



ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»

Ακαδημαϊκό έτος 2024-2026

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της Μαρίας Δημάκη (Α.Μ.: 2411)

ΣΥΣΤΗΜΑΤΑ ΑΝΑΓΝΩΡΙΣΗΣ ΠΡΟΣΩΠΟΥ ΣΕ ΔΗΜΟΣΙΟΥΣ ΧΩΡΟΥΣ ΓΙΑ ΣΚΟΠΟΥΣ
ΕΠΙΒΟΛΗΣ ΤΟΥ ΝΟΜΟΥ: ΚΙΝΔΥΝΟΙ ΣΤΟ ΠΛΑΙΣΙΟ ΤΟΥ ΚΑΝΟΝΙΣΜΟΥ ΓΙΑ ΤΗΝ
ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ

FACIAL RECOGNITION SYSTEMS IN PUBLIC SPACES FOR LAW ENFORCEMENT
PURPOSES: RISKS UNDER THE AI ACT

Επιβλέπουσα Καθηγήτρια:

Λίλιαν Μήτρου

Πειραιάς, Ιούλιος 2026

Ένα μεγάλο «Ευχαριστώ» στην οικογένειά μου
που στέκεται αρωγός σε κάθε μου βήμα.

© 2026

της

[ΜΑΡΙΑΣ ΔΗΜΑΚΗ]

Τμήμα Ψηφιακών Συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ.....	8
ABSTRACT.....	10
1 ΕΙΣΑΓΩΓΗ.....	11
2 ΒΙΟΜΕΤΡΙΑ ΚΑΙ ΒΙΟΜΕΤΡΙΚΑ ΔΕΔΟΜΕΝΑ.....	13
2.1 Βιομετρία.....	13
2.2 Βιομετρικά Δεδομένα	14
2.3 Λειτουργίες των βιομετρικών συστημάτων: Ταυτοποίηση και Επαλήθευση.....	17
3 ΣΥΣΤΗΜΑΤΑ ΑΝΑΓΝΩΡΙΣΗΣ ΠΡΟΣΩΠΟΥ	20
3.1 Έννοια	20
3.2 Τρόπος Λειτουργίας.....	23
3.3 Ιστορική Αναδρομή.....	26
3.3.1 Τα Πρώτα Αυτοματοποιημένα Συστήματα (1970–1990).....	27
3.3.2 Η μετάβαση από Γεωμετρικές μεθόδους σε Ολιστικές (1990–2000).....	29
3.3.3 Η συμβολή της βαθιάς μάθησης (Deep Learning) στην αναγνώριση προσώπου	30
3.4 Η εφαρμογή αναγνώρισης προσώπου για σκοπούς επιβολής του νόμου	34
4 ΤΟ ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ ΓΙΑ ΤΑ ΣΥΣΤΗΜΑΤΑ ΕΞ ΑΠΟΣΤΑΣΕΩΣ ΒΙΟΜΕΤΡΙΚΗΣ ΤΑΥΤΟΠΟΙΗΣΗΣ ΣΤΟΝ ΚΑΝΟΝΙΣΜΟ ΓΙΑ ΤΗΝ ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ	38
4.1 Εισαγωγή	38
4.2 Η νομοπαρασκευαστική πορεία	39
4.3 Συστήματα εξ απόστασεως ταυτοποίησης σε πραγματικό χρόνο (real time)	42
4.4 Βιομετρική ταυτοποίηση σε μεταγενέστερο χρόνο (post-remote biometric identification).....	47
5 ΣΧΕΣΗ ΤΗΣ ΠΡΑΞΗΣ ΓΙΑ ΤΗΝ ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ ΜΕ ΑΛΛΑ ΝΟΜΟΘΕΤΙΚΑ ΚΕΙΜΕΝΑ – ΑΛΛΗΛΕΠΙΔΡΑΣΗ ΜΕ ΓΚΠΔ ΚΑΙ ΟΔΗΓΙΑ (ΕΕ) 2016/680 ..	51
5.1 Γενικός Κανονισμός Προστασίας Δεδομένων	51
5.2 Οδηγία (ΕΕ) 2016/680 για την επιβολή του νόμου (LED)	55
5.2.1 Ιστορικό Πλαίσιο και Διάκριση από άλλα νομοθετήματα	55
5.2.2 Πεδίο εφαρμογής	57

5.3	Συμπεράσματα – Σχέσεις μεταξύ των νομοθετημάτων	63
5.3.1	Σχέση ΑΙΑ - LED	63
5.3.2	Σχέση ΓΚΠΔ – LED	65
5.3.3	Σχέση ΑΙΑ - ΓΚΠΔ	65
6	Ο ΑΝΤΙΚΤΥΠΟΣ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΑΝΑΓΝΩΡΙΣΗΣ ΠΡΟΣΩΠΟΥ ΣΤΑ ΘΕΜΕΛΙΩΔΗ ΔΙΚΑΙΩΜΑΤΑ.....	68
6.1	Γενικά	68
6.2	Επέμβαση στο δικαίωμα της Ιδιωτικής Ζωής και της Προστασίας Δεδομένων	69
6.2.1	Ιδιωτική Ζωή.....	70
6.2.2	Δικαίωμα στην προστασία προσωπικών δεδομένων.....	74
6.3	Επέμβαση στο δικαίωμα της μη διακριτικής μεταχείρισης	75
7	ΟΙ ΠΡΟΫΠΟΘΕΣΕΙΣ ΠΕΡΙΟΡΙΣΜΟΥ ΤΩΝ ΘΕΜΕΛΙΩΔΩΝ ΔΙΚΑΙΩΜΑΤΩΝ	79
7.1	Νομοθετική πρόβλεψη.....	79
7.2	Η Αρχή της Αναλογικότητας ως Κριτήριο Νομιμότητας.....	81
7.3	Αναγκαιότητα σε μία δημοκρατική κοινωνία	82
7.4	Τελικές Σκέψεις εν είδει συμπερασμάτων	83
8	ΣΥΜΠΕΡΑΣΜΑΤΑ	87
9	ΠΗΓΕΣ ΚΑΙ ΑΝΑΦΟΡΕΣ	89

ΑΚΡΩΝΥΜΙΑ

ΑΔΑΕ	Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών
ΑΠΔΠΧ	Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
ΓΚΠΔ	Γενικός Κανονισμός για την Προστασία Προσωπικών Δεδομένων
ΔΕΕ	Δικαστήριο της Ευρωπαϊκής Ένωσης
ΕΔΔΑ	Ευρωπαϊκό Δικαστήριο Δικαιωμάτων του Ανθρώπου
ΕΕ	Ευρωπαϊκή Ένωση
ΕΕΠΑ	Ευρωπαίος Επόπτης Προστασίας Δεδομένων
ΕΣΔΑ	Ευρωπαϊκή Σύμβαση Δικαιωμάτων Ανθρώπου
ΕΣΠΔ	Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων
ΣΛΕΕ	Συνθήκη Λειτουργίας Ευρωπαϊκής Ένωσης
TN	Τεχνητή Νοημοσύνη
ΧΘΔΕΕ	Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης
ΑΙΑ	Artificial Intelligence Act
CCTV	Closed Circuit TV
GDPR	General Data Protection Regulation
LED	Law Enforcement Directive
FR	Facial Recognition
FRT	Facial Recognition Technology
RBI	Remote Biometric Identification

ΠΕΡΙΛΗΨΗ

Για μισό και πλέον αιώνα, το όραμα μηχανών που «βλέπουν» και αναγνωρίζουν πρόσωπα έχει συναρπάσει την ερευνητική κοινότητα, μεταβαίνοντας από τον χώρο της επιστημονικής φαντασίας σε μια διάχυτη πραγματικότητα. Αυτό που ξεκίνησε ως ένα υπολογιστικά δυσχερές πρόβλημα, το οποίο απαιτούσε επίπονη χειροκίνητη εξαγωγή χαρακτηριστικών, εξελίχθηκε σε θεμέλιο λίθο της σύγχρονης ασφάλειας, της ευκολίας και ακόμη και της κοινωνικής αλληλεπίδρασης. Ωστόσο, αυτή η ραγδαία τεχνολογική εξέλιξη δεν στερείται πολυπλοκότητας. Η πορεία από το πρωτοποριακό έργο των Bledsoe και Kanade έως τα σημερινά «κολοσσιαία» μοντέλα βαθιάς μάθησης αποκαλύπτει όχι μόνο μια ιστορία αλγοριθμικής καινοτομίας, αλλά και ένα μεταβαλλόμενο τοπίο ηθικών προβληματισμών, εξαρτήσεων από τα βιομετρικά δεδομένα και μίας διαρκούς πρόκλησης ως προς τον ίδιο ορισμό της «ταυτότητας».

Σε απάντηση αυτών των ανησυχιών, η Ευρωπαϊκή Ένωση προέκρινε τη ρύθμιση των βιομετρικών τεχνολογιών μέσω της Πράξης για την Τεχνητή Νοημοσύνη (AI Act). Ενώ ο Κανονισμός θέτει ως αρχικό στόχο την απαγόρευση των συστημάτων εξ αποστάσεως βιομετρικής ταυτοποίησης σε πραγματικό χρόνο (real-time) για σκοπούς επιβολής του νόμου, λόγω των μη αποδεκτών κινδύνων που ενέχουν για τα θεμελιώδη δικαιώματα, εισάγει παράλληλα εκτεταμένες εξαιρέσεις. Οι εξαιρέσεις αυτές ενδέχεται να διευρύνουν το πεδίο εφαρμογής της τεχνολογίας, επεκτείνοντας τη χρήση της πέραν του αρχικού σκοπού. Στον αντίποδα, τα συστήματα βιομετρικής ταυτοποίησης «εκ των υστέρων» (post-remote) ταξινομούνται ως «υψηλού κινδύνου», υποκείμενα σε λιγότερο αυστηρές απαιτήσεις, γεγονός που εντείνει τους φόβους ότι η αλόγιστη χρήση τους θα μπορούσε να οδηγήσει σε συνθήκες μαζικής επιτήρησης.

Υπό το πρίσμα των αντιπαραθέσεων που περιβάλλουν το εν λόγω ρυθμιστικό πλαίσιο, η παρούσα μελέτη φιλοδοξεί να χαρτογραφήσει αυτήν την εξέλιξη, εξετάζοντας τα τεχνολογικά ορόσημα, τα επίμονα εμπόδια και τα νομικά ζητήματα που θα διαμορφώσουν το μέλλον της αυτοματοποιημένης αναγνώρισης προσώπου. Μέσα από την ανάλυση των σχετικών διατάξεων του Κανονισμού, διερευνώνται περαιτέρω οι επιπτώσεις αυτών των συστημάτων στα ανθρώπινα δικαιώματα και στις ελευθερίες των πολιτών, σε

αντιπαράθεση με τα προσδοκώμενα οφέλη ασφαλείας, με στόχο να αξιολογηθεί εάν η χρήση τους από τα κράτη είναι δικαιολογημένη ή εάν πρέπει να προταθεί η απαγόρευσή τους.

Λέξεις Κλειδιά: Βιομετρική Ταυτοποίηση, Αναγνώριση Προσώπου, AI Act

ABSTRACT

For more than half a century, the vision of machines that ‘see’ and recognize faces has captivated the research community, transitioning from the realm of science fiction to a pervasive reality. What began as a computationally challenging problem, requiring laborious manual feature extraction, has evolved into a cornerstone of modern security, convenience, and even social interaction. However, this rapid technological evolution is not without its complexities. The trajectory from the pioneering work of Bledsoe and Kanade to today’s ‘colossal’ deep learning models reveals not only a history of algorithmic innovation but also a shifting landscape of ethical concerns, reliance on biometric data, and an enduring challenge regarding the very definition of ‘identity’.

In response to these concerns, the European Union chose to regulate biometric technologies through the Artificial Intelligence Act (AI Act). While the Regulation aims to prohibit ‘real-time’ remote biometric identification systems for the purposes of law enforcement due to the unacceptable risks they pose to fundamental rights, it simultaneously introduces extensive exceptions. These exceptions may broaden the technology’s scope of application, extending its use beyond the original intent. Conversely, post-remote biometric identification systems are classified merely as ‘high-risk,’ subject to less stringent requirements, a fact that intensifies fears that their indiscriminate use could lead to conditions of mass surveillance.

In light of the controversies surrounding this regulatory framework, this study aims to map out this evolution by examining the technological milestones, persistent hurdles, and legal issues that will shape the future of automated facial recognition. Through an analysis of the Regulation’s relevant provisions, this thesis further investigates the implications of these systems for human rights and civil liberties, juxtaposing them against the anticipated security benefits, in order to assess whether their use by states is justified or if their prohibition is warranted.

Keywords: Biometric identification, Facial Recognition, AI Act

1 ΕΙΣΑΓΩΓΗ

Η ραγδαία εξέλιξη της Τεχνητής Νοημοσύνης (TN) την τελευταία δεκαετία έχει μεταμορφώσει ριζικά τον τρόπο με τον οποίο οι μηχανές αντιλαμβάνονται και επεξεργάζονται τον φυσικό κόσμο. Στην αιχμή αυτής της επανάστασης βρίσκεται η χρήση βιομετρικών τεχνολογιών, η οποία αποτελεί ένα πρόβλημα υποκατηγορίας της αναγνώρισης οπτικών προτύπων. Ενώ οι άνθρωποι αναγνωρίζουν οπτικά πρότυπα συνεχώς, μεταφράζοντας τις οπτικές πληροφορίες σε νοηματικές έννοιες, η πληροφορία για αυτή παραμένει για έναν υπολογιστή ένας πίνακας εικονοστοιχείων (pixels). Η μηχανή καλείται να προσδιορίσει ποια έννοια αντιπροσωπεύει ένα συγκεκριμένο τμήμα των δεδομένων, γεγονός που συνιστά ένα πρόβλημα αδρής ταξινόμησης. Στην περίπτωση της αναγνώρισης προσώπου, απαιτείται η περαιτέρω εξειδίκευση (subdivision problem) για τον προσδιορισμό της ταυτότητας του ατόμου, στο οποίο ανήκει το ήδη ανιχνευμένο πρόσωπο¹.

Τα Συστήματα Αναγνώρισης Προσώπου ως υποσύνολο της βιομετρικής τεχνολογίας ξεχωρίζουν ως ένα από τα πλέον ισχυρά, αλλά και αμφιλεγόμενα εργαλεία. Ενώ αρχικά η χρήση τους περιοριζόταν σε απλές εφαρμογές επαλήθευσης ταυτότητας σε ελεγχόμενα περιβάλλοντα, σήμερα η τεχνολογία αυτή έχει ενσωματωθεί στο οπλοστάσιο των αρχών επιβολής του νόμου για την πρόληψη και καταστολή του εγκλήματος.

Η ανάπτυξη τέτοιων συστημάτων σε δημοσίως προσβάσιμους χώρους δημιουργεί μια πρωτοφανή νομική και ηθική πρόκληση. Σε αντίθεση με τις παραδοσιακές μεθόδους αστυνόμευσης, η Αναγνώριση Προσώπου (FR) επιτρέπει την εξ αποστάσεως, αθέατη και αυτοματοποιημένη σάρωση ενός ακαθόριστου αριθμού πολιτών. Αυτή η δυναμική φέρνει στο προσκήνιο μια θεμελιώδη σύγκρουση: από τη μία πλευρά, προβάλλεται η επιτακτική ανάγκη των κρατών να διασφαλίσουν τη δημόσια τάξη και ασφάλεια -ιδίως απέναντι σε απειλές όπως η τρομοκρατία και το οργανωμένο έγκλημα- και από την άλλη, εγείρονται εύλογες ανησυχίες για τη δραματική συρρίκνωση των θεμελιωδών δικαιωμάτων, όπως η

¹ Li, L., Mu, X., Li, S. και Peng, H. (2020) 'A Review of Face Recognition Technology', *IEEE Access*, 8, σσ. 139110-139120. Διαθέσιμο στο: <https://doi.org/10.1109/ACCESS.2020.3011028> (Πρόσβαση: Φεβρουάριος 2026)

ιδιωτικότητα, η προστασία των προσωπικών δεδομένων, υπό τον φόβο της εγκαθίδρυσης ενός καθεστώτος μαζικής επιτήρησης.

Ως απάντηση σε αυτές τις προκλήσεις, η Ευρωπαϊκή Ένωση προχώρησε στη θέσπιση της Πράξης για την Τεχνητή Νοημοσύνη (AI Act), φιλοδοξώντας να θέσει ένα παγκόσμιο ρυθμιστικό πρότυπο. Ο Κανονισμός υιοθετεί μια προσέγγιση βασισμένη στον κίνδυνο (risk-based approach), προκειμένου να ρυθμίσει τη χρήση αυτών των συστημάτων.

Υπό το φως των αντιπαραθέσεων που περιβάλλουν αυτό το ρυθμιστικό πλαίσιο, η παρούσα μελέτη αναλύει την λειτουργία των συστημάτων εξ αποστάσεως βιομετρικής ταυτοποίησης, με ιδιαίτερη έμφαση στις τεχνολογίες αναγνώρισης προσώπου, εστιάζοντας στο νομοθετικό πλαίσιο που τις διέπει. Ειδικότερα, η εργασία επιδιώκει να απαντήσει στο ερώτημα εάν οι διατάξεις του Κανονισμού επιτυγχάνουν μια δίκαιη ισορροπία μεταξύ της διαφύλαξης της εθνικής ασφάλειας και της προστασίας των θεμελιωδών δικαιωμάτων των πολιτών, υπό το πρίσμα της αρχής της αναλογικότητας και της νομολογίας του Ευρωπαϊκού Δικαστηρίου Δικαιωμάτων του Ανθρώπου (ΕΔΔΑ).

Η παρούσα μελέτη διαρθρώνεται ως εξής:

Στο **Δεύτερο και Τρίτο Κεφάλαιο** αποσαφηνίζονται οι βασικές έννοιες και η τεχνική λειτουργία των συστημάτων FR, με έμφαση στα βιομετρικά δεδομένα και τη μετάβαση από τις παραδοσιακές μεθόδους στις εφαρμογές TN για την επιβολή του νόμου.

Στο **Τέταρτο Κεφάλαιο** αναλύεται το ρυθμιστικό πλαίσιο της Πράξης για την TN (AI Act), διακρίνοντας τη βιομετρική ταυτοποίηση σε πραγματικό και μεταγενέστερο χρόνο.

Στο **Πέμπτο Κεφάλαιο** επιχειρείται συγκριτική επισκόπηση του AI Act με τον ΓΚΠΔ και την Οδηγία LED, προκειμένου να εντοπιστούν τυχόν νομοθετικά κενά ή επικαλύψεις.

Στο **Έκτο και Έβδομο Κεφάλαιο** εξετάζεται ο αντίκτυπος στα θεμελιώδη δικαιώματα (ιδιωτικότητα, προσωπικά δεδομένα, απαγόρευση διακρίσεων) και οι προϋποθέσεις υπό τις οποίες είναι θεμιτός ο περιορισμός τους, ενώ παρατίθεται και η κριτική αποτίμηση του AI Act.

Τέλος, στα **Συμπεράσματα** αξιολογείται η αποτελεσματικότητα του νέου πλαισίου και διατυπώνονται προοπτικές για το μέλλον της βιομετρικής επιτήρησης στην Ευρώπη.

2 ΒΙΟΜΕΤΡΙΑ ΚΑΙ ΒΙΟΜΕΤΡΙΚΑ ΔΕΔΟΜΕΝΑ

Στο πλαίσιο της διερεύνησης του νομικού και τεχνολογικού τοπίου που διαμορφώνει ο Κανονισμός για την Τεχνητή Νοημοσύνη, η παρούσα έρευνα εκκινεί από τον προσδιορισμό του τι νοείται ως «βιομετρία» (“biometrics”) και «βιομετρικά δεδομένα» (“biometric data”). Η διάκριση αυτή είναι κρίσιμη για την κατανόηση των συστημάτων βιομετρικής ταυτοποίησης, δεδομένου ότι οι μηχανισμοί που εξετάζονται στην εργασία βασίζονται ακριβώς στην αυτοματοποιημένη αναγνώριση ατόμων μέσω φυσικών χαρακτηριστικών, με κυρίαρχο αυτό της αναγνώρισης προσώπου.

2.1 Βιομετρία

Ο όρος «βιομετρία», προερχόμενος από τη σύνθεση των λέξεων «βίος» και «μέτρον», αναφέρεται στην ποσοτική μέτρηση βιολογικών χαρακτηριστικών και στη μηχανική επεξεργασία τους². Κατά τον Albrizio, η βιομετρία αποτελεί ουσιαστικά προϊόν σύζευξης μεταξύ των επιστημών της ζωής και της μέτρησης. Ως εκ τούτου, περιλαμβάνει την ποσοτική έρευνα στον άνθρωπο, τα ζώα και τα φυτά. Μέσω της αξιοποίησης μαθηματικών και στατιστικών μεθόδων, η επιστήμη αυτή στοχεύει στον ακριβή προσδιορισμό της μοναδικότητας συγκεκριμένων χαρακτηριστικών -ανατομικών ή συμπεριφορικών- ενός υποκειμένου ή μιας ομάδας³.

Στη σύγχρονη εποχή, ωστόσο, ο εν λόγω όρος έχει προσλάβει μια στενότερη εννοιολογική σημασία, η οποία διαφοροποιείται αισθητά από την αρχική, όπου η βιομετρία αφορούσε κυρίως τη στατιστική μελέτη βιολογικών φαινομένων. Πλέον, η «βιομετρία» συνδέεται άρρηκτα με την αυτοματοποιημένη αναγνώριση ατόμων βάσει των συμπεριφορικών ή φυσικών χαρακτηριστικών τους. Μάλιστα, για να χαρακτηριστεί η διαδικασία ως

² Mordini, E. *et al.* (2012) ‘Introduction’, στο Mordini, E. και Tzovaras, D. (επιμ.) *Second Generation Biometrics: The Ethical, Legal and Social Context*. Springer, σ. 8.

³ Albrizio, A. (2007) ‘Biometry and Anthropometry: from Galton to Constitutional Medicine’, *Journal of Anthropological Sciences*, 85, σσ. 101-123.

«αυτόματη», απαιτείται η αναγνώριση ή επαλήθευση του χαρακτηριστικού να ολοκληρώνεται εντός εύλογου χρόνου και χωρίς υψηλό βαθμό ανθρώπινης παρέμβασης⁴.

Κατά συνέπεια, για τους σκοπούς της παρούσας μελέτης, ο όρος θα χρησιμοποιηθεί σύμφωνα με την επικρατούσα, στενή του έννοια. Κατά τον Hopkins, ως βιομετρία ορίζεται η εφαρμογή υπολογιστικών μεθόδων σε βιολογικά χαρακτηριστικά και, ειδικότερα, η μελέτη των βιολογικών χαρακτηριστικών του ανθρώπου⁵. Η τεχνική αυτή επιτρέπει την αυθεντικοποίηση ταυτοτήτων και τη συσχέτισή τους με γεγονότα, τοποθεσίες ή συγκεκριμένες ομάδες ενδιαφέροντος.

