ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»

Ακαδημαϊκό έτος 2021-2022

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της Δανάης- Διονυσίας Αθανασοπούλου (Α.Μ.: ΜΔΙ2001)

ΣΥΣΤΗΜΑΤΑ ΑΝΑΓΝΩΡΙΣΗΣ ΠΡΟΣΩΠΟΥ ΜΕ ΧΡΗΣΗ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ ΚΑΙ ΖΗΤΗΜΑΤΑ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Επιβλέπουσα Καθηγήτρια:

κα Λίλιαν Μήτρου

Πειραιάς, 2022

ΠΕΡΙΕΧΟΜΕΝΑ

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

ΑΠΔΠΧ:	Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
αρ.:	άρθρο
ΓΚΠΔ:	Γενικός Κανονισμός Προστασίας Δεδομένων
ΔΕΕ:	Δικαστήριο Ευρωπαϊκής Ένωσης
ΕΑΠΔ:	Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων
ΕΔΔΑ:	Ευρωπαϊκό Δικαστήριο Δικαιωμάτων του Ανθρώπου
ΕΕ:	Ευρωπαϊκή Ένωση
ΕΕΠΔ:	Ευρωπαίος Επόπτης Προστασίας Δεδομένων
ΕΣΔΑ:	Ευρωπαϊκή Σύμβαση των Δικαιωμάτων του Ανθρώπου
ΕΣΠΔ:	Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων
ΗΠΑ:	Ηνωμένες Πολιτείες της Αμερικής
κ.α.:	και άλλα
κ.ο.κ.:	και ούτω καθεξής
κλπ.:	και λοιπά
λ.χ.:	λόγου χάριν
ν.:	νόμος
ο.π.:	όπως παραπάνω
Π.Δ.:	Προεδρικό Διάταγμα
π.χ.:	παραδείγματος χάριν
παρ.:	παράγραφος
περ.:	περίπτωση
στοιχ.:	στοιχείο
σχ. Καν. ΤΝ:	Σχέδιο Κανονισμού για την Τεχνητή Νοημοσύνη
ΤΝ:	Τεχνητή Νοημοσύνη
ΧΘΕΕ:	Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης
AI:	Artificial Intelligence
C:	Case
CNIL:	Commission Nationale Informatique & Libertés
EDRI :	European Digital Rights
FRTs:	Facial Recognition Technologies
GDPR:	General Data Protection Regulation
ICO:	Information Commissioner's Office
LFRT:	Live Facial Recognition Technology
QR :	Quick Response
RBI:	Remote Biometric Identification

ΠΕΡΙΛΗΨΗ

Η αστραπιαία εξάπλωση των συστημάτων αναγνώρισης προσώπου, κατόπιν της ενδυνάμωσης αυτών με εφαρμογές τεχνητής νοημοσύνης, κατέστησε άμεσα αντιληπτή τη δυναμική της τεχνολογίας, αλλά και την εγγενώς παρεμβατική φύση της για τα θεμελιώδη δικαιώματα και τις ελευθερίες των ανθρώπων στις σύγχρονες δημοκρατικές κοινωνίες. Το παρόν πόνημα εκκινεί με την επισκόπηση της τεχνολογίας αναγνώρισης προσώπου, των ιδιαιτέρων χαρακτηριστικών και της εμβέλειας χρήσης της. Στη συνέχεια επιχειρείται η επισήμανση των ανεγειρόμενων ανησυχιών, όπως προκύπτουν από τα τρωτά σημεία της τεχνολογίας, αλλά και των επαπειλούμενων επιπτώσεων στα θεμελιώδη ανθρώπινα δικαιώματα, με ιδιαίτερη έμφαση στους νέους και πρωτοφανώς έντονους κινδύνους που απειλούν να κλονίσουν στον πυρήνα του το δικαίωμα στην προστασία δεδομένων προσωπικού χαρακτήρα. Ακολουθεί η αποτίμηση του ισχύοντος νομικού πλαισίου της Ευρωπαϊκής Ένωσης, σε πρωτογενές και δευτερογενές επίπεδο, και η ειδικότερη εξέταση της συμβατότητας της ανάπτυξης και χρήσης των συστημάτων αναγνώρισης προσώπου με τις αρχές και τα προαπαιτούμενα που θέτει το κοινοτικό κεκτημένο για την προστασία των δεδομένων προσωπικού χαρακτήρα. Τέλος, αναλύεται επικουρικά το προταθέν σχέδιο Κανονισμού της Ευρωπαϊκής Επιτροπής για την Τεχνητή Νοημοσύνη, στο βαθμό που ενδέχεται να συνδιαμορφώσει το ρυθμιστικό πλαίσιο της τεχνολογίας αναγνώρισης προσώπου στην Ευρωπαϊκή Ένωση.

Λέξεις- κλειδιά: συστήματα αναγνώρισης προσώπου, τεχνητή νοημοσύνη, βιομετρικά δεδομένα, προστασία δεδομένων προσωπικού χαρακτήρα, Γενικός Κανονισμός Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΕΕ) 2016/679, Οδηγία (ΕΕ) 2016/680

ΕΙΣΑΓΩΓΗ

Η ανάπτυξη και η καθολική χρήση τεχνολογιών αναγνώρισης προσώπου που αποσκοπούν στην ταυτοποίηση φυσικών προσώπων δια της επεξεργασίας των βιομετρικών τους δεδομένων, η οποία πολλώ δε μάλλον βασίζεται σε συστήματα, εφαρμογές και λογισμικά τεχνητής νοημοσύνης, ενδεχομένως να φαντάζει prima facie ως θεωρητικό κατασκεύασμα στη σφαίρα της δυστοπικής επιστημονικής φαντασίας· εντούτοις, οι απαρχές των συστημάτων αναγνώρισης προσώπου δύναται να εντοπιστούν ήδη από τη δεκαετία του 1960.

Το πρώτο γνωστό εγχείρημα εμφανίζεται το 1964, όταν ο Αμερικανός μαθηματικός και επιστήμονας υπολογιστών Woodrow Wilson Bledsoe ανέπτυξε ένα σύστημα ταξινόμησης φωτογραφιών μετρώντας τις αποστάσεις μεταξύ διαφορετικών χαρακτηριστικών προσώπων από φωτογραφίες συλλήψεων, τις οποίες εν συνεχεία εισήγαγε σε ένα πρόγραμμα υπολογιστή προκειμένου να τις αντιπαραβάλλει με πρόσωπα υπόπτων. Το σύστημα, παρότι ιδιαιτέρως αργό και κοστοβόρο για τα δεδομένα της εποχής, κατάφερε να αναδείξει τις δυνατότητες της τεχνολογίας και σύντομα κέντρισε το ενδιαφέρον των διωκτικών αρχών, οι οποίες φαίνεται ότι χρηματοδότησαν τη συνέχιση της έρευνας του Bledsoe, τα αποτελέσματα της οποίας εν τέλει δεν δόθηκαν στη δημοσιότητα[1]. Ωστόσο, η πρώιμη επιτυχία του εν λόγω προγράμματος έδωσε το έναυσμα για δεκαετίες ερευνών προσανατολισμένων στη διδασκαλία των μηχανών να αναγνωρίζουν και να ταυτοποιούν με αποτελεσματικότητα και ακρίβεια τα ανθρώπινα πρόσωπα[2].

Σήμερα, οι ερευνητές κατατάσσουν, κατ' αρχήν, την εξέλιξη των συστημάτων αναγνώρισης προσώπου σε τέσσερις μεγάλες ιστορικές περιόδους, καθεμία από τις οποίες επισφραγίζεται από την αυξανόμενη ανάγκη βελτίωσης της υπάρχουσας τεχνολογίας, προκειμένου να καταστεί εφικτό, ποιοτικά και ποσοτικά, το προσδοκώμενο αποτέλεσμα αναγνώρισης και ταυτοποίησης επί τη βάση της μορφολογίας του ανθρώπινου προσώπου. Η πρώτη περίοδος, η οποία διήρκησε μέχρι τη δεκαετία του 1990, χαρακτηριζόταν σε μεγάλο βαθμό από μη αυτοματοποιημένες -και ως εκ τούτου βραδείς- μεθόδους. Αναμφίβολα, όμως, καινοτόμες για την εποχή τους τεχνικές, όπως οι περίφημες «Eigenface» και

---

[1] Klosowski, T. (2020) 'Facial Recognition Is Everywhere . Here ' s What We Can Do About It.', *The New York Times*, σελ. 1–12. Διαθέσιμο στο: https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/.

[2] Hao, K. (2021) 'This is how we lost control of our faces', *MIT Technology Review*, σελ. 1–9. Διαθέσιμο στο: https://www.technologyreview.com/2021/02/05/1017388/ai-deep-learning-facial-recognition-data-history/.

«Fisherfaces» [3], βελτίωσαν αισθητά την ικανότητα της τεχνολογίας να εντοπίζει ένα πρόσωπο και να αναγνωρίζει τα χαρακτηριστικά του, χαράσσοντας έτσι το δρόμο για τα σύγχρονα αυτοματοποιημένα συστήματα.

Στη συνέχεια, νευραλγικό ρόλο στην εξέλιξη της τεχνολογίας αναγνώρισης προσώπου και στην απαρχή της δεύτερης ιστορικής περιόδου αυτής, διαδραμάτισαν το Υπουργείο Άμυνας των Η.Π.Α. και το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (National Institute of Science and Technology- NIST), τα οποία, με εφαλτήριο τη συνειδητοποίηση ότι η αναγνώριση προσώπου θα μπορούσε να υπερβαίνει σε αποτελεσματικότητα την παρακολούθηση και ταυτοποίηση δια μέσου των δακτυλικών αποτυπωμάτων, διέθεσαν το ποσό των 6,5 εκατομμυρίων δολαρίων για τη δημιουργία του πρώτου συνόλου δεδομένων προσώπου μεγάλης κλίμακας. Έτσι, κατόπιν δεκαπέντε συνεδριών φωτογράφισης σε διάστημα τριών ετών και σε ημι-ελεγχόμενο περιβάλλον, το πρόγραμμα κατέγραψε 14.126 εικόνες 1.199 ατόμων. Ακολούθως, η βάση δεδομένων κυκλοφόρησε το 1996 με το όνομα «FERET» (Face Recognition Technology) και αποτέλεσε τη μεγαλύτερη και πιο ολοκληρωμένη έως τότε προσπάθεια για τη δημιουργία ενός προτύπου αναφοράς για τη σύγκριση και ακριβή αξιολόγηση των υπαρχόντων αλγορίθμων αναγνώρισης προσώπου[4].

Η επιτυχία που σημείωσε η βάση δεδομένων «FERET» πυροδότησε κατά την επόμενη δεκαετία μια εντατικοποίηση της ακαδημαϊκής αλλά και της εμπορικής έρευνας ως προς την αξιοποίηση της τεχνολογίας αναγνώρισης προσώπου, με αποτέλεσμα να δημιουργηθούν πολλά ακόμη σύνολα δεδομένων. Η συντριπτική πλειονότητα των εν λόγω συνόλων δεδομένων προήλθε από φωτογραφίσεις μετά της πλήρους συγκατάθεσης των συμμετεχόντων, ενώ πολλά περιελάμβαναν, επίσης, μεταδεδομένα, όπως η ηλικία και η εθνικότητα των υποκειμένων. Εντούτοις αυτά τα πρώιμα συστήματα έπασχαν αποτελεσματικότητας σε πραγματικές συνθήκες, γεγονός που οδήγησε τους ερευνητές να αναζητήσουν ακόμη μεγαλύτερα και ποικιλόμορφα σύνολα δεδομένων.

Ακολούθησε, το 2007, η ανάπτυξη του συνόλου δεδομένων «Labeled Faces in the Wild» (LFW), η οποία άνοιξε τον ασκό του Αιόλου για την αχαλίνωτη συλλογή δεδομένων δια μέσου του Διαδικτύου και σηματοδότησε την αρχή της

---

[3] 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.

[4] Raji, I.D. and Fried, G. (2021) 'About Face: A Survey of Facial Recognition Evaluation'. σελ 2-4. Διαθέσιμο στο: http://arxiv.org/abs/2102.00813 (Ανάκτηση: Ιούνιος 2022)

τρίτης ιστορικής περιόδου των τεχνολογιών αναγνώρισης προσώπου. Οι ερευνητές άρχισαν πλέον να αντλούν δεδομένα απευθείας από ιστοσελίδες όπως οι Google, Flickr και Yahoo, δίχως να αναζητούν τη συγκατάθεση των υποκειμένων, ακόμα και όταν οι φωτογραφίες απεικόνιζαν ανηλίκους, με απώτερο στόχο να επιτύχουν την πολυπόθητη ποικιλομορφία που θα εξασφάλιζε την καλύτερη δυνατή απόδοση της τεχνολογίας. Πράγματι, κατ' αυτόν τον τρόπο δημιουργήθηκαν σημαντικά μεγαλύτερα σύνολα δεδομένων σε σύντομο χρονικό διάστημα, ωστόσο η τεχνολογία αναγνώρισης προσώπου εξακολουθούσε σε αυτό το χρονικό σημείο να είναι περιορισμένα αποτελεσματική, καθώς το ερευνητικό πρόβλημα της αναγνώρισης προσώπων σε πραγματικές συνθήκες, εκτός ελεγχόμενων περιβαλλόντων, παρέμεινε μια απροσπέλαστη τεχνική πρόκληση.

Κομβικό σημείο στην ιστορία των συστημάτων αναγνώρισης προσώπου, το οποίο άλλαξε ριζικά τα έως τότε τεχνολογικά δεδομένα σηματοδοτώντας την αρχή της τέταρτης και πλέον επαναστατικής ιστορικής τους περιόδου, αποτέλεσε η ανάπτυξη, το έτος 2014, ενός μοντέλου βαθιάς μάθησης επ' ονόματι DeepFace, από την εταιρεία Facebook. Αν και η εταιρεία δεν έδωσε ποτέ στη δημοσιότητα το σύνολο των δεδομένων που χρησιμοποιήθηκε για την εκπαίδευση του μοντέλου, η άνευ προηγουμένου επίδοση του συστήματος[5], το οποίο συνάγεται ότι άντλησε δεδομένα κυρίως από τις φωτογραφίες των χρηστών της πλατφόρμας, ανέδειξε τη βαθιά μάθηση ως την de facto μέθοδο ανάλυσης προσώπων. Ταυτοχρόνως όμως, η καθολική επικράτηση των τεχνικών βαθιάς μάθησης στην ανάπτυξη των συστημάτων αναγνώρισης προσώπου, έθεσε νέες προκλήσεις και συνέβαλε σε ακόμα μεγαλύτερη αύξηση του μεγέθους των συνόλων δεδομένων που κατασκευάστηκαν στη συνέχεια, προκειμένου να καλυφθούν οι επίσης αυξανόμενες απαιτήσεις ως προς τον επιζητούμενο όγκο των δεδομένων για την βέλτιστη εκπαίδευση των αλγορίθμων.

Επακολούθως, η ταχεία τεχνολογική πρόοδος και η πρωτοφανής αποτελεσματικότητα του μοντέλου DeepFace, προκάλεσαν υψηλό εμπορικό ενδιαφέρον και μια νοητή στροφή προς την εμπορική αξιοποίηση της τεχνολογίας αναγνώρισης προσώπου. Στον ιδιωτικό τομέα, επιχειρήσεις άρχισαν τον πειραματισμό και την εργαλειοποίηση μεθόδων αναγνώρισης προσώπου με γνώμονα τη μεγιστοποίηση των κερδών, με αποτέλεσμα ποικίλα συστήματα αναγνώρισης προσώπου να χρησιμοποιούνται πλέον ευρέως για σκοπούς διαφημιστικούς, κυρίως δε για την ταυτοποίηση των πελατών και την κατάρτιση προφίλ προκειμένου να προβλεφθούν οι καταναλωτικές συνήθειες και προτιμήσεις τους. Προσέτι, παρατηρήθηκε η αξιοποίηση της τεχνολογίας και για ποικίλους οργανωτικούς σκοπούς των εταιρειών, οι οποίοι κυμαίνονται από τη

[5] Το μοντέλο DeepFace πέτυχε ακρίβεια 97,35 % στο Labeled Faces in the Wild (LFW) test, ο.π. Raji, I.D. and Fried, G. (2021) σελ. 3.

βελτιστοποίηση των εσωτερικών λειτουργικών συστημάτων τους, έως την χρήση της τεχνολογίας κατά τη διενέργεια προσλήψεων ανθρώπινου δυναμικού[6].

Παραλλήλως, η δυναμική των τεχνολογιών αναγνώρισης προσώπου, η οποία από την πρώτη στιγμή προσέλκυσε τις αρχές επιβολής του νόμου, αναζωπύρωσε το ενδιαφέρον του δημοσίου τομέα, αφενός λόγω των νέων δυνατοτήτων που προσφέρει η τεχνολογία με την Τεχνητή Νοημοσύνη ως πολλαπλασιαστή δύναμης αυτής, αφετέρου λόγω του μειωμένου κόστους, της μαζικότητας και της ευκολίας συλλογής, σε σχέση με άλλα βιομετρικά δεδομένα, που παρέχουν τα αλγοριθμικά συστήματα.

Ακολούθως, συστήματα αναγνώρισης προσώπου εγκαταστάθηκαν σε αεροδρόμια, καταστήματα, εμπορικά κέντρα, στην είσοδο ελεγχόμενων χώρων, όπως και στη δημόσια σφαίρα[7]. Απέκτησαν δημοφιλία[8] τόσο στην Ευρώπη, ιδιαίτερα δε στο Ηνωμένο Βασίλειο, στην Ουγγαρία, στην Τσεχία, στη Σουηδία, στη Γερμανία, όσο και διεθνώς, με την Κίνα και τις Η.Π.Α. να πρωτοστατούν τόσο στη χρήση όσο και στην ίδια την ανάπτυξη της τεχνολογίας, επιδιδόμενες σε έναν αγώνα δρόμου για την επικράτηση στον εν λόγω τεχνολογικό τομέα διεκδικώντας – κατ' επέκτασην- τη μερίδα του λέοντος στην εμπορική εκμετάλλευση της τεχνολογίας. Αρχικώς, η χρήση των μεθόδων αναγνώρισης προσώπου επικεντρώθηκε στον ακριβή εντοπισμό ατόμων, στον έλεγχο των συνόρων και στην ενίσχυση της ασφάλειας. Σύντομα όμως, η αναγνώριση προσώπου εισήλθε σε όλες τις εκφάνσεις της σύγχρονης καθημερινότητας, ακόμη και στις προσωπικές συσκευές ως χαρακτηριστικό ασφαλείας, με την τεχνολογία Windows Hello και το Trusted Face του λειτουργικού συστήματος Android το 2015 να παίρνουν τα ηνία, και να ακολουθούνται, το 2017, από την εισαγωγή του Face ID στα μοντέλα iPhone X.

Ergo, η αστραπιαία εξάπλωση των τεχνολογιών αναγνώρισης προσώπου καθώς και η ενδυνάμωση αυτών με την ευρεία χρήση συστημάτων Τεχνητής Νοημοσύνης, κατέστησε άμεσα σαφές ότι η ανθρωπότητα έχει περιέλθει σε μια νέα κοινωνικοοικονομική πραγματικότητα, στην οποία η τεχνολογία αναγνώρισης προσώπου αποτελεί δεδομένο της καθημερινότητας. Εντούτοις,

---

[6] Η εταιρεία «HireVue» αναφέρει ότι παραπάνω από 700 εταιρείες, συμπεριλαμβανομένων των Unilever, Delta και Hilton, χρησιμοποιούν την τεχνολογία της, βλ. Knight, W. (2021) *Job Screening Service Halts Facial Analysis of Applicants*, *WIRED*. Διαθέσιμο στο: https://www.wired.com/story/job-screening-service-halts-facial-analysis-applicants/

[7] Κανέλλος, Λ. (2020) *The GDPR Handbook*. Νομική Βιβλιοθήκη. σελ. 337-338.

[8] European Union Agency for Fundamental Rights (2019) 'Facial recognition technology: fundamental rights considerations in the context of law enforcement'. σελ. 7-9. Διαθέσιμο στο: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf.

εξίσου άμεσα κατέστη αντιληπτό ότι η εγγενώς παρεμβατική φύση της τεχνολογίας αυτής, καθώς και η ανοριοθέτητη μετάβασή της στο δημόσιο forum, θέτει σοβαρά διλήμματα και προβληματισμούς αναφορικά με τις πιθανές παραβιάσεις θεμελιωδών δικαιωμάτων, κυρίως ως προς την επαπειλούμενη παραβίαση του πυρήνα των δικαιωμάτων στην ιδιωτικότητα και στην προστασία των δεδομένων προσωπικού χαρακτήρα.

Δεν αποτελεί, συνεπώς, έκπληξη πως οι αντιδράσεις της παγκόσμιας κοινότητας υπήρξαν σφοδρές από την πρώτη στιγμή που κατέστη σαφής η επέκταση της τεχνολογίας[9], με τους επιστήμονες να κρούουν τον κώδωνα του κινδύνου για τις αναπόφευκτες επιπτώσεις μίας άκριτης και απεριόριστης εξάπλωσης επεμβατικών τεχνολογιών τέτοιου βεληνεκούς στα ανθρώπινα δικαιώματα· μάλιστα, το 2011 ο επικεφαλής του τεχνολογικού κολοσσού της Google Inc. δήλωσε δημοσίως ότι η τεχνολογία αναγνώρισης προσώπου ήταν η μόνη που η εταιρεία αρνούταν να διερευνήσει επισταμένως, ακριβώς λόγω της κρισιμότητας των πιθανών επιπτώσεων[10]. Προσέτι, ιδιαίτερη ανησυχία προκάλεσε εξυπαρχής η κλίμακα χρήσης της τεχνολογίας αναγνώρισης προσώπου και των καμερών παρακολούθησης από τη Λαϊκή Δημοκρατία της Κίνας[11], έτι περισσότερο λόγω της ενσωμάτωση αυτών σε ένα πλαίσιο κοινωνικής αξιολόγησης και ιεράρχησης των πολιτών της, πρακτική που αποτέλεσε αντικείμενο έντονων συζητήσεων στη διεθνή κοινότητα.

Ωστόσο, η συνειδητοποίηση, ιδιαίτερα στην Ευρώπη, του κεφαλαιώδους αντικτύπου και των επακόλουθων της ένταξης στο δημόσιο βίο της τεχνολογίας αναγνώρισης προσώπου, εισέβαλε ως κεραυνός εν αιθρία το 2020, όταν η εφημερίδα New York Times έφερε στο προσκήνιο μια νεοφυή και εν πολλοίς άγνωστη μέχρι τότε εταιρεία, τη διαβόητη πλέον «Clearview AI»[12]. Όπως αποκαλύφθηκε, η Clearview AI, μια εταιρεία που ιδρύθηκε από τους Hoan Ton-

---

[9] Ήδη το 2001, κατόπιν χρήσης τεχνολογιών αναγνώρισης προσώπου στον αγώνα «Super Bowl» από τις διωκτικές αρχές, υπήρξε έντονη αντίδραση, με τους επικριτές να επικαλούνται παραβίαση της Τέταρτης Τροπολογίας. Λίγα χρόνια αργότερα, άρχισαν να υιοθετούνται νομοθετικά πλαίσια που έθεταν σαφείς περιορισμούς στην παράνομη συλλογή και αποθήκευση βιομετρικών πληροφοριών, συμπεριλαμβανομένων φωτογραφιών προσώπων. βλ. ό.π. Klosowski, T. (2020).

[10] Hill, K. (2020) 'The Secretive Company That Might End Privacy as We Know It', *The New York Times*. Διαθέσιμο στο: https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html. Ωστόσο, λίγα χρόνια αργότερα, ερευνητές της εταιρείας ανέπτυξαν το σύστημα αναγνώρισης προσώπου «FaceNet», βλ. Thales Group (2021) 'Facial Recognition'. Διαθέσιμο στο: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/facial-recognition

[11] Panahov, H. (2022) 'Why the US Needs Federal Law on Facial Recognition Technology', *Intersect*, 15(2) σελ. 5.

[12] Hill, K. (2020) ο.π.

That και Richard Schwartz στις Ηνωμένες Πολιτείες, δρούσε κρυφίως πωλώντας σε αρχές επιβολής του νόμου και σε ιδιωτικές επιχειρήσεις ασφάλειας, λογισμικό αναγνώρισης προσώπου το οποίο αντλεί δεδομένα από μια βάση δεδομένων που εμπεριέχει, κατά τα λεγόμενα της ίδιας της εταιρείας, κατ' ελάχιστον 3 δισεκατομμύρια φωτογραφίες, οι οποίες έχουν περισυλλεχθεί αδιακρίτως από πηγές σε όλο το διαδίκτυο, συμπεριλαμβανομένων των μέσων κοινωνικής δικτύωσης Facebook, YouTube και Venmo. Μάλιστα, τον Φεβρουάριο του 2020, κατόπιν διάρρευσης του πελατολογίου της εταιρείας, αποκαλύφθηκε προς έκπληξη της παγκόσμιας κοινής γνώμης ότι, εκτός από κυβερνητικές υπηρεσίες και εταιρείες των Η.Π.Α., στη λίστα πελατών συμπεριλαμβάνονταν, μεταξύ άλλων, η Μητροπολιτική Αστυνομική Υπηρεσία του Λονδίνου, καθώς και διωκτικές αρχές από το Βέλγιο, τη Δανία, τη Φινλανδία, τη Γαλλία, την Ιρλανδία, την Ιταλία, τη Λετονία, τη Λιθουανία, τη Μάλτα, τις Κάτω Χώρες, τη Νορβηγία, την Πορτογαλία, τη Σερβία, τη Σλοβενία, την Ισπανία, τη Σουηδία και την Ελβετία.

Οι αντιδράσεις ήταν, όπως εύλογα συνάγεται, θυελλώδεις και πολλές μη κυβερνητικές οργανώσεις προχώρησαν σε έκκληση ολικής απαγόρευσης της χρήσης του ανωτέρω λογισμικού εξαιτίας της ανήθικης συλλογής των δεδομένων μέσω της μεθόδου «ιστοσυγκομιδής» (data scrapping), αλλά και των επαπειλούμενων κινδύνων για τα θεμελιώδη δικαιώματα των πολιτών. Παραλλήλως, πολλές από τις εταιρείες κοινωνικής δικτύωσης που βρέθηκαν στο στόχαστρο μετά τις αποκαλύψεις, απαγόρευσαν στην Clearview AI να αντλεί δεδομένα από τις πλατφόρμες τους[13], ενώ πλειάδα χωρών κινήσαν νομικές διαδικασίες κατά της εταιρείας προκειμένου να προστατεύσουν τους πολίτες τους.

Η γνωστοποίηση της δράσης εταιρειών όπως η Clearview AI, η οποία αποτελεί κραυγαλέο αλλά όχι μοναδικό παράδειγμα εταιρείας που δραστηριοποιείται στο πεδίο της τεχνολογίας αναγνώρισης προσώπου χρησιμοποιώντας αθέμιτες πρακτικές συλλογής δεδομένων, ανέδειξε τη βαρύτητα της εργαλειοποίησης των συστημάτων τεχνητής νοημοσύνης στην ανάπτυξη και εξάπλωση μεθόδων αναγνώρισης και ταυτοποίησης προσώπου, όπως και την απτή πιθανότητα κεφαλαιωδών παραβιάσεων θεμελιωδών ανθρωπίνων δικαιωμάτων· η ασφάλεια που ευαγγελίζεται η τεχνολογία αναγνώρισης προσώπου και η εξασφάλιση της απρόσκοπτης επιστημονικής έρευνας, συγκρούονται με την ανάγκη θωράκισης των σύγχρονων δημοκρατιών έναντι μιας τεχνολογίας φύσει παρεμβατικής και απειλητικής για θεμελιώδη δικαιώματα, η οποία εγείρει, ευλόγως, μια σειρά από σοβαρούς προβληματισμούς

[13] Hill, K. (2020) 'Twitter Tells Facial Recognition Trailblazer to Stop Using Site's Photos', *The New York Times*. Διαθέσιμο στο: https://www.nytimes.com/2020/01/22/technology/clearview-ai-twitter-letter.html

και ανησυχίες για την σταδιακή εγκαθίδρυση ενός καθεστώτος «*κράτους παρακολούθησης*» (surveillance state).

Σκοπός της παρούσας μελέτης αποτελεί η κατά το δυνατόν πιο μεστή παρουσίαση της τεχνολογίας αναγνώρισης προσώπου, της εμβέλειας χρήσης και της θέσης της στον παγκόσμιο χάρτη, η ανάδειξη της προβληματικής που εγείρεται για τα θεμελιώδη δικαιώματα και ιδιαίτερα για την προστασία δεδομένων προσωπικού χαρακτήρα, καθώς και η αποτίμηση της αποτελεσματικότητας -ή μη- του ισχύοντος ρυθμιστικού πλαισίου στην Ευρωπαϊκή Ένωση.

1. Συστήματα αναγνώρισης προσώπου με χρήση Τεχνητής Νοημοσύνης: έννοια & χαρακτηριστικά

1.1 Οι εικόνες προσώπου ως βιομετρικά δεδομένα

Κατ' αρχάς, οφείλει να διασαφηνιστεί ότι οι ανθρώπινες εικόνες προσώπου συγκαταλέγονται στα λεγόμενα «*βιομετρικά δεδομένα*», λόγω της καθολικότητάς, της μοναδικότητάς και της μονιμότητάς τους στο χρόνο. Ειδικότερα, ο ορισμός των εν λόγω δεδομένων έχει αποκρυσταλλωθεί σε ποικίλα νομοθετήματα της Ευρωπαϊκής Ένωσης, αλλά και στην ελληνική νομοθεσία[14], ως εξής:

Ως βιομετρικά δεδομένα νοούνται «*δεδομένα προσωπικού χαρακτήρα τα 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*». Πρόκειται, δηλαδή, για ευαίσθητα προσωπικά δεδομένα που εξάγονται κατόπιν ειδικής τεχνικής επεξεργασίας ανθρώπινων χαρακτηριστικών, τα οποία, λόγω των εγγενών τους ιδιοτήτων, είναι πρόσφορα και ικανά να οδηγήσουν στην εξακρίβωση της ταυτότητας του υποκειμένου τους.

Περαιτέρω, ως ***βιομετρικές μέθοδοι*** νοούνται *οι τεχνικές πιστοποίησης της ταυτότητας των φυσικών προσώπων μέσω της ανάλυσης των σταθερών χαρακτηριστικών τους*[15]. Οι εν λόγω βιομετρικές τεχνικές δύναται να ταξινομηθούν, κατ' αρχήν, σε δύο κατηγορίες:

i) στις τεχνικές που στηρίζονται στην ανάλυση φυσικών ή γενετικών χαρακτηριστικών (κυρίως, δακτυλικών αποτυπωμάτων, της γεωμετρίας της παλάμης, της κόρης του ματιού, **των χαρακτηριστικών του προσώπου**, αίματος, σάλιου, D.N.A.) και

ii) στις τεχνικές που στηρίζονται στην ανάλυση συμπεριφοράς (όπως υπογραφής, φωνής, βαδίσματος, χειρονομιών[16]).

Πιο συγκεκριμένα, οι βιομετρικές μέθοδοι επιτρέπουν αρχικώς την ταυτοποίηση και ακολούθως την επιβεβαίωση της ταυτότητας ενός προσώπου,

---

[14] Βλ. αρθ. 3§13 της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, άρθ. 4§14 του Γενικού Κανονισμού Προστασίας Δεδομένων, αρθ. 3§18 του Κανονισμού (ΕΕ) 2018/1725, άρθ. 44 περ. ιβ' του ν. 4624/2019.

[15] Βλ. https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/eidikeskatigories/biometrikadedomena

[16] Thales Group (2021) 'Biometrics (facts, use cases, biometric security)'. Διαθέσιμο στο: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics

επί τη βάση επαληθεύσιμων μοναδικών και συγκεκριμένων δεδομένων. Ειδικότερα, η βιομετρική ταυτοποίηση συνίσταται στον προσδιορισμό της ταυτότητας ενός φυσικού προσώπου με τη λήψη ενός στοιχείου των βιομετρικών δεδομένων του (π.χ. της εικόνας προσώπου του) και τη σύγκρισή του με τα βιομετρικά δεδομένα που φυλάσσονται σε μια βάση δεδομένων, προκειμένου να εξεταστεί εάν αυτό συγκαταλέγεται μεταξύ των φυλασσόμενων υποδειγμάτων. Κατόπιν της ταυτοποίησης του υποκειμένου, ακολουθεί η επαλήθευση/ επιβεβαίωση της ταυτότητάς του, η οποία συντελείται δια της σύγκρισης αφενός των δεδομένων που αντλούνται από τα φυσικά χαρακτηριστικά του και αφετέρου των βιομετρικών δεδομένων που φυλάσσονται στην εκάστοτε βάση και θεωρείται ότι του ανήκουν, προκειμένου να εξεταστεί περαιτέρω η εντοπισθείσα ομοιότητα και τελικά να εξακριβωθεί εάν αφορούν πράγματι στο ίδιο φυσικό πρόσωπο.

Προσέτι, η κατά τα ανωτέρω επεξεργασία των εικόνων προσώπου ρυθμίζεται, σε ενωσιακό επίπεδο, από το προστατευτικό πλέγμα διατάξεων της ευρωπαϊκής νομοθεσίας για την προστασία δεδομένων προσωπικού χαρακτήρα. Μάλιστα, λόγω του ευαίσθητου χαρακτήρα τους και των πιθανών κινδύνων που εγκυμονεί η συλλογή και η επεξεργασία τους για θεμελιώδη ανθρώπινα δικαιώματα, οι εικόνες προσώπου εντάσσονται, κατ' αρχήν, στις «*ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα*», η επεξεργασία των οποίων, πλην ρητών εξαιρετέων περιπτώσεων, απαγορεύεται και απολαμβάνει ενισχυμένης προστασίας και πρόσθετων εγγυήσεων[17].

Ωστόσο, οφείλει να επισημανθεί εν προκειμένω ότι, σύμφωνα την υπ' αριθ. 51 αιτιολογική σκέψη του Γενικού Κανονισμού Προστασίας Δεδομένων[18], δεν

---

[17] Βλ. αρθ. 9§1 ΓΚΠΔ «*Απαγορεύεται η επεξεργασία 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 η επεξεργασία 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*»., καθώς και άρθ. 10§1 Οδηγίας (ΕΕ) 2018/680, άρθ. 10 §1 Κανονισμού (ΕΕ) 2018/1725. Μόνο αν συντρέχει κάποια από τις ρητές προβλεφθείσες εξαιρέσεις του άρθρου 9§2 του ΓΚΠΔ, οι οποίες θα αναλυθούν διεξοδικώς εν συνεχεία, είναι δυνατή η επεξεργασία τους.

[18] Αιτιολογική Σκέψη υπ' αριθ. 51 ΓΚΠΔ: «*Δεδομένα προσωπικού χαρακτήρα τα οποία είναι εκ φύσεως ιδιαίτερα ευαίσθητα σε σχέση με θεμελιώδη δικαιώματα και ελευθερίες χρήζουν ειδικής προστασίας, καθότι το πλαίσιο της επεξεργασίας τους θα μπορούσε να δημιουργήσει σημαντικούς κινδύνους για τα θεμελιώδη δικαιώματα και τις ελευθερίες. Τα εν λόγω δεδομένα προσωπικού χαρακτήρα θα πρέπει να περιλαμβάνουν δεδομένα προσωπικού χαρακτήρα που αποκαλύπτουν φυλετική ή εθνοτική καταγωγή, όπου η χρήση του όρου «φυλετική καταγωγή» στον παρόντα κανονισμό δεν συνεπάγεται ότι η Ένωση αποδέχεται θεωρίες που υποστηρίζουν την ύπαρξη χωριστών ανθρώπινων φυλών. Η επεξεργασία φωτογραφιών δεν θα πρέπει συστηματικά να θεωρείται ότι είναι επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα, καθώς αυτές καλύπτονται από τον ορισμό των βιομετρικών δεδομένων μόνο σε περίπτωση επεξεργασίας μέσω ειδικών τεχνικών μέσων*

αποτελεί *κάθε φωτογραφία* βιομετρικό δεδομένο· ο Κανονισμός κατέστησε σαφές ότι οι εικόνες προσώπου υπάγονται στην έννοια των βιομετρικών δεδομένων, και ως εκ τούτου των ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα, *μόνον σε περίπτωση επεξεργασίας τους μέσω ειδικών τεχνικών μέσων που επιτρέπουν την αδιαμφισβήτητη ταυτοποίηση ή επαλήθευση της ταυτότητας ενός φυσικού προσώπου.*

Όπως ευλόγως συνάγεται εκ των ανωτέρω, οι ψηφιακές εικόνες προσώπου συγκαταλέγονται στην κατηγορία των φυσικών χαρακτηριστικών του ατόμου και, επομένως, η ανάλυση τους μέσω των συστημάτων αναγνώρισης προσώπου για σκοπούς αδιαμφισβήτητης ταυτοποίησης των υποκειμένων τους, συνιστά βιομετρική τεχνική, η οποία μάλιστα παρουσιάζει πολλά πλεονεκτήματα σε σχέση με τις λοιπές βιομετρικές μεθόδους, καθώς η ταυτοποίηση συντελείται εξ αποστάσεως, ταχύτερα και δεν απαιτεί τη σύμπραξη του ατόμου, σε αντίθεση λ.χ. με τη λήψη δακτυλικών αποτυπωμάτων[19].

Καθώς, όμως, γίνεται ευκόλως αντιληπτό ότι η συλλογή και χρήση βιομετρικών δεδομένων για την εξ αποστάσεως ταυτοποίηση των υποκειμένων τους, πολλώ δε μάλλον όταν αυτή συντελείται με χρήση τεχνικών αναγνώρισης προσώπου, συνεπάγεται ειδικούς κινδύνους, το ενδεχόμενο των οποίων κρίνεται αφ' εαυτόν κρίσιμο, **η Ευρωπαϊκή Επιτροπή στη «*Λευκή Βίβλο για την Τεχνητή Νοημοσύνη*», μνημόνευσε ιδιαιτέρως τα συστήματα αναγνώρισης προσώπου, εντάσσοντας τα πάντοτε και ανεξαρτήτως περιστάσεων στις εφαρμογές ΤΝ «*υψηλού κινδύνου*[20]» όταν αποσκοπούν σε βιομετρική ταυτοποίηση**, διασαφηνίζοντας παραλλήλως τον σημασιολογικό πυρήνα των εννοιών της *ταυτοποίησης* και *επαλήθευσης*, ως εξής:

«*Σε ό,τι αφορά την αναγνώριση προσώπου, η ταυτοποίηση σημαίνει ότι το υπόδειγμα της εικόνας του προσώπου συγκρίνεται με πολλά άλλα υποδείγματα που βρίσκονται αποθηκευμένα σε βάση δεδομένων για να διαπιστωθεί εάν η εικόνα του προσώπου είναι αποθηκευμένη εκεί. Η επαλήθευση ταυτότητας (ή η επιβεβαίωση ταυτότητας), από την άλλη πλευρά, αναφέρεται συχνά ως «μονοσήμαντη αντιστοίχιση». Επιτρέπει τη σύγκριση δύο βιομετρικών υποδειγμάτων, που θεωρείται συνήθως ότι ανήκουν στο ίδιο άτομο. Συγκρίνονται δύο βιομετρικά υποδείγματα για να προσδιοριστεί εάν το πρόσωπο που απεικονίζεται στις δύο εικόνες είναι το ίδιο πρόσωπο. Η διαδικασία αυτή χρησιμοποιείται, για παράδειγμα,*

που επιτρέπουν την αδιαμφισβήτητη ταυτοποίηση ή επαλήθευση της ταυτότητας ενός φυσικού προσώπου […]».

[19] Κανέλλος, Λ. (2020) ο.π. σελ 337.

[20] Ευρωπαϊκή Επιτροπή (2020) *COM(2020) 65 final- Λευκή Βίβλος για την Τεχνητή Νοημοσύνη. Η ευρωπαϊκή προσέγγιση της αριστείας και της εμπιστοσύνης*, σελ. 21-22.

στις πύλες αυτοματοποιημένου συνοριακού ελέγχου (ABC) που χρησιμοποιούνται για τους συνοριακούς ελέγχους στους αερολιμένες[21]».

Υπερθεματίζοντας επί του δοθέντος ορισμού των ανωτέρω βασικών για την υπό κρίση τεχνολογία εννοιών, αμέσως παρακάτω θα αποσαφηνιστεί ενδελεχώς και στο σύνολό του το εννοιολογικό πλαίσιο των λεγόμενων «συστημάτων αναγνώρισης προσώπου».

1.2 Η τεχνολογία αναγνώρισης προσώπου

Οι τεχνολογίες αναγνώρισης προσώπου (Facial Recognition Technologies-FRTs) αποτελούν, όπως ήδη κατέστη σαφές, ειδικότερη κατηγορία των βιομετρικών τεχνολογιών που επιτρέπουν την αυτόματη αναγνώριση και ταυτοποίηση ενός ατόμου επί τη βάση της γεωμετρίας του προσώπου του. Ειδικότερα, η εν λόγω διαδικασία επιτυγχάνεται μέσω της εξαγωγής εκ των καταγεγραμμένων από την εικόνα δεδομένων, των ειδικών εκείνων χαρακτηριστικών του προσώπου του υποκειμένου που είναι απαραίτητα για τη δημιουργία ενός «βιομετρικού προτύπου», ήτοι μιας δομημένης απεικόνισης της βιομετρικής μέτρησής του[22]. Τα χαρακτηριστικά που αναζητά ένα σύστημα αναγνώρισης προσώπου είναι συνήθως αυτά που αλλοιώνονται κατά το δυνατόν λιγότερο με το πέρασμα του χρόνου, όπως η απόσταση ανάμεσα στα μάτια, στο στόμα και τη μύτη, το μήκος του μετώπου, το μέγεθος του χείλους, ο σχηματισμός των ζυγωματικών και της γνάθου κ.α.

Τα συστήματα αναγνώρισης προσώπου εμπερικλείουν ένα πλήθος τεχνολογιών, οι οποίες δύναται να χρησιμοποιηθούν για διαφορετικούς σκοπούς που κυμαίνονται από την απλή ανίχνευση της παρουσίας ενός προσώπου σε μια εικόνα, έως την εκτέλεση σύνθετων ενεργειών, όπως η ταυτοποίηση. Μάλιστα, μια πρώτη βασική διαφοροποίηση ανάμεσα στις εν θέματι τεχνολογίες εντοπίζεται ακριβώς στην εξέταση του επιδιωκόμενου σκοπού του εκάστοτε συστήματος αναγνώρισης προσώπου, συγκεκριμένα δε αν αυτό χρησιμοποιείται για την επαλήθευση, την ταυτοποίηση ή την κατηγοριοποίηση ενός ανθρώπινου προσώπου.

1.2.1 Η επαλήθευση («μονοσήμαντη αντιστοίχιση»)

Η **επαλήθευση ή πιστοποίηση ταυτότητας** επιτρέπει τη σύγκριση δύο βιομετρικών προτύπων, τα οποία συνήθως πιθανολογείται ότι ανήκουν στο ίδιο

---

[21] ο.π. *Λευκή Βίβλος για την Τεχνητή Νοημοσύνη*, υποσημείωση 56.

[22] Το σύστημα δεν αποθηκεύει την αρχική εικόνα του ατόμου, αλλά το βιομετρικό πρότυπο σε ψηφιακή μορφή. Βλ. https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/eidikeskatigories/biometrikadedomena/epexergasia_biometrikwn_dedomenwn_biometrika

άτομο[23], προκειμένου να διαπιστωθεί αν πρόκειται πράγματι για το ίδιο φυσικό πρόσωπο. Η εν λόγω τεχνολογία, όπως προαναφέρθηκε, χρησιμοποιείται ευρέως σε αεροδρόμια στα οποία είναι εγκατεστημένα «αυτοματοποιημένα συστήματα συνοριακού ελέγχου», ούτως ώστε να επαληθεύεται η ταυτότητα των διερχόμενων ατόμων βάσει της σάρωσης της φωτογραφίας διαβατηρίου τους: αν το σύστημα αναγνώρισης προσώπου, κατόπιν σύγκρισης της φωτογραφίας διαβατηρίου και της ληφθείσας επί τόπου εικόνας, διαγνώσει ότι η πιθανότητα να εμφαίνεται σε αυτές το ίδιο πρόσωπο υπερβαίνει ένα προκαθορισμένο όριο, η ταυτότητα του υποκειμένου επαληθεύεται.

1.2.2 Η ταυτοποίηση (αντιστοίχιση ενός προς πολλά)

Ως **ταυτοποίηση** νοείται η σύγκριση του προτύπου εκ της εικόνας ενός ατόμου με πολλά άλλα πρότυπα, τα οποία βρίσκονται αποθηκευμένα σε μια βάση δεδομένων, με σκοπό να διαπιστωθεί αν η εικόνα του βρίσκεται αποθηκευμένη στο εν λόγω σύνολο δεδομένων. Στην προκειμένη περίπτωση, η τεχνολογία αναγνώρισης προσώπου εμφανίζει, κατόπιν της σύγκρισης, μια βαθμολογία που υποδεικνύει την πιθανότητα οι διαφορετικές εικόνες να ανήκουν στο ίδιο φυσικό πρόσωπο. Άλλες φορές οι εικόνες συγκρίνονται με βάσεις δεδομένων στις οποίες είναι γνωστό ότι συμπεριλαμβάνεται το υπό κρίση άτομο («αναγνώριση κλειστού συνόλου»), ενώ άλλες φορές η σύγκριση διενεργείται δίχως προηγούμενη γνώση αυτού του δεδομένου («αναγνώριση ανοιχτού συνόλου»), όπως συμβαίνει, επί παραδείγματι, όταν το πρόσωπο ενός ατόμου αντιπαραβάλλεται με λίστες παρακολούθησης υπόπτων.

Η εν λόγω τεχνολογία αναφέρεται συχνά και ως ***αυτοματοποιημένη αναγνώριση προσώπου*** (Automated Facial Recognition- AFR). Χαρακτηριστικό γνώρισμά αυτής είναι ότι μπορεί να χρησιμοποιηθεί επί τη βάση εικόνων προσώπων που έχουν συλλεχθεί από βιντεοκάμερες (CCTV- Closed Circuit TV). Στην περίπτωση αυτή, το σύστημα αρχικώς ανιχνεύει αν απεικονίζεται ανθρώπινο πρόσωπο στο υπό εξέταση βίντεο και σε περίπτωση καταφατικής διάγνωσης, τα χαρακτηριστικά των απεικονισθέντων προσώπων εξάγονται και εν συνεχεία το εξ αυτών βιομετρικό υπόδειγμα συγκρίνεται με τα διαθέσιμα στις βάσεις δεδομένων βιομετρικά πρότυπα.

Ωστόσο, τα συγκεκριμένα συστήματα, γνωστά και ως ***τεχνολογία αναγνώρισης προσώπου σε ζωντανή μετάδοση*** (Live Facial Recognition Technology), παρουσιάζουν ορισμένες **αδυναμίες**, οι οποίες έγκεινται κυρίως στη δυσχέρεια επέμβασης στην ποιότητα των καταγεγραμμένων στο βίντεο εικόνων:

---

[23] Madiega, T., Mildebrath, H. (2021) *Regulating facial recognition in the EU. In-depth analysis, European Parliamentary Research Service*. σελ. 1-2. doi:10.2861/140928.

το φως, η απόσταση, η θέση του ατόμου περιορίζουν καταλυτικά την αποτύπωση των χαρακτηριστικών του προσώπου του, με αποτέλεσμα να καθίστανται πιθανές λανθασμένες ταυτοποιήσεις, οι οποίες, εξ αντιδιαστολής σε ελεγχόμενα περιβάλλοντα (όπως ένα σημείο διέλευσης συνόρων), είναι σαφώς πιο περιορισμένες[24].

1.2.3 Η κατηγοριοποίηση (αντιστοίχιση γενικών χαρακτηριστικών)

Τα συστήματα αναγνώρισης προσώπου χρησιμοποιούνται, επιπροσθέτως, για την εξαγωγή πληροφοριών και τη συνακόλουθη εκτέλεση μιας κατηγοριοποίησης (ή ταξινόμησης) ατόμων, με βάση τα προσωπικά τους χαρακτηριστικά, όπως η ηλικία, το φύλο και η εθνική καταγωγή. Ήδη ο εννοιολογικός προσδιορισμός της εν λόγω μεθόδου, καθιστά σαφές ότι η εν λόγω τεχνολογία, σε περίπτωση που ερείδεται σε συστήματα τεχνητής νοημοσύνης, δύναται να χρησιμοποιηθεί για την *κατάρτιση προφίλ* των υποκειμένων, προβληματική η οποία θα εξεταστεί περαιτέρω σε επόμενο κεφάλαιο.

Δέον επισημανθεί ότι η τεχνολογία αναγνώρισης προσώπου που αποβλέπει σε κατηγοριοποίηση, δεν αναφέρεται, per se, στην ταυτοποίηση ατόμων, αλλά μπορεί να αφορά μόνον στην *ταξινόμηση* των χαρακτηριστικών τους, τα οποία δεν επιτρέπουν απαραιτήτως οποιαδήποτε εξαγωγή συμπεράσματος ως προς την ταυτότητα του υποκειμένου. Η προβληματική εντοπίζεται, λοιπόν, κυρίως στην περίπτωση που συνάγονται από το ίδιο πρόσωπο περισσότερα χαρακτηριστικά και στη συνέχεια αυτά τα χαρακτηριστικά **συνδέονται με άλλα δεδομένα** (λ.χ. δεδομένα θέσης), με αποτέλεσμα να οδηγούν de facto στην εξακρίβωση της ταυτότητάς του.

1.2.4 Συστήματα αναγνώρισης συναισθημάτων & άλλες απόπειρες αξιοποίησης της τεχνολογίας

Η τεχνολογία αναγνώρισης προσώπου παρέχει αναρίθμητες δυνατότητες και η διεθνής επιστημονική κοινότητα εξερευνά επισταμένως τη δυναμική της. Στο πλαίσιο των μεθόδων κατηγοριοποίησης, ερευνητές έχουν αποπειραθεί να εξάγουν περαιτέρω συμπεράσματα από την ανάλυση εικόνων προσώπου, όπως τον σεξουαλικό προσανατολισμό, το φύλο, ή την εθνική καταγωγή του υποκειμένου, με απώτερο στόχο να προβούν σε μια *περαιτέρω* ταξινόμηση βάσει αυτών (face attribute classification), ή μια εκτίμηση, λ.χ. της ηλικίας του (face attribute estimation). Παραλλήλως, έχει παρατηρηθεί η ανάπτυξη μιας ειδικότερης κατηγορίας τεχνολογιών αναγνώρισης προσώπου, αυτής της «αναγνώρισης

[24] European Union Agency for Fundamental Rights (2019) ο.π.

συναισθημάτων»(Facial Emotion Technology)[25], η οποία αποσκοπεί στην εξαγωγή συμπερασμάτων για τη συναισθηματική κατάσταση των υποκειμένων (δηλαδή, αν το άτομο αισθάνεται τη δεδομένη στιγμή λύπη, χαρά, φόβο) ή τη διάγνωση των εκφράσεων του προσώπου τους (αν λ.χ. χαμογελούν). Χαρακτηριστικό παράδειγμα χρήσης της εν λόγω τεχνολογίας αποτελεί το σύστημα «iBorderCtrl», το οποίο εφαρμόστηκε, μεταξύ άλλων, στα σύνορα της Ελλάδας, και ενσωμάτωσε την ως άνω τεχνολογία αναγνώρισης προσώπου συνδυαστικά με άλλες τεχνολογίες, προκειμένου να δημιουργηθεί ένας ανιχνευτής ψεύδους για τα διερχόμενα άτομα.

1.3 Η Τεχνητή Νοημοσύνης ως πολλαπλασιαστής δύναμης των Συστημάτων Αναγνώρισης Προσώπου

Η δραματική εξέλιξη της τεχνολογίας αναγνώρισης προσώπου που σημειώθηκε ιδίως την τελευταία δεκαετία, οφείλεται κατά κύριο λόγο στην ανάπτυξη των συστημάτων τεχνητής νοημοσύνης και ιδιαίτερα στην χρήση τεχνικών μηχανικής μάθησης, η οποία επέτρεψε, μεταξύ άλλων, τη δημιουργία σημαντικότερων –ποιοτικά και ποσοτικά- βάσεων δεδομένων και τη βέλτιστη αξιοποίηση αυτών στις μεθόδους αναγνώρισης προσώπου. Πλέον, **τα συστήματα αναγνώρισης προσώπου αποτελούν, κατ' ουσίαν, το σημείο τομής ανάμεσα στην Τεχνητή Νοημοσύνη και στις βιομετρικές τεχνολογίες**.

Προκειμένου να γίνει αντιληπτή η επίδραση της ΤΝ στην τεχνολογία αναγνώρισης προσώπου, σκόπιμο είναι να αποσαφηνιστεί επιγραμματικά το εννοιολογικό πλαίσιο αυτής, καθώς και τα κύρια στοιχεία της που διαδραματίζουν καθοριστικό ρόλο για τις μεθόδους εξ αποστάσεως βιομετρικής ταυτοποίησης.

1.3.1 Εννοιολογική προσέγγιση

Η «Τεχνητή Νοημοσύνη» συνιστά έναν επιστημονικό κλάδο, ο οποίος αποτελεί συγκερασμό διαφόρων επιστημών, όπως η πληροφορική, η ψυχολογία, η φιλοσοφία, η νευρολογία και η μηχανική[26]. Ως εκ τούτου, λόγω της πολυπλοκότητας που τη χαρακτηρίζει, η ΤΝ αποτελεί έννοια δυσχερώς προσδιορίσιμη, για την οποία έχουν υπάρξει πολλές διαφορετικές προσεγγίσεις, οι οποίες με ενδελεχείς προσπάθειες της επιστημονικής κοινότητας εμπλουτίζονται διαρκώς ανά τα χρόνια, ακολουθώντας την εκρηκτική εξέλιξη του κλάδου.

---

[25] Vemou, K., Zerdick, T., Horvath, A. (2021) 'Facial Emotion Recognition', *EDPS TechDispatch*, (1). doi:10.2804/014217. σελ. 1-2. Διαθέσιμο στο: https://edps.europa.eu/system/files/2021-05/21-05-26_techdispatch-facial-emotion-recognition_ref_en.pdf

[26] Κανέλλος, Λ. (2021) *Εφαρμογές Τεχνητής Νοημοσύνης στο δίκαιο & στη δικαστική πρακτική*. Νομική Βιβλιοθήκη. σελ. 26-27.

Στην επιστημονική κοινότητα, οι απαρχές της έννοιας της ΤΝ εντοπίζονται για πρώτη φορά την δεκαετία του 1950, όταν ο μαθηματικός Alan Turing, με το άρθρο του "Computing Machinery and Intelligence" και το περίφημο «Turing Test[27]», επιχείρησε να εξακριβώσει εάν μία μηχανή διαθέτει ευφυΐα, θέτοντας ένα θεμελιώδες ερώτημα· *μπορούν οι μηχανές να σκεφτούν;* Λίγα χρόνια αργότερα, ο John McCarthy έπλασε τον όρο «Τεχνητή Νοημοσύνη» ως την «*επιστήμη και μεθοδολογία της δημιουργίας νοούντων μηχανών*».

Έκτοτε διατυπώθηκαν ποικίλοι ορισμοί, ανάλογα με την προσέγγιση των εκάστοτε ερευνητών και τον στόχο τον οποίο αποδίδουν στην ΤΝ, οι οποίοι δύναται να ενταχθούν, κατ' αρχήν, σε τέσσερις κατηγορίες[28]:

- Η πρώτη κατηγορία, αντιμετωπίζει την ΤΝ ως ένα σύστημα που επιδεικνύει ίδια σκέψη με τον άνθρωπο.
- Η δεύτερη κατηγορία, αντιμετωπίζει την ΤΝ ως ένα σύστημα που επιδεικνύει ορθολογική σκέψη.
- Η τρίτη κατηγορία, αντιμετωπίζει την ΤΝ ως ένα σύστημα που επιδεικνύει ίδια συμπεριφορά με την ανθρώπινη.
- Η τέταρτη κατηγορία, προσεγγίζει την ΤΝ ως ένα σύστημα που ενεργεί ορθολογικά.

Στην πλειονότητά τους οι ορισμοί που έχουν δοθεί κατά καιρούς συγκλίνουν στην προσέγγιση που εξέφρασαν οι Barr και Feigenbaum[29], ήτοι ότι «*η Τεχνητή Νοημοσύνη αποτελεί τομέα της επιστήμης των υπολογιστών, που αποσκοπεί στη σχεδίαση και υλοποίηση προγραμμάτων, τα οποία είναι ικανά να μιμηθούν τις ανθρώπινες γνωστικές ικανότητες, εμφανίζοντας έτσι χαρακτηριστικά που αποδίδουμε συνήθως σε ανθρώπινη συμπεριφορά, όπως η επίλυση προβλημάτων, η αντίληψη μέσω της όρασης, η μάθηση, η εξαγωγή συμπερασμάτων, η κατανόηση φυσικής γλώσσας κτλ.*».

Σε θεσμικό επίπεδο, η Τεχνητή Νοημοσύνη προσδιορίστηκε για πρώτη φορά το 2018 από την Ευρωπαϊκή Επιτροπή ως αναφερόμενη «*σε συστήματα που χαρακτηρίζονται από ευφυή συμπεριφορά, αναλύοντας το περιβάλλον τους και*

---

[27] Με την εν λόγω δοκιμασία, την οποία ο Α. Τούρινγκ κατονόμασε «παιχνίδι της μίμησης» ελέγχεται αν μία μηχανή μπορεί να επιδείξει ευφυή συμπεριφορά, ισοδύναμη ή διακριτή από την ανθρώπινη: ένας εξεταστής θέτει μέσω δύο τερματικών υπολογιστή, τις ίδιες ερωτήσεις προς έναν άνθρωπο και έναν υπολογιστή. Αν ο εξεταστής αδυνατεί να διακρίνει ποια απάντηση προήλθε από τη μηχανή, θεωρείται ότι αυτή διαθέτει ευφυία. Βλ. Touring, A.M. (1950) 'Computing Machinery and Intelligence', *Mind*, LIX(236), σελ. 433–460. doi:10.1093/MIND/LIX.236.433.

[28] Russell, S., & Norvig, P. (2002). *Artificial intelligence: a modern approach*.

[29] Βόρρας, Α., Μήτρου, Λ. (2018) 'Τεχνητή νοημοσύνη και προσωπικά δεδομένα - Μια θεώρηση υπό το πρίσμα του Ευρωπαϊκού Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 2016/679', *ΔΙΤΕ (π. ΔΙΜΕΕ)*,(4/2018).

ενεργώντας —με κάποιο βαθμό αυτονομίας— για την επίτευξη συγκεκριμένων στόχων. Τα συστήματα που λειτουργούν βάσει ΤΝ μπορούν 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 ΤΝ μπορεί να ενσωματώνεται σε συσκευές υλισμικού (π.χ. προηγμένα ρομπότ, αυτόνομα αυτοκίνητα, δρόνοι ή εφαρμογές του Διαδικτύου των Πραγμάτων)[30]». Ο εν λόγω ορισμός βελτιώθηκε περαιτέρω από την Ανεξάρτητη Ομάδα Εμπειρογνωμόνων υψηλού επιπέδου που συστάθηκε από την Επιτροπή τον Ιούνιο του 2018, και τα συστήματα της ΤΝ προσδιορίστηκαν ως «*συστήματα λογισμικού (ή ενδεχομένως και υλισμικού) που σχεδιάζονται από ανθρώπους και, βάσει ενός δεδομένου σύνθετου στόχου, ενεργούν στην υλική ή ψηφιακή διάσταση με το να αντιλαμβάνονται το περιβάλλον τους μέσω της απόκτησης δεδομένων, να ερμηνεύουν τα δομημένα ή αδόμητα δεδομένα που έχουν συλλεχθεί, να προβαίνουν σε συλλογισμούς με βάση τις γνώσεις ή να επεξεργάζονται τις πληροφορίες που εξάγονται από αυτά τα δεδομένα, και να αποφασίζουν ποια είναι η βέλτιστη ενέργεια (ή οι βέλτιστες ενέργειες) που θα πρέπει να εκτελέσουν για να επιτύχουν τον δεδομένο στόχο. Τα συστήματα ΤΝ μπορεί είτε να χρησιμοποιούν συμβολικούς κανόνες είτε να μαθαίνουν ένα αριθμητικό μοντέλο, και μπορεί επίσης να προσαρμόζουν τη συμπεριφορά τους με το να αναλύουν πώς επηρεάζεται το περιβάλλον από τις προηγούμενες ενέργειές τους*».

Πρόσφατα, στη Λευκή Βίβλο της Ευρωπαϊκής Επιτροπής για την Τεχνητή Νοημοσύνη[31], δόθηκε ακόμη ένας ορισμός στα συστήματα ΤΝ, σύμφωνα με τον οποίο η έννοια αυτών «*θα πρέπει να βασίζεται στα βασικά λειτουργικά χαρακτηριστικά του λογισμικού, ειδικότερα στην ικανότητα ενός δεδομένου συνόλου στόχων καθορισμένων από τον άνθρωπο, να παράγει στοιχεία εξόδου όπως περιεχόμενο, προβλέψεις, συστάσεις ή αποφάσεις που επηρεάζουν το περιβάλλον με το οποίο αλληλεπιδρά το σύστημα, είτε σε υλική είτε σε ψηφιακή διάσταση*».

1.3.2 Περιορισμένη & Γενική Τεχνητή Νοημοσύνη

Ανεξάρτητα από τον εκάστοτε υιοθετούμενο ορισμό, η Τεχνητή Νοημοσύνη διακρίνεται, κατ' αρχήν, σε δύο γενικά παραδεδεγμένες κατηγορίες, οι οποίες αναφέρονται κατά κύριο λόγο στην εξάρτηση της εφαρμογής της από τη

[30] COM(2018) 237 final, σ. 1.

[31] Ευρωπαϊκή Επιτροπή (2020) *COM(2020) 65 final- Λευκή Βίβλος για την Τεχνητή Νοημοσύνη. Η ευρωπαϊκή προσέγγιση της αριστείας και της εμπιστοσύνης*. στοιχ. 6.

συμμετοχή του ανθρώπινου παράγοντα[32]: στην περιορισμένη ή αδύναμη ΤΝ και στην γενική ή ισχυρή ΤΝ.

Η περιορισμένη/ αδύναμη ΤΝ αναφέρεται σε συστήματα τεχνητής νοημοσύνης τα οποία είναι σε θέση να χειριστούν την εκτέλεση ενός συγκεκριμένου έργου επί τη βάση και εντός του πλαισίου που θέτει ο προγραμματισμός τους από έναν άνθρωπο, δίχως να δύνανται, δηλαδή, να υπερβούν τον σχεδιασμό τους και να αναπτύξουν αυτόνομη γνώση και δράση. Άλλως, το συγκεκριμένο είδος ΤΝ αποτελεί απλή προσομοίωση της ανθρώπινης νοημοσύνης, καθώς διενεργεί εργασίες ειδικά σχεδιασμένες για αυτήν, δρώντας έτσι σε ένα πολύ περιορισμένο και προμελετημένο πλαίσιο, το οποίο δεν δύναται να υπερκεράσει. Τα συστήματα «περιορισμένης» ΤΝ είναι ευρέως διαδεδομένα και **συμπεριλαμβάνουν την τεχνολογία αναγνώρισης προσώπου.**

Στον αντίποδα της «αδύναμης» ΤΝ, στέκει η λεγόμενη «γενική ή ισχυρή», η οποία αναφέρεται σε μηχανές που παρουσιάζουν στοιχεία ανθρώπινης νοημοσύνης. Ένα σύστημα ισχυρής ΤΝ διαθέτει τις γνωστικές ικανότητες και την απαιτούμενη αντίληψη ώστε να καθίσταται ικανό να πραγματώνει αφ' εαυτού οποιαδήποτε εργασία μπορεί να αντιμετωπίσει ο ανθρώπινος νους, σε πολύ μεγαλύτερη εμβέλεια και με πολύ μεγαλύτερες ταχύτητες. Ως εκ τούτου, παρότι σε αυτό το χρονικό σημείο η ισχυρή ΤΝ παραμένει θεωρητικό κατασκεύασμα, η παγκόσμια επιστημονική κοινότητα επισημαίνει συχνά τις πιθανές κρίσιμες επιπτώσεις της εκθετικής εξέλιξης του εν λόγω είδους ΤΝ στον ανθρώπινο πολιτισμό, όπως αυτός γίνεται αντιληπτός σήμερα.

