς αναφοράς στα συστήματα Τεχνητής Νοημοσύνης και την προσέγγισή τους με βάση τον κίνδυνο, αλλά και τον αντίκτυπο αυτού στα θεμελιώδη ανθρώπινα δικαιώματα, κρίνεται ουσιώδες, βαίνοντας προς την ολοκλήρωση της παρούσας μελέτης, να θιγούν τρεις περιπτώσεις στο πλαίσιο της ανησυχίας που προκαλείται λόγω της καταστρατήγησης ενός εκ των θεμελιωδών ανθρωπίνων δικαιωμάτων, αυτού της ιδιωτικότητας, και αφορούν στο λεγόμενο ''σύνδρομο της Κίνας'', αλλά και στον τρόπο δράσης δύο εταιρειών (της Geofeedia και της Clearview) που προέβησαν σε παρακολούθηση στοιχείων ιδιωτών από τα μέσα κοινωνικής δικτύωσης κι άλλες πηγές στο διαδίκτυο και παρείχαν υπηρεσίες μέσω συστημάτων αναγνώρισης προσώπου σε εταιρείες και αστυνομικές αρχές προς επιβολή του νόμου, αλλά και διευκόλυνση εξιχνίασης εγκλημάτων.

3.3.1. Το ''Σύνδρομο της Κίνας'' ως μορφή συστήματος αυτοματοποιημένου κοινωνικού ελέγχου

Μία εκ των πιο γνωστών εφαρμοζόμενων πρακτικών αυτοματοποιημένων συστημάτων κοινωνικού ελέγχου, σε διεθνές επίπεδο, είναι αυτή της Κίνας, που στηρίζεται στην τεχνολογία τεχνητής νοημοσύνης και στην εξ αποστάσεως βιομετρική παρακολούθηση. Σύμφωνα με στοιχεία που δόθηκαν στη δημοσιότητα, ήδη από το 2014 βρίσκεται σε λειτουργία, με συνεχή επέκταση, ένα σύστημα μαζικής συλλογής πληροφοριών για **σκοπούς αυτοματοποιημένου Κοινωνικού Ελέγχου το οποίο έχει ποικίλες διαστάσεις (Social Credit System)** , επισημαίνοντας ότι το 2019 βρίσκονταν υπό μαζική παρακολούθηση περί το 1,4 δισεκατομμύριο πολίτες.[179] Προκειμένου να ευδοκιμήσει το εν λόγω σύστημα πραγματοποιείται συνεργασία μεταξύ κυβέρνησης, αστυνομίας και κρατικών υπηρεσιών (όπως η Κεντρική Τράπεζα της Κίνας) και εταιρειών κατασκευής εξοπλισμού τηλεπικοινωνιών, υψηλής τεχνολογίας και συστημάτων αναγνώρισης προσώπου, τραπεζών, εταιρειών μίσθωσης οχημάτων ταξί, κοινωνικών δικτύων και υπηρεσιών ανταλλαγής μηνυμάτων, καθώς και κολοσσών

[178] ό.π. υποσ 176 (τα ως άνω ρηθέντα φαίνεται ότι δε συμπεριλαμβάνουν τις περιπτώσεις χρήσης συστημάτων ΤΝ ετεροχρονισμένης λειτουργίας – post RBI)
[179] Κανέλλος, 2020, σελ.260

διαδικτυακής αναζήτησης και ηλεκτρονικού εμπορίου. Η **μέθοδος που ακολουθούν** συνίσταται στη **συλλογή και ανταλλαγή μαζικών δεδομένων (των λεγόμενων ''big data'') των πολιτών από διάφορες πηγές** όπως αγορές σε φυσικά και ηλεκτρονικά καταστήματα, από αρχεία ληξιαρχείων, κάμερες οι οποίες είχαν τοποθετηθεί σε δημόσιους χώρους και κρατικά κτήρια, αντληθέντα κατά τις ηλεκτρονικές αγορές στοιχεία, μέσω κοινωνικών επαφών αλλά φυσικά κι από το αναρτηθέν υλικό στα μέσα κοινωνικής δικτύωσης.

Η σύλληψη της ιδέας εφαρμογής αυτού του παράταιρου συστήματος εδράζεται σε φιλοσοφικό υπόβαθρο, τόσο στον πυρήνα της διδασκαλίας του Κομφούκιου περί ανάπτυξης αρετών του ιδανικού πολίτη, ο οποίος θα διακρίνεται για την καλή φήμη και την ειλικρίνειά του (το λεγόμενο ''xin''), στοιχεία που δύνανται να συμβάλλουν στη διεκδίκηση κυβερνητικών αξιωμάτων, όσο και στις αρχαίες κινεζικές παραδόσεις περί της σημασίας της ηθικής και της αξιοκρατίας. Η **αξιολόγηση της εντιμότητας και της αξιοπιστίας των πολιτών** δύναται να αποτυπωθεί εμπράκτως μέσω μηχανισμών καταγραφής και βιντεοεπιτήρησης κάθε τους κίνησης σε διάφορες στιγμές της καθημερινότητάς τους είτε είναι πεζοί είτε κινούνται με αυτοκίνητο είτε αναπαράγουν κάποιο άρθρο μέσω ανάρτησής τους στα μέσα κοινωνικής δικτύωσης. Αναλόγως της **αποτίμησης της συμπεριφοράς** τους, **προστίθενται ή αφαιρούνται πόντοι σε έκαστο πολίτη**, βάσει της υποχρεωτικότητας συμπερίληψης του συνόλου των Κινέζων πολιτών από το 2020 κι έπειτα στο εν λόγω σύστημα. Η διαδικασία πραγματοποιείται μέσω της εφαρμογής κινητής τηλεφωνίας της εταιρείας ηλεκτρονικού εμπορίου και πληρωμών Alibaba, η οποία είναι υπεύθυνη διαχείρισης μιας βαθμολογικής κλίμακας από 350 έως 950 πόντους. Αποσκοπώντας στην επιτυχή λειτουργία της κολοσσιαίας διαδικασίας συλλογής στοιχείων και επεξεργασίας αυτών[180], το κράτος προέβη στη δημιουργία ''φαρμών τεχνητής νοημοσύνης'' (AI farms) , στις οποίες **χιλιάδες εργαζόμενοι αναλύουν και εκπαιδεύουν σε καθημερινή βάση αλγορίθμους μηχανικής μάθησης και αναγνώρισης εικόνων.**[181] Ακόμη και το κεντρικό αρχείο εθνικής ασφαλείας, στο οποίο περιλαμβάνονται στοιχεία για ομάδες πολιτών όπως αντιφρονούντες, αλλόθρησκοι (π.χ. μουσουλμάνοι), εθνικές μειονότητες και μετανάστες, χρησιμοποιείται από τις κρατικές υπηρεσίες προς παρακολούθηση και αξιολόγησή τους, σύμφωνα με το περιγραφόμενο σύστημα.

Ο τρόπος λειτουργίας του συστήματος στηρίζεται συνδυαστικά σε κριτήρια του μυστικού αλγορίθμου αξιολόγησης της ως άνω εταιρείας και στη χρήση τεχνικών

[180] Προκειμένου να καταστεί προσδιορίσιμο το εύρος της διαδικασίας, να αναφερθεί ότι στην πόλη Chongquing η οποία έχει πληθυσμό 15,3 εκατομμύρια κατοίκους, έχουν εγκατασταθεί περισσότερες από 2,5 εκ. κάμερες ασφαλείας (κλειστού κυκλώματος τηλεόρασης – CCTV) , Jane Zhang ''In Chongquing, the world's most surveilled city, residents are happy to trade privacy for security'', Οκτώβριος 2019, διαθέσιμο σε https://www.scmp.com/tech/policy/article/3031390/chongqing-worlds-most-surveilled-city-these-residents-are-happy-trade

[181] Charlie Campbell, ''The entire system is designed to suppress us''. What the Chinese Surveillance state means for the rest of the world, Νοέμβριος 2019, διαθέσιμο σε https://time.com/5735411/china-surveillance-privacy-issues/

τεχνητής νοημοσύνης. Αποτέλεσμα αυτού η διαμόρφωση **προτύπων** που αποτελούν τις σταθερές πάνω στις οποίες δομείται η **''ορθή και ηθική κοινωνική συμπεριφορά''** που αναπαράγεται επαναλαμβανόμενα.[182] Εξ αυτών συμπεραίνει κανείς ότι μέσω αυτού του συστήματος καταργείται η βασική αρχή της ''διαφάνειας'', καθώς η ποιότητα μιας πράξης, ήτοι το αν κρίνεται ως ''καλή'' ή ''κακή'', συνεπάγεται συλλογή ή αφαίρεση πόντων, παραπέμποντας στο ελληνικό σύστημα των ποινών επί κυκλοφοριακών παραβάσεων. Οι πόντοι που συλλέγονται προσφέρουν διάφορα **προνόμια στους νομοταγείς πολίτες** όταν εξαργυρωθούν σε καίριους τομείς όπως η εκπαίδευση (τα παιδιά τους δύνανται να φοιτούν σε σχολεία υψηλού επιπέδου), η οικονομία σε συνδυασμό με το εμπόριο (τους παρέχουν σημαντικές εκπτώσεις κατά τις αγορές σε καταστήματα) κ.λπ., και η αρχή αυτή της ''επιβράβευσης'' των, κατά τα δικά τους μέτρα και σταθμά, εντίμων πολιτών και αντιστοίχως η τιμωρία των παραβατών και όλων όσοι δε συμμορφώνονται, εδράζεται στο οργουελιανό σύστημα ''Κοινωνικού ελέγχου'', το οποίο προωθούν προς εξαγωγή σε ξένες κυβερνήσεις, σε συνδυασμό με την τεχνολογία τους, έχοντας ως απώτερο στόχο, όπως παρατηρεί ο κ. Κανέλλος, την αύξηση της επιρροής της Κίνας σε πολιτικό επίπεδο.