2.2 Βιομετρικά Δεδομένα

Προτού προχωρήσουμε στον ορισμό των βιομετρικών δεδομένων, κρίνεται σκόπιμη η διάκρισή της από την προαναφερθείσα έννοια της «βιομετρίας». Από τη σύγκριση και ανάλυση των δύο εννοιών προκύπτει ότι οι δύο έννοιες δεν είναι ταυτόσημες, παρόλο που συχνά εμφανίζονται ως τέτοιες. Και αυτό διότι ο όρος «βιομετρικά δεδομένα» αποτελεί ταυτόχρονα τεχνική και νομική έννοια, ενώ η «βιομετρία» συνιστά αποκλειστικά τεχνική έννοια. Όπως προαναφέρθηκε, ο όρος «βιομετρία» προέρχεται ουσιαστικά από τον κλάδο της βιομετρικής αναγνώρισης. Ως εκ τούτου, στο πλαίσιο της προστασίας δεδομένων, θα πρέπει να χρησιμοποιείται μόνο ως μια «μέθοδος αυτόματης αναγνώρισης» που βασίζεται σε βιομετρικά χαρακτηριστικά. Από την άλλη πλευρά, ο όρος «βιομετρικά δεδομένα» αναφέρεται στην τεχνική μετατροπή των βιομετρικών γνωρισμάτων σε μορφή κατάλληλη για βιομετρική αναγνώριση. Σύμφωνα με τον τεχνικό ορισμό, η ύπαρξη συνδέσμου με ένα συγκεκριμένο ταυτοποιημένο πρόσωπο δεν αποτελεί προϋπόθεση. Αντίθετα, στο πλαίσιο της προστασίας δεδομένων, αυτή η σύνδεση είναι καθοριστική προκειμένου να προσδιοριστεί εάν τα τεχνικά "βιομετρικά δεδομένα" συνιστούν δεδομένα προσωπικού χαρακτήρα⁶.

⁴ Riera, A. *et al.* (2012) 'Electrophysiological Biometrics: Opportunities and Risks', στο Mordini, E. και Tzovaras, D. (επιμ.) *Second Generation Biometrics: The Ethical, Legal and Social Context*. Springer, σ. 152.

⁵ Hopkins, R. (2010) 'An Introduction to Biometrics and Large Scale Civilian Identification', *International Review of Law, Computers & Technology*, 13(3), σ. 337.

⁶ Jasserand, Catherine, Legal Nature of Biometric Data: From 'Generic' Personal Data to Sensitive Data' (June 1, 2016). *European Data Protection Law Review*, Vol. 2 (2016), Issue 3, pp. 297-311, University of

Είναι αξιοσημείωτο πως η έννοια των βιομετρικών δεδομένων απουσίαζε από τα δύο θεμελιώδη ευρωπαϊκά κείμενα για την προστασία των προσωπικών δεδομένων, τη Σύμβαση 108 και την Οδηγία 95/46/EK. Η απουσία αυτή κρίνεται ιστορικά εύλογη, καθώς κατά τον χρόνο υιοθέτησής τους -το 1981 και το 1995 αντίστοιχα- η χρήση βιομετρικών τεχνολογιών και οι συνέπειες αυτής δεν είχαν καταστεί ακόμη αντικείμενο συστηματικής μελέτης από τα ευρωπαϊκά θεσμικά όργανα. Η σχετική συζήτηση εκκίνησε στις αρχές της δεκαετίας του 2000, με τις πρώτες εκθέσεις να αποτυπώνουν έκδηλους δισταγμούς ως προς και τον ορισμό και τον ακριβή νομικό χαρακτηρισμό των δεδομένων αυτών⁷.

Η δυσκολία ως προς τον χαρακτηρισμό τους πηγάζει από την ίδια την τεχνική τους φύση. Τα βιομετρικά δεδομένα, τα οποία χρησιμοποιούνται για να εκπαιδεύσουν το σύστημα, αποτελούνται από μοναδικά φυσικά χαρακτηριστικά, όπως η γεωμετρία του προσώπου, που επιτρέπουν την μονοσήμαντη ταυτοποίηση του ατόμου. Είναι πρόδηλο, λοιπόν, ότι τα βιομετρικά δεδομένα είναι κάτι περισσότερο από απλά δεδομένα εικόνας. Είναι ευαίσθητα προσωπικά δεδομένα που απαιτούν ισχυρή προστασία λόγω της μόνιμης και μοναδικά αναγνωρίσιμης φύσης τους. Σε αντίθεση με τους κωδικούς πρόσβασης, τα βιομετρικά δεδομένα είναι εγγενώς σταθερά και αμετάβλητα με την πάροδο του χρόνου για κάθε άνθρωπο. Αυτή η μονιμότητα, σε συνδυασμό με την καθολικότητα και τη μοναδικότητά τους⁸, κρούει τον κώδωνα του κινδύνου, καθώς ενδέχεται η αθέμιτη επεξεργασία τους να προκαλέσει σοβαρό πλήγμα στην ιδιωτικότητα και στα θεμελιώδη ανθρώπινα δικαιώματα, ειδικά σε περιπτώσεις μαζικής επιτήρησης. Επιπλέον των ανωτέρω, πρέπει να προστεθεί

Groningen Faculty of Law Research Paper No. 24/2018, Available at SSRN: <https://ssrn.com/abstract=3230342>

⁷ Jasserand, Catherine, Legal Nature of Biometric Data: From 'Generic' Personal Data to Sensitive Data' (June 1, 2016). European Data Protection Law Review, Vol. 2 (2016), Issue 3, pp. 297-311, University of Groningen Faculty of Law Research Paper No. 24/2018, Available at SSRN: <https://ssrn.com/abstract=3230342>

⁸ Cotino Hueso, L. (2023) 'Automated facial recognition and biometric identification systems under the overlapping regulation of artificial intelligence and data protection', στο Balaguer Callejón, F. και Cotino Hueso, L. (επιμ.) *Derecho Público de la Inteligencia Artificial*. Zaragoza: Fundación Manuel Jiménez Abad de Estudios Parlamentarios y del Estado Autonómico, σ. 353.

ένα ακόμη ουσιώδες γνώρισμα, το οποίο είναι η συλλεξιμότητα (collectability), δηλαδή η δυνατότητα του χαρακτηριστικού να μετρηθεί ποσοτικά⁹.

Για τον λόγο αυτό, τα βιομετρικά δεδομένα αναγνωρίζονται ως προσωπικά δεδομένα, καθώς αφορούν ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο¹⁰ και ταξινομούνται από τον Κανονισμό 2016/679 («Γενικός Κανονισμός για την Προστασία Δεδομένων», εφεξής «ΓΚΠΔ») ως «ειδικές κατηγορίες προσωπικών δεδομένων». Συγκεκριμένα ορίζονται ως «τα δεδομένα προσωπικού χαρακτήρα τα οποία προκύπτουν από ειδική τεχνική επεξεργασία συνδεδεμένη με φυσικά βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου, όπως εικόνες προσώπου ή δακτυλосκοπικά δεδομένα, και τα οποία επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου»¹¹. Όπως θα αναλυθεί διεξοδικότερα στις επόμενες ενότητες, το ευρωπαϊκό νομικό πλαίσιο που διέπει τη χρήση τους εντός της Ευρωπαϊκής Ένωσης υπογραμμίζει την ανάγκη για συντονισμένες διασφαλίσεις με σκοπό τον μετριασμό των κινδύνων και τη διαφύλαξη των θεμελιωδών δικαιωμάτων.

Οι φωτογραφίες προσώπων, λοιπόν, που χρησιμοποιούνται από τις τεχνολογίες ανίχνευσης προσώπου εμπίπτουν στον ορισμό των βιομετρικών δεδομένων κατά άρθρο 4 παρ. 1 του ΓΚΠΔ, καθόσον επιτρέπουν την ταυτοποίηση ενός φυσικού προσώπου μέσω της αναφοράς σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική ή φυσιολογική ταυτότητά του. Στο ίδιο συμπέρασμα έχει καταλήξει και το ΔΕΕ, το οποίο έχει κρίνει ότι «η εικόνα ενός προσώπου την οποία καταγράφει μία κάμερα, συνιστά δεδομένο προσωπικού χαρακτήρα κατά την έννοια της ως άνω διατάξεως (του άρθρου 2 στοιχ. α' της Οδηγίας 95/46) στον βαθμό που παρέχει τη δυνατότητα ταυτοποίησεως του συγκεκριμένου προσώπου.»¹²

Η Οδηγία (ΕΕ) 2016/680 (εφεξής «LED»)¹³ δεν απομακρύνεται από τον ορισμό που δόθηκε για τα βιομετρικά δεδομένα υπό το πρίσμα του ΓΚΠΔ. Συγκεκριμένα, στο άρθρο 3 παρ. 13,

⁹ Jain, A.K., Ross, A. και Prabhakar, S. (2004) 'An Introduction to Biometric Recognition', *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1), σσ. 4-20.

¹⁰ Άρθρο 4 (1) GDPR.

¹¹ Άρθρο 4 (14) GDPR.

¹² Υπόθεση C-212/2013, František Ryneš κατά Úřad pro ochranu osobních údajů.

¹³ Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης (2016) *Οδηγία (ΕΕ) 2016/680 της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων*

διευκρινίζει ότι πρόκειται για «δεδομένα προσωπικού χαρακτήρα τα οποία προκύπτουν από ειδική τεχνική επεξεργασία, συνδεδεμένη 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 δακτυλосκοπικά δεδομένα.» Η σύγκλιση αυτή των ορισμών διασφαλίζει ένα ενιαίο επίπεδο προστασίας, ανεξαρτήτως του εάν η επεξεργασία γίνεται για εμπορικούς σκοπούς ή για σκοπούς επιβολής του νόμου.

2.3 Λειτουργίες των βιομετρικών συστημάτων: Ταυτοποίηση και Επαλήθευση

Μετά την αποσαφήνιση του όρου «βιομετρία» και του ορισμού των «βιομετρικών δεδομένων», κρίνεται απαραίτητο να διακριθούν οι δύο βασικές λειτουργίες της βιομετρικής αναγνώρισης, ήτοι η ταυτοποίηση (identification) και η επαλήθευση (verification). Η επαλήθευση, η οποία ενσωματώνει και τη διαδικασία της αυθεντικοποίησης (authentication), διαφοροποιείται εννοιολογικά από την ταυτοποίηση, καθώς περιορίζεται στην επιβεβαίωση ότι ένα πρόσωπο είναι πράγματι αυτό που ισχυρίζεται ότι είναι. Ο σκοπός της είναι σαφώς οριοθετημένος και αφορά στην πιστοποίηση της ταυτότητας για την παροχή πρόσβασης σε υπηρεσίες, τον έλεγχο εισόδου σε εγκαταστάσεις ή το ξεκλείδωμα συσκευών. Η διάκριση αυτή είναι θεμελιώδης, καθώς καθορίζει τον τεχνικό σχεδιασμό του συστήματος και επηρεάζει άμεσα τη νομιμότητα της επεξεργασίας, η οποία συναρτάται -μεταξύ άλλων- και από τον τρόπο αποθήκευσης των βιομετρικών δεδομένων.

Η διαφορά μεταξύ επαλήθευσης και ταυτοποίησης είναι ότι η πρώτη απαντά στο ερώτημα «είμαι πραγματικά αυτός που ισχυρίζομαι ότι είμαι;». Το σύστημα πιστοποιεί την ταυτότητα του προσώπου προβαίνοντας στην επεξεργασία στοιχείων βιομετρίας που αναφέρονται στο πρόσωπο που υποβάλλει το ερώτημα και λαμβάνει μια απάντηση ναι/όχι! Συνεπώς, η λειτουργία αυτή βασίζεται στη σύγκριση δύο υποδειγμάτων (σύγκριση 1:1)¹⁴.

προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων. Διαθέσιμο στο: <https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32016L0680> (Πρόσβαση: Δεκέμβριο 2025).

¹⁴ J Sanchez del Rio and others, 'Automated Border Control E-Gates and Facial Recognition Systems' (2016) 62 Computers & Security 49, <https://www.sciencedirect.com/science/article/pii/S0167404816300736?via%3Dihub>.

Χαρακτηριστικό παράδειγμα αποτελεί η τεχνολογία «Face ID» των έξυπνων συσκευών. Στο πλαίσιο αυτό, το υποκείμενο συμμετέχει ενεργά και οικειοθελώς στη διαδικασία, η οποία χαρακτηρίζεται ως «συνεργατικό σενάριο».

Από την άλλη πλευρά, η ταυτοποίηση ενός προσώπου δίνει απάντηση στο ερώτημα «ποιος είμαι;». Σε αυτή την περίπτωση, το σύστημα αναγνωρίζει το πρόσωπο που υποβάλλει το ερώτημα, μέσω της σύγκρισης των βιομετρικών του δεδομένων με όλα τα δεδομένα που περιέχονται σε μια βάση δεδομένων. Τούτο συμβαίνει παρόλο που το υποκείμενο ενδέχεται να μην έχει παράσχει τη συγκατάθεσή του ή να μην έχει καν λάβει γνώση της διαδικασίας. Επομένως, αυτή η λειτουργία βασίζεται στη σύγκριση ενός υποδείγματος με άλλα υποδείγματα που είναι αποθηκευμένα σε μια βάση δεδομένων (βάση αναφοράς) ή σε «λίστες παρακολούθησης». Η ανωτέρω διαδικασία ονομάζεται ταυτοποίηση «ένα προς πολλά».^{15 16} Η μέθοδος αυτή εφαρμόζεται κυρίως σε εγκληματολογικές έρευνες ή σε συστήματα εξ αποστάσεως βιομετρικής ταυτοποίησης σε δημόσιους χώρους. Όταν η συλλογή των δεδομένων διενεργείται χωρίς την πρόθεση ή τη ρητή συγκατάθεση των ατόμων, το σενάριο ορίζεται ως «μη συνεργατικό».

Συμπερασματικά, γίνεται κατανοητό ότι -από τεχνική σκοπιά- η ταυτοποίηση παρουσιάζει σημαντικά μεγαλύτερη πολυπλοκότητα σε σύγκριση με την επαλήθευση, λόγω του τεράστιου όγκου δεδομένων προς επεξεργασία. Ως εκ τούτου, τα συστήματα αυτά συχνά δεν επιστρέφουν μια μοναδική, αδιαμφισβήτητη ταυτότητα, αλλά μια ιεραρχημένη λίστα πιθανών αποτελεσμάτων, συνοδευόμενη από έναν δείκτη πιθανότητας αντιστοίχισης (match score). Αξίζει να σημειωθεί ότι η διαδικασία της ταυτοποίησης δεν συνεπάγεται υποχρεωτικά την ονομαστική ταυτοποίηση του ατόμου¹⁷.

¹⁵ ΕΣΠΑ (2022) Κατευθυντήριες γραμμές 05/2022 σχετικά με τη χρήση της τεχνολογίας αναγνώρισης προσώπου στον τομέα της επιβολής του νόμου. Έκδοση 2.0. Διαθέσιμο στο: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052022-use-facial-recognition-technology-area-law_el (Πρόσβαση: Φεβρουάριος 2026).

¹⁶ Έγγραφο εργασίας WP80/2003 σχετικά με τα στοιχεία βιομετρίας της Ομάδας Εργασίας του άρθρου 29, διαθέσιμο σε: http://efaidnbmninnbpcajpcglclefindmkaj/https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_el.pdf.

¹⁷ Greens/EFA (n.d.) Biometric surveillance. Διαθέσιμο στο: <https://www.greens-efa.eu/biometricsurveillance/> (Πρόσβαση: Φεβρουάριος 2026).

Η εν λόγω διάκριση μεταξύ ταυτοποίησης και επαλήθευσης επισημάνθηκε και στην Πράξη για την Τεχνητή Νοημοσύνη, η οποία στην αιτιολογική σκέψη 17 εξαίρεσε από το πεδίο εφαρμογής του Κανονισμού τα συστήματα ΤΝ που προορίζονται για βιομετρική εξακρίβωση, συμπεριλαμβανομένης της επαλήθευσης της ταυτότητας. Η εν λόγω εξαίρεση ερείδεται στην παραδοχή ότι τέτοια συστήματα επιφέρουν σαφώς ηπιότερο αντίκτυπο στα θεμελιώδη δικαιώματα συγκριτικά με τα συστήματα εξ αποστάσεως βιομετρικής ταυτοποίησης, τα οποία επεξεργάζονται μαζικά δεδομένα χωρίς την ενεργό συμμετοχή των υποκειμένων (πολλές φορές ακόμα και χωρίς γνώση αυτών). Έτσι, ενώ τα συστήματα εξ αποστάσεως βιομετρικής ταυτοποίησης μπορούν να σαρώσουν πλήθος εικόνες ατόμων εν αγνοία τους, τα συστήματα βιομετρικής εξακρίβωσης προϋποθέτουν για την λειτουργία τους τη συμμετοχή του ατόμου και εξυπηρετούν έναν συγκεκριμένο και πολύ περιορισμένο σκοπό, γεγονός που τα καθιστά λιγότερο παρεμβατικά για τις ατομικές ελευθερίες.

3 ΣΥΣΤΗΜΑΤΑ ΑΝΑΓΝΩΡΙΣΗΣ ΠΡΟΣΩΠΟΥ

3.1 Έννοια

Έχοντας αναλύσει τους όρους «βιομετρικά δεδομένα» και «βιομετρία» με τις διαφορετικές λειτουργίες και χρήσεις τους, στο παρόν κεφάλαιο θα αναλυθούν τα Συστήματα εξ Αποστάσεως Βιομετρικής Ταυτοποίησης (RBI) και, πιο συγκεκριμένα, η τεχνική της αναγνώρισης προσώπου σε δημόσιους χώρους για σκοπούς επιβολής του νόμου, η οποία αποτελεί και το κύριο αντικείμενο της παρούσας μελέτης.

Η αναγνώριση προσώπου έχει καταστεί μία από τις πλέον διαδεδομένες βιομετρικές μεθόδους που χρησιμοποιούνται σήμερα, αντανakλώντας σε μεγάλο βαθμό τον τρόπο με τον οποίο οι ίδιοι οι άνθρωποι αναγνωρίζουν ο ένας τον άλλον. Η διαδικασία αυτή εξελίσσεται σε δύο στάδια: αρχικά στη συλλογή της εικόνας και τη μετατροπή της σε ένα ψηφιακό «βιομετρικό υπόδειγμα» και ακολούθως στην αναγνώριση μέσω της σύγκρισης αυτού του υποδείγματος με άλλα που βρίσκονται ήδη αρχειοθετημένα. Ως βιομετρικό υπόδειγμα ορίζεται η ψηφιακή αναπαράσταση των μοναδικών χαρακτηριστικών του ατόμου που έχουν εξαχθεί από ένα βιομετρικό δείγμα, το οποίο μπορεί να αποθηκευτεί σε μια βιομετρική βάση δεδομένων. Το εν λόγω υπόδειγμα θεωρείται μοναδικό για κάθε άτομο και παραμένει, κατ' αρχήν, αναλλοίωτο με την πάροδο του χρόνου.¹⁸

Αν και δεν υπάρχει ένας κοινά αποδεκτός ορισμός για το τι συνιστά σύστημα αναγνώρισης προσώπου, η Ομάδα Εργασίας του Άρθρου 29 για την Προστασία των Δεδομένων όρισε την αναγνώριση προσώπου ως την «αυτόματη επεξεργασία ψηφιακών εικόνων που περιέχουν πρόσωπα ατόμων με σκοπό την ταυτοποίηση, την αυθεντικοποίηση/επαλήθευση ή την κατηγοριοποίηση των εν λόγω ατόμων»¹⁹, ενώ η Πράξη για την Τεχνητή Νοημοσύνη διατυπώνει έναν ορισμό για το σύστημα εξ αποστάσεως βιομετρικής ταυτοποίησης στο άρθρο 3 παρ. 41 που μπορεί να επεκταθεί και στην εν λόγω τεχνολογία. Ειδικότερα, ως

¹⁸ Ο.π. υποσημείωση 15

¹⁹ Ομάδα Εργασίας του Άρθρου 29 (2012) Γνωμοδότηση 02/2012 σχετικά με την αναγνώριση προσώπου στις διαδικτυακές υπηρεσίες και στις υπηρεσίες κινητής τηλεφωνίας (WP 192). 22 Μαρτίου. Διαθέσιμο στο: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_el.pdf (Πρόσβαση: Δεκέμβριος 2025).

«σύστημα εξ αποστάσεως βιομετρικής ταυτοποίησης» ορίζεται «το σύστημα τεχνητής νοημοσύνης για την ταυτοποίηση φυσικών προσώπων χωρίς την ενεργό συμμετοχή τους κατά κανόνα εξ αποστάσεως μέσω της αντιπαραβολής των βιομετρικών δεδομένων ενός προσώπου με τα βιομετρικά δεδομένα που περιέρχονται σε βάση δεδομένων αναφοράς». Συνεπώς, από τα ανωτέρω μπορεί να εξαχθεί ευκρινώς το συμπέρασμα ότι πρόκειται για σύστημα ΤΝ, το οποίο καθιστά δυνατή την ταυτοποίηση/επαλήθευση/κατηγοριοποίηση ατόμων μέσω των βιομετρικών τους πληροφοριών, και στη συγκεκριμένη περίπτωση μέσω του προσώπου τους, χρησιμοποιώντας τεχνικές Βαθιάς Μάθησης.

Η αναγνώριση προσώπου αποτελεί μέρος ενός ευρύτερου φάσματος τεχνικών επεξεργασίας εικόνας ή/και βίντεο. Ορισμένες βιντεοκάμερες μπορούν να βιντεοσκοπήσουν τα πρόσωπα ανθρώπων που ευρίσκονται σε μία συγκεκριμένη τοποθεσία, αλλά δεν μπορούν να χρησιμοποιηθούν για την αυτόματη αναγνώριση ατόμων. Συνεπώς, για να μιλούμε για σύστημα αναγνώρισης προσώπου πρέπει να υπάρχει λειτουργικότητα λογισμικού που μπορεί να εφαρμοστεί στο πλαίσιο υφιστάμενων συστημάτων (κάμερες, βάσεις δεδομένων εικόνων κ.λπ.) και να διασυνδεθεί με άλλα συστήματα.²⁰ Εάν, αντιθέτως, μέσω του συστήματος δεν γίνεται συλλογή δεδομένων εικόνας ή ήχου ταυτοποιήσιμων φυσικών προσώπων δεν θα πρόκειται μετά βεβαιότητας για επεξεργασία δεδομένων προσωπικού χαρακτήρα.²¹

Η εκτεταμένη χρήση της αναγνώρισης προσώπου αποδίδεται σε ένα σύνολο αλληλένδετων τεχνικών και επιχειρησιακών παραγόντων. Η δυνατότητα εξ αποστάσεως ταυτοποίησης προσώπων αναμφισβήτητα αποτελεί μια λιγότερο παρεμβατική βιομετρική μέθοδο σε σύγκριση με άλλες βιομετρικές μεθόδους, όπως η σάρωση της ίριδας και τα δακτυλικά αποτυπώματα που επιτρέπουν ομοίως την αναγνώριση ενός ατόμου μέσω της ψηφιακής του απεικόνισης²². Και αυτό διότι η τεχνολογία αναγνώρισης προσώπου αναπτύσσεται με τη

²⁰ Ο.π. υποσημείωση 15

²¹ ΕΣΠΑ (2019) *Κατευθυντήριες γραμμές 3/2019 σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω βιντεοσυσκευών*. Έκδοση 2.0. Διαθέσιμο στο: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video-devices_el (Πρόσβαση: Φεβρουάριος 2026).

²² Bennett, K. A. (2001) 'Can Facial Recognition Technology Be Used to Fight the New Way against Terrorism: Examining the Constitutionality of Facial Recognition Surveillance Systems', *North Carolina Journal of Law & Technology*, 3(1), σσ. 151–178.