1.3.3 Η μηχανική μάθηση (Machine Learning)

Η «μηχανική μάθηση» αποτελεί μία πολύ δημοφιλή επιμέρους τεχνική του επιστημονικού πεδίου της Τεχνητής Νοημοσύνης, η οποία προσδιορίζεται, κατ' αρχήν, ως η δυνατότητα ενός υπολογιστικού συστήματος να δημιουργεί μοντέλα ή πρότυπα όταν λαμβάνει ως είσοδο ένα σύνολο δεδομένων.

Η μηχανική μάθηση στοχεύει στην αυτοματοποίηση του έργου της δημιουργίας αναλυτικών μοντέλων για την εκτέλεση γνωστικών εργασιών, όπως η ανίχνευση ενός ανθρώπινου προσώπου. Τούτο επιτυγχάνεται με τη χρήση αλγορίθμων που «εκπαιδεύονται» από ογκώδη σύνολα δεδομένων και κατ' αυτόν τον τρόπο καθιστούν ικανούς τους υπολογιστές να ανιχνεύουν πληροφορίες και σύνθετα μοτίβα χωρίς να είναι ρητώς προγραμματισμένοι ως προς αυτό[33].

---

[32] Τάσσης, Σπ. (2018). *Η Εποχή της Τεχνητής Νοημοσύνης*, ΔΙΤΕ (πρώην ΔιΜΕΕ) 4/2018, σ. 484-494.

[33] Janiesch, C., Zschech, P. και Heinrich, K. (2021) 'Machine learning and deep learning', *Electronic Markets*, 31(3), σσ 686.. doi:10.1007/s12525-021-00475-2.

Ανάλογα με το είδος του υπό κρίση προβλήματος και των διαθέσιμων δεδομένων, η μηχανική μάθηση μπορεί να διακριθεί σε περισσότερες τεχνικές, μερικές από τις οποίες είναι: α) η μάθηση με επίβλεψη, στην οποία το σύστημα καλείται να εκπαιδευτεί από ένα σύνολο δεδομένων, β) η μάθηση χωρίς επίβλεψη, στην οποία το σύστημα καλείται να ανακαλύψει μόνο του συσχετίσεις ή ομάδες σε ένα σύνολο δεδομένων, δημιουργώντας πρότυπα και γ) η μάθηση με ενίσχυση, όπου το σύστημα μάθησης προσπαθεί να εκπαιδευτεί μέσα από την άμεση αλληλεπίδραση με το περιβάλλον[34].

Η αποτελεσματικότητα ενός συστήματος μηχανικής μάθησης εξαρτάται άρρηκτα από την ποσότητα, την ποιότητα και την ποικιλομορφία των συνόλων δεδομένων με τα οποία έχει εφοδιαστεί. Καθώς όμως η εφαρμογή των τεχνικών της μηχανικής μάθησης είναι πρόσφορη να παράγει αξιόπιστα αποτελέσματα, οι αλγόριθμοι μηχανικής μάθησης έχουν εφαρμοστεί με επιτυχία σε πολλούς τομείς, μεταξύ των οποίων τα συστήματα αναγνώρισης προσώπου, στα οποία η ένταξή τους υπήρξε νευραλγικής σημασίας. Χαρακτηριστικό παράδειγμα αποτελεί ο αλγόριθμος ανίχνευσης αντικειμένων **Viola-Jones**, ένας αλγόριθμος βαθιάς μάθησης με επίβλεψη ο οποίος κατέστησε εφικτή, ήδη το 2001, την ανίχνευση προσώπου σε πραγματικό χρόνο[35].

1.3.4 Η βαθιά μάθηση (Deep Learning)

Η «βαθιά μάθηση» συνιστά υποσύνολο της μηχανικής μάθησης και περιγράφει αλγορίθμους που αναλύουν δεδομένα μέσω μίας διεργασίας που προσομοιάζει στην ανθρώπινη ορθολογική σκέψη[36]. Προκειμένου να επιτευχθεί αυτό το αποτέλεσμα, οι εφαρμογές βαθιάς μάθησης χρησιμοποιούν μια πολυεπίπεδη δομή αλγορίθμων που ονομάζονται **τεχνητά νευρωνικά δίκτυα**, τα οποία είναι εμπνευσμένα από το βιολογικό νευρωνικό δίκτυο του ανθρώπινου εγκεφάλου. Η διαδικασία της βαθιάς μάθησης έχει αποδειχθεί πολύ πιο ικανή από εκείνη των τυπικών μοντέλων μηχανικής μάθησης, καθώς μπορεί να εξάγει χαρακτηριστικά από ανεπεξέργαστα δεδομένα μέσω πολλαπλών επιπέδων μη γραμμικών μονάδων επεξεργασίας προκειμένου να διενεργεί προβλέψεις ή να προβαίνει σε ενέργειες βάσει του εκάστοτε στόχου.

Η ένταξη της εν λόγω μεθόδου στα συστήματα αναγνώρισης προσώπου, με πρωτοστάτη την εταιρεία Facebook και το σύστημα DeepFace το έτος 2014,

---

[34] Βλαχάβας, Ι. κ.ά. (2011) *Τεχνητή Νοημοσύνη - Γ΄ Έκδοση*. Εκδόσεις Πανεπιστημίου Μακεδονίας.

[35] Βλ. Ragazzi, F. κ.ά. (2021) *Biometric and Behavioural Mass Surveillance in EU Member States: Report for the Greens/EFA in the European Parliament.* σελ. 30.

[36] Wolfewicz, A. (2022) *Deep learning vs. machine learning - What's the Difference?*, *Levity*. Διαθέσιμο στο: https://levity.ai/blog/difference-machine-learning-deep-learning

έφερε επανάσταση στα έως τότε δεδομένα, εφοδιάζοντας την τεχνολογία με άνευ προηγουμένου δυνατότητες.

1.3.5 Η μηχανική όραση (Computer Vision)

Η μηχανική ή υπολογιστική ή τεχνητή όραση, αποτελεί τομέα της τεχνητής νοημοσύνης και αφορά σε αλγόριθμους οι οποίοι λαμβάνουν οπτικά δεδομένα από ψηφιακές εικόνες ή βίντεο και στη συνέχεια παράγουν συμβολικές περιγραφές των εν λόγω οπτικών σκηνών. Η μηχανική όραση αποσκοπεί στην τεχνητή μίμηση της ανθρώπινης όρασης, επιτρέποντας στους υπολογιστές να αντιλαμβάνονται, να ερμηνεύουν, να αναλύουν και να ταξινομούν τα οπτικά ερεθίσματα που εισάγονται σε αυτούς από κάμερες ή αισθητήρες. Σε συνδυασμό με μοντέλα βαθιάς μάθησης τα οποία εκπαιδεύονται με ογκώδεις και ποικιλόμορφες βάσεις δεδομένων, η εν λόγω τεχνολογία επιτυγχάνει ακρίβεια και επιδόσεις εφάμιλλες ανθρώπινου επίπεδου κατά την εκτέλεση εργασιών, όπως η αναγνώριση προσώπου και η ταξινόμηση εικόνων[37].

1.3.6 Ο ρόλος των συστημάτων Τεχνητής Νοημοσύνης στην εξέλιξη της τεχνολογίας αναγνώρισης προσώπου

Τα συστήματα Τεχνητής Νοημοσύνης, ιδιαίτερα δε η βαθιά μάθηση, η οποία αποτελεί πλέον την κυρίαρχη προσέγγιση στην ανίχνευση και ανάλυση προσώπων, **έδωσαν νέα πνοή στα παραδοσιακά συστήματα αναγνώρισης προσώπου**. Αλγόριθμοι εκπαιδεύονται πλέον συστηματικά επί τη βάση τεράστιων και ποικιλόμορφων συνόλων δεδομένων, με **στόχο την όλο και πιο τελεσφόρο εξαγωγή και ανάλυση χαρακτηριστικών προσώπου, αναβαθμίζοντας κατ' αυτόν τον τρόπο την απόδοση και την αποτελεσματικότητά της τεχνολογίας αναγνώρισης προσώπου, και επιτρέποντας την ταχύτερη και ακριβέστερη αναγνώριση ακόμα και στα λεγόμενα «μη ελεγχόμενα» περιβάλλοντα**. Τούτο είχε ως αποτέλεσμα, πολύ σύντομα, η νεοαποκτηθείσα δυναμική που προσέφερε η Τεχνητή Νοημοσύνη στα συστήματα αναγνώρισης προσώπου, να ευνοήσει τη μετάβαση της τεχνολογίας στη δημόσια σφαίρα.

Παραλλήλως –και ευλόγως- η ενσωμάτωση των εφαρμογών τεχνητής νοημοσύνης στο ήδη αμφιλεγόμενο πεδίο της τεχνολογίας αναγνώρισης προσώπου, λειτούργησε ως μεγεθυντικός φακός της εγγενώς παρεμβατικής φύσης της τελευταίας. Σύντομα, η στροφή προς το δημόσιο χώρο και η συνακόλουθη εφαρμογή της τεχνολογίας αναγνώρισης προσώπου σε πραγματικές συνθήκες, σε συνδυασμό με το γεγονός της εξόρυξης εξαιρετικά

---

[37] Boesch, G. (2022) *What is Computer Vision? The Complete Tech Guide for 2022*, *Viso*. Διαθέσιμο στο: https://viso.ai/computer-vision/what-is-computer-vision/

ευαίσθητων προσωπικών δεδομένων, είχαν ως αποτέλεσμα η τεχνολογία αναγνώρισης προσώπου να χαρακτηριστεί από πολλούς ερευνητές ως το «***πλουτώνιο της τεχνητής νοημοσύνης***[38]» καθώς και ως τεχνολογία εκ φύσεως τοξική για το κοινωνικό σύνολο.

Δεν προκαλεί, συνεπώς, ουδεμία έκπληξη η, κατά τα οριζόμενα στην προαναφερθείσα Λευκή Βίβλο της Ευρωπαϊκής Επιτροπής, ένταξη της τεχνολογίας αναγνώρισης προσώπου στις λεγόμενες **«*υψηλού κινδύνου*» εφαρμογές της τεχνητής νοημοσύνης όταν η χρήση της αποσκοπεί στη βιομετρική ταυτοποίηση**, και η συνακόλουθη επιταγή να ισχύουν πάντοτε **ειδικότερες απαιτήσεις**, ώστε να εξασφαλίζεται ότι κάθε ρυθμιστική παρέμβαση θα είναι εστιασμένη και stricto sensu αναλογική[39].

Στα αμέσως επόμενα κεφάλαια της παρούσας μελέτης θα αναλυθούν εκτενέστερα το διακύβευμα της χρήσεως συστημάτων αναγνώρισης προσώπου για τα θεμελιώδη ανθρώπινα δικαιώματα, ιδιαίτερα σε ό,τι αφορά στο δικαίωμα προστασίας δεδομένων προσωπικού χαρακτήρα, καθώς και το ισχύον ενωσιακό νομοθετικό πλαίσιο και οι ρυθμιστικές προτάσεις της Ευρωπαϊκής Ένωσης.

1.4 Η βιομηχανία τεχνολογιών αναγνώρισης προσώπου: χρήσεις & έκταση εφαρμογής

1.4.1 Οι χρήσεις της τεχνολογίας αναγνώρισης προσώπου

Τα συστήματα αναγνώρισης προσώπου έχουν εμφιλοχωρήσει τόσο στο δημόσιο όσο και στον ιδιωτικό τομέα κι έχουν αναδειχθεί σε ένα ταχέως επεκτεινόμενο και ιδιαίτερα κερδοφόρο πεδίο στην παγκόσμια αγορά· η βιομηχανία αναγνώρισης προσώπου, μόνον το 2020, απέφερε **έσοδα ύψους 3,8 δισεκατομμυρίων δολαρίων**, ποσό το οποίο αναμένεται να υπερδιπλασιαστεί έως το 2025[40], ενώ μελέτη του Πανεπιστημίου του Στάνφορντ διαπίστωσε ότι η αναγνώριση προσώπου έλαβε **το τρίτο μεγαλύτερο μερίδιο των παγκόσμιων επενδύσεων που αφιερώθηκαν στην Τεχνητή Νοημοσύνη** το 2019, με σχεδόν 4,7 δις δολάρια.

Οι σημερινές χρήσεις της τεχνολογίας είναι ποικίλες και περιλαμβάνουν:

---

[38] Marks, P. (2021) 'Can the biases in facial recognition be fixed; Also, should they?', *Communications of the ACM*, 64(3), σελ. 20. doi:10.1145/3446877.
[39] ο.π. Λευκή Βίβλος για την Τεχνητή Νοημοσύνη σελ. 26-27.
[40] Bischoff, P. (2021) *Facial recognition technology (FRT): 100 countries analyzed - Comparitech*. Διαθέσιμο στο: https://www.comparitech.com/blog/vpn-privacy/facial-recognition-statistics/

- Εφαρμογές καταναλωτών:

Συσκευές αναπόσπαστες με την καθημερινότητα, όπως τα smartphones, οι υπολογιστές και τα «έξυπνα» κουδούνια, περιλαμβάνουν πλέον όλο και πιο εκτεταμένα τεχνολογίες αναγνώρισης προσώπου, προκειμένου να ταυτοποιούν τον εκάστοτε χρήστη και, κατόπιν επαλήθευσης, να παρέχουν σε αυτόν πρόσβαση στη χρήση των συσκευών ή/ και ψηφιακών υπηρεσιών. Χαρακτηριστικό παράδειγμα αποτελεί το σύστημα Face ID της Apple, το οποίο, σύμφωνα με την εταιρεία, **είναι έως και 20 φορές πιο ασφαλές από την ταυτοποίηση μέσω δακτυλικών αποτυπωμάτων**, με την πιθανότητα σφάλματος να είναι μικρότερη από μία στο εκατομμύριο ακόμα και όταν ο χρήστης φορά μάσκα[41].

Προσέτι, η τεχνολογία χρησιμοποιείται ευρέως για την πρόσβαση σε ψηφιακές υπηρεσίες ακόμα και σε εφαρμογές που είναι ιδιαίτερα δημοφιλείς (και απευθύνονται κυρίως) σε ανηλίκους, όπως το Snapchat, το οποίο βασίζεται στη μηχανική όραση, και το TikTok, το οποίο αν και στο παρελθόν είχε αρνηθεί τη χρήση της τεχνολογίας, κατόπιν ενός εξωδικαστικού συμβιβασμού ύψους 92 εκατομμυρίων δολαρίων[42], έχει συμπεριλάβει πλέον την αναγνώριση προσώπου στους όρους χρήσης του. Αξιοσημείωτο είναι, επίσης, ότι κατασκευαστές αυτοκινήτων ενσωματώνουν τις τεχνολογίες αναγνώρισης προσώπου όχι μόνον για να επιτρέπουν στους οδηγούς να έχουν πρόσβαση στα αυτοκίνητά τους, αλλά και για να παρακολουθούν αν εμφανίζουν κατά την οδήγηση σημάδια υπνηλίας ή απροσεξίας[43].

- Επιχειρηματικές εφαρμογές και εφαρμογές πληρωμών

Στον τραπεζικό τομέα, οι τεχνολογίες αναγνώρισης προσώπου αξιοποιούνται σε μεγάλη κλίμακα, προκειμένου οι συναλλαγές να πραγματοποιούνται γρηγορότερα, με μικρότερο κόστος και με τις μέγιστες δυνατές εγγυήσεις ασφάλειας. Τέτοια συστήματα χρησιμοποιούνται, λόγου χάριν, για την πιστοποίηση της ταυτότητας των πελατών όταν προβαίνουν σε συναλλαγές σε ATM, σε συναλλαγές μέσω e- banking, ή κατά την είσοδο στην τραπεζική εφαρμογή, μειώνοντας κατ' αυτόν τον τρόπο την ανάγκη για ανθρώπινη παρέμβαση, με παράλληλη όμως διενέργεια ενός αυξημένης ασφαλείας ελέγχου απάτης. Μάλιστα, λόγω της επιτυχούς εφαρμογής της τεχνολογίας στη διευκόλυνση των ηλεκτρονικών συναλλαγών, υπολογίζεται ότι ο αριθμός των μελλοντικών χρηστών της αναμένεται να ξεπεράσει τα 1,4 δις παγκοσμίως έως το 2025.

---

[41] https://support.apple.com/el-gr/HT208108

[42] 'TikTok agrees legal payout over facial recognition' (2021) *BBC News*. Διαθέσιμο στο: https://www.bbc.com/news/technology-56210052

[43] Madiega, T., Mildebrath, H. (2021), ο.π. σελ. 3.

- Διαφημιστικοί σκοποί

Η ενσωμάτωση συστημάτων πληρωμής βάσει αναγνώρισης προσώπου παρατηρείται εντόνως και από τους ιδιοκτήτες καταστημάτων, οι οποίοι χρησιμοποιούν την τεχνολογία για να προβαίνουν σε **εκτίμηση των δημογραφικών στοιχείων** των καταναλωτών τους για σκοπούς μάρκετινγκ, ακόμη και **για να εμποδίζουν την είσοδο** σε άτομα τα οποία το σύστημα χαρακτηρίζει ως «ύποπτα».

Ιδιαίτερο ενδιαφέρον, αλλά και έντονη ανησυχία, παρουσιάζουν οι λεγόμενες **«έξυπνες» διαφημιστικές πινακίδες** («smart billboards»), οι οποίες εξοπλίζονται με κάμερες και τεχνολογία αναγνώρισης προσώπου για μια σειρά από σκοπούς, όπως η εκτίμηση της απήχησης μίας διαφήμισης στο κοινό με τη μέτρηση της δέσμευσης στον διαφημιστικό χώρο (χρόνος παραμονής, μέτρηση προσοχής), η παροχή διαδραστικής εμπειρίας και η προβολή στοχευμένων διαφημίσεων στα διερχόμενα άτομα (δημογραφική ανάλυση)[44]. Μια πινακίδα με δυνατότητα αναγνώρισης προσώπου μπορεί να ανιχνεύσει έναν «αφοσιωμένο» περαστικό, να καταγράψει την εικόνα του προσώπου του και τελικά να δημιουργήσει ένα βιομετρικό πρότυπο βάσει του οποίου το σύστημα επιχειρεί μια περαιτέρω κατηγοριοποίηση, ήτοι ερειδόμενο σε χαρακτηριστικά τα οποία δύναται να περιλαμβάνουν ευαίσθητες πληροφορίες όπως η ηλικία, το φύλο, ο σεξουαλικός προσανατολισμός, η εθνικότητα κ.α. με απώτερο σκοπό την εμφάνιση στοχευμένων διαφημίσεων σε πραγματικό χρόνο.

- Βιομετρική παρακολούθηση και έλεγχος πρόσβασης σε φυσικούς χώρους

Η πλέον εκτεταμένη αλλά και πιο αμφιλεγόμενη χρήση των τεχνολογιών αναγνώρισης προσώπου, αφορά στην εργαλειοποίησή τους για σκοπούς επιβολής του νόμου, τόσο από τις αστυνομικές αρχές όσο και από ιδιωτικές εταιρείες. Στο πλαίσιο αυτό, η αναγνώριση προσώπου χρησιμοποιείται κυρίως για την πρόληψη και εξιχνίαση εγκλημάτων λ.χ. με την ανίχνευση καταζητούμενων προσώπων, για τη δημιουργία βάσεων δεδομένων με εικόνες υπόπτων (λίστες παρακολούθησης), και για τον εντοπισμό εξαφανισμένων ατόμων, ακόμα και παιδιών όταν η τεχνολογία συνεπικουρείται από αλγόριθμους προσομοίωσης γήρανσης[45]. Όπως έχει ήδη αναφερθεί, τέτοιες εφαρμογές της τεχνολογίας

---

[44] Information Commissioner's Office (2021) *The use of live facial recognition technology in public places*. Διαθέσιμο στο: https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf σελ. 17-18.

[45] Azria, S., Wickert, F. (2019) 'Facial Recognition: Current situation and challenges.', in *Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108).Council of Europe.* Διαθέσιμο σε: https://rm.coe.int/t-pd-2019-05rev-facial-recognition-report-003-/16809eadf1, σελ 11.

αναγνώρισης προσώπου απαντώνται ήδη ευρέως και για σκοπούς συνοριακού ελέγχου σε αεροδρόμια και λιμένες (επαλήθευση διαβατηρίων/ αστυνομικών ταυτοτήτων), ενώ συζητείται έντονα η μελλοντική επέκταση της εν λόγω πρακτικής για την ταυτοποίηση ταξιδιωτών και τη διεκπεραίωση αιτήσεων μετανάστευσης.

Η τάση υιοθέτησης της τεχνολογίας αναγνώρισης ταυτότητας για σκοπούς παρακολούθησης και ελέγχου πρόσβασης σε συγκεκριμένους χώρους, φαίνεται να αυξάνεται εκθετικά τόσο στο δημόσιο και όσο και στο ιδιωτικό πεδίο. Ήδη έχει παρατηρηθεί η χρήση της τεχνολογίας σε δημόσιες συγκεντρώσεις και διαμαρτυρίες (λ.χ. πορείες «Black Lives Matter» στις Η.Π.Α.),σε εκδηλώσεις ψυχαγωγίας (π.χ. αθλητικούς αγώνες), σε χώρους εργασίας ως εργαλείο αξιολόγησης υποψηφίων υπαλλήλων, αλλά και σε σχολεία για την καταγραφή της παρουσίας και την αξιολόγηση της προσοχής των μαθητών.

Επισημαίνεται ότι η αγορά της τεχνολογίας αναγνώρισης προσώπου συναπαρτίζεται κατά κύριο λόγο από ιδιωτικές εταιρείες, γνωστότερη εκ των οποίων είναι η διαβόητη Clearview AI, οι οποίες αναπτύσσουν και παρέχουν όλο και πιο ακριβή συστήματα αναγνώρισης προσώπου σε κυβερνήσεις, δημόσιες αρχές και ιδιωτικούς φορείς, προσφέροντας εξειδικευμένες υπηρεσίες για συνοριακούς ελέγχους, δημόσια ασφάλεια και επιβολή του νόμου, συμπεριλαμβανομένης της «ζωντανής» αναγνώρισης προσώπου σε πραγματικό χρόνο.

- Άλλοι σκοποί

Η τεχνολογία αναγνώρισης προσώπου τυγχάνει εφαρμογής σε πολλαπλά πεδία και για ποικίλους σκοπούς, όπως η υγειονομική περίθαλψη (π.χ. έλεγχος ασθενών, εντοπισμός σπάνιων γενετικών ασθενειών), η οργάνωση εκλογών (π.χ. ταυτοποίηση κατά την ηλεκτρονική ψηφοφορία) και η βελτιστοποίηση καθημερινών συνθηκών διαβίωσης (η τεχνολογία έχει αξιοποιηθεί λ.χ. για την παροχή δυνατότητας σε άτομα με προβλήματα όρασης να αποκτήσουν κάποιες βασικές πληροφορίες για τους ανθρώπους που συναντούν[46]). Σε αυτό το χρονικό σημείο, η τεχνολογία αναγνώρισης προσώπου δοκιμάζεται συνδυαστικά με την τεχνολογία αναγνώρισης συναισθημάτων για ένα ακόμη πιο ευρύ φάσμα εφαρμογών, όπως η αξιολόγηση των πολιτικών πεποιθήσεων των υπό κρίση ατόμων και η εξαγωγή συμπερασμάτων για τον σεξουαλικό προσανατολισμό και την ταυτότητα φύλου τους.

Οφείλει να επισημανθεί ότι η πανδημία του κορωνοϊού (Covid-19) ενίσχυσε έτι περαιτέρω το ενδιαφέρον για την ανάπτυξη και χρήση των συστημάτων

[46] Seeing AI : https://www.microsoft.com/en-us/ai/seeing-ai

αναγνώρισης προσώπου. Κυβερνήσεις στην Ευρώπη αλλά και διεθνώς, με πρωτεργάτες τη Ρωσία, την Κίνα, τη Νότιο Κορέα[47] και την Αυστραλία[48], χρησιμοποίησαν την τεχνολογία με γνώμονα την καταπολέμηση της εξάπλωσης της νόσου, λ.χ. για τον έλεγχο κυκλοφορίας σε περιόδους καραντίνας, τον εντοπισμό της μετάδοσης της μόλυνσης, την απομόνωση των κρουσμάτων, την ταυτοποίηση ατόμων που δεν φορούν μάσκες ή παραβιάζουν την καραντίνα τους κ.ο.κ.[49]

1.4.2 Η διεθνής διάσταση & η αποδοχή από το γενικό πληθυσμό

Σήμερα, κατ' ελάχιστον 109 χώρες είτε χρησιμοποιούν, είτε έχουν εγκρίνει την χρήση των συστημάτων αναγνώρισης προσώπου για σκοπούς επιτήρησης[50], ενώ υπολογίζεται ότι ποσοστό άνω του 80% των παγκόσμιων κυβερνήσεων αξιοποιούν με κάποιον τρόπο την τεχνολογία.

- Στην Ευρώπη η τεχνολογία αναγνώρισης προσώπου χρησιμοποιείται (ή έχει εγκριθεί η χρήση της) σε 32 χώρες, **συμπεριλαμβανομένης και της Ελλάδας**. Ειδικότερα, η χώρας μας ενέκρινε την προμήθεια συστημάτων αναγνώρισης προσώπου στο πλαίσιο δράσης για «Έξυπνη Αστυνόμευση», ενώ η ΕΛ.ΑΣ. συμμετέχει ήδη από τον Αύγουστο του 2018 σε ερευνητικό πρόγραμμα της Ευρωπαϊκής Ένωσης με την επωνυμία SPIRIT ("Scalable privacy preserving intelligence analysis for resolving identities"), στο πλαίσιο του οποίου δοκιμάζονται πιλοτικά λογισμικά αναγνώρισης προσώπων[51]. Επιπροσθέτως, επισημαίνεται ότι στην Ελλάδα κατά τη διάρκεια της πανδημίας, όπως προκύπτει από τις σχετικές αναρτήσεις στη «Διαύγεια», χρησιμοποιήθηκαν εκτεταμένα στο δημόσιο τομέα «*τερματικά βιομετρικής αναγνώρισης προσώπου και ανίχνευσης θερμοκρασίας*»[52].
- Πρωτοπόρος στην Ευρώπη όσον αφορά στην έγκριση της χρήσης της τεχνολογίας αναγνώρισης προσώπου από τις αρχές επιβολής του νόμου, είναι η Ουγγαρία, η οποία προέβη στην ανάπτυξη μιας εθνικής και κεντρικής βάσης δεδομένων («The Dragonfly Project») εγκαθιστώντας περί

---

[47] Roussi, A. (2020) 'Resisting the rise of facial recognition', *Nature*, 587(7834), σελ. 350–353.
[48] Guiao, J. (2021) 'Government's forced rollout of facial recognition for home quarantine needs strict limits and protections', *The Australia Institute*. Διαθέσιμο στο: https://australiainstitute.org.au/wp-content/uploads/2021/10/P1149-Facial-recognition-for-home-quarantine-needs-limits-and-protections-WEB.pdf.
[49] Pin, A. (2021). "A Novel and Controversial Technology." Artificial Face Recognition, Privacy Protection, and Algorithm Bias in Europe. *William & Mary Bill of Rights Journal*, 30(2), σελ. 293.
[50] https://surfshark.com/facial-recognition-map
[51] Homo digitalis (2019) *Προ των πυλών η χρήση τεχνολογίας αναγνώρισης προσώπου από την αστυνομία στην Ελλάδα*. Διαθέσιμο στο: https://www.homodigitalis.gr/posts/4662
[52] https://diavgeia.gov.gr/

τις 35.000 κάμερες κλειστού κυκλώματος σε κεντρικούς δημόσιους χώρους[53]. Εκτενής χρήση της τεχνολογίας έχει παρατηρηθεί επίσης από τη γερμανική αστυνομία, η οποία σχεδιάζει να εγκαταστήσει συστήματα αναγνώρισης προσώπου σε 134 σιδηροδρομικούς σταθμούς και 14 αεροδρόμια, από την Τσεχική Δημοκρατία, η οποία πολλαπλασίασε τις κάμερες που ενσωματώνουν την τεχνολογία στο Διεθνές Αεροδρόμιο της Πράγας, και μέχρι προσφάτως και από την αστυνομία του Ηνωμένου Βασιλείου, η οποία ωστόσο κατόπιν πρόσφατης νομολογίας[54] έχει προβεί σε περιορισμούς. Επιπλέον, η αρχή προστασίας δεδομένων της Σουηδίας προσφάτως ενέκρινε τη χρήση από τις αστυνομικές αρχές συστημάτων αναγνώρισης προσώπου που ερείδονται σε βάση δεδομένων (λίστα παρακολούθησης) που περιέχει πάνω από 40.000 φωτογραφίες[55].

- Όσον αφορά στις **βάσεις δεδομένων** που ερείδεται η τεχνολογία αναγνώρισης προσώπου, ορισμένες **ευρωπαϊκές χώρες** περιορίζουν τις αναζητήσεις των αστυνομικών αρχών σε ποινικές βάσεις δεδομένων (λ.χ. Γαλλία, Ιταλία, Ελλάδα, Ηνωμένο Βασίλειο), ενώ **άλλες επιτρέπουν τις αναζητήσεις και σε αστικές** (λ.χ. Φινλανδία, Κάτω Χώρες, Λετονία, Ουγγαρία).
- Περισσότερες από τις μισές χώρες της Βόρειας Αμερικής χρησιμοποιούν συστήματα αναγνώρισης προσώπου. Ενδεικτικά, **ποσοστό άνω του 50% των Αμερικανών πολιτών βρίσκονται σήμερα στις βάσεις δεδομένων της αστυνομίας**, ενώ το Υπουργείο Εσωτερικής Ασφάλειας των Η.Π.Α. αναμένει η εφαρμογή της τεχνολογίας να ανέλθει σε ποσοστό 97% στα αεροδρόμια της χώρας έως το 2023.
- Ακόμα πιο προσφιλής είναι η τεχνολογία αναγνώρισης προσώπου στη Νότια Αμερική, όπου χρησιμοποιείται στο 92% των χωρών της, κυρίως από τις αρχές επιβολής του νόμου.
- Η τεχνολογία αναγνώρισης προσώπου χρησιμοποιείται σε ποσοστό που αγγίζει το 76% και στις χώρες της Μέσης Ανατολής και της Κεντρικής Ασίας. Πρόσφατα, η αστυνομία των Ηνωμένων Αραβικών Εμιράτων, προμηθεύτηκε «έξυπνα γυαλιά» με ενσωματωμένη τεχνολογία αναγνώρισης προσώπου, η οποία θα επιτρέπει την ταυτοποίηση προσώπων σε ζωντανό χρόνο ανάμεσα στο πλήθος.

---

[53] Ragazzi, F. *κ.ά.* (2021), ο.π. σελ 99 επ.

[54] *R (Bridges) v Chief Constable of South Wales Police & Information Commissioner* [2020] EWCA Civ 1058. Διαθέσιμο σε: https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf

[55] Ανδρουλάκη, Ε. (2021) «Τεχνητή νοημοσύνη και προσωπικά δεδομένα : η περίπτωση της εξ αποστάσεως βιομετρικής ταυτοποίησης», *Επιθεώρηση Δικαίου Πληροφορικής*, τ. 1. Διαθέσιμο στο: https://ejournals.lib.auth.gr/infolawj/article/view/8236

- Η Λαϊκή Δημοκρατία της Κίνας πρωτοστατεί στη βιομηχανία αναγνώρισης προσώπου, τόσο αναφορικά με τη χρήση όσο και με την ανάπτυξη και εξαγωγή της τεχνολογίας παγκοσμίως. Αποτελεί την πρώτη χώρα που έχει εγκαθιδρύσει εμφανώς συστήματα αναγνώρισης προσώπου για σκοπούς μαζικής βιομετρικής επιτήρησης - υπάρχει περίπου μία κάμερα κλειστού κυκλώματος ανά 12 πολίτες- και **τα έχει εργαλειοποιήσει στο πλαίσιο συγκρότησης ενός συστήματος αξιολόγησης τής συμπεριφοράς των πολιτών της** («Social Credit System»). Περαιτέρω, οι εταιρείες που εμπλέκονται στο διάχυτο δίκτυο ψηφιακής παρακολούθησης της Κίνας, όπως οι Tencent, Dahua Technology, Hikvision, SenseTime, ByteDance και η ηγέτιδα στον τομέα **Huawei**, **εξάγουν την τεχνογνωσία τους σε ολόκληρη την υφήλιο υπό τη μορφή πακέτων "ασφαλούς πόλης"**.
- Η τεχνολογία αναγνώρισης προσώπου χρησιμοποιείται **μόλις στο 20% των αφρικανικών χωρών**, ωστόσο το ποσοστό αυτό είναι πιθανό να αυξηθεί στο εγγύς μέλλον, καθώς ήδη αρκετές χώρες έχουν προμηθευτεί σχετική τεχνολογία από την Κίνα. Αξίζει να σημειωθεί, ότι **ο κινεζικός τεχνολογικός κολοσσός «Cloudwalk»** συμφώνησε **να εξαγάγει συστήματα αναγνώρισης προσώπου** στη **Ζιμπάμπουε**, με **αντάλλαγμα βιομετρικά δεδομένα** που θα βοηθήσουν στην **εκπαίδευση του αλγορίθμου της προς τους σκουρόχρωμους τόνους δέρματος**.
- Όσο ωριμάζει η τεχνολογία, τόσο συνεχίζει η εκθετική ανάπτυξη των συστημάτων αναγνώρισης προσώπου. Λαμβάνοντας υπ' όψιν μόνον τα δεδομένα που αντλούνται από τις Η.Π.Α. και τη Λαϊκή Δημοκρατία της Κίνας, **ήδη τα πρόσωπα περισσότερων από 1,5 δις ενηλίκων βρίσκονται σήμερα σε βάσεις δεδομένων αναγνώρισης προσώπου**.
- Μόνον δύο χώρες **έχουν απαγορεύσει** την τεχνολογία αναγνώρισης προσώπου: το Βέλγιο και το Λουξεμβούργο. Ωστόσο, τόσο η Σουηδία όσο και η Γαλλία, δίχως να θέτουν την τεχνολογία εκτός νόμου, έχουν απαγορεύσει τη χρήση της στα σχολεία.
- Όσον αφορά στους διεθνείς οργανισμούς, η Interpol διαθέτει ένα σύστημα αναγνώρισης προσώπου που αντλεί δεδομένα από περισσότερες από 160 χώρες και η Europol διαθέτει δύο υπομονάδες που χρησιμοποιούν το σύστημα αναγνώρισης προσώπου επ' ονόματι «FACE»: το Ευρωπαϊκό Κέντρο Καταπολέμησης της Τρομοκρατίας και το Ευρωπαϊκό Κέντρο Καταπολέμησης του Ηλεκτρονικού Εγκλήματος.
- Προσφάτως έγινε γνωστό πως, κατόπιν της εισβολής της Ρωσίας στην Ουκρανία, **ο ιδρυτής της «Clearview AI» προσέφερε στην ουκρανική κυβέρνηση την τεχνολογία** - μια προσφορά που έγινε δεκτή. Σύμφωνα με την ίδια την εταιρεία, η τεχνολογία αναγνώρισης προσώπου

χρησιμοποιείται από την ουκρανική κυβέρνηση για την ταυτοποίηση νεκρών, αλλά και σε σημεία ελέγχου για τον εντοπισμό υπόπτων[56].

Η μαζικότητα της εμφάνισης των συστημάτων αναγνώρισης προσώπου στο δημόσιο βίο και η συνακόλουθη συνειδητοποίηση των ενδεχόμενων κρίσιμων επιπτώσεων αυτής, οδήγησε στη διενέργεια πολλαπλών «σφυγμομετρήσεων» του γενικού πληθυσμού. Οι έρευνες που έχουν δημοσιευτεί αναφορικά με τα ποσοστά αποδοχής της τεχνολογίας είναι εν πολλοίς αντικρουόμενες και σε ορισμένες χώρες, παρά την εκτεταμένη χρήση της τεχνολογίας, πρακτικά ανύπαρκτες. Ενδεικτικά αναφέρεται ότι έρευνα που διενεργήθηκε ανάμεσα σε 6.100 κινέζους πολίτες κατέδειξε ότι στην Κίνα το 83% των ερωτηθέντων θα ήθελε να έχει περισσότερο έλεγχο στα δεδομένα του, καθώς και ότι το 75% προτιμά τις παραδοσιακές μεθόδους ταυτοποίησης έναντι της τεχνολογίας αναγνώρισης προσώπου· άλλες έρευνες καθιστούν σαφές ότι οι κινέζοι πολίτες εμπιστεύονται περισσότερο την επεξεργασία των δεδομένων τους στην κυβέρνηση από ό,τι σε ιδιωτικούς παρόχους. Στο Ηνωμένο Βασίλειο, δημοσκόπηση του 2019[57] ανάμεσα σε 4109 ενήλικες, διαπίστωσε ότι το 77% των ερωτηθέντων δεν αισθάνεται άνετα με την ανάπτυξη της τεχνολογίας από εμπορικές εταιρείες, αλλά το 49% υποστηρίζει τη χρήση της για σκοπούς επιβολής του νόμου εφόσον υπάρχουν ασφαλιστικές δικλείδες, ενώ το 67% αντιτίθεται στη χρήση στα σχολεία και το 61% στη χρήση στα μέσα μαζικής μεταφοράς. Αναφορικά με τις Ηνωμένες Πολιτείες, έρευνα του Pew Research Center σε 4272 ενήλικες διαπίστωσε ότι η αποδοχή ποικίλλει αναλόγως του σκοπού στον οποίο αποβλέπει ένα σύστημα αναγνώρισης προσώπου, αλλά και αναλόγως του φορέα που χρησιμοποιεί την τεχνολογία: το 56% εμπιστεύεται τις αρχές επιβολής του νόμου, το 36% τις ιδιωτικές εταιρείες, ενώ μόνο το 18% εγκρίνει τη χρήση για διαφημιστικούς σκοπούς[58].

---

[56] Clayton, J. (2022) *How facial recognition is identifying the dead in Ukraine - BBC News*, *BBC News*. Διαθέσιμο στο: https://www.bbc.com/news/technology-61055319

[57] Ada Lovelace Institute (2019) *Beyond face value: public attitudes to facial recognition technology*. Διαθέσιμο στο: https://www.adalovelaceinstitute.org/report/beyond-face-value-public-attitudes-to-facial-recognition-technology/

[58] Kostka, G., Meckel, M. (2021) 'Between security and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United States', *Public Understanding of Science*, 30(6), σελ. 674-675.

2. Οι ανεγειρόμενες ανησυχίες από τη χρήση συστημάτων αναγνώρισης προσώπου

Τα συστήματα αναγνώρισης προσώπου, όπως έχει ήδη καταστεί σαφές, κατόπιν της δραματικής βελτιστοποίησης της αποτελεσματικότητας τους με την χρήση των τεχνικών μηχανικής μάθησης, εφαρμόζονται σε ένα ευρύ φάσμα τομέων για ποικίλους σκοπούς και συνεισφέρουν απτά οφέλη τόσο στην καθημερινότητα των απλών πολιτών και στην οικονομική ανάπτυξη των ιδιωτικών επιχειρήσεων, όσο και στην προστασία της δημόσιας ασφάλειας στο πλαίσιο δράσης των αρχών επιβολής του νόμου.

Ωστόσο, η εγγενής παρεμβατικότητα της τεχνολογίας αναγνώρισης προσώπου και η νέα δυναμική που προσφέρουν σε αυτή οι εφαρμογές τεχνητής νοημοσύνης, σε συνδυασμό με την αδύναμη θέση των ατόμων απέναντι στη μαζική, μη επεμβατική συλλογή ενός νευραλγικού για την ανθρώπινη ταυτότητα δεδομένου, αυτού του ανθρώπινου προσώπου, το οποίο πολλώ δε μάλλον δύναται να οδηγήσει στην περαιτέρω εξαγωγή –ευαίσθητης ή μη φύσεως- συμπερασμάτων, δίχως τη συγκατάθεση και πολλές φορές δίχως οποιαδήποτε γνώση του υποκειμένου, καθιστά εμφανείς τις προκλήσεις της χρήσης της τεχνολογίας για τα θεμελιώδη ανθρώπινα δικαιώματα.

Μέχρι προσφάτως, κατά τη δοκιμή και εφαρμογή των τεχνολογιών αναγνώρισης προσώπου, το επίκεντρο της προβληματικής εντοπιζόταν στη βελτίωση της τεχνικής ακρίβειας της τεχνολογίας, δίχως να αξιολογούνται ευρύτερα οι επιπτώσεις σε θεμελιώδη δικαιώματα[59]. Ωστόσο, οι κοινωνικές και πολιτικές εξελίξεις των τελευταίων ετών έφεραν στην επιφάνεια την κρισιμότητα της αντιμετώπισης των ανεγειρόμενων ανησυχιών και της χαλιναγώγησης –νομοθετικά, κοινωνικά, επιστημονικά- της τεχνολογίας αναγνώρισης προσώπου.

2.1 Τεχνικά όρια, προβλήματα και προκλήσεις των συστημάτων αναγνώρισης προσώπου που ερείδονται στην Τεχνητή Νοημοσύνη

Τα συστήματα αναγνώρισης προσώπου οφείλουν στις εφαρμογές τεχνητής νοημοσύνης την άνευ προηγουμένου απόδοση και κυριαρχία τους τόσο στον ιδιωτικό τομέα όσο και στη δημόσια σφαίρα· εντούτοις η τεχνολογία δεν είναι ούτε εντελώς αποτελεσματική ούτε πανίσχυρη. Αντιθέτως, υφίστανται τεχνικές προκλήσεις που περιορίζουν τη φαινομενική παντοδυναμία των εν θέματι συστημάτων, οι οποίες και θα πρέπει να λαμβάνονται υπ' όψιν κατά την ευρύτερη ανάλυση των ηθικών, νομικών και πολιτικών συνεπειών τους.

[59] European Union Agency for Fundamental Rights (2019), ο.π. σελ. 18 επ.

2.1.1 Προκλήσεις ως προς τη συλλογή δεδομένων

Οι τεχνολογικοί κολοσσοί που χρησιμοποιούν ή/ και εξάγουν συστήματα αναγνώρισης προσώπου ευαγγελίζονται ότι η αποτελεσματικότητά τους αγγίζει το 99,92% ακριβείας[60], ποσοστό το οποίο συνήθως στηρίζουν σε δοκιμές της αποτελεσματικότητας των αλγορίθμων τους σε ένα τυποποιημένο σύνολο δεδομένων, το επονομαζόμενο "Ongoing Face Recognition Vendor Test ("FRVT"), του Εθνικού Ινστιτούτου Προτύπων και Τεχνολογίας των Η.Π.Α. ("NIST").

Εντούτοις, τα ποσοστά τελειότητας που εκθειάζονται αφορούν στη χρήση της τεχνολογίας σε ιδανικές- απολύτως ελεγχόμενες συνθήκες, δίχως να προσμετράται η απόδοση των συστημάτων σε πραγματικές συνθήκες και στα λεγόμενα «*μη ελεγχόμενα περιβάλλοντα*», ήτοι σε «*χώρους ελεύθερα προσβάσιμους στα άτομα, όπου μπορούν επίσης να διέλθουν, συμπεριλαμβανομένων των δημόσιων και οιονεί δημόσιων χώρων, όπως εμπορικά κέντρα, νοσοκομεία ή σχολεία*»[61]. Στην πραγματικότητα, η ακρίβεια της τεχνολογίας εξαρτάται από ποικίλες παραμέτρους, μεταξύ των οποίων:

- **Η ανάλυση της κάμερας**, ιδίως δε η βασική μεταβλητή των pixels ανά μέτρο, είναι καθοριστική για να εξασφαλιστεί ότι παρέχονται επαρκείς πληροφορίες στον αλγόριθμο.
- Οι **συνθήκες φωτισμού**, καθώς τα ανεπαρκώς φωτισμένα πρόσωπα συνεπάγονται μεγάλο αριθμό σφαλμάτων.
- Ο **προσανατολισμός του προσώπου** σε σχέση με την κάμερα είναι ένας ακόμη βασικός παράγοντας, δεδομένου ότι μία κάμερα σπανίως θα τοποθετηθεί στο επίπεδο του προσώπου του ατόμου, με αποτέλεσμα πολύ συχνά το σύστημα να λαμβάνει αποσπασματική μόνον απεικόνιση ενός προσώπου.
- Η **λήψη της εικόνας προσώπου μπορεί συχνά να εμποδίζεται**, λ.χ. από άλλα άτομα, γυαλιά ηλίου ή μάσκες, ακόμη και εκουσίως όταν τα άτομα αποστρέφουν το πρόσωπό τους από το σύστημα.
- Αναφορικά με τη χρήση της τεχνολογίας για την **εξ αποστάσεως βιομετρική παρακολούθηση σε πραγματικό χρόνο**, οφείλει να

---

[60] Σύμφωνα με έρευνα του NIST το 2020, ο καλύτερος αλγόριθμος είχε ποσοστό αποτυχίας μόλις 0,08%, βλ. Thales Group (2021) 'Biometrics (facts, use cases, biometric security)'. Διαθέσιμο στο: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics Ομοίως, η εταιρεία Meta (πρώην Facebook) υποστηρίζει ότι το σύστημα Deepface έχει ποσοστό ακριβείας 97,25%, βλ. https://www.forbes.com/sites/amitchowdhry/2014/03/18/facebooks-deepface-software-can-match-faces-with-97-25-accuracy/?sh=66d2f58f54fc

[61] Council of Europe- Convention 108 (2021) *Guidelines on facial recognition'*. Διαθέσιμο στο: https://edoc.coe.int/en/artificial-intelligence/9753-guidelines-on-facial-recognition.html

επισημανθεί ότι **δεν ανταποκρίνονται όλα τα συστήματα αναγνώρισης προσώπου σε αυτή την τεχνική πρόκληση**, ήτοι πολλά αδυνατούν να ανιχνεύσουν επιτυχώς ανθρώπινα πρόσωπα ή είναι δυνατό να «ξεγελαστούν» λ.χ. από φωτογραφίες.

Όπως ευλόγως συνάγεται, η ακρίβεια ενός συστήματος αναγνώρισης προσώπου είναι σε τέτοιο βαθμό πολυπαραγοντική, ώστε ακόμη και σε ιδανικές συνθήκες να ελλοχεύει πάντοτε ο κίνδυνος σφάλματος. Πράγματι, έρευνες καταδεικνύουν πως **η τεχνική απόδοση της τεχνολογίας παραμένει αρκετά περιορισμένη** και ο αλγόριθμος συχνά υποπίπτει σε δύο είδη σφαλμάτων: είτε σε αποτέλεσμα **ψευδώς αρνητικό,** όταν το λογισμικό αποτυγχάνει να ανιχνεύσει αν υπάρχει ανθρώπινο πρόσωπο σε μια εικόνα, είτε **ψευδώς θετικό,** όταν το λογισμικό αναγνωρίζει ως πραγματικό πρόσωπο ένα μη- ανθρώπινο στοιχείο.

2.1.2 Προκλήσεις ως προς την ποιότητα των συνόλων δεδομένων

Τα συστήματα αναγνώρισης προσώπου αντιμετωπίζουν, επίσης, ορισμένες **τεχνικές προκλήσεις** που απορρέουν από την **ποιότητα και την ποσότητα των συνόλων δεδομένων στα οποία ερείδονται τα συστήματα μηχανικής μάθησης**.

Αρχικώς, τα μικρά σύνολα δεδομένων εκπαιδεύουν ανεπαρκώς τους αλγορίθμους, είτε επειδή δεν παρέχουν αρκετές διαφορετικές εκδοχές του ανθρώπινου προσώπου ώστε να καθίσταται σε κάθε περίπτωση ανιχνεύσιμο, είτε διότι δεν παρουσιάζουν την απαιτούμενη ποικιλομορφία που απαιτείται για τη λυσιτελή λειτουργία ενός τέτοιου συστήματος. Επιπλέον, συχνά τα σύνολα δεδομένων συλλέγονται για συγκεκριμένο σκοπό, με αποτέλεσμα η εκπαίδευση ενός αλγορίθμου αναγνώρισης προσώπου σε ένα σύνολο δεδομένων που δεν είναι αντιπροσωπευτικό των αποδεκτών του συστήματος, να καθίσταται ικανή να οδηγήσει σε σοβαρά ζητήματα αποτελεσματικότητας και υψηλά ποσοστά σφάλματος.

Εκ των ανωτέρω, ιδιαίτερα προβληματική έχει αποδειχθεί η **έλλειψη ποικιλομορφίας στις βάσεις δεδομένων**, κυρίως όσον αφορά στην εθνικότητα, στην ηλικία ή στο φύλο, διότι **οδηγεί σε μεροληψία** στον αλγόριθμο. Μάλιστα, μερικές από τις πιο δημοφιλείς στην εκπαίδευση αλγορίθμων αναγνώρισης προσώπου δημόσιες βάσεις δεδομένων, όπως οι VGGFace2 και MS-Celeb-1M42, απέχουν παρασάγγας από την αντιπροσωπευτική απεικόνιση του συνόλου του

πληθυσμού, φαινόμενο που ονομάζεται ***μεροληψία αντιπροσώπευσης***[62] και έχει βρεθεί στο επίκεντρο του προβληματισμού της παγκόσμιας κοινότητας, διότι συνεπάγεται **σημαντικά ποσοστά σφαλμάτων για τις λιγότερο αντιπροσωπευόμενες ομάδες πληθυσμού**.

Φυσικά, η ποσότητα δεν συνεπάγεται απαραιτήτως και ποιότητα· ο αλγόριθμος, προκειμένου να εκπαιδευτεί σωστά, θα πρέπει να ερείδεται σε ένα σύνολο με δεδομένα ποσοτικά επαρκή, αλλά και **ποιοτικώς κατάλληλα**, αφενός διότι ακόμη και φαινομενικά αδιαμφισβήτητες έννοιες γίνονται ρευστές τη στιγμή που πρέπει να οριοθετηθούν αυστηρά στο πλαίσιο ενός συνόλου δεδομένων, αφετέρου διότι θα πρέπει να εξασφαλισθεί η συμπερίληψη όλων των πιθανών ομάδων-αποδεκτών του συστήματος.

Προσέτι, σημαντικό ζήτημα με κρίσιμες ηθικές και πολιτικές προεκτάσεις αποτελεί η συλλογή δεδομένων με αθέμιτους τρόπους, όπως η **ιστοσυγκομιδή**, πρακτική στην οποία, όπως προαναφέρθηκε, επιδίδονται εκτεταμένα εταιρείες όπως η PimEyes[63] και η Clearview AI. Επιπροσθέτως, ιδιαίτερα εκτεταμένη είναι και η κατάρτιση των βάσεων δεδομένων με **χρήση υπηρεσιών που βασίζονται στο νέφος** (είτε για την επεξεργασία είτε για την αποθήκευση των ευαίσθητων πληροφοριών), με αποτέλεσμα να αυξάνονται οι κίνδυνοι αλλοίωσης αλλά και παραβίασης των δεδομένων συνεπεία κακόβουλων επιθέσεων.

2.1.3 Προκλήσεις ακριβείας που σχετίζονται με τον αλγόριθμο αναγνώρισης προσώπου

Αναπτύσσοντας επί των ανωτέρω, ένα νευραλγικό ζήτημα που σχετίζεται με τις ενδογενείς αδυναμίες της Τεχνητής Νοημοσύνης, είναι η εμφιλοχώρηση στους αλγορίθμους αναγνώρισης προσώπου, της λεγόμενης «*μεροληψίας του δράστη-παρατηρητή*» ή «*μεροληψίας επιβεβαίωσης*».

Ειδικότερα, η προβληματική εντοπίζεται στο γεγονός ότι τα δεδομένα εξόδου (outputs) ενός αλγορίθμου ενισχύουν τις -υποσυνείδητες ή μη- προκαταλήψεις που υπεισήλθαν στην παραγωγή του. Τούτο μπορεί να συμβεί

---

[62] Fernandez, V. κ.ά. (2020) '*Facial Recognition: Embodying European Values*'. Paris: Renaissance Numérique. σελ. 30. Διαθέσιμο στο: https://www.renaissancenumerique.org/wp-content/uploads/2022/06/renaissancenumerique_report_facialrecognition.pdf

[63] Με 29,99 δολάρια το μήνα, ένας ιστότοπος που ονομάζεται PimEyes προσφέρει τη δυνατότητα σε οποιονδήποτε να προβεί σε αναζήτηση ενός προσώπου, το οποίο θεωρητικά πρέπει ανήκει στον ίδιο, σε κάθε πιθανή «γωνιά» του διαδικτύου, βλ. Hill, K. (2022) 'A Face Search Engine Anyone Can Use Is Alarmingly Accurate', *The New York Times*. Διαθέσιμο στο: https://www.nytimes.com/2022/05/26/technology/pimeyes-facial-recognition-search.html

τόσο κατά τη δημιουργία του συνόλου δεδομένων, όσο και κατά τον σχεδιασμό, την εκπαίδευση ή/ και την εκτέλεση των αλγορίθμων. Η περιορισμένη ποικιλομορφία ως προς το εργατικό δυναμικό στην ΤΝ μπορεί επίσης να έχει αρνητικό αντίκτυπο σε διάφορα στάδια ανάπτυξης του συστήματος, καθώς οι προκαταλήψεις μπορούν είτε να ενσωματωθούν στον ίδιο τον αλγόριθμο, είτε να παρεισδύσουν στο αποτέλεσμα, κατά κύριο λόγο όταν τα άτομα καλούνται να αποφασίζουν ποια ενέργεια θα ακολουθήσει μια βιομετρική αντιστοίχιση[64]. Η μεροληψία στα συστήματα ΤΝ μπορεί να προέρχεται, επίσης, από προκαταλήψεις που ενυπάρχουν στις μεθόδους των επιστημόνων, στο αντικείμενο της έρευνάς τους, στις πηγές δεδομένων τους (π.χ. μεροληψία επιλογής) κ.ο.κ, ενώ συχνά, η μεροληψία οφείλεται στην πρακτική της ιστοσυγκομιδής, ως αποτέλεσμα της αφιλτράριστης μαζικότητας των δεδομένων που συναπαρτίζουν το σύνολο βάσει του οποίου εκπαιδεύεται ο αλγόριθμός.

Απόρροια των ανωτέρω, αποτελεί η εκπαίδευση των αλγορίθμων αναγνώρισης προσώπου σε βάσεις δεδομένων στις οποίες κοινωνικά κυρίαρχες ομάδες, όπως οι λευκοί άντρες, υπερ-αντιπροσωπεύονται, με αποτέλεσμα ο αλγόριθμος να αντανακλά τις σχέσεις εξουσίας, τις κοινωνικές ιεραρχίες και τις συστημικές ανισότητες που χαρακτηρίζουν την κοινωνικοπολιτική πραγματικότητα, αποτυγχάνοντας να αποτυπώσει ισορροπημένες αναπαραστάσεις των διαφορετικών πληθυσμιακών ομάδων, πολλές από τις οποίες καταλήγουν να υπο-εκπροσωπούνται και να πλήττονται δυσανάλογα από τα σφάλματα αποτελέσματος του αλγορίθμου.

Πληθώρα ερευνών ανέδειξαν το εν λόγω ζήτημα, αποδεικνύοντας ότι οι αλγόριθμοι αναγνώρισης προσώπου που χρησιμοποιούνται ευρέως από εταιρείες όπως οι IBM, Microsoft και Amazon παρουσιάζουν χειρότερες επιδόσεις σε πρόσωπα με σκουρόχρωμο δέρμα, και ιδίως σε γυναίκες με σκουρόχρωμο δέρμα, με ποσοστά σφάλματος που σύμφωνα με μία εκ των πλέον αναγνωρισμένων μελετών ανέρχεται έως και 34,7% υψηλότερα από ό,τι στους άνδρες με ανοιχτόχρωμο δέρμα[65]. Η έκταση της προβληματικής αναδείχθηκε ιδιαίτερα στις Η.Π.Α., με το NIST να επισημαίνει ότι η τεχνολογία αναγνώρισης προσώπου **ταυτοποιεί εσφαλμένα** ανθρώπους της μαύρης ή ασιατικής φυλής έως και **100 φορές περισσότερο** απ' ό,τι ανθρώπους της λευκής φυλής. Χαρακτηριστική είναι και η μελέτη της Αμερικανικής Ένωσης για τις Πολιτικές Ελευθερίες επί του λογισμικού Rekognition της Amazon το 2018, στην οποία έγινε αντιπαραβολή φωτογραφιών των μελών του Κογκρέσου έναντι ενός συνόλου δεδομένων με

---

[64] Gonzalez Fuster, G & Nadolna Peeters, M.A. (2021), ο.π. σελ 34-36. Διαθέσιμο στο: http://www.europarl.europa.eu/thinktank

[65] Βλ. Buolamwini, J. (2018) 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification', *Proceedings of Machine Learning Research*, τ. 81, σελ. 8.

φωτογραφίες συλλήψεων, με αποτέλεσμα 28 μέλη, στο μεγαλύτερο ποσοστό τους άνθρωποι με μαύρο δέρμα, να ταυτοποιηθούν εσφαλμένα από το σύστημα ως συλληφθέντες για ποινικά αδικήματα.

Αξίζει να σημειωθεί ότι πολλές από τις υπό εξέταση εταιρείες τροποποίησαν, κατόπιν της κατακραυγής, τα συστήματα αναγνώρισης προσώπου που χρησιμοποιούν προκειμένου να εξαλείψουν -κατά το δυνατό- τα υψηλά και δυσανάλογα ποσοστά σφάλματος, ωστόσο αυτό δεν κατέστη δυνατό και τα συστήματα **κατά τον επανέλεγχο εξακολουθούσαν να επιδεικνύουν –αν και λιγότερη- μεροληψία**. Το γεγονός αυτό καταδεικνύει τις δυσχέρειες ως προς την κατανόηση και τη λυσιτελή βελτιστοποίηση των αλγορίθμων, οι οποίες απορρέουν από **το φαινόμενο του «μαύρου κουτιού»** ("black box"), το οποίο χαρακτηρίζει εγγενώς τα αυτόματα συστήματα Τεχνητής Νοημοσύνης, στα οποία η επεξηγησιμότητα καθίσταται δυσχερώς επιτεύξιμη λόγω του πολύπλοκου και αδιαφανούς τρόπου λειτουργίας τους, ο οποίος δεν επιτρέπει να οριοθετηθεί επακριβώς πώς και γιατί κατέληξε ο αλγόριθμος στην εκάστοτε απόφαση[66].

2.2 Οι επιπτώσεις σε θεμελιώδη ανθρώπινα δικαιώματα

Τα απαραδέκτως υψηλά ποσοστά ψευδών αντιστοιχιών που αποκαλύφθηκαν από την επιστημονική κοινότητα, σε συνδυασμό με το όλο και αυξανόμενο –έμπρακτο- ενδιαφέρον που επιδεικνύουν οι αστυνομικές αρχές παγκοσμίως για τη χρήση συστημάτων αναγνώρισης προσώπου σε δημόσιους χώρους, αλλά και την εμπορική εκτίναξη της βιομηχανίας της τεχνολογίας με προμηθευτές που δε διστάζουν να καταφύγουν σε αθέμιτες πρακτικές συλλογής δεδομένων, πυροδότησαν μια έντονη συζήτηση σχετικά με τις βαρύτατες επιπτώσεις της τεχνολογίας στα ανθρώπινα δικαιώματα, με μεγάλη μερίδα θεωρητικών να αναρωτιούνται αν δύναται η τεχνολογία αναγνώρισης προσώπου να συνυπάρξει με αυτά, δίχως να οδηγήσει στην κατάλυσή τους.

2.2.1 Προκατάληψη & διακρίσεις

Πράγματι, η παγκόσμια τάση άκρατης και εν πολλοίς αρρύθμιστης γενίκευσης της χρήσης αλγορίθμων αναγνώρισης προσώπου έχει ήδη αποδειχθεί ικανή να καταπατήσει κάθε θεμελιώδες ανθρώπινο δικαίωμα. Στη Λαϊκή Δημοκρατία της Κίνας, η τεχνολογία χρησιμοποιείται, ως προαναφέρθη, στο πλαίσιο της **γενικευμένης κρατικής παρακολούθησης** μέσω ενός «συστήματος κοινωνικής πίστωσης», το οποίο αποσκοπεί στον έλεγχο και στην αξιολόγηση

---

[66] Παπαδούλη, Β. (2022) 'Εννοιολογικές Προσεγγίσεις της «Διαφάνειας» στο πεδίο της Τεχνητής Νοημοσύνης υπό ένα νομικό πρίσμα', *Pro Justitia: Ηλεκτρονική Επετηρίδα Νομικής Σχολής ΑΠΘ*, 5(0), σελ. 30–44.

κάθε πιθανής δραστηριότητας των πολιτών της, προκειμένου να προβαίνει σε κατάταξη αυτών βάσει των «επιδόσεων» τους και να καθίσταται έτσι δυνατή η συνακόλουθη επιβράβευση ή τιμώρησή τους από το καθεστώς. Έτι περαιτέρω, η τεχνολογία χρησιμοποιείται για την **παρακολούθηση –ακόμα και εντός της οικίας τους- και τον έλεγχο μειονοτικών ομάδων** του πληθυσμού, κυρίως δε της μουσουλμανικής μειονότητας των Ουιγούρων.[67]

Η **στοχοποίηση ευάλωτων κοινωνικών ομάδων** μέσω της χρήσης της συστημάτων αναγνώρισης προσώπου μπορεί να μην αποτελεί αυτοσκοπό σε μη-αυταρχικά καθεστώτα, ωστόσο έχει αποτελέσει το ανατριχιαστικό αποτέλεσμα της ανακρίβειας που κατατρέχει την τεχνολογία. Η αλγοριθμική μεροληψία και η εμφιλοχώρηση προκαταλήψεων κατά την ανάπτυξη και χρήση της τεχνολογίας αναγνώρισης προσώπου έχουν οδηγήσει στην διαιώνιση των ήδη υφιστάμενων κοινωνικών διακρίσεων: χαρακτηριστικό παράδειγμα αποτελεί η σύλληψη για κλοπή του αφροαμερικανού Robert Julian-Borchak Williams, κατόπιν ψευδούς θετικού αποτελέσματος του συστήματος αναγνώρισης προσώπου που χρησιμοποιεί η αστυνομία της πολιτείας του Μίσιγκαν: η ταυτοποίησή του έγινε με την αντιπαραβολή μιας παλιάς φωτογραφίας διπλώματος με μία εικόνα από την κάμερα ασφαλείας του καταστήματος που τελέστηκε η κλοπή. Ακολούθησε η -δίχως καμία εξήγηση- απαίτηση της αστυνομίας να παρουσιαστεί ενώπιον της και η αναίτια σύλληψη και κράτησή του για τριάντα ώρες.[68]

Το ανωτέρω παράδειγμα δεν αποτελεί μεμονωμένο περαστικό: εμπειρικές μελέτες δείχνουν ότι **ο κίνδυνος διακριτικής μεταχείρισης** όσον αφορά στους μαύρους ανθρώπους, στο πλαίσιο επιβολής του νόμου, είναι σε τέτοιο βαθμό δυσανάλογος, ώστε να **μεταβάλλει το παραδοσιακό τεκμήριο αθωότητας σε ποινικές υποθέσεις[69]**, αντιστρέφοντας το βάρος απόδειξης και εναποθέτοντάς το στους υπόπτους, οι οποίοι καλούνται να αποδείξουν ότι δεν είναι αυτοί που το σύστημα αναγνωρίζει. Ανησυχίες εγείρονται επιπροσθέτως, σχετικά με την αυτοματοποιημένη καταδίκη κατόπιν της αναγνωρίσεως ενός υπόπτου από το

---

[67] Mozur, P. (2019) *One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority - The New York Times*, *14 April*. Διαθέσιμο στο: https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html

[68] Hill, K. (2020) *Wrongfully Accused by an Algorithm - The New York Times*, *New York Times*. Διαθέσιμο στο: https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html

[69] The Office of the High Commissioner for Human Rights (UN Human Rights) (2020) *Report of the proceedings of the online expert seminar with the purpose of identifying how artificial intelligence, including profiling, automated decision-making and machine learning technologies may, without proper safeguards, affect the enjoyment of the right to privacy (2020)*. Διαθέσιμο στο: https://www.ohchr.org/sites/default/files/Documents/Issues/DigitalAge/ExpertSeminarReport-Right-Privacy.pdf

σύστημα. Τέτοιου ίδιους πρακτικές αντιβαίνουν ευθέως στο άρθρο 21 του Χάρτη Θεμελιωδών Δικαιωμάτων του Ανθρώπου (εφεξής, ο Χάρτης), το οποίο απαγορεύει *κάθε διάκριση, ιδίως λόγω φύλου, φυλής, χρώματος, εθνοτικής καταγωγής ή κοινωνικής προέλευσης, γενετικών χαρακτηριστικών, γλώσσας, θρησκείας ή πεποιθήσεων, πολιτικών φρονημάτων ή κάθε άλλης γνώμης, ιδιότητας μέλους εθνικής μειονότητας, περιουσίας, γέννησης, αναπηρίας, ηλικίας ή γενετήσιου προσανατολισμού.*

2.2.2 Κίνδυνος μαζικής επιτήρησης και ανησυχίες για τα θεμελιώδη δικαιώματα

Η παρεμβατικότητα της τεχνολογίας αναγνώρισης προσώπου πολλαπλασιάζεται εκθετικά όταν τα συστήματα μετατοπίζονται στο δημόσιο forum, στο πλαίσιο της δράσης των αστυνομικών αρχών.