Στο πλαίσιο, λοιπόν, της πρόληψης ή επαναφοράς/διόρθωσης κάθε συμπεριφοράς αντίθετης με τους αποδεκτούς κοινωνικούς κανόνες και αξίες, παρουσιάζεται έμπρακτο παράδειγμα διαπόμπευσης, καθώς το 2019 **κατόπιν διαταγής κινεζικού δικαστηρίου,** προβλήθηκαν **φωτογραφίες οφειλετών φόρων στην εφορία (συμπεριλαμβανομένων του ονοματεπωνύμου και του ύψους της κάθε οφειλής) σε οθόνη κινηματογράφων, προτού ξεκινήσει η προβολή δημοφιλούς ταινίας.**[183] Το εν λόγω σύστημα επιβράβευσης ή τιμωρίας πολιτών δεν προβαίνει σε διακρίσεις, αφού έχει γνωστοποιηθεί ότι έχει απαγορευτεί η επιβίβαση σε αεροπλάνο ή η δυνατότητα παρακολούθησης εκπαιδευτικών διά ζώσης σεμιναρίων στο εξωτερικό, ακόμη και σε δικηγόρους ή δημοσιογράφους λόγω του ότι κρίθηκαν ως επικίνδυνοι για το καθεστώς, είτε λόγω εκπροσώπησης ιδιαζουσών περιπτώσεων πελατών είτε λόγω δημοσίευσης άρθρων με τα οποία δεν ήταν σύμφωνη η κυβερνώσα παράταξη. Απόρροια της ως άνω πρακτικής, κατόπιν της έκδοσης παρεμφερών δικαστικών αποφάσεων για μεγάλο αριθμό Κινέζων πολιτών, είναι να τίθενται στη λεγόμενη ''μαύρη λίστα''. Αν επιθυμούν να αποκαταστήσουν την επελθούσα σπίλωση του ονόματός τους, δύνανται είτε να εξοφλήσουν τα χρέη απέναντι στο κράτος (εξαιτίας των οποίων υπήχθησαν στο σύστημα κοινωνικών κυρώσεων) είτε να κινηθούν δικαστικά επιχειρώντας την απόδειξη της ύπαρξης των κατά περίπτωση υποστηριζόμενων σφαλμάτων.

Η περιγραφείσα διαδικασία συλλογής πλήθους πληροφοριών για το σύνολο των πολιτών μέσω της παρακολούθησής τους από τον κρατικό μηχανισμό **αντίκειται στην προστασία της ιδιωτικότητας αυτών αλλά και στη διαφύλαξη των**

[182] Κανέλλος, 2020, σελ.262

[183]''Phoebe Zhang , ''Chinese court names and shames debtors in warm-up to Avengers movie'', Απρίλιος 2019, διαθέσιμο σε https://www.thestar.com.my/news/regional/2019/04/26/chinese-court-names-and-shames-debtors-in-warmup-to-avengers-movie

προσωπικών τους δεδομένων, τουλάχιστον όπως αυτή ορίζεται σύμφωνα με την ευρωπαϊκή νομοθεσία που έχει προσεγγιστεί μέσω της παρούσας μελέτης. Παρά την τεράστια αντίθεση στην προσέγγιση της προστασίας των προσωπικών δεδομένων μεταξύ της Κίνας και της Ευρώπης ή των ΗΠΑ, δεν είναι παντελώς απούσα η αντίληψη περί κανόνων της προστασίας τους στην πρώτη εξ αυτών, αλλά διαφοροποιείται η νομοθεσία που ρυθμίζει τον εν λόγω τομέα. Όπως επισημαίνει ο κ. Κανέλλος[184], παραθέτοντας τις απόψεις Κινέζων σχολιαστών, τα **τρωτά σημεία** συνίστανται **πρώτον** στο ότι το Σύνταγμα που θεωρείται ο πυλώνας ενός δημοκρατικού πολιτεύματος εκλαμβάνεται ως απειλή για το κυβερνών κόμμα και **δεύτερον** στην ύπαρξη διάκρισης ως προς την αντιμετώπιση του δημοσίου τομέα σε σχέση με τον ιδιωτικό καθώς στον πρώτο αναγνωρίζεται **διακριτική ευχέρεια** ως προς τις πληροφορίες που συλλέγονται κάνοντας επίκληση στους λόγους εθνικής ασφάλειας ενώ στον δεύτερο είναι **επιβεβλημένες** νομικές υποχρεώσεις όπως αυτές που αφορούν την τήρηση ορθών εμπορικών πρακτικών προκειμένου να προστατευτούν οι καταναλωτές.

Εκ των ως άνω συνθηκών, εξάγεται το συμπέρασμα ότι η κρατική παρακολούθηση και ο έλεγχος στις διάφορες εκφάνσεις του λόγου των πολιτών (μέσω διαδικτύου και μέσων κοινωνικής δικτύωσης) με απώτερο στόχο την παρεμπόδιση ανταλλαγής πληροφοριών, ιδεών και απόψεων που αντίκεινται στις εκπεφρασμένες αρχές των κυβερνώντων, δεν αφήνει περιθώρια δημιουργίας και ευδοκίμησης νομοθεσίας περί προστασίας της ιδιωτικότητας στην Κίνα, σύμφωνα με το ευρωπαϊκό πρότυπο του ΓΚΠΔ[185]. Ελλείψει του αξιακού υποβάθρου που θέτει ως προτεραιότητα το σεβασμό στην ανθρώπινη υπόσταση, καθίσταται ιδιαιτέρως δυσχερές να μπορέσει να επέλθει εξισορρόπηση αποκλειστικά και μόνο βάσει ενός νόμου.

3.3.2. Κοινωνικά δίκτυα και Αναγνώριση προσώπου- Περίπτωση ''Geofeedia''

Ένα ακόμη παράδειγμα που θυμίζει τη μέθοδο που ακολουθείται στην Κίνα είναι αυτό στη Βόρεια Καλιφόρνια, όπου γίνεται **χρήση συστημάτων παρακολούθησης μέσω social media (μέσων κοινωνικής δικτύωσης) για την επιβολή του νόμου**.

Πιο συγκεκριμένα, όπως επισημαίνεται[186], προκειμένου να αναγνωριστούν και να συλληφθούν άτομα που συμμετείχαν σε κοινωνικές διαμαρτυρίες, κατά των οποίων εκκρεμούσε ένταλμα σύλληψης, η Αστυνομία της Βαλτιμόρης χρησιμοποίησε το

[184] Κανέλλος, 2020, σελ.264

[185] Αυτό που παρατηρείται, παρ'όλα αυτά, είναι η ύπαρξη ορισμένων διατάξεων περί προστασίας της ιδιωτικότητας εντοπιζόμενες σε διάφορα νομοθετήματα μεταξύ των οποίων και ο νόμος περί κυβερνοασφάλειας (01- 06- 2017), στην ερμηνευτική εγκύκλιο του οποίου (2018) περιλαμβάνονται οδηγίες προς τους τηλεπικοινωνιακούς παρόχους να εφαρμόζουν ελαχιστοποίηση δεδομένων και κανόνες προστασίας των συνδρομητών τους, ομοιάζοντας ως προς τη στόχευση με αυτή του GDPR (DLA Piper, Data protection laws in the world, China, 27 Ιανουαρίου 2022, διαθέσιμο σε https://www.dlapiperdataprotection.com/index.html?c=CN&t=law)

[186] Miyamoto Inez, ''Debating aspects of surveillance through case studies – Social media and Facial Recognition'' στο *Surveillance Technology challenges political culture of democratic states*, σελ. 50-52, διαθέσιμο στο https://dkiapcss.edu/wp-content/uploads/2020/09/04-miyamoto-25thA.pdf

διαφημιστικό προϊόν που της προώθησε η εταιρεία '' Geofeedia''. Η εν λόγω εταιρεία ανέπτυσσε λογισμικό παρακολούθησης διαμέσου των μέσων κοινωνικής δικτύωσης και το πωλούσε σε εταιρείες και αρχές, όπως εν προκειμένω στην Αστυνομική Αρχή, η οποία κάνοντας χρήση αυτού απέκτησε πρόσβαση στις φωτογραφίες των διαδηλωτών που είχαν αναρτηθεί στα κοινωνικά δίκτυα. Εν συνεχεία, χρησιμοποιώντας την τεχνολογία αναγνώρισης προσώπου που διατηρούσε, οδηγήθηκε στην αναγνώριση και σύλληψή τους.

Όταν οι εταιρείες μέσων κοινωνικής δικτύωσης πληροφορήθηκαν τα σχετικά με την εν λόγω δράση της Geofeedia, ανέστειλαν την πρόσβαση της εταιρείας στα δεδομένα απαγορεύοντάς της τη χρήση τους για σκοπούς που εξυπηρετούν δραστηριότητες παρακολούθησης. Χωρίς τη συνεχή τροφοδοσία από τα social media, η Geofeedia δεν μπορούσε να συγκεντρώσει υλικό από τις αναρτήσεις για να παρέχει επικαιροποιημένη πληροφόρηση, με αποτέλεσμα να διαγράφει φθίνουσα πορεία με συνεπαγόμενες απολύσεις εργαζομένων και κατ' επέκταση μετατόπιση ως προς την παροχή επιχειρηματικών υπηρεσιών.