συλλογή εκατομμυρίων εικόνων είτε από κάμερες εγκατεστημένες σε δημόσιους χώρους ("CCTV") είτε από μέσα κοινωνικής δικτύωσης, άδειες οδήγησης κ.λπ., χωρίς να προαπαιτείται η συγκατάθεση των υποκειμένων των δεδομένων, αλλά ούτε και η φυσική αλληλεπίδραση με αυτά. Παράλληλα, το χαμηλό κόστος του απαιτούμενου εξοπλισμού (κάμερες) καθιστά την τεχνολογία οικονομικά προσιτή και εφαρμόσιμη σε ποικίλα περιβάλλοντα. Επιπροσθέτως, η αναγνώριση προσώπου χαρακτηρίζεται από υψηλή λειτουργική ευελιξία, καθώς δύναται να ενσωματωθεί άμεσα σε υφιστάμενες υποδομές επιτήρησης. Το γεγονός αυτό, σε συνδυασμό με την αξιοποίηση εκτεταμένων βάσεων δεδομένων (π.χ. αρχεία διαβατηρίων, ταυτοτήτων και αδειών οδήγησης), διευκολύνει την ενσωμάτωσή της σε διοικητικά, κρατικά και επιχειρησιακά πλαίσια. Ως εκ τούτου, η αναγνώριση προσώπου αναδεικνύεται ως η πλέον προσβάσιμη και λειτουργικά απλή βιομετρική τεχνολογία.

Στο σημείο αυτό, αξίζει να αναφερθεί ότι τα συστήματα βιντεοεπιτήρησης συλλέγουν συνήθως τεράστιο όγκο προσωπικών δεδομένων τα οποία ενδέχεται να αποκαλύψουν δεδομένα πολύ προσωπικής φύσης, ακόμη και ειδικών κατηγοριών δεδομένα. Ενδέχεται δηλαδή μη σημαντικά δεδομένα, που συλλέγονται αρχικά μέσω βίντεο, να χρησιμοποιηθούν για την εξαγωγή άλλων πληροφοριών για την επίτευξη διαφορετικού σκοπού (π.χ. για την χαρτογράφηση των συνηθειών ενός ατόμου). Ωστόσο, δεν πρέπει να θεωρείται ότι η βιντεοεπιτήρηση ισοδυναμεί πάντα με επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα. Σύμφωνα με τη γνώμη 3/2012 «προκειμένου να εκτιμηθεί η ευαισθησία των δεδομένων που επεξεργάζεται ένα βιομετρικό σύστημα πρέπει να λαμβάνεται επίσης υπόψη το πλαίσιο της επεξεργασίας [...], ενώ το κατά πόσο μια επεξεργασία περιέχει ευαίσθητα στοιχεία αξιολογείται με βάση τα ειδικά βιομετρικά χαρακτηριστικά που χρησιμοποιούνται σε αυτή τη βιομετρική εφαρμογή»²³. Συνεπώς, η εκτίμηση της ευαισθησίας των δεδομένων προϋποθέτει αξιολόγηση "in concreto", καθώς μόνο μέσω της συνεκτίμησης του συγκεκριμένου πλαισίου επεξεργασίας και των χρησιμοποιούμενων βιομετρικών χαρακτηριστικών μπορεί να αποτυπωθεί ο πραγματικός βαθμός κινδύνου για τα δικαιώματα των υποκειμένων.

²³ Γνώμη 3/2012 σχετικά με τις εξελίξεις στις βιομετρικές τεχνολογίες (WP 193), διαθέσιμη σε: http://efaidnbmnnnibpcajpcglclefindmkaj/https://ec.europa.eu/justice/article29/documentation/opinion-recommendation/files/2009/wp163_el.pdf [Πρόσβαση 6/2025]

Παρόλο που η εφαρμογή των βιομετρικών συστημάτων προοριζόταν αρχικώς για κρατική χρήση προκειμένου να εντοπιστούν και να επιλυθούν ζητήματα δημόσιας ασφάλειας, επιβολής του νόμου ή ελέγχου των συνόρων, εντούτοις τα τελευταία χρόνια παρατηρείται ραγδαία αύξηση της χρήσης βιομετρικών τεχνολογιών και από ιδιωτικούς φορείς για την επίτευξη σκοπών, που συνίστανται, κυρίως, στην ταυτοποίηση των χρηστών διαδικτυακών εφαρμογών, καθώς και στον έλεγχο της πρόσβασης των εργαζομένων στο χώρο εργασίας τους. Κύριοι τομείς εφαρμογής επίσης αποτελούν το ηλεκτρονικό εμπόριο, ο τραπεζικός κλάδος και οι υπηρεσίες υγείας.²⁴ Ένας από τους βασικούς παράγοντες που οδήγησαν στην ανωτέρω μετατόπιση είναι η ωρίμανση της τεχνολογίας, σε τέτοιο βαθμό ώστε τα βιομετρικά συστήματα, τα οποία παλαιότερα λειτουργούσαν ικανοποιητικά μόνο υπό ελεγχόμενες συνθήκες, να έχουν σημειώσει τόσο αξιοσημείωτη βελτίωση που να είναι πλέον κατάλληλα για εκτεταμένη χρήση σε ένα ευρύ φάσμα διαφορετικών περιβαλλόντων. Μολονότι τα συστήματα αναγνώρισης προσώπου τυγχάνουν ευρείας εφαρμογής τόσο στον ιδιωτικό όσο και στον δημόσιο τομέα, η παρούσα μελέτη εστιάζει αποκλειστικά στη χρήση τους από τις αρχές επιβολής του νόμου με σκοπό την προάσπιση της δημόσιας ασφάλειας. Ειδικότερα, σημείο αναφοράς αποτελούν οι μη ελεγχόμενοι χώροι, όπως δρόμοι, πλατείες κ.λπ., καθώς σε αυτούς οι μηχανισμοί είναι πιθανό να ταυτοποιήσουν έναν απροσδιόριστο αριθμό ατόμων, οδηγώντας σε καταστάσεις μαζικής επιτήρησης. Λόγω ακριβώς αυτής της δυνατότητας μαζικής εξαγωγής δεδομένων από μια απλή εικόνα, σε συνδυασμό με τη λήψη της (εικόνας) εξ αποστάσεως και εν αγνοία του υποκειμένου, καταδεικνύεται η παρεμβατικότητα των σύγχρονων μεθόδων επεξεργασίας στην ιδιωτική ζωή και αναδύονται σοβαροί κίνδυνοι για την ιδιωτικότητα και τα προσωπικά δεδομένα που σχετίζονται άμεσα με την λειτουργία αυτών των τεχνολογιών.

3.2 Τρόπος Λειτουργίας

Όπως προαναφέρθηκε, η εν λόγω τεχνολογία μπορεί να χρησιμοποιηθεί είτε για την ταυτοποίηση είτε για την επαλήθευση ενός ατόμου μέσω των χαρακτηριστικών του προσώπου, το οποίο αποτελεί το κατεξοχήν προσωπικό δεδομένο, καθώς είναι ιδιαίτερα

²⁴ Λαζαράκος, Γ. (2016) «Τα συνταγματικά όρια της επεξεργασίας βιομετρικών δεδομένων (Κεφάλαιο 11ο)», στο Κοτσαλής, Λ. και Λαζαράκος, Γ. (επιμ.) *Προσωπικά Δεδομένα*. Αθήνα: Νομική Βιβλιοθήκη.

ορατό και εύκολο να αναγνωριστεί, είτε στον φυσικό είτε στον ψηφιακό χώρο. Ωστόσο, οι τεχνολογίες αναγνώρισης προσώπου μπορούν να χρησιμοποιηθούν και για σκοπούς πέραν της βιομετρικής αναγνώρισης, όπως για βιομετρική κατηγοριοποίηση (που συνδέεται, για παράδειγμα, με την ταξινόμηση φύλου ή την εκτίμηση ηλικίας) ή για ανίχνευση συναισθημάτων. Επιπλέον, οι εξελίξεις στις υπολογιστικές τεχνολογίες και στα δίκτυα οδηγούν στην ανάδυση αυτού που θεωρείται η δεύτερη γενιά βιομετρικών συστημάτων, τα οποία βασίζονται στη χρήση συμπεριφορικών και ψυχολογικών χαρακτηριστικών, είτε μεμονωμένα είτε σε συνδυασμό με άλλα κλασικά συστήματα, σχηματίζοντας πολυτροπικά συστήματα²⁵.

Η διαδικασία περιλαμβάνει συνήθως τα ακόλουθα τέσσερα στάδια:^{26 27}

Το αρχικό στάδιο της διαδικασίας είναι η **ανίχνευση προσώπου ("face detection")**, μια υπολογιστική τεχνική που αποσκοπεί στον αυτόματο εντοπισμό και την απομόνωση του ανθρώπινου προσώπου από το υπόλοιπο περιβάλλον, όπως το φόντο ή άλλα αντικείμενα. Μέσω του προσδιορισμού συγκεκριμένων γεωμετρικών σημείων αναφοράς, το σύστημα υπολογίζει τις διαστάσεις, τις αποστάσεις των χαρακτηριστικών και τον προσανατολισμό του προσώπου, παρέχοντας τις ακριβείς συντεταγμένες του μέσα σε ένα πλαίσιο οριοθέτησης. Παρά την αποτελεσματικότητά της, η μέθοδος έρχεται αντιμέτωπη με σημαντικές προκλήσεις που αφορούν τη μεταβλητότητα των συνθηκών φωτισμού, την ανάλυση της εικόνας και τη στάση του σώματος. Ιδιαίτερη δυσκολία παρουσιάζεται στις περιπτώσεις μερικής απόκρυψης των χαρακτηριστικών, γεγονός που αποτελεί εγγενή περιορισμό στην αξιοπιστία της ανίχνευσης.

Το επόμενο στάδιο είναι η **ευθυγράμμιση προσώπου (face alignment)**. Αφού ανιχνεύσει το πρόσωπο, το σύστημα ευθυγραμμίζει τα χαρακτηριστικά του προσώπου, όπως τα μάτια, τη μύτη και το στόμα, σε μια τυπική μορφή. Αυτή η διαδικασία κανονικοποίησης διασφαλίζει

²⁵ Ομάδα Εργασίας του Άρθρου 29 (2012) Γνωμοδότηση 3/2012 σχετικά με τις εξελίξεις στις βιομετρικές τεχνολογίες (WP193). ²⁷ Απριλίου. Διαθέσιμο στο: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_el.pdf (Πρόσβαση: Ιανουάριος 2026).

²⁶ Guo, Z. and Kennedy, L. (2023) 'Policing based on facial recognition', *Artificial Intelligence and Law*, 31(4), σσ. 741–769. Διαθέσιμο στο: <https://link.springer.com/article/10.1007/s10506-022-09330-x> (Πρόσβαση: Ιανουάριος 2026).

²⁷ Sáez Trigueros, D. and Meng, L. (2018) 'Face Recognition: From Traditional to Deep Learning Methods', <https://arxiv.org/abs/1811.00116> (Πρόσβαση: Ιανουάριος 2026).

ότι η FRT μπορεί να λειτουργήσει με ακρίβεια ακόμα κι αν το πρόσωπο προβάλλεται από διαφορετικές γωνίες ή υπό διαφορετικές συνθήκες φωτισμού.

Το τρίτο στάδιο σχετίζεται με την **εξαγωγή χαρακτηριστικών προσώπου (facial feature extraction)**. Κατά τη διαδικασία αυτή, απομονώνονται συγκεκριμένα χαρακτηριστικά του προσώπου και πραγματοποιείται μέτρηση αποστάσεων και αναλογιών μεταξύ χαρακτηριστικών σημείων του προσώπου (π.χ. η απόσταση μεταξύ των ματιών ή το σχήμα της μύτης) με αναφορά σε μια λίστα που περιλαμβάνει αριθμητικές αναπαραστάσεις των χαρακτηριστικών αυτών. Αυτά τα χαρακτηριστικά μετατρέπονται σε ένα βιομετρικό πρότυπο, μια αριθμητική αναπαράσταση που ταυτοποιεί μοναδικά το άτομο. Το στάδιο αυτό είναι καθοριστικής σημασίας για την αναγνώριση προσώπου και, από την ανάπτυξη της βαθιάς μάθησης και έπειτα, έχει βελτιωθεί σημαντικά.

Το τέταρτο και τελευταίο στάδιο αφορά στην **αντιστοίχιση χαρακτηριστικών (face matching)** και στην **ταυτοποίηση** (ή στην **επαλήθευση**) του ατόμου. Το σύστημα συγκρίνει το βιομετρικό πρότυπο με αυτά που είναι ήδη αποθηκευμένα σε μια βάση δεδομένων (π.χ. λίστες παρακολούθησης, βάσεις δεδομένων ταυτοτήτων) για να βρει μια αντιστοιχία. Σε ορισμένες περιπτώσεις, αυτό το βήμα περιλαμβάνει τη σύγκριση του προσώπου εισόδου με χιλιάδες ή εκατομμύρια άλλα πρόσωπα για τον προσδιορισμό της ταυτότητας του ατόμου. Σε άλλες περιπτώσεις, το σύστημα απλώς επαληθεύει ότι το πρόσωπο εισόδου αντιστοιχεί σε ένα συγκεκριμένο άτομο στη βάση δεδομένων.

Η τεχνητή νοημοσύνη μπορεί να επεξεργαστεί τεράστιο όγκο δεδομένων, που περιλαμβάνει εκατομμύρια εικόνες, και να εντοπίσει πιθανές αντιστοιχίσεις μέσα σε λίγα δευτερόλεπτα²⁸. Το αποτέλεσμα της αντιστοίχισης εκφράζεται ως ποσοστό ομοιότητας. Σε μια κλίμακα τιμών από «0» έως «1», το «0» αντιστοιχεί στη χαμηλότερη ομοιότητα, ενώ το «1» υποδηλώνει τη μέγιστη ομοιότητα. Η ομοιότητα αποτελεί ένα είδος πιθανότητας ή πρόβλεψης και όχι ένα βέβαιο γεγονός²⁹. Ανάλογα με το αν το ποσοστό ομοιότητας βρίσκεται πάνω ή κάτω από

²⁸ Ammanath, B. (2022) *Trustworthy AI: A Business Guide for Navigating Trust and Ethics in AI*. Hoboken, New Jersey: John Wiley & Sons.

²⁹ Partnership on AI (2020) *Understanding Facial Recognition Systems*. Διαθέσιμο στο: <https://partnershiponai.org/paper/understanding-facial-recognition-systems/> (Πρόσβαση: Φεβρουάριος 2026).

το προκαθορισμένο όριο, εξάγεται συμπέρασμα ως προς το αν πρόκειται για το ίδιο ή για διαφορετικό άτομο.

Λόγω της πιθανοκρατικής της φύσης, η τεχνολογία αναγνώρισης προσώπου δεν παρέχει απόλυτα αποτελέσματα, αλλά αποδίδει ποσοστά πιθανότητας σχετικά με την ομοιότητα ή μη των προσώπων. Η ακρίβεια και αποτελεσματικότητα της FRT συνδέεται αναπόφευκτα με την ακρίβεια της χρησιμοποιούμενης τεχνολογίας, αλλά και με τα δεδομένα εκπαίδευσης. Δεδομένου ότι ακόμη και με τις πλέον προηγμένες τεχνολογίες αναγνώρισης προσώπου κανείς δεν μπορεί να εγγυηθεί ακρίβεια σε ποσοστό 100%, η χρήση της ενδέχεται να οδηγήσει σε ψευδώς θετικά αποτελέσματα (όταν ένα πρόσωπο αντιστοιχίζεται λανθασμένα με κάποιο άλλο) ή σε ψευδώς αρνητικά αποτελέσματα (όταν ένα πρόσωπο λανθασμένα δεν αναγνωρίζεται ως αντιστοιχία)³⁰. Οι πλέον διαδεδομένοι αλγόριθμοι αναγνώρισης προσώπου εκτιμάται ότι επιτυγχάνουν ποσοστά ακρίβειας της τάξεως του 90%.

3.3 Ιστορική Αναδρομή

Το πρόσωπό μας αποτελεί το βασικό σημείο εστίασης της προσοχής κατά την κοινωνική αλληλεπίδραση και παίζει καθοριστικό ρόλο στη μετάδοση της ταυτότητας και του συναισθήματος. Μέσω του ανθρώπινου προσώπου αντλούνται πολλαπλές πληροφορίες, όπως η ταυτότητα, το φύλο, η φυλή ή η εθνοτική καταγωγή, η ηλικία, η συναισθηματική κατάσταση, αλλά και η κοινωνική κατάσταση ενός ατόμου³¹. Μπορούμε να αναγνωρίζουμε χιλιάδες πρόσωπα που έχουμε μάθει σε όλη τη διάρκεια της ζωής μας και να ταυτοποιούμε γνώριμα πρόσωπα με μια ματιά ακόμα και μετά από χρόνια απουσίας. Αυτή η ικανότητα είναι ιδιαίτερα ανθεκτική, παρά τις μεγάλες αλλαγές στο οπτικό ερέθισμα που οφείλονται στις συνθήκες θέασης, στις εκφράσεις, στη γήρανση και σε παράγοντες όπως η χρήση γυαλιών και οι αλλαγές την εμφάνιση.

³⁰ Adler, A. and Schuckers, M. E. (2007) 'Comparing Human and Automatic Face Recognition Performance', *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, 37(5), σσ. 1248–1255. Διαθέσιμο σε: <https://sci2s.ugr.es/keel/pdf/specific/articulo/Comparing%20Human%20and%20Automatic%20Face%20Recognition%20Performance.pdf> (Πρόσβαση: Φεβρουάριος 2026).

³¹ Oosterhof, N. N. and Todorov, A. (2008) 'The functional basis of face evaluation', *Proceedings of the National Academy of Sciences (PNAS)*, 105(32), σσ. 11087–11092. Διαθέσιμο στο: <https://pubmed.ncbi.nlm.nih.gov/18685089/> (Πρόσβαση: Δεκέμβριος 2025).

Η συστηματική διερεύνηση των εκφράσεων του προσώπου και της φυσιογνωμικής ανάγεται στην αρχαιότητα, με χαρακτηριστικές αναφορές ήδη από τον 4ο αιώνα π.Χ με το φιλοσοφικό έργο του Αριστοτέλη.³² Ως φυσιογνωμική ορίζεται η μέθοδος που επιδιώκει να συναγάγει τα πάθη, τις διαθέσεις και τον χαρακτήρα της ψυχής από τα σωματικά γνωρίσματα, ιδίως από τη μορφή του προσώπου, τη στάση του σώματος και τις κινήσεις. Με το πέρασμα του χρόνου το ενδιαφέρον για την φυσιογνωμική ελαττώθηκε, καθώς δεν ανταποκρινόταν στις επιταγές της επιστήμης, αλλά τουναντίον βασιζόταν σε πιθανολογικές μεθόδους, υποκείμενες σε σφάλματα όπου απαιτούνταν η συνεκτίμηση πολλών παραγόντων πριν την εξαγωγή οποιουδήποτε συμπεράσματος.

3.3.1 Τα Πρώτα Αυτοματοποιημένα Συστήματα (1970–1990)

Παρότι οι άνθρωποι χρησιμοποιούν τα πρόσωπα για να αναγνωρίζουν ο ένας τον άλλον από αμνημονεύτων χρόνων,³³ η προσπάθεια να καταστούν οι υπολογιστές ικανοί να αναγνωρίζουν ανθρώπινα πρόσωπα μιμούμενοι την ανθρώπινη σκέψη ξεκίνησε στα μέσα της δεκαετίας του 1960 από τον Woodrow W. Bledsoe και τους συνεργάτες του (Helen Chan και Charles Bisson) στο Panoramic Research Institute. Το συγκεκριμένο εγχείρημα χαρακτηρίστηκε ως σύστημα «άνθρωπος-μηχανή» (man-machine), καθώς βασιζόταν στη χειροκίνητη εξαγωγή των συντεταγμένων ενός συνόλου χαρακτηριστικών, τα οποία εν συνεχεία τροφοδοτούνταν στον υπολογιστή για τη διαδικασία της αναγνώρισης. Ειδικότερα, μέσω της χρήσης μιας ταμπλέτας γραφικών (τύπου GRAFACON ή RAND tablet), ο χειριστής κατέγραφε τις συντεταγμένες συγκεκριμένων ανατομικών οροσίων, όπως το κέντρο της κόρης των οφθαλμών, η εσωτερική και εξωτερική γωνία των ματιών και η κορυφή του μετώπου. Βάσει αυτών των συντεταγμένων, το σύστημα υπολόγιζε έναν κατάλογο 20 διακριτών αποστάσεων, όπως το πλάτος του στόματος και των ματιών, με τους χειριστές να δύνανται να επεξεργαστούν περίπου 40 φωτογραφίες ανά ώρα. Κατά τη φάση δημιουργίας

³² Φυσιογνωμικά: Το έργο αυτό προσπαθεί να συσχετίσει τις εκφράσεις του προσώπου με τα στατικά χαρακτηριστικά του προσώπου και του σώματος, ώστε να μπορέσει να προβλέψει και να ορίσει τα στοιχεία του χαρακτήρα του ατόμου που μελετά (Λιγκοβανλή, 2008).

³³ A.K. Jain, K. Nandakumar, and A. Ross, 2016, "50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities," Pattern Recognition Letters 79(3.2):80–105, <https://doi.org/10.1016/j.patrec.2015.12.013>

της βάσης δεδομένων, το ονοματεπώνυμο του εικονιζόμενου προσώπου συσχετιζόταν με την αποθηκευμένη λίστα των υπολογισμένων αποστάσεων. Τέλος, κατά το στάδιο της αναγνώρισης, το σύνολο των αποστάσεων της εξεταζόμενης εικόνας συγκρινόταν με τα αντίστοιχα αποθηκευμένα δεδομένα και το σύστημα επέστρεφε ως ταυτοποιήσεις τα αποτελέσματα με τη μικρότερη απόκλιση.³⁴

Ο Bledsoe παρατήρησε ότι «η αναγνώριση προσώπου δυσχεραίνεται από τη μεγάλη μεταβλητότητα στην περιστροφή και την κλίση του κεφαλιού, την ένταση και τη γωνία του φωτισμού, την έκφραση του προσώπου, τη γήρανση κ.λπ. Ορισμένες άλλες προσπάθειες αναγνώρισης προσώπου από μηχανές έχουν επιτρέψει ελάχιστη ή καθόλου μεταβλητότητα σε αυτές τις ποσότητες. Ωστόσο, η μέθοδος συσχέτισης (ή αντιστοίχισης προτύπων) μη επεξεργασμένων οπτικών δεδομένων, η οποία χρησιμοποιείται συχνά από ορισμένους ερευνητές, είναι βέβαιο ότι θα αποτύχει σε περιπτώσεις όπου η μεταβλητότητα είναι μεγάλη. Συγκεκριμένα, η συσχέτιση είναι πολύ χαμηλή μεταξύ δύο εικόνων του ίδιου ατόμου με δύο διαφορετικές περιστροφές κεφαλής»³⁵

Το γεγονός ότι τα συστήματα αυτά βασίζονταν σε μεγάλο βαθμό στον χειροκίνητο εντοπισμό σημείων αναφοράς, περιορίσε γρήγορα την χρηστικότητά τους. Στη συνέχεια, αναπτύχθηκαν πολλές άλλες έρευνες προς αυτή την κατεύθυνση, ωστόσο δεν θα αναφερθούμε σε όλες, καθώς το έργο αυτό υπερβαίνει κατά πολύ το πεδίο της παρούσας ανάλυσης. Για τον λόγο αυτό, θα εστιάσουμε μόνο σε εκείνες που, κατά τη γνώμη μας, αντιπροσώπευσαν σημαντική πρόοδο στην εξέλιξη των συστημάτων μέχρι τη σημερινή κατάσταση. Έτσι, το έτος 1973 σημειώθηκε μια σημαντική τομή με την ανάπτυξη του πρώτου πλήρως αυτοματοποιημένου συστήματος αναγνώρισης προσώπου από τον Takeo Kanade στο πλαίσιο της διδακτορικής του διατριβής στο Πανεπιστήμιο του Κιότο.³⁶ Αντίθετα με το έργο του Bledsoe «άνθρωπος – μηχανή» όπου ο εντοπισμός των ανθρώπινων

³⁴ Petrescu, Rely Victoria, Face Recognition as a Biometric Application (April 13, 2019). Journal of Mechatronics and Robotics 2019, Volume 3: 237.257, Available at SSRN: <https://ssrn.com/abstract=3417325> or <http://dx.doi.org/10.2139/ssrn.3417325>

³⁵ W.W. Bledsoe, 1966, Man-Machine Facial Recognition: Report on a Large-Scale Experiment, Technical Report PRI 22, Panoramic Research, Inc., Palo Alto, California

³⁶ T. Kanade, "Picture processing system by computer complex and recognition of human faces," Kyoto University, Tech. Rep., 1974. Available online: <https://repository.kulib.kyoto>

χαρακτηριστικών προϋπέθετε χειροκίνητη ενέργεια, ο Takeo Kanade ανέπτυξε μεθόδους αυτόματου εντοπισμού χαρακτηριστικών του προσώπου, αξιοποιώντας μια στρατηγική ελέγχου από πάνω προς τα κάτω (top-down control). Το σύστημα του Kanade υπολόγιζε ένα σύνολο παραμέτρων του προσώπου από μία εικόνα και χρησιμοποιούσε τεχνικές ταξινόμησης προτύπων για την αντιστοίχιση της εικόνας με ένα σύνολο αναφοράς. Η προσέγγιση αυτή ήταν καθαρά στατιστική και βασισμένη κυρίως σε ανάλυση φωτεινότητας και τιμών γκρι. Επιπλέον, κατάφερε να αντιμετωπίσει για πρώτη φορά συστηματικά τη μεταβλητότητα που οφειλόταν σε παράγοντες όπως η στάση της κεφαλής, ο φωτισμός και η έκφραση του προσώπου, εισάγοντας πιο ανθεκτικές τεχνικές επεξεργασίας εικόνας.³⁷ Παρότι το επίτευγμα του Kanade ήταν ριζοσπαστικό από τεχνολογικής άποψης για την εποχή του, εντούτοις δεν γνώρισε ευρεία υιοθέτηση.