Ως έχει καταστεί ήδη σαφές, η ραγδαία ανάπτυξη και χρήση των συστημάτων αναγνώρισης προσώπου σε δημόσια προσβάσιμους χώρους για σκοπούς δημόσιας ασφάλειας, αποτελεί πλέον τη νόρμα τόσο στην Ευρώπη όσο και διεθνώς. Εν απουσία σαφούς ρυθμιστικού πλαισίου, η ερμηνεία εννοιών όπως η *δημόσια ασφάλεια* εναποτίθεται στις αρχές επιβολής του νόμου, με άμεσο επακόλουθο οι πολίτες συχνά είτε να **αγνοούν ότι βρίσκονται υπό παρακολούθηση**, είτε **να μην γνωρίζουν πότε και υπό ποιες προϋποθέσεις γίνεται χρήση της τεχνολογίας**: ένα σύστημα αναγνώρισης προσώπου καταγράφει μοναδικά χαρακτηριστικά του ανθρώπινου σώματος τα οποία είναι δύσκολο να κρυφτούν, ένας τεράστιος αριθμός εικόνων είναι πάντοτε έτοιμος προς «συγκομιδή» στο διαδίκτυο, ενώ η τεχνολογία συλλέγει έναν απίθανο όγκο εξαιρετικά ευαίσθητων δεδομένων αναρίθμητων υποκειμένων χάρη στη μηχανική μάθηση, **δίχως να είναι απαραίτητη σε κανένα στάδιο της διαδικασίας η συγκατάθεση του ατόμου προκειμένου να επιτευχθεί –τεχνικά- η συλλογή**. Αντιθέτως, το σύστημα αναγνώρισης προσώπου μπορεί ανά πάσα στιγμή να συλλάβει εξ αποστάσεως τις εικόνες προσώπων, **δίχως τη γνώση – πολλώ δε μάλλον τη συναίνεση-** των υπό παρακολούθηση υποκειμένων.

Ωστόσο, σε μια δημοκρατική κοινωνία, **η ανωνυμία αποτελεί χαρακτηριστικό γνώρισμα του δημόσιου χώρου**· το γεγονός ότι η τεχνολογία αναγνώρισης προσώπου είναι ανοριοθέτητα πανταχού παρούσα, αποτελεί πρωταρχική πηγή ανησυχίας με απτές συνέπειες στα ανθρώπινα δικαιώματα.

Μελέτες των τελευταίων ετών υπογραμμίζουν ότι **και μόνη η γνώση της πιθανότητας να τελεί το άτομο υπό παρακολούθηση**, είναι αρκετή για να παρεμποδίσει την απρόσκοπτη άσκηση δικαιωμάτων συνταγματικής περιωπής, όπως η **ελευθερία της έκφρασης** και της **ελεύθερης ανάπτυξης της**

προσωπικότητάς του, καθώς **το άτομο τροποποιεί τη συμπεριφορά του προκειμένου να μην παρεκκλίνει από τα κοινωνικά πρότυπα**. Όπως ευλόγως συνάγεται, θεμελιώδεις ελευθερίες, νευραλγικές για τη λειτουργία του δημοκρατικού πολιτεύματος, μεταξύ των οποίων **το δικαίωμα στο σεβασμό της ιδιωτικής και οικογενειακής ζωής**, **το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα, το δικαίωμα του συναθροίζεσθαι, το δικαίωμα χρηστής διοίκησης, το δικαίωμα πραγματικής προσφυγής, αλλά και τα ειδικότερα δικαιώματα ευάλωτων ομάδων** που χρήζουν υψηλότερου επιπέδου προστασίας καθώς βάλλονται δυσανάλογα από την τεχνολογία**, όπως οι ηλικιωμένοι, τα παιδιά και τα άτομα με αναπηρίες,** βρίσκονται στο απόσπασμα.

Ειδικότερα ως προς **το δικαίωμα του συνέρχεσθαι και συνεταιρίζεσθαι,** οφείλει να επισημανθεί ότι οι άνθρωποι, έχοντας επίγνωση ότι είναι κάθε στιγμή δυνατή η εξατομικευμένη ταυτοποίησή τους, περιορίζουν τη δραστηριότητα και τη συμμετοχή τους στο κοινωνικοπολιτικό γίγνεσθαι ("**chilling effect**"), απεμπολούν βασικά δικαιώματα τους ως πολίτες μιας δημοκρατικής κοινωνίας και στρέφονται προς τα έσω, προκειμένου να διαφυλάξουν κατά το δυνατό την ιδιωτική τους ζωή. **Εν τέλει το δικαίωμα στην ίδια την ανθρώπινη αξιοπρέπεια** βάλλεται στον πυρήνα του, ενώ καθίσταται ευλόγως εμφανές ότι η μαζική και άκρατη χρήση της τεχνολογίας στη δημόσια σφαίρα **καθιστά εκ των προτέρων όλους ανεξαιρέτως τους πολίτες «υπόπτους»**, με αποτέλεσμα να **παραβιάζεται** και η πεμπτουσία του δικαίου των ανθρωπίνων δικαιωμάτων: **η αρχή της αναλογικότητας**.

Οι φόβοι περί κατάχρησης της τεχνολογίας αναγνώρισης προσώπου από τις κυβερνήσεις διεθνώς με σκοπό **να παρακολουθούν, να εκφοβίζουν και να διώκουν τους διαδηλωτές**, έχουν ήδη **επιβεβαιωθεί**: για παράδειγμα, στην Αμερική οι πορείες "Black Lives Matter" παρακολουθούνται ήδη από το 2015 μέσω συστημάτων αναγνώρισης προσώπου, τα οποία αποτελούν επιβοηθητικό εργαλείο ταυτοποίησης και συλλήψεων, ενώ οι διαμαρτυρίες κατόπιν της δολοφονίας του George Floyd το 2020, βρίσκονταν υπό τόσο στενή παρακολούθηση, ώστε η Διεθνής Αμνηστία να κατασκευάσει μια **ιστοσελίδα-κάλεσμα για την ολική απαγόρευση της τεχνολογίας**, στην οποία ο καθένας μπορεί να διαπιστώσει, εισάγοντας οποιεσδήποτε συντεταγμένες, πόσες κάμερες με ενσωματωμένα συστήματα αναγνώρισης προσώπου είναι στραμμένα πάνω του σε μια οποιαδήποτε διαδρομή στη Νέα Υόρκη[70]. Ομοίως, οι διαδηλωτές στο Χονγκ Κονγκ καταστρέφουν τους «έξυπνους φανοστάτες» που βρίσκονται διάσπαρτοι σε όλη την πόλη, λόγω έντονων ανησυχιών ότι διαθέτουν

[70] https://banthescan.amnesty.org/

ενσωματωμένη τεχνολογία αναγνώρισης προσώπου[71], ενώ στη Ρωσία η τεχνολογία αναγνώρισης προσώπου χρησιμοποιείται όλο και περισσότερο εναντίον πολιτικών αντιφρονούντων και ακτιβιστών για τα ανθρώπινα δικαιώματα.

Όπως σαφώς προκύπτει, η de facto αδυναμία ανώνυμης μετακίνησης στον δημόσιο χώρο και ο επακόλουθος κομφορμισμός των πολιτών **οδηγεί στην στρέβλωση της ισορροπίας ισχύος μεταξύ των πολιτών και ενός κράτους** που μέσω της τεχνολογίας αναγνώρισης προσώπου είναι **πανταχού παρόν**, θυμίζοντας ευλόγως **ένα σύγχρονο ψηφιακό πανοπτικόν**[72]. Όπως υπογράμμισε η ιταλική Αρχή Προστασίας Δεδομένων, «***η αυτοματοποιημένη επεξεργασία βιομετρικών δεδομένων για την αναγνώριση προσώπου θα μπορούσε να αποτελέσει μια μορφή αδιάκριτης μαζικής επιτήρησης***».

2.2.3 Το δικαίωμα του σεβασμού της ιδιωτικής και οικογενειακής ζωής & το δικαίωμα στην προστασία δεδομένων προσωπικού χαρακτήρα

Οι επαπειλούμενες επιπτώσεις στα δικαιώματα στον σεβασμό της ιδιωτικής και οικογενειακής ζωής και στην προστασία των δεδομένων προσωπικού χαρακτήρα, βρίσκονται στο επίκεντρο του προβληματισμού κατά την ανάπτυξη και χρήση των συστημάτων αναγνώρισης προσώπου με ενσωματωμένες μεθόδους τεχνητής νοημοσύνης· όπως έχει επισημανθεί από θεσμικούς και επιστημονικούς φορείς, τα εν λόγω «*βιομετρικά συστήματα δεύτερου κύματος*»[73] εγκυμονούν νέους και πρωτοφανώς έντονους κινδύνους που απειλούν να κλονίσουν τα θεμελιώδη αυτά δικαιώματα στον πυρήνα τους.

Κατ' αρχάς, **η εικόνα του προσώπου ενός ατόμου αποτελεί κεφαλαιώδες στοιχείο της ταυτότητάς του**, πολύτιμη έκφραση της

---

[71] Zalnieriute, M. (2021) 'Burning Bridges: The Automated Facial Recognition Technology and Public Space Surveillance in the Modern State', *Columbia Science and Technology Law Review*, 22(2), σελ. 298–299.

[72] Το «Πανοπτικόν» αποτελεί θεωρητικό κατασκεύασμα του ωφελιμιστή φιλοσόφου και νομικού Jeremy Bentham. Πρόκειται για ένα αρχιτεκτονικό σχέδιο που αποσκοπεί στον αποτελεσματικό έλεγχο των κρατουμένων ενός σωφρονιστικού ιδρύματος με το λιγότερο δυνατό κόστος: στο «Πανοπτικόν» οι δεσμοφύλακες παρακολουθούν τους φυλακισμένους στα κελιά τους από έναν κεντρικό πύργο με απόλυτη ορατότητα σε αυτά, ο οποίος επιτρέπει την επίβλεψη κάθε πράξης τους δίχως οι φρουροί να είναι ποτέ ορατοί. Τούτο έχει ως αποτέλεσμα οι κρατούμενοι να γνωρίζουν ότι τελούν υπό παρακολούθηση, χωρίς να γνωρίζουν πότε ακριβώς αυτή συντελείται. Σύμφωνα με τον Μπένθαμ, αυτό είναι αρκετό για να εξαναγκαστούν οι κρατούμενοι σε μια μόνιμη κατάσταση παθητικότητας.

[73] Βλ. σχετικά και τη μελέτη της Ευρωπαϊκής Επιτροπής, Renda, A. *κ.ά.* (2021) *Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe*. σελ. Διαθέσιμο στο: https://op.europa.eu/en/publication-detail/-/publication/55538b70-a638-11eb-9585-01aa75ed71a1/language-en/format-PDF/source-204305195

μοναδικότητας κάθε ανθρώπου που αποκαλύπτει τις ιδιαίτερες πτυχές της προσωπικότητάς του. Η προστασία του δικαιώματος ενός φυσικού προσώπου στην εικόνα του, αποτελεί, συνεπώς, ουσιώδες προαπαιτούμενο της προσωπικής του ανάπτυξης και της θωράκισης της ευλόγως προσδωκόμενης ιδιωτικής σφαίρας αυτού, όπως και του δικαιώματός του στον πληροφοριακό αυτοκαθορισμό.

Η τεχνολογία αναγνώρισης προσώπου, δεδομένου ότι μετέρχεται βιομετρικών τεχνικών για τη **συλλογή, σύγκριση και αποθήκευση εικόνων προσώπου με σκοπό την αδιαμφισβήτητη ταυτοποίηση των υποκειμένων τους**, συνεπάγεται, ως έχει αναλυθεί στο πρώτο κεφάλαιο της παρούσας, την **επεξεργασία *βιομετρικών δεδομένων***. Ως εκ τούτου, **τόσο η ίδια η εγκατάσταση συστημάτων αναγνώρισης προσώπου** σε δημόσιους, ημι-δημόσιους ή ιδιωτικούς χώρους, **όσο και η λήψη της εικόνας προσώπου ενός ατόμου προκειμένου να εξαχθεί από αυτή ένα βιομετρικό υπόδειγμα** και στη συνέχεια **να συγκριθεί** με τα λοιπά βιομετρικά πρότυπα που φυλάσσονται στην εκάστοτε βάση δεδομένων **ώστε να επαληθευτεί- ή μη- η ταυτότητά του**, **συνιστούν άμεση επέμβαση/περιορισμό** τόσο στο δικαίωμα προστασίας των δεδομένων προσωπικού χαρακτήρα, όπως κατοχυρώνεται στο άρθρο 8 του Χάρτη, όσο και στο δικαίωμα στην ιδιωτική και οικογενειακή ζωή, κατά τα προβλεπόμενα στα άρθρα 7 του Χάρτη και 8 της Ευρωπαϊκής Σύμβασης Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ).

Έτι περαιτέρω, η **εργαλειοποίηση των εφαρμογών βαθιάς μάθησης** επιτρέπει την **εξόρυξη και ανάλυση εξαιρετικά ευαίσθητων δεδομένων σε τεράστια κλίμακα**, ενώ καθιστά **σχεδόν αδύνατη τη χειροκίνητη επαλήθευση** αυτών, καθόσον τα σύνολα δεδομένων επαυξάνονται ραγδαία. Παραλλήλως, το προαναφερθέν **φαινόμενο του «μαύρου κουτιού»**, δυσχεραίνει ουσιωδώς οποιαδήποτε απόπειρα κατανόησης ή/και επέμβασης στο modus operandi και στα αποτελέσματα του βιομετρικού λογισμικού (αλγοριθμική αδιαφάνεια). Περαιτέρω, ο όλο κι αυξανόμενος **συνδυασμός των τεχνολογιών τεχνητής νοημοσύνης και του Διαδικτύου των Πραγμάτων (Internet of Things)**[74] έχει ως επακόλουθο ακόμη περισσότερα δεδομένα –προσωπικά και μη- να συλλέγονται και να αναλύονται διαρκώς μέσω «έξυπνων» συσκευών της απλής καθημερινότητας (π.χ. βιντεοκαμερών με ενσωματωμένο αλγόριθμο

[74] Ο όρος Διαδίκτυο των πραγμάτων αναφέρεται σε σενάρια όπου η συνδεσιμότητα δικτύου και η υπολογιστική ικανότητα επεκτείνονται σε αντικείμενα καθημερινής χρήσης που κανονικά δεν θεωρούνται υπολογιστές, επιτρέποντας στις συσκευές αυτές να παράγουν, να ανταλλάσσουν και να καταναλώνουν δεδομένα με ελάχιστη ανθρώπινη παρέμβαση, βλ. Rose, K., Eldridge, S., & Chapin, L. (2015). The internet of things: An overview. *The internet society (ISOC), 80*, σελ. 3. https://www.academia.edu/download/48790442/ISOC-IoT-Overview-20151014_0.pdf

αναγνώρισης προσώπου), με αποτέλεσμα να πληθαίνει εξίσου εκθετικά η επεμβατικότητα στην προσωπική σφαίρα των υποκειμένων.

Προσέτι, οι ανεγειρόμενοι **κίνδυνοι ασφαλείας** που δημιουργούνται από τη συλλογή και τη διατήρηση δεδομένων αναγνώρισης προσώπου, κυρίως σε ό,τι αφορά στις κρίσιμες **ανησυχίες παραβίασης και κατάχρησης** των απαντληθέντων **δεδομένων** ή/ και **χρήσης αυτών για αθέμιτους ή διάφορους των αρχικώς εγκεκριμένων σκοπούς**, έχουν επισημανθεί εκτενώς και αποτελούν καίριο ζήτημα κατά την εκτίμηση της αποτελεσματικότητας του υφιστάμενου νομοθετικού πλαισίου στη χαλιναγώγηση της τεχνολογίας αναγνώρισης προσώπου.

Επιπροσθέτως, οι ανησυχίες επικεντρώνονται συχνά στο **μεγάλο βαθμό δυσκολίας διασφάλισης της απαιτούμενης ρητής συγκατάθεσης** των υποκειμένων κατά τη συλλογή των βιομετρικών τους δεδομένων, **ιδιαίτερα όταν τα συστήματα αναγνώρισης προσώπου χρησιμοποιούνται σε δημόσιους χώρους** για σκοπούς «δημόσιας ασφάλειας» και «ελέγχου των συνόρων». Σε αυτές τις περιπτώσεις, η γνωστοποίηση της χρήσης της τεχνολογίας στα φυσικά πρόσωπα είναι δυσχερής και εκ των πραγμάτων σπάνια, ενώ πολλές φορές μπορεί να αποτελέσει εμπόδιο στην επίτευξη του ίδιου του σκοπού χρήσης της τεχνολογίας. Παραλλήλως, οι **νέες ανακύπτουσες μέθοδοι συλλογής δεδομένων, όπως η ιστοσυγκομιδή**, επιτρέπουν τη συλλογή ασύλληπτου όγκου δεδομένων για την λυσιτελή εκπαίδευση ενός αλγορίθμου αναγνώρισης προσώπου, με **ασύγκριτη ταχύτητα και το λιγότερο δυνατό κόστος, δίχως να είναι απαραίτητη οποιαδήποτε σύμπραξη των υποκειμένων** προκειμένου να καταστεί τεχνικά δυνατή η διαδικασία. Τεχνολογικές εξελίξεις όπως η εν λόγω πρακτική, είχαν ως αποτέλεσμα **μεγάλη μερίδα ακόμη και των ερευνητών της τεχνολογίας να εγκαταλείψει κάθε προσπάθεια συναινετικής συλλογής των εικόνων προσώπου**[75].

Όπως καθίσταται ήδη εμφανές, η τεχνολογία αναγνώρισης προσώπου που ενσωματώνει εφαρμογές τεχνητής νοημοσύνης, **ναρκοθετεί θεμελιώδεις αρχές του δικαίου των προσωπικών δεδομένων**, μεταξύ των οποίων η αρχή της διαφάνειας, η αρχή της λογοδοσίας, η αρχή περιορισμού του σκοπού της επεξεργασίας, η ελαχιστοποίηση των δεδομένων και η απαγόρευση ατομικής λήψης αποφάσεων και κατάρτισης προφίλ βάσει αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Παραλλήλως, **νευραλγικά δικαιώματα του υποκειμένου των δεδομένων** προσωπικού χαρακτήρα, όπως τα δικαιώματα ενημέρωσης, εναντίωσης, διόρθωσης, διαγραφής και περιορισμού της

[75] Hao, K. (2021), ο.π.

επεξεργασίας, **βρίσκονται μετέωρα**.

Συνεπώς, η άκρατη και ανέλεγκτη σαρωτική εξέλιξη της βιομηχανίας τεχνολογιών αναγνώρισης προσώπου και η εκθετική επικράτησή της στο δημόσιο forum, ανεγείρουν ευλόγως **μια σειρά από μεγάλης ηθικής απαξίας και αδιευκρίνιστα νομικά ερωτήματα**:

- Θα μπορούσε άραγε να υπάρξει πράγματι έγκυρη νομική βάση για την εφαρμογή μιας τέτοιας τεχνολογίας, δεδομένου ότι βασίζεται στην επεξεργασία ευαίσθητων δεδομένων σε τόσο μεγάλη κλίμακα;

- Μπορεί να επιτευχθεί η παροχή ρητής συγκατάθεσης, που δίδεται ελεύθερα, είναι ενημερωμένη και συγκεκριμένη, όταν η τεχνολογία χρησιμοποιείται στη δημόσια σφαίρα και ως εκ τούτου το άτομο δεν μπορεί να εκφράσει την συγκατάθεσή του, πόσω μάλλον να την αποσύρει ή να προβεί σε άρνηση;

- Είναι δυνατό να πληρούται η υποχρέωση λογοδοσίας ή/ και διαφάνειας, όταν κατ' ουσίαν δεν είναι γνωστό πώς ακριβώς χρησιμοποιούνται τα δεδομένα που συλλέγονται, ποιος έχει πρόσβαση σε αυτά, πόσο καιρό διατηρούνται, πώς διαμορφώνεται ένα προφίλ και ποιος φέρει την ευθύνη κατόπιν μίας αυτοματοποιημένης λήψης αποφάσεως του λογισμικού;

- Είναι συμβατή η τεχνολογία αναγνώρισης προσώπου με την αποτελεσματική ενάσκηση των δικαιωμάτων των υποκειμένων των δεδομένων; Είναι δυνατή η συμμόρφωση των υπευθύνων επεξεργασίας με υποχρεώσεις όπως λ.χ. η ακρίβεια, η προστασία δεδομένων κατά τον σχεδιασμό και η γνωστοποίηση παραβιάσεων;

- Είναι δυνατή η εξασφάλιση της απαιτούμενης υψηλότερης προστασίας των προσωπικών δεδομένων των παιδιών;

Προκειμένου να καταστεί δυνατή η προσέγγιση των ανωτέρω προβληματικών, θα ακολουθήσει στο αμέσως επόμενο κεφάλαιο μια αναλυτική παρουσίαση των προαπαιτούμενων που θέτει το ενωσιακό ρυθμιστικό πλαίσιο στην τεχνολογία αναγνώρισης προσώπου, ούτως ώστε αφενός να αναδειχθεί η έκταση της επέμβασης στο δικαίωμα προστασίας των δεδομένων προσωπικού χαρακτήρα, αφετέρου να αποτιμηθεί η αποτελεσματικότητα του νομοθετικού πλαισίου και η συμβατότητα της τεχνολογίας με αυτό.

2.2.4 Οι αντιδράσεις

Η εκτεταμένη και αδιάκριτη χρήση τεχνολογιών αναγνώρισης προσώπου στο δημόσιο forum αποκάλυψε σύντομα τη βασιμότητα των εγειρόμενων ανησυχιών και οδήγησε στην εκδήλωση ηχηρών παγκόσμιων εκστρατειών που απαιτούν την άνευ εξαιρέσεων απαγόρευση της τεχνολογίας. Αυτή είναι και η θέση του Ευρωπαίου Επόπτη Προστασίας Δεδομένων, του Συμβουλίου της Ευρώπης και ενός μεγάλου συνασπισμού ΜΚΟ που έχουν συγκεντρωθεί υπό την ομπρέλα του Ευρωπαϊκού Οργανισμού Ψηφιακών Δικαιωμάτων (EDRi).

Ήδη, στις Η.Π.Α. οι πόλεις Όκλαντ, Μπέρκλεϊ και Σαν Φρανσίσκο στην Καλιφόρνια, καθώς και οι Μπρούκλαϊν, Κέιμπριτζ, Νορθάμπτον και Σόμερβιλ στη Μασαχουσέτη, υιοθέτησαν απαγορεύσεις της τεχνολογίας, ενώ η Καλιφόρνια, το Νιου Χάμσαϊρ και το Όρεγκον έχουν θεσπίσει νομοθεσία που απαγορεύει τη χρήση της αναγνώρισης προσώπου με κάμερες σώματος της αστυνομίας[76].

Παραλλήλως, ακτιβιστές και ερευνητές ομοίως, αναζητούν προσωρινές λύσεις όπως η χρήση μασκών ή ενδυμάτων προκειμένου να «ξεγελάσουν» τους αλγορίθμους αναγνώρισης προσώπου, ενώ πολύ δημοφιλή έχουν αποδειχθεί και λογισμικά «δηλητηρίασης δεδομένων»[77], όπως το περιβόητο για την αποτελεσματικότητά του Fawkes[78], τα οποία επιτρέπουν στους χρήστες τους να αλλοιώσουν (ανεπαίσθητα) τις εικόνες που δημοσιεύουν στο διαδίκτυο, έτσι ώστε τα αλγοριθμικά μοντέλα να ταξινομούν λανθασμένα τις μελλοντικές εικόνες προσώπου τους.

Στον απόηχο της κατακραυγής, ορισμένες εταιρείες αποφάσισαν να αποσυρθούν από την αγορά της τεχνολογίας αναγνώρισης προσώπου. Η **Axon**, κορυφαίος προμηθευτής αστυνομικών καμερών στις Η.Π.Α., αποφάσισε **να μην εκμεταλλευτεί εμπορικά την τεχνολογία**, ενώ η **Meta** (πρώην Facebook), παρότι ήταν η εταιρεία που έφερε την επανάσταση στην ανάπτυξη της τεχνολογίας με το σύστημα Deepface, κατόπιν μιας σειράς παχυλών προστίμων, **αποφάσισε να αποσύρει** το σύστημα αναγνώρισης προσώπου της και να διαγράψει «*περισσότερα από ένα δισεκατομμύριο βιομετρικά υποδείγματα αναγνώρισης προσώπου*»[79]. Επιπλέον, **εταιρείες όπως η Amazon και η Microsoft και**

---

[76] Kerry, C.F. (2020) 'Protecting privacy in an AI-driven world', *Brookings*. Διαθέσιμο στο: https://www.brookings.edu/research/protecting-privacy-in-an-ai-driven-world/.

[77] Thales Group (2021) 'Biometrics (facts, use cases, biometric security)'. Διαθέσιμο στο: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics

[78] Shan, S. *κ.ά.* (2020) 'Fawkes: Protecting privacy against unauthorized deep learning models', *Proceedings of the 29th USENIX Security Symposium*, σελ. 1589–1604.

[79] Η Facebook αναγκάστηκε να πληρώσει **650 εκατομμύρια** δολάρια για την παραβίαση του νόμου περί βιομετρικών πληροφοριών του Ιλινόις (BIPA), βλ. Panahov, H. (2022) 'Why

ανακοίνωσαν moratorium, ήτοι ότι θα παύσουν να προμηθεύουν για ένα χρονικό διάστημα στις αρχές επιβολής του νόμου την τεχνολογία αναγνώρισης προσώπου, ενώ **η IBM αποσύρθηκε από τη βιομηχανία**. Επισημαίνεται, ωστόσο, ότι **οι χειρονομίες είναι σε μεγάλο βαθμό συμβολικές**, δεδομένου ότι οι εν λόγω εταιρείες, αν και πολύ πιο γνώριμες στο μέσο άνθρωπο, δεν είναι οι κυρίαρχες στον κλάδο· εταιρείες άσημες για το κοινό όπως οι **Ayonix, SenseTime, Cognitec, iOmniscient, Kairos, ακόμα και η Clearview AI, δρουν κρυφίως και αναπτύσσουν τη δραστηριότητά τους εκθετικά εν απουσία ρυθμιστικού πλαισίου ικανού να τις περιορίσει ουσιωδώς**[80].

Ειδικότερα ως προς την Clearview, κατόπιν της αποκάλυψης της δράσης της, εταιρείες όπως οι Twitter, Google και Meta, της απαγόρευσαν τη **συλλογή των δημόσιων πληροφοριών των χρηστών τους**, ενώ **κινήθηκαν εισαγγελικές έρευνες** σε χώρες **διεθνώς**, συμπεριλαμβανομένων των ΗΠΑ, Καναδά, Αυστραλίας, Γερμανίας, του Ηνωμένου Βασιλείου και της Ελλάδας. Τον Νοέμβριο του 2021, η κυβέρνηση του Ηνωμένου Βασιλείου επέβαλε πρόστιμο ύψους 23 εκατομμυρίων δολαρίων στην Clearview, για παραβίαση της εθνικής νομοθεσίας τους για την προστασία των προσωπικών δεδομένων. Ήδη, η εταιρεία έχει παύσει την παροχή των υπηρεσιών της στην πολιτεία του Ιλινόις και της Καλιφόρνια, αλλά και στον Καναδά λόγω πρόσκρουσης με τη νομοθεσία.

Παραλλήλως, μία συμμαχία οργανώσεων, μεταξύ των οποίων και η ελληνική **Homo Digitalis,** υπέβαλαν καταγγελίες κατά της Clearview ενώπιον των αρμόδιων αρχών προστασίας δεδομένων προσωπικού χαρακτήρα (ΑΠΔΠΧ). Ήδη, πολλές από τις καταγγελίες έχουν ευοδωθεί, με τις **ΑΠΔΠΧ στην Ιταλία και στην Ελλάδα[81] να επιβάλουν ιδιαιτέρως υψηλά πρόστιμα στην εταιρεία**, επιτάσσοντας παράλληλα τη **διαγραφή των δεδομένων των κατοίκων τους**.

Σε θεσμικό επίπεδο, φορείς όπως το **Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο της Ευρώπης**, έχουν υπογραμμίσει ότι τα συστήματα εξ αποστάσεως βιομετρικής ταυτοποίησης ενέχουν σωρεία αγνώστων κινδύνων και επομένως πρέπει **να ανασταλούν**. Στις 20 Ιανουαρίου 2021, το Ευρωπαϊκό Κοινοβούλιο

---

the US Needs Federal Law on Facial Recognition Technology', Intersect, 15(2), σελ. 4, καθώς και **πέντε δισεκατομμύρια δολάρια** για να διευθετήσει τις κατηγορίες της Ομοσπονδιακής Επιτροπής Εμπορίου ότι η εταιρεία παραβίασε εντολή της, εξαπατώντας τους χρήστες σχετικά με τη δυνατότητά τους να ελέγχουν το απόρρητο της των προσωπικών τους πληροφοριών, βλ. Bu, Q. (2021) 'The global governance on automated facial recognition (AFR): ethical and legal opportunities and privacy challenges', *International Cybersecurity Law Review*, 2(1), σελ. 127.

[80] Panahov, H. (2022) ο.π., σελ. 4.

[81] Η ελληνική και η ιταλική ΑΠΔΠΧ επέβαλαν έκαστη **πρόστιμο- ρεκόρ 20 εκατομμυρίων ευρώ**. Ομοίως, και η αρμόδια αρχή του Ηνωμένου Βασιλείου (ICO) επέβαλε πρόστιμο £7.5 εκατομμυρίων.

ενέκρινε ψήφισμα[82], με το οποίο καλεί την Ευρωπαϊκή Επιτροπή να εξετάσει το ενδεχόμενο μορατόριουμ για τη χρήση συστημάτων αναγνώρισης προσώπου. Επιπλέον, σε ψήφισμα που εγκρίθηκε με συντριπτική πλειοψηφία, οι ευρωβουλευτές ζήτησαν επίσης την απαγόρευση των ιδιωτικών βάσεων δεδομένων αναγνώρισης προσώπου, όπως αυτές που χρησιμοποιεί η Clearview AI[83]. Ομοίως, το 2021, το Συμβούλιο της Ευρώπης εξέδωσε κατευθυντήριες γραμμές για την αναγνώριση προσώπου, οι οποίες ζητούν μορατόριουμ για τις τεχνολογίες αναγνώρισης προσώπου σε ζωντανή σύνδεση και θέτουν ορισμένες προϋποθέσεις για τη χρήση τεχνολογιών αναγνώρισης προσώπου από τις αρχές επιβολής του νόμου.

Ωστόσο, οφείλει να επισημανθεί ότι υπάρχουν φορείς, όπως το Ευρωπαϊκό Συμβούλιο και η Ευρωπαϊκή Επιτροπή, οι οποίοι έχουν ταχθεί υπέρ μιας προσεκτικής και ρυθμιζόμενης ανάπτυξης των συστημάτων αναγνώρισης προσώπου, στο πλαίσιο της ευρύτερης στρατηγικής της Ε.Ε. για την Τεχνητή Νοημοσύνη. Ένας **μεγάλος αριθμός τεχνολογικών εταιρειών ελπίζει ότι αυτή η θέση θα επικρατήσει και πολλές εξ αυτών είναι πρόθυμες να δεσμευτούν ως προς τα ηθικά και νομικά προαπαιτούμενα** προκειμένου να εξασφαλιστεί η συνέχιση της δραστηριότητάς τους[84].

---

[82] Βλ. Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 20ής Ιανουαρίου 2021 σχετικά με την τεχνητή νοημοσύνη: ζητήματα ερμηνείας και εφαρμογής του διεθνούς δικαίου στον βαθμό που η Ένωση επηρεάζεται στους τομείς που αφορούν στρατιωτική και μη στρατιωτική χρήση της και ζητήματα κρατικής εξουσίας εκτός του πεδίου εφαρμογής της ποινικής δικαιοσύνης (2020/2013(INI)), στοιχείο 56. Διαθέσιμο στο: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0009_EL.html

[83] Βλ. Ευρωπαϊκό Κοινοβούλιο-Επιτροπή Πολιτικών Ελευθεριών, Δικαιοσύνης και Εσωτερικών Υποθέσεων (2021) ‘Έκθεση σχετικά με την τεχνητή νοημοσύνη στο ποινικό δίκαιο και τη χρήση της από τις αστυνομικές και δικαστικές αρχές σε ποινικές υποθέσεις (2020/2016(INI))’, Διαθέσιμο στο: https://www.europarl.europa.eu/doceo/document/A-9-2021-0232_EN.pdf

[84] Samsel, H. (2019) *California Becomes Third State to Ban Facial Recognition Software in Police Body Cameras, Security Today*. Διαθέσιμο στο: https://securitytoday.com/articles/2019/10/10/california-to-become-third-state-to-ban-facial-recognition-software-in-police-body-cameras.aspx

3. Η προστασία των δεδομένων προσωπικού χαρακτήρα απέναντι στα συστήματα αναγνώρισης προσώπου: το ισχύον νομικό πλαίσιο

Στο πλαίσιο της έννομης τάξης της Ευρωπαϊκής Ένωσης, οι κανόνες δικαίου που κατοχυρώνουν τα δικαιώματα στην προστασία των δεδομένων προσωπικού χαρακτήρα και στον σεβασμό της ιδιωτικής και οικογενειακής ζωής, καθώς και δυνητικά το σχέδιο πρότασης Κανονισμού για την Τεχνητή Νοημοσύνη, θέτουν ένα γενικό νομοθετικό πλαίσιο για τα συστήματα αλγοριθμικής αναγνώρισης προσώπου, καθορίζοντας τις κρίσιμες παραμέτρους για την ανάπτυξη και τη χρήση τους τόσο στο δημόσιο, όσο και στον ιδιωτικό τομέα.

Οι σχετικοί κανόνες δικαίου κατανέμονται σε δύο άρρηκτα συνδεδεμένα επίπεδα της ενωσιακής έννομης τάξης. Πιο συγκεκριμένα, τα εν θέματι θεμελιώδη δικαιώματα κατοχυρώνονται **σε πρωτογενές επίπεδο στο Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης**, ο οποίος, μολονότι κατ' αρχήν απευθύνεται «*στα θεσμικά όργανα της Ε.Ε. και στα κράτη μέλη κατά την εφαρμογή του δικαίου της Ένωσης*» (άρθρο 51§1), μπορεί επίσης να επηρεάσει και τις σχέσεις μεταξύ ιδιωτών (τριτενέργεια). Σε δευτερογενές επίπεδο, **το παράγωγο δίκαιο της ένωσης**, ήτοι 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 και την κατάργηση της οδηγίας 95/46/ΕΚ* (Γενικός Κανονισμός για την Προστασία Δεδομένων, στο εξής: **ΓΚΠΔ**), και η **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* (στο εξής: **η Οδηγία**), θέτουν σε ισχύ τα θεμελιώδη αυτά δικαιώματα, όπως προβλέπονται και οριοθετούνται στον Χάρτη, και **καθορίζουν ένα αυστηρό και περισσότερο λεπτομερειακό πλαίσιο για την κατασκευή και την ανάπτυξη της τεχνολογίας αναγνώρισης προσώπου**. Σε αυτό το πολυεπίπεδο νομοθετικό πλαίσιο, η δευτερογενής νομοθεσία και η εφαρμογή της στην αλγοριθμική αναγνώριση προσώπου, πρέπει πάντοτε να συνάδει με το πρωτογενές δίκαιο της Ε.Ε.

3.1 Το πρωτογενές δίκαιο της ένωσης

Κατ' αρχάς, οφείλει να επισημανθεί ότι το δικαίωμα στον σεβασμό της ιδιωτικής και οικογενειακής ζωής (άρθρο 7 Χάρτη & 8 ΕΣΔΑ) και το δικαίωμα στην

προστασία των δεδομένων προσωπικού χαρακτήρα (άρθρο 8 Χάρτη), είναι στενά συνυφασμένα, καθώς αμφότερα αποσκοπούν στην προστασία παρόμοιων αξιών, ήτοι της αυτονομίας και της ανθρώπινης αξιοπρέπειας, παρέχοντας μια προσωπική σφαίρα στην οποία το άτομο να μπορεί να αναπτύσσει ανεμπόδιστα όλες τις πτυχές της προσωπικότητάς του, να σκέπτεται και να διαμορφώνει ελεύθερα τις απόψεις του. Αποτελούν, επομένως, ουσιαστική προϋπόθεση για την άσκηση και άλλων θεμελιωδών δικαιωμάτων, όπως η ελευθερία της έκφρασης και της πληροφόρησης (άρθρο 11 του Χάρτη) και η ελευθερία του συνέρχεσθαι και του συνεταιρίζεσθαι (άρθρο 12 του Χάρτη). Ωστόσο, πρόκειται για **δύο διακριτά και αυτοτελή δικαιώματα**[85], τα οποία διαφέρουν ως προς το περιεχόμενο και το πεδίο εφαρμογής τους· έχουν μάλιστα περιγραφεί ως το «κλασικό» δικαίωμα στην προστασία της ιδιωτικής ζωής και ένα περισσότερο «σύγχρονο» δικαίωμα, το δικαίωμα στην προστασία των προσωπικών δεδομένων.

Το **δικαίωμα στον σεβασμό της ιδιωτικής και οικογενειακής ζωής του ατόμου,** με την επιφύλαξη ορισμένων κριτηρίων δημόσιου συμφέροντος, **συνίσταται σε γενική απαγόρευση των επεμβάσεων** που αφορά σε ένα ευρύ φάσμα καταστάσεων, στις οποίες κρίνεται ότι θίγεται η ιδιωτική σφαίρα του προσώπου[86]. Η έννοια της «ιδιωτικής ζωής» είναι δυσχερώς προσδιορίσιμη· εν πολλοίς, αναφέρεται στη σωματική και ψυχολογική ακεραιότητα ενός ατόμου και εμπερικλείει πολλαπλές πτυχές της ταυτότητάς του, ακόμα και όταν εκδηλώνονται σε δημόσιο πλαίσιο. Ειδικότερα, το Ευρωπαϊκό Δικαστήριο Δικαιωμάτων του Ανθρώπου (ΕΔΔΑ) προκειμένου να αποφανθεί σχετικά με την παραβίαση του δικαιώματος, έχει χρησιμοποιήσει το κριτήριο της «*εύλογης προσδοκίας ιδιωτικής ζωής*», ούτως ώστε να καταλήξει στο βαθμό που είναι λογικό το άτομο να προσδοκά τη διαφύλαξη της ιδιωτικότητάς τους σε δημόσιους χώρους, δίχως να υπόκειται σε παρακολούθηση. Προσέτι, σύμφωνα με τους εμπειρογνώμονες του ΟΗΕ, **μόνο το γεγονός ότι οι διαδηλωτές σε**

---

[85] Το Σύνταγμα της Ελλάδας με τη σειρά του διακρίνει αυτά τα δύο δικαιώματα. Έτσι, το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα αναγνωρίζεται στο Άρθρο 9Α του Συντάγματος, ενώ οι διάφορες πτυχές του δικαιώματος στο σεβασμό της ιδιωτικής και οικογενειακής ζωής αναγνωρίζονται στο Άρθρο 9 (Άσυλο της κατοικίας), Άρθρο 19 (Απόρρητο επιστολών, ανταπόκρισης και επικοινωνίας), και Άρθρο 21 (Προστασία οικογένειας, γάμου, μητρότητας και παιδικής ηλικίας, δικαιώματα ατόμων με αναπηρίες). Το Σύνταγμα της Ελλάδας προβλέπει, επιπροσθέτως, και την ύπαρξη δυο διακριτών ανεξάρτητων διοικητικών αρχών: την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), η οποία διασφαλίζει την προστασία των προσωπικών δεδομένων και την Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία διασφαλίζει το απόρρητο των επιστολών και της ελεύθερης επικοινωνίας.

[86] European Union Agency for Fundamental Rights & Council of Europe (2018) *Handbook on European Data Protection Law*, *Publications Office of the European Union*. σελ. 21 επ. Διαθέσιμο στο: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf

συγκεντρώσεις διαμαρτυρίας βρίσκονται σε δημόσιο χώρο, δεν σημαίνει ότι απεκδύονται του δικαιώματος σεβασμού της ιδιωτικής τους ζωής. Ομοίως, η επιστημονική κοινότητα έχει επισημάνει ότι **το διαδικτυακό αποτύπωμα αποτελεί πλέον πραγματικό δεδομένο της ανθρώπινης ζωής και, ως εκ τούτου, τα άτομα εύλογα αναμένουν κάποιο επίπεδο ιδιωτικότητας και ελέγχου επί των προσωπικών πληροφοριών και εικόνων που επιλέγουν να δημοσιοποιήσουν** (δικαίωμα πληροφοριακού αυτοκαθορισμού)[87].

Η προστασία των δεδομένων προσωπικού χαρακτήρα γίνεται αντιληπτή ως ένα σύγχρονο και ενεργό δικαίωμα, που αξιώνει την καθιέρωση ενός συστήματος ελέγχων και ισορροπιών για την προστασία των προσώπων κατά την επεξεργασία των δεδομένων προσωπικού χαρακτήρα που τα αφορούν. Ειδικότερα, στο άρθρο 8 του Χάρτη όχι μόνον αναγνωρίζεται το εν λόγω δικαίωμα, αλλά επισημαίνονται επίσης οι βασικές συνιστώσες αυτού: *η επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να γίνεται* ***νομίμως, για καθορισμένους σκοπούς και με τη συγκατάθεση του ενδιαφερομένου ή για άλλους θεμιτούς λόγους που προβλέπονται από τον νόμο***. *Τα πρόσωπα πρέπει να έχουν* ***δικαίωμα πρόσβασης*** *στα δεδομένα προσωπικού χαρακτήρα που τα αφορούν, καθώς και* ***δικαίωμα διόρθωσης*** *αυτών, η δε συμμόρφωση προς το δικαίωμα αυτό πρέπει να υπόκειται στον* ***έλεγχο ανεξάρτητης αρχής***. Το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα **ενεργοποιείται κάθε φορά που πραγματοποιείται επεξεργασία τους**· επομένως, είναι **ευρύτερο** από το δικαίωμα στον σεβασμό της ιδιωτικής και οικογενειακής ζωής.

Εν προκειμένω, επισημαίνεται ότι το ΕΔΔΑ και το Δικαστήριο της Ευρωπαϊκής Ένωσης (ΔΕΕ) έχουν αμφότερα διασαφηνίσει ότι **οι εικόνες προσώπου συγκαταλέγονται στα δεδομένα προσωπικού χαρακτήρα**, **διότι η εικόνα του προσώπου ενός ατόμου αποτελεί ένα από τα πλέον ουσιώδη στοιχεία της προσωπικότητάς του**, καθώς αποκαλύπτει τα μοναδικά χαρακτηριστικά του και το διακρίνει από τους υπόλοιπους ανθρώπους. Συνεπώς, η επεξεργασία εικόνων προσώπου σε βάσεις δεδομένων μεγάλης κλίμακας μπορεί, καθώς ωριμάζει η τεχνολογία αναγνώρισης προσώπου, να εγείρει αδιευκρίνιστα ζητήματα σχετικά με τα δικαιώματα προστασίας της ιδιωτικής και οικογενειακής ζωής, όπως και των προσωπικών δεδομένων.

Ειδικότερα, αναφορικά με την **τεχνολογία αναγνώρισης προσώπου**, δεδομένου ότι αυτή συνεπάγεται, ως έχει ήδη αναλυθεί, την επεξεργασία *βιομετρικών δεδομένων* **για σκοπούς ταυτοποίησης**, η χρήση της συνιστά

---

[87] Sarabdeen, J. (2022) 'Protection of the rights of the individual when using facial recognition technology', *Heliyon*, 8(3). σελ. 3. doi:10.1016/J.HELIYON.2022.E09086.

επέμβαση σε αμφότερα τα ανωτέρω θεμελιώδη δικαιώματα. Εντούτοις, καθώς **τα εν θέματι δικαιώματα δεν είναι απόλυτα**, μπορούν να υπόκεινται σε περιορισμούς υπό την προϋπόθεση **κάθε παρέμβαση να είναι απολύτως αναγκαία και αναλογική**, κατά τα οριζόμενα στο άρθρο 52 Χάρτη, και **να μην θίγει τον ουσιώδη και αναφαίρετο πυρήνα τους**.

Πιο συγκεκριμένα, το άρθρο 52 του Χάρτη προβλέπει ότι **επιτρέπεται** ο περιορισμός στην άσκηση των δικαιωμάτων και ελευθεριών που αναγνωρίζονται σε αυτόν, εφόσον πληρούνται **οι ακόλουθες προϋποθέσεις ως προς την επέμβαση**:

- πρέπει να προβλέπεται από το νόμο,
- πρέπει να σέβεται το βασικό περιεχόμενο του δικαιώματος,
- πρέπει να ανταποκρίνεται πραγματικά σε στόχους γενικού συμφέροντος που αναγνωρίζονται από την Ένωση ή στην ανάγκη προστασίας των δικαιωμάτων και ελευθεριών των τρίτων (θεμιτός σκοπός),
- πρέπει να είναι σύμφωνη με την αρχή της αναλογικότητας.
- Επιπλέον, κάθε περιορισμός που επιβάλλεται σε δικαίωμα του Χάρτη που αντιστοιχεί σε δικαίωμα που διασφαλίζεται από την Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου (ΕΣΔΑ) πρέπει να πληροί τις προϋποθέσεις που προβλέπονται και σε αυτή.

Το ΔΕΕ διασαφήνισε ότι όλες οι ανωτέρω απαιτήσεις πρέπει να πληρούνται σωρευτικώς, καθώς και ότι πρωταρχικός είναι ο σεβασμός του πυρήνα του δικαιώματος: μόνον αφότου διαπιστωθεί ότι δεν παραβιάζεται η ουσία ενός δικαιώματος, ακολουθεί η εφαρμογή των κριτηρίων της αναγκαιότητας και της αναλογικότητας ως προς τις μη ουσιώδεις πτυχές του. Επίσης, έχει κριθεί ότι **ένας σκοπός γενικού συμφέροντος - όπως η πρόληψη της εγκληματικότητας ή η δημόσια ασφάλεια - δεν είναι άνευ ετέρου επαρκής για να δικαιολογήσει μια παρέμβαση**· η αξιολόγηση οποιουδήποτε περιορισμού ενός θεμελιώδους δικαιώματος θα πρέπει πάντοτε να εξετάζει ad hoc κατά πόσον ο συγκεκριμένος νόμιμος σκοπός δεν θα μπορούσε να επιτευχθεί με άλλα ηπιότερα μέσα που παρεμβαίνουν λιγότερο στο κατοχυρωμένο δικαίωμα.

Παρόμοιες απαιτήσεις επιβάλλονται επίσης από την ΕΣΔΑ, όπως αυτή ερμηνεύεται από το Ευρωπαϊκό Δικαστήριο Δικαιωμάτων του Ανθρώπου (ΕΔΔΑ). Το Δικαστήριο, προκειμένου να εκτιμήσει αν μία παρέμβαση σε θεμελιώδες δικαίωμα είναι επιτρεπτή, αρχικώς εξετάζει αν η κρινόμενη επέμβαση είναι σύμφωνη με το νόμο ή προβλεπόμενη στο νόμο, λαμβάνοντας υπ' όψιν κάποια ποιοτικά κριτήρια (ο νόμος στον οποίο ερείδεται ο περιορισμός θα πρέπει να είναι σαφής, προβλέψιμος και επαρκώς προσβάσιμος). Εν συνεχεία, το ΕΔΔΑ αξιολογεί αν η παρέμβαση είναι αναγκαία σε μια δημοκρατική κοινωνία (έλεγχος

αναγκαιότητας και αναλογικότητας), ήτοι αν υφίσταται πιεστική κοινωνική ανάγκη για τον υπό κρίση περιορισμό, ο οποίος θα πρέπει σε κάθε περίπτωση να είναι αναλογικός, καθώς και να εδράζεται σε λόγους συναφείς και επαρκείς. Ο απαραβίαστος πυρήνας του δικαιώματος, διατρέχει και εν προκειμένω όλη την εκτίμηση έως την τελική δικανική κρίση.

Όσον αφορά ειδικότερα στη χρήση των νέων τεχνολογιών, το ΕΔΔΑ έχει αποφανθεί ότι τα κράτη πρέπει να «βρίσκουν τη σωστή ισορροπία» μεταξύ της προστασίας των θεμελιωδών δικαιωμάτων και της ανάπτυξης νέων τεχνολογιών. Περαιτέρω, γίνεται παγίως δεκτό ότι **όσο πιο παρεμβατική είναι η τεχνολογία, τόσο πιο αυστηρή πρέπει να είναι η στάθμιση των εκατέρωθεν συμφερόντων**. Συνεπώς, **τα συστήματα αναγνώρισης προσώπου, ως τεχνολογία υπέρμετρης παρεμβατικότητας, θέτουν κάποια εύλογα ερωτήματα: υπάρχει κάποια απόδειξη ότι η τεχνολογία είναι αναγκαία; δεν υπάρχουν άλλα λιγότερο παρεμβατικά μέσα για την επίτευξη του ίδιου στόχου;**

Ως ευλόγως συνάγεται, **η αξιολόγηση πρέπει να διενεργείται ad hoc για κάθε περίπτωση χρήσης των συστημάτων αναγνώρισης προσώπου**. Άλλως, προκειμένου να είναι δυνατή η τεκμηριωμένη κρίση επί της αναγκαιότητας και της αναλογικότητας της τεχνολογίας, κάθε έλεγχος της νομιμότητας χρήσης της **θα πρέπει να λαμβάνει υπ' όψιν το σύνολο των πραγματικών περιστατικών της εκάστοτε περίπτωσης, από τον επιδιωκόμενο σκοπό** (π.χ. επαλήθευση, ταυτοποίηση, κατηγοριοποίηση) **και τον τρόπο λήψης των εικόνων προσώπου** (π.χ. κάμερες κλειστού κυκλώματος παρακολούθησης, κάμερες που ενσωματώνονται στις αστυνομικές στολές, εφαρμογές κινητών τηλεφώνων κ.ο.κ.), **έως το πλαίσιο χρήσης** (π.χ. για συνοριακό έλεγχο, στο πλαίσιο δράσης των αστυνομικών αρχών, για την πρόσβαση σε μία συσκευή) και την **πιθανότητα σφαλμάτων** του συστήματος.

Επισημαίνεται ότι όσον αφορά ειδικότερα στην **αδιάκριτη και γενικευμένη χρήση των συστημάτων βιομετρικής ταυτοποίησης σε δημόσιους χώρους από τις αρχές επιβολής του νόμου**, αμφότερα τα ανωτέρω Δικαστήρια έχουν επισημάνει εκτενώς στη νομολογία τους τις επιπτώσεις στο δικαίωμα των ατόμων στην ιδιωτική ζωή και στην προστασία των προσωπικών τους δεδομένων[88]. Το ΕΔΔΑ έχει επανειλημμένα προειδοποιήσει **ότι τα εργαλεία συγκεκαλυμμένης παρακολούθησης δεν πρέπει να χρησιμοποιούνται για την υπονόμευση της δημοκρατίας με το πρόσχημα της υπεράσπισής της** (Klass και άλλοι κατά Γερμανίας), ενώ **ιδιαίτερα σε ό,τι αφορά στη νομιμότητα της συλλογής βιομετρικών δεδομένων**, το δικαστήριο αναγνώρισε στην υπόθεση *S and Marper κατά Ηνωμένου Βασιλείου* ότι **η χρήση βιομετρικών**

[88] Ragazzi, F. *κ.ά.* (2021), ο.π. σελ. 48- 50.

δεδομένων που θα επέτρεπαν την ταυτοποίηση ενός ατόμου και τη δυνατότητα εξαγωγής «ευαίσθητων» προσωπικών δεδομένων, όπως η εθνοτική καταγωγή, **θα καθιστούσαν τα ενδιαφερόμενα άτομα ουσιωδώς ευάλωτα σε στιγματισμό και διακρίσεις**. Όπως τόνισε το ΕΔΔΑ στην εν λόγω υπόθεση, το εφαρμοστέο δίκαιο οφείλει να προβλέπει **κατάλληλα μέτρα προστασίας** για να αποτρέπει κάθε ασύμβατη με τις εγγυήσεις του Άρθρου 8 της ΕΣΔΑ επεξεργασία προσωπικών δεδομένων, **ιδιαίτερα στην περίπτωση που τα δεδομένα υπάγονται σε αυτοματοποιημένη επεξεργασία για σκοπούς αστυνόμευσης**.

Προσέτι, το ΕΔΔΑ έχει αποφανθεί ότι η **γενικευμένη και αδιάκριτη συλλογή και διατήρηση βιομετρικών δεδομένων δεν συμμορφώνεται με τις απαιτήσεις της ΕΣΔΑ**, καθώς ισοδυναμεί με **δυσανάλογη παρέμβαση στο κατ' άρθρο 8 ΕΣΔΑ προστατευόμενο δικαίωμα στην ιδιωτική ζωή.** Ομοίως, το ΔΕΕ απεφάνθη στις υποθέσεις *Digital Rights Ireland* (συνεκδικασθείσες υποθέσεις C293/12 και C594/12, σκέψη 37) καθώς και στην υπόθεση *Tele2* (C-203/15, σκέψη 100), ότι το δίκαιο της ένωσης **αποκλείει τη μαζική διατήρηση δεδομένων κίνησης και θέσης** για σκοπούς επιβολής του νόμου και ότι **μόνον η στοχευμένη διατήρηση** των εν λόγω δεδομένων θα μπορούσε να είναι επιτρεπτή.

Αναφορικά με τη **στοχευμένη βιομετρική παρακολούθηση** (ήτοι, παρακολούθηση προσώπων βάσει προηγούμενης υποψίας εμπλοκής τους σε εγκληματικές δραστηριότητες), το ΔΕΕ έχει εισαγάγει, κατ' αρχάς, ένα γεωγραφικό κριτήριο ως ικανοποιητικό περιορισμό για τη στοχευμένη διατήρηση δεδομένων κίνησης και θέσης (La Quadrature du net και άλλοι), **το οποίο ωστόσο ενδέχεται να μην επαρκεί στο πλαίσιο της χρήσης τεχνολογίας αναγνώρισης προσώπου.** Τούτο διότι από τη φύση της **η εγκατάσταση της τεχνολογίας σε ένα χώρο ισοδυναμεί με μαζική επιτήρηση όλων των υποκειμένων που βρίσκονται σε αυτόν**, δεδομένου ότι ένα σύστημα αναγνώρισης προσώπου θα παρακολουθούσε και θα ανέλυε αδιακρίτως τα υποκείμενα για να εντοπίσει άτομα που περιλαμβάνονται στη λίστα παρακολούθησης. Κατά συνέπεια, η χρήση της τεχνολογίας ακόμα και σε συγκεκριμένο χώρο για σκοπούς επιβολής του νόμου, θα μπορούσε να θεωρηθεί παρέμβαση στα δικαιώματα στην ιδιωτική ζωή και στην προστασία των προσωπικών δεδομένων.

Βεβαίως, ακόμα και όταν η εξ αποστάσεως βιομετρική παρακολούθηση πραγματοποιείται με στοχευμένο τρόπο, η νομιμότητά της εξαρτάται από το σκοπό για τον οποίο διεξάγεται, ο οποίος αξιολογείται υπό το πρίσμα των αρχών της αναλογικότητάς και αναγκαιότητάς, αλλά και **λαμβάνοντας υπόψη τον ευαίσθητο χαρακτήρα των βιομετρικών δεδομένων, ο οποίος επιτάσσει ο σκοπός να είναι ανάλογος προς το επίπεδο της παρεμβατικότητας** (κατά τα

οριζόμενα στην υπόθεση C-203/15, Tele2, σκέψη 102). Παραλλήλως, κατά τη νομολογία των υπό αναφορά Δικαστηρίων, πρέπει να υπάρχουν **κατάλληλες εγγυήσεις** ικανές να προστατεύουν τα υποκείμενα από πιθανές καταχρήσεις της τεχνολογίας, καθώς και **διαθέσιμα και αποτελεσματικά ένδικα μέσα**. Απαιτείται, επίσης, οι άδειες για στοχευμένη βιομετρική επιτήρηση να υπόκεινται σε αποτελεσματικό **έλεγχο από δικαστήριο ή ανεξάρτητο διοικητικό όργανο**, προκειμένου να διασφαλισθεί ότι τηρούνται οι προϋποθέσεις και οι εγγυήσεις του νόμου (C511/18, C512/18 και C520/18, La Quadrature du Net και άλλοι, σκέψη 179).

Επισημαίνεται, επιπροσθέτως, ότι σύμφωνα με το ΕΔΔΑ, όταν τα δεδομένα προσωπικού χαρακτήρα που συλλαμβάνονται στο δημόσιο χώρο σε πραγματικό χρόνο συνεπάγονται τη **χρήση περαιτέρω δεδομένων που το άτομο δεν μπορεί να προβλέψει, αυτή η αυτοματοποιημένη επεξεργασία σε πραγματικό χρόνο θα μπορούσε να ενεργοποιήσει το άρθρο 8 του Χάρτη στο πλαίσιο προστασίας των δεδομένων προσωπικού χαρακτήρα**, (Uzun κατά Γερμανίας, σκέψη 45). Ομοίως, **το ΔΕΕ έχει αποφανθεί** (υπόθεση La Quadrature du Net και λοιποί C511/18, C512/18 και C520/18) **ότι η αυτοματοποιημένη ανάλυση δεδομένων προσωπικού χαρακτήρα ισοδυναμεί με επέμβαση στο δικαίωμα προστασίας των δεδομένων προσωπικού χαρακτήρα, όπως ορίζεται στο άρθρο 8 του Χάρτη, ακόμη και αν αρχικά δεν συνεπάγετο τη συλλογή των δεδομένων**.

Εκ των ανωτέρω προκύπτει σαφώς ότι, στην πράξη, **τα εν λόγω κατοχυρωμένα στο Χάρτη θεμελιώδη δικαιώματα εξακολουθούν να διαμορφώνονται** και η **τριτενέργειά τους**, ήτοι η έκταση της εφαρμογής τους σε αμιγώς ιδιωτικές διαφορές, **δεν έχει ακόμη αποκρυσταλλωθεί**. **Από μόνα τους, κατά γενική ομολογία, δεν καθίστανται ικανά να παράσχουν αποτελεσματική καθοδήγηση για τη χρήση των συστημάτων αναγνώρισης προσώπου**, ενώ συχνά επιλύουν μόνο εμμέσως τις συγκρούσεις ανάμεσα στην ανάγκη προστασίας των δεδομένων προσωπικού χαρακτήρα και στην ανάπτυξη των αναδυόμενων τεχνολογιών[89]. Σε αυτό το χρονικό σημείο, **το παράγωγο δίκαιο της ένωσης αποτελεί το μοναδικό λειτουργικό πλαίσιο προστασίας απέναντι στην επεμβατικότητα της αλγοριθμικής αναγνώρισης προσώπου**: τόσο ο **Κανονισμός (ΕΕ) 2016/679** (**ΓΚΠΔ**), όσο και η **Οδηγία (ΕΕ) 2016/680** συναπαρτίζουν ουσιώδες μέρος του κεκτημένου της Ε.Ε. για την προστασία των δεδομένων προσωπικού χαρακτήρα και **θέτουν ένα αυστηρό πλαίσιο για την επεξεργασία των εικόνων προσώπου για σκοπούς βιομετρικής ταυτοποίησης**.

[89] Madiega, T., Mildebrath, H. (2021), ο.π. σελ. 9-11.

3.2 Το παράγωγο δίκαιο της Ε.Ε.: ο Γενικός Κανονισμός Προστασίας Δεδομένων & η Οδηγία (ΕΕ) 2016/680

Η συλλογή και επεξεργασία εικόνων προσώπων από τα συστήματα αναγνώρισης προσώπου με σκοπό την ταυτοποίηση των υποκειμένων τους, συνιστά, ως αναλύθηκε στο πρώτο κεφάλαιο της παρούσας, **επεξεργασία βιομετρικών δεδομένων** και, ως εκ τούτου, οφείλει να είναι **απολύτως σύμφωνη με τα οριζόμενα στην ενωσιακή νομοθεσία για την προστασία των δεδομένων προσωπικού χαρακτήρα, όπως και με τις βασικές νομικές αρχές που τη διέπουν στο σύνολό της**. Ergo, οποιαδήποτε επεξεργασία εικόνων προσώπου από τους αλγόριθμους αναγνώρισης προσώπου, προκειμένου να **είναι σύμφωνη και συμβατή με τις βασικές νομικές αρχές που διατρέχουν όλη τη νομοθεσία περί προστασίας των δεδομένων προσωπικού χαρακτήρα** (άρθρο 5 ΓΚΠΔ & άρθρο 4 Οδηγίας), οφείλει:

- να είναι **νόμιμη, αντικειμενική και διαφανής,**
- να διεξάγεται για **καθορισμένο, ρητό και νόμιμο σκοπό,** σαφώς καθορισμένο στο δίκαιο του κράτους μέλους ή της Ένωσης,
- να συμμορφώνεται, μεταξύ άλλων, με τις **αρχές της ελαχιστοποίησης, της ακρίβειας, του περιορισμού της περιόδου αποθήκευσης, της ακεραιότητας και εμπιστευτικότητας, όπως και με την υποχρέωση λογοδοσίας**.

Παραλλήλως, οι **υπεύθυνοι επεξεργασίας δεδομένων** (και εμμέσως, οι κατασκευαστές των συστημάτων αναγνώρισης προσώπου) θα πρέπει να σχεδιάζουν τις προβλεπόμενες δραστηριότητες επεξεργασίας δεδομένων από τα συστήματα αναγνώρισης προσώπου, με πλήρη **σεβασμό των αρχών προστασίας δεδομένων** («προστασία δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού», άρθρο 25 ΓΚΠΔ και άρθρο 20 Οδηγίας).

Εν προκειμένω, οφείλει να επισημανθεί ότι, **ούτως ώστε να υπάγεται η τεχνολογία αναγνώρισης προσώπου** στην αυξημένη προστασία που επιφυλάσσει ο ενωσιακός νομοθέτης **στην επεξεργασία των ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα,** και ειδικότερα των βιομετρικών δεδομένων, **θα πρέπει το σύστημα αλγοριθμικής αναγνώρισης** να συλλέγει, να επεξεργάζεται και να διατηρεί δεδομένα απαντληθέντα εκ της

εικόνας **ταυτοποιήσιμων**[90] **φυσικών προσώπων,** ήτοι προσώπων που καθίσταται δυνατό να ταυτοποιηθούν επί τη βάσει της γεωμετρίας του προσώπου τους, **ακριβώς με σκοπό την ταυτοποίηση τους**.

Η εν λόγω επισήμανση είναι σημαντική για τον προσδιορισμό των νομικών εφαρμοστέων κανόνων, διότι όπως προεκτέθηκε στο πρώτο κεφάλαιο της παρούσας, **η τεχνολογία αναγνώρισης προσώπου δύναται να χρησιμοποιηθεί για πληθώρα σκοπών πέραν της υπό κρίση εξεταζόμενης βιομετρικής ταυτοποίησης**, όπως η απλή ανίχνευση προσώπου (διαπίστωση της παρουσίας ανθρώπινου προσώπου σε ένα χώρο), η επαλήθευση (μονοσήμαντη αντιστοίχιση), ή η κατηγοριοποίηση (ταξινόμηση των ανιχνευθέντων προσώπων σε μια συγκεκριμένη κατηγορία). Ορισμένες από αυτές τις πρακτικές, όπως η χρήση της τεχνολογίας για την ανίχνευση προσώπου, περιλαμβάνουν μεν την επεξεργασία δεδομένων προσωπικού χαρακτήρα, δίχως όμως η επεξεργασία να εμπερικλείει βιομετρικά δεδομένα, διότι **σε αυτές τις περιπτώσεις ελλείπει ο σκοπός αδιαμφισβήτητης ταυτοποίησης ή επαλήθευσης της ταυτότητας του υποκειμένου των δεδομένων (βιομετρική ταυτοποίηση)**[91]. Ομοίως, αναφορικά με την περίπτωση χρήσης της τεχνολογίας για σκοπούς κατηγοριοποίησης, σύμφωνα με το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ)[92], εφόσον το σύστημα δε δημιουργεί βιομετρικά πρότυπα με σκοπό την αδιαμφισβήτητη ταυτοποίηση ενός ατόμου, αλλά απλώς εντοπίζει τα φυσικά χαρακτηριστικά του προκειμένου να το ταξινομήσει σε κάποια κατηγορία (λ.χ. βάσει φύλου), τότε η επεξεργασία δεν αφορά σε βιομετρικά δεδομένα.