Το ενδιαφέρον στοιχείο που εντοπίζει ο Miyamotto, είναι ότι όταν οι ίδιοι οι ιδιώτες επιλέγουν να κάνουν μία <u>δημόσια ανάρτηση</u> ή σχόλιο σε κάποιο εκ των μέσων κοινωνικής δικτύωσης είναι διότι επιθυμούν να δει το σύνολο του κοινού αυτό το περιεχόμενο, αποδεχόμενοι τις συνέπειες της ευρείας αυτής δημοσιοποίησης και <u>αγνοώντας συνειδητά το δικαίωμα στην ιδιωτικότητα</u>. Ως απόρροια αυτού, οι συγκεκριμένες αναρτήσεις καθίστανται προσβάσιμες στους πάντες και είναι δυνατή η επεξεργασία και χρήση τους κι από τις αρχές επιβολής του νόμου. Αναδιαμορφώνοντας, όμως, τις ρυθμίσεις απορρήτου οι πολίτες δύνανται να οριοθετούν την πρόσβαση στα δεδομένα που αναρτούν και να περιορίζεται η δημόσια έκθεσή τους. Στη δεύτερη περίπτωση, η αστυνομία, ως αρχή επιβολής του νόμου, θα έχει τη δυνατότητα πρόσβασης σε ιδιωτικά δεδομένα μόνο κατόπιν εισαγγελικής εντολής.

Το ουσιώδες, όπως διαπιστώνει ο συγγραφέας, είναι ο **σκοπός** της εκάστοτε **έρευνας** να είναι **ευκρινής** και να υπάρχει τεκμηριωμένη αιτιολόγηση, νόμιμη βάση για έρευνα, στο πλαίσιο της οποίας θα είναι δικαιολογημένη η χρήση λογισμικού αναγνώρισης προσώπου όταν, επί παραδείγματι, διαπράττεται κάποιο έγκλημα κατά τη διάρκεια μιας διαδήλωσης και απαιτούνται τεκμήρια για την ποινική διαδικασία και όχι να παρακολουθούνται μέσω του λογισμικού απλώς και μόνο επειδή ασκούν το νόμιμο δικαίωμα του ''συνέρχεσθαι''.

Καταληκτικά, το στοιχείο που επηρέασε περισσότερο τους πολίτες και συνετέλεσε στην υπονόμευση της εμπιστοσύνης τους ήταν το <u>υποβόσκον πρόβλημα της αδιαφάνειας.</u> Η προτεινόμενη αντιμετώπιση ως προς την ανεύρεση λύσης στην εν λόγω συνθήκη θα ήταν η αστυνομική Αρχή της Βαλτιμόρης να είναι πιο συγκεκριμένη και εναργής ως προς τις πολιτικές που εφαρμόζει στο ζήτημα των τεχνολογιών παρακολούθησης ώστε να μειώνονται οι προβληματισμοί και να περιορίζονται οι αντιδράσεις από πλευράς των πολιτών.

3.3.3. Περίπτωση ''Clearview AI''

Μία ακόμη εταιρεία που παρείχε υπηρεσίες αναγνώρισης προσώπου σε οργανισμούς, εταιρείες και αστυνομικές αρχές είναι η αμερικανική Clearview AI. Κατέστη ευρέως γνωστή τον Ιανουάριο 2020 όταν αποκαλύφθηκαν οι πρακτικές που εφάρμοζε από μια έρευνα των New York Times. Φέρεται να χρησιμοποιούσε ένα αυτοματοποιημένο εργαλείο, που συνέλεγε φωτογραφίες προσώπων σε μέσα κοινωνικής δικτύωσης και άλλους ιστότοπους, οι οποίες ήταν διαθέσιμες στο σύνολο του κοινού, αυτό όμως που τη διαφοροποιούσε ήταν ο **σκοπός** που δεν ήταν άλλος από **τη δημιουργία βιομετρικής βάσης δεδομένων**. Επιπροσθέτως αυτών των εικόνων και συνδυαστικά με αυτές, το αυτοματοποιημένο εργαλείο **συγκέντρωνε και τα μεταδεδομένα** που τις συμπλήρωναν, όπως τον τίτλο της ιστοσελίδας και το σύνδεσμο της πηγής της. Έχοντας τα στοιχεία αυτά, οι συλλεχθείσες εικόνες προσώπου **αντιπαραβάλλονταν στο λογισμικό αναγνώρισης προσώπου** της εταιρείας ώστε να δημιουργηθεί η βάση δεδομένων. Τέλος, κατόπιν της ολοκλήρωσης της ως άνω διαδικασίας , παρεχόταν πρόσβαση στην περιγραφείσα βάση δεδομένων – και κατ' επέκταση στη δυνατότητα αναγνώρισης ατόμων – σε αστυνομικές υπηρεσίες, αρχές και ιδιωτικές εταιρείες.[187]

Συνειδητοποιεί κανείς ότι ο ιδρυτής της πάλαι ποτέ μικρής start-up από τη Νέα Υόρκη, 31χρονος τότε Αυστραλός με καταγωγή από το Βιετνάμ Hoan Ton-That, έκανε αυτό που μέχρι εκείνη τη χρονική στιγμή κανείς δεν είχε τολμήσει, καθώς υπολογίζεται ότι ο όγκος των εικόνων προσώπου που έχει συλλέξει από δημόσια προσβάσιμες πηγές του διαδικτύου, σύμφωνα με την επίσημη σελίδα της εταιρείας, ξεπερνούσε το 2020 τις 3 δισεκατομμύρια φωτογραφίες πολιτών ενώ το 2022 έφτασε να υπερβαίνει τα 20 δισεκατομμύρια (!), τις οποίες **πωλούσε προς εξυπηρέτηση συγκεκριμένων σκοπών**, όπως προαναφέρθηκε. Παρέκαμψε κάθε προβληματισμό περί του αν είναι νόμιμο και ηθικό να αναπτυχθεί εμπορικά μια τέτοια τεχνολογία όταν, δεδομένης της λειτουργίας της, δύναται να οδηγήσει σε τόσο βίαιη και ολοκληρωτική άρση της ιδιωτικότητας του πολίτη.[188]

Η εταιρεία ισχυρίζεται ότι το προϊόν απευθύνεται πρωτίστως στις διωκτικές αρχές, με σκοπό να αποτελέσει ένα σημαντικό όπλο στην προσπάθεια εξιχνίασης εγκλημάτων. Στηριζόμενη σε αυτή την εξαγγελία, προβαίνει στην εφαρμογή για πολλούς μήνες μιας πολιτικής επιθετικού και εκτεταμένου μάρκετινγκ ερχόμενη σε απευθείας επαφή με αστυνομικά τμήματα σε όλες τις Πολιτείες των ΗΠΑ προκειμένου να παράσχει ενημέρωση για τη νέα εφαρμογή που μπορεί να δώσει τα

[187] Μπολέτση Άντζελα, ''Clearview AI: Καταγγελίες -και στην Ελλάδα- για παράνομη βάση δεδομένων από φωτογραφίες στα social media: '', 28-5-2021, διαθέσιμο στο https://www.newmoney.gr/roh/palmos-oikonomias/texnologia/clearview-ai-katangelies-ke-stin-ellada-gia-paranomi-vasi-dedomenon-apo-fotografies-sta-social-media

[188] Βέρρας Δημήτρης, ''Το χρονικό του προδιαγεγραμμένου τέλους της ιδιωτικότητας ;'', 01-05-2020, διαθέσιμο στο https://www.lawspot.gr/nomika-blogs/dimitris_verras/clearview-ai-hroniko-toy-prodiagegrammenoy-teloys-tis-idiotikotitas

βέλτιστα αποτελέσματα σε σχέση με αντίστοιχες προηγούμενες. Επιπλέον, έδιδαν τη δυνατότητα δωρεάν δοκιμής για διάστημα τριάντα ημερών ώστε να πειστούν για την αποτελεσματικότητά της οι υποψήφιοι πελάτες και η ανταπόκριση ήταν μεγάλη. Όπως επισημαίνεται στο εν λόγω άρθρο[189], η εφαρμογή χρησιμοποιήθηκε πολύ σύντομα από περισσότερες από 600 διωκτικές αρχές, ενώ η εταιρεία τη διέθεσε και σε ιδιώτες, που ήθελαν να τη χρησιμοποιήσουν για «λόγους ασφάλειας».

Οι πρώτες οξείες αντιδράσεις, κατόπιν της αποκάλυψης των New York Times, εκδηλώθηκαν σε σύντομο χρονικό διάστημα τόσο μέσω ανακοίνωσης από τα μέσα κοινωνικής δικτύωσης (όπως το twitter) όσο κι από ανώτερα όργανα (όπως ο Δημοκρατικός Γερουσιαστής της Μασαχουσέτης). Ακολούθησε η υποβολή εξωδίκων κι άλλων διάσημων εταιρειών (google, youtube κ.πλ.) ώστε η Clearview να απόσχει από κάθε παράνομη συμπεριφορά και να προβεί στον τερματισμό συλλογής δεδομένων σε συνδυασμό με τη διαγραφή όσων εξ αυτών έχει ήδη συλλέξει από τις πλατφόρμες αυτές. Όπως επισημαίνεται[190], η αρχή απορρήτου του Καναδά έκρινε ότι η τεχνική σάρωσης προσώπου της Clearview είναι «παράνομη» και ότι δημιουργεί ένα σύστημα που «προκαλεί ευρεία βλάβη σε όλα τα μέλη της κοινωνίας». Ακόμη, **στις ΗΠΑ,** μηνύθηκε ήδη από το 2020 από την Αμερικανική Ένωση Πολιτικών Ελευθεριών στην πολιτεία του Ιλινόις για παραβίαση του νόμου περί βιομετρικών δεδομένων, με αποτέλεσμα τον **τερματισμό παροχής του προϊόντος σε αμερικάνικες ιδιωτικές εταιρείες**.