3.3.2 Η μετάβαση από Γεωμετρικές μεθόδους σε Ολιστικές (1990–2000)

Η δεκαετία του 1990 σηματοδότησε μια πρωτοφανή μετατόπιση για τις τεχνολογίες αναγνώρισης προσώπου από τις άλλοτε βασισμένες στη γεωμετρία σε ολιστικές μεθόδους³⁸. Αναφέρονται ως ολιστικές καθώς χρησιμοποιούν ολόκληρη την περιοχή του προσώπου ως δεδομένο εισόδου. Σταθμό στην εξέλιξη της αναγνώρισης προσώπου αποτέλεσε η μέθοδος «Eigenfaces» («Ιδιοπρόσωπα») των Turk και Pentland, η οποία οδήγησε στις πρώτες περιπτώσεις αυτόματης αναγνώρισης προσώπου.³⁹ Συγκεκριμένα, αξιοποιώντας τη μέθοδο της Ανάλυσης Κύριων Συνιστωσών (PCA), το σύστημα δεν εστίαζε στην αναγνώριση μεμονωμένων χαρακτηριστικών, αλλά αντιμετώπιζε κάθε εικόνα προσώπου ως ένα ενιαίο σύνολο τιμών εικονοστοιχείων (pixels). Μέσω αυτής της «ολιστικής» προσέγγισης, τα πρόσωπα αναπαρίσταντο ως διανύσματα σε έναν χώρο υψηλών διαστάσεων, γεγονός που απλοποίησε τη διαδικασία παρακάμπτοντας την ανάγκη για λεπτομερή εξαγωγή

³⁷ T. Kanade, 1974, Picture Processing System by Computer Complex and Recognition of Human Faces, https://repository.kulib.kyoto-u.ac.jp/dspace/bitstream/2433/162079/2/D_Kanade_Takeo.pdf.

³⁸ National Academies of Sciences, Engineering, and Medicine. 2024. Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance. Washington, DC: The National Academies Press. <https://doi.org/10.17226/62>.

³⁹ M. Turk and A. Pentland, 1991, "Eigenfaces for Recognition," Journal of Cognitive Neuroscience 3(1):71–86, <https://doi.org/10.1162/jocn.1991.3.1.71>.

χαρακτηριστικών. Παρόλο που η εν λόγω μέθοδος παρουσίασε πλεονεκτήματα έναντι άλλων σχημάτων αναγνώρισης προσώπου ως προς την ταχύτητα και την απλότητά της, ωστόσο εμφάνισε περιορισμούς ανάλογα με τον φωτισμό και την έκφραση του προσώπου⁴⁰.

Για την αντιμετώπιση αυτού του ζητήματος, οι Belhumeur κ.ά. εισήγαγαν τα Fisherfaces, τα οποία εφαρμόζουν τη Γραμμική Διακριτική Ανάλυση (LDA) για τον καλύτερο διαχωρισμό των ατόμων σε έναν χώρο χαμηλής διάστασης, ο οποίος απομονώνει τις ουσιώδεις πληροφορίες και απορρίπτει περιττές λεπτομέρειες που δεν συμβάλλουν στο έργο της αναγνώρισης, βελτιώνοντας την ανθεκτικότητα του συστήματος π.χ. σε περιπτώσεις μεταβαλλόμενου φωτισμού⁴¹.

Με την πάροδο του χρόνου αναπτύχθηκαν και άλλες τεχνικές αναγνώρισης προσώπου που προϋπέθεταν ότι τα πρόσωπα μπορούν να ευθυγραμμιστούν και να κανονικοποιηθούν, τόσο γεωμετρικά όσο και φωτομετρικά. Η ευθυγράμμιση πραγματοποιείται συνήθως με βάση τη θέση των δύο ματιών στο πρόσωπο. Το σύστημα ανίχνευσης προσώπων που αναπτύχθηκε από τους Viola και Jones αποτέλεσε ορόσημο, καθώς επέτρεψε την ανίχνευση προσώπων σε πραγματικό χρόνο ακόμη και παρουσία «θορύβου» στο φόντο, μια κατάσταση που συναντάται συχνά σε εφαρμογές επιτήρησης.⁴² Παρότι ο ανιχνευτής Viola-Jones αποδίδει πολύ καλά σε εφαρμογές πραγματικού χρόνου, εξακολούθησε να αντιμετωπίζει δυσκολίες σε μεταβολές φωτισμού, σε μη μετωπικές στάσεις του προσώπου και σε περιπτώσεις απόκρυψης των χαρακτηριστικών του προσώπου από έτερα αντικείμενα και ως εκ τούτου γρήγορα θεωρήθηκε παρωχημένος.⁴³

3.3.3 Η συμβολή της βαθιάς μάθησης (Deep Learning) στην αναγνώριση προσώπου

Στο σύγχρονο επιστημονικό πλαίσιο, η σχέση μεταξύ της Τεχνητής Νοημοσύνης, της Μηχανικής Μάθησης (Machine Learning) και της Βαθιάς Μάθησης (Deep Learning)

⁴⁰ <https://www.face-rec.org/interesting-papers/General/Random.pdf>

⁴¹ P.N. Belhumeur, J.P. Hespanha, and D.J. Kriegman, 1997, "Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection," IEEE Transactions on Pattern Analysis and Machine Intelligence 19(7):711-720.

⁴² P. Viola and M.J. Jones, 2004, "Robust Real-Time Face Detection," International Journal of Computer Vision 57(2):137-154. Διαθέσιμο σε : <https://link.springer.com/article/10.1023/B:VISI.0000013087.49260.fb>

⁴³ <https://www.nationalacademies.org/read/27397/chapter/4>

αναπαριστάται ως μια ιεραρχική δομή διαδοχικών υποσυνόλων. Η Τεχνητή Νοημοσύνη αποτελεί το ευρύτερο πεδίο, το οποίο αποσκοπεί στην ανάπτυξη συστημάτων ικανών να επιλύουν σύνθετα προβλήματα μέσω της εύρεσης βέλτιστων συναρτήσεων μετασχηματισμού. Η Μηχανική Μάθηση συνιστά εξειδικευμένο κλάδο της Τεχνητής Νοημοσύνης, περιλαμβάνοντας αλγορίθμους που επιτρέπουν τη μείωση της διαστατικότητας των δεδομένων και την αυτοματοποιημένη ταξινόμηση. Η Βαθιά Μάθηση αποτελεί με τη σειρά της έναν προηγμένο κλάδο της Μηχανικής Μάθησης, η οποία διαφοροποιείται λόγω της ικανότητάς της να εντοπίζει αυτόματα τα αναγκαία χαρακτηριστικά για την αναγνώριση και ταξινόμηση, χωρίς να απαιτείται η χειροκίνητη εξαγωγή γνωρισμάτων, προσομοιάζοντας στον τρόπο που λειτουργεί η ανθρώπινη όραση. Στην τρέχουσα τεχνολογική πραγματικότητα, τα Συνελικτικά Νευρωνικά Δίκτυα (εφεξής 'CNNs') αντιπροσωπεύουν την πλέον διαδεδομένη και αποτελεσματική εφαρμογή της Βαθιάς Μάθησης ⁴⁴.

Τα CNNs μοιάζουν πολύ με τα κοινά νευρωνικά δίκτυα, καθώς η εσωτερική τους δομή αποτελείται από ψηφιακούς "νευρώνες". Κάθε νευρώνας έχει κάποιες ρυθμίσεις (βάση) και τιμές απόκλισης (bias) που προσαρμόζονται κατά την εκπαίδευση, ώστε το σύστημα να μαθαίνει από τα λάθη του. Όταν το δίκτυο δέχεται μια νέα εικόνα, εκτελεί γρήγορους μαθηματικούς υπολογισμούς για να συγκρίνει τα δεδομένα της εισόδου με όσα έχει ήδη μάθει. Στο τέλος, το δίκτυο δίνει μια "βαθμολογία" που αντιστοιχεί στην πιθανότητα το πρόσωπο που βλέπει να είναι ο "x" ή ο "y". Αυτή η ικανότητα να απλοποιούν την πολυπλοκότητα μιας εικόνας τα καθιστά το πιο ισχυρό εργαλείο στην αναγνώριση προσώπων σήμερα.

Κατά την τελευταία δεκαετία, ο τομέας της αναγνώρισης προσώπου έχει σημειώσει σημαντικότερη πρόοδο, κυρίως λόγω των καινοτομιών σε μια τεχνική τεχνητής νοημοσύνης γνωστή ως Βαθιά Συνελικτικά Νευρωνικά Δίκτυα (εφεξής 'DCNNs'). Αυτά αναπτύχθηκαν αρχικά για την οπτική αναγνώριση χαρακτήρων και αργότερα εφαρμόστηκαν σε ποικίλες εργασίες υπολογιστικής όρασης, όπως η αυτόνομη οδήγηση και η ανάλυση ιατρικών

⁴⁴ W. Wang, Y. Jie, J. Xiao, L. Sheng, and D. Zhou, "Face recognition based on deep learning," in Proc. Int. Conf. Hum. Centered Comput., 2014, pp. 812–820.

εικόνων.⁴⁵ Οι αλγόριθμοι αυτοί εκπαιδεύονται σε τεράστια σύνολα από εικόνες προσώπων για να μάθουν τα μοναδικά μοτίβα των ανθρώπινων προσώπων, βελτιώνοντας την ακρίβεια και την αποτελεσματικότητα της διαδικασίας αναγνώρισης. Τα DCNNs αποτελούν σήμερα το κυρίαρχο πρότυπο στην υπολογιστική αναγνώριση προσώπου. Μάλιστα, έρευνες κατέδειξαν ότι η μετάβαση από τις παραδοσιακές μεθόδους στα DCNNs έχει αναβαθμίσει την αλγοριθμική ακρίβεια σε επίπεδα που εξισώνονται με τις ανθρώπινες ικανότητες σε εργασίες ταυτοποίησης υπό πραγματικές συνθήκες.⁴⁶

Από θεωρητική σκοπιά, τα DCNNs περιγράφονται ως μοντέλα «άμεσης προσαρμογής» (direct-fit), τα οποία λειτουργούν μέσω της υπερπαραμετροποίησης. Αυτό σημαίνει ότι το σύστημα δεν βασίζεται σε απλούς, ερμηνεύσιμους κανόνες ή μεμονωμένα χαρακτηριστικά, αλλά μαθαίνει να τοποθετεί κάθε νέα παρατήρηση στο πλαίσιο μιας τεράστιας βάσης προηγούμενης εμπειρίας. Αυτή η προσέγγιση καθιστά δύσκολη την απόδοση της απόφασης του συστήματος σε συγκεκριμένα χαρακτηριστικά του προσώπου, καθώς η πληροφορία είναι κατανεμημένη σε όλο το εύρος του δικτύου. Αυτή ακριβώς η αδυναμία επεξήγησης θεμελιώνει το «πρόβλημα του μαύρου κουτιού» (black box problem).

Η εφαρμογή των DCNNs στην αναγνώριση προσώπου επιδείχθηκε με εμβληματικό τρόπο το 2014 μέσω του μοντέλου DeepFace, το οποίο αναπτύχθηκε από ερευνητές της Facebook, Inc. Το DeepFace αποτέλεσε ορόσημο για τον κλάδο, καθώς ήταν η πρώτη φορά που ένα υπολογιστικό σύστημα προσέγγισε την ανθρώπινη απόδοση σε σχετικές εργασίες ταυτοποίησης. Για την εκπαίδευσή του χρησιμοποιήθηκε το μεγαλύτερο σύνολο δεδομένων της εποχής, αποτελούμενο από τέσσερα εκατομμύρια εικόνες προσώπου σε μη ελεγχόμενα περιβάλλοντα, με τις παραλλαγές που παρατηρούνται στην καθημερινή ζωή (στάση, φωτισμός, φύλο, ηλικία, φυλή, στυλ ένδυσης, στυλ μαλλιών, ποιότητα κάμερας, κορεσμός

⁴⁵ National Academies of Sciences, Engineering, and Medicine. 2024. Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance. Washington, DC: The National Academies Press. <https://doi.org/10.17226/62>.

⁴⁶ P.J. Phillips, A.N. Yates, Y. Hu, C.A. Hahn, E. Noyes, K. Jackson, J.G. Cavazos, G. Jeckeln, R. Ranjan, S. Sankaranarayanan, J. Chen, C.D. Castillo, R. Chellappa, D. White, & A.J. O'Toole, Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms, Proc. Natl. Acad. Sci. U.S.A. 115 (24) 6171-6176, <https://doi.org/10.1073/pnas.1721355115> (2018).

χρώματος κ.λπ.)⁴⁷. Ο αντίκτυπος αυτής της προσέγγισης ήταν εντυπωσιακός, καθώς το μοντέλο πέτυχε ακρίβεια 97,35% στο διεθνές πρότυπο αξιολόγησης Labeled Faces in the Wild (LFW), μειώνοντας το σφάλμα των προγενέστερων μεθόδων κατά 27%.⁴⁸

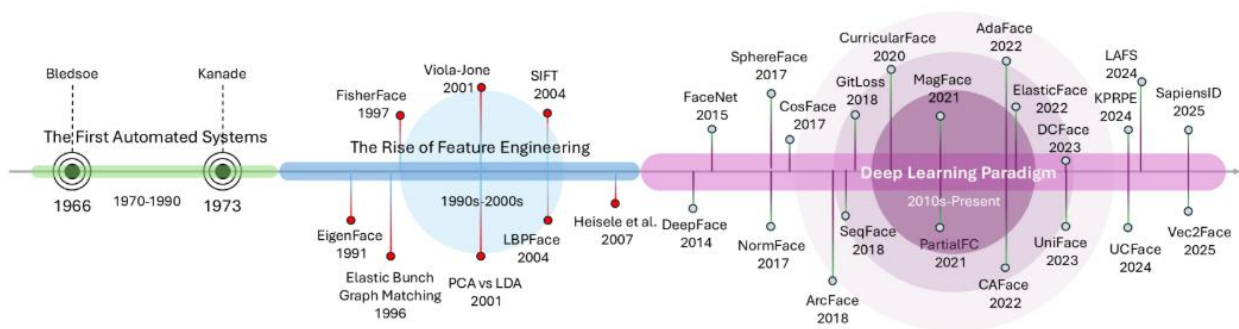
Από την εφαρμογή της, η ακρίβεια του συστήματος έφτασε το 99,80% σε μόλις τρία χρόνια⁴⁹. Η εντυπωσιακή αυτή βελτίωση οφείλεται στην ικανότητα των δικτύων DCNNs να εστιάζουν στα μόνιμα χαρακτηριστικά του προσώπου, αγνοώντας παράγοντες που συνήθως δυσκολεύουν την αναγνώριση, όπως ο κακός φωτισμός ή η γωνία λήψης. Παρόλο που αρχικά υπήρχαν αμφιβολίες για το αν αυτοί οι αλγόριθμοι θα μπορούσαν να λειτουργήσουν αποτελεσματικά σε πληθυσμούς εκατομμυρίων ανθρώπων, η στρατηγική του Facebook να χρησιμοποιήσει τεράστιο όγκο δεδομένων από τα κοινωνικά δίκτυα αποδείχθηκε καθοριστική και άλλαξε τα δεδομένα στον κλάδο.

Μέσα στην επόμενη δεκαετία, ο κλάδος των βιομετρικών συστημάτων εγκατέλειψε τις παραδοσιακές «χειροκίνητες» μεθόδους σχεδιασμού χαρακτηριστικών και υιοθέτησε πλήρως τα DCNNs. Η έρευνα που ακολούθησε βελτίωσε σημαντικά τον τρόπο που τα δίκτυα «μαθαίνουν» να ξεχωρίζουν τα πρόσωπα (μέσω των συναρτήσεων απώλειας- loss functions), καθιερώνοντας αυτές τις μεθόδους ως το νέο παγκόσμιο πρότυπο. Σήμερα, αυτές οι προσεγγίσεις αποτελούν τη βάση για κάθε σύγχρονη εφαρμογή αναγνώρισης προσώπου, έχοντας κερδίσει την καθολική αποδοχή της επιστημονικής κοινότητας.

⁴⁷ Taigman, Y., Yang, M., Ranzato, M.A. and Wolf, L. (2014) 'Deepface: Closing the gap to human-level performance in face verification', in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 1701–1708.

⁴⁸ I. Raji and G. Fried, About Face: A Survey of Facial Recognition Evaluation, 2021.

⁴⁹ Wang, M. and Deng, W. (2021) 'Deep face recognition: A survey', *Neurocomputing*, 429, p. 216.



Εικόνα 1: Χρονολόγο της εξέλιξης της αναγνώρισης προσώπου, το οποίο αποτυπώνει τη μετάβαση από χειροκίνητες μεθόδους σε προσεγγίσεις που βασίζονται στη βαθιά μάθηση. Το μέγεθος των χρωματιστών κύκλων αντιπροσωπεύει τον ετήσιο όγκο επιστημονικών δημοσιεύσεων για κάθε χρονική περίοδο.

3.4 Η εφαρμογή αναγνώρισης προσώπου για σκοπούς επιβολής του νόμου

Η ιστορία της αναγνώρισης προσώπου είναι άρρηκτα συνδεδεμένη με την ευρύτερη ανάγκη για αξιόπιστη ταυτοποίηση προσώπων, η οποία αρχικά καθοδηγήθηκε από τις απαιτήσεις της επιβολής του νόμου και της δημόσιας ασφάλειας. Η θέσπιση του Habitual Criminals Act το 1869 στο Ηνωμένο Βασίλειο αποτέλεσε μία από τις πρώτες προσπάθειες τυποποίησης της βιομετρικής ταυτοποίησης των κατ' επανάληψη δραστών. Η εν λόγω προσπάθεια έθεσε το εννοιολογικό υπόβαθρο για τη βιομετρική ταυτοποίηση, η οποία -όπως αναλύθηκε προηγουμένως- μετασχηματίστηκε από τις παραδοσιακές χειροκίνητες μεθόδους στα σημερινά προηγμένα συστήματα υπολογιστικής όρασης ^{50 51}.

Παρά την απουσία ενός σαφούς νομικού πλαισίου -ή ίσως ακριβώς εξαιτίας αυτής- αρκετές ευρωπαϊκές αστυνομικές αρχές έχουν καταφύγει στη χρήση της συγκεκριμένης τεχνολογίας. Η πιο ακραία περίπτωση χρήσης συστημάτων καμερών παρακολούθησης με FRT, συμπεριλαμβανομένης της αναγνώρισης σε πραγματικό χρόνο, εντοπίζεται στην Κίνα. Δημοσιογραφικές πηγές αναφέρουν, μεταξύ άλλων, ότι χάρη σε ένα σύστημα καμερών

⁵⁰ Kim, M., Jain, A. and Liu, X. (2025) '50 Years of Automated Face Recognition', *arXiv preprint arXiv:2505.24247*. Διαθέσιμο στο: <https://arxiv.org/abs/2505.24247> (Πρόσβαση: Φεβρουάριος 2026)

⁵¹ Spearman, E. (1869) *Crime and Punishment in England: A Sourcebook*. London: Routledge

παρακολούθησης στην πόλη Guiyang, η αστυνομία είναι σε θέση να εντοπίσει και να ταυτοποιήσει οποιοδήποτε φυσικό πρόσωπο μέσα σε λίγα μόνο λεπτά, καθώς και να ιχνηλατήσει τις παρελθούσες κινήσεις του⁵². Ωστόσο, οι ακριβείς πληροφορίες σχετικά με τέτοιες πρακτικές είναι συχνά δύσκολο να βρεθούν, λόγω της έλλειψης διαφάνειας και της μυστικότητας της αστυνομίας⁵³.

Στον Ευρωπαϊκό χώρο, και συγκεκριμένα στο Ηνωμένο Βασίλειο, η χρήση της τεχνολογίας αναγνώρισης προσώπου αποδείχθηκε αρκετά εκτεταμένη και ταυτόχρονα αμφιλεγόμενη. Οι αστυνομικές δυνάμεις της Νότιας Ουαλίας, του Λέστερσιρ και η Μητροπολιτική Αστυνομία του Λονδίνου (Metropolitan Police Service) διεξήγαγαν δοκιμές αναγνώρισης προσώπου σε πραγματικό χρόνο σε δημόσιους χώρους μεταξύ 2016 και 2019. Λαμβάνοντας ως παράδειγμα τη Μητροπολιτική Αστυνομία του Λονδίνου, διενήργησε δέκα τέτοιες δοκιμές, χρησιμοποιώντας κάμερες σταθερής θέσης, είτε εγκατεστημένες κατά παρόμοιο τρόπο με τις κάμερες CCTV, είτε σε κινητές μονάδες.

Οι εικόνες που καταγράφονταν από τις κάμερες μεταδίδονταν σε πραγματικό χρόνο στο σύστημα αναγνώρισης προσώπου, το οποίο επεξεργαζόταν τις εικόνες για τον εντοπισμό προσώπων, την εξαγωγή βιομετρικών χαρακτηριστικών και την αντιπαραβολή τους με μία «λίστα παρακολούθησης», μιας βάσης δεδομένων δηλαδή με εικόνες καταζητούμενων προσώπων. Σε περίπτωση ταύτισης, ειδοποιούταν το κέντρο ελέγχου και το λογισμικό ελεγχόταν χειροκίνητα από αστυνομικούς. Συγκεκριμένα, το λογισμικό εμφάνιζε παράλληλα τη ζωντανή λήψη και την εικόνα αναφοράς από τη λίστα, επιτρέποντας στους αστυνομικούς να τις συγκρίνουν και να αποφασίσουν για τη διενέργεια ελέγχου στο υποκείμενο⁵⁴.