Η κρισιμότητα της διάκρισης καθίσταται περαιτέρω αντιληπτή από το γεγονός πως πράγματι **έχει αναδειχθεί ένα ολόκληρο φάσμα πρακτικών στο πλαίσιο χρήσης των συστημάτων αναγνώρισης προσώπου**, το οποίο έχει προκαλέσει **έντονους προβληματισμούς** σχετικά με τον τρόπο με τον οποίο μπορεί να διασφαλιστεί ότι η επεξεργασία των δεδομένων προσωπικού

---

[90] Βλ. αρ. 4 στοιχ. 1 του ΓΚΠΔ όπου ορίζεται ως δεδομένο προσωπικού χαρακτήρα *κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου.*

[91] Gonzalez Fuster, G & Nadolna Peeters, M.A. (2021), ο.π. 15-16.

[92] Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (2020) 'Κατευθυντήριες γραμμές 3/2019 σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω βιντεοσυσκευών'. σελ. 20-23. Διαθέσιμο στο: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_el.pdf

χαρακτήρα αναγνωρίζεται νομικά ως τέτοια- **ιδίως όταν οι φορείς επεξεργασίας δεδομένων ισχυρίζονται ότι τα συστήματα δεν αποσκοπούν στην ταυτοποίηση φυσικών προσώπων, ή ότι τα άτομα που παρακολουθούνται δεν μπορούν να ταυτοποιηθούν**. Χαρακτηριστικό παράδειγμα της προβληματικής αποτελούν οι προαναφερθείσες «έξυπνες» πινακίδες ψηφιακής διαφήμισης (βλ. 1.4.1). Η εν λόγω εμπορική πρακτική έχει εγείρει αντιδράσεις και το ΕΣΠΔ έχει επισημάνει τη δυνατότητα των διαφημιστικών πινακίδων να «θυμούνται» τους πελάτες, καταγράφοντας και αποθηκεύοντας τα βιομετρικά τους δεδομένα, παρά τον ισχυρισμό όσων χρησιμοποιούν αυτού του είδους τη διαφήμιση ότι δεν αποσκοπούν σε ταυτοποίηση των διερχόμενων πελατών τους και ότι σε κάθε περίπτωση τα διερχόμενα άτομα δεν μπορούν να ταυτοποιηθούν, με αποτέλεσμα η επεξεργασία στην οποία προβαίνουν να μην συμπεριλαμβάνει προσωπικά –πολλώ δε μάλλον βιομετρικά- δεδομένα. Μάλιστα, το 2017, **η ιταλική αρχή προστασίας δεδομένων διερεύνησε την εγκατάσταση μίας έξυπνης διαφημιστικής πινακίδας** σε κεντρικό σταθμό στο Μιλάνο, καταλήγοντας στο συμπέρασμα ότι οι συσκευές της εταιρείας επεξεργάζονταν εφήμερα μόνο εικόνες των περαστικών, **όχι με σκοπό να αποκτήσουν κάποιο βιομετρικό πρότυπο του προσώπου τους ή να τους αναγνωρίσουν, αλλά προκειμένου να προσδιορίσουν την παρουσία ενός ανθρώπινου προσώπου σε μια συγκεκριμένη περιοχή, να υπολογίσουν τη διάρκεια αυτής της παρουσίας, να συμπεράνουν πληροφορίες όπως το φύλο και το εύρος ηλικίας και να πραγματοποιήσουν στατιστική ανάλυση για να αξιολογήσουν το επίπεδο αποδοχής των διαφημιστικών μηνυμάτων.** Συμπερασματικά, **η αρχή κατέληξε στο συμπέρασμα ότι οι συσκευές πραγματοποιούσαν «*ανίχνευση προσώπου*» αλλά όχι «*αναγνώριση προσώπου*»,** με αποτέλεσμα η επεξεργασία να αφορά μεν σε δεδομένα προσωπικού χαρακτήρα, χωρίς όμως αυτά να συγκαταλέγονται στις ειδικές κατηγορίες δεδομένων[93].

Επισημαίνεται επιπροσθέτως, ότι τα συστήματα αναγνώρισης προσώπου με χρήση εφαρμογών τεχνητής νοημοσύνης εγείρουν ορισμένες περαιτέρω προκλήσεις ως προς το περιεχόμενο της έννοιας των «ταυτοποιήσιμων» φυσικών προσώπων. Η προβληματική εντοπίζεται κυρίως στη δυνατότητα των εφαρμογών ΤΝ να επαναπροσδιορίζουν και να επανασυνδέουν κατ' αρχήν *μη ταυτοποιήσιμα δεδομένα*, με το υποκείμενο στο οποίο ανήκουν. Συνέπεια αυτής της δυνατότητας, αποτελεί η επεξεργασία των προσωπικών δεδομένων των υποκειμένων σε ένα πλαίσιο πλήρους αδιαφάνειας, το οποίο εκθέτει τα άτομα σε κάθε λογής προσβολή των θεμελιωδών δικαιωμάτων και ελευθεριών τους, αποστερώντας

---

[93] European Parliament (2021) *Person identification, human rights and ethical principles. Rethinking biometrics in the era of artificial intelligence., EPRS European Parliamentary Research Service*. Διαθέσιμο στο: http://www.europarl.europa.eu/thinktank σελ. 15-16.

τους περαιτέρω τη δυνατότητα άσκησης των δικαιωμάτων τους λόγω της άγνοιας της επεξεργασίας των –προσωπικών πλέον και πιθανώς ευαίσθητων- δεδομένων τους.

3.2.1 Η νομιμότητα της επεξεργασίας των βιομετρικών εικόνων προσώπου

Η **αρχή της νομιμότητας** αποτελεί πεμπτουσία του δικαίου προστασίας των δεδομένων προσωπικού χαρακτήρα και εξασφαλίζει ότι τα προσωπικά δεδομένα –ευαίσθητα ή μη- των υποκειμένων υποβάλλονται πάντοτε σε θεμιτή, σύννομη και δίκαιη επεξεργασία. Η κατοχύρωσή της είναι ρητή και προβλέπεται στα άρθρα 4§1 της Οδηγίας και στο άρθρο 5§1 στοιχείο α' του ΓΚΠΔ, στο πλαίσιο του οποίου αποτελεί συστατικό της αρχής της *νομιμότητας, αντικειμενικότητας και διαφάνειας* της επεξεργασίας προσωπικών δεδομένων, ενώ διέπει το σύνολο των διατάξεων αμφότερων των νομοθετημάτων.

Ειδικότερα ως προς τη νομιμότητα της επεξεργασίας των εικόνων προσώπου από τους αλγορίθμους αναγνώρισης προσώπου, οφείλει να διασαφηνισθεί ότι το ενωσιακό νομικό πλαίσιο, κατ' αρχήν, **απαγορεύει την επεξεργασία βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση ενός προσώπου[94].**

Εξετάζοντας κατ' αρχάς τον ΓΚΠΔ, προκειμένου να είναι νόμιμη η επεξεργασία των «απλών» προσωπικών δεδομένων, αρκεί να συντρέχει μία από τις νομικές βάσεις του άρθρου 6 του Κανονισμού. Όσον αφορά όμως ειδικότερα στις ειδικές κατηγορίες δεδομένων, οι οποίες, όπως γίνεται δεκτό στο πλαίσιο του Κανονισμού, χρήζουν ιδιαίτερης προστασίας λόγω των επαπειλούμενων επιπτώσεων στα θεμελιώδη ανθρώπινα δικαιώματα, η επεξεργασία τους κατ' αρχήν απαγορεύεται και **επιτρέπεται μόνον εάν συντρέχει σωρευτικά αφενός κάποια από τις νομικές βάσεις του άρθρου 6, και αφετέρου κάποια από τις**

---

[94] Βλ. άρθρο **9§1 ΓΚΠΔ** «*Απαγορεύεται η επεξεργασία 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 η επεξεργασία 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.*», άρθρο **10 της Οδηγίας** «*Η επεξεργασία 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 η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων για την αποκλειστική ταυτοποίηση ενός φυσικού προσώπου ή δεδομένων που αφορούν στην υγεία ή τη σεξουαλική ζωή ή τον σεξουαλικό προσανατολισμό επιτρέπονται μόνο* […]». Ομοίως **και στο άρθρο 10§1 του Κανονισμού (ΕΕ) 2018/1725.**

εξαιρέσεις του άρθρου 9§2 ΓΚΠΔ.

Η ανωτέρω άποψη περί υποχρεωτικής σώρευσης ενός εκ των απαιτούμενων νομικών βάσεων του άρθρου 6 και ενός εκ των προβλεπόμενων εξαιρέσεων του άρθρου 9§2 ΓΚΠΔ, προκειμένου η επεξεργασία των ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα να μπορεί να θεωρηθεί επιτρεπτή και σύννομη, υιοθετείται τόσο από την «Ομάδα Εργασίας του άρθρου 29 για την προστασία δεδομένων» στη Γνώμη 6/2014 *σχετικά με την έννοια των εννόμων συμφερόντων του υπευθύνου επεξεργασίας κατ' άρθρον 7 της Οδηγίας 95/46/ΕΚ*[95], όσο και από το ΕΣΠΔ στις Κατευθυντήριες γραμμές 8/2020 αναφορικά με τη *στόχευση χρηστών μέσων κοινωνικής δικτύωσης*[96] και στις Κατευθυντήριες γραμμές 3/2019 σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω βιντεοσυσκευών[97]. Ωστόσο, οφείλει να επισημανθεί παρενθετικά, ότι μια μερίδα θεωρητικών υποστηρίζει ότι το άρθρο 9 ΓΚΠΔ υπερισχύει του άρθρου 6, ως *lex specialis*. Η ανάλυση που ακολουθεί υιοθετεί την άποψη υποχρεωτικής σωρευτικής συνδρομής κατ' ελάχιστον μίας εκ των νομικών βάσεων του άρθρου 6 και μίας εκ των εξαιρέσεων του άρθρου 9§2 ΓΚΠΔ.

3.2.1.1 Οι νομικές βάσεις που απαιτεί το άρθρο 6 του ΓΚΠΔ

Κατ' αρχάς, η επεξεργασία των εικόνων προσώπου από τα συστήματα αναγνώρισης προσώπου, προκειμένου να είναι νόμιμη, θα πρέπει να ερείδεται σε μία εκ των περιοριστικά προβλεπόμενων **στο άρθρο 6§1 του ΓΚΠΔ** νομικών βάσεων, ήτοι:

> α) το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους συγκεκριμένους σκοπούς,
>
> β) 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

---

[95] Βλ. Γνώμη 6/2014 σχετικά με την έννοια των εννόμων συμφερόντων του υπευθύνου επεξεργασίας κατ' άρθρο 7 της Οδηγίας 95/46, σελ. 14. Διαθέσιμο στο: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_el.pdf

[96] Βλ. Κατευθυντήριες γραμμές 8/2020 σχετικά με τη στόχευση χρηστών μέσων κοινωνικής δικτύωσης, σελ. 40. Διαθέσιμο στο: https://edpb.europa.eu/system/files/2021-11/edpb_guidelines_082020_on_the_targeting_of_social_media_users_el_0.pdf

[97] Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (2020) 'Κατευθυντήριες γραμμές 3/2019 σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω βιντεοσυσκευών'. Διαθέσιμο στο: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_el.pdf

σύναψη σύμβασης

γ) η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας,

δ) η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου,

ε) η επεξεργασία είναι απαραίτητη για την **εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας** που έχει ανατεθεί στον υπεύθυνο επεξεργασίας,

στ) η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων 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 που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί.

Όσον αφορά συγκεκριμένα στις τεχνολογίες αναγνώρισης προσώπου, κατ' αρχήν δεν αποκλείεται καμία από τις νομικές βάσεις του ανωτέρω άρθρου. Εντούτοις, στην πράξη οι διατάξεις που είναι **περισσότερο πρόσφορες** να χρησιμοποιηθούν ως νομικό έρεισμα κατά την εργαλειοποίηση των συστημάτων, είναι η κατ' άρθρο **6§1 στοιχείο στ'**, καθώς και η κατ' **άρθρο 6§1 στοιχείο ε'**.

Κατ' αρχάς, **η υπό στοιχεία στ' του άρθρου 6§1 νομική βάση θεωρείται το πλέον λυσιτελές και, ως εκ τούτου, το συνηθέστερο νομικό έρεισμα που επικαλούνται οι κατασκευαστές και οι χρήστες της τεχνολογίας (μεταξύ αυτών και η Clearview AI) κατά την ανάπτυξη και εργαλειοποίηση συστημάτων αλγοριθμικής αναγνώρισης προσώπου**.

Στο πλαίσιο της ανωτέρω νομικής βάσης, ο Κανονισμός επιβάλλει τις κάτωθι προϋποθέσεις:

- η επεξεργασία να είναι απαραίτητη για την επίτευξη του σκοπού της
- ο σκοπός της να συνίσταται σε έννομο συμφέρον του υπευθύνου επεξεργασίας ή τρίτου
- να μην υπερτερούν τα δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων έναντι του εννόμου συμφέροντος προς εκπλήρωση του οποίου διενεργείται η επεξεργασία.

Ειδικότερα, ο ΓΚΠΔ, στο πλαίσιο που συνδιαμορφώνεται και από την αρχή της λογοδοσίας, απαιτεί ο υπεύθυνος επεξεργασίας να προβαίνει σε μία **ad hoc στάθμιση** μεταξύ αφενός των εννόμων συμφερόντων του ίδιου και αφετέρου των προσβαλλομένων δικαιωμάτων και ελευθεριών των υποκειμένων των δεδομένων· συνεπώς, η εκτίμηση την οποία οφείλει να εκπονεί ο υπεύθυνος επεξεργασίας δεν περιορίζεται στην εξέταση της πιθανής σύγκρουσης μόνον με το δικαίωμα στην προστασία δεδομένων προσωπικού χαρακτήρα, αλλά απαιτείται μια γενικότερη αξιολόγηση των επιπτώσεων στα θεμελιώδη ανθρώπινα δικαιώματα.

Νευραλγική, κατά την ανωτέρω στάθμιση, αποτελεί **η αρχή της αναλογικότητας**. Ειδικότερα, ο υπεύθυνος επεξεργασίας θα πρέπει να σταθμίσει τα αντικρουόμενα συμφέροντα με γνώμονα τις τρεις πτυχές που συναπαρτίζουν την εν λόγω αρχή, ήτοι να εξετάσει: α) την **αναγκαιότητα** της επεξεργασίας για την επίτευξη του σκοπού χωρίς υπέρβαση του αναγκαίου μέτρου κι εφόσον δεν υπάρχει άλλο ηπιότερο μέτρο επίτευξης του σκοπού, β) την **προσφορότητα και καταλληλότητά** της για την επίτευξη του συγκεκριμένου σκοπού και γ) την **stricto sensu αναλογικότητα**, κατά την οποία εξετάζεται αν η προσβολή των θεμελιωδών δικαιωμάτων και ελευθεριών είναι δυσανάλογη σε σχέση με τα πλεονεκτήματα της επεξεργασίας των δεδομένων.

Εν προκειμένω, τίθεται ήδη ευλόγως ένα ερώτημα: **δεδομένης της ιδιαιτέρως παρεμβατικής φύσης της τεχνολογίας αναγνώρισης προσώπου και των κρίσιμων επιπτώσεων αυτής -ήδη από την εγκατάσταση ενός συστήματος σε ένα χώρο- ταυτοχρόνως σε σωρεία θεμελιωδών δικαιωμάτων ανυπολόγιστου αριθμού φυσικών προσώπων,** μπορούν να υπάρξουν πράγματι περιστάσεις στις οποίες, κατόπιν της ad hoc στάθμισης του πλαισίου, των συνθηκών και της σοβαρότητας των ποικίλων και αλλεπάλληλων παραβιάσεων, **να καθίσταται αναλογική η επεξεργασία στην οποία προβαίνουν οι αλγόριθμοι αναγνώρισης προσώπου επ' αυτής της νομικής βάσης;** Το γεγονός ότι η εν λόγω νομική βάση αποτελεί το συνηθέστερο επικαλούμενο έρεισμα κατά τη χρήση της τεχνολογίας, σε συνδυασμό με την ανησυχητική διαπίστωση ότι έχει παρατηρηθεί μια **διαρκής κατάχρηση της επίκλησης των εννόμων συμφερόντων του υπευθύνου επεξεργασίας**[98], εγείρει ακόμη περισσότερες ανησυχίες σχετικά με τη νομιμότητα των συστημάτων

[98] «*Το Ευρωπαϊκό Κοινοβούλιο […] επισημαίνει ότι οι υπεύθυνοι επεξεργασίας εξακολουθούν να βασίζονται στο έννομο συμφέρον χωρίς να διεξάγουν τον απαιτούμενο έλεγχο της ισορροπίας των συμφερόντων, ο οποίος περιλαμβάνει αξιολόγηση των θεμελιωδών δικαιωμάτων […]*» βλ. Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 25ης Μαρτίου 2021 σχετικά με την έκθεση αξιολόγησης της Επιτροπής για την εφαρμογή του γενικού κανονισμού για την προστασία δεδομένων δύο έτη μετά την εφαρμογή του (2020/2717(RSP)) παράγραφος 7. Διαθέσιμο σε: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_EL.pdf

αναγνώρισης προσώπου που χρησιμοποιούνται ήδη ή πρόκειται να χρησιμοποιηθούν στο εγγύς μέλλον.

Περαιτέρω, σε σχέση με τη διάταξη αυτή, η αιτιολογική σκέψη 47 του ΓΚΠΔ διευκρινίζει ότι τα έννομα συμφέροντα ενός υπεύθυνου επεξεργασίας δύναται να παρέχουν τη νομική βάση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα, *υπό τον όρο ότι δεν υπερισχύουν των συμφερόντων ή των θεμελιωδών δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων,* ***λαμβάνοντας υπόψη τις θεμιτές προσδοκίες των υποκειμένων των δεδομένων βάσει της σχέσης τους με τον υπεύθυνο επεξεργασίας.*** *Τέτοιο έννομο συμφέρον θα μπορούσε λόγου χάρη να υπάρχει όταν* ***υφίσταται σχετική και κατάλληλη σχέση μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας****, όπως αν το υποκείμενο των δεδομένων είναι πελάτης του υπευθύνου επεξεργασίας ή βρίσκεται στην υπηρεσία του. Εν πάση περιπτώσει η ύπαρξη έννομου συμφέροντος θα χρειαζόταν προσεκτική αξιολόγηση, μεταξύ άλλων* ***ως προς το κατά πόσον το υποκείμενο των δεδομένων, κατά τη χρονική στιγμή και στο πλαίσιο της συλλογής*** *των δεδομένων προσωπικού χαρακτήρα,* ***μπορεί εύλογα να αναμένει ότι για τον σκοπό αυτό μπορεί να πραγματοποιηθεί επεξεργασία****.*

Οι **θεμιτές προσδοκίες** του υποκειμένου σε σχέση με την επεξεργασία των δεδομένων του τονίζονται ως σημαντική παράμετρος κατά τον ανωτέρω έλεγχο και από την Ομάδας Εργασίας του άρθρου 29 στη προαναφερθείσα Γνώμη 6/2014, στην οποία διευκρινίζεται επίσης ότι **τα προσωπικά δεδομένα εξακολουθούν να θεωρούνται ως τέτοια και να υπόκεινται στις εγγυήσεις του ενωσιακού νομοθετικού πλαισίου, ακόμη και αν έχουν καταστεί δημόσια**[99]. Επισημάνθηκε, ωστόσο, επιπλέον ότι η δημοσιοποίηση των προσωπικών δεδομένων δύναται να αποτελέσει κρίσιμη παράμετρο κατά την αξιολόγηση της συνδρομής «έννομων συμφερόντων», ιδίως **εάν πραγματοποιήθηκε με εύλογη προσδοκία περαιτέρω χρήσης των δεδομένων για συγκεκριμένους σκοπούς** (π.χ. για σκοπούς έρευνας).

Εν προκειμένω ιδιαίτερη μνεία οφείλεται στην πλέον δημοφιλή πρακτική της ιστοσυγκομιδής, η οποία κυριαρχεί κατά την ανάπτυξη των συστημάτων αναγνώρισης προσώπου από τις ιδιωτικές εταιρείες που εμπορεύονται την τεχνολογία. Συγκεκριμένα, κατά την ad hoc στάθμιση των επιμέρους συμφερόντων, μπορεί σαφώς να συναχθεί ότι **τα άτομα που έχουν δημοσιεύσει φωτογραφίες σε ιστότοπους, δεν αναμένουν ότι οι φωτογραφίες ή/και τα βίντεο τους θα επαναχρησιμοποιηθούν για τους σκοπούς που επιδιώκει η εταιρεία που κατασκευάζει το σύστημα αναγνώρισης προσώπου**.

[99] Ομάδα Εργασίας του άρθρου 29 για την προστασία δεδομένων (2014), σελ. 19 και υποσημείωση 31.

Αντιθέτως, η συγκρότηση βάσεων δεδομένων κατ' αυτόν τον τρόπο, συνιστά παραβίαση του πυρήνα των δικαιωμάτων προστασίας της ιδιωτικής ζωής και των προσωπικών δεδομένων των φυσικών προσώπων, ούσα εμφανώς δυσανάλογη σε σχέση με τα συμφέροντα του υπεύθυνου επεξεργασίας δεδομένων, ιδίως όταν αυτά είναι μόνον εμπορικά και οικονομικά[100].

Εν συνεχεία, αναφορικά με την περίπτωση που η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται *προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας* (άρθρο 6§1 στοιχείο ε'), λεκτέα είναι τα ακόλουθα:

Κατ' αρχάς, η εν λόγω νομική βάση προϋποθέτει την προηγούμενη ρητή ανάθεση στον υπεύθυνο επεξεργασίας καθήκοντος προς το δημόσιο συμφέρον ή την εκ μέρους του άσκηση δημόσιας εξουσίας, εφόσον αυτή προβλέπεται στο εκάστοτε εθνικό δίκαιο και σύμφωνα με τα οριζόμενα σε αυτό. Επιπλέον, απαραίτητη προϋπόθεση αποτελεί και εν προκειμένω η συνδρομή του στοιχείου αναγκαιότητας της επεξεργασίας για την εκπλήρωση του *συγκεκριμένου* ανατεθειμένου καθήκοντος, με αποτέλεσμα **να μην είναι επιτρεπτή η επίκληση της εν λόγω νομικής βάσης σε περίπτωση γενικευμένης χρήσης της τεχνολογίας** λ.χ. σε συγκροτήματα σχολείων[101], καθώς προϋποτίθεται προηγούμενη **αξιολόγηση της επικινδυνότητας** όλων των επιμέρους υπό παρακολούθηση χώρων (λ.χ. των συγκροτημάτων), η οποία θα πρέπει να ερείδεται σε **συγκεκριμένους παράγοντες κινδύνου**. Περαιτέρω, επισημαίνεται ότι σύμφωνα με την αρχή της λογοδοσίας, η ως άνω αξιολόγηση οφείλει να τεκμηριώνεται από τον υπεύθυνο επεξεργασίας, ενώ είναι πολύ πιθανό να είναι απαραίτητη και η εκπόνηση μελέτης εκτίμησης αντικτύπου, κατά τα οριζόμενα στο άρθρο 35 ΓΚΠΔ.

3.2.1.2 Οι εξαιρέσεις που προβλέπει το άρθρο 9§2 του ΓΚΠΔ

Εν συνεχεία, προκειμένου να πληρούται η διττή επιταγή περί της νομιμότητας της επεξεργασίας βιομετρικών δεδομένων, πέραν της ύπαρξης μίας εκ των ανωτέρω νομίμων βάσεων, απαιτείται επιπροσθέτως και η συνδρομή τουλάχιστον μίας εκ των εξαιρέσεων που προβλέπονται στον Κανονισμό.

---

[100] Commission Nationale de l'Informatique et des Libertés (CNIL) 'Decision n° MED 2021-134 of 1st November 2021 issuing an order to comply to the company CLEARVIEW AI' Διαθέσιμο σε: https://www.cnil.fr/sites/default/files/atoms/files/decision_ndeg_med_2021-134.pdf. Βλ. και ΔΕΕ, υπόθεση Google Spain, στην οποία το Δικαστήριο απεφάνθη ότι η επέμβαση «*λόγω της ενδεχόμενης σοβαρότητάς της, δεν μπορεί να δικαιολογείται μόνο με βάση το οικονομικό συμφέρον του φορέα εκμετάλλευσης της μηχανής αναζήτησης στην ως άνω επεξεργασία*».

[101] Σκόνδρα, Μ. (2020) 'Συστήματα Βιντεοεπιτήρησης , αναγνώριση προσώπου και προστασία προσωπικών δεδομένων', *ΔΙΤΕ (π. ΔΙΜΕΕ)*, (1), σελ. 48-49.

Σύμφωνα με το **άρθρο 9§2 του Κανονισμού**, η επεξεργασία των εικόνων προσώπου από τα συστήματα αλγοριθμικής αναγνώρισης προσώπου, είναι δυνατή **μόνον εφόσον συντρέχει μία εκ των περιοριστικά προβλεπόμενων σε αυτό εξαιρέσεων**, ήτοι μόνον εάν:

- το υποκείμενο των δεδομένων έχει παράσχει **ρητή συγκατάθεση** για την επεξεργασία αυτών των δεδομένων προσωπικού χαρακτήρα **για έναν ή περισσότερους συγκεκριμένους σκοπούς**, εκτός εάν το δίκαιο της Ένωσης ή κράτους μέλους προβλέπει ότι η απαγόρευση που αναφέρεται στην παράγραφο 1 του άρθρου δεν μπορεί να αρθεί από το υποκείμενο των δεδομένων,
- η επεξεργασία είναι **απαραίτητη για την εκτέλεση των υποχρεώσεων και την άσκηση συγκεκριμένων δικαιωμάτων του υπευθύνου επεξεργασίας ή του υποκειμένου των δεδομένων** στον τομέα του **εργατικού δικαίου** και του **δικαίου κοινωνικής ασφάλισης και κοινωνικής προστασίας**, εφόσον επιτρέπεται από το δίκαιο της Ένωσης ή κράτους μέλους ή από συλλογική συμφωνία σύμφωνα με το εθνικό δίκαιο παρέχοντας κατάλληλες εγγυήσεις για τα θεμελιώδη δικαιώματα και τα συμφέροντα του υποκειμένου των δεδομένων,
- η επεξεργασία είναι απαραίτητη για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου, εάν το υποκείμενο των δεδομένων είναι σωματικά ή νομικά ανίκανο να συγκατατεθεί
- η επεξεργασία διενεργείται, με κατάλληλες εγγυήσεις, στο πλαίσιο των νόμιμων δραστηριοτήτων ιδρύματος, οργάνωσης ή άλλου μη κερδοσκοπικού φορέα με πολιτικό, φιλοσοφικό, θρησκευτικό ή συνδικαλιστικό στόχο και υπό την προϋπόθεση ότι η επεξεργασία αφορά αποκλειστικά τα μέλη ή τα πρώην μέλη του φορέα ή πρόσωπα τα οποία έχουν τακτική επικοινωνία μαζί του σε σχέση με τους σκοπούς του και ότι τα δεδομένα προσωπικού χαρακτήρα δεν κοινοποιούνται εκτός του συγκεκριμένου φορέα χωρίς τη συγκατάθεση των υποκειμένων των δεδομένων,
- η επεξεργασία αφορά δεδομένα προσωπικού χαρακτήρα τα οποία έχουν **προδήλως δημοσιοποιηθεί** από το υποκείμενο των δεδομένων,
- η επεξεργασία είναι απαραίτητη για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων ή όταν τα δικαστήρια ενεργούν υπό τη δικαιοδοτική τους ιδιότητα
- η επεξεργασία είναι απαραίτητη για **λόγους ουσιαστικού δημοσίου συμφέροντος**, **βάσει του δικαίου της Ένωσης ή**

κράτους μέλους, το οποίο είναι ανάλογο προς τον επιδιωκόμενο στόχο, σέβεται την ουσία του δικαιώματος στην προστασία των δεδομένων και προβλέπει κατάλληλα και συγκεκριμένα μέτρα για τη διασφάλιση των θεμελιωδών δικαιωμάτων και των συμφερόντων του υποκειμένου των δεδομένων,

- η επεξεργασία είναι απαραίτητη για σκοπούς προληπτικής ή επαγγελματικής ιατρικής, εκτίμησης της ικανότητας προς εργασία του εργαζομένου, ιατρικής διάγνωσης, παροχής υγειονομικής ή κοινωνικής περίθαλψης ή θεραπείας ή διαχείρισης υγειονομικών και κοινωνικών συστημάτων και υπηρεσιών βάσει του ενωσιακού δικαίου ή του δικαίου κράτους μέλους ή δυνάμει σύμβασης με επαγγελματία του τομέα της υγείας και με την επιφύλαξη των προϋποθέσεων και των εγγυήσεων που αναφέρονται στην παράγραφο 3,
- η επεξεργασία είναι απαραίτητη **για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας**, όπως η προστασία έναντι σοβαρών διασυνοριακών απειλών κατά της υγείας ή η διασφάλιση υψηλών προτύπων ποιότητας και ασφάλειας της υγειονομικής περίθαλψης και των φαρμάκων ή των ιατροτεχνολογικών προϊόντων, βάσει του δικαίου της Ένωσης ή του δικαίου κράτους μέλους, το οποίο προβλέπει κατάλληλα και συγκεκριμένα μέτρα για την προστασία των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων, ειδικότερα δε του επαγγελματικού απορρήτου, ή
- η επεξεργασία είναι απαραίτητη για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς σύμφωνα με το άρθρο 89 παράγραφος 1 βάσει του δικαίου της Ένωσης ή κράτους μέλους, οι οποίοι είναι ανάλογοι προς τον επιδιωκόμενο στόχο, σέβονται την ουσία του δικαιώματος στην προστασία των δεδομένων και προβλέπουν κατάλληλα και συγκεκριμένα μέτρα για τη διασφάλιση των θεμελιωδών δικαιωμάτων και των συμφερόντων του υποκειμένου των δεδομένων.

Εκ των ανωτέρω εξαιρέσεων, συνηθέστερο νομικό έρεισμα κατά τη χρήση συστημάτων αλγοριθμικής αναγνώρισης προσώπου, αποτελεί η **ρητή συγκατάθεση** του υποκειμένου των δεδομένων, εφόσον βέβαια αυτή μπορεί να δοθεί με συνθήκες εγκυρότητας.

Ειδικότερα, η συγκατάθεση του υποκειμένου των δεδομένων, προκειμένου να δύναται να αποτελέσει νόμιμη βάση επεξεργασίας δεδομένων προσωπικού

χαρακτήρα, θα πρέπει, κατ' αρχήν, να είναι ελεύθερη, συγκεκριμένη, ρητή και να παρέχεται με πλήρη επίγνωση του υποκειμένου, ήτοι θα πρέπει να πληροί τα αυστηρά προαπαιτούμενα του Κανονισμού, όπως τίθενται σαφώς στα άρθρα 4 περίπτωση 11 και 7 ΓΚΠΔ[102].

Οι κατευθυντήριες του ΕΣΠΔ[103] όσον αφορά ειδικότερα στη **συστηματική παρακολούθηση στο πλαίσιο της βιντεοεπιτήρησης**, συνιστούν χρήσιμα ερμηνευτικά εργαλεία στην τεχνολογία αναγνώρισης προσώπου, ιδιαίτερα δε όταν αυτή χρησιμοποιείται σε πραγματικό χρόνο, είτε σε δημόσιους και ημι-δημόσιους χώρους (λ.χ. μέσα μαζικής μεταφοράς, αεροδρόμια), είτε σε ιδιωτικούς (λ.χ. στην είσοδο ενός καταστήματος). Όπως επισημάνθηκε, στην εν λόγω περίπτωση **μόνο σε εξαιρετικές περιπτώσεις θα μπορούσε η συγκατάθεση να αποτελέσει νόμιμη βάση επεξεργασίας, καθώς το σύστημα αναγνώρισης προσώπου θέτει εγγενώς υπό παρακολούθηση έναν απροσδιόριστο αριθμό ανθρώπων, ακόμη και όταν εργαλειοποιείται στοχευμένα σε περιορισμένους γεωγραφικά χώρους.** Η ακαταλληλότητα του εν λόγω νομικού ερείσματος καταδεικνύεται περαιτέρω από το γεγονός πως, εκ των πραγμάτων **ο υπεύθυνος επεξεργασίας θα είναι σε ελάχιστες περιπτώσεις σε θέση να αποδείξει ότι**

---

[102] Στο άρθρο 4 στοιχείο 11 του ΓΚΠΔ η συγκατάθεση ορίζεται ως: «*κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν*». Ο ΓΚΠΔ παρέχει πρόσθετη καθοδήγηση στο άρθρο 7 «*1. Όταν η επεξεργασία βασίζεται σε συγκατάθεση, ο υπεύθυνος επεξεργασίας είναι σε θέση να αποδείξει ότι το υποκείμενο των δεδομένων συγκατατέθηκε για την επεξεργασία των δεδομένων του προσωπικού χαρακτήρα. 2. Εάν η συγκατάθεση του υποκειμένου των δεδομένων παρέχεται στο πλαίσιο γραπτής δήλωσης η οποία αφορά και άλλα θέματα, το αίτημα για συγκατάθεση υποβάλλεται κατά τρόπο ώστε να είναι σαφώς διακριτό από τα άλλα θέματα, σε κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση. Κάθε τμήμα της δήλωσης αυτής το οποίο συνιστά παράβαση του παρόντος κανονισμού δεν είναι δεσμευτικό. 3. Το υποκείμενο των δεδομένων έχει δικαίωμα να ανακαλέσει τη συγκατάθεσή του ανά πάσα στιγμή. Η ανάκληση της συγκατάθεσης δεν θίγει τη νομιμότητα της επεξεργασίας που βασίστηκε στη συγκατάθεση προ της ανάκλησής της. Πριν την παροχή της συγκατάθεσης, το υποκείμενο των δεδομένων ενημερώνεται σχετικά. Η ανάκληση της συγκατάθεσης είναι εξίσου εύκολη με την παροχή της. 4. Κατά την εκτίμηση κατά πόσο η συγκατάθεση δίνεται ελεύθερα, λαμβάνεται ιδιαιτέρως υπόψη κατά πόσο, μεταξύ άλλων, για την εκτέλεση σύμβασης, συμπεριλαμβανομένης της παροχής μιας υπηρεσίας, τίθεται ως προϋπόθεση η συγκατάθεση στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που δεν είναι αναγκαία για την εκτέλεση της εν λόγω σύμβασης.*» Βλ. επίσης και τις αιτιολογικές σκέψεις 32, 33, 42 και 43 σχετικά με τη συμπεριφορά που πρέπει να επιδεικνύει ο υπεύθυνος επεξεργασίας προκειμένου να συμμορφώνεται προς την απαίτηση συγκατάθεσης.

[103] Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (2020) 'Κατευθυντήριες γραμμές 3/2019 σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω βιντεοσυσκευών'. σελ. 15-16. Διαθέσιμο στο: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_el.pdf

κάθε υποκείμενο που εισέρχεται στον επιτηρούμενο χώρο έχει δώσει εκ των προτέρων τη συγκατάθεσή του, η οποία θα πρέπει πάντοτε να έχει δοθεί σύμφωνα με τις αυστηρές προϋποθέσεις που θέτει ο Κανονισμός[104], ενώ κι εάν υποτεθεί ότι το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία, σε περίπτωση που επιθυμεί να ανακαλέσει τη συγκατάθεσή του θα είναι ιδιαιτέρως δυσχερές για τον υπεύθυνο επεξεργασίας να αποδείξει ότι τα δεδομένα προσωπικού χαρακτήρα πράγματι δεν υποβάλλονται πλέον σε επεξεργασία (άρ. 7§3 ΓΚΠΔ).

Επιπροσθέτως, η συγκατάθεση δεν είναι δυνατό να αποτελέσει τη νόμιμη βάση επεξεργασίας όταν υφίσταται **ανισότητα ισχύος** μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου της επεξεργασίας (λ.χ. σχέση μεταξύ εργαζομένου- εργοδότη), καθώς στο πλαίσιο αυτό τυχούσα συγκατάθεση δεν μπορεί να θεωρηθεί ελεύθερη και ως εκ τούτου έγκυρη. Για το λόγο αυτό, έχει υποστηριχθεί εκτενώς ότι **η συναίνεση δεν θα πρέπει, κατά κανόνα, να αποτελεί** το **νομικό έρεισμα που χρησιμοποιείται κατά τη χρήση συστημάτων αναγνώρισης προσώπου από δημόσιες αρχές ή από ιδιωτικές εταιρείες που δραστηριοποιούνται στους τομείς της δημόσιας ασφάλειας και του ελέγχου των συνόρων**, λόγω της ανισορροπίας των εξουσιών μεταξύ των υποκειμένων των δεδομένων και των αρχών αυτών[105].

Παρά την εγγενή ακαταλληλότητα της εν λόγω νομικής βάσης, στην πράξη αποτελεί **το συχνότερο έρεισμα που επικαλούνται οι χρήστες και οι κατασκευαστές των συστημάτων αναγνώρισης προσώπου κατά τη χρήση της τεχνολογίας**. Ήδη, οι ΑΠΔΠΧ διεθνώς έχουν εξετάσει την επάρκεια της συγκατάθεσης ως εξαιρετικής νομίμου βάσεως κατά τη χρήση της τεχνολογίας αναγνώρισης προσώπου, ιδιαίτερα όταν αποδέκτες αυτής είναι άτομα που χρήζουν μεγαλύτερης προστασίας, **όπως τα παιδιά.** Ενδεικτικά αναφέρεται ότι, με απόφαση του Διοικητικού Δικαστηρίου της Μασσαλίας το 2020, ακυρώθηκε η απόφαση της περιφέρειας Προβηγκίας-Αλπεων-Κυανής Ακτής της Γαλλίας να πραγματοποιήσει **δύο πιλοτικές δοκιμές αναγνώρισης προσώπου σε εισόδους σχολείων**. Ενόσω η υπόθεση εκκρεμούσε, η Γαλλική ΑΠΔΠΧ (CNIL) εξέφρασε ανησυχίες σχετικά με την εφαρμογή ενός τέτοιου συστήματος, δεδομένου του κοινού- στόχου (παιδιά) και της έτι υψηλότερης ευαισθησίας των βιομετρικών

---

[104] Παραδείγματος χάριν, η είσοδος σε σηματοδοτημένο παρακολουθούμενο χώρο (π.χ. όταν οι άνθρωποι καλούνται να διέλθουν από ένα χώρο υποδοχής ή μία πύλη προκειμένου να εισέλθουν σε παρακολουθούμενο με την τεχνολογία αναγνώρισης προσώπου χώρο, στον οποίο υπάρχει σχετική σήμανση χρήσης της τεχνολογίας) γίνεται δεκτό ότι δεν αποτελεί **δήλωση ή σαφή θετική ενέργεια**, όπως απαιτείται για τη συγκατάθεση.

[105] Council of Europe- Convention 108 (2021) *Guidelines on facial recognition'*. σελ. 9-10. Διαθέσιμο στο: https://edoc.coe.int/en/artificial-intelligence/9753-guidelines-on-facial-recognition.html

δεδομένων που διακυβεύονται[106]. Η ακυρωτική απόφαση του Δικαστηρίου ελήφθη με την αιτιολογία ότι **η συγκατάθεση που συλλέχθηκε από τους μαθητές γυμνασίου δεν δόθηκε με ελεύθερο, ρητό, συγκεκριμένο και ενημερωμένο, κατά τα προβλεπόμενα στο άρθρο 9§2 στοιχ. α' ΓΚΠΔ , καθώς και ότι τα σχολεία είχαν στη διάθεσή τους λιγότερο παρεμβατικά μέσα για να ελέγχουν την πρόσβαση των μαθητών τους στους χώρους τους**. Ομοίως, τον Ιούνιο του 2021, το Διοικητικό Δικαστήριο της Στοκχόλμης επικύρωσε την απόφαση της σουηδικής ΑΠΔΠΧ να επιβάλει πρόστιμο ύψους 200.000 SEK σε γυμνάσιο για **παράνομη χρήση αυτοματοποιημένων συστημάτων αναγνώρισης προσώπου για την καταγραφή της παρουσίας των μαθητών σε μια εξέταση**. Μεταξύ άλλων διαπιστώσεων, το Δικαστήριο τόνισε ότι υπήρχε **ανισορροπία ισχύος μεταξύ του σχολείου και των υποκειμένων των δεδομένων (δηλαδή των μαθητών), με αποτέλεσμα η συγκατάθεση των τελευταίων για την επεξεργασία των βιομετρικών τους δεδομένων να μη δύναται να θεωρηθεί ελεύθερη και, ως εκ τούτου, έγκυρη**[107]. Το δικαστήριο έκρινε επίσης ότι το σχολείο είχε το δικαίωμα να παρακολουθεί τη φοίτηση των μαθητών, αλλά όχι με τη συλλογή της εικόνας προσώπου τους, λόγω της ευαίσθητης φύσης τους σύμφωνα με το άρθρο 9 του ΓΚΠΔ.

Τονίζεται παρενθετικά ότι παρόμοιες δικαιοδοτικές κρίσεις έχουν παρατηρηθεί διεθνώς. Παραδείγματος χάριν, στην **Κίνα**, σε μια απόφαση-ορόσημο για την εμπορική αξιοποίηση της τεχνολογίας αναγνώρισης προσώπου (Bing Guo κατά Hangzhou Safari Park)[108], το κινεζικό δικαστήριο Hangzhou Fuyang έκρινε ότι είναι παράνομο για ένα νομικό πρόσωπο (ιδιωτικό πάρκο) να συλλέγει βιομετρικά δεδομένα των καταναλωτών του (μέσω σάρωσης προσώπου προκειμένου να εγκριθεί η είσοδος), χωρίς τη συγκατάθεσή τους. Το δικαστήριο απεφάνθη ότι ο χρήστης ενός συστήματος αναγνώρισης προσώπου θα πρέπει να λαμβάνει εκ των προτέρων τη συγκατάθεση των υποκειμένων, καθώς και να συμμορφώνεται με τις αρχές της «νομιμότητας, της αναλογικότητας και της αναγκαιότητας» όταν συλλέγει προσωπικά δεδομένα.

Προσέτι, η εκτεταμένη **πρακτική της ιστοσυγκομιδής** από τις εταιρείες που προμηθεύουν την τεχνολογία αναγνώρισης προσώπου, καθιστά σαφές ότι **η συγκατάθεση των υποκειμένων δεν έχει ληφθεί για την πλειονότητα των συστημάτων αναγνώρισης προσώπου που χρησιμοποιούνται αυτή τη**

---

[106] Γαλλική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (2019), 'Expérimentation de la reconnaissance faciale dans deux lycées : la CNIL précise sa position', October 29, 2019, Διαθέσιμο σε: https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position

[107] Σουηδική Αρχή Προστασίας Δεδομένων (IMY) 'IMY får rätt om ansiktsigenkänning' https://www.imy.se/nyheter/imy-far-ratt-om-ansiktsigenkanning/

[108] Bu, Q. (2021), ο.π. σελ. 122-123.

χρονική στιγμή παγκοσμίως. Εξίσου ανησυχητικό αποτελεί το γεγονός ότι **μεγάλη μερίδα των ερευνητών της τεχνολογίας αναγνώρισης προσώπου, χρησιμοποιεί δημόσιες βάσεις δεδομένων δίχως να αποζητά τη συγκατάθεση των υποκειμένων**, αλλά και χωρίς να θεωρεί ότι η πιθανή έλλειψη συναίνεση πρέπει να αποτελεί ανασταλτικό παράγοντα για τους ίδιους, δεδομένου ότι πρωταρχικός στόχος τους αποτελεί η λυσιτελής εκπαίδευση αλγορίθμων[109].

Εν συνεχεία, αναφορικά με την κατ' άρθρο 9§2 περ. ε' εξαίρεση της **προδήλου δημοσιοποίησης**, όπως προαναφέρθηκε, η Ομάδας Εργασίας του άρθρου 29 έχει επισημάνει ότι «*θα ήταν λάθος να συμπεράνουμε ότι το γεγονός ότι κάποιος έχει προδήλως δημοσιοποιήσει ειδικές κατηγορίες δεδομένων σύμφωνα με το άρθρο 8 παράγραφος 2 στοιχείο ε) της Οδηγίας 95/46* (σήμερα του άρθρου 9 παρ. 2 στοιχ. ε' ΓΚΠΔ*) θα ήταν -πάντα αυτό καθαυτό- επαρκής συνθήκη για να επιτραπεί κάθε είδος επεξεργασίας δεδομένων χωρίς αξιολόγηση της στάθμισης των διακυβευόμενων συμφερόντων και δικαιωμάτων, όπως απαιτείται από το άρθρο 7 στοιχ. στ' της Οδηγίας 95/46* (σήμερα του άρθρου 6 παρ. 1 στοιχ. στ' ΓΚΠΔ)» Τούτο τόνισε προσφάτως και η Γαλλική ΑΠΔΠΧ στην απόφασή της σχετικά με τη νομιμότητα της επεξεργασίας στην οποία προβαίνει η Clearview[110], στην οποία διασαφήνισε ότι **τα προσωπικά δεδομένα δεν απεκδύονται την ιδιότητά τους εκ μόνης της δημοσιοποίησης τους, ούτε ότι η δημοσιοποίησή τους αυτή συνιστά κάποιου είδους συναίνεση για την εκ νέου επεξεργασία τους, ιδίως όταν λαμβάνει χώρα χωρίς τη γνώση των υποκειμένων**. Άλλως, μόνον το γεγονός ότι μια φωτογραφία έχει προδήλως δημοσιοποιηθεί από το υποκείμενο των δεδομένων δεν συνεπάγεται αυτομάτως ότι τα σχετικά βιομετρικά δεδομένα, τα οποία μπορούν να ανακτηθούν από τη φωτογραφία μέσω της τεχνολογίας αναγνώρισης προσώπου, έχουν προδήλως δημοσιοποιηθεί. Περαιτέρω, οφείλει να επισημανθεί ότι πολλές φωτογραφίες, ιδιαίτερα στα μέσα κοινωνικής δικτύωσης, δεν δημοσιοποιούνται από τα ίδια τα υποκείμενα των δεδομένων, αλλά τρίτους, πολλές φορές εν αγνοία των υποκειμένων.

Τέλος, επισημαίνεται ότι το **ουσιαστικό δημόσιο συμφέρον** (άρθρο 9§2 περ. ζ') θεωρείται **ο βασικότερος από τους ανωτέρω λόγους εξαίρεσης**, όπως έχει υπογραμμιστεί μεταξύ άλλων και από την Ευρωπαϊκή Επιτροπή, στη Λευκή

---

[109] Έρευνα του επιστημονικού περιοδικού Nature σε 480 ερευνητές που έχουν δημοσιεύσει άρθρα σχετικά με την αναγνώριση προσώπου, την τεχνητή νοημοσύνη και την επιστήμη των υπολογιστών, κατέδειξε ότι το 60% των ερωτηθέντων θεώρησαν ότι δεν είναι απαραίτητο για τους ερευνητές να λαμβάνουν τη συγκατάθεση των ατόμων πριν χρησιμοποιήσουν τα πρόσωπά τους σε ένα σύνολο δεδομένων αναγνώρισης προσώπου, βλ. Roussi, A. (2020) 'Resisting the rise of facial recognition', *Nature*, 587(7834), σελ. 350–353. doi:10.1038/d41586-020-03188-2. Διαθέσιμο σε: https://www.nature.com/articles/d41586-020-03188-2

[110] CNIL'Decision n° MED 2021-134' ο.π.

Βίβλο για την Τεχνητή Νοημοσύνη[111]. Ειδικότερα, η Επιτροπή διευκρίνισε ότι όταν η επεξεργασία ερείδεται στην εν λόγω νομική βάση, *πρέπει να πραγματοποιείται βάσει του ενωσιακού ή του εθνικού δικαίου, με την επιφύλαξη των απαιτήσεων αναλογικότητας, σεβασμού της ουσίας του δικαιώματος στην προστασία των δεδομένων και κατάλληλων εγγυήσεων*. Επιπλέον η Επιτροπή υπενθύμισε ότι, δεδομένου ότι οποιαδήποτε επεξεργασία βιομετρικών δεδομένων με σκοπό τη μοναδική ταυτοποίηση φυσικού προσώπου αφορά εξαίρεση σε απαγόρευση που προβλέπεται στο ενωσιακό δίκαιο, θα υπόκειται στις απαιτήσεις του Χάρτη.

3.2.1.3 Οι απαιτήσεις της Οδηγίας (ΕΕ) 2016/680

Κατ' αναλογίαν, στο **άρθρο 10 της Οδηγίας** η επεξεργασία βιομετρικών δεδομένων[112] ορίζεται επιτρεπτή **μόνον** όταν είναι **απολύτως αναγκαία, υπό την επιφύλαξη των κατάλληλων διασφαλίσεων για τα δικαιώματα και τις ελευθερίες του υποκειμένου** των δεδομένων, και εφόσον:

- το επιτρέπει το δίκαιο της Ένωσης ή των κρατών μελών,
- επιβάλλεται για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου, ή
- η επεξεργασία αφορά σε δεδομένα τα οποία έχουν προδήλως δημοσιοποιηθεί από το υποκείμενο των δεδομένων.

Παραλλήλως, κατά το άρθρο 8 της Οδηγίας η επεξεργασία προσωπικών δεδομένων είναι σύννομη «***μόνον εάν και στον βαθμό που είναι απαραίτητη για την εκτέλεση καθήκοντος που ασκείται από αρχή αρμόδια για τους σκοπούς που προβλέπονται στο άρθρο 1 παράγραφος 1[113] και βασίζεται στο δίκαιο της Ένωσης ή των κρατών μελών.*** *Το δίκαιο κράτους μέλους που ρυθμίζει την επεξεργασία στο πλαίσιο της παρούσας οδηγίας καθορίζει τουλάχιστον* ***τους στόχους της επεξεργασίας, τα δεδομένα προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία και τους σκοπούς της επεξεργασίας***».

Στην πράξη, τα νομικά ερείσματα που επικαλούνται συχνότερα οι

---

[111] Βλ. Λευκή Βίβλος για την ΤΝ ο.π. σελ. 26-27.

[112] Στο αρ. 3 στοιχ. 13 της Οδηγίας ως βιομετρικά δεδομένα ορίζονται τα *δεδομένα προσωπικού χαρακτήρα τα 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.*

[113] αρ.1 §1 Οδηγίας: *Η παρούσα οδηγία θεσπίζει τους κανόνες που αφορούν στην προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, της διερεύνησης, της ανίχνευσης ή της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, περιλαμβανομένων της προστασίας από απειλές κατά της δημόσιας ασφάλειας και της αποτροπής τους.*

δημόσιες αρχές κατά τη χρήση της τεχνολογίας αναγνώρισης προσώπου, είναι οι κώδικες ποινικής δικονομίας και τα συναφή νομοθετήματα, ενώ έχουν υπάρξει και περιπτώσεις θεμελίωσης της επεξεργασίας στη συγκατάθεση των υποκειμένων. Εντούτοις, συχνά οι επικληθείσες νομικές βάσεις δεν είναι αρκούντως σαφείς, ενώ οι αρχές επιβολής του νόμου αποτυγχάνουν επανειλημμένα να θεμελιώσουν επαρκώς την αναγκαιότητα χρήσης των συστημάτων αναγνώρισης προσώπου.

Επί παραδείγματι, στην πολύκροτη υπόθεση 'R (Bridges) v Chief Constable of South Wales Police & Information Commissioner', το Εφετείο του Ηνωμένου Βασιλείου ακύρωσε πρωτοβάθμια απόφαση, **μεταξύ άλλων επειδή το νομικό πλαίσιο δεν μπορούσε να χαρακτηριστεί ως νόμιμη βάση, επειδή ήταν ασαφές και παρείχε σε μεμονωμένους αστυνομικούς υπερβολικά ευρεία διακριτική ευχέρεια όσον αφορά στην κατάρτιση λιστών παρακολούθησης και στον καθορισμό του τρόπου και του τόπου που μπορεί να χρησιμοποιηθεί η τεχνολογία αναγνώρισης προσώπου**. Ομοίως, η Αρχή Προστασίας Δεδομένων του Αμβούργου έκρινε ότι **η αδιάκριτη βιντεοεπιτήρηση και η συνακόλουθη εξαγωγή και αποθήκευση βιομετρικών δεδομένων** κατά τη διάρκεια της Συνόδου Κορυφής της G20 το 2017**, δεν διέθετε επαρκή νομική βάση**. Μάλιστα, κατόπιν της δικαστικής ακύρωσης της εντολής διαγραφής της βάσεως βιομετρικών δεδομένων, η ΑΠΔΠΧ του Αμβούργου υποστήριξε στην έφεσή της ότι η έλλειψη επαρκώς καθορισμένων νομικών βάσεων παραβιάζει, επίσης, το άρθρο 8§2 του Χάρτη, το άρθρο 4§1 στοιχ. α' της Οδηγίας, καθώς και τη νομοθεσία με την οποία ενσωματώθηκε η Οδηγία στη γερμανική έννομη τάξη[114].

Εν συνεχεία, όπως προκύπτει εκ των ανωτέρω, **η αρχή της αναγκαιότητας** βρίσκεται στο επίκεντρο των υπό κρίση διατάξεων της Οδηγίας, και απαιτεί οι αρχές επιβολής του νόμου, κατά τη χρήση της τεχνολογίας αναγνώρισης προσώπου, να είναι σε θέση να αποδεικνύουν ότι υφίσταται μία **συγκεκριμένη, σαφής και άμεση απειλή της εθνικής ή της δημόσιας ασφάλειας,** η οποία δικαιολογεί την αναγκαιότητα επεξεργασίας των ευαίσθητων προσωπικών δεδομένων των πολιτών της, μέσω της χρήσης παρεμβατικής τεχνολογίας τέτοιου βεληνεκούς.

Το Γραφείο του Επιτρόπου Πληροφοριών του Ηνωμένου Βασιλείου (ICO) υποστηρίζει, περαιτέρω, ότι η εν στενή εννοία αναγκαιότητα, **στο πλαίσιο χρήσης της «ζωντανής» τεχνολογίας αναγνώρισης προσώπου από τις αρχές επιβολής του νόμου**, απαιτεί ο υπεύθυνος επεξεργασίας να προβαίνει σε εκτίμηση της **αναλογικότητας** της επεξεργασίας των βιομετρικών δεδομένων των υποκειμένων τους **και της διαθεσιμότητας** λιγότερο παρεμβατικών

[114] Madiega, T., Mildebrath, H. (2021), ο.π. σελ. 11-12.

εναλλακτικών[115]. Πράγματι, τόσο τα κατοχυρωμένα στο Χάρτη θεμελιώδη δικαιώματα στην προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων, όσο και η συνεπής ερμηνεία του ΓΚΠΔ και της Οδηγίας, απαιτούν η επεξεργασία δεδομένων που σχετίζεται με την τεχνολογία αναγνώρισης προσώπου να διεξάγεται με απόλυτο σεβασμό στην **αρχή της αναλογικότητας**· συνεπώς, ακόμα και αν η χρήση ενός συστήματος αλγοριθμικής αναγνώρισης προσώπου από τις αρχές συνιστά στην προκειμένη περίπτωση stricto sensu αναγκαίο μέτρο, προκειμένου η επεξεργασία των ευαίσθητων δεδομένων των πολιτών να είναι σύννομη, θα οφείλει ταυτοχρόνως να είναι και αναλογικό.

Η σημασία της αρχής της αναλογικότητας κατά τη χρήση της τεχνολογίας αναγνώρισης προσώπου από τις αρχές επιβολής του νόμου έχει επίσης υπογραμμιστεί από την ΑΠΔΠΧ του Αμβούργου. Ερειδόμενη στις υποθέσεις Digital Rights Ireland και Tele2 Sverige του ΔΕΕ, η ανωτέρω αρχή απεφάνθη σχετικά με την προαναφερθείσα υπόθεση, ότι η νομική βάση που επικαλέστηκε η αστυνομία **δεν ήταν επαρκώς συγκεκριμένη και καθορισμένη** και, ως εκ τούτου, δεν πληρούσε **τις απαιτήσεις αναλογικότητας** σύμφωνα με το άρθρο 8 του Χάρτη, αλλά και σύμφωνα με το προβλεπόμενο στο γερμανικό δίκαιο δικαίωμα πληροφοριακού αυτοκαθορισμού. Η αρχή επεσήμανε, επίσης, ότι ακόμη και αν η νομική βάση της επεξεργασίας ήταν συμβατή με το ενωσιακό και εθνικό δίκαιο, η πρακτική εφαρμογή της τεχνολογίας αναγνώρισης προσώπου, σε κάθε περίπτωση, δεν ικανοποιούσε την απαίτηση της εν στενή εννοία αναγκαιότητας. Εξ αντιδιαστολής, στην ως άνω υπόθεση του Ηνωμένου Βασιλείου, το Εφετείο φαίνεται ότι θα θεωρούσε την εφαρμογή της τεχνολογίας αναλογική, εάν δεν είχε κρίνει ότι είναι παράνομη λόγω των αόριστων νομικών βάσεων, της ανεπαρκούς εκτίμησης αντικτύπου για την προστασία των δεδομένων και της μη αξιολόγησης των πιθανών αλγοριθμικών διακρίσεων.

Επιπροσθέτως, **τα ζητήματα προστασίας δεδομένων που σχετίζονται με την πρακτική της ιστοσυγκομιδής πολλαπλασιάζονται εκθετικά όταν αυτή εργαλειοποιείται από τις αρχές επιβολής του νόμου** για την ενίσχυση των χρησιμοποιούμενων από αυτές συστημάτων αναγνώρισης προσώπου.

Κατ' αρχάς, η συγκρότηση των βάσεων δεδομένων στις οποίες ερείδονται τα συστήματα που χρησιμοποιεί μία αστυνομική αρχή, με τη μέθοδο της ιστοσυγκομιδής, συνεπάγεται τη **μαζική συλλογή βιομετρικών δεδομένων εν πλήρει αγνοία των υποκειμένων τους, αποστερώντας τους εκ προοιμίου τη δυνατότητα να ασκήσουν τα δικαιώματα που επιφυλάσσει σε αυτά η**

[115] Information Commissioner's Office (2021) *The use of live facial recognition technology in public places*. σελ 34-37. Διαθέσιμο στο: https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf

Οδηγία.

Επιπροσθέτως, οι αστυνομικές αρχές συχνά δεν αντλούν απευθείας δεδομένα από δημόσιες βάσεις, αλλά προμηθεύονται από τρίτους – οι οποίοι συνήθως είναι εγκατεστημένοι εκτός Ε.Ε.- λογισμικά που έχουν εκπαιδευτεί μέσω της ιστοσυγκομιδής (όπως το λογισμικό της Clearview). Επομένως, αναλόγως του τόπου στον οποίο έχει έδρα ο πάροχος της βάσης δεδομένων, η χρήση μιας τέτοιας υπηρεσίας μπορεί να συνεπάγεται τη **διαβίβαση ευαίσθητων προσωπικών δεδομένων εκτός της Ευρωπαϊκής Ένωσης**[116], καθώς και τη **βιομετρική αντιστοίχιση των δεδομένων αυτών με την -ενδεχομένως αυθαίρετα καταρτισθείσα- βάση δεδομένων φωτογραφιών του παρόχου.** Προσέτι, η **κοινολόγηση των βιομετρικών δεδομένων** από την αρχή επιβολής του νόμου στην εταιρεία που της παρέχει το λογισμικό αναγνώρισης προσώπου, έχει ως αποτέλεσμα αφενός την **έλλειψη ελέγχου εκ μέρους της αρχής επί των ευαίσθητων δεδομένων που επεξεργάζεται η ιδιωτική εταιρεία**, και αφετέρου την **αφαίρεση από τα υποκείμενα των δεδομένων της πραγματικής δυνατότητας να ασκήσουν τα δικαιώματά τους**, αφού τις περισσότερες των φορών δεν θα γνωρίζουν ότι τα δεδομένα τους υποβάλλονται σε επεξεργασία (και) με αυτόν τον τρόπο.

Δεν αποτελεί συνεπώς έκπληξη ότι το ΕΣΠΔ στις «Κατευθυντήριες γραμμές 05/2022 *σχετικά με τη χρήση της αναγνώρισης προσώπου τεχνολογίας στον τομέα της επιβολής του νόμου*», υποστήριξε ότι η επεξεργασία βιομετρικών δεδομένων που τελείται στο πλαίσιο επιβολής του νόμου και ερείδεται σε βάση δεδομένων που καταρτίζεται με τη συλλογή δεδομένων προσωπικού χαρακτήρα σε μαζική κλίμακα και κατά τρόπο αδιάκριτο (όπως συμβαίνει στην ιστοσυγκομιδή), χωρίς κανένα περιορισμό ή οποιαδήποτε σαφή σύνδεση μεταξύ των δεδομένων που συλλέγονται και του επιδιωκόμενου σκοπού, **δεν πληροί την απαίτηση της αυστηρής αναγκαιότητας που προβλέπεται από το δίκαιο της Ένωσης**[117].

---

[116] Σε αυτή την περίπτωση, θα πρέπει να εξασφαλίζεται ότι πληρούνται και οι ειδικές προϋποθέσεις που προβλέπει η διάταξη 39 της Οδηγίας αναφορικά με τη διαβίβαση των δεδομένων προσωπικού χαρακτήρα.

[117] European Data Protection Board (EDPB) (2022) 'Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement', σελ. 26 και 48-49. Περαιτέρω, το ΕΣΠΔ επεσήμανε ότι το γενικό συμφέρον της αποτελεσματικότητας κατά την καταπολέμηση των σοβαρών εγκλημάτων, δεν μπορεί αυτό καθ' εαυτό να δικαιολογήσει την επεξεργασία βιομετρικών όταν συλλέγονται αδιακρίτως τεράστιες ποσότητες δεδομένων, διότι κατ' αναλογίαν με τα ανωτέρω, μια τέτοια επεξεργασία δεν θα πληρούσε τις επιταγές αναγκαιότητας και αναλογικότητας. Διαθέσιμο στο: https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf

3.2.2 Η αρχή της διαφάνειας & το δικαίωμα ενημέρωσης

Ακρογωνιαίος λίθος του θεμελιώδους δικαιώματος στην προστασία των δεδομένων προσωπικού χαρακτήρα, αποτελεί **η αρχή της διαφάνειας,** η οποία απαιτεί **δίκαιη και διαφανή επεξεργασία** των προσωπικών δεδομένων, καθώς και **επαρκή πληροφόρηση των υποκειμένων ότι τα δεδομένα τους συλλέγονται και υπόκεινται σε επεξεργασία**. Η επιταγή διαφανούς παροχής πληροφοριών και η εν συνόλω εφαρμογή της εν λόγω αρχής, αποκτά έτι μεγαλύτερη σημασία στο πλαίσιο εφαρμογής των τεχνολογιών αναγνώρισης προσώπου, καθότι, εν τοις πράγμασι, ιδίως όταν η τεχνολογία χρησιμοποιείται στο δημόσιο forum, **η συλλογή και επεξεργασία των εικόνων προσώπου των υποκειμένων διεξάγεται αδιαφανώς και δίχως τη γνώση τους, πολλώ δε μάλλον τη συνεργασία ή τη συγκατάθεσή τους, με αποτέλεσμα τα θιγόμενα πρόσωπα να στερούνται εκ προοιμίου της δυνατότητας ασκήσεως των δικαιωμάτων τους**.