Στον ευρωπαϊκό χώρο, η Σουηδική Αρχή Προστασίας Δεδομένων Datainspektionen, καθίσταται η πρώτη εποπτική αρχή της ΕΕ που δημοσιοποιεί την απόφασή της να διερευνήσει το ενδεχόμενο χρήσης της εφαρμογής (αν λαμβάνει χώρα και σε περίπτωση καταφατικής απάντησης, με ποια νομική βάση). Κατόπιν της έρευνάς της, **προέβη στην τιμώρηση της Σουηδικής Αστυνομίας, καθώς χρησιμοποίησε τις υπηρεσίες της Clearview για «παράνομη» αναγνώριση πολιτών.** Σύμφωνα με τα υποστηριζόμενα στο προαναφερθέν άρθρο[191], ευρωπαϊκοί οργανισμοί απορρήτου και ψηφιακών δικαιωμάτων υπέβαλαν **ομαδικές καταγγελίες κατά της εταιρείας αναγνώρισης προσώπου, Clearview AI**. Οι καταγγελίες που υποβλήθηκαν στη Γαλλία, την Αυστρία, την Ελλάδα, την Ιταλία και το Ηνωμένο Βασίλειο αναφέρουν ότι η μέθοδος συλλογής και εξόρυξης (το λεγόμενο ''scraping'') δεδομένων και εικόνων της εταιρείας **παραβιάζει τους ευρωπαϊκούς νόμους περί απορρήτου.**

Στο πλαίσιο αυτό, κι η ελληνική Homo Digitalis πέραν της ομαδικής καταγγελίας απευθύνθηκε και κατά μόνας, όπως κατέστη γνωστό, αρχικώς μέσω επιστολής της προς τον Υπουργό Προστασίας του Πολίτη για τη χρήση της εφαρμογής από τις αρχές επιβολής του νόμου στην ελληνική επικράτεια αλλά και κατόπιν κατατεθεισών από την πλευρά της ερωτήσεων, η Ελληνική Αστυνομία δήλωσε επίσημα ότι δεν έχει χρησιμοποιήσει τις υπηρεσίες της εν λόγω εταιρείας.

Αξιοσημείωτη, τέλος, είναι η πρόσφατη **επιβολή προστίμου άνω των 7,5**

[189] ό.π. υποσ 179
[190] ό.π. υποσ 178
[191] ό.π. υπ.178

εκατομμυρίων λιρών στην Clearview για παράνομη αποθήκευση εικόνων προσώπου από το Γραφείο Επιτροπής Πληροφοριών **ICO** (Information Commissioner's Office) του **Ηνωμένου Βασιλείου**[192]. Ζητήθηκε από αυτή να διαγράψει τα δεδομένα φωτογραφιών που υπήρχαν στους server της, από κατοίκους του Ηνωμένου Βασιλείου καθώς και ό,τι δεδομένα υπάρχουν από πολίτες του Ηνωμένου Βασιλείου. Το **ICO** διαπίστωσε ότι η **Clearview AI Inc** *παραβίασε τους νόμους περί προστασίας δεδομένων του Ηνωμένου Βασιλείου* με ουσιώδεις παραλείψεις, όπως καταγράφεται στο ως άνω αναφερθέν άρθρο, που αφορούσαν τα κάτωθι: **1**. Χρησιμοποιούσε προσωπικές πληροφορίες ανθρώπων του Ηνωμένου Βασιλείου με τρόπο αδιαφανή και παρέδιδε ευαίσθητα δεδομένα για επεξεργασία σε τρίτες χώρες, **2**. δεν είχε νόμιμους λόγους για να προβεί σε φωτογραφική αναγνώριση και αρχειοθέτηση τέτοιων πληροφοριών, **3**. δεν υπήρχε μια διαδικασία που να επιβάλλει να σταματήσει η διατήρηση των δεδομένων κάποιου χρήστη που δεν την επιθυμεί και, τέλος, **4**. Δεν πληρούνταν η ύπαρξη των υψηλότερων προτύπων προστασίας δεδομένων που απαιτούνταν για τέτοιου είδους βιομετρικά δεδομένα.

Ο διευθύνων σύμβουλος της Clearview εξέφρασε την απογοήτευσή του περί παρερμηνείας της τεχνολογίας που χρησιμοποιεί και των προθέσεών του από τον τρόπο αντιμετώπισης του Επιτρόπου Πληροφοριών του Ηνωμένου Βασιλείου, καθώς όπως υποστηρίζει, ''συλλέγει μόνο δημόσια δεδομένα από το ανοιχτό διαδίκτυο και συμμορφώνεται με τα πρότυπα απορρήτου και νόμου''. Η εν λόγω δήλωση έρχεται να προστεθεί σε πολλές προηγηθείσες παρόμοιου τύπου, προς δικαιολόγηση της συγκεκριμένης εταιρείας περί υποτιθέμενης ''νομότυπης δράσης'' της , καθώς το Ηνωμένο Βασίλειο είναι η τέταρτη χώρα μετά τη Γαλλία, την Ιταλία και την Αυστραλία που λαμβάνει μέτρα επιβολής κατά της εταιρείας.

Σε συνέχεια των όσων εκτέθηκαν και παρακολουθώντας κανείς τη δράση της εν λόγω εταιρείας και τον παγκόσμιο αντίκτυπό της, συνειδητοποιεί τη σπουδαιότητα θεμελίωσης και συνεχούς υπενθύμισης στην πράξη των ανθρωπίνων δικαιωμάτων προς την εδραίωση της ευνομίας σε μια εποχή που ένα εκ των σημαντικότερων εξ αυτών, αυτό της ιδιωτικότητας, αποτελεί αντικείμενο ποικίλων (παρ) ερμηνειών και βάλλεται συνεχώς.

[192] Webmedia, ''Πρόστιμο στην Clearview AI για παράνομη αποθήκευση εικόνων προσώπου στο Ηνωμένο Βασίλειο'', 27-5-2022, διαθέσιμο στο https://thinktech.gr/%CF%80%CF%81%CF%8C%CF%83%CF%84%CE%B9%CE%BC%CE%BF-%CF%83%CF%84%CE%B7%CE%BD-clearview-ai-%CE%B3%CE%B9%CE%B1-%CF%80%CE%B1%CF%81%CE%AC%CE%BD%CE%BF%CE%BC%CE%B7-%CE%B1%CF%80%CE%BF%CE%B8%CE%AE%CE%BA%CE%B5

ΕΠΙΛΟΓΟΣ - ΣΥΜΠΕΡΑΣΜΑΤΑ

Ολοκληρώνοντας την παρούσα μελέτη, ένα εκ των κυριοτέρων συμπερασμάτων που εξάγονται είναι ότι η συνεισφορά των εφαρμογών τεχνητής νοημοσύνης στην ανάπτυξη και διαμόρφωση των συστημάτων – βιομετρικών τεχνολογιών αναγνώρισης προσώπου υπό τη σημερινή τους μορφή είναι καταλυτικής σημασίας και καθίσταται καίρια η συμβολή τους σε αρκετούς τομείς, όπως αυτός της υγείας, της ασφάλειας, του ελέγχου των συνόρων (περίπτωση άρ. 9 παρ. 2 περ.ζ' ΓΚΠΔ , όπου αίρεται ο κανόνας της απαγόρευσης επεξεργασίας λόγω ουσιαστικού δημοσίου συμφέροντος). Παρ' όλα αυτά και στην εν λόγω περίπτωση, όπως στις πλείστες όσες παρεμφερώς εξεταζόμενες, ειδικά κατά τα τελευταία έτη με την ταχύτατη ανάπτυξη των τεχνολογικών μεθόδων, τα θετικά αποτελέσματα που είναι αναντίρρητα πολλά, διαδέχονται προβληματισμοί και ανησυχίες περί της χρησιμοποίησης των εφαρμογών τεχνητής νοημοσύνης.

Και τούτο διότι παρά τις ουσιαστικές και καθ' όλα μελετημένες ενέργειες που λαμβάνουν χώρα σε επίπεδο νομοθεσίας προς αποφυγή αρνητικών συνεπειών, η πρακτική εφαρμογή των συστημάτων αναγνώρισης προσώπου στις περισσότερες περιπτώσεις διαψεύδει τις αρχικές προθέσεις και εγείρει ολοένα και πιο σοβαρά ζητήματα ως προς τον κίνδυνο παραβίασης δικαιωμάτων, ιδίως κατόπιν της έκτασης που έλαβε η παράνομη συλλογή βιομετρικών δεδομένων, μέσω της προρρηθείσας περίπτωσης της Clearview AI , με τη συνακόλουθη δημιουργία βάσεως δεδομένων. Η ιδιωτικότητα δέχεται συνεχή πλήγματα λόγω της ραγδαίας ανάπτυξης της τεχνολογίας και των απεριόριστων δυνατοτήτων που προσφέρει γι' αυτό σήμερα περισσότερο παρά ποτέ θεωρείται σώφρον και πλέον αναγκαίο να καλλιεργηθεί η κουλτούρα του μέτρου και του λελογισμένου διαμοιρασμού δεδομένων κι από την πλευρά των νέων και ιδίως των παιδιών, τα οποία λόγω των αναδυομένων προτύπων εκτίθενται ολοένα και περισσότερο εκουσίως ή ακουσίως σε πολλαπλές διαδικτυακές απειλές, μη συνειδητοποιώντας επί της ουσίας τι πράττουν όταν αναρτούν επί παραδείγματι κάποια προσωπική τους φωτογραφία που απευθύνεται σε ογκώδες και ποικίλο κοινό, στους λεγόμενους ''φίλους'', τους οποίους ενδεχομένως να μη γνωρίζει καν, διευκολύνοντας με αυτό τον τρόπο το έργο όλων όσοι έχουν εργαλειοποιήσει τη χρησιμότητα των βιομετρικών τεχνολογιών προς αποκόμιση ιδίου οφέλους.