⁵² Liu, J. (2017) *In Your Face: China's all-seeing state* [Video]. BBC News, 10 December. Διαθέσιμο στο: <https://www.bbc.com/news/av/world-asia-china-42248056> (Πρόσβαση: 24 Ιανουαρίου 2020).

⁵³ Kayser-Bril, N. (2019) *At least 11 police forces use face recognition in the EU, AlgorithmWatch reveals*. AlgorithmWatch, 11 December. Διαθέσιμο στο: <https://algorithmwatch.org/en/face-recognition-police-europe/> (Πρόσβαση: 8 Φεβρουαρίου 2026).

⁵⁴ Fussey, P. and Murray, D. (2019) *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*. Colchester: Human Rights Centre, University of Essex. Διαθέσιμο στο: <https://repository.essex.ac.uk/24946/> (Πρόσβαση Ιανουάριο 2026).

Σύμφωνα με τη διαθέσιμη τεκμηρίωση, σε περίπτωση που δεν προέκυπτε ταύτιση, τα ψηφιακά δεδομένα διαγράφονταν αμέσως μετά την επεξεργασία. Εάν προέκυπτε ταύτιση, διατηρούνταν για περίοδο 30 ημερών.

Με συνολικό αριθμό που αγγίζει τα 5,9 εκατομμύρια κάμερες CCTV, το Ηνωμένο Βασίλειο κατατάσσεται στην τρίτη θέση παγκοσμίως ως προς την αναλογία καμερών ανά κάτοικο, ακολουθώντας τις ΗΠΑ και την Κίνα. Ως εκ τούτου, οι δυνατότητες επιτήρησης είναι ευρύτατες. Εκτιμάται μάλιστα ότι, χάρη στις σύγχρονες τεχνολογίες, ο εντοπισμός ενός υπόπτου σε μητροπολιτική περιοχή τριών εκατομμυρίων κατοίκων καθίσταται εφικτός εντός μόλις επτά λεπτών.

Ωστόσο, η αποτελεσματικότητα αυτή συχνά συνοδεύεται από σοβαρά σφάλματα. Χαρακτηριστική είναι η περίπτωση της αστυνομίας της Νότιας Ουαλίας, η οποία χρησιμοποίησε την εν λόγω τεχνολογία στον τελικό του Champions League το έτος 2017 χωρίς να υφίσταται νομοθετικό πλαίσιο που να επιτρέπει τη χρήση της εν λόγω τεχνολογίας από τις αρχές⁵⁵. Αργότερα αποκαλύφθηκε ότι 2.297 από τις 2.470 ταυτοποιήσεις ήταν εσφαλμένες (εμφάνισαν ψευδώς θετικά αποτελέσματα), γεγονός που εγείρει σοβαρά ζητήματα αξιοπιστίας αλλά και προσβολής των δικαιωμάτων και ελευθεριών των πολιτών⁵⁶. Επιπλέον, αστυνομικές αρχές άλλων ευρωπαϊκών χωρών, όπως του Βερολίνου και της Νίκαιας της Γαλλίας, δοκίμασαν την ακρίβεια της τεχνολογίας σε πειράματα μεγαλύτερης κλίμακας με εθελοντές.⁵⁷

Στη Σουηδία, το 2021, η Αρχή Προστασίας Δεδομένων επέβαλε πρόστιμο στη σουηδική αστυνομία, ύψους 248.218 ευρώ, για τη χρήση τεχνολογίας αναγνώρισης προσώπου στο πλαίσιο πιλοτικού προγράμματος, χωρίς την πλήρη συμμόρφωση με τον ΓΚΠΔ. Η σουηδική αστυνομία εφάρμοσε την εν λόγω τεχνολογία για την υποστήριξη ποινικών ερευνών,

⁵⁵ Κ. Χαμπίδης, Γ. Κιουμουρτζής (2019) Πρέπει να μπει φρένο στην αναγνώριση προσώπου; Εφημερίδα Καθημερινή, Διαθέσιμο σε : <https://www.kathimerini.gr/opinion/1025741/prepei-na-mpei-freno-stin-anagnorisi-prosopoy/> (Πρόσβαση: Δεκέμβριος 2025)

⁵⁶ Σ. Γεωργίου (2021) Αυτόματη αναγνώριση προσώπου στους δημόσιους χώρους: Μεταξύ πραγματικότητας και δυστοπίας, Διαθέσιμο σε: https://www.syntagmawatch.gr/trending-issues/aytomati-anagnwrisi-proswpou-stous-dhmosious-xwrous-metaxy-pragmatikothtas-kai-dystopias/#_ftn4 (Πρόσβαση: Δεκέμβριος 2025)

⁵⁷ O'Flaherty, M. (2020). Facial recognition technology and fundamental rights. European Data Protection Law Review (EDPL), 6(2), 170-173.

ωστόσο η Αρχή διαπίστωσε σειρά παραβιάσεων των απαιτήσεων του ΓΚΠΔ, υπογραμμίζοντας την ανάγκη για ισχυρά μέτρα προστασίας των δεδομένων, ιδίως όσον αφορά τα βιομετρικά δεδομένα. Συγκεκριμένα, η αστυνομία χρησιμοποιούσε το Clearview AI, μια αμφιλεγόμενη αμερικανική εφαρμογή, χωρίς να έχει διενεργήσει προγενέστερα Εκτίμηση Αντικτύπου σχετικά με την προστασία δεδομένων (DPIA). Στη συγκεκριμένη περίπτωση, η Αρχή έκρινε ότι η Αστυνομία επεξεργάστηκε βιομετρικά δεδομένα χωρίς νόμιμη βάση κατά τον ΓΚΠΔ. Επιπλέον, η έλλειψη επαρκούς αιτιολόγησης από πλευράς της αστυνομίας για την επεξεργασία αυτών των δεδομένων ανέδειξε την αποτυχία συμμόρφωσης με τα πρότυπα του ΓΚΠΔ⁵⁸.

Όπως προκύπτει από τα ανωτέρω, οι τεχνολογίες αναγνώρισης προσώπου χρησιμοποιούνται ήδη από αστυνομικές αρχές παγκοσμίως, ενώ αρκετές ευρωπαϊκές αστυνομικές υπηρεσίες πραγματοποιούν δοκιμές και πιλοτικές εφαρμογές -κυρίως με τη συμμετοχή εθελοντών- με σκοπό την καθιέρωση της συστηματικής τους χρήσης. Κατά συνέπεια, η θέσπιση ρυθμιστικού πλαισίου καθίσταται επιτακτική.

⁵⁸ Swedish Privacy Authority (2021) *Decision DI-2020-2719*. 10 Φεβρουαρίου. Διαθέσιμο στο: [https://gdprhub.eu/index.php?title=IMY_\(Sweden\)_-DI-2020-2719](https://gdprhub.eu/index.php?title=IMY_(Sweden)_-DI-2020-2719) (Πρόσβαση: Φεβρουάριο 2026).

4 ΤΟ ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ ΓΙΑ ΤΑ ΣΥΣΤΗΜΑΤΑ ΕΞ ΑΠΟΣΤΑΣΕΩΣ ΒΙΟΜΕΤΡΙΚΗΣ ΤΑΥΤΟΠΟΙΗΣΗΣ ΣΤΟΝ ΚΑΝΟΝΙΣΜΟ ΓΙΑ ΤΗΝ ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ

4.1 Εισαγωγή

Το γεγονός ότι στην τεχνολογία αναγνώρισης προσώπου (FRT) χρησιμοποιείται Τεχνητή Νοημοσύνη αποτελεί πρόσθετη πηγή ανησυχίας. Το θεσμικό πλαίσιο για την ανάπτυξη, διάθεση στην αγορά, θέση σε λειτουργία και χρήση συστημάτων τεχνητής νοημοσύνης εντός της ΕΕ έμελλε να ρυθμιστεί με την Πράξη για την Τεχνητή Νοημοσύνη που τέθηκε σε ισχύ την 1η Αυγούστου 2024. Η Πράξη αποσκοπεί στη βελτίωση της λειτουργίας της εσωτερικής αγοράς κατά τρόπο σύμφωνο με τις αξίες της Ένωσης και προσανατολισμένο προς μία ανθρωποκεντρική και αξιόπιστη τεχνητή νοημοσύνη. Περαιτέρω, στόχος της Πράξης είναι η στήριξη της καινοτομίας με ταυτόχρονη διασφάλιση υψηλού επιπέδου προστασίας της υγείας, της ασφάλειας, των θεμελιωδών δικαιωμάτων που κατοχυρώνονται στον Χάρτη, συμπεριλαμβανομένης της δημοκρατίας, του κράτους δικαίου και της προστασίας του περιβάλλοντος από τις επιζήμιες συνέπειες των συστημάτων ΤΝ.

Υιοθετώντας μία ιεραρχική (top-down) προσέγγιση βάσει επικινδυνότητας, ο Κανονισμός διαβαθμίζει τα συστήματα ΤΝ σύμφωνα με την απειλή που συνιστούν για τα ατομικά δικαιώματα και τις αρχές της Ένωσης. Ειδικότερα, τα συστήματα ΤΝ κατατάσσονται σε τέσσερις κατηγορίες κινδύνου, οι οποίες έχουν ως εξής: συστήματα μη αποδεκτού, υψηλού, περιορισμένου ή ελάχιστου κινδύνου, όπου και εμπίπτει η συντριπτική πλειονότητα των συστημάτων ΤΝ⁵⁹. Η ταξινόμηση με βάση τον βαθμό του δυνητικού τους κινδύνου να προκαλέσουν βλάβη είναι στενά συνδεδεμένη με τον επιδιωκόμενο σκοπό κάθε συστήματος ΤΝ, δηλαδή την χρήση για την οποία προορίζεται από τον πάροχο, συμπεριλαμβανομένου του ειδικότερου πλαισίου και των οδηγιών χρήσης⁶⁰. Συνεπώς, οι ίδιοι αλγόριθμοι και το ίδιο λογισμικό που εφαρμόζονται τόσο στο σύστημα Α όσο και στο σύστημα Β μπορούν να

⁵⁹ Βλ. Ευρωπαϊκή Επιτροπή, Μια Ευρώπη έτοιμη για την ψηφιακή εποχή: η Επιτροπή προτείνει νέους κανόνες και δράσεις για την αριστεία και την εμπιστοσύνη στην τεχνητή νοημοσύνη, Δελτίο Τύπου, 21 Απριλίου 2021, Βρυξέλλες, σελ. 1-2.

⁶⁰ άρθρο 3 παρ.12 AI ACT

οδηγήσουν σε διαφορετική ταξινόμηση κινδύνου. Η προσέγγιση δεν εστιάζει στην τεχνολογία, αλλά στον σκοπό του κάθε συστήματος. Αξιοσημείωτο είναι επίσης ότι τα συστήματα TN που αναπτύσσονται ή χρησιμοποιούνται αποκλειστικά για στρατιωτικούς σκοπούς θα πρέπει να εξαιρούνται από το πεδίο εφαρμογής του παρόντος Κανονισμού⁶¹.

4.2 Η νομοπαρασκευαστική πορεία

Η διαμόρφωση του κανονιστικού πλαισίου για τα συστήματα αναγνώρισης προσώπου υπήρξε το αποτέλεσμα μιας μακράς και σύνθετης νομοπαρασκευαστικής διαδικασίας. Η απαρχή των συζητήσεων εντοπίζεται στη Λευκή Βίβλο για την TN το 2020. Παρόλο που η Λευκή Βίβλος δεν θεωρείται νομικά δεσμευτικό έγγραφο, οι διατάξεις της είναι χρήσιμες για την κατανόηση της αρχικής προσέγγισης της Ευρωπαϊκής Ένωσης σχετικά με τα βιομετρικά συστήματα. Η χρήση εφαρμογών που στοχεύουν στην εξ αποστάσεως βιομετρική ταυτοποίηση θεωρήθηκε ότι θα έχει πάντοτε τον χαρακτήρα «υψηλού κινδύνου», αναγνωρίζοντας τις σημαντικές επιπτώσεις που δύναται να προκαλέσει στα θεμελιώδη δικαιώματα. Επομένως, το συμπέρασμα της Λευκής Βίβλου, ακολουθώντας τους κανόνες προστασίας δεδομένων της ΕΕ και του Χάρτη Θεμελιωδών Δικαιωμάτων, ήταν ότι η χρήση της TN σε συστήματα αναγνώρισης προσώπου θα πρέπει να είναι δεόντως αιτιολογημένη, αναλογική και να υπόκειται σε κατάλληλες εγγυήσεις⁶², έννοιες που αναμφισβήτητα παραμένουν «ανοιχτές» σε ερμηνείες⁶³.

Η μετάβαση σε ένα αυστηρότερο ρυθμιστικό πλαίσιο σηματοδοτήθηκε, ένα έτος αργότερα, με την αρχική πρόταση της Επιτροπής για την Πράξη για την TN τον Απρίλιο του 2021⁶⁴.

⁶¹ Άρθρο 2 Πράξη TN

⁶² Ευρωπαϊκή Επιτροπή (2020) *Λευκή Βίβλος για την Τεχνητή Νοημοσύνη - Η ευρωπαϊκή προσέγγιση της αριστείας και της εμπιστοσύνης*. COM(2020) 65 final. Διαθέσιμο στο: <https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52020DC0065> (Πρόσβαση: 25 Ιανουαρίου 2026).

⁶³ Vera Lúcia Raposo (2024) 'Look at the camera and say cheese': the existing European legal framework for facial recognition technology in criminal investigations, *Information & Communications Technology Law*, 33:1, 1-20, DOI: 10.1080/13600834.2023.2239621

⁶⁴ 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) και για την τροποποίηση ορισμένων νομοθετικών πράξεων της Ένωσης*.

Υιοθετώντας μια προσέγγιση βασισμένη στην επικινδυνότητα (risk-based approach), η Επιτροπή είχε ταξινομήσει ήδη από τότε τις εφαρμογές ΤΝ σε τέσσερις κατηγορίες (απαράδεκτου, υψηλού, περιορισμένου και ελάχιστου κινδύνου). Στο Άρθρο 5 παρ. 1(δ) της αρχικής πρότασης, εισήχθη για πρώτη φορά η απαγόρευση των συστημάτων βιομετρικής ταυτοποίησης σε πραγματικό χρόνο (real-time) για σκοπούς επιβολής του νόμου σε δημόσιους χώρους, προβαίνοντας παράλληλα σε σαφή διαχωρισμό από τα συστήματα «μεταγενέστερου χρόνου» (post-remote). Παρά το γεγονός ότι τα συστήματα αναγνώρισης προσώπου εμπίπτουν και στις δύο κατηγορίες, η Ευρωπαϊκή Επιτροπή εστίασε το ενδιαφέρον της κυρίως στην απαγόρευση των συστημάτων βιομετρικής ταυτοποίησης σε πραγματικό χρόνο. Η απαγόρευση αυτή αντανάκλασε τον έντονο ηθικό και νομικό προβληματισμό γύρω από τις τεχνολογίες αυτές, οι οποίες θεωρήθηκαν ως άμεση απειλή για τα θεμελιώδη δικαιώματα.

Κατά τη διάρκεια των διαβουλεύσεων, οι θέσεις των θεσμικών οργάνων εμφάνισαν σημαντικές αποκλίσεις. Η τελική έκδοση του συμβιβαστικού κειμένου που εγκρίθηκε από το Συμβούλιο της ΕΕ τον Νοέμβριο του 2022 και υποβλήθηκε τον Δεκέμβριο του 2022 ευθυγραμμίστηκε ευρέως με την πρόταση της Επιτροπής, επιχειρώντας να ισορροπήσει τις ανάγκες της επιβολής του νόμου με τα θεμελιώδη δικαιώματα. Το Συμβούλιο ενέκρινε την απαγόρευση της χρήσης συστημάτων εξ αποστάσεως βιομετρικής ταυτοποίησης σε πραγματικό χρόνο σε δημόσια προσβάσιμους χώρους από τις αρχές επιβολής του νόμου, προτείνοντας όμως την αναθεώρηση της έννοιας «επιβολή του νόμου», ώστε να περιλαμβάνει και μη κρατικούς φορείς που λειτουργούν για λογαριασμό των αρχών επιβολής του νόμου, χωρίς όμως να έχουν εξουσιοδοτηθεί από τη νομοθεσία των κρατών μελών να εκτελούν τέτοια καθήκοντα. Επιπλέον, το Συμβούλιο τροποποίησε το πεδίο εφαρμογής της τεχνολογίας, επεκτείνοντας τις εξαιρέσεις που είχε προτείνει αρχικά η Επιτροπή και σε άλλα αδικήματα εκτός από αυτά για τα οποία μπορεί να εκδοθεί ευρωπαϊκό ένταλμα σύλληψης, τα οποία τιμωρούνται με ποινή φυλάκισης τουλάχιστον πέντε ετών, όπως καθορίζεται από το εθνικό ποινικό δίκαιο.⁶⁵

COM(2021) 206 final. Διαθέσιμο στο: <https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:52021PC0206> (Πρόσβαση: 25 Ιανουαρίου 2026).

⁶⁵ Συμβούλιο της Ευρωπαϊκής Ένωσης (2022) Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη θέσπιση εναρμονισμένων κανόνων σχετικά με την τεχνητή νοημοσύνη (πράξη

Η πλέον καταλυτική καμπή στη νομοπαρασκευαστική διαδικασία της Πράξης για την ΤΝ σημειώθηκε με την τοποθέτηση του Ευρωπαϊκού Κοινοβουλίου τον Ιούνιο του 2023⁶⁶. Το Κοινοβούλιο, ανταποκρινόμενο στις έντονες ανησυχίες για τον κίνδυνο διολίσθησης σε πρακτικές μαζικής επιτήρησης, υιοθέτησε μία πιο αυστηρή θέση για το Άρθρο 5. Επισημαίνεται ότι το Ευρωπαϊκό Κοινοβούλιο, ήδη από το ψήφισμά του τον Οκτώβριο του 2021 και μέσω της ειδικής επιτροπής AIDA, είχε εκφράσει έντονες ανησυχίες για την ασυμμετρία ισχύος μεταξύ κρατών και πολιτών και την παράνομη χρήση ιδιωτικών βάσεων δεδομένων, όπως η Clearview AI. Το 2023, μέσω της Τροπολογίας 220, αξίωσε για πρώτη φορά την καθολική απαγόρευση των συστημάτων βιομετρικής ταυτοποίησης σε πραγματικό χρόνο σε δημόσιους χώρους, διαφωνώντας με τις εξαιρέσεις που είχε προτείνει αρχικά η Επιτροπή το 2021⁶⁷. Επίσης, θέλησε να διευρύνει τον κατάλογο ώστε να συμπεριλάβει απαγορεύσεις και για άλλες παρεμβατικές χρήσεις της ΤΝ, που δεν είχαν μέχρι τότε συμπεριληφθεί. Η ρηξικέλευθη αυτή στάση μετέτρεψε το ζήτημα της βιομετρικής επιτήρησης σε πεδίο τριβής, καθώς συγκρούστηκε ευθέως με την πρόθεση του Συμβουλίου να διατηρήσει παρεκκλίσεις για λόγους επιβολής του νόμου και συνακόλουθα ασφαλείας.

Η αντιπαράθεση αυτή οδηγήθηκε σε εκτόνωση τον Δεκέμβριο του 2023 μέσω μιας άτυπης σειράς συναντήσεων, γνωστής και ως «τριλόγων», κατά τις οποίες το Κοινοβούλιο, το Συμβούλιο και η Επιτροπή διαβουλευόνταν για να διαμορφώσουν τις τελικές διατάξεις. Στο τελικό κείμενο, το Κοινοβούλιο υποχώρησε από τη θέση της απόλυτης απαγόρευσης, αποδεχόμενο την επαναφορά περιορισμένων εξαιρέσεων για τις αρχές επιβολής του νόμου, οι οποίες όμως συνοδεύονται από αυστηρότερες δικλείδες ασφαλείας σε σχέση με την αρχική

για την τεχνητή νοημοσύνη) και την τροποποίηση ορισμένων νομοθετικών πράξεων της Ένωσης - Γενικός προσανατολισμός. 2021/0106 (COD), ST 14954 2022 INIT. [Online]. Διαθέσιμο στο: <https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/el/pdf> (Πρόσβαση: 25 Ιανουαρίου 2026).

⁶⁶ Ευρωπαϊκό Κοινοβούλιο (2023) Τροπολογίες που εγκρίθηκαν από το Ευρωπαϊκό Κοινοβούλιο στις 14 Ιουνίου 2023 σχετικά με την πρόταση κανονισμού για την Πράξη για την Τεχνητή Νοημοσύνη. P9_TA(2023)0236. [Online]. Διαθέσιμο στο: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EL.html (Πρόσβαση: 25 Ιανουαρίου 2026).

⁶⁷ Bertuzzi, L. (2022) *AI Act: Οι συζητήσεις του Ευρωπαϊκού Κοινοβουλίου εντείνονται για την αναγνώριση προσώπων και το πεδίο εφαρμογής*. Euractiv, 6 Οκτωβρίου. [Online]. Διαθέσιμο στο: <https://www.euractiv.com/section/digital/news/ai-act-eu-parliaments-discussions-heat-up-over-facial-recognition-scope/> (Πρόσβαση: 25 Ιανουαρίου 2026).

πρόταση. Συγκεκριμένα, η χρήση συστημάτων βιομετρικής ταυτοποίησης σε πραγματικό χρόνο επιτράπηκε μόνο για συγκεκριμένες απειλές (όπως τρομοκρατικές επιθέσεις ή αναζήτηση θυμάτων εμπορίας ανθρώπων ή υπόπτων για μια προκαθορισμένη λίστα σοβαρών εγκλημάτων), υπό την απαρέγκλιτη προϋπόθεση προηγούμενης δικαστικής άδειας και εφόσον η χρήση τους είναι περιορισμένη χρονικά και τοπικά. Από την άλλη πλευρά η χρήση συστημάτων βιομετρικής ταυτοποίησης σε μεταγενέστερο χρόνο θα χρησιμοποιείται αυστηρά για τη στοχευμένη αναζήτηση προσώπου που έχει καταδικαστεί ή είναι ύποπτο για τη διάπραξη σοβαρού εγκλήματος⁶⁸.

Συμπερασματικά, η κατάληξη σε μια πολιτική συμφωνία για την Πράξη για την ΤΝ, μετά από έναν εξαντλητικό διαπραγματευτικό μααραθώνιο 36 ωρών τον Δεκέμβριο του 2023, συνιστά ένα ορόσημο παγκόσμιας εμβέλειας. Αν και το τελικό κείμενο φιλοδοξεί να αποτελέσει το διεθνές σημείο αναφοράς για τη ρύθμιση της τεχνολογίας, ο «ιστορικός συμβιβασμός» που επετεύχθη αντανακλά μια εύθραυστη ισορροπία. Η υποχώρηση από την αρχική θέση του Ευρωπαϊκού Κοινοβουλίου για πλήρη απαγόρευση της βιομετρικής ταυτοποίησης σε πραγματικό χρόνο, προκειμένου να καμφθούν οι αντιστάσεις των κρατών μελών, άφησε ένα σημαντικό μέρος των νομοθετών και της κοινωνίας των πολιτών ανικανοποίητο.^{69 70}

4.3 Συστήματα εξ αποστάσεως ταυτοποίησης σε πραγματικό χρόνο (real time)

Όπως προαναφέρθηκε, η Πράξη για την ΤΝ εισάγει διάκριση στη χρήση συστημάτων βιομετρικής ταυτοποίησης, διαχωρίζοντας την ταυτοποίηση σε πραγματικό χρόνο (real-time)

⁶⁸ European Parliament (2024) *Artificial Intelligence Act: deal on comprehensive rules for trustworthy AI* [Δελτίο Τύπου]. 9 Δεκεμβρίου. Διαθέσιμο στο: <https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai> (Πρόσβαση: Ιανουάριος 2026).