Κατ' αρχάς, η διαφάνεια είναι πρωτεύον συστατικό της πρώτης αρχής προστασίας δεδομένων, όπως αυτή προβλέπεται στο Άρθρο 5§1 στοιχ. α' του Κανονισμού, στην οποία ερείδεται και το δικαίωμα ενημέρωσης των άρθρων 13 και 14 ΓΚΠΔ[118]. Πιο συγκεκριμένα, σε περίπτωση επεξεργασίας δεδομένων προσωπικού χαρακτήρα, θα πρέπει να παρέχονται επαρκείς πληροφορίες στα υποκείμενα, είτε η συλλογή γίνεται απευθείας από τα ίδια είτε από τρίτους, ούτως ώστε να καθίσταται αντιληπτό σε αυτά ότι τα δεδομένα τους *συλλέγονται, χρησιμοποιούνται, λαμβάνονται υπόψη ή υποβάλλονται κατ' άλλο τρόπο σε επεξεργασία, καθώς και σε ποιο βαθμό τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται ή θα υποβληθούν σε επεξεργασία*[119]. Περαιτέρω, η ως άνω αρχή επιβάλλει **η ενημέρωση** του υποκειμένου των δεδομένων να είναι **συνοπτική, διαφανής, κατανοητή, εύκολα προσβάσιμη και διατυπωμένη σε απλή και σαφή γλώσσα**. Ιδιαίτερα όταν τα υποκείμενα των δεδομένων είναι **παιδιά**, η αρχή της διαφάνειας επιτάσσει **η γλώσσα να προσαρμόζεται αναλόγως,** ούτως ώστε το περιεχόμενο να μπορεί να είναι πλήρως αντιληπτό από αυτά[120]. Στο εν λόγω πλαίσιο, ο υπεύθυνος επεξεργασίας επιφορτίζεται με την υποχρέωση να παρέχει στα υποκείμενα **κάθε περαιτέρω απαραίτητη πληροφορία**, λαμβάνοντας υπ' όψιν τα πραγματικά περιστατικά και τις επιμέρους

---

[118] Βλ. και Αιτ. Σκέψη 60 ΓΚΠΔ: «*Οι αρχές της δίκαιης και διαφανούς επεξεργασίας απαιτούν να ενημερώνεται το υποκείμενο των δεδομένων για την ύπαρξη της πράξης επεξεργασίας και τους σκοπούς της. Ο υπεύθυνος επεξεργασίας θα πρέπει να παρέχει στο υποκείμενο των δεδομένων κάθε περαιτέρω πληροφορία που είναι αναγκαία για τη διασφάλιση δίκαιης και διαφανούς επεξεργασίας, λαμβάνοντας υπόψη τις ειδικές συνθήκες και το πλαίσιο εντός του οποίου πραγματοποιείται η επεξεργασία των δεδομένων προσωπικού χαρακτήρα. […]*»

[119] Βλ. Αιτ. Σκέψη 39 ΓΚΠΔ.

[120] Βλ. Αιτ. Σκέψη 58 ΓΚΠΔ.

παραμέτρους της εκάστοτε επεξεργασίας.

Επισημαίνεται ότι στο πλαίσιο του Κανονισμού, το δικαίωμα ενημέρωσης δύναται να περιορίζεται θεμιτά, όταν τα υποκείμενα των δεδομένων διαθέτουν ήδη τις πληροφορίες, είτε η συλλογή γίνεται απευθείας από τα ίδια είτε από άλλες πηγές, ενώ συγκεκριμένα στην περίπτωση συλλογής δεδομένων από άλλες πηγές, τα υποκείμενα των δεδομένων δεν έχουν το δικαίωμα ενημέρωσης, κατ' αρχήν, 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.

Προσέτι, η Οδηγία απηχεί ομοίως τα ανωτέρω προαπαιτούμενα που θέτει ο Κανονισμός, όπως συνάγεται αφενός από την αιτιολογική σκέψη 26, στην οποία προβλέπεται ότι «*κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα θα πρέπει να είναι σύννομη, θεμιτή και διαφανής σε σχέση με τα φυσικά πρόσωπα τα οποία αφορά και να πραγματοποιείται μόνο για συγκεκριμένους σκοπούς που προβλέπονται από το νόμο*», και αφετέρου από την ειδικότερη πρόβλεψη του δικαιώματος ενημέρωσης των υποκειμένων στο άρθρο 13. Τόσο τα άρθρα 13 και 14 του ΓΚΠΔ, όσο το άρθρο 13 της Οδηγίας απαιτούν, κατ' αρχήν, την **ενημέρωση των υποκειμένων των δεδομένων σχετικά με την ταυτότητα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας,** συμπεριλαμβανομένου και του υπευθύνου προστασίας των δεδομένων, **τον σκοπό της επεξεργασίας των δεδομένων τους, τους χρόνους διατήρησης αυτών, το δικαίωμα να ζητούν πρόσβαση στα αποθηκευμένα δεδομένα και τη διαγραφή ή τη διόρθωσή τους, καθώς και το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή**.

Στο πλαίσιο της Οδηγίας, προβλέπεται επιπροσθέτως η παροχή επιπλέον πληροφοριών στο υποκείμενο των δεδομένων σε «*συγκεκριμένες περιπτώσεις*», ρητά κατοχυρωμένες στο εθνικό δίκαιο του κράτους μέλους, οι οποίες δικαιολογούν την πρόσθετη ενημέρωση προκειμένου να εξασφαλιστεί ότι το υποκείμενο δύναται να ασκεί λυσιτελώς τα δικαιώματά του (αρ. 13§2 Οδηγίας). Στην εν λόγω περίπτωση, στο υποκείμενο των δεδομένων παρέχονται πρόσθετες πληροφορίες σχετικά με: α) τη νομική βάση για την επεξεργασία, β) **συμπληρωματικές πληροφορίες, ιδίως όταν τα προσωπικά δεδομένα συλλέγοντα εν αγνοία του υποκειμένου** (π.χ. τον τόπο όπου συλλέχθηκαν τα δεδομένα χωρίς τη γνώση του υποκειμένου των δεδομένων), γ) τη χρονική περίοδο για την οποία θα αποθηκευτούν τα δεδομένα προσωπικού χαρακτήρα ή, όταν αυτό δεν είναι δυνατό, τα κριτήρια που χρησιμοποιήθηκαν για τον καθορισμό της

περιόδου αυτής, δ) κατά περίπτωση, τις κατηγορίες αποδεκτών των δεδομένων προσωπικού χαρακτήρα (συμπεριλαμβανομένων τρίτων χωρών ή διεθνών οργανισμών).

Επισημαίνεται, εν προκειμένω, ότι δεν υπάρχει σαφής ορισμός του εννοιολογικού περιεχομένου των «συγκεκριμένων περιπτώσεων». Το ΕΣΠΔ στις κατευθυντήριές του σχετικά με την χρήση της τεχνολογίας αναγνώρισης προσώπου από τις δημόσιες αρχές, επισημαίνει ότι κατά την αξιολόγηση της συνδρομής του όρου των «συγκεκριμένων περιπτώσεων», θα πρέπει να ληφθούν υπ' όψιν διάφοροι παράγοντες, **μεταξύ των οποίων αν η συλλογή των βιομετρικών δεδομένων διεξήχθη χωρίς τη γνώση του υποκειμένου τους, καθώς αυτός θα ήταν ο μοναδικός τρόπος για να μπορέσει το άτομο να ασκήσει ουσιωδώς και αποτελεσματικά τα δικαιώματά του**[121].

Εν συνεχεία, κατά την εφαρμογή της εν θέματι αρχής στα συστήματα αναγνώρισης προσώπου, χρήσιμες αποδεικνύονται οι τοποθετήσεις του ΕΣΠΔ σχετικά με τη βιντεοεπιτήρηση. Το Συμβούλιο έχει επισημάνει **ότι τα κράτη-μέλη έχουν την υποχρέωση να ενημερώνουν τα άτομα για τη χρήση των συστημάτων σε δημόσιους χώρους**[122]. Ως βέλτιστη πρακτική, το ΕΣΠΔ συστήνει μια **προσέγγιση δύο επιπέδων**: Σε πρώτο επίπεδο, οι σημαντικότερες πληροφορίες θα πρέπει να παρέχονται με τη **χρήση προειδοποιητικών πινακίδων** σε εύλογη απόσταση από τα σημεία που παρακολουθούνται και χωρίς να απαιτείται το άτομο να εισέλθει στον επιτηρούμενο χώρο. Σε αυτές θα αναγράφεται με ακρίβεια και σαφήνεια η ταυτότητα του υπευθύνου επεξεργασίας, ο σκοπός αυτής, τα δικαιώματα των υποκειμένων, η περίοδος διατήρησης και αποθήκευσης των δεδομένων, οι συνέπειες επεξεργασίας και κάθε άλλη πληροφορία που δεν μπορεί να αναμένει ευλόγως το υποκείμενο. Σε δεύτερο επίπεδο, προτείνεται η παροχή λεπτομερούς ενημέρωσης με **κάθε άλλο ευκόλως προσβάσιμο μέσο** (λ.χ. μία αφίσα, ένας ιστότοπος), το οποίο θα πρέπει να αναφέρεται σαφώς στην προειδοποιητική πινακίδα (π.χ. να αναγράφεται το QRcode ή η διεύθυνση ιστοτόπου).

Παρομοίως, **το Συμβούλιο της Ευρώπης υιοθετεί μια πολυεπίπεδη προσέγγιση στις κατευθυντήριες γραμμές του για την αναγνώριση προσώπου**[123]. Οι **υπεύθυνοι επεξεργασίας** καλούνται να παρέχουν στα

---

[121] European Data Protection Board (EDPB) (2022), ο.π. σελ. 21-22.

[122] Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (2020) 'Κατευθυντήριες γραμμές 3/2019 σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω βιντεοσυσκευών'. σελ. 26-27. Διαθέσιμο στο: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_el.pdf

[123] Council of Europe- Convention 108 (2021) ο.π.

υποκείμενα των δεδομένων όλες τις απαραίτητες πληροφορίες σχετικά με την επεξεργασία, λαμβάνοντας υπόψη το **πλαίσιο της συλλογής** των δεδομένων, την **εμβέλεια χρήσης** της τεχνολογίας αναγνώρισης προσώπου, τις **εύλογες προσδοκίες** των υποκειμένων, **τις συνέπειες σε αυτά (ιδίως όταν πρόκειται για ευάλωτα άτομα)**, ενημερώνοντας τα επιπλέον για **τα δικαιώματα και τα ένδικα μέσα και βοηθήματα** που έχουν στη διάθεσή τους.

Προσέτι, το Συμβούλιο της Ευρώπης υπογράμμισε ότι **οι πολιτικές απορρήτου** θα πρέπει να περιλαμβάνουν επιπροσθέτως πληροφορίες σχετικά: α) με την πιθανότητα διαβίβασης των βιομετρικών δεδομένων σε τρίτους (και όταν αυτό συμβαίνει, πληροφορίες σχετικά με την ταυτότητα των τρίτων συμβατικών εταίρων), β) τη διατήρηση, τη διαγραφή ή την από-ταυτοποίηση (de-identification)[124] των δεδομένων αναγνώρισης προσώπου, γ) τους τρόπους επικοινωνίας που είναι διαθέσιμοι για να υποβάλουν τα υποκείμενα ερωτήσεις σχετικά με τη συλλογή, τη χρήση και την κοινολόγηση των δεδομένων τους. Ωστόσο, το Συμβούλιο τόνισε επιπροσθέτως ότι, σε περίπτωση που οι βάσεις δεδομένων δημιουργούνται **από τις αρχές επιβολής του νόμου** για σκοπούς ταυτοποίησης, **η υποχρέωση διαφάνειας θα πρέπει να περιορίζεται αναλογικά ώστε να μην θίγονται οι σκοποί επιβολής του νόμου.**

3.2.2.1 Οι περιορισμοί του δικαιώματος στην ενημέρωση στο πλαίσιο της Οδηγίας

Όσον αφορά ειδικότερα στην Οδηγία, στο άρθρο 13§3 προβλέπεται ότι **τα κράτη μέλη μπορούν να θεσπίζουν εξαιρέσεις στο πλαίσιο της υποχρέωσης ενημέρωσης του υποκειμένου, κυρίως για να αποφευχθεί η πιθανή παρεμπόδιση εν εξελίξει ερευνών, καθώς και για την προστασία της δημόσιας και εθνικής ασφάλειας**. Η Οδηγία επισημαίνει, εντούτοις, ότι κάθε νομοθετικό μέτρο που καθυστερεί, περιορίζει ή παρεμποδίζει την παροχή ενημέρωσης στο υποκείμενο, οφείλει πάντοτε να είναι **αναγκαίο και αναλογικό**, λαμβάνοντας υπ' όψιν τα έννομα συμφέροντα των θιγόμενων προσώπων, κατά τα ήδη αναλυθέντα προαπαιτούμενα του ενωσιακού δικαίου.

Η πρόβλεψη των εν λόγω εξαιρέσεων εκ πρώτης όψεως είναι εύλογη, καθώς

---

[124] «Αποταυτοποίηση» είναι ο γενικός όρος για τη διαδικασία αφαίρεσης προσωπικών πληροφοριών από ένα αρχείο ή σύνολο δεδομένων προκειμένου να μην είναι δυνατή η ταυτοποίηση των υποκειμένων των προσωπικών δεδομένων. Η διαδικασία δεν μηδενίζει τις πιθανότητες ταυτοποίησης, αλλά παράγει σύνολα δεδομένων για τα οποία ο κίνδυνος εκ νέου ταυτοποίησης είναι πολύ μικρός. Βλ. Information and Privacy Commisioner of Ontario (2016) 'De-identification Guidelines for Structured Data'. Διαθέσιμο στο: https://www.ipc.on.ca/wp-content/uploads/2016/08/Deidentification-Guidelines-for-Structured-Data.pdf

πράγματι **καθίσταται πιθανό η αποκάλυψη στο υποκείμενο των δεδομένων ότι τελεί υπό παρακολούθηση μέσω ενός συστήματος αναγνώρισης προσώπου, να υποσκάψει τον ίδιο το θεμελιωτικό λόγο** που χρησιμοποιήθηκε η τεχνολογία. Ωστόσο, όπως προαναφέρθηκε, **οι δημόσιες αρχές συχνά επικαλούνται αορίστως και καταχρηστικώς τις έννοιες της δημόσιας ασφάλειας και του γενικού συμφέροντος** προκειμένου να αιτιολογήσουν τη χρήση της τεχνολογίας, **δίχως να εξετάζουν αν τα μέτρα που λαμβάνουν είναι αναγκαία και αναλογικά** για την εκάστοτε περίπτωση και **δίχως αξιολογούν τις πιθανές κρίσιμες επιπτώσεις στα θιγόμενα πρόσωπα, τα οποία αγνοούν πλήρως ότι τα βιομετρικά δεδομένα τους υπόκεινται σε επεξεργασία,** προκειμένου μάλιστα να εξακριβωθεί η ταυτότητά τους στο πλαίσιο δράσης των αρχών.

Το γεγονός αυτό καθίσταται έτι περαιτέρω ανησυχητικό όταν τα **συστήματα αναγνώρισης προσώπου εγκαθίστανται στο δημόσιο χώρο και χρησιμοποιούνται αδιακρίτως στο σύνολο του πληθυσμού**, καθιστώντας a priori **όλους ανεξαιρέτως τους πολίτες ως «υπόπτους»**. Παραλλήλως, η εκτενής χρήση από τις αρχές δημοσίων βάσεων δεδομένων ή/ και η προμήθεια αμφιβόλου ποιότητας βάσεων δεδομένων από τρίτους, όπως και τα παρατηρηθέντα υψηλά ποσοστά ανακρίβειας της τεχνολογίας σε μη- ελεγχόμενους χώρους, καθιστούν σαφές ότι **οποιοσδήποτε πολίτης εκτίθεται -εν αγνοία του- στον κίνδυνο ταυτοποίησης και -δυνητικά εσφαλμένης- προσαγωγής**. Ο κίνδυνος, όμως, πολλαπλασιάζεται εκθετικά για ανθρώπους που ανήκουν σε μειονότητες, οι οποίοι στοχοποιούνται δυσανάλογα, άλλοτε συνειδητά κι άλλοτε ασυνείδητα, λόγω των προκαταλήψεων που, όπως προεκτέθηκε, είτε φέρουν οι χειριστές των συστημάτων, είτε παρεισφρέουν στους αλγορίθμους.

Όπως ευλόγως συνάγεται, το εν λόγω ζήτημα είναι μείζονος σημασίας καθώς **αποκλείει τα υποκείμενα των βιομετρικών δεδομένων από την άσκηση των δικαιωμάτων τους**, και κατ' επέκταση **αποδυναμώνει την οποιαδήποτε άμυνα του πολίτη έναντι τυχόν αυθαιρεσιών** της δημόσιας αρχής, ή τυχόν εσφαλμένων αποτελεσμάτων των συστημάτων εξαιτίας ανεπαρκώς εκπαιδευμένων αλγορίθμων αναγνώρισης προσώπου**.** Σύμφωνα με την ΑΠΔΠΧ του Αμβούργου, **λόγω της τεχνολογίας αναγνώρισης προσώπου, μια προηγουμένως νομικά καθορισμένη ισορροπία μεταξύ της παρέμβασης των αρχών για τους σκοπούς της επιβολής του νόμου και του δικαιώματος στον πληροφοριακό αυτοκαθορισμό, μεταβάλλεται ανεπίτρεπτα σε βάρος του τελευταίου**[125]. Ομοίως, ο Επίτροπος Βιομετρικών Δεδομένων του Ηνωμένου

[125] Βλ. European Union Agency for Fundamental Rights (2019) 'Facial recognition technology: fundamental rights considerations in the context of law enforcement'. σελ. 25 Διαθέσιμο στο:

Βασίλειου, αναφερόμενος στην τεχνολογία αναγνώρισης προσώπου, τόνισε ότι «εν απουσία ειδικότερου νομικού πλαισίου, **επαφίεται στην αστυνομία να αποφασίσει πότε το δημόσιο όφελος αντισταθμίζει τη «σημαντική επέμβαση στην ιδιωτική ζωή ενός ατόμου»** που προκύπτει από την αναγνώριση προσώπου και άλλους τύπους βιομετρικής ταυτοποίησης»[126].

Βέβαια, όπως έχει ήδη καταστεί σαφές, στο πλαίσιο της ενωσιακής νομοθεσίας για την προστασία των προσωπικών δεδομένων, **οποιοσδήποτε περιορισμός του δικαιώματος ενημέρωσης των υποκειμένων θα πρέπει πάντοτε να ερείδεται στο νόμο και να αιτιολογείται σθεναρά**, όπως και να πληροί τα αυστηρά προαπαιτούμενα που θέτουν οι αρχές της αναγκαιότητας και αναλογικότητας.

3.2.2.2 Ειδικότερα, η αλγοριθμική αδιαφάνεια

Εν συνεχεία, αξίζει να σημειωθεί ότι **η συμμόρφωση** με τις επιταγές της αρχής της διαφάνειας, αλλά και της αρχής της λογοδοσίας, **τίθεται εν αμφιβόλω στο πλαίσιο ανάπτυξης και χρήσης των συστημάτων αναγνώρισης προσώπου, λόγω της ενσωμάτωσης σε αυτά εφαρμογών Τεχνητής Νοημοσύνης**.

Κατ' αρχάς, ως προαναφέρθη (βλ. 2.1.3.) τα αυτόνομα συστήματα τεχνητής νοημοσύνης χαρακτηρίζονται εγγενώς από **το φαινόμενο του «μαύρου κουτιού»** ("black box"), ήτοι είναι ιδιαιτέρως δυσχερές **να αποκρυσταλλωθεί** ακριβώς ο τρόπος και ο λόγος που ο αλγόριθμος κατέληξε στην εκάστοτε απόφαση[127], πολλώ δε μάλλον **να αποτυπωθεί** με τρόπο κατανοητό προς τα υποκείμενα των δεδομένων. Ως εκ τούτου, η απαίτηση διαφάνειας του ευρωπαϊκού κεκτημένου για την προστασία των προσωπικών δεδομένων, συγκρούεται με την δυσχερώς επιτεύξιμη επεξηγησιμότητα των συστημάτων ΤΝ, τα οποία, ως φύσει πολύπλοκα και αδιαφανή, **επιβραδύνουν κάθε απόπειρα αξιολόγησης της διαδικασίας λήψης αποφάσεων και των αποτελεσμάτων αυτής.**

Ωστόσο, **η αρχή της διαφανούς επεξεργασίας και η αρχή της λογοδοσίας εξακολουθούν να δεσμεύουν τον υπεύθυνο επεξεργασίας, θεσπίζοντας παραλλήλως κάποιες αναγκαίες εγγυήσεις.** Μία εκ των εγγυήσεων αυτών,

---

https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf

[126] The Guardian (2019) 'Watchdog criticises 'chaotic' police use of facial recognition', *2019*. Διαθέσιμο στο: https://www.theguardian.com/uk-news/2019/jun/27/watchdog-criticises-chaotic-police-use-of-facial-recognition

[127] Παπαδούλη, Β. (2022) 'Εννοιολογικές Προσεγγίσεις της «Διαφάνειας» στο πεδίο της Τεχνητής Νοημοσύνης υπό ένα νομικό πρίσμα', *Pro Justitia: Ηλεκτρονική Επετηρίδα Νομικής Σχολής ΑΠΘ*, 5(0), σελ. 30–44.

αποτελεί **το δικαίωμα του υποκειμένου σε επεξήγηση της απόφασης που λαμβάνεται αυτοματοποιημένα, λ.χ. από έναν αλγόριθμο αναγνώρισης προσώπου, συμπεριλαμβανομένων των πληροφοριών σε σχέση με τη λογική που ακολουθείται**, κατά τα οριζόμενα σχετικά με την προστασία των υποκειμένων από την αυτοματοποιημένη λήψη αποφάσεων στα άρθρα 13§2 περ. στ', 14§2 περ. ζ', 15§1 περ. η' και 22 ΓΚΠΔ, στην αιτιολογική σκέψη 71 ΓΚΠΔ, καθώς και στα άρθρα 11, 13, 14 της Οδηγίας και στην αιτιολογική σκέψη 38 αυτής (βλ. και κατωτέρω).

Ειδικότερα, επιφυλάσσεται ιδιαίτερη μνεία τόσο στον Κανονισμό όσο και στην Οδηγία, αναφορικά με την περίπτωση της **αυτοματοποιημένης λήψης αποφάσεων**[128], συμπεριλαμβανομένης της κατάρτισης προφίλ[129]. Πιο συγκεκριμένα, προβλέπεται ρητά ότι **το υποκείμενο των δεδομένων θα πρέπει να ενημερώνεται τόσο για την ύπαρξη αυτοματοποιημένης λήψης αποφάσεως, όσο και για τη λογική που ακολουθείται, για τη σημασία αυτής και τις πιθανές εξ αυτής συνέπειες που δύναται να προκύψουν για το ίδιο**. Περαιτέρω, οι αιτιολογικές σκέψεις 71 του ΓΚΠΔ και 38 της Οδηγίας, προβλέπουν ορισμένες επιπρόσθετες εγγυήσεις για το υποκείμενο των δεδομένων, κυρίως δε το δικαίωμα σε ***αιτιολόγηση*** της απόφασης που ελήφθη[130]. Κατ' αυτόν τον τρόπο, επιβάλλεται στον υπεύθυνο επεξεργασίας η αυξημένη υποχρέωση, όχι μόνον να ενημερώσει εκ των προτέρων το υποκείμενο της επεξεργασίας ότι τα δεδομένα του υπόκεινται σε αυτοματοποιημένη διαδικασία, δίνοντας πληροφορίες και για τη λογική αυτής, αλλά έτι περαιτέρω, κατόπιν λήψης της απόφασης από το σύστημα, ο υπεύθυνος υποχρεούται να τεκμηριώσει συγκεκριμένα τη ληφθείσα απόφαση.

Η αλγοριθμική αδιαφάνεια έχει εκκινήσει μια εκτενή συζήτηση ανάμεσα στις ρυθμιστικές αρχές, στους ενδιαφερόμενους φορείς και στους ακαδημαϊκούς, **σχετικά με το περιεχόμενο και τον τρόπο άσκησης του εν λόγω δικαιώματος στις αυτοματοποιημένες αποφάσεις που βασίζονται στην τεχνολογία**

---

[128] Σύμφωνα με την Ομάδα Εργασίας του άρθρου 29, ως αυτοματοποιημένη λήψη αποφάσεων νοείται η διαδικασία με την οποία οι αποφάσεις λαμβάνονται με τεχνικά μέσα, κατά κύριο λόγο χωρίς ανθρώπινη επέμβαση.

[129] αρ. 4 §4 ΓΚΠΔ και αρ. 3 §4 Οδηγίας *«κατάρτιση προφίλ»: οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που συνίσταται στη χρήση δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση ορισμένων προσωπικών πτυχών ενός φυσικού προσώπου, ιδίως για την ανάλυση ή την πρόβλεψη πτυχών που αφορούν την απόδοση στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις, τα ενδιαφέροντα, την αξιοπιστία, τη συμπεριφορά, τη θέση ή τις μετακινήσεις του εν λόγω φυσικού προσώπου.*

[130] Επισημαίνεται ότι υπάρχει διχογνωμία στη θεωρία αναφορικά με την δυνατότητα επιβολής στον υπεύθυνο επεξεργασίας μιας περαιτέρω υποχρέωσης επί τη βάση των αιτιολογικών σκέψεων καθώς αυτές, κατ' αρχήν, δεν έχουν δεσμευτικό χαρακτήρα.

αναγνώρισης προσώπου, ενώ συζητείται ακόμα και η συμβατότητα του δικαιώματος με την τεχνολογία. Επιπλέον, πρόσκομμα στην ικανοποίηση του δικαιώματος ενημέρωσης μπορεί επίσης να αποτελέσει η πιθανή **άρνηση των κατασκευαστών των αλγορίθμων αναγνώρισης προσώπου** να παράσχουν πληροφορίες στα υποκείμενα των δεδομένων, επί τη βάση των **δικαιωμάτων διανοητικής ιδιοκτησίας ή επιχειρησιακών απορρήτων**[131]. Η στάθμιση των συγκρούσεων και των αντικρουόμενων συμφερόντων, θα είναι νευραλγική τόσο για την συμμόρφωση με τις ανωτέρω αρχές, όσο και για την εξασφάλιση της -ουσιαστικής και όχι μόνον τύποις- δυνατότητας των υποκειμένων να ασκούν τα δικαιώματά τους.

3.2.3 Η αρχή της αντικειμενικότητας

Η αρχή της αντικειμενικότητας κατοχυρώνεται στο άρθρο 4§1 στοιχ. α' της Οδηγίας και αποτελεί τον τρίτο πυλώνα της πρώτης αρχής επεξεργασίας δεδομένων του άρθρου 5§1 περ. α' του ΓΚΠΔ.

Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων στις Κατευθυντήριες γραμμές 4/2019 «*σύμφωνα με το άρθρο 25 Προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού*», διευκρίνισε το εννοιολογικό περιεχόμενο της αρχής ως εξής: «*Η αντικειμενικότητα είναι μια θεμελιώδης αρχή σύμφωνα με την οποία τα δεδομένα προσωπικού χαρακτήρα δεν πρέπει να υποβάλλονται σε επεξεργασία κατά τρόπο που είναι* ***αδικαιολόγητα επιζήμιος, εισάγει αθέμιτα διακρίσεις, είναι απρόβλεπτος ή παραπλανητικός για το υποκείμενο των δεδομένων***». *Επίσης, τόνισε ότι κατά την εφαρμογή της εν λόγω αρχής,* ***τα υιοθετούμενα μέτρα θα πρέπει να υποστηρίζουν τα θεμελιώδη δικαιώματα των υποκειμένων,*** *και ιδίως «το δικαίωμα στην ενημέρωση (διαφάνεια), το δικαίωμα παρέμβασης (πρόσβαση, διαγραφή, φορητότητα των δεδομένων, διόρθωση) και το δικαίωμα περιορισμού της επεξεργασίας (το δικαίωμα να μην υπόκειται κάποιος σε αυτοματοποιημένη μεμονωμένη διαδικασία λήψης αποφάσεων και μη εισαγωγής διακρίσεων των υποκειμένων των δεδομένων στις εν λόγω διαδικασίες)*».

Επιπροσθέτως, σύμφωνα με το Γραφείο του Επιτρόπου Πληροφοριών του Ηνωμένου Βασιλείου (ICO), πυρήνας της αρχής της αντικειμενικότητας αποτελεί η απαίτηση η εκάστοτε επεξεργασία δεδομένων **να είναι σύμφωνη με τις εύλογες προσδοκίες** των υποκειμένων και **να μην διενεργείται με τρόπο που θα έχει αδικαιολόγητα δυσμενείς επιπτώσεις σε αυτά**[132]. Κατά την Επίτροπο, η

---

[131] Miyamoto, I. (2020) 'Surveillance Technology Challenges Political Culture of Democratic States', *Hindsight, Insight, Foresight*, σελ. 59.

[132] ICO, 'Guide to the General Data Protection Regulation (GDPR) – Principle (a): Lawfulness, fairness and transparency'. https://ico.org.uk/for-organisations/guide-to-data-

αξιολόγηση της επιτυχούς συμμόρφωσης του υπευθύνου επεξεργασίας με την εν λόγω αρχή εξαρτάται από ποικίλους παράγοντες, όπως ο τρόπος συλλογής των δεδομένων και οι επιπτώσεις στα θιγόμενα άτομα -**ατομικά αλλά και ως μέλη μίας ομάδας. Η εν λόγω προσέγγιση μπορεί να αποτελέσει σημαντικό όπλο στη φαρέτρα των μειονοτήτων που βάλλονται δυσανάλογα από την τεχνολογία αναγνώρισης προσώπου**, θωρακίζοντάς τες ενάντια στη διαιώνιση, κατά τη χρήση των συστημάτων αναγνώρισης προσώπου, των υφιστάμενων συστημικών διακρίσεων, με σκοπό την πρόληψη των βαρύτατων και συχνά ανεπανόρθωτων επιπτώσεων που δύναται να επιφέρει σε αυτές η τεχνολογία.

Οι ανωτέρω ερμηνείες φωτίζουν το εννοιολογικό πλαίσιο της αρχής της αντικειμενικότητας, ωστόσο γίνεται παγίως δεκτό ότι η εν θέματι αρχή χαρακτηρίζεται από ασάφεια. Μάλιστα, μια μερίδα θεωρητικών υποστηρίζει ότι πρόκειται για μια γενική αρχή (a catch- all principle), η οποία μπορεί να αξιοποιηθεί σε περιπτώσεις όπου η επεξεργασία θα ήταν κατά τα λοιπά επιτρεπτή, αλλά εν προκειμένω είναι καταφανώς άδικη[133]. Προσέτι, έχει προταθεί να αποτελέσει η αρχή της αντικειμενικότητας **διορθωτικό εργαλείο** στην περίπτωση που υφίσταται ανισότητα ισχύος μεταξύ του υπευθύνου της επεξεργασίας και των υποκειμένων. Έτι περαιτέρω, η ακαδημαϊκή κοινότητα έχει υποστηρίξει ότι **η προοδευτική ερμηνεία της αρχής της αντικειμενικότητας θα μπορούσε να αποτελέσει χρήσιμο εργαλείο κατά τον περιορισμό των αλγοριθμικών διακρίσεων**, συνιστώντας **δεσμευτική κατευθυντήρια γραμμή**, αφενός για τους προγραμματιστές κατά το σχεδιασμό των αλγορίθμων αναγνώρισης προσώπου, αφετέρου για τους φορείς εκμετάλλευσης κατά τη σύλληψη του τρόπου χρήσης των συστημάτων που ενσωματώνουν την τεχνολογία[134].

Επισημαίνεται, εν προκειμένω, ότι τα αλλεπάλληλα περιστατικά διακρίσεων κατά τη χρήση των συστημάτων αναγνώρισης προσώπου, καταδεικνύουν ότι **η άνευ ετέρου εναπόθεση τήρησης της αρχής της αντικειμενικότητας στον αλγόριθμο δεν είναι επαρκές εχέγγυο δίκαιης λήψης αποφάσεων**· ενώ εκ πρώτης όψεως, οι αποφάσεις του αλγορίθμου φαντάζουν **πιο δίκαιες από τις ανθρώπινες**, ακριβώς διότι δεν παρεμβάλλεται ο ανθρώπινος παράγοντας, η διαμορφωθείσα πραγματικότητα έχει αποδείξει ότι

---

protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/#fairness

[133] Madiega, T., Mildebrath, H. (2021), ο.π. σελ. 13-14.

[134] Hacker, P, 'Teaching fairness to artificial intelligence: Existing and novel strategies against algorithmic discrimination under EU law', (2018), 55, Common Market Law Review, Issue 4, pp. 1172- 1173, Διαθέσιμο σε: https://kluwerlawonline.com/journalarticle/Common+Market+Law+Review/55.4/COLA2018095

καθοριστική παράμετρος της «αντικειμενικότητας» του συστήματος, αποτελεί η λυσιτελής εκπαίδευσή του σε κατάλληλα, συναφή με το σκοπό και αντιπροσωπευτικά σύνολα δεδομένων.

3.2.4 Η αρχή του περιορισμού του σκοπού

Η **αρχή του περιορισμού του σκοπού** αποτελεί μια από τις θεμελιώδεις αρχές του ευρωπαϊκού δικαίου προστασίας δεδομένων, η οποία αντικατοπτρίζεται τόσο στο πρωτογενές ενωσιακό δίκαιο, ήτοι στο άρθρο 8§2 του Χάρτη, όσο και στο ευρωπαϊκό κεκτημένο για την προστασία προσωπικών δεδομένων, ειδικότερα δε στα άρθρα 5§1 στοιχ. β' του ΓΚΠΔ και 4§1 στοιχ. β' της Οδηγίας.

Σύμφωνα με την εν θέματι αρχή, η επεξεργασία των δεδομένων προσωπικού χαρακτήρα θα πρέπει να διεξάγεται **μόνο για καθορισμένους, ρητούς και νόμιμους σκοπούς**. Περαιτέρω, η εν λόγω αρχή επιτάσσει τα δεδομένα προσωπικού χαρακτήρα **να μην υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο με τους –σαφείς και εξαρχής καθορισμένους λεπτομερώς- αυτούς σκοπούς, τους οποίους μάλιστα το υποκείμενο των δεδομένων θα πρέπει να μπορεί να προβλέψει.**

Στο πλαίσιο ανάπτυξης και χρήσης των συστημάτων αναγνώρισης προσώπου, η συμμόρφωση με την αρχή του περιορισμού του σκοπού έχει αποδειχθεί προβληματική. Ειδικότερα, η δυναμική της αλγοριθμικής αναγνώρισης προσώπου **εγείρει κινδύνους αναφορικά με την πιθανή επέκταση της χρήσης των συστημάτων αναγνώρισης προσώπου πέραν του αρχικώς εγκεκριμένου και ελεγχόμενου σκοπού τους.** Πρόκειται για τον κίνδυνο της λεγόμενης «υφέρπουσας διεύρυνσης των λειτουργιών» (**function creep**), ήτοι της χρήσης των προσωπικών δεδομένων για σκοπούς που αρχικά δεν είχαν προβλεφθεί, **δίχως να υφίσταται μια διακριτή, έγκυρη και νόμιμη βάση**. Τούτο μπορεί να συμβεί, επί παραδείγματι: α) με τη χρήση βάσεων δεδομένων που καταρτίζονται **μέσω της ιστοσυγκομιδής**, β) με τη χρήση μιας βάσης δεδομένων **πέραν του αρχικού σκοπού της,** και γ) με την **εκμετάλλευση της διαλειτουργικότητας μεταξύ των πληροφοριακών συστημάτων και την εισαγωγή νέων λειτουργιών σε ένα υπάρχον σύστημα αναγνώρισης προσώπου, λ.χ. με την ενσωμάτωση ενός αλγορίθμου αναγνώρισης προσώπου που χρησιμοποιείται για τον έλεγχο διαβατηρίων, στο σύστημα που χρησιμοποιείται για τις πληρωμές στο ίδιο αεροδρόμιο (και δυνητικά στη συνέχεια σε ολόκληρη την πόλη)**. Αυτή η πρακτική έχει ως αποτέλεσμα να χρησιμοποιούνται τα ευαίσθητα προσωπικά δεδομένα των υποκειμένων πέραν του αρχικού τους σκοπού, του αρχικού τους πλαισίου και με τρόπους που το άτομο **δεν μπορεί ευλόγως να αναμένει**.

Περαιτέρω έχει υποστηριχθεί από τους θεωρητικούς, ότι η ανωτέρω πρακτική μπορεί να αποτελεί μέρος **μιας σκόπιμης στρατηγικής** από τους φορείς που χρησιμοποιούν συστήματα αναγνώρισης προσώπου, οι οποίοι ενδέχεται σε αρχικό στάδιο να βασίζουν τη χρήση της τεχνολογίας σε έναν φαινομενικά νόμιμο σκοπό, και στη συνέχεια να επεκτείνουν κρυφίως και σταδιακά τη χρήση των συστημάτων τους.[135] Έτι ανησυχητικότερο αποτελεί το γεγονός ότι πληθώρα κυβερνήσεων δεν διστάζει να χρησιμοποιεί τα μεταδεδομένα που αντλούνται από τη διασύνδεση βάσεων δεδομένων μεγάλης κλίμακας, στην οποία προβαίνουν με πρόσχημα την καταπολέμηση σοβαρών εγκλημάτων και την προστασία της δημόσιας ασφάλειας.[136]

Αξίζει, επίσης, να σημειωθεί ότι **το ζήτημα παραβίασης της αρχής περιορισμού του σκοπού ανέκυψε από τις πρώτες εφαρμογές της τεχνολογίας αναγνώρισης προσώπου**. Προτού εμφανιστεί στο προσκήνιο το λογισμικό DeepFace και πριν η ιστοσυγκομιδή καθιερωθεί ως πρακτική, η Ομάδα του Άρθρου 29 εντόπισε την προβληματική και υπογράμμισε στη Γνώμη 3/2012 *σχετικά με τις εξελίξεις στις βιομετρικές τεχνολογίες* ότι: οι «*φωτογραφίες στο Διαδίκτυο, σε κοινωνικά δίκτυα, σε επιγραμμικές εφαρμογές διαχείρισης ή ανταλλαγής φωτογραφιών* ***δεν επιτρέπεται να τυγχάνουν περαιτέρω επεξεργασίας για την εξαγωγή βιομετρικών υποδειγμάτων ή για την καταχώρισή τους σε βιομετρικό σύστημα με σκοπό την αυτόματη αναγνώριση των ατόμων στις φωτογραφίες (αναγνώριση προσώπου) χωρίς συγκεκριμένη νομική βάση (π.χ. συγκατάθεση) για τον νέο αυτό σκοπό***. *Εάν υπάρχει* ***νομική βάση γι' αυτόν τον δευτερογενή σκοπό*** *επεξεργασίας, πρέπει επίσης να είναι* ***κατάλληλη, συναφής και όχι υπερβολική σε σχέση με τον εν λόγω σκοπό***. *Εάν το πρόσωπο στο οποίο αναφέρονται τα δεδομένα έχει* ***δώσει τη συγκατάθεσή του*** *ότι οι φωτογραφίες στις οποίες εμφανίζεται μπορούν να τυγχάνουν επεξεργασίας ώστε να είναι δυνατή η αυτόματη επισήμανσή του (tag) σε ένα επιγραμμικό φωτογραφικό λεύκωμα με αλγόριθμο αναγνώρισης προσώπου,* ***η εν λόγω επεξεργασία πρέπει να επιτυγχάνεται κατά τρόπο φιλικό προς την προστασία δεδομένων: τα βιομετρικά δεδομένα που δεν είναι πλέον αναγκαία μετά την επισήμανση των φωτογραφιών με το όνομα, το ψευδώνυμο ή άλλο κείμενο που ορίζεται από το πρόσωπο στο οποίο αναφέρονται τα δεδομένα πρέπει να διαγράφονται. Η δημιουργία μιας μόνιμης βάσης***

---

[135] Salama AbdELminaam D, *κ.ά.* (2020) 'A deep facial recognition system using computational intelligent algorithms', *PLoS ONE*, 15(12 December), σελ. 7. Διαθέσιμο σε: https://doi.org/10.1371/journal.pone.0242269

[136] Smith, M. and Miller, S. (2022) 'The ethical application of biometric facial recognition technology', *AI & Society*, 37, σελ. 173. doi:10.1007/s00146-021-01199-9.

βιομετρικών δεδομένων δεν είναι εκ των προτέρων αναγκαία για τον σκοπό αυτό.[137]

Η ανωτέρω τοποθέτηση υπενθυμίζει ότι η αρχή της αναγκαιότητας πρέπει να διέπει κάθε στάδιο της επεξεργασίας των προσωπικών δεδομένων, ιδίως όταν αυτά ανήκουν στις ειδικές κατηγορίες, τονίζει ότι οφείλεται η συνεκτίμηση των ευλόγων προσδοκιών του υποκειμένου για την τύχη των δημοσίως προσβάσιμων φωτογραφιών του και φωτίζει ένα ακόμα θεμελιώδες προαπαιτούμενο της αρχής του περιορισμού του σκοπού: **την απαγόρευση της απεριόριστης διατήρησης δεδομένων προσωπικού χαρακτήρα**.

3.2.5 Η αρχή της ελαχιστοποίησης των δεδομένων

Η αρχή της ελαχιστοποίησης των δεδομένων συνιστά εκδήλωση της αρχής της αναλογικότητας και επιτάσσει τα προσωπικά δεδομένα που υφίστανται επεξεργασία να είναι, κατ' αρχήν, **πρόσφορα, συναφή και αναγκαία** για τους επιδιωκόμενους σκοπούς. Ειδικότερα, σύμφωνα με την εν λόγω αρχή, η επεξεργασία θα πρέπει **να περιορίζεται στο απολύτως αναγκαίο** (άρ. 5§1 στοιχ. γ' ΓΚΠΔ), **ή να μην είναι υπερβολική** (άρ. 4§1 στοιχ. γ' Οδηγίας), **για την εκπλήρωση του νόμιμου σκοπού που επιδιώκεται**.

Ειδικότερα, ο υπεύθυνος επεξεργασίας, προκειμένου να συμμορφωθεί στα προαπαιτούμενα της ως άνω αρχής, σε πρώτο στάδιο θα πρέπει να αξιολογήσει εάν τα υπό κρίση προσωπικά δεδομένα πρέπει να τύχουν επεξεργασίας για το συγκεκριμένο σκοπό και να εξετάσει εάν αυτός μπορεί να επιτευχθεί με άλλα ηπιότερα μέσα[138], λ.χ. μέσω της επεξεργασίας λιγότερων προσωπικών δεδομένων, μη ευαίσθητων προσωπικών δεδομένων, λιγότερο λεπτομερών και συγκεντρωμένων δεδομένων, ή χωρίς καθόλου επεξεργασία δεδομένων προσωπικού χαρακτήρα. Στη συνεχεία, ο υπεύθυνος επεξεργασίας θα πρέπει να προκαθορίσει ποιες παράμετροι είναι αναγκαίες για την επεξεργασία, και να ελέγχει τακτικά, σε όλα τα στάδια αυτής, ότι τα προσωπικά δεδομένα εξακολουθούν να είναι επαρκή, σαφή και αναγκαία. Διαφορετικά, κατά το ΕΣΠΔ, ο υπεύθυνος επεξεργασίας θα πρέπει να προβαίνει σε διαγραφή, ανωνυμοποίηση, ή ψευδωνυμοποίηση[139].

---

[137] Ομάδα Εργασίας του άρθρου 29 για την προστασία δεδομένων (2012) 'Γνώμη 3/2012 σχετικά με τις εξελίξεις στις βιομετρικές τεχνολογίες'. Διαθέσιμο σε: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_el.pdf

[138] Βλ. Αιτ. Σκέψη 39 ΓΚΠΔ.

[139] Βλ. ΕΣΠΔ 'Κατευθυντήριες γραμμές 4/2019 σύμφωνα με το άρθρο 25 Προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού', ο.π. σελ. 25-26.

Εφαρμόζοντας τις επιταγές της ανωτέρω αρχής, η CNIL στην προαναφερθείσα κρίση της περί της νομιμότητας της πιλοτικής χρήση**ς συστημάτων αναγνώρισης προσώπου στις εισόδους σχολείων**, διέγνωσε ότι **παραβιάζονται οι αρχές της αναλογικότητας και της ελαχιστοποίησης των δεδομένων**, διότι ο στόχος ελέγχου της εισόδου των μαθητών θα μπορούσε να επιτευχθεί **με λιγότερο παρεμβατικά μέσα**, όπως ένα σύστημα ηλεκτρονικών καρτών.

Περαιτέρω, **η ενσωμάτωση των εφαρμογών ΤΝ, και ιδιαίτερα της μηχανικής μάθησης, στα συστήματα αναγνώρισης προσώπου θέτει το ερώτημα αν η τεχνολογία είναι αυτή καθαυτή συμβατή με την αρχή της ελαχιστοποίησης**, ή αν, εκ των πραγμάτων, προσκρούει εγγενώς με αυτή, γεγονός που επεσήμανε και ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων (ΕΕΠΔ)[140]. Ειδικότερα, η μηχανική μάθηση απαιτεί εξ ορισμού την τροφοδότηση των αλγορίθμων με τεράστιους όγκους δεδομένων, προκειμένου να εκπαιδευτούν επαρκώς και να καταστεί δυνατό για το υπολογιστικό σύστημα να δημιουργεί αναλυτικά μοντέλα ικανά να ανιχνεύουν και να ταυτοποιούν ένα ανθρώπινο πρόσωπο. Εξ αντιδιαστολής, η αρχή της ελαχιστοποίησης απαιτεί τόσο η συλλογή όσο και κάθε μετέπειτα επεξεργασία να περιορίζεται στο απολύτως αναγκαίο. Όπως ευλόγως συνάγεται, **η συμμόρφωση με την αρχή αυτή, όχι μόνον είναι δυσχερής, αλλά δύναται να οδηγήσει και σε ανεπαρκώς εκπαιδευμένους αλγορίθμους αναγνώρισης προσώπου**, **με ακόμα υψηλότερα ποσοστά εσφαλμένων αποτελεσμάτων**, τα οποία, συνακόλουθα, θα βλάπτουν δυσανάλογα τα υπό παρακολούθηση υποκείμενα και –έτι μια φορά- θα θέτουν στο απόσπασμα τους μειονοτικούς πληθυσμούς. Επιπροσθέτως, όπως προαναφέρθηκε, τα συστήματα ΤΝ λόγω του πολύπλοκου και αδιαφανούς τρόπου λειτουργίας τους, δεν επιτρέπουν να προσδιοριστεί a priori τι συνιστά «αναγκαίο» για την εκπαίδευσή τους, προκειμένου να προβούν οι υπεύθυνοι επεξεργασίας στις απαιτούμενες ενέργειες ούτως ώστε να εκπαιδευτεί ο αλγόριθμος να αξιολογεί ποια δεδομένα είναι συναφή και σημαντικά για τον εκάστοτε σκοπό. Απόρροια των ανωτέρω, είναι οι κατασκευαστές και οι χρήστες της τεχνολογίας να επιλέγουν συχνά την αδιάκριτη και μαζική συλλογή και επεξεργασία προσωπικών δεδομένων μέσω των αλγορίθμων αναγνώρισης προσώπου, η οποία προσομοιάζει πολύ στη μαζική συλλογή ομάδων δεδομένων και, κατ' επέκταση, στη μαζική παρακολούθηση.

---

[140] Wiewiórowski, W. (2019) 'Facial recognition: A solution in search of a problem? European Data Protection Supervisor', *European Data Protection Supervisor*, 389(8602), σελ. 1–3. Διαθέσιμο στο: https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en

Εν προκειμένω, οφείλει να σημειωθεί ότι **η αρχή της ελαχιστοποίησης δεν αφορά μόνον σε έναν ποσοτικό περιορισμό της ποσότητας των δεδομένων που τροφοδοτούν έναν αλγόριθμο**, αλλά πρεσβεύοντας γενικότερα την αρχή της αναλογικότητας, **κατ' ουσίαν απαιτεί τον περιορισμό του εύρους της παραβίασης στα δικαιώματα της ιδιωτικής ζωής και της προστασίας των προσωπικών.** Τούτο μπορεί να επιτευχθεί, στο πλαίσιο της ΤΝ, με τη λήψη μέτρων εκ μέρους του υπευθύνου επεξεργασίας (λ.χ. ανωνυμοποίησης, ψευδωνυμοποίησης), ώστε να μην καθίσταται εύκολη η ταυτοποίηση των υποκειμένων, και κατ' επέκταση να περιορίζεται ο βαθμός επέμβασης στην ιδιωτική ζωή[141]. Το Γραφείο του Επιτρόπου Πληροφοριών του Ηνωμένου Βασιλείου συστήνει να υιοθετούνται πρακτικές διαχείρισης κινδύνου ικανές να διασφαλίζουν ότι η ελαχιστοποίηση των δεδομένων λαμβάνεται πλήρως υπόψη ήδη **από το στάδιο του σχεδιασμού ενός συστήματος αναγνώρισης προσώπου**, όπως λ.χ. μέσω της μετατροπής των δεδομένων σε λιγότερο «αναγνώσιμες από τον άνθρωπο» μορφές: αντί να αποστέλλονται οι ίδιες οι εικόνες προσώπου στους διακομιστές από τα συστήματα αναγνώρισης προσώπου, προτείνεται να μετατραπούν σε βιομετρικά υποδείγματα απευθείας στη συσκευή των υποκειμένων, και να μεταβιβάζονται υπό αυτή τη μορφή στο μοντέλο για την αναζήτηση στη βάση δεδομένων.[142]

Αξίζει να σημειωθεί, επίσης, ότι η σουηδική ΑΠΔΠΧ, κατά την εξέταση της νομιμότητας χρήσης της τεχνολογίας αναγνώρισης προσώπου στα σχολεία, οδηγήθηκε στο συμπέρασμα πως, **παρόλο που η επεξεργασία ήταν αρκετά περιορισμένη** -αφορούσε λίγους μαθητές και η χρονική περίοδος ήταν σύντομη – **η παραβίαση της αξιοπρέπειας των μαθητών ήταν δυσανάλογη του σκοπού**, επισημαίνοντας παραλλήλως ότι υφίστανται λιγότερο παρεμβατικοί τρόποι καταγραφής της παρουσίας τους στην τάξη[143].

3.2.6 Η αρχή του περιορισμού της περιόδου αποθήκευσης

Στη συνέχεια, τόσο ο ΓΚΠΔ (άρ. 5§1 στοιχ. ε') όσο και η Οδηγία (άρ. 4§1 στοιχ. ε') κατοχυρώνουν **την αρχή του περιορισμού της περιόδου αποθήκευσης**. Η εν λόγω αρχή ορίζει ότι τα δεδομένα προσωπικού χαρακτήρα, δεν πρέπει να διατηρούνται σε μορφή που επιτρέπει την ταυτοποίηση των

---

[141] Βόρρας, Α., Μήτρου, Λ. (2018) 'Τεχνητή νοημοσύνη και προσωπικά δεδομένα - Μια θεώρηση υπό το πρίσμα του Ευρωπαϊκού Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 2016/679', *ΔΙΤΕ (π. ΔΙΜΕΕ)*,(4/2018). σελ. 462.

[142] https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/how-should-we-assess-security-and-data-minimisation-in-ai/#whatdataminimisation

[143] Swedish Data Protection Authority (2019)- Ref. no: DI-2019-2221. Διαθέσιμο σε: https://www.imy.se/globalassets/dokument/beslut/facial-recognition-used-to-monitor-the-attendance-of-students.pdf

υποκειμένων των δεδομένων για χρονικό διάστημα μεγαλύτερο από αυτό που είναι απολύτως αναγκαίο για τους επιδιωκόμενους σκοπούς. Μάλιστα, η Οδηγία (άρθρο 5) επιτάσσει ρητώς ότι τα κράτη- μέλη οφείλουν να προβλέπουν κατάλληλες προθεσμίες για τη διαγραφή ή την περιοδική επαναξιολόγηση της αναγκαιότητας αποθήκευσης των προσωπικών δεδομένων.

Αναφορικά με τον Κανονισμό, χρήσιμα ερμηνευτικά εργαλεία κατά τον προσδιορισμό των επιτρεπτών χρονικών διαστημάτων αποθήκευσης των δεδομένων στο πλαίσιο χρήσης των συστημάτων αναγνώρισης προσώπου, αποτελούν οι κατευθυντήριες γραμμές που έχουν δοθεί από τις Αρχές Προστασίας Δεδομένων αναφορικά με τη βιντεοεπιτήρηση. Ενδεικτικά, η ελληνική ΑΠΔΠΧ στην Οδηγία 1/2011, όρισε ως κανόνα την καταστροφή των δεδομένων **το αργότερο εντός δεκαπέντε (15) εργάσιμων ημερών από τη λήψη των εικόνων προσώπου**, με την επιφύλαξη ειδικότερων διατάξεων για συγκεκριμένες κατηγορίες υπεύθυνων επεξεργασίας, και εφόσον δεν προκύπτει επέλευση συμβάντος που εμπίπτει στον επιδιωκόμενο σκοπό[144]. Προσέτι, το ΕΣΠΔ στις κατευθυντήριες γραμμές 3/2019[145] έθεσε ακόμη μικρότερα όρια, θεωρώντας ότι η διατήρηση των δεδομένων πέραν των **72 ωρών, θα πρέπει να τεκμηριώνεται ειδικά.** Μάλιστα, κατά το Συμβούλιο, σε κάποιες περιπτώσεις, όπως οι καταγραφές παρακολούθησης με σκοπό τον εντοπισμό βανδαλισμών, τα δεδομένα θα πρέπει να διαγράφονται **αυτομάτως** μετά από μερικές ημέρες. Αξίζει να σημειωθεί ότι στις εν λόγω κατευθυντήριες, το ΕΣΠΔ διευκρίνισε περαιτέρω ότι οι υπεύθυνοι επεξεργασίας δεδομένων πρέπει να διασφαλίζουν ότι τα δεδομένα που εξάγονται από μια εικόνα για τη δημιουργία ενός προτύπου, δεν θα είναι υπερβολικά και θα περιέχουν μόνο τις πληροφορίες που απαιτούνται για τον εκάστοτε καθορισμένο σκοπό, αποτρέποντας κατ' αυτόν τον τρόπο κάθε πιθανή περαιτέρω επεξεργασία. Επιπλέον, υπογράμμισε ότι αναλόγως τον σκοπό, **μόλις δημιουργηθεί ένα πρότυπο προσώπου, ανεπεξέργαστα δεδομένα** (όπως η απεικόνιση προσώπου) **μπορεί να χρειαστεί να διαγραφούν για λόγους προστασίας των υποκειμένων των δεδομένων από την ενδεχόμενη εκ νέου δημιουργία βιομετρικών προτύπων εξ αυτών.**[146]

Οι γερμανικές ΑΠΔΠΧ συντάσσονται με τον εν λόγω χρονικό περιορισμό των 72 ωρών, αναφέροντας επιπροσθέτως ότι, κατόπιν του ελέγχου, οποιοδήποτε πλεονάζον υλικό θα πρέπει να διαγράφεται, ενώ αν κριθεί ότι τα δεδομένα πρέπει

---

[144] Βλ. Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (2011), Οδηγία 1/2011 'Χρήση συστημάτων βιντεοεπιτήρησης για την προστασία προσώπων και αγαθών' άρθρο 8. Διαθέσιμο στο: https://www.dpa.gr/sites/default/files/2020-01/ODIGIA_CCTV_FINAL_1_2011.PDF

[145] ΕΣΠΔ (2020), ο.π. σελ. 34.

[146] ΕΣΠΔ (2020), ο.π. σελ. 25.

να διατηρηθούν, θα πρέπει να συντρέχουν πάντοτε ειδικοί σκοποί που δικαιολογούν την επιτήρηση.

3.2.7 Η αρχή της ακρίβειας των δεδομένων

Η αρχή της ακρίβειας των δεδομένων απαιτεί, κατ' αρχήν, τα προσωπικά δεδομένα που υποβάλλονται σε επεξεργασία να είναι ακριβή από πραγματική και χρονική άποψη (άρ. 5§1 στοιχ. δ' ΓΚΠΔ, άρ. 4§1 στοιχ. δ' Οδηγίας). Ειδικότερα δε, απαιτείται τα συλλεχθέντα προσωπικά δεδομένα να ελέγχονται και, αν κριθεί αναγκαίο, να επικαιροποιούνται, ενώ πρέπει να λαμβάνονται και τα κατάλληλα μέτρα για την άμεση διόρθωση ή διαγραφή ανακριβών, σε σχέση με τους επιδιωκόμενους σκοπούς επεξεργασίας, δεδομένων προσωπικού χαρακτήρα.

Η αρχή της ακρίβειας σχετίζεται, κατ' αρχήν, με την **ποιότητα των δεδομένων**. Στο πλαίσιο της τεχνολογίας αναγνώρισης προσώπου, αυτό συνεπάγεται την ανάγκη **οι αλγόριθμοι να εκπαιδεύονται επί συνόλων δεδομένων στα οποία έχει προηγηθεί ένας ποιοτικός έλεγχος ικανός να εξασφαλίσει την ορθότητά τους**. Προκειμένου να καταστεί αυτό δυνατό, οι υπεύθυνοι επεξεργασίας θα πρέπει να διασφαλίζουν, κατ' αρχάς, ότι τα δεδομένα εκπαίδευσης των αλγορίθμων αναγνώρισης προσώπου έχουν εξαχθεί από βιομετρικά πρότυπα τα οποία συλλέχθησαν **υπό κατάλληλες τεχνικές συνθήκες**, οι οποίες επέτρεψαν την **ευκρινή απεικόνιση των προσώπων** των υποκειμένων και, κατ' επέκταση, την **ακριβή εξαγωγή του βιομετρικού υποδείγματος**. Κατ' αυτόν τον τρόπο, δύναται να περιοριστεί ο αριθμός των σφαλμάτων και των ψευδών αντιστοιχιών που οφείλεται στη συλλογή και επεξεργασία εικόνων χαμηλής ποιότητας/ ευκρίνειας.

Έχοντας υπ' όψιν τα ανωτέρω, το Συμβούλιο της Ευρώπης, στις κατευθυντήριες γραμμές του για την αναγνώριση προσώπου υποστήριξε ότι οι υπεύθυνοι ή εκτελούντες την επεξεργασία θα πρέπει κατ' αρχάς να αποφεύγουν την «εσφαλμένη επισήμανση», κάνοντας επαρκείς δοκιμές στα συστήματά τους, ώστε να εντοπίζονται και να εξαλείφονται τυχούσες ανακρίβειες, *ιδιαίτερα όσον αφορά στο χρώμα του δέρματος, στην ηλικία και στο φύλο*, με συνειδητό στόχο να αποτρέπονται ακούσιες διακρίσεις[147].

Περαιτέρω όμως, καθώς το εννοιολογικό πλαίσιο της ακρίβειας δύναται να ερμηνευτεί και ευρύτερα του «απλού» ελέγχου ορθότητας των δεδομένων[148],

---

[147] Council of Europe- Convention 108 (2021) *Guidelines on facial recognition'*. σελ. 15. Διαθέσιμο στο: https://edoc.coe.int/en/artificial-intelligence/9753-guidelines-on-facial-recognition.html

[148] European Union Agency for Fundamental Rights (2019) 'Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights', *FRA Focus*. σελ.

υποστηρίζεται επίσης, ότι οι υπεύθυνοι επεξεργασίας θα πρέπει να φροντίζουν στο πλαίσιο της ανωτέρω αρχής, να τροφοδοτούν τους αλγορίθμους αναγνώρισης προσώπου με **αντιπροσωπευτικά σύνολα δεδομένων**, ήτοι να χρησιμοποιούν σύνολα που δεν είναι ακριβή (ορθά) μόνον εν στενή εννοία, αλλά περαιτέρω, **δεν αντανακλούν τις υφιστάμενες συστημικές προκαταλήψεις.** Αυτό μπορεί να επιτευχθεί λ.χ. με τη χρήση συνθετικών συνόλων δεδομένων που χαρακτηρίζονται από ποικιλομορφία, βασιζόμενα σε φωτογραφίες ή βίντεο που απεικονίζουν άτομα όλων των φύλων, όλων των φυλών, όλων των ηλικιών, και που έχουν συλληφθεί από διαφορετικές γωνίες λήψης[149]. Η εν λόγω προσέγγιση της αρχής της ακρίβειας, μπορεί να αποδειχθεί καθοριστική για τον περιορισμό της διαιώνισης των κοινωνικών διακρίσεων μέσω της «ψηφιοποίησης τους» από τα συστήματα αναγνώρισης προσώπου. Κατ' αυτόν τον τρόπο, η αύξηση της αποτελεσματικότητας των αλγορίθμων και η μείωση των εσφαλμένων αποτελεσμάτων (ψευδών θετικών), θα μειώσει αναλογικά και τη βλάβη που υφίστανται τα άτομα μειονοτικών πληθυσμών, η οποία είναι **ιδιαιτέρως κρίσιμη όταν τα ανακριβή δεδομένα αποθηκεύονται σε βάσεις δεδομένων που χρησιμοποιούν οι διωκτικές αρχές.**

Η ανωτέρω άποψη αντανακλάται και στις κατευθυντήριες γραμμές αναφορικά με την αυτοματοποιημένη λήψη αποφάσεων και την κατάρτιση προφίλ της Ομάδας Εργασίας του άρθρου 29[150], η οποία φαίνεται να υποστηρίζει ότι ακόμη και όταν εξάγονται **ανακριβή συμπεράσματα από ακριβή ακατέργαστα δεδομένα μέσω της χρήσης τεχνητής νοημοσύνης, αυτό μπορεί να παραβιάζει την αρχή της ακρίβειας**. Κατά συνέπεια, η Ομάδα Εργασίας κατέληξε ότι η εν λόγω αρχή **δεν απαιτεί μόνο ότι τα δεδομένα εισόδου είναι ακριβή,** αλλά και ότι οι αλγόριθμοι εκπαιδεύονται σε **αντιπροσωπευτικό σύνολο δεδομένων**, ούτως ώστε να μην υποκρύπτουν προκαταλήψεις. Περαιτέρω, επισημάνθηκε ότι οι υπεύθυνοι επεξεργασίας πρέπει να θεσπίζουν αξιόπιστα μέτρα προκειμένου να διασφαλίζουν, **καθ' όλη τη διάρκεια της επεξεργασίας,** ότι τα δεδομένα που χρησιμοποιούνται είναι ακριβή και επικαιροποιημένα. Σ' αυτό το πλαίσιο αναδεικνύεται και **η κρισιμότητα συμμόρφωσης με την αρχή της διαφάνειας**, καθώς η επαρκής πληροφόρηση του υποκειμένου των δεδομένων είναι άρρηκτα συνδεδεμένη με τη δυνατότητα του να ασκεί τα δικαιώματά του και να διατηρεί τον έλεγχο επί των δεδομένων

9.Διαθέσιμο στο: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-data-quality-and-ai_en.pdf

[149] Council of Europe- Convention 108 (2021), ο.π.

[150] Ομάδα Εργασίας του άρθρου 29 για την προστασία δεδομένων (2018) 'Κατευθυντήριες γραμμές για την αυτοματοποιημένη λήψη αποφάσεων και την κατάρτιση προφίλ για τους σκοπούς του κανονισμού 2016/679'. σελ. 13-14. Διαθέσιμο στο: https://www.dpa.gr/sites/default/files/2020-05/wp251rev01_el.pdf

του, δυνάμενο να υποδεικνύει και να αξιώνει τη διόρθωση τυχόν ανακριβειών (με αποτέλεσμα να βελτιώνεται, ως επακόλουθο, και η ποιότητα του συνόλου των δεδομένων).

3.2.8 Η αρχή της ασφάλειας των δεδομένων

Σύμφωνα με την αρχή της «ακεραιότητας και εμπιστευτικότητας», τα δεδομένα προσωπικού χαρακτήρα πρέπει να υποβάλλονται σε επεξεργασία κατά τρόπο που να διασφαλίζει την ενδεδειγμένη ασφάλεια και προστασία τους, μεταξύ άλλων, από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και από τυχαία απώλεια, καταστροφή ή φθορά, μέσω της εφαρμογής κατάλληλων τεχνικών ή οργανωτικών μέτρων (άρθρο 5§1 στοιχ. στ' ΓΚΠΔ και ως αρχή της ασφάλειας στο άρθρο 4§1 στοιχ. στ' Οδηγίας). Στο πλαίσιο του κοινοτικού κεκτημένου για την προστασία των δεδομένων προσωπικού χαρακτήρα, η έννοια της «ασφάλειας δεδομένων» συναπαρτίζεται από τρεις πτυχές: α) την **εμπιστευτικότητα** (τα δεδομένα είναι προσπελάσιμα μόνο από εξουσιοδοτημένα άτομα), β) την **ακεραιότητα** (προλαμβάνεται η απώλεια ή η παραποίηση των δεδομένων) και γ) τη **διαθεσιμότητα** (τα δεδομένα, όταν απαιτείται, είναι προσπελάσιμα).