Ακόμη, η βιντεοεπιτήρηση, η οποία εκτείνεται σε συνεχώς μεγαλύτερο εύρος, θα πρέπει να υπόκειται εν τη πράξει στους νομοθετικούς κανόνες που αναλύθηκαν στην εν λόγω μελέτη, ως προς τη νομιμότητα της επεξεργασίας της, τηρώντας τις ουσιώδεις αρχές, ιδίως της λογοδοσίας (άρ.5 παρ. 2 ΓΚΠΔ), που λειτουργεί ως μηχανισμός εγγύησης της τήρησης των αρχών που διέπουν την επεξεργασία των προσωπικών

δεδομένων και εξασφαλίζουν την έμπρακτη προστασία τους αλλά και την αρχή της ελαχιστοποίησης (άρ.5.παρ.1 στοιχ.γ' ΓΚΠΔ), η οποία αποτελεί και το απώτατο όριο για τους αλγορίθμους, και έγκειται στο ότι τα δεδομένα προσωπικού χαρακτήρα πρέπει να είναι κατάλληλα, συναφή και να περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία [193] . Κι αυτό διότι αν δεν εδραιωθεί η νοοτροπία περί περιφρούρησης της ιδιωτικότητας, θα διαμορφώνονται όλο και λιγότερες αντιστάσεις στη συνεχή παρακολούθηση , η οποία ενδεχομένως με το πέρας των ετών θεωρηθεί ότι λαμβάνει χώρα στο πλαίσιο του φυσιολογικού και του αναμενόμενου (περίπτωση ''Συνδρόμου Κίνας''), ιδίως για τις νέες γενεές που δε θα έχουν βιώσει την προτέρα κατάσταση προκειμένου να έχουν μέτρο σύγκρισης.

Εξ αυτού του λόγου, θεωρείται απαραίτητο να πραγματοποιηθεί μια συνολική προσπάθεια ως προς το συντονισμό των ενεργειών **τόσο** από την πλευρά των κρατικών φορέων ως προς την αυστηροποίηση των παραμέτρων της χρήσης των βιομετρικών τεχνολογιών αναγνώρισης προσώπου και της βιντεοεπιτήρησης, την εντατικοποίηση των ελέγχων και την τήρηση των υποχρεώσεων των υπευθύνων επεξεργασίας σύμφωνα με τον Ευρωπαϊκό Γενικό Κανονισμό περί προστασίας προσωπικών δεδομένων και την προσαρμογή στην εθνική νομοθεσία μέσω του νόμου 4624/2019 - ως προς την εφαρμογή των κατάλληλων τεχνικών και οργανωτικών μέτρων, των αρχών επεξεργασίας εκ του σχεδιασμού, της διενέργεια εκτίμησης αντικτύπου- ως προληπτικό μέτρο - , των επιταγών του Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ, της Ευρωπαϊκής Σύμβασης Δικαιωμάτων του Ανθρώπου και της νομολογίας του Ευρωπαϊκού Δικαστηρίου Ανθρωπίνων Δικαιωμάτων και του Δικαστηρίου της ΕΕ, αλλά και της νομολογίας τη Αρχής Προστασίας προσωπικών δεδομένων όπως και του προταθέντος Σχεδίου Κανονισμού Τεχνητής Νοημοσύνης της Ευρωπαϊκής Επιτροπής βάσει των διατυπωθεισών απαιτήσεων στη Λευκή Βίβλο -περί των προϋποθέσεων θεώρησης των εφαρμογών Τεχνητής Νοημοσύνης ως ''υψηλού κινδύνου'' ή όχι – **όσο** και σε ιδιωτικό πλαίσιο, από την πλευρά της οικογένειας, ως βασικού πυλώνα διαπαιδαγώγησης, θωρακίζοντας τα παιδιά με αξίες που θέτουν, μεταξύ άλλων, ως προτεραιότητα τη διαφύλαξη της ιδιωτικότητας, ώστε να μην είναι διαπραγματεύσιμη απέναντι σε οποιαδήποτε πιθανή ενέργεια καταστρατήγησής της, ιδίως διαμέσου των μέσων κοινωνικής δικτύωσης που θεωρούνται ο πιο εύκολα προσβάσιμος δίαυλος άντλησης προσωπικών δεδομένων.

[193] Σκέψη 156 του Γενικού Κανονισμού Προστασίας Δεδομένων (περί αρχής ελαχιστοποίησης)

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΕΛΛΗΝΙΚΗ

Ακριβοπούλου, Χ. (2012), Το δικαίωμα στην ιδιωτική ζωή (από τη γένεση, στη σύγχρονη διαμόρφωση και προστασία του), Εκδ. Α. Σάκκουλα, Αθήνα

Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2007), Προσωπικά Δεδομένα, Εκδ. Α. Σάκκουλα, Αθήνα-Κομοτηνή

Βασιλοπούλου Ν. Ευαγγελία (2018), ''Βιομετρικά και Γενετικά Δεδομένα'' σε Κοτσαλή Λ., Μενουδάκο Κ., *Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων (GDPR), Νομική Διάσταση και Πρακτική Εφαρμογή*, Αθήνα, Νομική Βιβλιοθήκη

Βλαχάβας, Κεφαλάς κ. ά.(2020), Τεχνητή Νοημοσύνη, Δ' έκδοση, Εκδόσεις Πανεπιστημίου Μακεδονίας, Αύγουστος 2020 (http://aibook.csd.auth.gr/)

Βουτσάκη, Β. (2004), Το δικαίωμα στην ιδιωτική ζωή: υποκειμενικές και αντικειμενικές πτυχές, σε Γ. Παπαδημητρίου (επιμ.), Νέες Τεχνολογίες και συνταγματικά δικαιώματα, Αθήνα

Δαγτόγλου, Π.Δ. (2005) Συνταγματικό Δίκαιο, Ατομικά Δικαιώματα Α', Εκδ. Α. Σάκκουλα, Αθήνα.

Δημητρόπουλος, Α. (2005) Συνταγματικό Δίκαιο, Ειδικό μέρος. Παραδόσεις συνταγματικού δικαίου, τόμος ΙΙΙ, τεύχη ΙV επ. ια' έκδοση, Αθήνα

Δόνος, Π.(2004), ''Τεχνολογική διακινδύνευση και προστασία προσωπικών δεδομένων'' σε: Νέες τεχνολογίες και συνταγματικά δικαιώματα, Αθήνα-Θεσσαλονίκη

Ηλιάδου, Α.Ν. (2016). Η συνταγματική προστασία των δεδομένων προσωπικού χαρακτήρα, σε: Λεωνίδα Κοτσαλή (επιμ.), Προσωπικά Δεδομένα: Ανάλυση-Σχόλια-Εφαρμογή, Εκδόσεις Νομική Βιβλιοθήκη, Αθήνα

Ιγγλεζάκης Ι. (2004), Ευαίσθητα Προσωπικά Δεδομένα, Εκδόσεις Σάκκουλα, Αθήνα-Θεσσαλονίκη

Κανέλλος Λ. (2020), Εφαρμογές Τεχνητής Νοημοσύνης (στο δίκαιο και στη δικαστική πρακτική), Εκδ. Νομική Βιβλιοθήκη

Καρακώστας, Ι. (2012), Το δίκαιο της προσωπικότητας, Νομική Βιβλιοθήκη, Αθήνα

Κονιδιτσιώτου Β (1978), Η Νεωτέρα Παιδαγωγική, Αθήνα

Κουκιάδης, Ι.Δ. (επιμ.), (2008). Η παραδοσιακή προστασία της προσωπικότητας του εργαζομένου, σε: Προστασία Προσωπικότητας, Αθήνα-Θεσσαλονίκη.

Κουκιάδης, Ι. Δ. (2019), Ο εργαζόμενος ως υποκείμενο προσωπικών δεδομένων, κατά το Γενικό Κανονισμό Προστασίας Δεδομένων, Εκδ. Σάκκουλα, Αθήνα

Κυριαζόγλου, Ι. (2019) Προστασία Προσωπικών Δεδομένων, Εκδόσεις Φυλάτος

Μαλαγαρδή, Α.Κ. (2010). Νέες τεχνολογίες-προσωπικά δεδομένα και εργατικό δίκαιο. Εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα-Κομοτηνή.