⁶⁹ Bertuzzi, L. (2024) *Η Ευρωπαϊκή Ένωση «τετραγωνίζει τον κύκλο» για το πρώτο ρυθμιστικό πλαίσιο παγκοσμίως σχετικά με την Τεχνητή Νοημοσύνη*. Euractiv, 15 Φεβρουαρίου. [Online]. Διαθέσιμο στο: <https://www.euractiv.com/section/artificial-intelligence/news/europeanunion-squares-the-circle-on-the-worlds-first-ai-rulebook/> (Πρόσβαση: 25 Ιανουαρίου 2026).

⁷⁰ Wachter, S. (2024) *Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond*. [Online]. Διαθέσιμο στο: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4743200 (Πρόσβαση: 25 Ιανουαρίου 2026).

από την ταυτοποίηση σε μεταγενέστερο χρόνο (post-remote biometric identification). Η χρήση FRT σε πραγματικό χρόνο σε δημόσια προσβάσιμους χώρους για σκοπούς επιβολής του νόμου θεωρείται σύστημα που ενέχει μη αποδεκτό ρίσκο και κατ' αρχήν απαγορεύεται, εκτός εάν συντρέχουν ουσιαστικές και δικονομικές προϋποθέσεις (Άρθρο 5 παρ. 1η).

Για να είναι πλήρως κατανοητό σε τι συνίσταται η χρήση συστημάτων εξ αποστάσεως βιομετρικής ταυτοποίησης «σε πραγματικό χρόνο», σε «δημόσια προσβάσιμους χώρους» για τους «σκοπούς επιβολής του νόμου» πρέπει προηγουμένως να αναλυθούν οι επιμέρους έννοιες. Χρήση «σε πραγματικό χρόνο» σημαίνει ότι διαδικασίες, όπως η λήψη βιομετρικών δεδομένων, η σύγκριση με άλλα βιομετρικά δεδομένα και η ταυτοποίηση ατόμων λαμβάνουν χώρα αμέσως ή σχεδόν αμέσως ή τουλάχιστον χωρίς σημαντική καθυστέρηση⁷¹. Ο ορισμός του «πραγματικού χρόνου» είναι ασαφής και δεν βασίζεται σε μια επιστημονική κατανόηση του όρου.

Ως «σκοποί επιβολής του νόμου» νοούνται εκείνοι που περιγράφονται στο Άρθρο 1(1) της Οδηγίας για την Επιβολή του Νόμου (LED) και επαναλαμβάνονται στο Άρθρο 3(46) της Πράξης για την TN, δηλαδή: «η πρόληψη, η διερεύνηση, η ανίχνευση ή η δίωξη αξιόποινων πράξεων ή η εκτέλεση ποινικών κυρώσεων, περιλαμβανομένων της προστασίας από απειλές κατά της δημόσιας ασφάλειας και της αποτροπής αυτών». Τέλος, από τον συνδυασμό της αιτιολογικής σκέψης 19 του Κανονισμού και του άρθρου 3 στ. 44) προκύπτει ότι για τους σκοπούς του Κανονισμού ως «δημόσια προσβάσιμος χώρος» θεωρείται ο χώρος που είναι προσβάσιμος σε απροσδιόριστο αριθμό φυσικών προσώπων, είτε ο χώρος αυτός είναι ιδιωτικός είτε δημόσιος, ανεξάρτητα από τη δραστηριότητα για την οποία μπορεί να χρησιμοποιηθεί. Για τους σκοπούς του Κανονισμού, από την ανωτέρω έννοια εξαιρούνται οι φυλακές και οι χώροι συνοριακού ελέγχου.

Χαρακτηριστικό παράδειγμα συστημάτων εξ αποστάσεως βιομετρικής ταυτοποίησης σε πραγματικό χρόνο είναι τα συστήματα σε σημεία ελέγχου του αεροδρομίου. Μια κάμερα καταγράφει μια ζωντανή εικόνα του προσώπου ενός επιβάτη καθώς αυτός πλησιάζει στο σημείο ελέγχου και τη συγκρίνει με μια βάση δεδομένων για την ταυτοποίηση του ατόμου. Αυτή η διαδικασία σύγκρισης και ταυτοποίησης πραγματοποιείται στιγμιαία.

⁷¹ Αιτιολογική Σκέψη 17 TN

Η ανωτέρω απαγόρευση χρήσης αίρεται μόνο σε τρεις εξαντλητικά απαριθμούμενες και αυστηρά καθορισμένες περιπτώσεις, όπου η χρήση επιτρέπεται ως «απολύτως αναγκαία», για λόγους προστασίας του δημόσιου συμφέροντος που ως υπέρτερο έννομο αγαθό υπερισχύει. Έτσι, η χρήση επιτρέπεται εάν ο στόχος αφορά: (1) στην αναζήτηση θυμάτων απαγωγής, εμπορίας ανθρώπων ή σεξουαλικής εκμετάλλευσης, καθώς και σε αγνοούμενα πρόσωπα, (2) στην πρόληψη συγκεκριμένης, ουσιαστικής και επικείμενης απειλής για τη ζωή ή την ασφάλεια ή την πρόληψη τρομοκρατικής επίθεσης και (3) στον εντοπισμό ή στην ταυτοποίηση προσώπου που είναι ύποπτο για τη διάπραξη σοβαρών αδικημάτων που απαριθμούνται στο Παράρτημα II του Κανονισμού και τιμωρούνται στο οικείο κράτος μέλος με στερητική της ελευθερίας ποινή ή στερητικό της ελευθερίας μέτρο ασφάλειας ανώτατης διάρκειας τουλάχιστον τεσσάρων ετών (π.χ. τρομοκρατία, οργανωμένο έγκλημα, σεξουαλική εκμετάλλευση παιδιών).

Στις τρεις αυτές εξαιρετικές περιπτώσεις, εάν τα κράτη μέλη επιθυμούν να κάνουν χρήση της FRT σε πραγματικό χρόνο, πρέπει να θεσπίσουν εθνική νομοθεσία που να επιτρέπει τη χρήση της. Η κατ' εξαίρεση αδειοδότηση της FRT σε πραγματικό χρόνο στο εθνικό δίκαιο απαιτεί τήρηση της αρχής αναλογικότητας, δηλαδή εφαρμογή χρονικών, γεωγραφικών και προσωπικών περιορισμών, διενέργεια εκτίμησης αντικτύπου στα θεμελιώδη δικαιώματα (FRISA) από την αρχή επιβολής του νόμου (άρθρο 27) και καταχώριση στη βάση δεδομένων της ΕΕ (άρθρο 49)⁷². Ωστόσο, στον Κανονισμό προβλέπεται εξαίρεση όπου σε δεόντως αιτιολογημένες επείγουσες περιπτώσεις, η χρήση τέτοιων συστημάτων μπορεί να αρχίσει χωρίς την καταχώριση στη βάση δεδομένων της ΕΕ, υπό την προϋπόθεση ότι η εν λόγω καταχώριση θα ολοκληρωθεί χωρίς αδικαιολόγητη καθυστέρηση. Επιπλέον, κάθε κατ' εξαίρεση χρήση FRT σε πραγματικό χρόνο απαιτεί προηγούμενη έγκριση από δικαστική ή ανεξάρτητη διοικητική αρχή, η οποία βασίζεται σε «αντικειμενικά στοιχεία ή σαφείς ενδείξεις» ότι η χρήση τους είναι αναγκαία και αναλογική προς έναν από τους τρεις επιδιωκόμενους στόχους⁷³. Εξαιρέσεις από αυτόν τον κανόνα θα πρέπει να επιτρέπονται σε δεόντως αιτιολογημένες περιπτώσεις επείγουσας ανάγκης, όπου η χρήση τους μπορεί να ξεκινήσει χωρίς έγκριση, υπό την προϋπόθεση ότι η άδεια θα ληφθεί το αργότερο εντός 24

⁷² Αιτιολογική Σκέψη 34 TN

⁷³ Άρθρο 5(3) της TN

ωρών. Εάν η έγκριση απορριφθεί, η χρήση τους πρέπει να σταματήσει αμέσως και όλα τα δεδομένα και οι πληροφορίες να διαγραφούν. Καμία απόφαση που παράγει δυσμενές έννομο αποτέλεσμα για ένα πρόσωπο δεν θα πρέπει να λαμβάνεται αποκλειστικά βάσει του αποτελέσματος του συστήματος εξ αποστάσεως βιομετρικής ταυτοποίησης⁷⁴. Η Πράξη για την ΤΝ απαιτεί επίσης να ενημερώνεται η σχετική αρχή εποπτείας της αγοράς και η εθνική αρχή προστασίας δεδομένων για κάθε χρήση του συστήματος βιομετρικής ταυτοποίησης σε «πραγματικό χρόνο»⁷⁵. Τα κράτη μέλη μπορούν να επιτρέψουν πλήρως ή μερικώς τη χρήση των RBIs σε πραγματικό χρόνο. Επίσης, έχουν τη διακριτική ευχέρεια είτε να μην προβλέψουν καθόλου μια τέτοια δυνατότητα είτε να την προβλέψουν μόνο όσον αφορά ορισμένους από τους στόχους που μπορούν να δικαιολογήσουν την εγκεκριμένη χρήση, όπως ορίζονται στην Πράξη για την ΤΝ⁷⁶. Σε περίπτωση που επιτρέψουν τη χρήση, η εθνική τους νομοθεσία θα πρέπει να προσδιορίζει λεπτομερώς τους κανόνες για τη λήψη της έγκρισης, τους επιδιωκόμενους στόχους και, στην περίπτωση εντοπισμού ή ταυτοποίησης υπόπτου, τα συγκεκριμένα ποινικά αδικήματα για τα οποία επιτρέπεται η χρήση, καθώς και τις αρμόδιες αρχές. Τα κράτη μέλη οφείλουν να αναφέρουν τους κανόνες που υιοθετούν στην Ευρωπαϊκή Επιτροπή και μπορούν να αποφασίσουν να θεσπίσουν ακόμη πιο αυστηρούς κανόνες.⁷⁷

Προκειμένου να διασφαλιστεί ότι τα συστήματα αυτά χρησιμοποιούνται κατά τρόπο υπεύθυνο και αναλογικό, είναι επίσης σημαντικό να καθοριστεί ότι, σε καθεμία από αυτές τις εξαντλητικά απαριθμούμενες και αυστηρά καθορισμένες περιπτώσεις, θα πρέπει να λαμβάνονται υπόψη ορισμένα στοιχεία, όπως η σοβαρότητα και το μέγεθος της απειλούμενης βλάβης σε περίπτωση μη χρήσης του συστήματος και δεύτερον οι πιθανές επιπτώσεις και η έκταση της παρέμβασης στα δικαιώματα και στις ελευθερίες των επηρεαζόμενων προσώπων. Τέλος, η χρήση των συστημάτων αυτών επιτρέπεται αποκλειστικά και μόνο για την επαλήθευση συγκεκριμένων ατόμων - στόχων, ενώ και τα δεδομένα αναφοράς που χρησιμοποιούνται για τη σύγκριση πρέπει να είναι απόλυτα συναφή με την εκάστοτε υπόθεση. Η χρήση των συστημάτων αυτών πρέπει να περιορίζεται

⁷⁴ Αιτιολογική σκέψη 35

⁷⁵ Αιτιολογική σκέψη 36

⁷⁶ Αιτιολογική σκέψη 37

⁷⁷ Άρθρο 5(5) της Πράξης για την ΤΝ

στο απολύτως απαραίτητο μέτρο, με σαφή χρονικό και γεωγραφικό προσδιορισμό, βασισμένη σε συγκεκριμένες ενδείξεις ή αποδεικτικά στοιχεία, αφού πρότερα έχει διενεργηθεί σχετική εκτίμηση επιπτώσεων στα θεμελιώδη δικαιώματα και η επίσημη καταχώριση του συστήματος στη σχετική βάση δεδομένων.

Σύμφωνα με την Πράξη για την Τεχνητή Νοημοσύνη, η χρήση συστημάτων βιομετρικής ταυτοποίησης σε «πραγματικό χρόνο» προϋποθέτει την ενημέρωση τόσο της αρχής εποπτείας της αγοράς όσο και της ΑΠΔΠΧ. Ειδικότερα, βάσει του άρθρου 74 παρ. 8 του Κανονισμού, για τα συστήματα υψηλού κινδύνου που χρησιμοποιούνται για σκοπούς επιβολής του νόμου, τα Κράτη Μέλη δύναται να ορίσουν ως αρχές εποπτείας της αγοράς τις αρμόδιες εποπτικές αρχές προστασίας δεδομένων (βάσει του Κανονισμού 2016/679 ή της Οδηγίας 2016/680). Στην ελληνική πραγματικότητα, ωστόσο, μια τέτοια ενδεχόμενη συνένωση ρόλων υπό τη δράση της ΑΠΔΠΧ, η οποία θα καλούταν να αποτελέσει το μοναδικό σημείο επαφής για το κοινό και τους αντίστοιχους φορείς σε επίπεδο κράτους μέλους και Ένωσης, πιθανόν θα προκαλούσε δυσανάλογη διοικητική επιβάρυνση στην εν λόγω ανεξάρτητη αρχή, επιφορτίζοντάς την με αρμοδιότητες που εκτείνονται πολύ πέραν της αμιγούς τεχνογνωσίας της. Λαμβάνοντας υπόψη τις ανωτέρω παραμέτρους και με γνώμονα τη βαρύτητα της επέμβασης στα θεμελιώδη δικαιώματα, κατά την άποψη της γράφουσας κρίνεται βέλτιστη η υιοθέτηση ενός «υβριδικού» μοντέλου. Στο πλαίσιο αυτό, η σχετική γνωμοδότηση περί χρήσης ή μη των εν λόγω συστημάτων θα μπορούσε να εξάγεται συνεργατικά, αφενός από την ΑΠΔΠΧ και αφετέρου από άλλες υφιστάμενες ανεξάρτητες αρχές με συναφή τεχνογνωσία, όπως για παράδειγμα από την ΑΔΑΕ. Μέσω αυτής της θεσμικής σύμπραξης, οι εν λόγω φορείς θα μπορούσαν να αναλάβουν ρόλο τεχνικού θεματοφύλακα, περιφρουρώντας την όλη διαδικασία απέναντι στους εγγενείς κινδύνους των βιομετρικών συστημάτων.

Τέλος, αξίζει να αναφερθεί ότι η εν λόγω απαγόρευση που θεσπίζεται στο Άρθρο 5 παρ. 1 η) είναι εφαρμοστέα μόνο στους φορείς εφαρμογής τέτοιων συστημάτων, ενώ η διάθεση στην αγορά ή η χρήση άλλων μορφών βιομετρικής τεχνολογίας δεν απαγορεύεται κανονιστικά. Αντίθετα, οι δραστηριότητες αυτές, σύμφωνα με το Άρθρο 6 παράγραφος 2 και το Παράρτημα III, εντάσσονται στην κατηγορία των συστημάτων υψηλού κινδύνου, υπαγόμενες στις αντίστοιχες αυστηρές υποχρεώσεις συμμόρφωσης. Σημειώνεται επίσης ότι ακόμη και στις εξαιρετικές περιπτώσεις όπου ένα κράτος μέλος επιτρέπει τη χρήση RBI σε

πραγματικό χρόνο για την επίτευξη των τριών περιοριστικά αναφερόμενων στόχων του Αρθρου 5, η χρήση αυτή οφείλει να πληροί σωρευτικά όλες τις προδιαγραφές που ορίζονται για τα συστήματα TN υψηλού κινδύνου.

4.4 Βιομετρική ταυτοποίηση σε μεταγενέστερο χρόνο (post-remote biometric identification)

Στον αντίποδα της βιομετρικής ταυτοποίησης σε πραγματικό χρόνο (real-time), η Πράξη για την TN ρυθμίζει διακριτά και τη χρήση συστημάτων εξ αποστάσεως ταυτοποίησης σε μεταγενέστερο χρόνο. Τα τελευταία διαφέρουν από τα συστήματα πραγματικού χρόνου ως προς το ότι αναλύουν βιομετρικά δεδομένα εκ των υστέρων. Η πρακτική αυτή, εν αντιθέσει με τη βιομετρική ταυτοποίηση σε πραγματικό χρόνο, δεν εμπίπτει στο πεδίο των απαγορευμένων πρακτικών, αλλά κατηγοριοποιείται ως σύστημα «υψηλού κινδύνου»⁷⁸, με την ρητή εξαίρεση των συστημάτων που προορίζονται αποκλειστικά για βιομετρική εξακρίβωση, όπως ήδη αναφέρθηκε⁷⁹. Η κατηγοριοποίηση ως σύστημα «υψηλού κινδύνου» επεκτείνεται επίσης και σε άλλες ευαίσθητες βιομετρικές τεχνολογίες, όπως τα συστήματα βιομετρικής κατηγοριοποίησης και τα συστήματα αναγνώρισης συναισθημάτων, τα οποία θεωρούνται υψηλού κινδύνου λόγω της δυνατότητάς τους να προσβάλλουν τα θεμελιώδη δικαιώματα, η ανάλυση των οποίων όμως δεν αποτελεί αντικείμενο της παρούσας.

Για να γίνει κατανοητή η έννοια των εν λόγω συστημάτων, επισημαίνεται ότι τα συστήματα βιομετρικής ταυτοποίησης σε μεταγενέστερο χρόνο καλύπτουν όλες τις λοιπές περιπτώσεις, καθώς ορίζονται ως «συστήματα βιομετρικής ταυτοποίησης από απόσταση πλην των συστημάτων πραγματικού χρόνου». Η Αιτιολογική Σκέψη 17 διευκρινίζει ότι, στο πλαίσιο του εκ των υστέρων RBI, τα δεδομένα επί των οποίων διενεργείται η ταυτοποίηση «έχουν ήδη ληφθεί και η σύγκριση και η ταυτοποίηση συμβαίνουν μόνο μετά από σημαντική καθυστέρηση». Στις Κατευθυντήριες Γραμμές της, η Ευρωπαϊκή Επιτροπή θεωρεί ότι η διαφορά μεταξύ «πραγματικού χρόνου» και «μεταγενέστερης» επεξεργασίας είναι χρονική και προσδιορίζει ότι «μια καθυστέρηση είναι σημαντική τουλάχιστον όταν το άτομο είναι πιθανό να έχει εγκαταλείψει τον χώρο όπου ελήφθησαν τα βιομετρικά δεδομένα».

⁷⁸ Άρθρο 6(2) TN

⁷⁹ Παράρτημα III, 1, α) TN

Αν και ο πραγματικός χρόνος δεν μπορεί να οριστεί από τεχνική άποψη, το κριτήριο που επέλεξε η Ευρωπαϊκή Επιτροπή ενδέχεται να εγείρει ερμηνευτικά ζητήματα, ειδικά εάν οι τεχνολογίες χρησιμοποιούνται κατά τη διάρκεια ενός γεγονότος που διαρκεί (π.χ. ένα φεστιβάλ, μια διαδήλωση). Εναλλακτικά, η διάκριση μεταξύ πραγματικού χρόνου και μεταγενέστερου γεγονότος θα μπορούσε να συνδεθεί με την αποθήκευση (ή την έλλειψη αυτής) των δεδομένων που χρησιμοποιούνται για σκοπούς σύγκρισης. Οι περιπτώσεις όπου τα βιομετρικά δεδομένα αποθηκεύονται για σκοπούς σύγκρισης (π.χ. καταγεγραμμένες ροές βίντεο) θα μπορούσαν να θεωρηθούν «μεταγενέστερη» ανάπτυξη, ενώ οι περιπτώσεις όπου τα βιομετρικά δεδομένα συγκρίνονται άμεσα, δηλαδή χωρίς να αποθηκεύονται, θα μπορούσαν να θεωρηθούν ως «πραγματικού χρόνου».⁸⁰

Η χρήση των εν λόγω συστημάτων εξ αποστάσεως βιομετρικής ταυτοποίησης σε μεταγενέστερο χρόνο από τις αρχές επιβολής του νόμου υπόκειται σε αυστηρές εγγυήσεις. Ειδικότερα, για τη στοχευμένη αναζήτηση υπόπτων ή καταδικασθέντων, ο φορέας εκμετάλλευσης οφείλει να λάβει εκ των προτέρων άδεια από δικαστική ή ανεξάρτητη διοικητική αρχή, η οποία εκδίδει δεσμευτική και δικαστικά ελεγχόμενη απόφαση. Σε επείγουσες περιπτώσεις, η άδεια μπορεί να ζητηθεί εντός 48 ωρών, ενώ η μόνη εξαίρεση από την υποχρέωση αδειοδότησης αφορά την αρχική ταυτοποίηση δυνητικού υπόπτου βάσει αντικειμενικών στοιχείων που συνδέονται άμεσα με το αδίκημα.⁸¹ Σε περίπτωση απόρριψης του αιτήματος, η χρήση του συστήματος διακόπτεται πάραυτα και τα σχετικά δεδομένα προσωπικού χαρακτήρα διαγράφονται οριστικά.

Από τα ανωτέρω γίνεται κατανοητό ότι και τα συστήματα εκ των υστέρων βιομετρικής ταυτοποίησης δεν μπορούν να χρησιμοποιούνται αδιακρίτως, δηλαδή χωρίς σύνδεση με ποινικό αδίκημα, ποινική διαδικασία, πραγματική απειλή ποινικού αδικήματος ή αναζήτηση συγκεκριμένου αγνοουμένου. Επιπλέον, η χρήση πρέπει να είναι περιορισμένη ως προς την τοποθεσία και το χρονικό εύρος, και να συνδέεται με ένα «κλειστό σύνολο δεδομένων νομίμως αποκτηθέντος οπτικοακουστικού υλικού». Περιορίζοντας τη χρήση της σε σαφώς καθορισμένες περιπτώσεις, όπου είναι «αυστηρώς αναγκαίο» για σκοπούς έρευνας, η

⁸⁰ Jasserand, C. (2025) 'Facial Recognition in Public Spaces and the Principle of Necessity', in Menéndez González, N. and Mobilio, G. (eds.) *Next Democratic Frontiers for Facial Recognition Technology (FRT): The Legal, Ethical and Democratic Implications of FRT*. Cham: Springer, pp. 49–69.

⁸¹ Άρθρο 26 (10) TN

διάταξη αυτή στοχεύει στην αποτροπή της μαζικής επιτήρησης και στην ανάπτυξη συστημάτων αναγνώρισης προσώπου που θα μπορούσαν να παραβιάσουν την ιδιωτική ζωή των ατόμων, χωρίς να διαθέτουν επαρκή αιτιολόγηση.

Επιπροσθέτως, τα αποτελέσματα που παράγονται από τα εν λόγω συστήματα δεν επιτρέπεται να αποτελούν τη μοναδική βάση για τη λήψη αποφάσεων που επιφέρουν δυσμενείς έννομες συνέπειες στα υποκείμενα των δεδομένων. Για παράδειγμα, οι αρχές επιβολής του νόμου δεν μπορούν να βασιστούν αποκλειστικά και μόνο στα αποτελέσματα της ΤΝ για να συλλάβουν ή να απαγγείλουν κατηγορίες σε κάποιον, αναγνωρίζοντας την πιθανότητα ανακριβειών ή μεροληψίας στα αποτελέσματα αυτά. Αυτή η δικλίδα ασφαλείας εγγυάται ότι οι κρίσιμες αποφάσεις που επηρεάζουν τη ζωή και τις ελευθερίες των ατόμων βασίζονται σε ένα ευρύτερο αποδεικτικό πλαίσιο και όχι αποκλειστικά σε αλγοριθμικές ενδείξεις, οι οποίες ενδέχεται να παράγουν εσφαλμένα αποτελέσματα (ψευδώς θετικά ή αρνητικά).