Προσέτι, τα άρθρα 32 ΓΚΠΔ και 29 της Οδηγίας προβλέπουν ότι ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία, λαμβάνοντας υπ' όψιν ορισμένες παραμέτρους, όπως *τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων*, θα πρέπει να εφαρμόζουν **αναλογικά τεχνικά και οργανωτικά μέτρα** (π.χ. την ψευδωνυμοποίηση και κρυπτογράφηση των δεδομένων, την τακτική δοκιμή και αξιολόγηση της αποτελεσματικότητας των μέτρων ώστε να διασφαλίζεται η ασφάλεια της επεξεργασίας δεδομένων κ.τ.λ.)[151], **προκειμένου να αποτρέπουν τη γνωστοποίηση δεδομένων προσωπικού χαρακτήρα σε μη εξουσιοδοτημένα πρόσωπα ή/ και την πρόσβαση τους σε αυτά**. Σύμφωνα με τις συστάσεις του ΕΣΠΔ για τη βιντεοεπιτήρηση, ο υπεύθυνος επεξεργασίας θα πρέπει να προστατεύει επαρκώς τόσο το σύστημα, όσο και τα δεδομένα, **σε όλα τα στάδια της επεξεργασίας**, ήτοι κατά την αποθήκευση (δεδομένα σε αδράνεια), τη μετάδοση (δεδομένα σε διαμετακόμιση) και την επεξεργασία (δεδομένα σε

[151] European Union Agency for Fundamental Rights & Council of Europe (2018) *Handbook on European Data Protection Law*, *Publications Office of the European Union*. σελ. 131-134. Διαθέσιμο στο: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf

χρήση)[152], καθώς **και σε όλες τις συσκευές και τους κόμβους μετάδοσης**[153] (λ.χ. κάμερες, μηχανήματα καταγραφής, ασύρματη/ ενσύρματη μετάδοση, δικτυακή ή διαδικτυακή σύνδεση κ.τ.λ.) που συναποτελούν το σύστημα βιντεοεπιτήρησης (και **κατ' αναλογίαν**, το σύστημα αναγνώρισης προσώπου).

Περαιτέρω, κατά το ΕΣΠΔ, προκειμένου να καταστούν τα ανωτέρω δυνατά, ο υπεύθυνος επεξεργασίας θα πρέπει να λαμβάνει **όλα τα απαιτούμενα προληπτικά μέτρα**, μεταξύ άλλων: να διαχωρίζει τα δεδομένα κατά τη διαβίβαση και την αποθήκευση, να αποθηκεύει τα βιομετρικά πρότυπα και τα ακατέργαστα δεδομένα ή τα δεδομένα ταυτότητας σε διακριτές βάσεις δεδομένων, να κρυπτογραφεί τα βιομετρικά δεδομένα, ιδίως δε τα βιομετρικά πρότυπα, να καθορίζει πολιτική για την κρυπτογράφηση και τη διαχείριση των κλειδιών, να ενσωματώνει οργανωτικά και τεχνικά μέτρα για την ανίχνευση απάτης, να συνδέει έναν κωδικό ακεραιότητας με τα δεδομένα (π.χ. με ψηφιακή υπογραφή ή κατακερματισμό) και να απαγορεύει κάθε μη εξουσιοδοτημένη πρόσβαση στα βιομετρικά δεδομένα.

Ειδικότερα ***αναφορικά με την τεχνολογία αναγνώρισης προσώπου***, το ΕΣΠΔ τόνισε ότι η ασφάλεια επεξεργασίας θα πρέπει να βρίσκεται στο επίκεντρο της προσοχής ιδιαιτέρα όταν γίνεται χρήση της τεχνολογίας **από τις αρχές επιβολής του νόμου**, λόγω της εξαιρετικά ευαίσθητης φύσης των δεδομένων που υφίστανται επεξεργασία, καθώς **ο μοναδικός χαρακτήρας των βιομετρικών δεδομένων καθιστά αδύνατη την αλλαγή τους από το υποκείμενο των δεδομένων σε περίπτωση που τεθούν σε κίνδυνο, π.χ. ως αποτέλεσμα παραβίασης δεδομένων (data breach).** Κατά το Συμβούλιο, η αρχή επιβολής του νόμου θα πρέπει να διασφαλίζει ότι **το σύστημα συμμορφώνεται με τα σχετικά πρότυπα ασφαλείας** και να υιοθετεί **μέτρα προστασίας βιομετρικών προτύπων**, όπως το διεθνές πρότυπο **ISO/IEC 24745** που αφορά στην ασφάλεια των πληροφοριών που εξάγονται από βιομετρικά δεδομένα, **πριν από την έναρξη της επεξεργασίας δεδομένων προσωπικού χαρακτήρα**. Η επιταγή αυτή καθίσταται ακόμα πιο επιτακτική, όταν η δημόσια αρχή προμηθεύεται το σύστημα από εξωτερικούς παρόχους (εκτελούντες την επεξεργασία). Στις εν λόγω περιπτώσεις, προκειμένου να εξασφαλιστεί η προστασία των βιομετρικών δεδομένων στον απαιτούμενο βαθμό, τα μέτρα θα μπορούσαν να ενσωματωθούν ως όρος λ.χ. κατά τη διαδικασία σύναψης συμβάσεως με τον πάροχο.[154]

---

[152] ΕΣΠΔ (2020) 'Κατευθυντήριες γραμμές 3/2019 σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω βιντεοσυσκευών'. σελ. 37-39.

[153] Σκόνδρα, Μ. (2020) 'Συστήματα Βιντεοεπιτήρησης , αναγνώριση προσώπου και προστασία προσωπικών δεδομένων', *ΔΙΤΕ (π. ΔΙΜΕΕ)*, (1), σελ. 47.

[154] European Data Protection Board (EDPB) (2022) 'Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement'. σελ. 5, 24 και υποσημείωση 59.

Το Συμβούλιο της Ευρώπης αναγνώρισε ομοίως ότι η αποτυχία επαρκούς προστασίας των βιομετρικών δεδομένων μπορεί να έχει μη αναστρέψιμες επιπτώσεις για τα υποκείμενα των δεδομένων και υιοθέτησε **μία αυστηρότερη προσέγγιση αναφορικά με την τεχνολογία αναγνώρισης προσώπου**. Το Συμβούλιο επεσήμανε την ανάγκη υιοθέτησης τεχνικών και οργανωτικών μέτρων, όπως τα ανωτέρω προεκτεθέντα, τονίζοντας όμως περαιτέρω την **ανάγκη εφαρμογής μέτρων πρόληψης επιθέσεων απέναντι στις οποίες τα συστήματα αναγνώρισης προσώπου έχουν βρεθεί ευάλωτα**, συμπεριλαμβανομένων των **επιθέσεων παρουσίασης προσώπου** (face presentation attacks)[155] και των **επιθέσεων μορφοποίησης** (morphing attacks)[156]. Περαιτέρω, επισημάνθηκε ότι τα υιοθετούμενα μέτρα ασφαλείας οφείλουν να είναι ανάλογα της ευαίσθητης φύσης των δεδομένων, του πλαισίου που χρησιμοποιούνται και του σκοπού της επεξεργασίας, ενώ **θα πρέπει και να εξελίσσονται με την πάροδο του χρόνου, σε ανταπόκριση με τις μεταβαλλόμενες απειλές, τα εντοπισμένα τρωτά σημεία των συστημάτων, και την εξέλιξη της τεχνολογίας**[157]. Επιπλέον, επισημάνθηκε ότι κάθε κρίσιμη για τα θεμελιώδη δικαιώματα των υποκειμένων παραβίαση της ασφαλείας, **θα πρέπει να κοινοποιείται στην εποπτική αρχή και, κατά περίπτωση, στα ίδια τα υποκείμενα**.

Όπως ευλόγως προκύπτει, οι εν λόγω αυξημένες απαιτήσεις του Συμβουλίου, αντανακλούν την ανάγκη ενισχυμένης περιφρούρησης της ασφάλειας των δεδομένων κατά τη χρήση της τεχνολογίας αναγνώρισης προσώπου, και μπορούν να αποτελέσουν σημείο αναφοράς κατά τον σχεδιασμό

Διαθέσιμο στο: https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf

[155] Οι επιθέσεις παρουσίασης περιλαμβάνουν την παρουσίαση ενός βίντεο, μιας φωτογραφίας ή μιας μάσκας στην κάμερα ή στον ψηφιακό αισθητήρα του συστήματος αναγνώρισης προσώπου προκειμένου να τα «ξεγελάσουν» και να αποκτήσουν πρόσβαση μη εξουσιοδοτημένοι χρήστες. Βλ. Abdullakutty, F., Elyan, E. και Johnston, P. (2021) 'A review of state-of-the-art in Face Presentation Attack Detection: From early development to advanced deep learning and multi-modal fusion methods', *Information Fusion*, 75, σσ 55–69. doi:10.1016/J.INFFUS.2021.04.015.

[156] Στις επιθέσεις μορφοποίησης, οι εικόνες προσώπου δύο (ή περισσότερων) ατόμων συνδυάζονται (μορφοποιούνται) και η προκύπτουσα μορφοποιημένη εικόνα προσώπου παρουσιάζεται στη συνέχεια κατά την καταχώριση ως βιομετρική αναφορά. Εάν η μορφοποιημένη εικόνα γίνει αποδεκτή, είναι πιθανό ότι όλα τα άτομα που συνέβαλαν στη μορφοποιημένη εικόνα προσώπου μπορούν να πιστοποιηθούν επιτυχώς έναντι αυτής. Οι επιθέσεις μορφοποίησης αποτελούν έτσι σοβαρή απειλή για τα συστήματα αναγνώρισης προσώπου, ιδίως σε σενάρια όπου η εικόνα αναφοράς παρέχεται συχνά σε εκτυπωμένη μορφή από τον αιτούντα. Βλ. Scherhag, U., Rathgeb, C. και Busch, C. (2022) 'Face Morphing Attack Detection Methods', *Advances in Computer Vision and Pattern Recognition*, σσ 331–349. doi:10.1007/978-3-030-87664-7_15/TABLES/7.

[157] Συμβουλευτική Επιτροπή της Σύμβασης 108 (2021), ο.π. σελ.

και την υιοθέτηση τεχνικών και οργανωτικών μέτρων για την επιτυχή αποφυγή των ενδεχόμενων παραβιάσεων και των πιθανών διαρροών, ιδιαίτερα σε περίπτωση που τα συστήματα αναγνώρισης προσώπου καταστούν διαλειτουργικά.

3.2.9 Η αρχή της λογοδοσίας & τα εργαλεία συμμόρφωσης με αυτή

Σύμφωνα με την αρχή της λογοδοσίας (accountability), ο υπεύθυνος επεξεργασίας δεδομένων επιφορτίζεται με την ευθύνη να αποδεικνύει την κατ' ουσίαν συμμόρφωσή του με το σύνολο των αρχών επεξεργασίας των δεδομένων προσωπικού χαρακτήρα (αρ. 5§2 ΓΚΠΔ και αρ. 4§4 Οδηγίας). Προς διασφάλιση αυτού του σκοπού, ο υπεύθυνος επεξεργασίας οφείλει να σχεδιάζει και να εφαρμόζει, ενεργώς και αδιαλείπτως, τεχνικά και οργανωτικά μέτρα για την προώθηση και εξασφάλιση της προστασίας των δεδομένων, καθ' όλον τον κύκλο ζωής μίας επεξεργασίας (αρ. 24 και αιτιολογική σκέψη 84 ΓΚΠΔ, αρ. 19 και αιτιολογική σκέψη 53 Οδηγίας).

Οι υπεύθυνοι επεξεργασίας πρέπει, δηλαδή, να είναι σε θέση να αποδεικνύουν ανά πάσα στιγμή ότι συμμορφώνονται προς τις διατάξεις περί προστασίας των δεδομένων προσωπικού χαρακτήρα τόσο στα υποκείμενά τους, όσο και στο ευρύ κοινό, αλλά και στις εποπτικές και δικαστικές αρχές. Προσέτι, παρότι κατά τη γραμματική της αποτύπωση η αρχή της λογοδοσίας απευθύνεται μόνο στους υπευθύνους επεξεργασίας, οι εκτελούντες την επεξεργασία οφείλουν επίσης να συμμορφώνονται προς ορισμένες υποχρεώσεις που απορρέουν ευθέως από την αρχή (λ.χ. η τήρηση αρχείου πράξεων επεξεργασίας και ο διορισμός υπευθύνου προστασίας δεδομένων), η οποία διαπνέει το σύνολο των υπό εξέταση νομοθετημάτων και τονίζεται σε πληθώρα διατάξεων[158].

Αν και έχει προταθεί η υιοθέτηση ενός ενδεικτικού καταλόγου μέτρων πρόσφορων να συνεπικουρήσουν τον υπεύθυνο επεξεργασίας στην απόδειξη της ουσιώδους συμμόρφωσης με την ενωσιακή νομοθεσία για την προστασία των προσωπικών δεδομένων, τα υπό κρίση νομοθετήματα δεν εξειδικεύουν τον τρόπο ανταπόκρισης στη λογοδοσία. Εντούτοις, η συνολική επισκόπηση της νομοθεσίας καταδεικνύει ορισμένες σαφείς –κατά περίπτωση- υποχρεώσεις του υπευθύνου της επεξεργασίας ως προς τα απαραίτητα μέτρα οργάνωσης και επίδειξης της συμμόρφωσης, μεταξύ των οποίων:

- η εκτίμηση του αντικτύπου της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα (άρθρα 35 ΓΚΠΔ & 27 Οδηγίας)

[158] European Union Agency for Fundamental Rights & Council of Europe (2018), ο.π. σελ. 171-174.

- η προηγούμενη διαβούλευση και η συνεργασία με την αρμόδια αρχή προστασίας δεδομένων (άρθρα 36 ΓΚΠΔ & 28 Οδηγίας)
- η εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων ασφαλείας (άρθρα 32 ΓΚΠΔ & 29 Οδηγίας)
- η τήρηση αρχείων επεξεργασίας (άρθρο 30 ΓΚΠΔ & άρθρο 24 Οδηγίας)
- η γνωστοποίηση παραβίασης δεδομένων (άρθρα 33-34 ΓΚΠΔ & 30-31 Οδηγίας)
- ο διορισμός υπευθύνου προστασίας δεδομένων (άρθρα 37-39 ΓΚΠΔ & 32-34 Οδηγίας)
- η υιοθέτηση κωδίκων δεοντολογίας και μηχανισμών πιστοποίησης (άρθρα 40-43 ΓΚΠΔ)
- η τήρηση καταχωρίσεων (άρθρο 25 Οδηγίας)

Η υιοθέτηση των κατάλληλων οργανωτικών και τεχνικών μέτρων κρίνεται ad hoc από τον υπεύθυνο επεξεργασίας, κατόπιν συνεκτίμησης της φύσεως, του πεδίου εφαρμογής, του πλαισίου και των σκοπών της επεξεργασίας, πάντοτε **με γνώμονα τους κινδύνους**, την πιθανότητα επέλευσης αυτών και τη σοβαρότητά τους για τα δικαιώματα των υποκειμένων των δεδομένων. Αμφότερα τα νομοθετήματα[159], κατά την επεξήγηση της έννοιας του κινδύνου και της αποτίμησης του μεγέθους αυτού για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, προβαίνουν σε **ιδιαίτερη μνεία στη βλάβη που προκύπτει από την επεξεργασία προσωπικών δεδομένων όταν αυτή μπορεί να οδηγήσει**, μεταξύ άλλων, **σε διακρίσεις** και οιοδήποτε άλλο **σημαντικό οικονομικό ή κοινωνικό μειονέκτημα**, καθώς και όταν **τα υποκείμενα των δεδομένων ενδέχεται να στερηθούν τα δικαιώματα και τις ελευθερίες τους ή τη δυνατότητα άσκησης ελέγχου επί των προσωπικών τους δεδομένων**, όταν υπόκεινται σε επεξεργασία δεδομένα τα οποία αποκαλύπτουν **φυλετική ή εθνοτική καταγωγή, πολιτικά φρονήματα, θρησκεία ή φιλοσοφικές πεποιθήσεις, συνδικαλιστική δράση, όταν γίνεται επεξεργασία γενετικών δεδομένων** (**κατά την Οδηγία και βιομετρικών δεδομένων για την αδιαμφισβήτητη ταυτοποίηση ενός προσώπου**), δεδομένων που αφορούν στην υγεία ή δεδομένων που αφορούν στη σεξουαλική ζωή και στον σεξουαλικό προσανατολισμό ή σε ποινικές καταδίκες και σε αδικήματα, **όταν αξιολογούνται προσωπικές πτυχές, ιδίως όταν επιχειρείται ανάλυση και πρόβλεψη πτυχών για την κατάρτιση προφίλ**, όταν τα υπό επεξεργασία δεδομένα αφορούν σε **ευάλωτα πρόσωπα, ιδίως παιδιά**, όπως και όταν η επεξεργασία περιλαμβάνει **μεγάλο αριθμό δεδομένων** προσωπικού χαρακτήρα και επηρεάζει **μεγάλο αριθμό υποκειμένων δεδομένων**.

[159] Αιτ. Σκέψη 75 ΓΚΠΔ, 51 Οδηγίας.

Εν προκειμένω εύλογα συνάγεται ότι **τα συστήματα αναγνώρισης προσώπου προβαίνουν σε υψηλού κινδύνου επεξεργασία**, ικανή να πραγματώσει **σωρευτικά** την πλειονότητα των ενδεικτικώς αναφερόμενων στη νομοθεσία κρίσιμων απειλών για τα θεμελιώδη δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων. Κατ' αυτόν τον τρόπο καθίσταται σαφές, ότι οι υπεύθυνοι και οι εκτελούντες την επεξεργασία **θα πρέπει να συνεκτιμούν το μέγεθος κινδύνου της τεχνολογίας κατά το σχεδιασμό και την υιοθέτηση των κατάλληλων για την εκάστοτε περίπτωση μέτρων, και να επαναξιολογούν καθ' όλη τη διάρκεια της επεξεργασίας τα ληφθέντα μέτρα**, προκειμένου να επιδείξουν -και να είναι σε θέση να αποδείξουν- επιτυχώς και ουσιωδώς την απαιτούμενη συμμόρφωση.

Προκειμένου να επιβοηθηθεί ο υπεύθυνος επεξεργασίας στην διεκπεραίωση της υπό αναφορά υποχρέωσης λογοδοσίας, έχουν προταθεί επιπροσθέτως τα εξής μέτρα: η έγκαιρη χαρτογράφηση εργασιών επεξεργασίας, η θέσπιση εσωτερικών πολιτικών προστασίας δεδομένων, η υιοθέτηση πρόσφορων και αποτελεσματικών διαδικασιών και εργαλείων εφαρμογής των πολιτικών, ο έλεγχος και η αξιολόγηση της αποτελεσματικότητάς τους καθώς και η πρόβλεψη διαδικασιών αντιμετώπισης της ενδεχόμενης ελλιπούς συμμόρφωσης ή/ και παραβίασης των δεδομένων, η θέσπιση διαδικασιών για την ανταπόκριση στα αιτήματα των υποκειμένων, η οργάνωση εσωτερικού μηχανισμού χειρισμού των καταγγελιών κ.α.[160]

Όσον αφορά ειδικότερα στις εφαρμογές τεχνητής νοημοσύνης, στα ανωτέρω μέτρα θα πρέπει να συμπεριλαμβάνονται **έλεγχοι για την επάρκεια** και την **ποιότητα των δεδομένων** που τροφοδοτούν τον αλγόριθμο, δοκιμές της απόδοσης του λογισμικού και εκτίμηση του ευλόγου των αποτελεσμάτων, καθώς και ειδικότερα εξέταση για την ενδεχόμενη εμφιλοχώρηση, κατά το σχεδιασμό ή κατά την εφαρμογή, πάσης φύσεως προκαταλήψεων και κοινωνικών αδικιών.[161]

Εντούτοις, η εργαλειοποίηση των αλγορίθμων στην τεχνολογία αναγνώρισης προσώπου θέτει έτι μία φορά προσκόμματα στην εκπλήρωση των προϋποθέσεων της νομοθεσίας. Κατ' αρχάς, **το «φαινόμενο του μαύρου κουτιού», όπως προαναφέρθηκε, συσκοτίζει τις προσπάθειες του υπευθύνου επεξεργασίας τόσο να λάβει τα κατάλληλα οργανωτικά και τεχνικά μέτρα**

---

[160] Μήτρου Λ. (2021) 'Οι υποχρεώσεις του υπευθύνου επεξεργασίας, '*Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων (GDPR), Νομική Διάσταση και πρακτική εφαρμογή- Β' Έκδοση*'. Κοτσαλής Λ. κ.ά. Νομική Βιβλιοθήκη. σελ. 169-176.

[161] EPRS | European Parliamentary Research Service (2020) *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*. Διαθέσιμο στο: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf

που θα διασφαλίζουν την τήρηση των κανόνων προστασίας δεδομένων στο πλαίσιο των πράξεων επεξεργασίας, όσο και να αποδείξει τη συμμόρφωσή του προς την επιταγή αυτή. Η εγγενής πολυπλοκότητα και αδιαφάνεια της τεχνητής νοημοσύνης καθιστά δυσχερή -έως αδύνατη- κάθε προσπάθεια κατανόησης του εσωτερικού τρόπου λειτουργίας ενός συστήματος μηχανικής μάθησης, πόσω μάλλον σε βαθμό που να καθίσταται δυνατός ο σαφής προσδιορισμός της αλγοριθμικής λογικής, η οποία βασίζει σε στατιστικούς συσχετισμούς ενός τεράστιου όγκου δεδομένων τη λήψη της εκάστοτε απόφασης. Στο πλαίσιο αυτό, η ανταπόκριση στην αρχή της λογοδοσίας συγκρούεται με την ίδια τη φύση της τεχνητής νοημοσύνης· εντούτοις, ταυτοχρόνως, **τα συστήματα αναγνώρισης προσώπου, καθότι σχεδόν συνεπάγονται εγγενώς την επέλευση κρίσιμων κινδύνων** για τα υποκείμενα των δεδομένων, απαιτούν **έτι ενισχυμένη λογοδοσία** όλων των εμπλεκόμενων μερών.

Εν προκειμένω όμως ανακύπτει μία ακόμα προβληματική από την ενσωμάτωση των αλγορίθμων στα συστήματα αναγνώρισης προσώπου, η οποία αφορά στην **εξακρίβωση της ταυτότητας των υπευθύνων επεξεργασίας και των εκτελούντων την επεξεργασία, καθώς και στον προσδιορισμό και την έκταση της ευθύνης τους (liability)**[162]. Κατ' αρχάς, το κοινοτικό κεκτημένο για την προστασία των προσωπικών δεδομένων προβλέπει ότι η παράνομη επεξεργασία δεδομένων προσωπικού χαρακτήρα συνεπάγεται ευθύνη για αμφότερους τον υπεύθυνο και τον εκτελούντα την επεξεργασία δεδομένων. Εντούτοις, η τεχνητή νοημοσύνη και η αυτοματοποιημένη λήψη αποφάσεων στην οποία προβαίνουν οι αλγόριθμοι, **εγείρουν ερωτήματα σχετικά με το ποιος είναι υπεύθυνος για παραβάσεις οι οποίες έχουν αντίκτυπο στα θεμελιώδη δικαιώματα και στις ελευθερίες των υποκειμένων των δεδομένων, σε περίπτωση που αυτές, λόγω της αλγοριθμικής αδιαφάνειας και του όγκου των υπό επεξεργασία δεδομένων, δεν μπορούν να αποδοθούν με ακρίβεια σε κάποιο από τα εμπλεκόμενα μέρη.**

Περαιτέρω, όταν η τεχνητή νοημοσύνη και οι αλγόριθμοι θεωρούνται προϊόντα, τίθενται κρίσιμα ζητήματα αναφορικά με την εφαρμογή του κατάλληλου νομοθετικού πλαισίου επί επέλευσης ζημίας, ιδίως δε της κρίσης αν η παραβίαση πρέπει να αντιμετωπιστεί βάσει της **προσωπικής ευθύνης του υπευθύνου/ εκτελούντα την επεξεργασία**, όπως αυτή ρυθμίζεται στην ευρωπαϊκή νομοθεσία για την προστασία προσωπικών δεδομένων, **ή βάσει της ευθύνης λόγω ελαττωματικών προϊόντων**, η οποία δεν ρυθμίζεται από το συγκεκριμένο πλέγμα διατάξεων και, ως εκ τούτου, δεν προασπίζει τα

[162] European Union Agency for Fundamental Rights & Council of Europe (2018), ο.π. σελ. 355- 356.

δικαιώματα των υποκειμένων των βιομετρικών δεδομένων στον ίδιο βαθμό και στην ίδια έκταση.

3.2.9.1 Ειδικότερα, η εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα & η προηγούμενη διαβούλευση με την εποπτική αρχή

Η εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων (άρθρο 35 ΓΚΠΔ & 27 Οδηγίας, εφεξής: ΕΑΠΔ), αποτελεί καίριο εργαλείο συμμόρφωσης με την αρχή της λογοδοσίας. Πρόκειται για μια διαδικασία που έχει σχεδιαστεί προκειμένου να περιγράψει την επεξεργασία των δεδομένων προσωπικού χαρακτήρα, να αξιολογήσει την αναγκαιότητα και αναλογικότητά της και να συνδράμει κατά την διαχείριση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, μέσω της αξιολόγησής τους και του καθορισμού μέτρων για την αντιμετώπισή τους[163].

Στο πλαίσιο του Κανονισμού, η διεξαγωγή ΕΑΠΔ αποτελεί **εύλογη υποχρέωση του υπευθύνου επεξεργασίας όταν μετέρχεται της τεχνολογίας αναγνώρισης προσώπου**, καθώς η επεξεργασία εμπίπτει σχεδόν πάντοτε σε κατ' ελάχιστον μία εκ των κάτωθι περιπτώσεων:

- είναι πιθανόν να προκαλέσει μεγάλο κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων (άρ. 35§1 ΓΚΠΔ), όπως εκτέθηκε αναλυτικά στο κεφάλαιο 2 της παρούσας
- **αφορά σε μεγάλης κλίμακας επεξεργασία των ειδικών κατηγοριών δεδομένων που αναφέρονται στο άρθρο 9§1** (αρ. 35§3 περ. β' ΓΚΠΔ)
- **εμπερικλείει συχνά τη συστηματική και εκτενή αξιολόγηση προσωπικών πτυχών σχετικά με φυσικά πρόσωπα, η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία, συμπεριλαμβανομένης της κατάρτισης προφίλ**, και στην οποία βασίζονται αποφάσεις που παράγουν έννομα αποτελέσματα σχετικά με το φυσικό πρόσωπο ή ομοίως επηρεάζουν σημαντικά το φυσικό πρόσωπο (άρθρο 35§3 περ. α' ΓΚΠΔ)
- χρησιμοποιείται ευρέως για τη **συστηματική παρακολούθηση δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα** (άρθρο 35§3 περ. γ' ΓΚΠΔ)

Η υποχρέωση εκτίμησης αντικτύπου κατά την χρήση συστημάτων αναγνώρισης προσώπου καθίσταται, έτι περαιτέρω, προφανής από την εκδοθείσα

[163] Μήτρου Λ. (2021), ο.π. σελ. 465.

κατ' άρθρο 35§4 ΓΚΠΔ, υπ' αριθ. 65/2018 απόφαση της ελληνικής ΑΠΔΠΧ, σύμφωνα με την οποία μεταξύ των επεξεργασιών που περιλαμβάνονται στον κατάλογο πράξεων που απαιτούν ΕΑΠΔ, συμπεριλαμβάνεται και η: «***συστηματική και σε μεγάλη κλίμακα επεξεργασία για την παρακολούθηση, την παρατήρηση ή τον έλεγχο των φυσικών προσώπων με χρήση δεδομένων που συλλέγονται μέσω συστημάτων βιντεοεπιτήρησης ή μέσω δικτύων ή με οποιοδήποτε άλλο μέσο σε δημόσιο χώρο, δημοσίως προσβάσιμο χώρο ή ιδιωτικό χώρο προσιτό σε απεριόριστο αριθμό προσώπων***. *Περιλαμβάνει την παρακολούθηση των κινήσεων της τοποθεσίας/γεωγραφικής θέσης σε πραγματικό ή μη χρόνο ταυτοποιημένων ή ταυτοποιήσιμων φυσικών προσώπων.* ***Σχετικά παραδείγματα είναι η χρήση καμερών σε εμπορικό κέντρο ή σε σταθμούς μέσων μαζικής μεταφοράς, ή η επεξεργασία δεδομένων θέσης των επιβατών σε αεροδρόμιο ή σε μέσα μαζικής μεταφοράς***.»[164]

Εν συνεχεία, στο πλαίσιο της Οδηγίας (αρ. 27§1), η ΕΑΠΔ καθίσταται ακόμη πιο επιτακτική και η κρισιμότητα των επαπειλούμενων για τα θεμελιώδη δικαιώματα των υποκειμένων, κινδύνων από την επεξεργασία που διενεργείται στο πλαίσιο επιβολής του νόμου, καθιστά την διεξαγωγή της σχεδόν αυτονόητη. Σύμφωνα το ΕΣΠΔ[165], **όταν η τεχνολογία αναγνώρισης προσώπου χρησιμοποιείται από τις δημόσιες αρχές, ο υπεύθυνος επεξεργασίας οφείλει απαραιτήτως** να προβαίνει σε εκτίμηση αντικτύπου **πριν από τη χρήση των τεχνολογιών αναγνώρισης προσώπου**, η οποία θα πρέπει να περιλαμβάνει κατ' ελάχιστον «*τη γενική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας, την αξιολόγηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε σχέση με τους σκοπούς, την αξιολόγηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, τα μέτρα που προβλέπονται για την αντιμετώπιση των εν λόγω κινδύνων, εγγυήσεις, μέτρα ασφαλείας και μηχανισμούς για τη διασφάλιση της προστασίας των δεδομένων προσωπικού χαρακτήρα και την απόδειξη της συμμόρφωσης*». Περαιτέρω, το ΕΣΠΔ συνιστά ως επιπλέον μέτρο ενίσχυσης της εμπιστοσύνης και της διαφάνειας, **τη δημοσιοποίηση των αποτελεσμάτων αυτών των αξιολογήσεων**, ή τουλάχιστον των κύριων ευρημάτων και συμπερασμάτων της εκτίμησης αντικτύπου.

Περαιτέρω, **ο υπεύθυνος επεξεργασίας οφείλει να διαβουλεύεται με την εποπτική αρχή πριν προβεί στην επεξεργασία**, κατ' αρχήν, όταν η ΕΑΠΔ υποδεικνύει ότι η επεξεργασία θα είχε ως αποτέλεσμα υψηλό κίνδυνο ελλείψει

---

[164] Ελληνική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (2018) *Απόφαση 65/2018*. Διαθέσιμη στο: https://www.dpa.gr/sites/default/files/2019-09/65_2018anonym.pdf σελ. 8.

[165] European Data Protection Board (EDPB) (2022), ο.π. σελ. 24-25.

μέτρων μετριασμού του κινδύνου (άρθρο 36 §1 ΓΚΠΔ & άρθρο 28§1 Οδηγίας). Καθώς, όπως έχει καταστεί σαφές, η ανάπτυξη και χρήση της τεχνολογίας αναγνώρισης προσώπου ενέχει εγγενώς υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, ο υπεύθυνος ή ο εκτελών την επεξεργασία θα πρέπει να συμβουλεύεται απαραιτήτως την αρμόδια εποπτική αρχή, πριν από την ανάπτυξη του συστήματος. Όπως ευλόγως συνάγεται, **ο ρόλος των ΑΠΔΠΧ**, ως ανεξάρτητων φορέων, είναι **καθοριστικός για τη διασφάλιση των θεμελιωδών δικαιωμάτων των υποκειμένων απέναντι στην υψηλή παρεμβατικότητα της τεχνολογίας αναγνώρισης προσώπου**.

Αξίζει να σημειωθεί εν προκειμένω, ότι **ήδη έχουν καταγραφεί προσπάθειες για τη διενέργεια εκτίμησης αντικτύπου σε αρκετές δοκιμές της τεχνολογίας αναγνώρισης προσώπου στο πλαίσιο δράσης των αστυνομικών αρχών**. Στη Γερμανία πριν την πιλοτική χρήση της τεχνολογίας, καταρτίστηκε σε συνεργασία με την ΑΠΔΠΧ σχέδιο προστασίας των προσωπικών δεδομένων. Επίσης, ΕΑΠΔ δημοσιεύθηκαν από την αστυνομία της Νότιας Ουαλίας και τη μητροπολιτική αστυνομία του Λονδίνου, ενώ και η αστυνομία της Γαλλίας ενημέρωσε τη CNIL σχετικά με τα σχέδιά της λίγες εβδομάδες προτού χρησιμοποιήσει συστήματα αναγνώρισης προσώπου[166].

3.2.9.2 Ειδικότερα η προστασία δεδομένων από το σχεδιασμό και εξ ορισμού

Η νομοθεσία της ΕΕ για την προστασία των δεδομένων προσωπικού χαρακτήρα, απαιτεί από τους υπευθύνους επεξεργασίας, στο πλαίσιο της συμμόρφωσής τους προς τις επιταγές της, να προστατεύουν τα προσωπικά δεδομένα **ήδη από τον σχεδιασμό**, ήτοι να λαμβάνουν εγκαίρως, από το στάδιο σχεδιασμού (και δια του σχεδιασμού) μέτρα, για την ενσωμάτωση εγγυήσεων ικανών να διασφαλίζουν την προστασία της πληροφοριακής ιδιωτικότητας των υποκειμένων των δεδομένων (άρθρο 20 Οδηγίας & 25 ΓΚΠΔ). Άλλως, ο σχεδιασμός, η λειτουργία και η διαχείριση των τεχνολογιών επεξεργασίας πληροφορίας και των πληροφοριακών συστημάτων, θα πρέπει να ανταποκρίνονται σε **προδιατυπωμένες** ανάγκες και απαιτήσεις, προκειμένου να καθίσταται ουσιωδώς δυνατή η λυσιτελής κάλυψή τους. Τα οργανωτικά και τεχνικά μέσα που επιλέγει ο υπεύθυνος επεξεργασίας προς αυτό το σκοπό (λ.χ. ψευδωνυμοποίηση), θα πρέπει να εφαρμόζονται **τόσο κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας, όσο και καθ' όλη τη διάρκεια αυτής**, ενώ θα πρέπει να έχουν σχεδιαστεί ώστε να είναι πρόσφορα για την πραγμάτωση των αρχών επεξεργασίας δεδομένων, κυρίως δε της αρχής της ελαχιστοποίησης,

[166] European Union Agency for Fundamental Rights (2019) 'Facial recognition technology: fundamental rights considerations in the context of law enforcement', ο.π. σελ. 26.

και για την ενσωμάτωση των εγγυήσεων προστασίας καθ' όλο τον κύκλο ζωής της επεξεργασίας.

Κατά συνέπεια, **όταν σχεδιάζεται ένα σύστημα αλγοριθμικής αναγνώρισης προσώπου, και προτού ακόμη ξεκινήσει η επεξεργασία των βιομετρικών δεδομένων**, ο υπεύθυνος επεξεργασίας θα πρέπει να προβαίνει στην **κατάρτιση μιας ολοκληρωμένης ανάλυσης**, ενός σχεδίου και μιας διαδικασίας για την προστασία των δεδομένων των υποκειμένων, προκειμένου να αποσοβεί τον κίνδυνο παραβίασης των ευαίσθητων αυτών πληροφοριών, ρυθμίζοντας κατάλληλα τις τεχνολογικές εφαρμογές που αναπτύσσει και χρησιμοποιεί.

Προσέτι, αμφότερα τα υπό κρίση νομοθετήματα, επιφυλάσσουν ιδιαίτερη μνεία στην πραγμάτωση της αρχής της ελαχιστοποίησης εντός του ανωτέρω πλαισίου. Ειδικότερα, απαιτείται η εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων για τη διασφάλιση ότι, εξ ορισμού, μόνο δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για κάθε συγκεκριμένο σκοπό της επεξεργασίας υποβάλλονται σε αυτή. Τα μέτρα αυτά θα πρέπει να αφορούν στον όγκο των δεδομένων προσωπικού χαρακτήρα που συλλέγονται, στην έκταση της επεξεργασίας, στην περίοδο αποθήκευσης και στην προσβασιμότητά τους. Ως εκ τούτου, η ενσωμάτωση των εφαρμογών τεχνητής νοημοσύνης στην τεχνολογία αναγνώρισης προσώπου, εγείρει ερωτηματικά ως προς το βαθμό που το «φαινόμενο του μαύρου κουτιού» επηρεάζει –και επιτρέπει- τη συμμόρφωση στην υπό κρίση υποχρέωση.[167]

Σε κάθε περίπτωση, ο υπεύθυνος επεξεργασίας καλείται πριν την χρήση ενός αλγορίθμου και καθ' όλη τη διάρκεια αυτής, να εφαρμόζει τα καταλληλότερα για τον εκάστοτε σκοπό μέτρα, να αξιολογεί και να τεκμηριώνει τις απειλούμενες επιπτώσεις στα υποκείμενα των δεδομένων, ως μονάδες αλλά και ως μέρος του κοινωνικού συνόλου, και να εντοπίζει τις ειδικές απαιτήσεις του εκάστοτε συστήματος, για να εξασφαλισθεί αφενός η ηθική και δίκαιη ανάπτυξη και χρήση του, και αφετέρου ο σεβασμός στα θεμελιώδη ανθρώπινα δικαιώματα.[168] Προκειμένου να πληρούται η εν λόγω απαίτηση, το ΕΣΠΔ συστήνει ειδικότερα για την περίπτωση που μία αρχή επιβολής του νόμου προτίθεται να προμηθευτεί την τεχνολογία αναγνώρισης προσώπου από **εξωτερικούς παρόχους**, να λαμβάνονται **αντίστοιχα μέτρα**, για παράδειγμα μέσω της σύναψης συμβάσεων, ώστε να διασφαλίζεται στο μέγιστο ότι η τεχνολογία που

[167] EPRS (2020), ο.π. σελ 67- 68.
[168] Βόρρας, Α., Μήτρου, Λ., (2018) ο.π. σελ. 465.

θα χρησιμοποιηθεί θα αναπτυχθεί με πλήρη σεβασμό στην αρχή της προστασίας δεδομένων από το σχεδιασμό και εξ ορισμού[169].

3.2.9.3 Ειδικότερα, οι καταχωρίσεις

Η Οδηγία προβλέπει ένα πρόσθετο επωφελές μεθοδολογικό εργαλείο ώστε ο υπεύθυνος ή ο εκτελών της επεξεργασίας να είναι σε θέση να αποδείξει τη νομιμότητα αυτής, καθώς και να διασφαλίζει αποτελεσματικά την ακεραιότητα των δεδομένων και την ασφάλειας αυτών: την τήρηση αρχείων καταχωρίσεων.

Τα αρχεία καταχώρισης του συστήματος αποτελούν ένα πολύ χρήσιμο εργαλείο και μια σημαντική εγγύηση για την επαλήθευση της νομιμότητας της επεξεργασίας, τόσο εσωτερικά (ήτοι, ως αυτοέλεγχος) όσο και από τις εποπτικές αρχές. Ειδικότερα, σύμφωνα με το άρθρο 25 της Οδηγίας, στα συστήματα αυτοματοποιημένης επεξεργασίας θα πρέπει να τηρούνται αρχεία καταχωρίσεων, κατ' ελάχιστον για τις ακόλουθες πράξεις επεξεργασίας: *συλλογή, μεταβολή, αναζήτηση πληροφοριών, κοινολόγηση, περιλαμβανομένων των διαβιβάσεων, συνδυασμό και διαγραφή*. Επιπλέον, τα αρχεία καταχωρίσεων της αναζήτησης πληροφοριών και της κοινολόγησης, θα πρέπει να καθιστούν δυνατή τη διαπίστωση της αιτιολόγησης, της ημερομηνίας και της ώρας των εν λόγω πράξεων και, στο μέτρο του εφικτού, την ταυτοποίηση του προσώπου που αναζήτησε πληροφορίες ή κοινολόγησε δεδομένα προσωπικού χαρακτήρα, καθώς και την ταυτότητα των αποδεκτών τους. Κατά το ΕΣΠΔ, **στο πλαίσιο χρήσης των συστημάτων αναγνώρισης προσώπου από τις δημόσιες αρχές, συνιστάται, πέραν των ανωτέρω, και η καταχώριση των ακόλουθων πράξεων επεξεργασίας**:

- Αλλαγών στη βάση δεδομένων αναφοράς (προσθήκη, διαγραφή ή ενημέρωση). Στην καταχώριση θα πρέπει να διατηρείται αντίγραφο της σχετικής (προστιθέμενης, διαγραφόμενης ή ενημερωμένης) εικόνας, όταν δεν είναι δυνατόν να επαληθευτεί με άλλο τρόπο η νομιμότητα ή το αποτέλεσμα των πράξεων επεξεργασίας.
- Προσπαθειών ταυτοποίησης ή επαλήθευσης, συμπεριλαμβανομένου του αποτελέσματος και του βαθμού εμπιστοσύνης (confidence score). Εν προκειμένω, θα πρέπει να εφαρμόζεται η αρχή της ελαχιστοποίησης, έτσι ώστε να διατηρείται στα αρχεία καταγραφής μόνο το αναγνωριστικό της εικόνας από τη βάση δεδομένων αναφοράς, αντί να αποθηκεύεται η ίδια η εικόνα αναφοράς. Η καταγραφή των βιομετρικών δεδομένων εισόδου, θα πρέπει να

[169] ΕΣΠΔ (2022), ο.π.

αποφεύγεται, εκτός αν υφίσταται ανάγκη (π.χ. μόνο σε περιπτώσεις ταυτοποίησης).

- Του αναγνωριστικού του χρήστη που υπέβαλε αίτημα ταυτοποίησης ή επαλήθευσης.

Περαιτέρω, επισημάνθηκε ότι τα προσωπικά δεδομένα που αποθηκεύονται στα αρχεία καταχωρίσεων των συστημάτων, θα πρέπει να υπόκεινται σε αυστηρούς περιορισμούς σκοπού, ενώ υπογραμμίστηκε και η ανάγκη να εφαρμόζονται μέτρα ασφαλείας για τη διασφάλιση της ακεραιότητας των αρχείων καταχώρισης. Ως προς αυτό το σκοπό, το ΕΣΠΔ συνιστά ανεπιφύλακτα τη χρήση συστημάτων **αυτόματης παρακολούθησης**, αφενός για τον εντοπισμό καταχρήσεων των εν λόγω αρχείων, αφετέρου για την εξασφάλιση της εκάστοτε επιβεβλημένης χρονικής περιόδου διατήρησης δεδομένων για τα αρχεία καταγραφής.

3.2.10 Τα δικαιώματα των υποκειμένων των δεδομένων

Δεδομένου ότι η τεχνολογία αναγνώρισης προσώπου βασίζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα, και δη βιομετρικών δεδομένων, όλα τα προβλεπόμενα στην ενωσιακή νομοθεσία για την προστασία προσωπικών δεδομένων δικαιώματα, τυγχάνουν εφαρμογής. Όπως έχει ήδη επισημανθεί, τα εν λόγω δικαιώματα δύναται να περιοριστούν, υπό την προϋπόθεση ότι ο εκάστοτε περιορισμός προβλέπεται στο νόμο, σέβεται τον πυρήνα των θεμελιωδών δικαιωμάτων και ελευθεριών των υποκειμένων των δεδομένων και αποτελεί αναγκαίο και αναλογικό μέτρο σε μια δημοκρατική κοινωνία για την επίτευξη συγκεκριμένων και νόμιμων σκοπών.

Ιδιαίτερη μνεία οφείλεται, όμως, εν προκειμένω, **στα δικαιώματα που δύναται να περιοριστούν υπέρμετρα, λόγω των προκλήσεων που θέτει η τεχνολογία αναγνώρισης προσώπου** στην άσκησή τους: α) το δικαίωμα πρόσβασης, β) το δικαίωμα διόρθωσης, γ) το δικαίωμα διαγραφής, δ) το δικαίωμα περιορισμού της επεξεργασίας των δεδομένων, ε) το δικαίωμα εναντίωσης και στ) το δικαίωμα στη μη αυτοματοποιημένη ατομική λήψη αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ.

Επισημαίνεται, επιπροσθέτως, ότι, ως έχει ήδη αναλυθεί, απαραίτητο εχέγγυο και αλλά και αναπόσπαστο προαπαιτούμενο της λυσιτελούς άσκησης οποιουδήποτε εκ των δικαιωμάτων του υποκειμένου, είναι η **εκπλήρωση από τον υπεύθυνο επεξεργασίας των υποχρεώσεών του όσον αφορά στην ενημέρωση αυτών.** Αναγνωρίζοντας ότι η αποτελεσματική άσκηση των δικαιωμάτων από τα υποκείμενα των δεδομένων είναι ιδιαιτέρως δυσχερής στο πλαίσιο χρήσης συστημάτων αναγνώρισης προσώπου, το ΕΣΠΔ συνέστησε στις κατευθυντήριές

του για τη χρήση της τεχνολογίας από τις δημόσιες αρχές, προτού ο υπεύθυνος επεξεργασίας προβεί σε επεξεργασία μέσω των συστημάτων αναγνώρισης προσώπου, να εξετάζει προσεκτικά[170]:

- ποια είναι τα υποκείμενα των δεδομένων και σε τι βαθμό ο αριθμός αυτών τυχόν υπερβαίνει το μέτρο του αναγκαίου για τον σκοπό της επεξεργασίας,
- τον τρόπο με τον οποίο τα υποκείμενα των δεδομένων ενημερώνονται για την επεξεργασία
- πώς τα υποκείμενα των δεδομένων μπορούν να ασκήσουν τα δικαιώματά τους, ιδίως τα δικαιώματα ενημέρωσης, πρόσβασης, διόρθωσης και περιορισμού της επεξεργασίας.

3.2.10.1 Το δικαίωμα πρόσβασης

Το υποκείμενο των δεδομένων προσωπικού χαρακτήρα που υφίστανται επεξεργασία, δικαιούται, κατ' αρχήν, να λάβει θετική ή αρνητική επιβεβαίωση για οποιαδήποτε επεξεργασία των προσωπικών του δεδομένων και, σε περίπτωση που η απάντηση είναι θετική, δικαιούται την πρόσβαση στα προσωπικά δεδομένα ως έχουν, καθώς και σε πρόσθετες πληροφορίες, όπως αυτές αναφέρονται στα άρθρα 15 ΓΚΠΔ και 14 της Οδηγίας.

Όσον αφορά στην τεχνολογία αναγνώρισης προσώπου, καθώς κατά την αποθήκευση των βιομετρικών δεδομένων, αυτά **συνδέονται με μια ταυτότητα και με αλφαριθμητικά δεδομένα**, τούτο επιτρέπει την ικανοποίηση ενός αιτήματος πρόσβασης, κατόπιν διενέργειας μιας αναζήτησης με βάση τα εκάστοτε αλφαριθμητικά δεδομένα στη βάση δεδομένων αναφοράς. Κατά το ΕΣΠΔ, κρίσιμο αποτελεί, εν προκειμένω, να μη δρομολογείται οποιαδήποτε περαιτέρω επεξεργασία, καθώς και να τηρείται αυστηρά η αρχή της ελαχιστοποίησης των δεδομένων, προκειμένου να μην αποθηκεύονται περισσότερα δεδομένα από όσα είναι απολύτως απαραίτητα για τον σκοπό της επεξεργασίας.[171]

Εντούτοις, η ικανοποίηση του δικαιώματος πρόσβασης παρουσιάζει ιδιαίτερες δυσχέρειες όταν η επεξεργασία συντελείται από την τεχνολογία αναγνώρισης προσώπου, ιδίως στην περίπτωση της **«ζωντανής» αναγνώρισης προσώπου**, ήτοι της χρήσης της τεχνολογίας σε πραγματικό χρόνο. Ο προβληματισμός εντοπίζεται στην ίδια τη φύση της εν λόγω πρακτικής, καθότι **κατά τη «ζωντανή» παρακολούθηση και ταυτοποίηση, τα συστήματα δεν αποθηκεύουν τα βιομετρικά δεδομένα ή/και τα πρότυπα εξ αυτών,** των

[170] European Data Protection Board (EDPB) (2022), ο.π. σελ. 21.
[171] European Data Protection Board (EDPB) (2022), ο.π.

υποκειμένων που διέρχονται από τον επιτηρούμενο χώρο. Όπως εύλογα συνάγεται, στο εν λόγω πλαίσιο, το δικαίωμα πρόσβασης ίσως να μην είναι καν νοητό.

Το ως άνω δικαίωμα, δύναται, ωστόσο, να περιορίζεται θεμιτά σε ορισμένες περιπτώσεις. Κατ' αρχάς, ο υπεύθυνος επεξεργασίας θα πρέπει να λαμβάνει ιδιαίτερη μέριμνα ώστε να μην προσβάλλονται, κατά την ικανοποίηση ενός αιτήματος πρόσβασης, τα δικαιώματα των άλλων υποκειμένων που έχουν ενδεχομένως καταγραφεί από το σύστημα αναγνώρισης προσώπου. Δεδομένου ότι η χρήση της τεχνολογίας καθιστά δυνατή τη μαζική καταγραφή και ταυτοποίηση ενός απροσδιόριστου αριθμού υποκειμένων, ο έλεγχος του αποθηκευμένου υλικού θα έχει ως αποτέλεσμα την πρόσθετη επεξεργασία των βιομετρικών δεδομένων και άλλων ατόμων, ενώ έτι περαιτέρω, τυχούσα επιθυμία του υποκειμένου των δεδομένων να λάβει αντίγραφο του υλικού (κατ' άρθρο 15§3 του ΓΚΠΔ) θα μπορούσε να επηρεάσει δυσανάλογα τα δικαιώματα των λοιπών καταγεγραμμένων από το σύστημα φυσικών προσώπων. Ως εκ τούτου, **ο υπεύθυνος επεξεργασίας θα πρέπει να λαμβάνει τα κατάλληλα τεχνικά μέτρα** (π.χ. θόλωση των προσώπων), ώστε να ανταποκριθεί στο αίτημα πρόσβασης, δίχως να παραβιάσει τα δικαιώματα τρίτων. Αν τούτο δεν καθίσταται δυνατό, ο υπεύθυνος επεξεργασία σε ορισμένες περιπτώσεις δυσανάλογης παραβίασης των δικαιωμάτων των τρίτων μερών, δεν θα πρέπει να ικανοποιεί το αίτημα του υποκειμένου.

Επιπροσθέτως, σε περίπτωση που ο υπεύθυνος επεξεργασίας δεν είναι σε θέση να εξακριβώσει την ταυτότητα του υποκειμένου των δεδομένων στο καταγεγραμμένο υλικό (άρθρο 11§2 του ΓΚΠΔ), ιδίως όταν θα πρέπει να ερευνήσει έναν ικανό όγκο δεδομένων μέχρι την ταυτοποίηση, το υποκείμενο των δεδομένων ενδεχομένως θα πρέπει **να προσδιορίζει χρονικά** στο αίτημά του το χρόνο που πιθανολογεί ότι καταγράφηκε και ταυτοποιήθηκε από το σύστημα αναγνώρισης προσώπου. Σε περίπτωση που **δεν καταστεί δυνατή η ικανοποίηση του αιτήματος**, κι εφόσον ο υπεύθυνος επεξεργασίας δύναται να αποδείξει ότι δεν είναι σε θέση να εξακριβώσει την ταυτότητα του υποκειμένου, **οφείλει να ενημερώσει το υποκείμενο για τον ακριβή χρόνο και χώρο όπου χρησιμοποιήθηκαν τα συστήματα**, ώστε να γνωρίζει ακριβώς ποια δεδομένα προσωπικού χαρακτήρα που το αφορούν μπορεί να έχουν υποβληθεί σε επεξεργασία.[172]

Αξίζει, επίσης, να σημειωθεί ότι στο πλαίσιο της Οδηγίας, κατ' αναλογία με τα προαναλυθέντα για το δικαίωμα ενημέρωσης, το δικαίωμα πρόσβασης

[172] Κατ' αναλογίαν με τις κατευθυντήριες του ΕΣΠΔ (2020) για την επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω βιντεοσυσκευών, σελ. 26-27.

δύναται να περιοριστεί, εν όλω ή εν μέρει, σε περιπτώσεις στις οποίες **θα ήταν επιζήμιο για τον επιδιωκόμενο σκοπό να επιτραπεί η πρόσβαση του υποκειμένου στα δεδομένα** (λ.χ. όταν η τεχνολογία χρησιμοποιείται για τη διαλεύκανση ενός σοβαρού εγκλήματος). Βεβαίως, οποιοσδήποτε περιορισμός θα επιτρέπεται μόνο εφόσον προβλέπεται σε νόμο του κράτους- μέλους, ο οποίος θα πρέπει επίσης να πληροί τα προαπαιτούμενα αναγκαιότητας και αναλογικότητας σε μια δημοκρατική κοινωνία, λαμβάνοντας δεόντως υπόψη τα θεμελιώδη δικαιώματα και τα έννομα συμφέροντα του ενδιαφερόμενου φυσικού προσώπου (άρθρα 15 και 16§4 Οδηγίας).

3.2.10.2 Το δικαίωμα διόρθωσης

Τα υποκείμενα των δεδομένων έχουν, επίσης, δικαίωμα να αξιώσουν από τον υπεύθυνο επεξεργασίας τη διόρθωση των προσωπικών δεδομένων τους όταν αυτά είναι ανακριβή, ή τη συμπλήρωση αυτών, όταν είναι ελλιπή, μεταξύ άλλων, μέσω συμπληρωματικής δήλωσης (άρθρα 16 ΓΚΠΔ και 16§1 Οδηγίας).

Δεδομένου ότι η τεχνολογία αναγνώρισης προσώπου παρουσιάζει **σημαντικά ποσοστά ανακρίβειας**, ιδίως όταν χρησιμοποιείται σε **μη ελεγχόμενα περιβάλλοντα**, με κρίσιμες συνακόλουθες επιπτώσεις για τα θεμελιώδη δικαιώματα των υποκειμένων των δεδομένων, **οι υπεύθυνοι επεξεργασίας θα πρέπει να επιδεικνύουν ιδιαίτερη προσοχή σε αιτήματα διόρθωσης προσωπικών δεδομένων**. Η ανακρίβεια, στο πλαίσιο ενός συστήματος αλγοριθμικής αναγνώρισης προσώπου, μπορεί να συνίσταται όχι μόνον στην εσφαλμένη ταυτοποίηση του υποκειμένου, αλλά και στη λανθασμένη περαιτέρω ταξινόμησή του σε ανακριβή κατηγορία, λ.χ. κατόπιν εσφαλμένου θετικού αποτελέσματος, τοποθέτηση του ατόμου σε λίστα υπόπτων. **Το ΕΣΠΔ κρούει τον κώδωνα του κινδύνου σχετικά με τις κρίσιμες επιπτώσεις σε περίπτωση που τα εν λόγω ανακριβή δεδομένα αποθηκεύονται σε αστυνομικές βάσεις δεδομένων ή/ και κοινολογούνται σε τρίτους.** Περαιτέρω, σε περίπτωση διαπίστωσης ύπαρξης ανακριβών δεδομένων στη βάση δεδομένων αναφοράς, ο υπεύθυνος επεξεργασίας οφείλει να διορθώσει άμεσα τόσο τα αποθηκευμένα προσωπικά δεδομένα, όσο και να λάβει τα απαραίτητα μέτρα ως προς τη διόρθωση των ίδιων των αλγορίθμων αναγνώρισης προσώπου[173].

3.2.10.3 Το δικαίωμα διαγραφής

Στο πλαίσιο του ΓΚΠΔ, το δικαίωμα διαγραφής («δικαίωμα στη λήθη») προσδιορίζεται ως το δικαίωμα του υποκειμένου να ζητά τη χωρίς αδικαιολόγητη καθυστέρηση διαγραφή των δεδομένων προσωπικού χαρακτήρα που το αφορούν, εφόσον δεν επιθυμεί πια αυτά τα δεδομένα να αποτελούν

[173] Βλ. ΕΣΠΔ (2022) ο.π., και αιτ. σκέψη 47 Οδηγίας.

αντικείμενο επεξεργασίας και εφόσον δεν υφίσταται νόμιμος λόγος να τα κατέχει ο υπεύθυνος επεξεργασίας (βλ. άρθρο 17 και αιτιολογικές σκέψεις 65 και 66 ΓΚΠΔ)[174].

Αξίζει να σημειωθεί, επιπροσθέτως, ότι το ΔΕΕ στη θεμελιώδη απόφαση Google Spain (C-131/12), υπήγαγε στην εμβέλεια του εν λόγω δικαιώματος και την αξίωση από το υποκείμενο της **διαγραφής των προσωπικών του δεδομένων, όταν αυτά εμφανίζονται σε λίστες αποτελεσμάτων μηχανών αναζήτησης, κατόπιν έρευνας βάσει του ονοματεπωνύμου τους**[175]. Η συμπερίληψη στο δικαίωμα διαγραφής, προσωπικών δεδομένων που έχουν μεν δημοσιοποιηθεί, εμφανίζονται δε συγκεντρωτικά βάσει ενός εργαλείου αναζήτησης σε ένα πλαίσιο το οποίο το υποκείμενο δεν αναμένει ευλόγως, **θα μπορούσε να είναι ιδιαιτέρως χρήσιμη κατά την εξέταση του τρόπου που χρησιμοποιούνται τα συστήματα αναγνώρισης προσώπου, ιδίως δε κατά την ανάλυση του τρόπου που παρέχει τις υπηρεσίες της η βιομηχανία αναγνώρισης προσώπου**· τόσο η Clearview και έτι περαιτέρω η PimEyes επιτρέπουν (η δεύτερη εξ αυτών στον οποιονδήποτε) τη χρήση μίας μηχανής αναζήτησης βάσει εικόνας ή βίντεο, και εμφανίζουν τα σχετικά αποτελέσματα από κάθε πιθανή γωνιά του Διαδικτύου.

Εν συνεχεία, η Οδηγία (άρθρο 16§2) επιτάσσει τα κράτη μέλη αφενός να επιβάλλουν στον υπεύθυνο επεξεργασίας την υποχρέωση να διαγράφει, χωρίς αδικαιολόγητη καθυστέρηση, τα προσωπικά δεδομένα των υποκειμένων των δεδομένων, και αφετέρου να κατοχυρώνουν ρητά το δικαίωμα των ίδιων των υποκειμένων να αξιώνουν από τον υπεύθυνο επεξεργασίας τη διαγραφή των δεδομένων τους, όταν η επεξεργασία τους παραβιάζει τις διατάξεις της Οδηγίας. Η διαγραφή δεδομένων προσωπικού χαρακτήρα απαιτείται ιδίως σε περίπτωση που αυτά αποκτήθηκαν κατά παραβίαση των αρχών που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα, όταν η επεξεργασία είναι παράνομη, **παραβαίνει τα προβλεπόμενα σχετικά με την επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα,** ή όταν τα δεδομένα προσωπικού χαρακτήρα πρέπει να διαγραφούν για λόγους τήρησης νόμιμης υποχρέωσης στην οποία υπόκειται ο υπεύθυνος επεξεργασίας.

Εν προκειμένω, η τεχνολογία αναγνώρισης προσώπου θέτει ακόμα μία φορά προσκόμματα κατά την άσκηση του ως άνω δικαιώματος, το οποίο **σε περίπτωση που η τεχνολογία χρησιμοποιείται σε πραγματικό χρόνο, καθίσταται μάλλον ανενεργό.** Επιπροσθέτως, επισημαίνεται ότι, εκτός από την περίπτωση που η τεχνολογία χρησιμοποιείται για μονοσήμαντη επαλήθευση (λ.χ. «ξεκλείδωμα» συσκευής μέσω FaceID), η χρήση της θα ισοδυναμεί σχεδόν

---

[174] Ορισμός κατά την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα: https://www.dpa.gr/el/polites/gkpd/dikaiwma_diagrafis

[175] Ιγγλεζάκης, Ι. (2021), ο.π. σελ. 348-349.

αυτονόητα **με την επεξεργασία τεράστιου αριθμού βιομετρικών δεδομένων των υποκειμένων των δεδομένων**. Ως εκ τούτου, προκειμένου να είναι η δυνατή η ικανοποίηση του δικαιώματος, καθίσταται νευραλγικής σημασίας η έγκαιρη λήψη μέτρων από τον υπεύθυνο επεξεργασίας, ο οποίος οφείλει να εξετάζει εκ των προτέρων τα **όρια του σκοπού και της αναγκαιότητας της επεξεργασίας**, **ούτως ώστε να δύναται να διεκπεραιώσει χωρίς αδικαιολόγητη καθυστέρηση ένα αίτημα διαγραφής**. Διαφορετικά η υποχρέωσή του να διαγράφει τα βιομετρικά δεδομένα σε περίπτωση που παραβιάζονται τα προαπαιτούμενα της εφαρμοστέας νομοθεσίας για την επεξεργασία των ειδικών κατηγοριών δεδομένων, θα καθίσταται δυσχερής, έως αδύνατη.

3.2.10.4 Το δικαίωμα περιορισμού της επεξεργασίας

Τα υποκείμενα των δεδομένων έχουν επίσης το δικαίωμα να ζητούν τον περιορισμό της επεξεργασίας των δεδομένων τους. Στο πλαίσιο του Κανονισμού, αυτό είναι δυνατό μόνον όταν: α) το υποκείμενο των δεδομένων επικαλείται την ανακρίβεια των δεδομένων του και ο υπεύθυνος επεξεργασίας εξετάζει το σχετικό αίτημα, β) η επεξεργασία είναι παράνομη και το υποκείμενο των δεδομένων αντιτάσσεται στη διαγραφή των δεδομένων και ζητά, αντ' αυτής, τον περιορισμό της χρήσης τους, γ) τα δεδομένα δεν είναι απαραίτητα πλέον για τον σκοπό της επεξεργασίας, αλλά το υποκείμενο των δεδομένων επιθυμεί την τήρησή τους για την άσκηση νομικών του αξιώσεων, δ) το υποκείμενο των δεδομένων έχει ασκήσει το δικαίωμα εναντίωσης (αρ. 21 ΓΚΠΔ) και ο υπεύθυνος επεξεργασίας εξετάζει την συνδρομή υπέρτερου εννόμου συμφέροντός του[176]. Στο πλαίσιο της Οδηγίας, το δικαίωμα μπορεί να ασκηθεί σε περίπτωση που η ακρίβεια των δεδομένων αμφισβητείται από το υποκείμενο των δεδομένων και η βασιμότητα του ισχυρισμού δεν μπορεί να εξακριβωθεί, ή όταν τα δεδομένα προσωπικού χαρακτήρα πρέπει να διατηρηθούν για σκοπούς μελλοντικής απόδειξης (αρ. 16).

Το υπό κρίση δικαίωμα καθίσταται ιδιαίτερα σημαντικό κατά την εξέταση της τεχνολογίας αναγνώρισης προσώπου, **λόγω των ανακριβειών** που κατατρέχουν τα συστήματα, κυρίως όταν αυτά εγκαθίστανται σε μη- ελεγχόμενα περιβάλλοντα. Όπως αναλύθηκε ήδη διεξοδικά, το γεγονός ότι η τεχνολογία βασίζεται σε αλγόριθμους και συνεπώς δεν εμφανίζει ποτέ οριστικό αποτέλεσμα, σε συνδυασμό με την εκτεταμένη ενσωμάτωση εφαρμογών μηχανικής μάθησης, συνεπάγεται τη συλλογή μεγάλης ποσότητας δεδομένων, η ποιότητα και η ακρίβεια των οποίων ποικίλλει σημαντικά και οδηγεί συχνά σε εσφαλμένα αποτελέσματα ικανά να παραβιάσουν θεμελιώδη ανθρώπινα δικαιώματα των υποκειμένων. Επισημαίνεται, περαιτέρω, ότι σε ειδικές περιπτώσεις στις οποίες τα

[176] Όπως εμφαίνεται στην ιστοσελίδα της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα: https://www.dpa.gr/el/polites/gkpd/dikaiwma_periorismou_epexergasias

δεδομένα δεν μπορούν να διαγραφούν λόγω της ύπαρξης βάσιμων λόγων που καταδεικνύουν ότι η διαγραφή θα μπορούσε να θίξει τα έννομα συμφέροντα του υποκειμένου των δεδομένων, τα δεδομένα θα πρέπει αντ' αυτού να περιορίζονται και να υποβάλλονται σε επεξεργασία μόνο για τον σκοπό που εμπόδισε τη διαγραφή τους[177].