Μάνεσης, Α. (1978). Συνταγματικά Δικαιώματα, Πανεπιστημιακές Παραδόσεις, Εκδ. Οίκος Α. Σάκκουλα, Θεσ/νικη

Μαυριάς, Κ. (1982), Το συνταγματικό δίκαιο του ιδιωτικού βίου, Εκδ. Α. Σάκκουλα, Αθήνα

Μήτρου, Λ. (2001), Προστασία Προσωπικών Δεδομένων: ένα νέο δικαίωμα; στο έργο Δ. Τσάτσου - Ευ. Βενιζέλου - Ξ. Κοντιάδη (επιμ.), Το νέο Σύνταγμα - Πρακτικά συνεδρίου για το αναθεωρημένο Σύνταγμα του 1975/1986/2001, Αθήνα- Κομοτηνή

Μήτρου Λ. (2008), Βιοτράπεζες, Έρευνα και γενετικά δεδομένα, σε Γεώργιο Μανιάτη-Λίλιαν Μήτρου, Η προστασία των γενετικών δεδομένων, Εκδόσεις Σάκκουλα, Αθήνα-Θεσσαλονίκη

Μήτρου Λίλιαν (2017), «Άρθρο 9Α » σε επιμέλεια των Καθηγητών Φ. Σπυρόπουλου, Ξ. Κοντιάδη, Χ. Ανθόπουλου και Γ. Γεραπετρίτη, Σύνταγμα, κατ' άρθρο Ερμηνεία, Εκδ. Σάκκουλα Αθήνα-Θεσσαλονίκη

Παναγοπούλου-Κουντατζή, Φ. (2017). Ο Γενικός Κανονισμός για την προστασία των Δεδομένων 679/2016/ΕΕ, Εκδ. Οίκος Α. Σάκκουλα, Αθήνα-Θεσ/νίκη

Πλατής, Ε. (2018), Προσωπικά Δεδομένα, προστασία GDPR, Εκδ. Παπαδόπουλος,

Αθήνα

Σακκά Δ. (1977), Παιδαγωγική Ψυχολογία, Αθήνα

Σαρίπολος, ΝΤ. (1874), Πραγματεία του Συνταγματικού Δικαίου, Αθήνα: Τυπογραφείο Μιχαήλ Ν. Αγγελίδη

Συμεωνίδου-Καστανίδου Ε. (2013), Ανάλυση DNA και ποινική δίκη: το ευρωπαϊκό θεσμικό πλαίσιο, σε: Σύνταγμα, Δημοκρατία και Πολιτειακοί Θεσμοί, Μνήμη Γιώργου Παπαδημητρίου ΙΙ, Εκδόσεις Σάκκουλα, Αθήνα-Θεσσαλονίκη

Τσεβά, Α.Δ. (2010). Προσωπικά δεδομένα και μέσα ενημέρωσης, Εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα-Κομοτηνή.

Φιτσιάλος Γ. (2014), Αποδεικτική αξία της γενετικής πληροφορίας, σε Μαρία Κανελλοπούλου-Μπότη/Φερενίκη Παναγοπούλου-Κουντατζή (επιμ.), Ιατρική ευθύνη και Βιοηθική, Ιατρικές εκδόσεις Πασχαλίδη, Αθήνα

Χρυσόγονος, Κ. (2017). Ατομικά και κοινωνικά δικαιώματα (4η έκδοση). Νομική Βιβλιοθήκη

ΞΕΝΟΓΛΩΣΣΗ

Ariès, Ph. (1973). 'The Family and the City in the Old World and the New', στο V. Tutte & B. Meyerhoff,(επιμ.), Changing Images of the Family, Harmondsworth: Penguin

Barr A. & Feigenbaum E. (1981) The Handbook of Artificial Intelligence

Betzel M. (2005) Biometrics: Privacy Year in Review: Recent Changes in the Law of Biometrics, 1 ISJLP

Fungsang Fr. (2006), Government Information Collection: U.S. E-Passports: ETA August 2006: Recent Changes Provide Additional Protection for Biometric Information Contained in U.S. Electronic Passports, 2 ISJLP 2006

Habermas, J. (1991), The Structural Transformation of the Public Sphere: An Inquiry into the Category of Bourgeois Society. Cambridge: MIT Press

Hareven, T.K. (1991), 'The Home and the Family in Historical Perspective', Social Research, 58

Introna L. and **Nissenbaum H.**, Facial Recognition Technology: A Survey of Policy and Implementation Issues, Lancaster University Management School Working Paper 2010/030

Laney, D. (2001) ''3-D Data Management: Controlling Data volume, Velocity and Variety, ''META Group Research Note

Lytras, M., Raghavan, V., & Damiani, E. (2017). Cognitive computing and big data analytics research: From metaphors to value space for collective wisdom in human decision making and smart machines. International Journal on Semantic Web and Information Systems, 13(1)

Meyer-Spacks, P. (2003). Privacy, Concealing the Eighteenth-Century Self. Chicago & London: The University of Chicago Press.

McGuire L. J. (2000), Comment, Banking on Biometrics: Your Bank's New High-Tech Method of Identification May Mean Giving Up You Privacy, 33 AKRON L. REV.

Negnevitsky M.(2020), Artificial Intelligence: A Guide to Intelligence Systems (3rd Edition), Addison Wesley

Norvig R. & P. (2021), Τεχνητή Νοημοσύνη, μια σύγχρονη προσέγγιση, Εκδόσεις Κλειδάριθμος

The Norwegian Data Protection Authority, (Report January 2018), *Artificial Intelligence and Privacy*

Rodota, S. (2004) Privacy, Freedom and Dignity - Closing Remarks at the 26th International Conference on Privacy and Personal Data Protection.

Rybczynski, W. (1987). Home: A short history of an idea. New York: Penguin

Schneider I. (2002), Biobanken: Korpermaterial und Gendaten im Spannungsfeld von Gemeinwohl und privaer Aneignung στο έργο Nationaler Ethikrat. Biobanken:Chance fur den eissenschaftlichen Fortschritt oder Ausverkauf der ''Ressource Mensch? Tagungsdokumentation

Sivarajah, U., Kamal, M. M., Irani, Z., & Weerakkody, V. (2017), Critical analysis of big data challenges and analytical methods. Journal of Business Research, 70

Solove, D. (2002) 'Conceptualizing Privacy', California Law Review. 90:1087-1155.

Solove, D. (2006) A Taxonomy of Privacy, University of Penn Law Review, Vol.154, No 3

Stone, L. (1991). 'The Public and Private Stately Homes of England, 1500-1990', Social Research, 58

Tomkos, I., **Klonidis**,D., **Pikasis**,E. and **Theodoridis**,S., 2020, Toward the 6G network era: Opportunities and Challenges, IT Professional , 22(1)

Warren, S.D. and **Brandeis**, L.D. (1890). The Right to Privacy, 5 (4) Harvard Law Review

Westin, A. 1967. Privacy and Freedom, 1st edition, New York

Zeldin, Th. (1996). An Intimate History of Humanity. London: Minerva

ΑΡΘΡΟΓΡΑΦΙΑ

Ακριβοπούλου, Χ. (2010), ''Η ιδιωτικότητα του προσώπου μέσα από τη συνθετική αντίθεση δημόσιου-ιδιωτικού'', *Επιστήμη και Κοινωνία (επιθεώρηση πολιτικής και ηθικής θεωρίας),* τεύχος 26

Ακριβοπούλου Χρ. (2011), Το δικαίωμα στην προστασία των προσωπικών δεδομένων μέσα από το φακό του δικαιώματος στην ιδιωτική ζωή, *ΘΠΔΔ*, τεύχος 7

Ανδρουλάκη Ευ. (2021), ''Τεχνητή νοημοσύνη και προσωπικά δεδομένα: η περίπτωση της εξ αποστάσεως βιομετρικής ταυτοποίησης'', *Επιθεώρηση Δικαίου Πληροφορικής*, Τομ.1 , αρ.1 (διαθέσιμο σε https://ejournals.lib.auth.gr/infolawj/article/view/8236)

Αυγουστιανάκη, Μ.(2001), ''Προστασία του ατόμου από την επεξεργασία προσωπικών δεδομένων'', *ΔτΑ* No11

Βόρρας Κ. Απ., **Μήτρου** Λ. (2018), ''Τεχνητή Νοημοσύνη και προσωπικά δεδομένα, Μια θεώρηση υπό το πρίσμα του Ευρωπαϊκού Γενικού Κανονισμού Προστασίας

Δεδομένων (ΕΕ) 2016/679'', *ΔΙΤΕ(πρώην ΔΙΜΕΕ),* Τεύχος 4/2018, Οκτώβριος- Νοέμβριος- Δεκέμβριος

Ζερμιώτη, Κ. (2012) ''Δημόσια Πρόσωπα και προστασία της προσωπικότητας (δημόσια πρόσωπα)'', Διπλ. Εργασία, Τμήμα Νομικής ΕΚΠΑ, Αθήνα

Λούντου Μ. (2021), ''Η προστασία των προσωπικών δεδομένων των εργαζομένων στο Δημόσιο και Ιδιωτικό τομέα υπό το πρίσμα των πρόσφατων νομοθετικών εξελίξεων (σύκριση-αντιπαραβολή και προοπτικές εξέλιξης)'', Διπλ. Εργασία, Π.Μ.Σ. Δημόσια Διοίκηση- Δημόσιο Μάνατζμεντ, Τμ. Διοίκησης Επιχειρήσεων Πανεπιστημίου Δυτικής Αττικής, Αιγάλεω

Μαλακασιώτης, Πρ. (2005) ''Αναγνώριση μερών του λόγου σε ελληνικά κείμενα με τεχνικές ενεργητικής μάθησης'', Διπλ. εργασία, Π.Μ.Σ. στην Επιστήμη των υπολογιστών Οικονομικού Πανεπιστημίου Αθηνών