Όπως προαναφέρθηκε, τα συστήματα βιομετρικής ταυτοποίησης σε μεταγενέστερο χρόνο ταξινομούνται ως «υψηλού κινδύνου» και, ως εκ τούτου, υπάγονται σε αυστηρό κανονιστικό πλαίσιο, το οποίο επιτάσσει, μεταξύ άλλων, τη διενέργεια εκτίμησης αντικτύπου στα θεμελιώδη δικαιώματα (FRIA).⁸² Στο νομοθετικό κείμενο για την ΤΝ περιλαμβάνονται επίσης μέτρα διαφάνειας και λογοδοσίας. Περαιτέρω, καθίσταται υποχρεωτική η τεκμηρίωση κάθε χρήσης βιομετρικής ταυτοποίησης σε μεταγενέστερο χρόνο εντός του οικείου αστυνομικού φακέλου, διασφαλίζοντας παράλληλα ότι τα στοιχεία αυτά θα είναι προσβάσιμα στις αρχές εποπτείας της αγοράς και προστασίας δεδομένων κατόπιν σχετικού αιτήματος. Επιπλέον, οι αρχές επιβολής του νόμου υπέχουν υποχρέωση υποβολής ετήσιων εκθέσεων προς τις αρμόδιες εποπτικές αρχές, με αντικείμενο τη χρήση συστημάτων βιομετρικής ταυτοποίησης.

Τέλος, διασαφηνίζεται από το γράμμα του Νόμου ότι και σε αυτά τα συστήματα πρέπει να έχει προηγηθεί θέσπιση σχετικής εθνικής νομοθεσίας. Συμπερασματικά και εξ αντιδιαστολής των όσων αναφέρθηκαν, όσα συστήματα ΤΝ χρησιμοποιούνται για σκοπούς επιβολής του νόμου και δεν εμπίπτουν στις απαγορεύσεις ούτε ταξινομούνται ως υψηλού κινδύνου, θεωρούνται ελάχιστου κινδύνου και διέπονται από εύελικτα, κυρίως εθελοντικά

⁸² Άρθρο 27 (1) ΤΝ

πρότυπα. Αυτή η προσέγγιση είναι κρίσιμης σημασίας λόγω της απουσίας ειδικών (ad hoc) κανόνων που να διέπουν την αυτοματοποιημένη επιβολή του νόμου και την αξιοποίηση των αποτελεσμάτων της στην ποινική δικαιοσύνη.

5 ΣΧΕΣΗ ΤΗΣ ΠΡΑΞΗΣ ΓΙΑ ΤΗΝ ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ ΜΕ ΑΛΛΑ ΝΟΜΟΘΕΤΙΚΑ ΚΕΙΜΕΝΑ – ΑΛΛΗΛΕΠΙΔΡΑΣΗ ΜΕ ΓΚΠΔ ΚΑΙ ΟΔΗΓΙΑ (ΕΕ) 2016/680

Όπως αναφέρθηκε στην προηγούμενη ενότητα, η ανάπτυξη της Τεχνολογίας Αναγνώρισης Προσώπου από τις αρχές επιβολής του νόμου στην ΕΕ υπόκειται σε μια σύνθετη ρυθμιστική αρχιτεκτονική, η οποία επιδιώκει τη χρυσή τομή μεταξύ της αποτελεσματικής αστυνόμευσης και της προστασίας των θεμελιωδών δικαιωμάτων. Το πλαίσιο αυτό δομείται σε τρεις συμπληρωματικούς πυλώνες, οι οποίοι παρουσιάζονται ακολούθως βάσει χρονολογικής σειράς. Πρώτος πυλώνας είναι ο ΓΚΠΔ θεσπίζοντας τις γενικές αρχές επεξεργασίας και τις εγγυήσεις για τα ευαίσθητα δεδομένα (π.χ. διεξαγωγή εκτίμησης αντικτύπου) και εν συνεχεία ακολουθεί η LED εξειδικεύοντας τους κανόνες στο πεδίο της αστυνομικής δράσης, θέτοντας ως φίλτρο τις αρχές της αναγκαιότητας και αναλογικότητας. Τελευταίος πυλώνας είναι η Πράξη για την ΤΝ που εισάγει την παράμετρο της προϊόντικής ασφάλειας, επιβάλλοντας αυστηρές δικλίδες στους παρόχους των συστημάτων «υψηλού κινδύνου» και απαγορεύοντας συγκεκριμένες πρακτικές, ως επιβλαβείς για τα ατομικά δικαιώματα.

Μολονότι το θεσμικό πλαίσιο εμφανίζεται πλήρες, η αποσπασματική θεώρηση των επιμέρους νομοθετημάτων τείνει να επισκιάζει τις κρίσιμες μεταξύ τους αλληλεπιδράσεις. Υπό το πρίσμα αυτό, η παρούσα ανάλυση υιοθετεί μια ολιστική προσέγγιση, αναγνωρίζοντας ότι ο κανονιστικός κατακερματισμός επιφέρει σημαντικό ερμηνευτικό βάρος στις αρχές εφαρμογής του νόμου. Κατά συνέπεια, κρίνεται επιβεβλημένη η συγκριτική επισκόπηση των σχετικών κανόνων, προκειμένου να εντοπιστούν ασάφειες ή πιθανές συγκρούσεις που ενδέχεται να διακυβεύσουν την ασφάλεια δικαίου, αλλά και να θέσουν σε κίνδυνο το θεμελιώδες δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα, όπως ορίζεται στο άρθρο 16 της ΣΛΕΕ και στο άρθρο 8 του Χάρτη.

5.1 Γενικός Κανονισμός Προστασίας Δεδομένων

Όπως προαναφέρθηκε στην Ενότητα 2, ο ΓΚΠΔ ορίζει τα βιομετρικά δεδομένα στο άρθρο 4 παρ. 14, εντάσσοντάς τα στις ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα. Ως εκ τούτου, η επεξεργασία τους απαγορεύεται κατ' αρχήν, βάσει του άρθρου 9 παρ. 1, υπό την

επιφύλαξη των περιοριστικά απαριθμούμενων εξαιρέσεων της παραγράφου 2 του ίδιου άρθρου.

Το σκεπτικό πίσω από τη διαφορετική ρύθμιση ορισμένων κατηγοριών δεδομένων προσωπικού χαρακτήρα εδράζεται στην παραδοχή ότι η μη εξουσιοδοτημένη χρήση τους δύναται να έχει σοβαρότερες και συχνά μη αναστρέψιμες συνέπειες για τα θεμελιώδη δικαιώματα του ατόμου, σε αντιδιαστολή με την αθέμιτη χρήση των απλών δεδομένων. Ειδικότερα, δεδομένα που αποκαλύπτουν πτυχές της ανθρώπινης ζωής όπως την υγεία, τον σεξουαλικό προσανατολισμό, τη φυλετική ή εθνοτική καταγωγή ενδέχεται, εάν δημοσιοποιηθούν ή χρησιμοποιηθούν αθέμιτα, να επιφέρουν δυσμενείς επιπτώσεις με μακροχρόνια επίδραση όχι μόνο στο ίδιο το υποκείμενο των δεδομένων, αλλά και στο κοινωνικό του περιβάλλον, επηρεάζοντας την κοινωνική του ένταξη, την επαγγελματική πορεία, ακόμα και την προσωπική του αυτονομία.

Σύμφωνα με τις παρατηρήσεις του ΕΣΠΔ, η λειτουργία βιομετρικών συστημάτων σε μη ελεγχόμενα περιβάλλοντα εγείρει σημαντικά ζητήματα συμβατότητας με το ισχύον κανονιστικό πλαίσιο. Κατά τη διαδικασία αυτή, οι κάμερες καταγράφουν αδιακρίτως τα χαρακτηριστικά προσώπου όλων των ατόμων που εισέρχονται στο πεδίο λήψης, συμπεριλαμβανομένων εκείνων που δεν έχουν παράσχει τη συγκατάθεσή τους. Η τεχνική αναγκαιότητα δημιουργίας βιομετρικών προτύπων για το σύνολο των διερχομένων, προκειμένου αυτά να αντιπαραβληθούν με τα πρότυπα των εγγεγραμμένων -στη βάση αναφοράς- χρηστών για σκοπούς διαχωρισμού και ταυτοποίησης, συνιστά επεξεργασία ευαίσθητων προσωπικών δεδομένων. Ως εκ τούτου, δεδομένου ότι ο αντικειμενικός σκοπός είναι η αδιαμφισβήτητη ταυτοποίηση φυσικών προσώπων, η εν λόγω πρακτική καθίσταται σύλληψη μόνο εάν πληρούνται μία από τις ειδικές εξαιρέσεις που προβλέπονται στο Άρθρο 9 παρ. 2 του ΓΚΠΔ για κάθε υποκείμενο των δεδομένων που εκτίθεται στην επιτήρηση.

Είναι σημαντικό να επισημανθεί ότι εκτός από τις ειδικές ως άνω απαιτήσεις θα πρέπει να εφαρμόζονται και οι γενικές αρχές νόμιμης επεξεργασίας κατ' άρθρο 5 του ΓΚΠΔ. Ειδικότερα, θα πρέπει να λαμβάνεται υπόψη η αρχή της νομιμότητας, αντικειμενικότητας και διαφάνειας, η αρχή του περιορισμού του σκοπού, η αρχή της ελαχιστοποίησης των δεδομένων, της ακρίβειας, του περιορισμού της περιόδου αποθήκευσης και τέλος της ακεραιότητας και εμπιστευτικότητας. Ως εκ τούτου η κρίση περί της νομιμότητας της επεξεργασίας των εν λόγω δεδομένων και περί συνδρομής μίας εκ των εξαιρέσεων του αρ.

9 (2) του ΓΚΠΔ εναπόκειται πλέον στον υπεύθυνο επεξεργασίας, ο οποίος θα πρέπει -σε συνεργασία με τον υπεύθυνο προστασίας δεδομένων- να βρει την κατάλληλη προς εφαρμογή νομική βάση τηρώντας παράλληλα τις αρχές της επεξεργασίας και τα κατάλληλα τεχνικά και οργανωτικά μέτρα για τη διασφάλιση των θεμελιωδών δικαιωμάτων και συμφερόντων του υποκειμένου των δεδομένων και αφετέρου να είναι σε θέση να αποδείξουν τη συμμόρφωσή τους με τα ανωτέρω. Έτσι, γίνεται κατανοητό ότι υπό το υφιστάμενο νομοθετικό πλαίσιο καταργείται το καθεστώς της προηγούμενης άδειας της ΑΠΔΠΧ για την επεξεργασία των ειδικών κατηγοριών δεδομένων.⁸³

Η πρακτική των εποπτικών αρχών επιβεβαιώνει την ανωτέρω ανυσημία. Οι αποφάσεις της CNIL και της σουηδικής Datainspektionen καταδεικνύουν ότι ακόμη και όταν δεν αμφισβητείται ευθέως η νομική βάση της επεξεργασίας, η χρήση αναγνώρισης προσώπου μπορεί να κριθεί παράνομη λόγω παραβίασης των αρχών της αναγκαιότητας και της αναλογικότητας. Παράλληλα, η υποχρέωση διενέργειας Εκτίμησης Αντικτύπου (DPIA) κατά το άρθρο 35 ΓΚΠΔ αναδεικνύεται σε κρίσιμο μηχανισμό πρόληψης, χωρίς ωστόσο να εξαλείφεται ο κίνδυνος η αξιολόγηση να παραμείνει σε μεγάλο βαθμό αυτοαναφορική και ελλιπώς ελεγχόμενη.

Ωστόσο, η κανονιστική προσέγγιση του ΓΚΠΔ, αν και αυστηρή σε θεωρητικό επίπεδο, εγείρει σημαντικά ερωτήματα ως προς την πρακτική της επάρκεια έναντι των σύγχρονων συστημάτων αναγνώρισης προσώπου που βασίζονται στην τεχνητή νοημοσύνη. Τα λεγόμενα βιομετρικά συστήματα «δεύτερου κύματος» λειτουργούν σε μεγάλη κλίμακα, με υψηλό βαθμό αυτοματοποίησης και δυνατότητα εξαγωγής δευτερογενών πληροφοριών, γεγονός που δυσχεραίνει την εφαρμογή βασικών αρχών του ΓΚΠΔ, όπως ο περιορισμός του σκοπού και η ελαχιστοποίηση των δεδομένων. Η ρητή συγκατάθεση ως συχνότερη εξαίρεση του άρθρου 9 παρ. 2 ΓΚΠΔ αποδεικνύεται συχνά προβληματική, ιδίως σε περιβάλλοντα ανισορροπίας ισχύος ή παθητικής επιτήρησης, όπου η συγκατάθεση δεν μπορεί να θεωρηθεί ουσιαστικά ελεύθερη⁸⁴.

⁸³ Ε. Βασιλακοπούλου (2021) Βιομετρικά και Γενετικά δεδομένα, Γενικός Κανονισμός για την Επεξεργασία Προσωπικών δεδομένων, Νομική διάσταση και πρακτική εφαρμογή, Νομική Βιβλιοθήκη

⁸⁴ Μ. Σκόνδρα (2020) Συστήματα Βιντεοεπιτήρησης, αναγνώριση προσώπου και Προστασία Προσωπικών Δεδομένων, Μελέτες Γνωμοδοτήσεις, σελ. 53 επ.

Σε αυτό το πνεύμα κινείται και η Γνώμη 6/2014 της Ομάδας Εργασίας του άρθρου 29 επισημαίνοντας 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)»⁸⁵.

Συμπερασματικά, οι ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα δεν θα πρέπει να υποβάλλονται σε επεξεργασία εκτός και εάν εφαρμόζεται κάποια εκ των εξαιρέσεων, ήτοι αφορούν συμμόρφωση με έννομη υποχρέωση ή εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας. Παρεκκλίσεις από τη γενική απαγόρευση επεξεργασίας δεδομένων προσωπικού χαρακτήρα που υπάγονται στις εν λόγω ειδικές κατηγορίες θα πρέπει να προβλέπονται ρητώς, μεταξύ άλλων, σε περίπτωση ρητής συγκατάθεσης του υποκειμένου των δεδομένων. Μάλιστα, η επεξεργασία αυτή πρέπει να λαμβάνει χώρα βάσει του δικαίου της ΕΕ ή των κρατών μελών, με την τήρηση των απαιτήσεων αναλογικότητας, με σεβασμό στην προστασία των δεδομένων, με τις κατάλληλες και επαρκείς εγγυήσεις και υπό την προϋπόθεση αυστηρής αναγκαιότητας και πλήρους αιτιολογίας για την εν λόγω επεξεργασία.⁸⁶

⁸⁵ Γνώμη 6/2014 σχετικά με την έννοια των εννόμων συμφερόντων του υπευθύνου επεξεργασίας κατ' άρθρο 7 της Οδηγίας 95/46 σελ. 14. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_el.pdf

⁸⁶ Ευρωπαϊκή Επιτροπή, Λευκή Βίβλος, Τεχνητή νοημοσύνη - Η ευρωπαϊκή προσέγγιση της αριστείας και της εμπιστοσύνης, διαθέσιμο σε : <https://op.europa.eu/el/publication-detail/-/publication/ac957f13-53c6-11ea-aece-01aa75ed71a1/language-el> [Πρόσβαση 6/2025]

5.2 Οδηγία (ΕΕ) 2016/680 για την επιβολή του νόμου (LED)

5.2.1 Ιστορικό Πλαίσιο και Διάκριση από άλλα νομοθετήματα

Η προστασία των δεδομένων εξειδικεύεται περαιτέρω από το παράγωγο δίκαιο της ΕΕ, συγκεκριμένα από τον ΓΚΠΔ, όπως αναφέρθηκε, και την Οδηγία 2016/680 («Οδηγία για την επιβολή του νόμου» ή αλλιώς «LED»), η οποία αποτελεί το ειδικό νομικό πλαίσιο για την προστασία των δεδομένων στον τομέα της επιβολής του νόμου. Η LED εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης και δίωξης ποινικών αδικημάτων και της εκτέλεσης ποινικών κυρώσεων⁸⁷. Παρά το γεγονός ότι η δικαιοδοσία της Ευρωπαϊκής Ένωσης στον τομέα του ουσιαστικού ποινικού δικαίου των κρατών μελών παραμένει περιορισμένη, η ΕΕ δύναται να θεσπίζει κανονιστικά πλαίσια ερειδόμενη στην αρμοδιότητά της για την προστασία των δεδομένων προσωπικού χαρακτήρα⁸⁸. Η LED, δυνάμει της νομικής της φύσης, απαιτεί τη μεταφορά της στο εθνικό δίκαιο των κρατών μελών, διατηρώντας παράλληλα τον δεσμευτικό της χαρακτήρα ως προς το επιδιωκόμενο αποτέλεσμα. Με τον τρόπο αυτό, εγκαθιδρύει τις γενικές αρχές και προϋποθέσεις για την επεξεργασία δεδομένων, οι οποίες καταλαμβάνουν και τη χρήση συστημάτων αναγνώρισης προσώπου από τις αρχές επιβολής του νόμου⁸⁹.

Η Οδηγία τέθηκε σε ισχύ στις 5 Μαΐου του 2016 και αντικατέστησε το προηγούμενο νομικό πλαίσιο της απόφασης 2008/977/ΔΕΥ του Συμβουλίου⁹⁰ σχετικά με την προστασία προσωπικών δεδομένων στο πλαίσιο της αστυνομικής και δικαστικής συνεργασίας σε ποινικές υποθέσεις.⁹¹ Όπως ο Κανονισμός 2016/679 έτσι και η Οδηγία 2016/680 που

⁸⁷ Άρθρο 1 (1) LED

⁸⁸ Άρθρο 16 ΣΛΕΕ

⁸⁹ Simmler, M. και Canova, G. (2020) 'Facial recognition technology in law enforcement: Regulating data analysis of another kind', *Computer Law & Security Review*, 39, άρθρο 105494.

⁹⁰ Απόφαση πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου της 27^{ης} Νοεμβρίου 2008 για την προστασία των δεδομένων προσωπικού χαρακτήρα που τυγχάνουν επεξεργασίας στο πλαίσιο της αστυνομικής και δικαστικής συνεργασίας σε ποινικές υποθέσεις

⁹¹ Salami, Emmanuel, The Impact of Directive (EU) 2016/680 on the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties and on the Free Movement of Such Data on the

υιοθετήθηκαν από κοινού το έτος 2016, επιχείρησαν να φέρουν σημαντικές βελτιώσεις στο προϋφιστάμενο νομικό καθεστώς όσον αφορά την προστασία προσωπικών δεδομένων. Είναι χαρακτηριστικό ότι, σύμφωνα με την Πρώτη έκθεση αξιολόγησης της Ευρωπαϊκής Επιτροπής που δημοσιεύθηκε στις 22 Ιουλίου 2022, 19 κράτη-μέλη, μεταξύ των οποίων και η Ελλάδα, είχαν παραλείψει να μεταφέρουν την Οδηγία 2016/680 στο εθνικό δίκαιο έως τις 6 Μαΐου 2018. Η ενσωμάτωσή της έγινε με καθυστέρηση, εντός του 2019, με το ν. 4624/2019, ως τροποποιήθηκε με τον Ν. 5002/2022, αφήνοντας αδιευκρίνιστα αρκετά ζητήματα, και αφού η Επιτροπή είχε κινήσει διαδικασίες επί παραβάσει του ενωσιακού δικαίου κατά αρκετών χωρών, μεταξύ των οποίων και κατά της Ελλάδας.⁹²

Μια από τις σημαντικότερες καινοτομίες της Οδηγίας σε σχέση με το προϋφιστάμενο νομοθετικό καθεστώς (Οδηγία 95/46/EK) είναι η ρητή συμπερίληψη των βιομετρικών και γενετικών δεδομένων στις ειδικές κατηγορίες δεδομένων (Άρθρο 10), τα οποία επιτρέπουν την αδιαμφισβήτητη ταυτοποίηση ενός φυσικού προσώπου. Το σκεπτικό αυτής της προσθήκης εκκινεί από τη νομολογία και συγκεκριμένα από την απόφαση του Ευρωπαϊκού Δικαστηρίου Δικαιωμάτων του Ανθρώπου (ΕΔΔΑ) στην υπόθεση *S. και Marper* κατά Ηνωμένου Βασιλείου. Το ΕΔΔΑ στην εν λόγω υπόθεση έκρινε ότι η διατήρηση κυτταρικών δειγμάτων, προφίλ DNA και δακτυλικών αποτυπωμάτων ατόμων που ήταν μεν ύποπτοι τέλεσης ποινικού αδικήματος αλλά δεν είχαν καταδικαστεί, συνιστούσε παρέμβαση στο δικαίωμα της ιδιωτικής ζωής.

Καθίσταται σαφές ότι η LED λειτουργεί ως ειδικότερο πλαίσιο (*lex specialis*) που συμπληρώνει τον ΓΚΠΔ, ωστόσο η αυστηρή οριοθέτησή τους παραμένει μία σύνθετη πρόκληση. Η αυτή γνώμη έχει διατυπωθεί τόσο από την ομάδα εμπειρογνομόνων των κρατών⁹³, όσο και από το ΕΣΠΔ⁹⁴. Ως προς τα βιομετρικά δεδομένα τα δύο νομοθετήματα

Existing Privacy Regime (February 6, 2017). Available at SSRN: <https://ssrn.com/abstract=2912449> or <http://dx.doi.org/10.2139/ssrn.2912449>

⁹² Κανέλλος, Λ. (επιμ.) (2023) *The GDPR Handbook: Η κανονιστική συμμόρφωση στο εργασιακό και επιχειρησιακό περιβάλλον*. 2η έκδ. Αθήνα: Νομική Βιβλιοθήκη.

⁹³ Βλ. πρακτικά της συνεδρίασης της ομάδας εμπειρογνομόνων της Επιτροπής, της 5ης Μαΐου 2021, σχετικά με τον κανονισμό (ΕΕ) 2016/679 και την οδηγία (ΕΕ) 2016/680 <https://ec.europa.eu/transparency/expertgroupsregister/screen/meetings/consult?lang=el&meetingId=25283&fromExpertGroups=true>

⁹⁴ Συμβολή του ΕΣΠΔ στην αξιολόγηση της οδηγίας, σημείο 7.

ομοιάζουν και κινούνται προς την ίδια κατεύθυνση. Ειδικότερα, το Άρθρο 3(13) της LED υιοθετεί έναν ορισμό παρόμοιο με εκείνον του ΓΚΠΔ, υπάγοντας τα βιομετρικά δεδομένα στην ειδική κατηγορία των προσωπικών δεδομένων και επιβάλλοντας γενική απαγόρευση επεξεργασίας τους, η οποία κάμπτεται μόνο υπό τις αυστηρές προϋποθέσεις του Άρθρου 10.

5.2.2 Πεδίο εφαρμογής

Το πεδίο εφαρμογής της Οδηγίας αποτελείται από δύο βασικά στοιχεία: την έννοια της αρμόδιας αρχής (προσωπικό πεδίο) και την έννοια του ποινικού αδικήματος (καθ' ύλην πεδίο εφαρμογής), τα οποία (στοιχεία) πρέπει να συντρέχουν ταυτόχρονα.