3.2.10.5 Το δικαίωμα «έμμεσης πρόσβασης»: άσκηση δικαιωμάτων μέσω της εποπτικής αρχής

Στο πλαίσιο της Οδηγίας, σε περίπτωση που ο νόμος προβλέπει περιορισμούς στα δικαιώματα ενημέρωσης, πρόσβασης, διόρθωσης ή διαγραφής, το υποκείμενο των δεδομένων έχει δικαίωμα «*έμμεσης πρόσβασης*»[178] (άρθρο 17 της Οδηγίας), ήτοι άσκησης των εν λόγω δικαιωμάτων **μέσω της αρμόδιας εποπτικής αρχής**. Επισημαίνεται, ότι το εν λόγω δικαίωμα έμμεσης πρόσβασης, συνιστά πρόσθετο δικαίωμα στο πλαίσιο της οδηγίας και δεν υποκαθιστά το δικαίωμα υποβολής καταγγελίας στην εποπτική αρχή.

Οφείλει, εν προκειμένω, επίσης να σημειωθεί ότι σε περίπτωση περιορισμού των δικαιωμάτων των υποκειμένων των δεδομένων, **οι αρχές επιβολής του νόμου οφείλουν να ενημερώνουν τα υποκείμενα των δεδομένων, μεταξύ άλλων, και για το δικαίωμά τους να υποβάλουν καταγγελία στις εποπτικές αρχές και για το γενικότερο δικαίωμά τους να προσφύγουν σε ένδικα μέσα.**

3.2.10.6 Το δικαίωμα εναντίωσης

Ο Κανονισμός προβλέπει, επιπροσθέτως, το δικαίωμα του υποκειμένου να αντιτάσσεται ανά πάσα στιγμή και για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή του, στην επεξεργασία των προσωπικών του δεδομένων, εφόσον αυτή ερείδεται σε καθήκον που εκτελείται προς το δημόσιο συμφέρον (αρ. 6 §1 στοιχ. ε΄ ΓΚΠΔ) ή στην ύπαρξη εννόμου συμφέροντος του υπευθύνου επεξεργασίας (αρ. 6 §1 στοιχ. στ΄ ΓΚΠΔ), συμπεριλαμβανομένης της κατάρτισης προφίλ βάσει των εν λόγω διατάξεων. Στην περίπτωση που το υποκείμενο των δεδομένων ασκήσει το εν λόγω δικαίωμα, ο υπεύθυνος επεξεργασίας οφείλει να σταματήσει την επεξεργασία των προσωπικών δεδομένων, εκτός και αν δύναται να αποδείξει τη συνδρομή επιτακτικών και νόμιμων λόγων για την επεξεργασία, οι οποίοι υπερισχύουν των συμφερόντων, των δικαιωμάτων και των ελευθεριών του υποκειμένου των δεδομένων, ή για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων (αρ. 21§1 ΓΚΠΔ). Σε κάθε περίπτωση, ο υπεύθυνος επεξεργασίας θα

---

[177] Αιτιολογική Σκέψη 47 Οδηγίας.

[178] Ομάδα Εργασίας του άρθρου 29 για την προστασία των δεδομένων 'Γνώμη σχετικά με ορισμένα βασικά ζητήματα της οδηγίας (ΕΕ) 2016/680 για την επιβολή του νόμου' σελ. 20.

πρέπει να απαντήσει δικαιολογημένα στο αίτημα του υποκειμένου εντός ενός μήνα[179].

Στο πλαίσιο των συστημάτων αναγνώρισης προσώπου, η λυσιτελής άσκηση του εξεταζόμενου δικαιώματος είναι ιδιαιτέρως δυσχερής. Κατ' αρχάς, δεν είναι ευκρινές πώς ακριβώς το υποκείμενο θα μπορεί να αντιτάσσεται στην καταγραφή και ταυτοποίησή του, ιδιαίτερα όταν η τεχνολογία χρησιμοποιείται στο δημόσιο χώρο, λ.χ. στα μέσα μαζικής μεταφοράς. Κατ' αναλογία με τα αναφερόμενα από το ΕΣΠΔ στην περίπτωση της βιντεοεπιτήρησης, είτε ο υπεύθυνος επεξεργασίας, σε περίπτωση που δεν συντρέχουν επιτακτικοί λόγοι που δικαιολογούν την επεξεργασία εκ μέρους του, θα πρέπει να είναι διαρκώς σε θέση να σταματήσει το σύστημα αμέσως μόλις λάβει αίτημα από το υποκείμενο, είτε η πρόσβαση στον επιτηρούμενο χώρο θα πρέπει να είναι τόσο αυστηρώς ελεγχόμενη, ώστε τα υποκείμενα να πρέπει να δώσουν, προτού διέλθουν από το σημείο εγκατάστασης του συστήματος αναγνώρισης προσώπου, έγκριση στον υπεύθυνο επεξεργασίας. Ως ευλόγως συνάγεται, τούτο καθίσταται μάλλον **αδύνατο στις περιπτώσεις που η τεχνολογία χρησιμοποιείται στη δημόσια σφαίρα**.

Προσέτι, σε περιπτώσεις χρήσης της τεχνολογίας για σκοπούς άμεσης εμπορικής προώθησης, συμπεριλαμβανομένης της κατάρτισης προφίλ, το δικαίωμα εναντίωσης είναι **απόλυτο** και τα υποκείμενα δύνανται να το ασκούν οποτεδήποτε και κατά τη διακριτική τους ευχέρεια**.**

Όπως απορρέει εκ των ανωτέρω, ο Κανονισμός επιφυλάσσει αυξημένα εχέγγυα προστασίας στο υποκείμενο των δεδομένων, στην περίπτωση «κατάρτισης προφίλ». Το δικαίωμα αντίταξης σε αυτοματοποιημενες ατομικές αποφάσεις, ήτοι η αξίωση του υποκειμένου να μην υπόκειται σε μέτρα ικανά να παράγουν έννομες συνέπειες για το πρόσωπό του μόνον επί τη βάση μίας αυτοματοποιημένης διαδικασίας που αξιολογεί πτυχές της προσωπικότητάς του, λαμβάνει ακόμα μεγαλύτερες διαστάσεις κατά την ανάλυση των συστημάτων αναγνώρισης προσώπου, τα οποία με τη δυναμική που προσφέρει σε αυτά η μηχανική μάθηση, καθιστούν την κατάρτιση προφίλ έναν εύκολο και φθηνό στόχο με πολλαπλά οικονομικά – και όχι μόνον- οφέλη.

3.2.10.7 Το δικαίωμα στη μη αυτοματοποιημένη ατομική λήψη αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ

Όσον αφορά στην κατάρτιση προφίλ και στην αυτοματοποιημένη λήψη αποφάσεων, το ευρωπαϊκό κεκτημένο για την προστασία των δεδομένων

[179] ΕΣΠΔ (2020), ο.π.

προσωπικού χαρακτήρα, **κατ' αρχήν απαγορεύει την αυτοματοποιημένη λήψη αποφάσεων**, ήτοι κάθε απόφαση «που βασίζεται αποκλειστικά σε αυτοματοποιημένη επεξεργασία, περιλαμβανομένης της κατάρτισης προφίλ, **η οποία παράγει έννομα αποτελέσματα που αφορούν στο υποκείμενο των δεδομένων ή το επηρεάζουν σημαντικά** (άρθρο 22 του ΓΚΠΔ, όσο και το άρθρο 11 της Οδηγίας).

Περαιτέρω, σύμφωνα με τα άρθρα 3§4 της Οδηγίας και 4§4 του ΓΚΠΔ, ως «κατάρτιση προφίλ» νοείται «*οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που συνίσταται στη χρήση δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση ορισμένων προσωπικών πτυχών ενός φυσικού προσώπου, ιδίως για την ανάλυση ή την πρόβλεψη πτυχών που αφορούν την απόδοση στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις, τα ενδιαφέροντα, την αξιοπιστία, τη συμπεριφορά, τη θέση ή τις μετακινήσεις του εν λόγω φυσικού προσώπου*». Όπως συνάγεται, αντικείμενο ρύθμισης συνιστά *κάθε απόφαση, η οποία μπορεί να περιλαμβάνει κάποιο μέτρο, με την οποία αξιολογούνται προσωπικές πτυχές που αφορούν το υποκείμενο, λαμβανομένη αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας και η οποία παράγει έννομα αποτελέσματα έναντι του προσώπου αυτού, ή το επηρεάζει σημαντικά κατά ανάλογο τρόπο, όπως οι πρακτικές ηλεκτρονικών προσλήψεων*, **χωρίς ανθρώπινη παρέμβαση**[180].

Στο πλαίσιο του Κανονισμού, το άρθρο 22§1 κατοχυρώνει, κατά την Ομάδα Εργασίας του άρθρου 29, τη **γενική απαγόρευση της πλήρως αυτοματοποιημένης λήψης αποφάσεων**[181]. Οι υπεύθυνοι επεξεργασίας δεδομένων δύναται, ωστόσο, να απαλλάσσονται από την εν λόγω απαγόρευση σε τρεις περιοριστικά αναφερόμενες περιπτώσεις, ήτοι όταν η απόφαση: α) είναι αναγκαία για τη σύναψη ή την εκτέλεση σύμβασης μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας, β) επιτρέπεται από το δίκαιο της ένωσης ή το δίκαιο κράτους μέλους, στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας και το οποίο προβλέπει κατάλληλα μέτρα για την προστασία των δικαιωμάτων του υποκειμένου, ή γ) βασίζεται σε ρητή συγκατάθεση.

Προσέτι, αν η υπό κρίση απόφαση λήφθηκε ως αναγκαία στο πλαίσιο εκτέλεσης σύμβασης μεταξύ του υπευθύνου επεξεργασίας και του υποκειμένου των δεδομένων ή επί τη βάσει της ρητής συγκατάθεσης αυτού, το μεν υποκείμενο έχει το δικαίωμα να την αμφισβητήσει, ενώ παραλλήλως, ο δε υπεύθυνος επεξεργασίας υποχρεούται να εφαρμόσει κατάλληλα μέτρα για την προστασία των δικαιωμάτων του υποκειμένου, όπως να εξασφαλίζει την ανθρώπινη

---

[180] Αιτιολογική σκέψη 71 ΓΚΠΔ.

[181] Ομάδα Εργασίας του άρθρου 29 για την προστασία δεδομένων (2018), ο.π. σελ. 23 επ.

παρέμβαση στη λήψη της απόφασης ή το δικαίωμα έκφρασης άποψης καθώς και αμφισβήτησης της απόφασης από το υποκείμενο. Περαιτέρω επισημαίνεται ότι σύμφωνα με την αιτιολογική σκέψη 71 του ΓΚΠΔ, **τα παιδιά** δεν θα πρέπει, κατ' αρχήν, να υπόκεινται σε τέτοιου είδους αποφάσεις.

Ειδικότερα ως προς τα βιομετρικά δεδομένα, ο Κανονισμός ορίζει ότι η αυτοματοποιημένη λήψη αποφάσεων που περιλαμβάνει ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα **επιτρέπεται μόνον** αν η επεξεργασία ερείδεται στη ***ρητή συγκατάθεση*** του υποκειμένου, ή αν η επεξεργασία είναι απαραίτητη ***για λόγους ουσιαστικού δημόσιου συμφέροντος, βάσει του δικαίου της ένωσης ή κράτους μέλους,*** *το οποίο είναι ανάλογο προς τον επιδιωκόμενο στόχο, σέβεται την ουσία του δικαιώματος στην προστασία των δεδομένων και προβλέπει κατάλληλα και συγκεκριμένα μέτρα για τη διασφάλιση των θεμελιωδών δικαιωμάτων και των συμφερόντων του υποκειμένου των δεδομένων.* Σε αμφότερες περιπτώσεις, ο υπεύθυνος επεξεργασίας **θα πρέπει να εξασφαλίζει ότι υφίστανται κατάλληλα μέτρα για τη διασφάλιση των δικαιωμάτων, των ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων, καθώς και να μεριμνά για τη λυσιτελή τους εφαρμογή**.

Υπό το φως των ανωτέρω, η βουλγαρική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, σε γνωμοδότηση που εξέδωσε το 2020 αναφορικά με την **εγκατάσταση συστήματος αναγνώρισης προσώπου και μέτρησης θερμοκρασίας στην είσοδο ενός σχολείου**, αφότου τόνισε αρχικώς ότι **η συγκατάθεση σε ένα τέτοιο σενάριο δεν θα ήταν ελεύθερη**, υπογράμμισε περαιτέρω ότι οι αποφάσεις για την παρεμπόδιση των υποκειμένων των δεδομένων να εισέλθουν στους χώρους ενός σχολείου με τη χρήση αυτών των συστημάτων **δεν θα ήταν σύμφωνες με το άρθρο 22 ΓΚΠΔ,** καθώς και ότι **ο έλεγχος πρόσβασης στο σχολείο θα πρέπει να διεξάγεται χωρίς την επεξεργασία ειδικών κατηγοριών δεδομένων**[182].

Κατ' αναλογία με τα ανωτέρω, το άρθρο 11§1 της Οδηγίας προβλέπει την υποχρέωση των κρατών μελών να απαγορεύουν γενικά τις αποφάσεις που βασίζονται αποκλειστικά σε αυτοματοποιημένη επεξεργασία, συμπεριλαμβανομένης της κατάρτισης προφίλ, οι οποίες παράγουν **δυσμενή έννομα αποτελέσματα** όσον αφορά στο υποκείμενο των δεδομένων **ή το επηρεάζουν σημαντικά**. Κατ' εξαίρεση, η επεξεργασία αυτή μπορεί να είναι δυνατή **μόνον εάν επιτρέπεται από το δίκαιο της ένωσης ή του κράτους μέλους** στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας, εφόσον αυτό παρέχει

---

[182] Vale, S. και Zanfir- Fortuna, G. (2022) 'FPF Report: Automated Decision-Making Under the GDPR - A Comprehensive Case-Law Analysis. *Future of Privacy Forum*. σελ 40-43. https://fpf.org/wp-content/uploads/2022/05/FPF-ADM-Report-R2-singles.pdf

κατάλληλες εγγυήσεις για τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων, **κατ' ελάχιστον το δικαίωμα ανθρώπινης παρέμβασης εκ μέρους του υπευθύνου επεξεργασίας.**

Ομοίως με τον Κανονισμό, η Οδηγία διευκρινίζει ότι οι ανωτέρω αποφάσεις, κατ' αρχήν, δεν πρέπει να βασίζονται σε ειδικές κατηγορίες δεδομένων. Εξαίρεση μπορεί να προβλεφθεί **μόνο εάν υπάρχουν κατάλληλα μέτρα για τη διασφάλιση των δικαιωμάτων, των ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων** (αρ. 11§2). Κατά το ΕΣΠΔ, η εν λόγω εξαίρεση πρέπει να ερμηνεύεται πάντοτε υπό το πρίσμα των προϋποθέσεων του άρθρου 10 της Οδηγίας.[183] Περαιτέρω, στο άρθρο 11§3 της Οδηγίας εισάγεται **απόλυτη απαγόρευση στην πρακτική κατάρτισης προφίλ, όταν αυτή οδηγεί σε διακρίσεις εις βάρος φυσικών προσώπων βάσει των ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα.** Το ΕΣΠΔ μάλιστα τόνισε ότι, κατά την εξέταση του κατά πόσον προβλέπονται κατάλληλα μέτρα για τη διασφάλιση των δικαιωμάτων, των ελευθεριών και των συμφερόντων του υποκειμένου των δεδομένων, θα πρέπει να λαμβάνεται πάντοτε υπόψη ότι **η χρήση της τεχνολογίας αναγνώρισης προσώπου, ανάλογα με τον τρόπο και τον σκοπό για τον οποίο εφαρμόζεται, μπορεί σαφώς να οδηγήσει σε κατάρτιση προφίλ.** Η εν λόγω επισήμανση είναι σημαντική, καθώς η τεχνολογία έχει αποδειχθεί **ικανή να ψηφιοποιήσει τις συστημικές κοινωνικές προκαταλήψεις και να τις διαιωνίσει κατά τρόπο που θίγει τον πυρήνα ποικίλων θεμελιωδών δικαιωμάτων**, όπως το δικαίωμα στην ανθρώπινη αξιοπρέπεια, ιδιαιτέρως των μειονοτικών ομάδων του πληθυσμού.

Εν συνεχεία, επισημαίνεται ότι **οι περισσότερες γνωστές έως τώρα δοκιμές της τεχνολογίας αναγνώρισης προσώπου στα κράτη μέλη της ΕΕ, προβλέπουν την ανθρώπινη παρέμβαση**. Ειδικότερα, οι αντιστοιχίες που βασίζονται στον αλγόριθμο αναγνώρισης προσώπου αξιολογούνται από ανθρώπους (π.χ. αστυνομικούς), οι οποίοι, κατόπιν της ανάλυσης, αναλαμβάνουν δράση. Ωστόσο, έχει παρατηρηθεί, ότι **σε αρκετές περιπτώσεις, η ανθρώπινη παρέμβαση απλώς «προσυπογράφει» τα αποτελέσματα του συστήματος, καθώς το φυσικό πρόσωπο ακούσια εμπιστεύεται πλήρως τη «δίκαιη κρίση» της τεχνητής νοημοσύνης, καθιστώντας έτσι το σύστημα ουσιαστικά αυτοματοποιημένο. Εξ αντιδιαστολής, αλλά με παρόμοιες προεκτάσεις, έρευνες καταδεικνύουν ότι οι άνθρωποι που εξετάζουν τα αποτελέσματα του αλγορίθμου, συχνά παρακάμπτουν τα αποτελέσματα του συστήματος, όταν αυτά είναι σύμφωνα με τα στερεότυπά τους, θέτοντας λ.χ. και πάλι σε μειονεκτική θέση τις μειονοτικές ομάδες.** Αυτή η συμπεριφορά απειλεί την

[183] ΕΣΠΔ (2022), ο.π. σελ 19- 20.

πιθανή προστιθέμενη αξία της αυτοματοποιημένης επεξεργασίας βάσει των αλγορίθμων, οι αναλύσεις των οποίων υποστηρίζεται ότι θα μπορούσαν να είναι πιο ακριβείς και σε ορισμένες περιπτώσεις πιο δίκαιες από τις ανθρώπινες.[184].

Τέλος, οφείλει επίσης να επισημανθεί, ότι η **ενσωμάτωση της μηχανικής μάθησης** στην τεχνολογία αναγνώρισης προσώπου θα πρέπει να αποτελεί αφορμή για **ακόμη αυστηρότερη εξέταση** της συνδρομής μη επιτρεπτής αυτοματοποιημένης λήψης αποφάσεως. Κατ' αρχάς, με τη χρήση της βαθιάς μάθησης, καθίσταται αυτονόητο ότι το αποτέλεσμα εξόδου θα βασίζεται αποκλειστικά σε αυτοματοποιημένη διαδικασία. Λαμβάνοντας υπ' όψιν, περαιτέρω το φαινόμενο του μαύρου κουτιού και της αλγοριθμικής αδιαφάνειας, το αποτέλεσμα του λογισμικού είναι πιθανό να μην μπορεί να εξηγηθεί ή να γίνει πλήρως αντιληπτό – ή και καθόλου, αναλόγως της πολυπλοκότητας του συστήματος- από τον υπεύθυνο ή εκτελούντα την επεξεργασία, με επακόλουθο να μην δύναται κατ' ουσίαν να παρέμβει ο ανθρώπινος παράγοντας σε αυτό.

Επιπλέον, **η εφαρμογή της γενικής απαγόρευσης αυτοματοποιημένης λήψης αποφάσεων επί τη βάση επεξεργασίας ειδικών κατηγοριών δεδομένων**, όπως οι εικόνες προσώπου που υφίστανται επεξεργασίας από τα συστήματα αναγνώρισης προσώπου με σκοπό την ταυτοποίηση του υποκειμένου τους, **καθίσταται αμφίβολη**, καθώς **η τεχνητή νοημοσύνη καθιστά δυνατή τη συναγωγή ευαίσθητων δεδομένων από μη ευαίσθητα δεδομένα**, λ.χ. υποστηρίζεται ότι σε ορισμένες περιπτώσεις ο σεξουαλικός προσανατολισμός ενός ατόμου μπορεί να συναχθεί επί τη βάση της γεωμετρίας του προσώπου του.[185] Περαιτέρω, **τα «απλά» προσωπικά δεδομένα μπορούν**, όταν υπόκεινται σε επεξεργασία από εφαρμογές τεχνητής νοημοσύνης, **να αποτελέσουν «διακομιστές μεσολάβησης» ('proxy servers')** για ευαίσθητα δεδομένα που συσχετίζονται με αυτά, παρόλο που τα τελευταία δεν συνάγονται απευθείας από το σύστημα, λ.χ. ο τόπος κατοικίας μπορεί να λειτουργήσει ως δείκτης για την εθνοτική καταγωγή του υποκειμένου των δεδομένων. Όπως έχει επισημάνει η Ευρωπαϊκή Υπηρεσία Κοινοβουλευτικής Έρευνας (EPRS), αυτή η πρακτική μπορεί να οδηγήσει εμμέσως σε **διακρίσεις**[186], οι οποίες ενδέχεται να μην αντιμετωπιστούν ως ορίζει η νομοθεσία, ήτοι με απαγόρευση της κατάρτισης προφίλ που ερείδεται στις ειδικές κατηγορίες δεδομένων και οδηγεί σε αυτές, αν δεν ληφθούν κατάλληλα και αποτελεσματικά μέτρα ελέγχου του αλγορίθμου, **ώστε να είναι ορατές** στα εμπλεκόμενα μέρη -και ως εκ τούτου αντιμετωπίσιμες.

---

[184] European Union Agency for Fundamental Rights (2019) 'Facial recognition technology: fundamental rights considerations in the context of law enforcement', ο.π. σελ. 26.

[185] Γίνεται δεκτό ότι τα εξαχθέντα εκ των μη ευαίσθητων, ευαίσθητα δεδομένα θα υπόκεινται στη νομοθεσία για την προστασία των προσωπικών δεδομένων.

[186] EPRS | European Parliamentary Research Service (2020), ο.π. σελ. 59-66.

3.3 Η Πρόταση Κανονισμού (ΕΕ) για την Τεχνητή Νοημοσύνη

Προτού ολοκληρωθεί η παρούσα μελέτη, κρίνεται σκόπιμη η επισκόπηση της Πρότασης Κανονισμού Τεχνητής Νοημοσύνης της Ευρωπαϊκής Επιτροπής[187], καθώς σε αυτή λαμβάνεται **ειδική μέριμνα για τα συστήματα εξ αποστάσεως βιομετρικής ταυτοποίησης και παρακολούθησης**.

Η Ευρωπαϊκή Επιτροπή παρουσίασε τον Απρίλιο του 2021 μια νέα πρόταση για τη θέσπιση ενός συνεκτικού ρυθμιστικού πλαισίου σχετικά με την τεχνητή νοημοσύνη, ιδίως σε ό,τι αφορά στην ανάπτυξη, τη διάθεση στην αγορά και τη χρήση των συστημάτων ΤΝ στην Ένωση. Η Επιτροπή προτείνει να κατοχυρωθεί στο δίκαιο της ΕΕ **ένας τεχνολογικά ουδέτερος ορισμός των συστημάτων ΤΝ** και να θεσπιστεί μια **ταξινόμηση,** με διαφορετικές απαιτήσεις και υποχρεώσεις, προσαρμοσμένες σε μια **προσέγγιση με βάση τον κίνδυνο** που ενδέχεται να προκαλέσουν τα συστήματα στα θεμελιώδη ανθρώπινα δικαιώματα και τις ελευθερίες των πολιτών (risk- based approach).

- Ορισμένα συστήματα ΤΝ που θεωρούνται σαφής απειλή για την ασφάλεια, τα μέσα διαβίωσης και τα δικαιώματα των ανθρώπων, **απαγορεύονται εξαιτίας του «μη επιτρεπτού κινδύνου» που δημιουργούν**[188]. Σε αυτά περιλαμβάνονται και τα συστήματα που έχουν σχεδιαστεί για να χειραγωγούν την ανθρώπινη συμπεριφορά μέσω πρακτικών **κοινωνικής βαθμολόγησης** από τις κυβερνήσεις.
- Άλλες εφαρμογές ΤΝ κατατάσσονται ως «**υψηλού κινδύνου συστήματα**», επειδή δημιουργούν δυσμενείς επιπτώσεις για την ασφάλεια των ανθρώπων ή τα θεμελιώδη δικαιώματά τους[189]. Στο πλαίσιο αυτό, συμπεριλαμβάνεται η χρήση της τεχνολογίας ΤΝ, μεταξύ άλλων, σε υποδομές ζωτικής σημασίας (π.χ. τα μέσα μαζικής μεταφοράς), στην επιβολή του νόμου, στη διαχείριση της μετανάστευσης, του ασύλου και των συνοριακών ελέγχων, ενώ ειδικότερη μνεία επιφυλάσσεται για **τα βιομετρικά συστήματα ΤΝ, όπως η τεχνολογία αναγνώρισης προσώπου, τα οποία έχουν αναγνωριστεί ρητά ως υψηλού κινδύνου εφαρμογές**. Τα εν λόγω συστήματα υψηλού κινδύνου θα πρέπει να συμμορφώνονται με μια σειρά απαιτήσεων ασφαλείας (λ.χ. πρόβλεψη ανθρώπινης εποπτείας)

---

[187] Ευρωπαϊκή Επιτροπή (2021) *Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη θέσπιση εναρμονισμένων κανόνων σχετικά με την τεχνητή νοημοσύνη (Πράξη για την τεχνητή νοημοσύνη) [COM/2021/206 final]*. Διαθέσιμο στο: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0009.02/DOC_1&format=PDF.

[188] αρ. 5 Σχ. Καν. ΤΝ .

[189] αρ. 6 Σχ. Καν. ΤΝ .

και να υποβάλλονται σε **αξιολόγηση συμμόρφωσης πριν διατεθούν στην αγορά.** Επιπλέον, θα πρέπει να θεσπίζεται **εκ των υστέρων εποπτεία και έλεγχος** της αγοράς, προκειμένου να διασφαλιστεί η συμμόρφωση με τις ανωτέρω υποχρεώσεις όλων των συστημάτων ΤΝ υψηλού κινδύνου που έχουν ήδη διατεθεί στην αγορά[190].

- Τα συστήματα τεχνητής ΤΝ που παρουσιάζουν «περιορισμένο κίνδυνο» θα πρέπει να υπόκεινται σε ένα σύνολο υποχρεώσεων διαφάνειας.
- Όλα τα άλλα συστήματα ΤΝ που παρουσιάζουν «ελάχιστο κίνδυνο» μπορούν να αναπτυχθούν και να χρησιμοποιηθούν στην ΕΕ χωρίς πρόσθετες νομικές υποχρεώσεις, πέραν της υφιστάμενης νομοθεσίας.

3.3.1 Ειδικότερα, τα βιομετρικά συστήματα & η τεχνολογία αναγνώρισης προσώπου

Στο πλαίσιο της προτεινόμενης πρότασης, η έννοια του συστήματος εξ αποστάσεως βιομετρικής ταυτοποίησης, προσδιορίζεται ως ένα «*σύστημα ΤΝ που προορίζεται για την* ***εξ αποστάσεως ταυτοποίηση φυσικών προσώπων μέσω της αντιπαραβολής των βιομετρικών δεδομένων του προσώπου με τα βιομετρικά δεδομένα που περιέχονται σε βάση δεδομένων αναφοράς και χωρίς να είναι γνωστό εκ των προτέρων αν το στοχευόμενο πρόσωπο θα είναι παρόν και αν μπορεί να ταυτοποιηθεί****, ανεξάρτητα από τη συγκεκριμένη τεχνολογία, τις διαδικασίες ή τους τύπους βιομετρικών δεδομένων που χρησιμοποιούνται.*» [191]

Καθώς το σχέδιο κανονισμού υιοθετεί **ουδέτερη τεχνολογικά στάση** και στοχεύει να είναι όσο το δυνατόν πιο ανθεκτικό στο μέλλον, σε συνδυασμό με τη συστηματική ερμηνεία του άρθρου 6 και του Παραρτήματος ΙΙΙ[192] περ. 1 α' και περ. 6' αυτού, προκύπτει ευλόγως ότι **ο κανονισμός εφαρμόζεται σε όλα τα συστήματα εξ αποστάσεως βιομετρικής ταυτοποίησης, συμπεριλαμβανομένων των τεχνολογιών αναγνώρισης προσώπου, είτε χρησιμοποιούνται από ιδιώτες είτε από τις δημόσιες αρχές για σκοπούς επιβολής του νόμου**[193]**.**

---

[190] αρ. 61 Σχ. Καν. ΤΝ .

[191] Αιτ. Σκέψη 8 και άρ. 3 στοιχ. 33 Σχ. Καν. ΤΝ .

[192] Παράρτημα ΙΙΙ της Πρότασης κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου *για τη θέσπιση εναρμονισμένων κανόνων σχετικά με την τεχνητή νοημοσύνη (Πράξη για την τεχνητή νοημοσύνη)* {SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}. Διαθέσιμο σε: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0009.02/DOC_2&format=PDF

[193] Madiega, T., Mildebrath, H. (2021), ο.π. σελ. 24-25.

Τα εν λόγω συστήματα, παρότι στο πλαίσιο του προταθέντος Κανονισμού, εμπίπτουν στην κατηγορία «***υψηλού κινδύνου***», **δεν απαγορεύονται εξ ορισμού**, αλλά αντίθετα υπόκεινται σε διάφορες **υποχρεώσεις συμμόρφωσης**. Ειδικότερα, πριν από την κυκλοφορία τους στην αγορά, θα πρέπει να έχει προηγηθεί αξιολόγηση της συμμόρφωσης προς τις απαιτήσεις του κανονισμού, μεταξύ των οποίων: η εγκατάσταση και λειτουργία συστήματος εποπτείας και διαχείρισης κινδύνου καθ' όλον τον κύκλο ζωής του συστήματος ΤΝ, η τήρηση κανόνων για τη χρήση υψηλών προδιαγραφών ακριβείας και ποιότητας δεδομένων κατά την εκπαίδευση των αλγορίθμων, η τεχνική τεκμηρίωση του συστήματος ΤΝ προ της θέσης του σε κυκλοφορία στην αγορά, ο σχεδιασμός του συστήματος κατά τρόπο ώστε να διατηρεί αυτομάτως καταγραφές συμβάντων (logs) με περαιτέρω δυνατότητα αναγνώρισης προτύπων ή κοινά αποδεκτών χαρακτηριστικών που θα καθιστούν εφικτή την ιχνηλάτηση του συστήματος, οι υποχρεώσεις διαφάνειας ώστε οι χρήστες των συστημάτων ΤΝ να μπορούν να ερμηνεύουν το εξαχθέν αποτέλεσμα του συστήματος, η υποχρέωση ανθρώπινης εποπτείας κατά τη λειτουργία του συστήματος και ο σχεδιασμός του ώστε να επιτυγχάνεται το κατάλληλο επίπεδο ακριβείας, διαθεσιμότητας και κυβερνοασφάλειας[194] κ.α.

Προσέτι, ο έλεγχος της πλήρωσης των ανωτέρω υποχρεώσεων, θα πρέπει να ανατίθεται σε **ειδικές ελεγκτικές αρχές**, οι οποίες θα προβαίνουν στην σχετική επιβεβαίωση συμμόρφωσης προς τις απαιτήσεις του κανονισμού, η οποία μπορεί να συνίσταται και στην έκδοση πιστοποιητικών συμβατότητας[195] ή δήλωση συμμόρφωσης της ΕΕ με σήμανση CE[196]. Περαιτέρω, πριν την κυκλοφορία του στην αγορά και κατόπιν ολοκλήρωσης των προηγούμενων ελέγχων, το σύστημα καταχωρείται σε **ειδική βάση δεδομένων** της ένωσης[197]. Μετά την κυκλοφορία του συστήματος στην αγορά, το προταθέν σχέδιο κανονισμού περιλαμβάνει ένα δεύτερο επίπεδο υποχρεώσεων συμμόρφωσης, στο οποίο συμπεριλαμβάνεται η εγκατάσταση και λειτουργία **συστήματος παρακολούθησης[198]** του συστήματος ΤΝ και η υποχρεωτική υποβολή αναφοράς, στις δημόσιες αρχές, τυχόν σοβαρών περιστατικών ή παραβιάσεων της εθνικής ή της ενωσιακής νομοθεσίας για την προστασία των θεμελιωδών δικαιωμάτων που προκύπτουν από τη χρήση του συστήματος.[199]

---

[194] αρ. 8-15 Σχ. Καν. ΤΝ και περαιτέρω εξειδίκευση τους στα άρθρα 16-29 του κανονισμού.
[195] αρ. 44 Σχ. Καν. ΤΝ
[196] Conformité Européenne βλ. αρ. 48-49 σχ. Καν. ΤΝ
[197] αρ. 51 και 60 σχ Καν ΤΝ.
[198] Αιτ. Σκέψη 78 σχ Καν ΤΝ.
[199] Τσόλιας, Γ. (2021) 'Η περίπτωση των Συστημάτων Απομακρυσμένης Βιομετρικής Αναγνώρισης και Ταυτοποίησης φυσικών προσώπων για σκοπούς δίωξης του εγκλήματος σύμφωνα με το σχέδιο πρότασης Κανονισμού Ε.Ε. για την Τεχνητή Νοημοσύνη', σε *Διαρκής Επιστημονική Επιτροπή του Υπουργείου Δικαιοσύνης για την Τεχνητή Νοημοσύνη*.

3.3.2 Συστήματα εξ αποστάσεως βιομετρικής ταυτοποίησης σε «πραγματικό χρόνο» και «σε ύστερο χρόνο»

Η Επιτροπή στο προταθέν σχέδιο Κανονισμού, προβαίνει σε διάκριση μεταξύ των συστημάτων εξ αποστάσεως βιομετρικής αναγνώρισης (*Remote Biometric Identification*-RBI) σε «**πραγματικό χρόνο**» και σε «**ύστερο χρόνο**» και προτείνει να υπαχθούν σε διαφορετικό σύνολο κανόνων ανάλογα με τη χρήση τους και τους επαπειλούμενους κινδύνους που ενέχουν έκαστα[200]. Ως **συστήματα βιομετρικής ταυτοποίησης «σε πραγματικό χρόνο»** ορίζονται τα συστήματα που είναι σε θέση να συλλέγουν βιομετρικά δεδομένα και να εκτελούν τις διαδικασίες σύγκρισης και ταυτοποίησης αμέσως, σχεδόν αμέσως ή χωρίς σημαντική καθυστέρηση, επί τη βάση υλικού που λαμβάνεται σε «ζωντανή μετάδοση» ή «σχεδόν ζωντανή μετάδοση», όπως ένα βίντεο που παράγεται από κάμερα. Αντιθέτως, τα **συστήματα βιομετρικής ταυτοποίησης σε «ύστερο χρόνο»** αφορούν συστήματα ΤΝ που επιτρέπουν τη συλλογή βιομετρικών δεδομένων και την εκτέλεση των διαδικασιών σύγκρισης και ταυτοποίησης **με σημαντική καθυστέρηση**, επί τη βάση φωτογραφιών ή βίντεο που έχουν ληφθεί πριν χρησιμοποιηθεί το σύστημα για την ταυτοποίηση συγκεκριμένων υποκειμένων, από κάμερες κλειστού κυκλώματος τηλεόρασης (CCTV) ή ιδιωτικές συσκευές. Επισημαίνεται, επιπροσθέτως, ότι διάκριση γίνεται περαιτέρω και σε σχέση με τη χρήση των ανωτέρω συστημάτων **σε δημόσια προσβάσιμους- ή μη- χώρους**[201].

3.3.3 Η ρύθμιση της χρήσης των συστημάτων εξ αποστάσεως βιομετρικής ταυτοποίησης για σκοπούς επιβολής του νόμου

Ως θέμα αρχής, η Ευρωπαϊκή Επιτροπή προτείνει **να απαγορευτεί η χρήση, στο πλαίσιο δράσης των δημοσίων αρχών, συστημάτων τεχνητής νοημοσύνης για την εξ αποστάσεως βιομετρική ταυτοποίηση φυσικών προσώπων σε «πραγματικό χρόνο», σε χώρους προσβάσιμους από το κοινό για σκοπούς επιβολής του νόμου**. Τα εν λόγω συστήματα, εξαιτίας της υπέρμετρης φύσει επεμβατικότητάς τους στα δικαιώματα των θιγόμενων προσώπων, κατατάσσονται στην κατηγορία συστημάτων «**μη αποδεκτού κινδύνου**» και υπόκεινται σε **γενική απαγόρευση**.

Ωστόσο, το προτεινόμενο σχέδιο προβλέπει **τρεις εξαιρέσεις**[202]**,** στις οποίες η ύπαρξη σημαντικών λόγων ***δημοσίου συμφέροντος*** κρίνεται ότι αντισταθμίζει

σελ. 8-9. Διαθέσιμο στο: https://www.ministryofjustice.gr/wp-content/uploads/2021/11/TSOLIAS_sxKan_TNFRT.pdf

[200] Αιτ. Σκέψη 8, αρ. 3§36-38 Σχ. Καν. ΤΝ .

[201] Βλ. αρ. 3§39 Σχ. Καν. ΤΝ . «*δημόσια προσβάσιμος χώρος*»: *κάθε φυσικός χώρος προσβάσιμος στο κοινό, ανεξάρτητα από το αν τυχόν ισχύουν ορισμένοι όροι πρόσβασης*»

[202] αρ. 5 Σχ. Καν. ΤΝ .

τους κινδύνους για τα θεμελιώδη δικαιώματα των φυσικών προσώπων. Ειδικότερα, η χρήση των ανωτέρω συστημάτων σε πραγματικό χρόνο και σε δημόσια προσβάσιμους χώρους από τις αρχές, δύναται -κατ' εξαίρεση- να είναι επιτρεπτή για τους κάτωθι σκοπούς επιβολής του νόμου:

- τη στοχευμένη αναζήτηση πιθανών θυμάτων εγκλημάτων, συμπεριλαμβανομένων των εξαφανισμένων παιδιών.
- την πρόληψη επέλευσης συγκεκριμένης, σοβαρής και άμεσης απειλής για τη ζωή ή τη φυσική ασφάλεια προσώπων, ή τρομοκρατικών επιθέσεων
- την ανίχνευση, τον εντοπισμό, την αναγνώριση και τη δίωξη δράστη εγκλήματος ή υπόπτου ενός εκ των ποινικών αδικημάτων που περιλαμβάνονται στον κατάλογο της απόφασης-πλαίσιο για το ευρωπαϊκό ένταλμα σύλληψης, και **εφόσον τιμωρείται και κατά το δίκαιο του κράτους μέλους** με ποινή με ανώτατο όριο τουλάχιστον τα 3 έτη στέρησης της ελευθερίας.

Συνεπώς, η υιοθέτηση του υπό κρίση Κανονισμού[203], **θα θέσει εκτός νόμου τη χρήση συστημάτων αναγνώρισης προσώπου από τις αστυνομικές αρχές** για την ταυτοποίηση προσώπων που συμμετέχουν λ.χ. σε **δημόσιες διαμαρτυρίες,** ή για τον εντοπισμό ατόμων που έχουν διαπράξει **ήσσονος σημασίας αδικήματα**.

Προσέτι, οφείλει να καταστεί σαφές ότι **η χρήση των ανωτέρω συστημάτων εξακολουθεί να υπόκειται στις απαιτήσεις σεβασμού των αρχών που κατοχυρώνονται στο ευρωπαϊκό κεκτημένο για την προστασία των δεδομένων προσωπικού χαρακτήρα, καθώς και στις επιταγές συμμόρφωσης με επαρκείς διαδικαστικές εγγυήσεις.**

Ειδικότερα ως προς τα επαρκή διαδικαστικά εχέγγυα, το σχέδιο του Κανονισμού ορίζει[204] ότι **πριν από τη χρήση** των συστημάτων εξ αποστάσεως βιομετρικής ταυτοποίησης, θα πρέπει να χορηγείται **ρητή και ειδική άδεια από δικαστική αρχή ή από ανεξάρτητη διοικητική αρχή** του κράτους μέλους, δοθείσα μόνον εφόσον έχουν προσκομισθεί αντικειμενικά αποδεικτικά στοιχεία ή υπάρχουν εναργείς ενδείξεις ότι η χρήση του εν λόγω συστήματος είναι αναγκαία και αναλογική για την επίτευξη ενός εκ των εξαιρετικών ως άνω σκοπών, **εκτός από δεόντως αιτιολογημένες καταστάσεις**, ήτοι περιπτώσεις κατά τις οποίες η ανάγκη άμεσης χρήσης των εν λόγω συστημάτων καθιστά τη λήψη άδειας πριν από την έναρξη της χρήσης τους, πρακτικά και αντικειμενικά αδύνατη. **Σε αυτές**

[203] Σε περίπτωση υιοθέτησής του, οι διατάξεις του Κανονισμού θα εφαρμόζονται ως lex specialis εκείνων του άρθρου 10 της Οδηγίας, βλ. Τσόλιας (2021) ο.π. σελ. 13.
[204] αρ. 5 Σχ. Καν. ΤΝ .

τις κατεπείγουσες περιπτώσεις, η χρήση θα πρέπει να περιορίζεται στο απολύτως αναγκαίο και να υπόκειται σε κατάλληλες εγγυήσεις, όπως προβλέπονται σε εναργείς και αναλυτικές ρυθμίσεις του εκάστοτε εθνικού δικαίου και **εξειδικεύονται στο πλαίσιο κάθε επιμέρους περίπτωσης** επείγουσας χρήσης από την ίδια την αρχή επιβολής του νόμου. Επισημαίνεται επιπροσθέτως, ότι σε τέτοιες περιπτώσεις, **η αρχή επιβολής του νόμου θα πρέπει να επιδιώκει να λάβει άδεια το συντομότερο δυνατόν**, αιτιολογώντας, παραλλήλως, σαφώς τους λόγους για τους οποίους δεν ήταν σε θέση να υποβάλλει αίτημα χορήγησης άδειας προ της χρήσεως της τεχνολογίας.[205]

Όπως προκύπτει εκ των ανωτέρω, στο πλαίσιο του προτεινόμενου κανονισμού, **επαφίεται στη διακριτική ευχέρεια των κρατών μελών η απόφαση ενσωμάτωσης ή μη, εν όλω ή εν μέρει, των προαναφερθεισών εξαιρέσεων στην εθνική τους νομοθεσία**. Σε περίπτωση, όμως, που επιτραπεί από το κράτος- μέλος η κατ' εξαίρεσιν χρήση συστημάτων απομακρυσμένης βιομετρικής ταυτοποίησης για σκοπούς επιβολής του νόμου σε δημόσια προσβάσιμους χώρους και σε πραγματικό χρόνο, αυτή θα πρέπει να διενεργείται πάντοτε σύμφωνα με τους προβλεπόμενους όρους και τις εγγυήσεις που θέτει ο κανονισμός, τα οποία θα πρέπει να ενσωματωθούν στον εθνικό νόμο, στον οποίο επιπλέον θα πρέπει να προσδιορίζεται η αρμόδια αρχή που θα παρέχει την άδεια για τη χρήση των συστημάτων αυτών. Επισημαίνεται, επιπροσθέτως, ότι **στην προστατευτική εμβέλεια των ανωτέρω εγγυήσεων φαίνεται ότι δεν εντάσσονται οι περιπτώσεις χρήσης συστημάτων ΤΝ ετεροχρονισμένης λειτουργίας από τις δημόσιες αρχές.**

3.3.4 Βιομετρικά συστήματα κατηγοριοποίησης

Οφείλει, επίσης, να επισημανθεί ότι στο προταθέν σχέδιο Κανονισμού τα βιομετρικά συστήματα κατηγοριοποίησης, ήτοι τα συστήματα ΤΝ που έχουν ως σκοπό την κατανομή των φυσικών προσώπων σε συγκεκριμένες κατηγορίες, ανάλογα με *το φύλο, την ηλικία, το χρώμα μαλλιών, το χρώμα οφθαλμών, τη δερματοστιξία, την εθνοτική καταγωγή ή το γενετήσιο ή πολιτικό προσανατολισμό*[206], βάσει της επεξεργασίας των βιομετρικών δεδομένων τους, **όταν δεν στοχεύουν σαφώς και στην ταυτοποίηση αυτών, δεν κατατάσσονται στην κατηγορία βιομετρικών συστημάτων υψηλού κινδύνου**. Ως εκ τούτου τα συστήματα αυτά θα υπόκεινται μόνο σε **μέτρα διαφάνειας** και σε υποχρέωση ενημέρωσης των υποκειμένων που εκτίθενται σε

[205] Αιτ. Σκέψη 21 Σχ. Καν. ΤΝ .
[206] αρ. 3§35 σχ. Καν. ΤΝ

αυτό, εκτός εάν η χρήση επιτρέπεται από τον νόμο για την ανίχνευση, την πρόληψη και τη διερεύνηση ποινικών αδικημάτων.[207]

Ως ευλόγως συνάγεται, η εν λόγω πρόβλεψη αφήνει μετέωρη τη ρύθμιση των συστημάτων αναγνώρισης προσώπου που χρησιμοποιούνται μεν για σκοπούς κατηγοριοποίησης, δύνανται, δε, λόγω της ενσωμάτωσης εφαρμογών τεχνητής νοημοσύνης, να ταυτοποιούν εμμέσως τα υποκείμενα, συσχετίζοντας τα δεδομένα τους, και καταρτίζοντας εξ αυτών ένα πλήρες προφίλ που εμπεριέχει τόσο απλά, όσο και ευαίσθητα δεδομένα του υποκειμένου.

3.3.5 Η κριτική

Η δημοσίευση του υπό κρίση σχεδίου Κανονισμού, προκάλεσε θετικές αλλά και αρνητικές αντιδράσεις, οι οποίες, αναφορικά με τα συστήματα αναγνώρισης προσώπου, επικεντρώθηκαν στην πλημμελή προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών των ατόμων από την επικινδυνότητα της τεχνολογίας. Κατ' αρχάς, κατακρίθηκε έντονα η διάκριση και η διαφορετική ρύθμιση των συστημάτων εξ αποστάσεως βιομετρικής παρακολούθησης σε «πραγματικό χρόνο» και «σε ύστερο χρόνο», καθώς, όπως επισημάνθηκε, η ετεροχρονισμένη ταυτοποίηση των φυσικών προσώπων δύναται να παραβιάσει τα δικαιώματα των υποκειμένων στο ίδιο μέτρο και με την ίδια ένταση με τη «ζωντανή» τεχνολογία αναγνώρισης προσώπου. Ομοίως, η διάκριση των συστημάτων σε συστήματα «βιομετρικής κατηγοριοποίησης» και «βιομετρικής αναγνώρισης», υποστηρίχθηκε ότι είναι αυθαίρετη, διότι η βιομετρική κατηγοριοποίηση μπορεί εκ των πραγμάτων να επιτρέπει την ταυτοποίηση (π.χ. ad hoc αναζήτηση ατόμων με σκούρο δέρμα που διήλθαν από μια συγκεκριμένη τοποθεσία στην οποία υπάρχει κάμερα CCTV), και ως εκ τούτου μπορεί να έχει εξίσου αρνητικές επιπτώσεις στα θεμελιώδη δικαιώματα με τα συστήματα που αποβλέπουν ευθέως σε ταυτοποίηση. Για το λόγο αυτό, ερευνητές τονίζουν ότι οι βιομετρικές κατηγοριοποιήσεις πληρούν όλες τις προϋποθέσεις για να χαρακτηριστούν ως συστήματα υψηλού κινδύνου και να ενταχθούν ρητά στον κατάλογο του παραρτήματος ΙΙΙ της πρότασης[208].

Επιπλέον, επισημάνθηκε ότι η προτεινόμενη προσέγγιση θα μπορούσε να παραβλέψει την ικανότητα των βιομετρικών συστημάτων που αναπτύσσονται από ιδιωτικούς φορείς να έχουν ανασταλτικό αποτέλεσμα στην άσκηση των θεμελιωδών δικαιωμάτων (π.χ. εάν οι ιδιωτικοί φορείς μοιράζονται πληροφορίες με τις αρχές επιβολής του νόμου ή συνεργάζονται με αυτές, όπως στην περίπτωση της Clearview AI). Στο πλαίσιο αυτό, ακαδημαϊκοί έχουν προτείνει την

[207] αρ. 52§2 σχ. Καν. ΤΝ
[208] Madiega, T., Mildebrath, H. (2021), ο.π. σελ. 28-30.

αναθεώρηση των προτεινόμενων ορισμών, συμπεριλαμβανομένων των «βιομετρικών δεδομένων» και των «συστημάτων βιομετρικής ταυτοποίησης», οι οποίοι θεωρούνται πολύ στενοί, και τη δυνατότητα πιο ευέλικτης προσαρμογής του καταλόγου των απαγορευμένων πρακτικών ΤΝ. Επιπλέον, αποζητάται μια πιο αυστηρή αιτιολόγηση της διάκρισης που γίνεται μεταξύ ιδιωτικών και δημόσιων χρήσεων των απομακρυσμένων βιομετρικών συστημάτων, ώστε να υποστηριχθεί η διαφοροποίηση των εφαρμοστέων νομικών κανόνων.

Ομοίως, ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων τόνισε ότι η πρόταση δεν αντιμετωπίζει λυσιτελώς τον επαπειλούμενο κίνδυνο όσον αφορά στην εξ αποστάσεως βιομετρική ταυτοποίηση και τάχθηκε υπέρ μιας **αυστηρότερης προσέγγισης στην αυτοματοποιημένη αναγνώριση σε δημόσιους χώρους**, ανεξάρτητα από το αν χρησιμοποιείται για εμπορικούς σκοπούς ή για σκοπούς επιβολής του νόμου[209]. Επιπροσθέτως, σε κοινή μη δεσμευτική γνωμοδότηση[210], ο ΕΕΠΔ και το ΕΣΠΔ **ζήτησαν τη γενική απαγόρευση κάθε χρήσης της ΤΝ για την αυτοματοποιημένη αναγνώριση ανθρώπινων χαρακτηριστικών** -όπως η αναγνώριση προσώπου- **σε χώρους προσβάσιμους στο κοινό.** Προσέτι, το ΕΣΠΔ και ο ΕΕΠΔ συνιστούν την **πλήρη απαγόρευση και των εξίσου επικίνδυνων συστημάτων αναγνώρισης προσώπου που χρησιμοποιούνται για την κατηγοριοποίηση** ατόμων ανάλογα με ευαίσθητα χαρακτηριστικά, όπως η εθνικότητα, το φύλο, ο πολιτικός ή σεξουαλικός προσανατολισμός, καθώς η χρήση τους μπορεί να οδηγήσει σε **αθέμιτες διακρίσεις**.

---

[209] European Data Protection Supervisor (2021) *Artificial Intelligence Act: a welcomed initiative, but ban on remote biometric identification in public space is necessary*. Διαθέσιμο στο: https://edps.europa.eu/press-publications/press-news/press-releases/2021/artificial-intelligence-act-welcomed-initiative_en

[210] EDPB-EDPS (2021) '*Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*'. Διαθέσιμο στο: https://edps.europa.eu/system/files/2021-06/2021-06-18-edpb-edps_joint_opinion_ai_regulation_en.pdf

ΕΠΙΛΟΓΟΣ

Οι εφαρμογές τεχνητής νοημοσύνης έδωσαν νέα πνοή στα συστήματα αναγνώρισης προσώπου, μεγιστοποιώντας τη δυναμική τους και καθιστώντας τα ηγέτη στην αγορά των βιομετρικών τεχνολογιών. Η τεχνολογία αναγνώρισης προσώπου ενέχει πράγματι πληθώρα δυνατοτήτων και έχει αποδειχθεί πολύτιμο και καινοτόμο εργαλείο για ποικίλους σκοπούς, ιδίως σε ό,τι αφορά στη δημόσια ασφάλεια, στη δημόσια υγεία και στο συνοριακό έλεγχο. Παραλλήλως, η τεχνολογία γίνεται όλο και πιο παρούσα σε πολλές πτυχές της καθημερινής ζωής, από το «ξεκλείδωμα» μίας συσκευής, έως τον έλεγχο πρόσβασης σε χώρους ζωτικής σημασίας, όπως τα μέσα μαζικής μεταφοράς και τα σχολεία.

Ενώ υπάρχουν αδιαμφισβήτητα οφέλη από τη χρήση συστημάτων αναγνώρισης προσώπου, η εγγενής διεισδυτικότητα και παρεμβατικότητα της τεχνολογίας, σε συνδυασμό με την ευαισθησία της σε σφάλματα, ανήγειραν μια σειρά από ανησυχίες για τα θεμελιώδη δικαιώματα και τις ελευθερίες των πολιτών στις σύγχρονες δημοκρατικής κοινωνίες και οδήγησαν την παγκόσμια επιστημονική κοινότητα στον χαρακτηρισμό της ως «*το πλουτώνιο της τεχνητής νοημοσύνης*». Ο προβληματισμός εντοπίζεται ιδιαίτερα στην κρισιμότητα των αλγοριθμικών σφαλμάτων, τα οποία οφείλονται σε γνωστούς αλλά και εν πολλοίς άγνωστους λόγους, αφού ο επακριβής καθορισμός των παραμέτρων και της «λογικής» που οδηγούν το λογισμικό στην εξαγωγή του εκάστοτε αποτελέσματος συσκοτίζονται από το φαινόμενο του «μαύρου κουτιού». Ιδιαίτερα επιβλαβής έχει αποδειχθεί η ανακρίβεια που κατατρέχει την τεχνολογία όταν χρησιμοποιείται σε μη- ελεγχόμενα περιβάλλοντα, κυρίως λόγω της ανεπαρκούς εκπαίδευσης των αλγορίθμων σε πλημμελή ποσοτικά ή/ και ποιοτικά σύνολά, τα οποία συχνά πάσχουν από φαινόμενα υπερ- εκπροσώπησης κυριάρχων κοινωνικά ομάδων και υπο-εκπροσώπησης μειονοτικών πληθυσμών, καθώς και η συνακόλουθη – εκούσια ή ακούσια- ενσωμάτωση κοινωνικών προκαταλήψεων, η οποία δύναται να «ψηφιοποιήσει» και να διαιωνίσει τις συστημικές κοινωνικές ανισότητες, βάλλοντας δυσανάλογα τις μειονοτικές ομάδες του πληθυσμού.

Περαιτέρω, η δυναμική που προσέφερε η τεχνητή νοημοσύνη, ιδίως η βαθιά μάθηση, στα συστήματα αναγνώρισης προσώπου, σε συνδυασμό με την απουσία ενός σαφούς νομικού πλαισίου, ευνόησε σύντομα την άκρατη μετατόπισή τους στη δημόσια σφαίρα, αρχικώς σε ημι- δημόσιους χώρους (λ.χ. τα αεροδρόμια) και σταδιακά σε δημόσιους, όπου χρησιμοποιήθηκαν σε μεγάλης κλίμακας συλλογή και επεξεργασία δεδομένων, ελεγχόμενες κατά κύριο λόγο από τις αρχές επιβολής του νόμου, ή ιδιωτικές εταιρείες που δραστηριοποιούνται στον τομέα της ασφάλειας και εμπορεύονται τις υπηρεσίες τους στις αστυνομικές αρχές όλης της υφηλίου. Κατ' αυτόν τον τρόπο, η τεχνολογία αναγνώρισης προσώπου επέφερε ένα βαρύ πλήγμα στην –εύθραυστη- ισορροπία ανάμεσα στο

κράτος και τους πολίτες, επιτείνοντας την αδύναμη θέση των υποκειμένων απέναντι σε ένα «πανταχού παρόν» κράτος, το οποίο δύναται ανά πάσα στιγμή να συλλέγει μαζικά και να θέτει κατά το δοκούν υπό επεξεργασία για σκοπούς αδιαμφισβήτητης ταυτοποίησης ένα νευραλγικό δεδομένο της ανθρώπινης ταυτότητας· την εικόνα προσώπου του.

Ο κίνδυνος γενικευμένης κρατικής παρακολούθησης, και η δυνατότητα των συστημάτων αναγνώρισης προσώπου να προβαίνουν σε τεχνικά μη επεμβατική συλλογή των βιομετρικών δεδομένων, ήτοι χωρίς να απαιτείται η σύμπραξη, η συναίνεση ή και η ίδια η γνώση των υποκειμένων τους, καλλιεργούν ένα αίσθημα φόβου ικανό να περιορίσει σημαντικά θεμελιώδεις ελευθερίες, όπως το δικαίωμα στην ελεύθερη έκφραση, στην ανάπτυξη της προσωπικότητας και στο συνέρχεσθαι και συνεταιρίζεσθαι. Τα άτομα με μόνη την γνώση της εγκατάστασης της τεχνολογίας, αυτοπεριορίζονται, απομακρύνονται από το δημόσιο χώρο και στρέφονται προς τα έσω, προσπαθώντας να διαφυλάξουν την ιδιωτικότητα τους. Τα απτά παραδείγματα κρύφιας χρήσης της τεχνολογίας από τις αρχές, και προμήθειάς της από σκιώδεις εταιρείες που μετέρχονται αθέμιτων πρακτικών, όπως η ιστοσυγκομιδή, για τη μαζική και αδιάκριτη συλλογή βιομετρικών δεδομένων από κάθε πιθανή γωνιά του κυβερνοχώρου, επιτείνουν την προβληματική κι εύλογα θέτουν το ερώτημα αν η de facto αδυναμία ανώνυμης μετακίνησης στο δημόσιο χώρο, και ο επακόλουθος κομφορμισμός των πολιτών προκειμένου να μην απόσχουν από τις κοινωνικές νόρμες, μπορεί τελικά να σηματοδοτεί το τέλος της ιδιωτικότητας.

Εν προκειμένω εντοπίζεται η καρδιά της προβληματικής: η ιδιωτικότητα και το δικαίωμα του ατόμου στον πληροφοριακό του αυτοκαθορισμό, αποτελούν προϋπόθεση για την οικοδόμηση και διαφύλαξη της προσωπικής του σφαίρας -δίχως αυτή απειλείται η ίδια η ανθρώπινη αξιοπρέπεια- αλλά και για τη συμμετοχή του στο κοινωνικοπολιτικό γίγνεσθαι- δίχως αυτή απειλείται το ίδιο το δημοκρατικό πολίτευμα. Οι κρίσιμες ηθικές και κοινωνικοπολιτικές προεκτάσεις της εργαλειοποίησης της τεχνολογίας αναγνώρισης προσώπου, φωτίζουν τις νομικές πλημμέλειες κατά την ανάπτυξη και χρήση της και καλούν για μια επισκόπηση του ισχύοντος νομικού πλαισίου, προκειμένου αυτό να αποτιμηθεί και να διασαφηνιστεί αν μπορεί να αντιμετωπίσει επαρκώς τις επαπειλούμενες επιπτώσεις, δίχως να αναχαιτίσει υπέρμετρα την καινοτομία, τη -θεμιτή και προσδωκόμενη- ανάπτυξη και τα επακόλουθα οφέλη που προσφέρει στην κοινωνία και στην επιστήμη η Τεχνητή Νοημοσύνη.

Σε πρωτογενές επίπεδο, ο Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης προασπίζει τα δικαιώματα στο σεβασμό της ιδιωτικής ζωής και στην προστασία των προσωπικών δεδομένων και ορίζει ρητώς ότι οποιαδήποτε επέμβαση σε αυτά, όπως η επεξεργασία βιομετρικών δεδομένων,

οφείλει να περιορίζεται στο απολύτως αναγκαίο και αναλογικό, πάντοτε με σεβασμό στον ουσιώδη και αναφαίρετο πυρήνα των δικαιωμάτων. Η νομολογία των ευρωπαϊκών δικαστηρίων προσφέρει πολύτιμη καθοδήγηση κατά την εκτίμηση της νομιμότητας του περιορισμού των εν θέματι δικαιωμάτων και της αναγκαιότητας και αναλογικότητας χρήσης της τεχνολογίας αναγνώρισης προσώπου σε μια δημοκρατική κοινωνία, ιδιαίτερα στο πλαίσιο δράσης των δημοσίων αρχών, συνεισφέροντας παραλλήλως χρήσιμα ερμηνευτικά εργαλεία ως προς τη διασαφήνιση αόριστων εννοιών όπως «ο σκοπός γενικού συμφέροντος».

Δίπλα στις εγγυήσεις και στις βασικές αρχές που απορρέουν από το Χάρτη, στέκουν τα ειδικότερα εχέγγυα που προβλέπει το κοινοτικό κεκτημένο για την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως ο Γενικός Κανονισμός για την Προστασία των Δεδομένων και η Οδηγία επιβολής του νόμου. Εντός του κανονιστικού πλαισίου που θέτουν αυτά, μόνον κατ' εξαίρεση δύναται να επιτρέπεται η επεξεργασία των εικόνων προσώπου μέσω των συστημάτων αναγνώρισης προσώπου και υπό την απαρέγκλιτη προϋπόθεση της συμμόρφωσης και του σεβασμού των θεμελιωδών αρχών επεξεργασίας.

Εντούτοις, η τεχνολογία αναγνώρισης προσώπου, η οποία ενσωματώνει εξ ορισμού πλέον τις εφαρμογές μηχανικής μάθησης, εγείρει προκλήσεις κατά τη συμμόρφωση στις επιταγές της νομοθεσίας περί την προστασία προσωπικών δεδομένων. Η αλγοριθμική αδιαφάνεια και η ανάγκη μεγάλης ποσότητας και ποικιλομορφίας δεδομένων προκειμένου να εκπαιδευτεί λυσιτελώς το λογισμικό αναγνώρισης προσώπου και να αποφευχθούν τα ποσοστά τεχνικών ανακριβειών, σε συνδυασμό με τη δυνατότητα της τεχνολογίας να συλλέγει μαζικά, αδιάκριτα και εξ αποστάσεως, δίχως τη συγκατάθεση, τη γνώση και τη συνδρομή των υποκειμένων, τα βιομετρικά τους δεδομένα, θέτουν υπό αμφισβήτηση την ίδια τη συμβατότητα της τεχνολογίας με τις αρχές, μεταξύ άλλων, της διαφάνειας, της λογοδοσίας, της ελαχιστοποίησης και της ασφαλείας, δυσχεραίνοντας κάθε προσπάθεια του υπευθύνου επεξεργασίας να συμμορφωθεί προς τις υποχρεώσεις του.

Περαιτέρω όμως, η δυσχέρεια -ή αδυναμία- πλήρωσης των απαιτήσεων που θέτει η νομοθεσία στον υπεύθυνο επεξεργασίας, ιδίως δε τα προσκόμματα κατά την διασφάλιση της αρχής της διαφάνειας, συμπαρασύρουν επακόλουθα τη δυνατότητα λυσιτελούς άσκησης εκ μέρους των υποκείμενων των κατοχυρωμένων δικαιωμάτων τους έναντι της επεξεργασίας των βιομετρικών τους δεδομένων. Ιδιαίτερα σε περίπτωση πλήρους άγνοιας της χρήσης της τεχνολογίας αναγνώρισης προσώπου, κατάσταση υπό την οποία συχνά τελείται η επεξεργασία, τα υποκείμενα στερούνται πλήρως και εκ προοιμίου τη δυνατότητα άσκησης οποιουδήποτε εκ των δικαιωμάτων τους. Το γεγονός αυτό

καθίσταται ακόμη κρισιμότερο κατά τη χρήση της τεχνολογίας για σκοπούς επιβολής του νόμου, καθώς στρεβλώνεται έτι περαιτέρω η ανισορροπία δυνάμεων κράτους και πολιτών, οι οποίοι εκτίθενται ανεξαρτήτως αποχρωσών ενδείξεων σε τυχούσες αυθαιρεσίες των αρχών, αλλά και στις εγγενείς αδυναμίες της τεχνολογίας να παράγει πάντοτε ακριβή, δίκαια και διαφανή αποτελέσματα.