Μήτρου Λ. (2017), ''Ιδιωτικότητα, προσωπικά δεδομένα και εργασιακές σχέσεις'', *Επιθεώρησις Εργατικού Δικαίου*, τόμος 76, τεύχος 2

Μήτρου Λ. (2018), ''Η αρχή της λογοδοσίας'' (ως υποκεφάλαιο ενότητας ''Υποχρεώσεις του υπευθύνου επεξεργασίας''- Γιώργος Ν. Γιαννόπουλος, Λίλιαν Μήτρου, Γρηγόρης Τσόλιας) σε Κοτσαλή Λ., Μενουδάκο Κ., *Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων (GDPR), Νομική Διάσταση και Πρακτική Εφαρμογή*, Αθήνα, Νομική Βιβλιοθήκη

Παναγοπούλου-Κουντατζή Φ. (2013)**,** ''Βιομετρικές μέθοδοι και προστασία ιδιωτικότητας: Σκέψεις με αφορμή την απόφαση ΔΕΕ Michael Schwarz κατά κρατιδίου Bochum (C-291/2012), *ΔΙΤΕ (π. ΔΙΜΕΕ),* τεύχος 4, Οκτώβριος- Νοέμβριος- Δεκέμβριος

Πολλάτου Ι. (2001), Ανάλυση του DNA και νέοι ορίζοντες στη διερεύνηση του εγκλήματος, *ΠοινΔικ*

Σκόνδρα Μ. (2020), ''Συστήματα Βιντεοεπιτήρησης, αναγνώριση προσώπου και προστασία προσωπικών δεδομένων'', *ΔΙΤΕ (πρώην ΔΙΜΕΕ),* τεύχος 1, Ιανουάριος- Φεβρουάριος- Μάρτιος

ΝΟΜΟΘΕΣΙΑ

Σύνταγμα της Ελλάδας, όπως αναθεωρήθηκε με το ψήφισμα της 27ης Μαΐου 2008 της Η' Αναθεωρητικής Βουλής των Ελλήνων, διαθέσιμο σε https://www.hellenicparliament.gr/UserFiles/f3c70a23-7696-49db-9148-f24dce6a27c8/SYNTAGMA1_1.pdf

Νόμος 3471/2006 (ΦΕΚ 133/Α'/28.6.2006) με τίτλο «Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997» ως αυτός τροποποιήθηκε με το Νόμο 4070/2012 (Α' 82/10.4.2012**),** διαθέσιμος σε https://www.e-nomothesia.gr/kat-dedomena-prosopikou-kharaktera/n-3471-2006.html

Νόμος 4624/2019 (ΦΕΚ 137/1/29.8.2019) - 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, διαθέσιμος σε https://www.lawspot.gr/nomikes-plirofories/nomothesia/nomos-4624-2019

Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων - ΓΚΠΔ**)** διαθέσιμος σε https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679&from=HR

Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, διαθέσιμη σε https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A31995L0046

Οδηγία (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 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 και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου, διαθέσιμη σε https://www.dpa.gr/sites/default/files/2020-05/CELEX_32016L0680_EL_TXT.pdf

Οδηγία 1/2011 της Αρχής Προστασίας Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) σχετικά

με τη χρήση συστημάτων βιντεοεπιτήρησης για την προστασία προσώπων και αγαθών, 13-04-2011 διαθέσιμο σε https://www.dpa.gr/el/enimerwtiko/deltia/odigia-12011-tis-arhis-prostasias-dedomenon-prosopikoy-haraktira-shetika-me-ti

Απόφαση 29/2012 ΑΠΔΠΧ, διαθέσιμη σε https://www.dpa.gr/sites/default/files/2020-12/ARXH%20PROSTASIAS%20APOLOGISMOS%202012_%20WEBUSE.PDF

Απόφαση 10/2022 ΑΠΔΠΧ, διαθέσιμη σε https://www.dpa.gr/sites/default/files/2022-03/10_2022anonym.pdf

Γνωμοδότηση 15/2001 ΑΠΔΠΧ, διαθέσιμη σε https://www.dpa.gr/sites/default/files

Έγγραφο εργασίας WP80/2003 σχετικά με τα στοιχεία βιομετρίας, Ομάδα Εργασίας του άρθρου 29, διαθέσιμο σε https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_el.pdf

Γνώμη 4/2007 σχετικά με την έννοια του όρου «δεδομένα προσωπικού χαρακτήρα», Ομάδα Εργασίας του άρθρου 29, διαθέσιμη σε https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_el.pdf

Γνώμη 3/2010 σχετικά με την αρχή της λογοδοσίας, Ομάδα εργασίας του Άρθρου 29 για την Προστασία των δεδομένων, διαθέσιμη σε https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_el.pdf

Γνώμη 3/2012 για την προστασία των δεδομένων σχετικά με τις εξελίξεις στις βιομετρικές τεχνολογίες, Ομάδα Εργασίας του άρθρου 29, διαθέσιμη σε: https://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_el.pdf

Γνώμη 06/2014 σχετικά με την έννοια των εννόμων συμφερόντων του υπευθύνου επεξεργασίας, σύμφωνα με το άρθρο 7 της οδηγίας 95/46/ΕΚ (WP217), Ομάδα εργασίας του άρθρου 29, διαθέσιμη σε https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_el.pdf

Γνωμοδότηση 15/2011 του Εισαγγελέα του Αρείου Πάγου Αθανασίου Κονταξή διαθέσιμη σε https://eisap.gr/%CE%B3%CE%BD%CF%89%CE%BC%CE%BF%CE%B4%CF%8C%CF%84%CE%B7%CF%83%CE%B7-15-2011/

Γνωμοδότηση της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής με θέμα «Η τεχνητή νοημοσύνη — Η επίδραση της τεχνητής νοημοσύνης στην (ψηφιακή)

ενιαία αγορά, στην παραγωγή, στην κατανάλωση, στην απασχόληση και στην κοινωνία» (υπ' αρ. 2017/C 288/01) της **31.8.2017**, διαθέσιμο σε https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A52016IE5369

Ομάδα εργασίας του άρθρου 29, **Κατευθυντήριες γραμμές σχετικά με τη συγκατάθεση βάσει του κανονισμού 2016/679** (W P 259 αναθ. 01) (Εκδόθηκαν στις 28 Νοεμβρίου 2017 - τελικώς αναθεωρήθηκαν και εκδόθηκαν στις 10 Απριλίου 2018), διαθέσιμο σε https://www.dpa.gr/sites/default/files/2020-02/wp259%20rev%200.1_EL.pdf

Κατευθυντήριες Γραμμές 3/2019 σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω βιντεοσυσκευών διαθέσιμο σε https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_el

Λευκή Βίβλος -- Τεχνητή νοημοσύνη - Η ευρωπαϊκή προσέγγιση της αριστείας και της εμπιστοσύνης, της Ευρωπαϊκής Επιτροπής, COM (2020) 65 final της 19.2.2020, διαθέσιμο σε https://op.europa.eu/el/publication-detail/-/publication/ac957f13-53c6-11ea-aece-01aa75ed71a1

Απόφαση 2008/615/ΔΕΥ του Συμβουλίου, της 23ης Ιουνίου 2008 , σχετικά με την αναβάθμιση της διασυνοριακής συνεργασίας, ιδίως όσον αφορά την καταπολέμηση της τρομοκρατίας και του διασυνοριακού εγκλήματος, διαθέσιμο σε https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:72008D0615GRC_202107343

Πρόταση Απόφαση του Συμβουλίου για την εξουσιοδότηση των κρατών μελών να κυρώσουν, προς το συμφέρον της Ευρωπαϊκής Ένωσης, το πρωτόκολλο για την τροποποίηση της σύμβασης του Συμβουλίου της Ευρώπης για την προστασία των ατόμων σε σχέση με την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα (ETS αριθ. 108) COM(2018) 451 final της 5.6.2018, διαθέσιμο σε https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52018PC0451&from=en

Ευρωπαϊκή Σύμβαση δικαιωμάτων του ανθρώπου, όπως τροποποιήθηκε από τα Πρωτόκολλα υπ' αριθ. 11, 14 και 15, συνοδευόμενη από τα Πρωτόκολλα υπ' αριθ. 1, 4, 6, 7, 12, 13 και 16, υπεγράφη το 1950 διαθέσιμη σε https://www.echr.coe.int/documents/convention_ell.pdf

Οικουμενική Διακήρυξη για τα Ανθρώπινα Δικαιώματα, 10 Δεκεμβρίου 1948, διαθέσιμη σε https://unric.org/el/%CE%BF%CE%B9%CE%BA%CE%BF%CF%85%CE%BC%CE%B5%CE%BD%CE%B9%CE%BA%CE%B7-

%CE%B4%CE%B9%CE%B1%CE%BA%CE%B7%CF%81%CF%85%CE%BE%CE%B7-%CE%B3%CE%B9%CE%B1-%CF%84%CE%B1-%CE%B1%CE%BD%CE%B8%CF%81%CF%89%CF%80%CE%B9-2/

Σύμβαση 108 του Συμβουλίου της Ευρώπης για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων, Στρασβούργο 28-1-1981, διαθέσιμη σε https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108

Συνθήκη Λισαβόνας για την ΕΕ 2012/c326/01 διαθέσιμο στο https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:326:FULL:EL:PDF

Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (2000/C 364/01) διαθέσιμο στο https://www.europarl.europa.eu/charter/pdf/text_el.pdf

ΝΟΜΟΛΟΓΙΑ

ΕΔΔΑ, Υπόθεση S. και Marper κατά Ηνωμένου Βασιλείου, 4.12.2008, σκ. 104-105

ΔΕΕ, Υπόθεση C-212/13, František Ryneš v Úřad pro ochranu osobních údajů, 11.12.2014, παρ. 33

ΔΕΕ, Υπόθεση C-101/01, Ποινική Δίκη Bodil Lindqvist, 6.11.2003, σκ. 47

ΠορισμΑναφΕισΕφΘεσ της 14.10.2013, ''Λήψη και εξέταση γενετικού υλικού'' (**Πορισματική Αναφορά** Ηλία Νικ. Σεφερίδη Εισαγγελέως Εφετών Θεσσαλονίκης προς τον Διευθύνοντα την Εισαγγελία Εφετών Θεσσαλονίκης, διαθέσιμο σε https://www.dsanet.gr/Epikairothta/Nomologia/poranafefthes2013.htm)

ΔΙΑΔΙΚΤΥΑΚΕΣ ΠΗΓΕΣ

Ανδρουλάκη Ευ. (2021), ''Τεχνητή Νοημοσύνη και Προσωπικά Δεδομένα: η περίπτωση της εξ αποστάσεως βιομετρικής ταυτοποίησης'', διαθέσιμο στο https://ejournals.lib.auth.gr/infolawj/

Αρχή Προστασίας Δεδομένων, Τα δικαιώματά μου στο πλαίσιο του ΓΚΠΔ - Δικαίωμα πρόσβασης του υποκειμένου των δεδομένων σε https://dpa.gr/index.php/el/polites/gkpd/dikaiwma_prosvasis_upokeimenou

Βέρρας Δ., ''Το χρονικό του προδιαγεγραμμένου τέλους της ιδιωτικότητας ;'', 01-05-2020, διαθέσιμο στο https://www.lawspot.gr/nomika-blogs/dimitris_verras/clearview-ai-hroniko-toy-prodiagegrammenoy-teloys-tis-idiotikotitas

Διάλεξη του καθηγητή του MIT κ. Κωνσταντίνου **Δασκαλάκη** στο Ευγενίδειο ίδρυμα στις 14.1.2020 σε https://www.youtube.com/watch?v=NWGUjC8f7jQ

Καρβούνης Μ. (2007), Αλγόριθμοι για υπολογιστές, ένας μικρός οδηγός, διαθέσιμο στο https://cgi.di.uoa.gr/~ip/Odigos.pdf

Μπολέτση Ά., ''Clearview AI: Καταγγελίες -και στην Ελλάδα- για παράνομη βάση δεδομένων από φωτογραφίες στα social media: '', 28-5-2021, διαθέσιμο στο https://www.newmoney.gr/roh/palmos-oikonomias/texnologia/clearview-ai-katangelies-ke-stin-ellada-gia-paranomi-vasi-dedomenon-apo-fotografies-sta-social-media

Μπρούμας Αντ. (2011), ''Η Λήψη και Διατήρηση DNA στο Πλαίσιο της Ποινικής Διαδικασίας'', διαθέσιμο σε https://lawandtech.eu/2011/11/18/dna/

Σταμούλης Δημ., Νέες δυνατότητες αναγνώρισης εν κινήσει της ίριδας, 21-4-2015, διαθέσιμο στο https://securityreport.gr/archeio-periodikoy/2015/teychos-42/nees-dynatotites-anagnorisis-en-kinisei-tis-iridas/

Τάσσης Σπ. (2019), ''Το δίκαιο στην εποχή της τεχνητής νοημοσύνης- Μια νέα οπτική στο δίκαιο και την ηθική'', διαθέσιμο στο https://www.lawspot.gr/nomika-blogs/spiros_tassis/dikaio-stin-epohi-tis-tehnitis-noimosynis

Τσόλιας Γρ. (2021), ''Η αναγνώριση και ταυτοποίηση προσώπων για σκοπούς δίωξης του εγκλήματος σύμφωνα με το Σχέδιο Κανονισμού Ε.Ε. για την Τεχνητή Νοημοσύνη'', διαθέσιμο σε https://www.lawspot.gr/nomika-nea/i-anagnorisi-kai-taytopoiisi-prosopon-gia-skopoys-dioxis-toy-egklimatos-symfona-me-shedio (Το κείμενο αποδίδει εμπλουτισμένη προφορική εισήγηση στην εκδήλωση του IAPP Knowledge Net Chapter Greece της 06.5.2021)

Lawspot.gr, ''Κάμερες σε κατοικία: Απαγόρευση χρήσης συστήματος βιντεοεπιτήρησης σε κοινόχρηστο χώρο (ΑΠΔΠΧ 10/2022) '', 15-3-2022, διαθέσιμο στο https://www.lawspot.gr/nomika-nea/kameres-se-katoikia-apagoreysi-hrisis-systimatos-vinteoepitirisis-se-koinohristo-horo

Anil K. Jain/Salil Prabhakar/Arun Ross, An Introduction to Biometric Recognition, σε: 14 IEEE Transactions on Circuits and Systems for Video Technology: Special Issue on Image- and Video-based Biometrics 4, 2004, διαθέσιμο σε: http://biometrics.cse.msu.edu/JainRossPrabhakarCSVT_v15.pdf

Burrows J. (2016), Structure in AI, Law, Ethics, the World and the Mind , διαθέσιμο στο https://medium.com/personified-systems/structure-in-ai-law-ethics-the-world-and-the-mind-7e00c5e0ae2b

Campbell Ch, ''The entire system is designed to suppress us''. What the Chinese Surveillance state means for the rest of the world, Νοέμβριος 2019, διαθέσιμο σε https://time.com/5735411/china-surveillance-privacy-issues/

Dickson B., What is transfer learning?, 10TH June 2019, διαθέσιμο στο https://bdtechtalks.com/2019/06/10/what-is-tranfer-learning

DLA Piper, Data protection laws in the world, China, 27 Ιανουαρίου 2022, διαθέσιμο σε https://www.dlapiperdataprotection.com/index.html?c=CN&t=law

Int'l Civil Aviation Org. (ICAO), Technical Report: Development of a Logical Data Structure- (LDS) for Optional Capacity Expansion Technologies, Revision 1.7, 10-16 (18.5.2004) , διαθέσιμο σε http://www.icao.int/mrtd/download/documents/LDS-technical%20 report%202004.pdf

Logg J. (2018), ''Do People Trust Algorithms More Than Companies Realize?'', https://hbr.org/2018/10/do-people-trust-algorithms-more-than-companies-realize

Logg, J.M., Minson, J.A., & Moore,D.A. (2019). Algorithm Appreciation : People prefer algorithmic to human judgement. Organizational Behavior and Human Decision Processes, 151, 90-103, https://www.sciencedirect.com/science/article/abs/pii/S0749597818303388

McCarthy J., ''WHAT IS ARTIFICIAL INTELLIGENCE ? , Basic Questions'', διαθέσιμο στο http://www-formal.stanford.edu/jmc/whatisai.pdf

Miyamoto I.(2020), ''Debating aspects of surveillance through case studies – Social media and Facial Recognition'' στο *Surveillance Technology challenges political culture of democratic states*, διαθέσιμο στο https://dkiapcss.edu/wp-content/uploads/2020/09/04-miyamoto-25thA.pdf

Shaw R. (2019), ''The 10 best machine learning algorithms for date science beginners'', διαθέσιμο στο https://www.dataquest.io/blog/top-10-machine-learning-algorithms-for-beginners/

Syta E., Fischer M. J., Wolinsky D., Silberschatz A., Gallegos-Garcia G. and Ford B. (2015), ''Private Eyes: Secure Remote Biometric Authentication'', https://dedis.cs.yale.edu/dissent/papers/secrypt15- biometric.pdf

Turing Alan, ''Computing machinery and intelligence'', Mind, 59, 1950 διαθέσιμο στο http://www.turing.org.uk/turing/scrapbook/test.html

Webmedia, ''Πρόστιμο στην Clearview AI για παράνομη αποθήκευση εικόνων προσώπου στο Ηνωμένο Βασίλειο'', 27-5-2022, διαθέσιμο στο https://thinktech.gr/%CF%80%CF%81%CF%8C%CF%83%CF%84%CE%B9%CE%BC%CE%BF-%CF%83%CF%84%CE%B7%CE%BD-clearview-ai-%CE%B3%CE%B9%CE%B1-%CF%80%CE%B1%CF%81%CE%AC%CE%BD%CE%BF%CE%BC%CE%B7-%CE%B1%CF%80%CE%BF%CE%B8%CE%AE%CE%BA%CE%B5

Zhang Ph. , ''Chinese court names and shames debtors in warm-up to Avengers movie'', Απρίλιος 2019, διαθέσιμο σε https://www.thestar.com.my/news/regional/2019/04/26/chinese-court-names-and-shames-debtors-in-warmup-to-avengers-movie

Zhang J., ''In Chongquing, the world's most surveilled city, residents are happy to trade privacy for security'', Οκτώβριος 2019, διαθέσιμο σε https://www.scmp.com/tech/policy/article/3031390/chongqing-worlds-most-surveilled-city-these-residents-are-happy-trade

''Types of artificial intelligence Algorithms You Should know (A Complete Guide)''(2022), διαθέσιμο στο https://www.upgrad.com/blog/types-of-artificial-intelligence-algorithms/

https://el.wikipedia.org/wiki/%CE%91%CE%BB%CE%B3%CF%8C%CF%81%CE%B9%CE%B8%CE%BC%CE%BF%CF%82

https://en.wikipedia.org/wiki/List_of_artificial_intelligence_films

https://techcrunch.com/2017/01/28/artificial-intelligence-and-the-law/?guccounter