Προκειμένου να είσαι σε θέση να αποδείξει τη συμμόρφωσή του στις αυξημένες απαιτήσεις που θέτουν οι αλγόριθμοι αναγνώρισης προσώπου, ο υπεύθυνος επεξεργασίας καλείται κατ' αρχάς να ελέγχει κάθε φορά ότι συντρέχει μία εκ των εξαιρετικών περιπτώσεων που επιτρέπουν την επεξεργασία των εικόνων προσώπου, εξετάζοντας παραλλήλως την αναγκαιότητα της επεξεργασίας των βιομετρικών δεδομένων των υποκειμένων, την προσφορότητα και καταλληλότητα αυτής για την επίτευξη του εκάστοτε νόμιμου και συγκεκριμένου σκοπού, όπως και την τυχούσα ύπαρξη ηπιότερων μέσων εκπλήρωσης αυτού, συνυπολογίζοντας κατά την εκάστοτε ανάλυση επιμέρους παραμέτρους όπως οι **εύλογες προσδοκίες** των υποκειμένων, ούτως ώστε να διασφαλιστεί η υπαγωγή της τεχνολογίας κατ' ουσίαν και όχι τύποις στα προαπαιτούμενα του νόμου. Παραλλήλως, ο υπεύθυνος επεξεργασίας οφείλει να διασφαλίζει ότι τα θιγόμενα άτομα μπορούν να ασκήσουν αποτελεσματικά τα δικαιώματά τους, λ.χ. ενημερώνοντας εναργώς τα υποκείμενα για την επεξεργασία των βιομετρικών δεδομένων τους, ιδίως όταν αυτά ανήκουν σε ευάλωτες κατηγορίες (λ.χ. παιδιά), όπως και όταν η απόφαση λαμβάνεται με πλήρως αυτοματοποιημένη διαδικασία, ήτοι χωρίς υπεισέλευση του ανθρώπινου παράγοντα, παρέχοντας κατά το δυνατό κάθε πληροφορία για τη λογική που ακολουθήθηκε και αιτιολογώντας την εκάστοτε απόφαση, στο μέτρο που καθίσταται εφικτό από την τεχνολογία και από τους περιορισμούς που τίθενται από το δίκαιο διανοητικής ιδιοκτησίας και τα επιχειρηματικά απόρρητα.

Περαιτέρω ιδιαίτερη μέριμνα πρέπει να λαμβάνεται ούτως ώστε να διασφαλίζεται η συμμόρφωση με την **αρχή του περιορισμού του σκοπού της επεξεργασίας**, ήτοι να εξασφαλιστεί ότι η επεξεργασία διεξάγεται για νόμιμους καθορισμένους και ρητούς σκοπούς και ότι τα βιομετρικά δεδομένα δεν θα υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο με αυτούς, δίχως να υπάρχει μια διακριτή, έγκυρη και νόμιμη βάση. Η εν λόγω επιταγή καθίσταται κρίσιμη λόγω της **διαλειτουργικότητας των συστημάτων τεχνητής νοημοσύνης**, η οποία εντείνει τον **κίνδυνο «υφέρπουσας διεύρυνσης των λειτουργιών»** των συστημάτων αναγνώρισης προσώπου, δηλαδή επέκτασης τής μέσω αυτών επεξεργασίας των βιομετρικών δεδομένων για άλλους σκοπούς, δίχως να υφίσταται νόμιμο έρεισμα που να τους δικαιολογεί. Η συμμόρφωση με την εν λόγω αρχή αποκτά **ιδιαίτερη σημασία εντός της Ε.Ε.**, δεδομένης της διαθεσιμότητας ποικίλων **βάσεων βιομετρικών δεδομένων τεράστιας**

κλίμακας.[211] Εν προκειμένω, αναδεικνύεται και η ανάγκη αυστηρής εφαρμογής της αρχής περιορισμού της περιόδου αποθήκευσης των δεδομένων, κατ' αναλογία με τα προβλεπόμενα για τα συστήματα βιντεοεπιτήρησης.

Προσέτι, ο υπεύθυνος επεξεργασίας, οφείλει να μετριάζει τους κινδύνους που απορρέουν από την αλγοριθμική αδιαφάνεια, προβαίνοντας σε έναν **ποιοτικό έλεγχο των δεδομένων που τροφοδοτούν τον αλγόριθμο**. Στόχος του πρέπει να είναι η διασφάλιση ότι τα εκπαιδευτικά σύνολα δεδομένων απαρτίζονται από βιομετρικά πρότυπα που έχουν ληφθεί υπό κατάλληλες τεχνικές συνθήκες, οι οποίες επέτρεψαν την ευκρινή απεικόνιση των υποκειμένων, καθώς και η μέριμνα συλλογής δεδομένων που αντιπροσωπεύουν δίκαια το σύνολο των ομάδων του πληθυσμού, ανεξαρτήτως λ.χ. φύλου, εθνοτικής καταγωγής, ηλικίας, προκειμένου να αποσοβηθούν οι κίνδυνοι που απορρέουν τόσο από τις τεχνικές ανακρίβειες, όσο και από την παρείσδυση στον αλγόριθμο πάσης φύσεως μεροληψιών[212].

Τα κατάλληλα τεχνικά και οργανωτικά μέτρα που καλείται να υιοθετεί ο υπεύθυνος και ο εκτελών την επεξεργασία καθ' όλη τη διάρκεια της επεξεργασίας των βιομετρικών δεδομένων, πρέπει σε κάθε περίπτωση να εξασφαλίζουν την ασφάλεια των δεδομένων από κάθε πιθανή παραβίαση, αλλοίωση, φθορά ή απώλεια, γεγονότα που λόγω του ευαίσθητου χαρακτήρα και της μοναδικότητας της εικόνας προσώπου για την ταυτότητα του ατόμου, δύνανται να επιφέρουν κρίσιμα και μη αναστρέψιμα αποτελέσματα σε περίπτωση που επέλευσης κάποιου εκ των κινδύνων. Σε αυτό το σημείο χρήσιμη αποδεικνύεται η **ενσωμάτωση και η συμμόρφωση με διεθνή πρότυπα ασφαλείας**, με χαρακτηριστικό παράδειγμα το **ISO 24745** που αφορά ειδικότερα στην ασφάλεια των πληροφοριών που εξάγονται από βιομετρικά δεδομένα. Επιπρόσθετα, σε περίπτωση προμήθειας της τεχνολογίας αναγνώρισης προσώπου από τρίτους, θα πρέπει να συμπεριλαμβάνονται κατά τη σύναψη των σχετικών συμβάσεων, ειδικές προβλέψεις ικανές να εγγυηθούν ότι ο **εξωτερικός πάροχος θα**

---

[211] Όπως το Σύστημα Πληροφοριών Σένγκεν (SIS), το Σύστημα Πληροφοριών για τις Θεωρήσεις (VIS), το Eurodac,το Σύστημα Πληροφοριών και Αδειοδότησης Ταξιδιού (ETIAS), το Ευρωπαϊκό Σύστημα Πληροφοριών Ποινικού Μητρώου (ECRIS-TCN) κ.α.

[212] Οφείλει να σημειωθεί ότι, όπως υπογράμμισε ο ΕΕΠΔ, προκειμένου να αυξήσουν την αποτελεσματικότητα των συστημάτων τους, οι ιδιωτικές εταιρείες αναθέτουν συχνά την «εργασία» της διόρθωσης των μεροληψιών σε χώρες εκτός Ε.Ε., στις οποίες η προστασία και τα δικαιώματα των εργαζομένων είναι πολύ πιο περιορισμένα. Συνεπώς, προ της υιοθέτησης οποιουδήποτε μέτρου, θα πρέπει πάντοτε να λαμβάνεται υπόψη και ο ευρύτερος αντίκτυπος στην κοινωνία και στα θεμελιώδη ανθρώπινα δικαιώματα, ο οποίος εν προκειμένω καθίσταται μάλλον αβέβαιος. Βλ. European Data Protection Supervisor (2020) 'AI and Facial Recognition: Challenges and Opportunities'. Διαθέσιμο στο: https://edps.europa.eu/press-publications/press-news/blog/ai-and-facial-recognition-challenges-and-opportunities_en

δεσμεύεται να παραδώσει ένα σύστημα αναγνώρισης προσώπου που θα ανταποκρίνεται πλήρως στις αυξημένες απαιτήσεις ασφαλείας. Προσέτι, ιδιαίτερη μέριμνα θα πρέπει να ληφθεί και για την **ενσωμάτωση κατάλληλων τεχνικών μέτρων ώστε να αντιμετωπίζονται συγκεκριμένα οι επιθέσεις απέναντι στις οποίες τα συστήματα έχουν βρεθεί ευάλωτα** (όπως οι επιθέσεις morphing), μέτρα τα οποία θα πρέπει να είναι ευέλικτα και να εξελίσσονται διαρκώς προκειμένου να ανταποκρίνονται στις μεταβαλλόμενες απειλές.

Η ανάγκη ενισχυμένης περιφρούρησης της ασφάλειας της επεξεργασίας αντανακλάται περαιτέρω στην απαίτηση να υιοθετεί ο υπεύθυνος επεξεργασίας **εγκαίρως ήδη από το σχεδιασμό** και καθ' όλη τη διάρκειά της τα κατάλληλα εργαλεία συμμόρφωσης, αφότου έχει συνεκτιμήσει μια σειρά κρίσιμων για την εκάστοτε περίπτωση ανάπτυξης ή/ και χρήσης της τεχνολογίας παραγόντων, όπως η ιδιαίτερη φύση, του πεδίο εφαρμογής, το πλαίσιο και οι εκάστοτε σκοποί επεξεργασίας, πάντοτε με γνώμονα τους κινδύνους για τα θεμελιώδη δικαιώματα των υποκειμένων. Στο εν λόγω πλαίσιο, ο υπεύθυνος θα πρέπει να χρησιμοποιεί τεχνολογίες ενίσχυσης της ιδιωτικότητας, όπως η ψευδωνυμοποίηση, το συντομότερο δυνατόν, φροντίζοντας περαιτέρω για την κρυπτογράφηση, ελαχιστοποίηση της επεξεργασίας των δεδομένων και ενσωμάτωση των απαραίτητων εγγυήσεων, κατά τρόπο ώστε να πληρούνται οι απαιτήσεις του νομικού πλαισίου και να προστατεύονται ουσιωδώς τα δικαιώματα των υποκειμένων των δεδομένων.

Περαιτέρω, λόγω του φύσει **υψηλού κινδύνου** των συστημάτων αναγνώρισης προσώπου, χρήσιμο εργαλείο αλλά και αδήριτη υποχρέωση για τον υπεύθυνο επεξεργασίας, συνιστά η **διενέργεια εκτίμησης αντικτύπου για την προστασία των δεδομένων προσωπικού χαρακτήρα** (ΕΑΠΔ), καθώς και η **προηγούμενη διαβούλευση με την αρμόδια εποπτική αρχή**. Προκειμένου να ενισχυθεί η εμπιστοσύνη και η ασφάλεια, θα μπορούσε να υιοθετηθεί και η πρόταση του ΕΣΠΔ περί **δημοσίευσης των αποτελεσμάτων** της ΕΑΠΔ, ή τουλάχιστον των κύριων ευρημάτων αυτής. Ο ρόλος του Αρχών Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, ως ανεξάρτητων φορέων, θα είναι καθοριστικός για τη λυσιτελή διασφάλιση των δικαιωμάτων και ελευθεριών των υποκειμένων απέναντι στην παρεμβατικότητα της αλγοριθμικής αναγνώρισης προσώπου. Παραλλήλως, το ΕΣΠΔ καλείται να συνεχίσει να συνεπικουρεί το έργο των υπευθύνων επεξεργασίας, όσο η βιομηχανία αναγνώρισης προσώπου εξελίσσεται και οι εφαρμογές της -και μαζί οι κίνδυνοι που ενέχει- πολλαπλασιάζονται.

Επισημαίνεται εν προκειμένω ότι έχει προταθεί και η διενέργεια **άλλων ειδών εκτιμήσεων αντικτύπου** «κατ' εικόνα και καθ' ομοίωσιν» της ΕΑΠΔ. Ειδικότερα, κατά την πρακτική που ακολουθείται στον Καναδά και στις Η.Π.Α.

έχει προταθεί η **εκτίμηση «αλγοριθμικού» αντικτύπου**, αλλά και η **εκτίμηση αντικτύπου για τα θεμελιώδη δικαιώματα**. Η τελευταία, αν και τελικά απορρίφθηκε ως περιττή λόγω ύπαρξης της ΕΑΠΔ, αποτέλεσε αντικείμενο συζήτησης κατά την κατάρτιση του σχεδίου Κανονισμού για την Τεχνητή Νοημοσύνη[213]. Επιπλέον, έχει προταθεί η προηγούμενη λήψη **γνωμοδοτήσεων** α) από επιτροπές εμπειρογνωμόνων, οι οποίες θα επικεντρώνονται στην τεχνική αρτιότητα των αλγορίθμων, β) από επιτροπές ηθικής, αλλά και γ) από την κοινή γνώμη, κατόπιν δημοσιοποίησης των αποτελεσμάτων της ΕΑΠΔ[214].

Παραλλήλως, όμως θα πρέπει να υπάρξει και **ευαισθητοποίηση των πολιτών** σχετικά με τη χρήση της τεχνολογίας αναγνώρισης προσώπου και των συνεπειών που ενδέχεται να επιφέρει σε αυτά, ώστε αφενός τα υποκείμενα των δεδομένων να δύναται να παρέχουν **έγκυρη συγκατάθεση** κατά τη χρήση της τεχνολογίας, αφετέρου να καλλιεργηθούν **οξυμένα δημοκρατικά αντανακλαστικά**, ούτως ώστε να μην ομαλοποιηθεί στη συλλογική συνείδηση, μέσω της σταδιακής ενσωμάτωσης της τεχνολογίας σε κάθε πτυχή της καθημερινότητας και στο δημόσιο forum, η μαζική και αδιάκριτη συλλογή βιομετρικών δεδομένων για σκοπούς αδιαμφισβήτητης ταυτοποίησης. Κατ' αυτόν τον τρόπο, οι πολίτες θα μπορούν να διατηρούν ουσιωδώς τον έλεγχο των πληροφοριών τους και να διεκδικούν την αποτελεσματική άσκηση, στο σύνολό τους, των δικαιωμάτων τους, όπως αυτά κατοχυρώνονται ρητά στο κοινοτικό κεκτημένο για την προστασία των προσωπικών δεδομένων.

Ως ευλόγως συνάγεται, η ευρωπαϊκή νομοθεσία για την προστασία των δεδομένων προσωπικού χαρακτήρα θέτει, παρά τις όποιες δυσχέρειες, επιτυχώς **ένα βασικό ρυθμιστικό πλαίσιο** για τη λελογισμένη και σύννομη επεξεργασία των εικόνων προσώπου από τους αλγορίθμους αναγνώρισης προσώπου. Εντούτοις, η ισχυρή δυναμική της τεχνολογίας, σε συνδυασμό με τη μείωση του κόστους της και την εξ αυτής γενίκευση χρήσης της, καθιστά **ολοένα και πιο επιτακτική την ανάγκη για εξειδικευμένη νομοθεσία ικανή να ενθαρρύνει τις νόμιμες χρήσεις της, αποθαρρύνοντας παραλλήλως τις αθέμιτες πρακτικές.** Χαρακτηριστική της προβληματικής, είναι η στάση της εταιρείας Clearview AI Inc., η οποία, όχι μόνον αμφισβητεί τη δικαιοδοσία[215] των ευρωπαϊκών ΑΠΔΠΧ, επειδή

---

[213] Gonzalez Fuster, G & Nadolna Peeters, M.A. (2021), σελ. 50-52.

[214] Council of Europe- Convention 108 (2021), σελ. 14.

[215] Φυσικά, αυτός ο ισχυρισμός είναι **αβάσιμος**, καθώς η επεξεργασία στην οποία προβαίνει η Clearview AI ενεργοποιεί το άρθρο 3§2 στ. β' (βλ και αιτιολογική σκέψη 24) του ΓΚΠΔ, γεγονός που έχουν υπογραμμίσει οι ευρωπαϊκές ΑΠΔΠΧ, μεταξύ αυτών και η ελληνική βλ. απόφαση 35/2022 Ελληνικής ΑΠΔΠΧ σελ 6-9 και 15-17. Διαθέσιμη σε: https://www.dpa.gr/sites/default/files/2022-07/35_2022%20anonym_0.pdf (Ημερομηνία Πρόσβασης: Ιούνιος 2022). Αξίζει να σημειωθεί εν προκειμένω ότι και η πολωνική εταιρεία PimEyes μετέφερε προσφάτως την έδρα της στις Σεϋχέλλες.

η έδρα της βρίσκεται στις Η.Π.Α.[216] , αλλά ισχυρίζεται περαιτέρω ότι η εταιρεία δεν μπορεί να συμμορφωθεί με τις εντολές διαγραφής δεδομένων, διότι δεν υπάρχει τρόπος να εξακριβωθεί πού ζουν οι άνθρωποι στις περισυλλεχθείσες φωτογραφίες. Επιβάλλεται, συνεπώς, μια ειδική νομοθετική ρύθμιση η οποία θα προβλέπει λεπτομερειακώς τις παραμέτρους σύννομης ανάπτυξης και χρήσης της τεχνολογίας, καθορίζοντας ρητά τις υποχρεώσεις των υπευθύνων και εκτελούντων την επεξεργασία, τους σκοπούς για τους οποίους θα είναι επιτρεπτή, ποιοι φορείς δικαιούνται να τη διεξάγουν, ποιοι οι αποδέκτες αυτής, ποια τα δικαιώματα των υποκειμένων, ποια μέτρα οφείλει να λαμβάνει ο υπεύθυνος επεξεργασίας και υπό ποιους όρους είναι επιτρεπτή η διαβίβαση των δεδομένων. Το Σχέδιο του Κανονισμού για την Τεχνητή Νοημοσύνη της Επιτροπής, αν και συνεισφέρει σημαντικές ρυθμίσεις, δεν αντιμετωπίζει καθ' ολοκληρίαν την προβληματική.

Προσέτι, το Ευρωπαϊκό Κοινοβούλιο έχει επισημάνει την ανάγκη να συμβαδίσει η ένωση με την εξέλιξη στον τομέα της ΤΝ που έχει επιτευχθεί στην Κίνα και στην Αμερική, οι οποίες πρωτοστατούν στη βιομηχανία αναγνώρισης προσώπου και καθορίζουν τα διεθνή πρότυπα[217]. Πράγματι, η καινοτομία και η ανάπτυξη των εφαρμογών της Τεχνητής Νοημοσύνης θα πρέπει να ενισχύονται και να προστατεύονται· εντούτοις η ανάπτυξη αυτή δεν θα πρέπει να συντελείται εις βάρος των αξιών και των θεμελιωδών ανθρωπίνων δικαιωμάτων. Ο ευρωπαϊκός νομοθέτης καλείται να σταθμίσει τα εκατέρωθεν συμφέροντα και να παρέχει ένα ειδικότερο νομοθετικό πλαίσιο για την τεχνολογία αναγνώρισης προσώπου, **ενδεχομένως θέτοντας εκτός νόμου κάποιες εφαρμογές της** που μπορούν να οδηγήσουν σε μαζική επιτήρηση, όπως η αδιάκριτη χρήση της τεχνολογίας στη δημόσια σφαίρα, **αλλά και κάποιες αθέμιτες πρακτικές** αφενός κατά τη συλλογή των βιομετρικών δεδομένων, όπως **η ιστοσυγκομιδή**, αλλά και αφετέρου κατά τη διατήρηση και περαιτέρω χρήση των δεδομένων για διαφορετικούς των αρχικώς εγκεκριμένων σκοπούς, όπως **η εγκαθίδρυση συστημάτων κοινωνικής πίστωσης**. Στον προστατευτικό κλοιό της νομοθεσίας καλείται να υπαχθεί και η χρήση της τεχνολογίας αναγνώρισης προσώπου **για σκοπούς κατηγοριοποίησης**, καθώς καθίσταται εύλογα αντιληπτό ότι οι δυνατότητες που προσφέρει η τεχνητή νοημοσύνη στα συστήματα αλγοριθμικής αναγνώρισης προσώπου, μπορούν όχι μόνον να επιτρέψουν μέσω της συσχέτισης

---

[216] Perrigo, B. (2022) 'An AI Company Scraped Billions of Photos For Facial Recognition. Regulators Can't Stop It.', *Time*. Διαθέσιμο στο: https://time.com/6182177/clearview-ai-regulators-uk/ (Ημερομηνία πρόσβασης: Ιούνιος 2022).

[217] Ευρωπαϊκό Κοινοβούλιο- Ειδική Επιτροπή για την τεχνητή νοημοσύνη στην ψηφιακή εποχή (2022) 'Τεχνητή νοημοσύνη στην ψηφιακή εποχή (2020/2266(INI))'. σκέψη υπ' αριθ. 3. Διαθέσιμο στο: https://www.europarl.europa.eu/doceo/document/A-9-2022-0088_EN.pdf.

δεδομένων την ταυτοποίηση των υποκειμένων, αλλά έτι περαιτέρω, να οδηγήσουν και σε αθέμιτες διακρίσεις.

Όπως ευλόγως προκύπτει εκ των ανωτέρω, καθίσταται ζωτικής σημασίας για την Ευρωπαϊκή Ένωση, η οποία δηλώνει τη φιλοδοξία της να ηγηθεί των παγκόσμιων προτύπων Τεχνητής Νοημοσύνης, να συμμετάσχει ενεργά στις παγκόσμιες συζητήσεις σχετικά με τη ρύθμιση της τεχνολογίας αναγνώρισης προσώπου. Προκειμένου το περιγραφόμενο στην παρούσα διακύβευμα να αντιμετωπιστεί ριζικά, θα πρέπει στο επίκεντρο της συζήτησης να βρίσκεται η ιδιαιτερότητα των βιομετρικών δεδομένων: το πρόσωπο ενός ατόμου είναι ένα πολύτιμο και ευαίσθητο στοιχείο της ταυτότητάς του και της ίδιας της αίσθησης της μοναδικότητάς του[218]. Η μετατροπή του ανθρώπινου προσώπου σε ένα ακόμη αντικείμενο δεκτικό μέτρησης και κατηγοριοποίησης από αυτοματοποιημένες διαδικασίες, οι οποίες μάλιστα ελέγχονται από ισχυρές εταιρείες και κυβερνήσεις, υφαρπάζει ένα μέρος της ανθρώπινης ουσίας και θίγει το δικαίωμα στην αξιοπρέπεια, ακόμη και χωρίς να επικρέμαται ως δαμόκλειος σπάθη η πιθανή χρήση της τεχνολογίας ως μέσο καταστολής από αυταρχικά κράτη. Ο ενωσιακός νομοθέτης καλείται να συνταιριάξει τα αντικρουόμενα συμφέροντα όλων των εμπλεκόμενων μερών, δίχως να λησμονά την ιδιαιτερότητα των συστημάτων αναγνώρισης προσώπου και τη βαθύτητα της επέμβασης, αφ' εαυτής της εγκατάστασής τους, στα θεμελιώδη ανθρώπινα δικαιώματα.

[218] Wiewiórowski, W. (2019) 'Facial recognition: A solution in search of a problem? European Data Protection Supervisor', *European Data Protection Supervisor*, 389(8602), σελ. 1–3. Διαθέσιμο στο: https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en (Ημερομηνία πρόσβασης: Ιούνιος 2022).

ΒΙΒΛΙΟΓΡΑΦΙΑ

Ι. ΞΕΝΟΓΛΩΣΣΗ

- Abdullakutty, F., Elyan, E. και Johnston, P. (2021) 'A review of state-of-the-art in Face Presentation Attack Detection: From early development to advanced deep learning and multi-modal fusion methods', *Information Fusion*, 75, σσ 55–69. doi:10.1016/J.INFFUS.2021.04.015. Διαθέσιμο στο: https://www.sciencedirect.com/science/article/abs/pii/S1566253521000919 (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Ada Lovelace Institute (2019) *Beyond face value: public attitudes to facial recognition technology*. Διαθέσιμο στο: https://www.adalovelaceinstitute.org/report/beyond-face-value-public-attitudes-to-facial-recognition-technology/ (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Ada Lovelace Institute (2021) '*The Citizens' Biometrics Council'; Report with recommendations and findings of a public deliberation on biometrics technology, policy and governance.*' Διαθέσιμο στο: https://www.adalovelaceinstitute.org/wp-content/uploads/2021/03/Citizens_Biometrics_Council_final_report.pdf (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Almeida, D., Shmarko, K., Lomas, E. (2021) 'The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks', *AI and Ethics*. doi:10.1007/s43681-021-00077-w.
- Amnesty International (2020) *Russia: Intrusive facial recognition technology must not be used to crackdown on protests*. Διαθέσιμο στο: https://www.amnesty.org/en/latest/news/2020/01/russia-intrusive-facial-recognition-technology-must-not-be-used-to-crackdown-on-protests/ (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Andrejevic, M., Selwyn, N. (2020) 'Facial recognition technology in schools: critical questions and concerns', *Learning, Media and Technology*, 45(2), σελ. 115–128. doi:10.1080/17439884.2020.1686014.
- Azria, S., Wickert, F. (2019) 'Facial Recognition: Current situation and challenges.', in *Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108).Council of Europe.* Διαθέσιμο σε: https://rm.coe.int/t-pd-2019-05rev-facial-recognition-report-003-/16809eadf1 (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- BBC News (2021) 'TikTok agrees legal payout over facial recognition' Διαθέσιμο στο: https://www.bbc.com/news/technology-56210052 (Ημερομηνία πρόσβασης: Ιούνιος 2022).

- 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.
- Bernard, M. (2019) 'Technology : Here Are The Important Pros And Cons', *Forbes*. Διαθέσιμο στο: https://www.forbes.com/sites/bernardmarr/2019/08/19/facial-recognition-technology-here-are-the-important-pros-and-cons/?sh=35a9ea0514d1.
- Bischoff, P. (2021) *Facial recognition technology (FRT): 100 countries analyzed - Comparitech*. Διαθέσιμο στο: https://www.comparitech.com/blog/vpn-privacy/facial-recognition-statistics/ (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Bloch-Wehba, H. (2021) 'Visible policing: Technology, transparency, and democratic control', *California Law Review*, 109(3), σελ. 917–978. doi:10.15779/Z38NS0KZ51.
- Boesch, G. (2022) *What is Computer Vision? The Complete Tech Guide for 2022*, *Viso*. Διαθέσιμο στο: https://viso.ai/computer-vision/what-is-computer-vision/ (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Bu, Q. (2021) 'The global governance on automated facial recognition (AFR): ethical and legal opportunities and privacy challenges', *International Cybersecurity Law Review*, 2(1), σελ. 113–145. doi:10.1365/s43439-021-00022-x.
- Buolamwini, J. (2018) 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification', *Proceedings of Machine Learning Research*, τ. 81, σελ. 1-15.
- Chae, Y. (2020) 'U.S. AI Regulation Guide: Legislative Overview and Practical Considerations', *The Journal of Robotics, Artificial Intelligence & Law*, 3(1), σελ. 17–40. Διαθέσιμο στο: https://www.bakermckenzie.com/-/media/files/people/chae-yoon/rail-us-ai-regulation-guide.pdf (Ημερομηνία Πρόσβασης: Ιούνιος 2022).
- Clayton, J. (2022) *How facial recognition is identifying the dead in Ukraine - BBC News*, *BBC News*. Διαθέσιμο στο: https://www.bbc.com/news/technology-61055319 (Ημερομηνία πρόσβασης: Αύγουστος 2022).
- Commission nationale de l'informatique et des libertés (2019), 'Expérimentation de la reconnaissance faciale dans deux lycées: la CNIL précise sa position', Διαθέσιμο σε: https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position (Ημερομηνία Πρόσβασης: Ιούνιος 2022).
- Council of Europe- Convention 108 (2021) *Guidelines on facial recognition'*. Διαθέσιμο στο: https://edoc.coe.int/en/artificial-intelligence/9753-guidelines-on-facial-recognition.html (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Dastin J (2018) 'Amazon scraps secret AI recruiting tool that showed bias against women - Reuters', *Reuters*, σελ. 1–6. Διαθέσιμο στο: https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G (Ημερομηνία πρόσβασης: Ιούνιος 2022).

- Davis, P.A.E. (2020) 'Facial detection and smart billboards: Analysing the "identified" criterion of personal data in the GDPR', *European Data Protection Law Review*, 6(3), σελ. 365–377. doi:10.21552/edpl/2020/3/7.
- Dion, A. (2019) 'Social implications of the facial recognition system', *University of Twente*.
- ECI (2021) 'Initiative detail | European Citizens' Initiative'. Διαθέσιμο στο: https://europa.eu/citizens-initiative/initiatives/details/2021/000001_en.
- EDPB-EDPS (2021) '*Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*'. Διαθέσιμο στο: https://edps.europa.eu/system/files/2021-06/2021-06-18-edpb-edps_joint_opinion_ai_regulation_en.pdf (Ημερομηνία Πρόσβασης: Ιούνιος 2022).
- EDRi (2020) 'Use cases : Impermissible AI and fundamental rights breaches'. Διαθέσιμο στο: https://edri.org/wp-content/uploads/2021/06/Case-studies-Impermissible-AI-biometrics-September-2020.pdf (Ημερομηνία Πρόσβασης: Ιούνιος 2022).
- EPRS | European Parliamentary Research Service (2020) *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*. Διαθέσιμο στο: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Eriksson, P. *κ.ά.* (2019) 'Surveillance Using Facial Recognition and Social Media Data', *Uppsala Universitet*. Διαθέσιμο στο: http://www.it.uu.se.
- European Data Protection Board (2022) *Facial recognition: Italian SA fines Clearview AI EUR 20 million*. Διαθέσιμο στο: https://edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- European Data Protection Board (2022) *Facial recognition: Italian SA fines Clearview AI EUR 20 million*. Διαθέσιμο στο: https://edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- European Data Protection Board (EDPB) (2019) 'Guidelines 5 /2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR, Διαθέσιμο στο: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201905_rtbfsearchengines_afterpublicconsultation_en.pdf (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- European Data Protection Board (EDPB) (2022) 'Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement' Διαθέσιμο στο: https://edpb.europa.eu/system/files/2022-05/edpb-

guidelines_202205_frtlawenforcement_en_1.pdf (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- European Data Protection Supervisor (2020) 'Opinion on the possibility to use Clearview AI and similar services at Europol (Case 2020-0372)'. Διαθέσιμο στο: https://edps.europa.eu/system/files/2022-01/21-03-29_edps_opinion_2020-0372.pdf (Ημερομηνία Πρόσβασης: Ιούνιος 2022).
- European Data Protection Supervisor (2021) *Artificial Intelligence Act: a welcomed initiative, but ban on remote biometric identification in public space is necessary*. Διαθέσιμο στο: https://edps.europa.eu/press-publications/press-news/press-releases/2021/artificial-intelligence-act-welcomed-initiative_en (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- European Union Agency for Fundamental Rights & Council of Europe (2018) *Handbook on European Data Protection Law, Publications Office of the European Union*. Διαθέσιμο στο: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- European Union Agency for Fundamental Rights (2019) 'Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights', *FRA Focus*. Διαθέσιμο στο: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-data-quality-and-ai_en.pdf (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- European Union Agency for Fundamental Rights (2019) 'Facial recognition technology: fundamental rights considerations in the context of law enforcement'. Διαθέσιμο στο: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf. (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Farivar, C. (2022) *Clearview AI Settles Facial Recognition Suit With ACLU, Will Alter Some Practices, Forbes*. Διαθέσιμο στο: https://www.forbes.com/sites/cyrusfarivar/2022/05/09/clearview-ai-facial-recognition-suit-with-aclu/?sh=c56144b7f41a (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Fernandez, E. (2020) 'Facial Recognition Violates Human Rights, Court Rules', *Forbes*. Διαθέσιμο στο: https://www.forbes.com/sites/fernandezelizabeth/2020/08/13/facial-recognition-violates-human-rights-court-rules/?sh=14811bea5d44 (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Fernandez, V. κ.ά. (2020) '*Facial Recognition: Embodying European Values*'. Paris: Renaissance Numérique. Διαθέσιμο στο: https://www.renaissancenumerique.org/wp-content/uploads/2022/06/renaissancenumerique_report_facialrecognition.pdf (Ημερομηνία Πρόσβασης: Ιούνιος 2022)
- Fussey, P., Murray, D. (2019) 'Independet Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology. The Human Rights,

Big Data and Technology Project', (July), p. 128. Διαθέσιμο στο: https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf (Ημερομηνία πρόσβασης: Ιούνιος 2022).

- Global Privacy Assembly (2020), 'Adopted Resolution on Facial Recognition Technology', σε: 42η Διεθνής Σύνοδος της Παγκόσμιας Συνέλευσης Προστασίας Ιδιωτικότητας. Διαθέσιμο σε: https://edps.europa.eu/sites/edp/files/publication/final_gpa_resolution_on_facial_recognition_technology_en.pdf (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Gonzalez Fuster, G & Nadolna Peeters, M.A. (2021), *Person identification, human rights and ethical principles: Rethinking biometrics in the era of artificial intelligence*. European Parliament. Διαθέσιμο στο: http://www.europarl.europa.eu/thinktank (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Guiao, J. (2021) 'Government's forced rollout of facial recognition for home quarantine needs strict limits and protections', *The Australia Institute*. Διαθέσιμο στο: https://australiainstitute.org.au/wp-content/uploads/2021/10/P1149-Facial-recognition-for-home-quarantine-needs-limits-and-protections-WEB.pdf. (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Hacker, P. 'Teaching fairness to artificial intelligence: Existing and novel strategies against algorithmic discrimination under EU law', (2018), 55, *Common Market Law Review*, Issue 4, σελ. 1143-1185, Διαθέσιμο σε: https://kluwerlawonline.com/journalarticle/Common+Market+Law+Review/55.4/COLA2018095 (Ημερομηνία Πρόσβασης: Ιούνιος 2022)
- Hao, K. (2021) 'This is how we lost control of our faces', *MIT Technology Review*, σελ. 1–9. Διαθέσιμο στο: https://www.technologyreview.com/2021/02/05/1017388/ai-deep-learning-facial-recognition-data-history/ (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Hart, R. (2022) *Clearview AI Fined $9.4 Million In U.K. For Illegal Facial Recognition Database*, *Forbes*. Διαθέσιμο στο: https://www.forbes.com/sites/roberthart/2022/05/23/clearview-ai-fined-94-million-in-uk-for-illegal-facial-recognition-database/?sh=9a98a8619636 (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Hill, K. (2020) 'The Secretive Company That Might End Privacy as We Know It', *The New York Times*. Διαθέσιμο στο: https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Hill, K. (2020) 'Twitter Tells Facial Recognition Trailblazer to Stop Using Site's Photos', *The New York Times*. Διαθέσιμο στο: https://www.nytimes.com/2020/01/22/technology/clearview-ai-twitter-letter.html (Ημερομηνία πρόσβασης: Ιούνιος 2022).

- Hill, K. (2020) 'Wrongfully Accused by an Algorithm', *The New York Times*. Διαθέσιμο στο: https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Hill, K. (2022) 'A Face Search Engine Anyone Can Use Is Alarmingly Accurate', *The New York Times*. Διαθέσιμο στο: https://www.nytimes.com/2022/05/26/technology/pimeyes-facial-recognition-search.html (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Homo Digitalis (2020) *Facial recognition: Homo Digitalis calls on Greek DPA to speak up*, *European Digital Rights (EDRi)*. Διαθέσιμο στο: https://edri.org/our-work/facial-recognition-homo-digitalis-calls-on-greek-dpa-to-speak-up/ (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Information and Privacy Commisioner of Ontario (2016) 'De-identification Guidelines for Structured Data'. Διαθέσιμο στο: https://www.ipc.on.ca/wp-content/uploads/2016/08/Deidentification-Guidelines-for-Structured-Data.pdf (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Information Commissioner's Office (2021) *The use of live facial recognition technology in public places*. Διαθέσιμο στο: https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Integritetsskyddsmyndigheten (IMY) 'IMY får rätt om ansiktsigenkänning' https://www.imy.se/nyheter/imy-far-ratt-om-ansiktsigenkanning/ (Ημερομηνία Πρόσβασης: Ιούνιος 2022).
- Jakubowska, E. (2020) 'Ban Biometric Mass Surveillance: A set of fundamental rights demands for the European Commission and EU Member States Published', *European Digital Rights 12*, 32(0).
- Janiesch, C., Zschech, P. και Heinrich, K. (2021) 'Machine learning and deep learning', *Electronic Markets*, 31(3), σελ. 685–695. doi:10.1007/s12525-021-00475-2.
- Jungyun, S. (2020) 'Clearview AI revelations spark action on use of facial recognition'.
- Kerry, C.F. (2020) 'Protecting privacy in an AI-driven world', *Brookings*. Διαθέσιμο στο: https://www.brookings.edu/research/protecting-privacy-in-an-ai-driven-world/ (Ημερομηνία Πρόσβασης: Ιούνιος 2022).
- Klosowski, T. (2020) 'Facial Recognition Is Everywhere . Here ' s What We Can Do About It.', *The New York Times*, σελ. 1–12. Διαθέσιμο στο: https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/ (Ημερομηνία Πρόσβασης: Ιούνιος 2022).
- Knight, W. (2021) *Job Screening Service Halts Facial Analysis of Applicants*, *WIRED*. Διαθέσιμο στο: https://www.wired.com/story/job-screening-service-halts-facial-analysis-applicants/ (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Kosinski, M. (2021) 'Facial recognition technology can expose political orientation from naturalistic facial images', *Scientific Reports*, 11(1), σελ. 1–7. doi:10.1038/s41598-020-79310-1.

- Kostka, G., Meckel, M. (2021) 'Between security and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United States', *Public Understanding of Science*, 30(6), σελ. 671–690. doi:10.1177/09636625211001555.
- Madiega, T., Mildebrath, H. (2021) *Regulating facial recognition in the EU. In-depth analysis, European Parliamentary Research Service*. doi:10.2861/140928.
- Marks, P. (2021) 'Can the biases in facial recognition be fixed; Also, should they?', *Communications of the ACM*, 64(3), σελ. 20–22. doi:10.1145/3446877.
- Miyamoto, I. (2020) 'Surveillance Technology Challenges Political Culture of Democratic States', *Hindsight, Insight, Foresight*, σελ. 49–66.
- Mozur, P. (2019) *One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority - The New York Times*, *14 April*. Διαθέσιμο στο: https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Muller, C. (2021) 'Γνωμοδότηση της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής με θέμα «Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη θέσπιση εναρμονισμένων κανόνων σχετικά με την τεχνητή νοημοσύνη (Πράξη για την τεχνητή νοημοσύνη) και για την τροποποίηση ορισμένων νομοθετικών πράξεων της Ένωσης'. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52021AE2482&from=EN.
- O'flaherty, M. (2020) 'Facial recognition technology and fundamental rights', *European Data Protection Law Review*, 6(2), σελ. 170–173. doi:10.21552/edpl/2020/2/4.
- Panahov, H. (2022) 'Why the US Needs Federal Law on Facial Recognition Technology', *Intersect*, 15(2).
- Perrigo, B. (2022) 'An AI Company Scraped Billions of Photos For Facial Recognition. Regulators Can't Stop It.', *Time*. Διαθέσιμο στο: https://time.com/6182177/clearview-ai-regulators-uk/ (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Pin, A. (2021). "A Novel and Controversial Technology." Artificial Face Recognition,
- Privacy Protection, and Algorithm Bias in Europe. *William & Mary Bill of Rights Journal*, 30(2), 291-318.
- Rachmaniar, A. *κ.ά.* (2020) 'Regulating Facial Recognition Technology under the Indonesian Privacy and Data Protection Frameworks: The Pacing Problem?', *1st International Conference on Law Studies "Law Policy on Transnational Issues" Jakarta, 19th November 2020*, σελ. 23–44.
- Radiya-Dixit, E. *κ.ά.* (2021) 'Data Poisoning Won't Save You From Facial Recognition'. Διαθέσιμο στο: http://arxiv.org/abs/2106.14851 (Ημερομηνία πρόσβασης: Ιούνιος 2022).

- Ragazzi, F. *κ.ά.* (2021) *Biometric and Behavioural Mass Surveillance in EU Member States: Report for the Greens/EFA in the European Parliament.* Διαθέσιμο στο: http://extranet.greens-efa.eu/public/media/file/1/7297 (Ημερομηνία Πρόσβασης: Ιούνιος 2022).
- Raji, I.D. and Fried, G. (2021) 'About Face: A Survey of Facial Recognition Evaluation'. Διαθέσιμο στο: http://arxiv.org/abs/2102.00813 (Ημερομηνία Πρόσβασης: Ιούνιος 2022).
- Rezende, I.N. (2020) 'Facial recognition in police hands: Assessing the "Clearview case" from a European perspective', *New Journal of European Criminal Law*, 11(3), σελ. 375–389. doi:10.1177/2032284420948161.
- Rose, K., Eldridge, S., & Chapin, L. (2015). The internet of things: An overview. *The internet society (ISOC), 80*. https://www.academia.edu/download/48790442/ISOC-IoT-Overview-20151014_0.pdf (Ημερομηνία Πρόσβασης: Ιούνιος 2022).
- Roussi, A. (2020) 'Resisting the rise of facial recognition', *Nature*, 587(7834), σελ. 350–353. doi:10.1038/d41586-020-03188-2. Διαθέσιμο σε: https://www.nature.com/articles/d41586-020-03188-2 (Ημερομηνία Πρόσβασης: Ιούνιος 2022).
- Russell, S., & Norvig, P. (2002). *Artificial intelligence: a modern approach*. Prentice Hall.
- Salama AbdELminaam D, *κ.ά.* (2020) 'A deep facial recognition system using computational intelligent algorithms', *PLoS ONE*, 15(12 December). Διαθέσιμο σε: https://doi.org/10.1371/journal.pone.0242269 (Ημερομηνία Πρόσβασης: Ιούνιος 2022).
- Samsel, H. (2019) *California Becomes Third State to Ban Facial Recognition Software in Police Body Cameras*, *Security Today*. Διαθέσιμο στο: https://securitytoday.com/articles/2019/10/10/california-to-become-third-state-to-ban-facial-recognition-software-in-police-body-cameras.aspx. (Ημερομηνία Πρόσβασης: Ιούνιος 2022).
- Sarabdeen, J. (2022) 'Protection of the rights of the individual when using facial recognition technology', *Heliyon*, 8(3). doi:10.1016/J.HELIYON.2022.E09086.
- Scherhag, U., Rathgeb, C. και Busch, C. (2022) 'Face Morphing Attack Detection Methods', *Advances in Computer Vision and Pattern Recognition*, σσ 331–349. doi:10.1007/978-3-030-87664-7_15/TABLES/7.
- Scipione, J. (2022) 'Has the Horse Bolted? Dealing with Legal and Practical Challenges of Facial Recognition', *MediaLaws*, σελ. 9–12. doi:10.2139/ssrn.4019105.
- Shackelford, S.J. (2020) 'Protecting Privacy in an Internet of Everything', in *The Internet of Things*, σελ. 36–39. doi:10.1093/wentk/9780190943813.003.0004.
- Shan, S. *κ.ά.* (2020) 'Fawkes: Protecting privacy against unauthorized deep learning models', *Proceedings of the 29th USENIX Security Symposium*, σελ. 1589–1604.

- Siapka, A. (2019) 'The Ethical and Legal Challenges of Artificial Intelligence: The EU response to biased and discriminatory AI', *SSRN Electronic Journal*. doi:10.2139/ssrn.3408773.
- Smith, M. and Miller, S. (2022) 'The ethical application of biometric facial recognition technology', *AI & Society*, 37, σελ. 167–175. doi:10.1007/s00146-021-01199-9.
- Special Committee on Artificial Intelligence in a Digital Age- European Parliament (2021) *Draft Report on artificial intelligence in a digital age (2020/2266(INI))*. Διαθέσιμο στο: https://www.europarl.europa.eu/doceo/document/AIDA-PR-680928_EN.pdf (Ημερομηνία Πρόσβασης: Ιούνιος 2022).
- Spielkamp, M. (2017) *Inspecting Algorithms for Bias - MIT Technology Review*, *MIT Technology Review*. Διαθέσιμο στο: https://www.technologyreview.com/2017/06/12/105804/inspecting-algorithms-for-bias/ (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Takhshid, Z. (2020) 'Retrievable Images on Social Media Platforms: A Call for a New Privacy Tort, 68 Buff. L. Rev. 139', *Buffalo Law Review*, 68(1). Διαθέσιμο στο: https://digitalcommons.law.buffalo.edu/buffalolawreview/vol68/iss1/3 (Ημερομηνία Πρόσβασης: Ιούνιος 2022).
- Thales Group (2021) 'Biometrics (facts, use cases, biometric security)'. Διαθέσιμο στο: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Thales Group (2021) 'Facial Recognition'. Διαθέσιμο στο: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/facial-recognition (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- The Guardian (2019) 'Watchdog criticises 'chaotic' police use of facial recognition', *2019*. Διαθέσιμο στο: https://www.theguardian.com/uk-news/2019/jun/27/watchdog-criticises-chaotic-police-use-of-facial-recognition (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- The Office of the High Commissioner for Human Rights (UN Human Rights) (2020) *Report of the proceedings of the online expert seminar with the purpose of identifying how artificial intelligence, including profiling, automated decision-making and machine learning technologies may, without proper safeguards, affect the enjoyment of the right to privacy (2020)*. Διαθέσιμο στο: https://www.ohchr.org/sites/default/files/Documents/Issues/DigitalAge/ExpertSeminarReport-Right-Privacy.pdf (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Touring, A.M. (1950) 'Computing Machinery and Intelligence', *Mind*, LIX(236), σελ. 433–460. doi:10.1093/MIND/LIX.236.433.
- Turk, M. και Pentland, A. (1991) 'Eigenfaces for Recognition', *Journal of Cognitive Neuroscience*, 3(1), σελ. 71–86.

- Ullah, N. *κ.ά.* (2021) 'A novel DeepMaskNet model for face mask detection and masked facial recognition', *Journal of King Saud University - Computer and Information Sciences* [Preprint], (xxxx). doi:10.1016/j.jksuci.2021.12.017.
- United Nations- General Assembly (2021) *The right to privacy in the digital age* Report of the United Nations High Commissioner for Human Rights*.
- Vale, S. και Zanfir- Fortuna, G. (2022) 'FPF Report: Automated Decision-Making Under the GDPR - A Comprehensive Case-Law Analysis. *Future of Privacy Forum*. Διαθέσιμο σε: https://fpf.org/wp-content/uploads/2022/05/FPF-ADM-Report-R2-singles.pdf (Ημερομηνία Πρόσβασης: Ιούνιος 2022)
- Van Noorden, R. (2020) 'The ethical questions that haunt facial-recognition research', *Nature*, 587(7834), σελ. 354–358. doi:10.1038/d41586-020-03187-3.
- Varley-Winter, O. (2020) 'The overlooked governance issues raised by facial recognition', *Biometric Technology Today*, 2020(5), σελ. 5–8. doi:10.1016/S0969-4765(20)30061-8.
- Vemou, K., Zerdick, T., Horvath, A. (2021) 'Facial Emotion Recognition', *EDPS TechDispatch*, (1). doi:10.2804/014217. Διαθέσιμο στο: https://edps.europa.eu/system/files/2021-05/21-05-26_techdispatch-facial-emotion-recognition_ref_en.pdf (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Wiewiórowski Wojciech (2020) *AI and Facial Recognition: Challenges and Opportunities | European Data Protection Supervisor*, *European Data Protection Supervisor*. Διαθέσιμο στο: https://edps.europa.eu/press-publications/press-news/blog/ai-and-facial-recognition-challenges-and-opportunities_en (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Wiewiórowski, W. (2019) 'Facial recognition: A solution in search of a problem? European Data Protection Supervisor', *European Data Protection Supervisor*, 389(8602), σελ. 1–3. Διαθέσιμο στο: https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Wolfewicz, A. (2022) *Deep learning vs. machine learning - What's the Difference?*, *Levity*. Διαθέσιμο στο: https://levity.ai/blog/difference-machine-learning-deep-learning (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Woods, L. (2020) 'Automated facial recognition in the uk: The bridges case and beyond', *European Data Protection Law Review*, 6(3), σελ. 455–463. doi:10.21552/edpl/2020/3/16.
- Yeung, M.K. (2022) 'A systematic review and meta-analysis of facial emotion recognition in autism spectrum disorder: The specificity of deficits and the role of task characteristics', *Neuroscience and Biobehavioral Reviews*, 133. doi:10.1016/J.NEUBIOREV.2021.104518.
- Zalnieriute, M. (2021) 'Burning Bridges: The Automated Facial Recognition Technology and Public Space Surveillance in the Modern State', *Columbia Science*

and Technology Law Review, 22(2), σελ. 284–307. Διαθέσιμο στο: https://ssrn.com/abstract=3805494 (Ημερομηνία Πρόσβασης: Ιούνιος 2022).

ΙΙ. ΕΛΛΗΝΙΚΗ

- Ανδρουλάκη, Ε. (2021) «Τεχνητή νοημοσύνη και προσωπικά δεδομένα: η περίπτωση της εξ αποστάσεως βιομετρικής ταυτοποίησης», *Επιθεώρηση Δικαίου Πληροφορικής*, τ. 1, σελ. 1–17. Διαθέσιμο στο: https://ejournals.lib.auth.gr/infolawj/article/view/8236 (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (2022) «Ανακοίνωση σχετικά με την επιβολή προστίμου στην εταιρεία Clearview AI, Inc.» Διαθέσιμη στο: https://www.dpa.gr/el/enimerwtiko/deltia/anakoinosi-shetika-me-tin-epiboli-prostimoy-stin-etaireia-clearview-ai-inc (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Βέρρας, Δ. (2020) 'Clearview AI: Εντολή για διαγραφή βιομετρικών δεδομένων πολίτη από τον Επίτροπο Προστασίας Προσωπικών Δεδομένων Αμβούργου', *Lawspot*. Διαθέσιμο στο: https://www.lawspot.gr/nomika-nea/clearview-ai-entoli-gia-diagrafi-viometrikon-dedomenon-politi-apo-ton-epitropo-prostasias (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Βλαχάβας, Ι. *κ.ά.* (2011) *Τεχνητή Νοημοσύνη - Γ' Έκδοση*. Εκδόσεις Πανεπιστημίου Μακεδονίας.
- Βόρρας, Α., Μήτρου, Λ., (2018) 'Τεχνητή νοημοσύνη και προσωπικά δεδομένα - Μια θεώρηση υπό το πρίσμα του Ευρωπαϊκού Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 2016/679', *ΔΙΤΕ (π. ΔΙΜΕΕ)*,(4/2018).
- Γεωργίου, Σ. (2021) 'Αυτόματη αναγνώριση προσώπου στους δημόσιους χώρους: Μεταξύ πραγματικότητας και δυστοπίας', *Syntagma Watch*, σελ. 1–12. Διαθέσιμο στο: https://www.syntagmawatch.gr/trending-issues/aytomati-anagnwrisi-proswpou-stous-dhmosious-xwrous-metaxy-pragmatikothtas-kai-dystopias/ (Ημερομηνία Πρόσβασης: Ιούνιος 2022).
- Διεθνής Αμνηστία (2021) 'Να απαγορευτεί η επικίνδυνη τεχνολογία αναγνώρισης προσώπου που ενισχύει τη ρατσιστική αστυνόμευση', σελ. 1–13. Διαθέσιμο στο: https://www.amnesty.gr/news/articles/article/24168/na-apagoreytei-i-epikindyni-tehnologia-anagnorisis-prosopoy-poy-enishyei (Ημερομηνία Πρόσβασης: Ιούνιος 2022).
- Διεθνής Αμνηστία (2022) *ΗΠΑ: Η τεχνολογία αναγνώρισης προσώπου ενισχύει τη ρατσιστική αστυνόμευση σωματικού ελέγχου στη Νέα Υόρκη – νέα έρευνα*. Διαθέσιμο στο: https://www.amnesty.gr/news/articles/article/24966/ipa-i-tehnologia-anagnorisis-prosopoy-enishyei-ti-ratsistiki-astynomeysi (Ημερομηνία πρόσβασης: Ιούνιος 2022).

- Ευρωπαϊκή Επιτροπή (2020) *COM(2020) 65 final- Λευκή Βίβλος για την Τεχνητή Νοημοσύνη. Η ευρωπαϊκή προσέγγιση της αριστείας και της εμπιστοσύνης.*
- Ευρωπαϊκή Επιτροπή (2021) 'Παραρτήματα της Πρότασης κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη θέσπιση εναρμονισμένων κανόνων σχετικά με την τεχνητή νοημοσύνη (Πράξη για την τεχνητή νοημοσύνη) {SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}. Διαθέσιμο σε: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0009.02/DOC_2&format=PDF (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Ευρωπαϊκή Επιτροπή (2021) *Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη θέσπιση εναρμονισμένων κανόνων σχετικά με την τεχνητή νοημοσύνη (Πράξη για την τεχνητή νοημοσύνη) [COM/2021/206 final]*. Διαθέσιμο στο: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0009.02/DOC_1&format=PDF (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Ευρωπαϊκό Κοινοβούλιο (2021) 'Ψήφισμα της 20ής Ιανουαρίου 2021 σχετικά με την τεχνητή νοημοσύνη: ζητήματα ερμηνείας και εφαρμογής του διεθνούς δικαίου στον βαθμό που η Ένωση επηρεάζεται στους τομείς που αφορούν στρατιωτική και μη στρατιωτική χρήση της και ζητήματα κρατικής εξουσίας εκτός του πεδίου εφαρμογής της ποινικής δικαιοσύνης (2020/2013(INI))'Διαθέσιμο στο: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0009_EL.html (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Ευρωπαϊκό Κοινοβούλιο (2021) 'Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 25ης Μαρτίου 2021 σχετικά με την έκθεση αξιολόγησης της Επιτροπής για την εφαρμογή του γενικού κανονισμού για την προστασία δεδομένων δύο έτη μετά την εφαρμογή του (2020/2717(RSP))'. Διαθέσιμο σε: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_EL.pdf (Ημερομηνία Πρόσβασης: Ιούνιος 2022).
- Ευρωπαϊκό Κοινοβούλιο (2022) 'Δελτίο τύπου: Η Ε.Ε. να καθορίσει τα παγκόσμια πρότυπα για την τεχνητή νοημοσύνη ζητά το Κοινοβούλιο', σελ. 1–2. Διαθέσιμο στο: https://www.europarl.europa.eu/news/el/press-room/20220429IPR28228/i-ee-na-kathorisei-ta-pagkosmia-protupa-gia-tin-techniti-noimosuni-zita-to-ek (Ημερομηνία Πρόσβασης: Ιούνιος 2022).
- Ευρωπαϊκό Κοινοβούλιο (2022) *Τεχνητή νοημοσύνη στην ψηφιακή εποχή- Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 3ης Μαΐου 2022 σχετικά με την τεχνητή νοημοσύνη στην ψηφιακή εποχή (2020/2266(INI))*. Διαθέσιμο στο: https://www.europarl.europa.eu/doceo/document/TA-9-2022-0140_EL.pdf (Ημερομηνία Πρόσβασης: Ιούνιος 2022).
- Ευρωπαϊκό Κοινοβούλιο- Ειδική Επιτροπή για την τεχνητή νοημοσύνη στην ψηφιακή εποχή (2022) 'Τεχνητή νοημοσύνη στην ψηφιακή εποχή

(2020/2266(INI))'. Διαθέσιμο στο: https://www.europarl.europa.eu/doceo/document/A-9-2022-0088_EN.pdf (Ημερομηνία πρόσβασης: Ιούνιος 2022).

- Ευρωπαϊκό Κοινοβούλιο-Επιτροπή Πολιτικών Ελευθεριών, Δικαιοσύνης και Εσωτερικών Υποθέσεων (2021) 'Έκθεση σχετικά με την τεχνητή νοημοσύνη στο ποινικό δίκαιο και τη χρήση της από τις αστυνομικές και δικαστικές αρχές σε ποινικές υποθέσεις (2020/2016(INI))', Διαθέσιμο στο: https://www.europarl.europa.eu/doceo/document/A-9-2021-0232_EN.pdf (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (2020) 'Κατευθυντήριες γραμμές 3/2019 σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω βιντεοσυσκευών'. Διαθέσιμο στο: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_el.pdf (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (2020) 'Κατευθυντήριες γραμμές 4/2019 σύμφωνα με το άρθρο 25 Προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού'. Διαθέσιμο στο: https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_el.pdf (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (2021) 'Κατευθυντήριες γραμμές 8/2020 σχετικά με τη στόχευση χρηστών μέσων κοινωνικής δικτύωσης' Διαθέσιμο στο: https://edpb.europa.eu/system/files/2021-11/edpb_guidelines_082020_on_the_targeting_of_social_media_users_el_0.pdf (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Ιγγλεζάκης, Ι. (2021) '*Δίκαιο πληροφορικής- Δ΄ Έκδοση*'. Εκδόσεις Σάκκουλα.
- Καλλιντέρης, Ν. (2020) 'Ψηφιακή αναγνώριση προσώπου: μια διεθνής χαρτογράφηση', *Homo digitalis*. Διαθέσιμο στο: https://www.homodigitalis.gr/posts/6911 (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Κανέλλος, Λ. (2020) *The GDPR Handbook*. Νομική Βιβλιοθήκη.
- Κανέλλος, Λ. (2021) *Εφαρμογές Τεχνητής Νοημοσύνης στο δίκαιο & στη δικαστική πρακτική*. Νομική Βιβλιοθήκη.
- Καρκατζούνης, Β., Τσόλιας, Γ. (2021) 'Εξέταση των επιπτώσεων στο δικαστικό σύστημα της εισαγωγής της τεχνητής νοημοσύνης (artificial intelligence)»'σε: *Διαρκής Επιστημονική Επιτροπή του Υπουργείου Δικαιοσύνης για την Τεχνητή Νοημοσύνη*. Διαθέσιμο στο: https://www.ministryofjustice.gr/wp-content/uploads/2021/10/Praktiko-Synedriasis-10-Iouniou-2021.pdf (Ημερομηνία πρόσβασης: Ιούνιος 2022).

- Κοτσαλής Λ. *κ.ά.* (2021) *'Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων (GDPR), Νομική Διάσταση και πρακτική εφαρμογή- Β' Έκδοση'*. Νομική Βιβλιοθήκη.
- Ομάδα Εργασίας του άρθρου 29 για την προστασία δεδομένων (2012) 'Γνώμη 3/2012 σχετικά με τις εξελίξεις στις βιομετρικές τεχνολογίες'. Διαθέσιμο σε: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_el.pdf (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Ομάδα Εργασίας του άρθρου 29 για την προστασία δεδομένων (2014) 'Γνώμη 06/2014 σχετικά με την έννοια των εννόμων συμφερόντων του υπευθύνου επεξεργασίας, σύμφωνα με το άρθρο 7 της οδηγίας 95/46/ΕΚ' Διαθέσιμο στο: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_el.pdf (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Ομάδα Εργασίας του άρθρου 29 για την προστασία δεδομένων (2017), 'Κατευθυντήριες γραμμές σχετικά με τη συγκατάθεση βάσει του κανονισμού 2016/679' Διαθέσιμο προς λήψη στο: https://ec.europa.eu/newsroom/article29/items/623051/en (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Ομάδα Εργασίας του άρθρου 29 για την προστασία δεδομένων (2018) 'Κατευθυντήριες γραμμές για την αυτοματοποιημένη λήψη αποφάσεων και την κατάρτιση προφίλ για τους σκοπούς του κανονισμού 2016/679'. Διαθέσιμο στο: https://www.dpa.gr/sites/default/files/2020-05/wp251rev01_el.pdf (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Παπαδούλη, Β. (2022) 'Εννοιολογικές Προσεγγίσεις της «Διαφάνειας» στο πεδίο της Τεχνητής Νοημοσύνης υπό ένα νομικό πρίσμα', *Pro Justitia: Ηλεκτρονική Επετηρίδα Νομικής Σχολής ΑΠΘ*, 5(0), σσ 30–44. doi:10.26262/pj.v5i0.8670.
- Σκόνδρα, Μ. (2020) 'Αναγνώριση προσώπου (Face Recognition) και προσωπικά δεδομένα', *Lawspot*. Διαθέσιμο στο: https://www.lawspot.gr/nomika-blogs/magdalini_skondra/anagnorisi-prosopoy-face-recognition-kai-prosopika-dedomena (Ημερομηνία πρόσβασης Ιούνιος 2022).
- Σκόνδρα, Μ. (2020) 'Συστήματα Βιντεοεπιτήρησης , αναγνώριση προσώπου και προστασία προσωπικών δεδομένων', *ΔΙΤΕ (π. ΔΙΜΕΕ)*, (1), σελ. 45–56.
- Συμβουλευτική Επιτροπή της Σύμβασης 108 (2021) *'Κατευθυντήριες γραμμές για την αναγνώριση προσώπου'*. Διαθέσιμο στο: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000 (Ημερομηνία πρόσβασης Ιούνιος 2022).
- Τάσσης, Σπ. (2018). *Η Εποχή της Τεχνητής Νοημοσύνης* , ΔΙΤΕ (πρώην ΔιΜΕΕ) 4/2018, σ. 484-494.

- Τσόλιας, Γ. (2021) 'Η περίπτωση των Συστημάτων Απομακρυσμένης Βιομετρικής Αναγνώρισης και Ταυτοποίησης φυσικών προσώπων για σκοπούς δίωξης του εγκλήματος σύμφωνα με το σχέδιο πρότασης Κανονισμού Ε.Ε. για την Τεχνητή Νοημοσύνη', σε *Διαρκής Επιστημονική Επιτροπή του Υπουργείου Δικαιοσύνης για την Τεχνητή Νοημοσύνη*. Διαθέσιμο στο: https://www.ministryofjustice.gr/wp-content/uploads/2021/11/TSOLIAS_sxKan_TNFRT.pdf (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Homo digitalis (2019) *Προ των πυλών η χρήση τεχνολογίας αναγνώρισης προσώπου από την αστυνομία στην Ελλάδα*. Διαθέσιμο στο: https://www.homodigitalis.gr/posts/4662 (Ημερομηνία πρόσβασης: Ιούνιος 2022).

III. ΝΟΜΟΘΕΣΙΑ:

- 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)*.
- Κανονισμός (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Οκτωβρίου 2018, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης και την ελεύθερη κυκλοφορία των δεδομένων αυτών, και για την κατάργηση του κανονισμού (ΕΚ) αριθ. 45/2001 και της απόφασης αριθ. 1247/2002/ΕΚ.
- 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.

IV. ΑΠΟΦΑΣΕΙΣ ΑΡΧΩΝ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

- Ελληνική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (2021) *Απόφαση 32/2021*. Διαθέσιμη στο: https://www.dpa.gr/sites/default/files/2021-08/32_2021anonym.pdf (Ημερομηνία Πρόσβασης: Ιούνιος 2022).

- Ελληνική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (2022) *Απόφαση 35/2022*. Διαθέσιμη στο: https://www.dpa.gr/sites/default/files/2022-07/35_2022%20anonym_0.pdf (Ημερομηνία Πρόσβασης: Ιούνιος 2022).
- Ελληνική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (2018) *Απόφαση 65/2018*. Διαθέσιμη στο: https://www.dpa.gr/sites/default/files/2019-09/65_2018anonym.pdf (Ημερομηνία Πρόσβασης: Ιούνιος 2022).
- Commission Nationale de l'Informatique et des Libertés (CNIL) 'Decision n° MED 2021-134 of 1st November 2021 issuing an order to comply to the company CLEARVIEW AI' Διαθέσιμο σε: https://www.cnil.fr/sites/default/files/atoms/files/decision_ndeg_med_2021-134.pdf (Ημερομηνία Πρόσβασης: Ιούνιος 2022).
- Swedish Data Protection Authority (2019)- Ref. no: DI-2019-2221 'Supervision pursuant to the General Data Protection Regulation (EU) 2016/679 – facial recognition used to monitor the attendance of students'. Διαθέσιμο σε: https://www.imy.se/globalassets/dokument/beslut/facial-recognition-used-to-monitor-the-attendance-of-students.pdf (Ημερομηνία Πρόσβασης: Ιούνιος 2022).

V. ΝΟΜΟΛΟΓΙΑ

- European Court of Human Rights (1978) *Klass and Others v. Germany*. Διαθέσιμο στο: https://hudoc.echr.coe.int/eng#%7B%22itemid%22:[%22001-57510%22]%7D (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Ευρωπαϊκό Δικαστήριο Δικαιωμάτων του Ανθρώπου (2008) *S and Marper κατά Ηνωμένου Βασιλείου*. Διαθέσιμο στο: https://rm.coe.int/168067d216 (Ημερομηνία πρόσβασης: Ιούνιος 2022).
- Δικαστήριο της Ευρωπαϊκής Ένωσης (2014) *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* (συνεκδικαζόμενες υποθέσεις C-293/12 και C-594/12). Διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:62012CJ0293&from=EN (Ημερομηνία Πρόσβασης: Ιούνιος 2022).
- Εφετείο Ηνωμένου Βασιλείου (2020) *R (Bridges) v Chief Constable of South Wales Police & Information Commissioner* (EWCA Civ 1058). Διαθέσιμο σε: https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf (Ημερομηνία Πρόσβασης: Ιούνιος 2022).