Στον ορισμό της «**αρμόδιας αρχής**» κατά την Οδηγία περιλαμβάνονται είτε όργανα του κράτους, όπως διωκτικές και εισαγγελικές αρχές, υπηρεσίες εσωτερικής ασφάλειας και προστασίας του συντάγματος είτε ακόμα, κατά περίπτωση, σε ορισμένα άλλα κράτη-μέλη, και δημόσιοι ή ιδιωτικοί φορείς (π.χ. στην Ελλάδα από το τροποποιημένο άρθρο 44 περ. 1δ του Ν 4624/2019) που έχουν τον ρόλο δημόσιας αρχής και είναι επιφορτισμένοι με την εκτέλεση δημοσίων εξουσιών για σκοπούς πρόληψης, διερεύνησης, εξιχνίασης ή δίωξης ποινικών αδικημάτων ή εκτέλεση ποινικών κυρώσεων (π.χ. ιδιωτικές αστυνομίες, ιδιωτικές ή ημι-ιδιωτικές φυλακές κ.λπ). Οι αρχές αυτές θεωρούνται αρμόδιες βάσει της Οδηγίας όταν επεξεργάζονται προσωπικά δεδομένα για σκοπούς πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή εκτέλεσης ποινικών κυρώσεων, περιλαμβανομένης της προστασίας από απειλές κατά της δημόσιας ασφάλειας και της αποτροπής τους, με σεβασμό στην ειδική φύση των εν λόγω δραστηριοτήτων⁹⁵. Αντιθέτως, οποιαδήποτε άλλη επεξεργασία διενεργείται από τις αναφερόμενες αρχές για σκοπούς που δεν αφορούν στην Οδηγία και στο πλαίσιο επιβολής του νόμου (π.χ. σχετίζονται με διοικητικούς σκοπούς, όπως η επεξεργασία δεδομένων προσωπικού χαρακτήρα από μονάδες χρηματοοικονομικών πληροφοριών για την καταπολέμηση της νομιμοποίησης εσόδων) διέπεται από το κανονιστικό πλαίσιο του ΓΚΠΔ.

Με τον τρόπο αυτό, το δίκαιο της Ένωσης διασφαλίζει ότι η εφαρμογή της Οδηγίας περιορίζεται αυστηρά στο καθ' ύλην πεδίο της ποινικής καταστολής, αποτρέποντας τη χρήση της για γενικές διοικητικές λειτουργίες του κράτους. Σύμφωνα με το Άρθρο 1, η

⁹⁵ Αιτιολογική σκέψη 11

Οδηγία δεν εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα σε τομείς που δεν εμπίπτουν στο δίκαιο της Ένωσης, όπως η εθνική ασφάλεια. Επομένως, ερμηνευτικά πρέπει να γίνει δεκτό ότι δεν αφορά στρατονομικές υπηρεσίες, όπως η στρατονομία, η αερονομία και η ναυτονομία⁹⁶. Ομοίως, η Οδηγία εξαιρεί ρητά επεξεργασίες, οι οποίες διενεργούνται από τα θεσμικά και λοιπά ευρωπαϊκά όργανα και τους οργανισμούς της Ένωσης.

Το δεύτερο στοιχείο με κεντρική σημασία, ως αναφέρθηκε ανωτέρω, για την υπαγωγή μιας επεξεργασίας προσωπικών δεδομένων στο ρυθμιστικό πεδίο της Οδηγίας είναι ο προσδιορισμός της έννοιας του «**ποινικού αδικήματος**». Σύμφωνα με την πάγια νομολογία του ΔΕΕ, τρία κριτήρια είναι συναφή για την εκτίμηση του ποινικού χαρακτήρα μιας παράβασης: (i) αν η παράβαση χαρακτηρίζεται ως ποινική κατά το εθνικό δίκαιο, (ii) η φύση της παράβασης και (iii) ο βαθμός αυστηρότητας της κύρωσης η οποία επαπειλείται εις βάρος του ενδιαφερομένου⁹⁷. Η αξιόποινη πράξη θα πρέπει να αποτελεί αυτοτελή έννοια του δικαίου της Ένωσης⁹⁸. Αυτό συνεπάγεται ότι τα κράτη μέλη στερούνται της ευχέρειας να χαρακτηρίζουν μια παράβαση ως «ποινική» προσχηματικά, με αποκλειστικό στόχο την σκόπιμη υπαγωγή της στο πεδίο εφαρμογής της LED.

Όπως αναφέρθηκε, η επεξεργασία επιτρέπεται μόνο όταν προβλέπεται ρητά από τον νόμο ή όταν κρίνεται «απολύτως αναγκαία» (*strictly necessary*) για την προστασία ζωτικών συμφερόντων ή όταν αφορά δεδομένα που έχουν προδήλως δημοσιοποιηθεί από το ίδιο το υποκείμενο. Η απαίτηση αυτή της «απόλυτης αναγκαιότητας», σε συνδυασμό με την υποχρέωση παροχής κατάλληλων εγγυήσεων για τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων⁹⁹, υπογραμμίζει ότι η επεξεργασία τέτοιων δεδομένων δεν πρέπει να αποτελεί συνήθη πρακτική, λόγω του σοβαρού δυνητικού αντικτύπου στα δικαιώματα και τις ελευθερίες του ατόμου. Στην ίδια συλλογιστική, το άρθρο 11 της Οδηγίας

⁹⁶ Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης (2019) *Κανονισμός (ΕΕ) 2019/1896 της 13ης Νοεμβρίου 2019 για την Ευρωπαϊκή Συνοριοφυλακή και Ακτοφυλακή και για την κατάργηση των κανονισμών (ΕΕ) αριθ. 1052/2013 και (ΕΕ) 2016/1624*. Διαθέσιμο στο: <https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32019R1896> (Πρόσβαση: Φεβρουάριος 2026).

⁹⁷ Απόφαση της 22ας Ιουνίου 2021, Β κατά Latvijas Republikas Saeima, C-439/19, EU:C:2021:504, σκέψη 87

⁹⁸ αιτιολογική σκέψη 13 της Οδηγίας,

⁹⁹ Κατάλογος πιθανών διασφαλίσεων παρατίθεται στην αιτιολογική σκέψη 37 LED

απαγορεύει την αυτοματοποιημένη λήψη ατομικών αποφάσεων με έννομες συνέπειες για το άτομο (π.χ. σύλληψη, παραβίαση προσωπικών ή επαγγελματικών απορρήτων, περιορισμός ατομικών ελευθεριών).

Ως πρώτη θεμελιώδης προϋπόθεση για τη νομιμότητα της επεξεργασίας βιομετρικών δεδομένων, σύμφωνα με την LED (**Άρθρο 10, παρ. 1α**), αποτελεί η ύπαρξη ρητής νομικής βάσης στο ενωσιακό ή εθνικό δίκαιο. Το άρθρο 10 πρέπει να ερμηνεύεται σε συνδυασμό με το άρθρο 8 της Οδηγίας. Επομένως, εάν δεν προβλέπεται από το δίκαιο της Ένωσης, η επεξεργασία ειδικών κατηγοριών δεδομένων προϋποθέτει πάντα ειδική νομική βάση στο εθνικό δίκαιο. Η απαίτηση αυτή εναρμονίζεται πλήρως και με το Άρθρο 8 παρ. 2 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ, το οποίο επιτάσσει η επεξεργασία να διενεργείται για συγκεκριμένους σκοπούς και με βάση τη συγκατάθεση του ενδιαφερομένου ή για άλλους θεμιτούς λόγους που προβλέπονται από το νόμο. Όπως προκύπτει από τις Αιτιολογικές Σκέψεις 33 και 34 της LED, η αναγκαιότητα της επεξεργασίας συναρτάται άμεσα με την πρόληψη, διερεύνηση, ανίχνευση ή δίωξη ποινικών αδικημάτων ή εκτέλεση ποινικών κυρώσεων, σκοποί οι οποίοι οφείλουν να είναι σαφείς, νόμιμοι και προσδιορισμένοι ήδη κατά τον χρόνο της συλλογής των δεδομένων¹⁰⁰. Επισημαίνεται ότι μόνο η ενσωμάτωση του Άρθρου 10 της Οδηγίας στο εθνικό δίκαιο δεν συνεπάγεται ύπαρξη επαρκούς νομικής βάσης, καθώς απαιτείται ένας σαφής, δεσμευτικός κανόνας δικαίου που να προβλέπει εξειδικευμένες εγγυήσεις.

Αναφορικά με τη συγκατάθεση που εκτέθηκε ανωτέρω ως νόμιμη βάση επεξεργασίας κατά Άρθρο 8 παρ. 2 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ αλλά και σύμφωνα με τον ΓΚΠΔ λεκτέο ότι σε περιπτώσεις όπου οι αρμόδιες αρχές, στις οποίες ανατίθεται θεσμικά από το νόμο η εκτέλεση των καθηκόντων πρόληψης, διερεύνησης ανίχνευσης ή δίωξης ποινικών αδικημάτων και οι οποίες έχουν τη δυνατότητα να απαιτούν από φυσικά πρόσωπα ή να δίνουν εντολή σε αυτά να συμμορφωθούν προς τα σχετικά αιτήματα, δεν θα πρέπει να χρησιμοποιούν ως νομική βάση για την επεξεργασία τη συγκατάθεση του υποκειμένου των δεδομένων. Και αυτό διότι όταν το υποκείμενο των δεδομένων υποχρεούται να συμμορφωθεί

¹⁰⁰ Αιτιολογική σκέψη 26

προς νομική υποχρέωση δεν έχει ουσιαστικά ελεύθερη επιλογή και κατά συνέπεια η αντίδρασή του δεν μπορεί να θεωρηθεί ως εκδήλωση ελεύθερης βούλησης¹⁰¹.

Από νομολογιακή άποψη παρατηρείται ότι απουσιάζει ο διαχωρισμός των εννοιών «απαραίτητη» του Άρθρου 8 και «απολύτως αναγκαίες» του Άρθρου 10. Ειδικότερα, η υπόθεση «Digital Rights Ireland» επιβεβαιώνει την πάγια θέση του ΔΕΕ ότι κάθε περιορισμός στην προστασία δεδομένων πρέπει να περιορίζεται στον «απολύτως αναγκαίο» βαθμό¹⁰². Στο πλαίσιο αυτό, η Ομάδα Εργασίας του Άρθρου 29 υπογραμμίζει ότι η διατύπωση του Άρθρου 10 αποσκοπεί στην τήρηση της αρχής της αναγκαιότητας όταν πρόκειται για ειδικές κατηγορίες δεδομένων, απαιτώντας μια ιδιαίτερα τεκμηριωμένη αιτιολόγηση της επεξεργασίας των εν λόγω δεδομένων¹⁰³. Η νομολογία του ΔΕΕ επιβεβαιώνει αυτή την προσέγγιση, αλλά θέτει ακόμα υψηλότερο όριο αναγκαιότητας για την επεξεργασία ευαίσθητων δεδομένων από τις αστυνομικές αρχές.¹⁰⁴ Ως εκ τούτου, η επεξεργασία ευαίσθητων πληροφοριών απαιτεί μια λεπτή στάθμιση μεταξύ ιδιωτικότητας και δημοσίου συμφέροντος, η οποία, κατά την Ομάδα Εργασίας, οφείλει να υλοποιείται μέσω της διενέργειας Εκτίμησης Αντικτύπου (DPIA). Στόχος είναι να αποδεικνύεται ότι ο επιδιωκόμενος σκοπός δεν μπορεί να επιτευχθεί με ηπιότερα μέσα και ότι δεν ελλοχεύει ο κίνδυνος διακρίσεων εις βάρος των υποκειμένων.

Πέρα από τη νομική βάση, η Οδηγία LED (Άρθρο 10 παρ. 1β) θέτει ως προτεραιότητα τη διαφύλαξη των ζωτικών συμφερόντων των φυσικών προσώπων. Η διάταξη αυτή συνδέεται άρρηκτα με μια δέσμη δικαιωμάτων των υποκειμένων, όπως η ενημέρωση, η πρόσβαση και η διόρθωση δεδομένων (Άρθρα 12-15). Ειδικότερα, το δικαίωμα στην ενημέρωση λειτουργεί ως βάση και προαπαιτούμενο για την ενεργοποίηση των υπόλοιπων εγγυήσεων. Παράλληλα, το δικαίωμα πρόσβασης προσδίδει μια συλλογική αξία στη διαδικασία, αφού ενισχύει τη λογοδοσία των αρχών επιβολής του νόμου. Στο πλαίσιο της αναγνώρισης

¹⁰¹ Αιτιολογική σκέψη 35 και

¹⁰² ΔΕΕ, συνεκδικασθείσες υποθέσεις C-293/12 και C-594, Digital Rights Ireland, 8 Απριλίου 2014, σκέψη 52· βλ. επίσης, ΔΕΕ, C-362/14, Schrems, 6 Οκτωβρίου 2015, σκέψη 92· όσον αφορά τη χρήση του κριτηρίου της απόλυτης αναγκαιότητας για την αξιολόγηση νομικών μέτρων

¹⁰³ Γνώμη σχετικά με ορισμένα βασικά ζητήματα της οδηγίας (ΕΕ) 2016/680 για την επιβολή του νόμου <https://ec.europa.eu/newsroom/article29/items/610178> (Πρόσβαση: Ιανουάριος 2026)

¹⁰⁴ Markus Naarttijärvi, AI and Sensitive Personal Data Under the Law Enforcement Directive: Between Operational Efficiency and Legal Necessity

προσώπου, η πληροφόρηση διακρίνεται σε προληπτική (ex-ante), με γενική ενημέρωση του κοινού και σε κατασταλτική (ex-post), όπου η ενημέρωση των θιγόμενων προσώπων οφείλει να είναι πιο αυστηρή. Στην τελευταία περίπτωση, η ενημέρωση περιλαμβάνει πληροφορίες σχετικά με το εάν τα προσωπικά δεδομένα του εν λόγω ατόμου υπόκεινται σε επεξεργασία και, σε περίπτωση καταφατικής απάντησης, πληροφορίες για τους σκοπούς της επεξεργασίας, τα συγκεκριμένα δεδομένα που αφορά, καθώς και τα πρόσωπα που έχουν πρόσβαση σε αυτά. Υπό το πρίσμα αυτού του δικαιώματος, όταν αναπτύσσεται τεχνολογία αναγνώρισης προσώπου, τα άτομα που παρακολουθούνται μέσω αυτής θα πρέπει να ενημερώνονται για τη χρήση της και για τις τοποθεσίες των καμερών. Ακόμη και σε περιπτώσεις που η μυστικότητα της έρευνας επιβάλλει προσωρινούς περιορισμούς, η ενημέρωση πρέπει να παρέχεται αμέσως μόλις καταστεί εφικτό. Προβληματική φαίνεται η διάταξη του Άρθρου 15 της LED, όπου αναφέρεται ότι τα ανωτέρω δικαιώματα μπορούν να περιοριστούν.

Η τελευταία προϋπόθεση για την επεξεργασία που θέτει η LED (**Άρθρο 10 παρ. 1γ**) είναι η απαίτηση τα δεδομένα να έχουν «προδήλως δημοσιοποιηθεί» από το ίδιο το υποκείμενο. Η έννοια αυτή υποδηλώνει μια έμμεση παραίτηση του ατόμου από το δικαίωμα προστασίας των εν λόγω πληροφοριών, ωστόσο η πρακτική της εφαρμογή προκαλεί έντονες αμφισβητήσεις ως προς την προέλευση του οπτικού υλικού. Η ομάδα εργασίας του Άρθρου 29 είχε τονίσει ότι η διάταξη αυτή πρέπει να ερμηνεύεται υπό την έννοια ότι το υποκείμενο των δεδομένων γνώριζε ότι τα αντίστοιχα δεδομένα θα δημοσιοποιηθούν, ήτοι στο ευρύ κοινό, μεταξύ άλλων και στις αρχές. Σε περίπτωση αμφιβολίας, πρέπει να εφαρμόζεται συσταλτική ερμηνεία, δεδομένης της παραδοχής ότι το υποκείμενο των δεδομένων παραιτήθηκε οικειοθελώς από την ειδική προστασία των δεδομένων του λόγω της δημοσιοποίησής τους, μεταξύ άλλων και σε αρχές. Το ζήτημα περιπλέκεται από το γεγονός ότι μια φωτογραφία μπορεί να αναρτηθεί ή να επισημανθεί από τρίτους χωρίς τη θέληση του υποκειμένου. Επί του συγκεκριμένου θέματος, το ΕΣΠΔ κατέληξε στο συμπέρασμα ότι το γεγονός ότι ένα άτομο δεν ενεργοποίησε συγκεκριμένες ρυθμίσεις απορρήτου δεν αρκεί για να θεωρηθεί ότι επιθυμούσε την δημοσιοποίηση των δεδομένων του και ότι αυτά μπορούν να χρησιμοποιηθούν για σκοπούς ταυτοποίησης χωρίς τη συγκατάθεσή του¹⁰⁵.

¹⁰⁵ Ο.π. υποσημείωση 15

Η ανωτέρω περιπτώσιολογία αναδεικνύει το ζήτημα της σταδιακής επέκτασης της χρήσης των δεδομένων (function creep), πέραν των αρχικά προβλεπόμενων σκοπών¹⁰⁶. Για παράδειγμα, όταν ένα άτομο βγάζει μια φωτογραφία για την εθνική του ταυτότητα, δεν αναμένει εύλογα ότι τα βιομετρικά του δεδομένα θα χρησιμοποιηθούν για σκοπό άλλον από την καταχώριση στα εθνικά συστήματα για λόγους ταυτοποίησης. Ομοίως, ένα άτομο που αναρτά μια φωτογραφία σε μέσο κοινωνικής δικτύωσης, δεν αναμένει εύλογα την επεξεργασία της εν λόγω αναρτημένης φωτογραφίας του από τις αστυνομικές αρχές. Επομένως, το γεγονός και μόνο ότι μια φωτογραφία έχει δημοσιοποιηθεί από το υποκείμενο των δεδομένων δεν σημαίνει αυτόματα ότι τα σχετικά βιομετρικά δεδομένα, τα οποία μπορούν να ανακτηθούν από τη φωτογραφία με ειδικά τεχνικά μέσα, έχουν προδήλως δημοσιοποιηθεί. Μάλιστα, σύμφωνα με την αρχή του περιορισμού του σκοπού και της θεμιτής επεξεργασίας, καθώς και σε συνδυασμό με το αρ. 4 παρ. 1 β) της LED δεν επιτρέπεται χρήση των δεδομένων για σκοπό διαφορετικό από εκείνον για τον οποίο συλλέχθηκαν, θεμελιώνοντας έτσι την εύλογη προσδοκία ότι μια εικόνα που συλλέχθηκε για συγκεκριμένο σκοπό (π.χ. για ψυχαγωγικούς σκοπούς) δεν θα χρησιμοποιηθεί για άλλο σκοπό, όπως π.χ. σε ποινικές έρευνες ή για βιομετρική κατηγοριοποίηση.

Τέλος, διασαφηνίζεται ότι η LED δεν αντιμετωπίζει όλα τα βιομετρικά δεδομένα με τον ίδιο τρόπο. Το Άρθρο 6 διακρίνει τα προσωπικά δεδομένα ανάλογα με τις κατηγορίες υποκειμένων των δεδομένων, εάν δηλαδή πρόκειται για υπόπτους για την τέλεση εγκλήματος ή προετοιμάζονται να διαπράξουν έγκλημα [Άρθρο 6(α)], ή για καταδικασθέντες για έγκλημα [Άρθρο 6(β)], ή για τα θύματα ποινικού αδικήματος [Άρθρο 6(γ)] ή για άλλους συμμετέχοντες σε ποινικά αδικήματα που δεν είναι ούτε δράστες ούτε θύματα, όπως οι αυτόπτες μάρτυρες [Άρθρο 6(δ)]. Βέβαια, αν και λαμβάνει χώρα ο ανωτέρω διαχωρισμός, δεν θεσπίζεται καμία συνέπεια από αυτή τη διάκριση, αλλά είναι λογικό να πιστεύουμε ότι η διάκριση αυτή μπορεί να οδηγήσει σε διαφορετικές απαντήσεις όσον αφορά το νομικό καθεστώς που ισχύει για τα δεδομένα αυτά.

Συνοψίζοντας, η LED θέτει ένα όριο για την επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα, ορίζοντας ότι η επεξεργασία αυτή πρέπει να είναι «απολύτως

¹⁰⁶ Koops, Bert-Jaap, The Concept of Function Creep (March 3, 2020). Bert-Jaap Koops (2021), 'The Concept of Function Creep', 13 Law, Innovation and Technology (1) (Forthcoming), Διαθέσιμο στο: <https://ssrn.com/abstract=3547903> (Πρόσβαση: Ιανουάριος 2026)

αναγκαία» και να συνοδεύεται από «κατάλληλες εγγυήσεις». Αυτό σημαίνει ότι οι αρχές επιβολής του νόμου μπορούν να επεξεργάζονται ευαίσθητα δεδομένα μόνο όταν αυτό είναι απαραίτητο για τον επιδιωκόμενο σκοπό, όπως η διερεύνηση ενός σοβαρού εγκλήματος, και μόνο εάν δεν υπάρχουν διαθέσιμα λιγότερο παρεμβατικά μέσα. Επιπλέον, η επεξεργασία πρέπει να επιτρέπεται νομικά, είτε από το δίκαιο της ΕΕ είτε από το δίκαιο κρατών μελών, είτε για την προστασία ζωτικών συμφερόντων είτε όταν τα δεδομένα έχουν προδήλως δημοσιοποιηθεί από το υποκείμενο των δεδομένων. Τέλος, λόγω της ευαισθησίας της τεχνολογίας αναγνώρισης προσώπου και των δυνητικών κινδύνων που αυτή συνεπάγεται, κρίνεται καθοριστικής σημασίας η προηγούμενη διενέργεια εκτίμησης αντικτύπου (DPIA)¹⁰⁷, καθώς και η προηγούμενη διαβούλευση με την εποπτική αρχή¹⁰⁸. Η εκτίμηση αντικτύπου σχετικά με την Προστασία Δεδομένων (DPIA) δεν είναι πάντα εύκολο να υλοποιηθεί, επειδή η Τεχνητή Νοημοσύνη αποτελεί εκ φύσεως ένα «μαύρο κουτί» (black box) με εγγενή ασάφεια¹⁰⁹. Ακόμη και ως προς τα χαρακτηριστικά που μας είναι γνωστά, η ύπαρξη εμπορικών απορρήτων και ρητρών εμπιστευτικότητας ενδέχεται να εμποδίσει τους κατασκευαστές συστημάτων αναγνώρισης προσώπου από το να τα αποκαλύψουν με διαφανή τρόπο, όπως απαιτείται, για τη διεξαγωγή εκτίμησης αντικτύπου. Ωστόσο, τα όρια που θέτει η LED είναι πιο ειδικά από εκείνα του ΓΚΠΔ, όχι μόνο λόγω του διαφορετικού πεδίου εφαρμογής του νόμου, αλλά και λόγω της ιδιαίτερα λεπτής ισορροπίας που πρέπει να επιτευχθεί.

5.3 Συμπεράσματα – Σχέσεις μεταξύ των νομοθετημάτων

5.3.1 Σχέση AIA - LED

Όπως αναφέρεται στην Αιτιολογική Σκέψη 38 της Πράξης για την Τεχνητή Νοημοσύνη (AI Act), οι κανόνες που απαγορεύουν την εξ αποστάσεως βιομετρική ταυτοποίηση σε

¹⁰⁷ Αιτιολογικές Σκέψεις 53 και 58 και Άρθρο 27 της LED

¹⁰⁸ Αιτιολογική Σκέψη 96 και Άρθρο 28 της LED

¹⁰⁹ Bathaee, Y. (2018) 'The Artificial Intelligence Black Box and the Failure of Intent and Causation', *Harvard Journal of Law & Technology*, 31(2), σσ. 889-938. Διαθέσιμο στο: <https://jolt.law.harvard.edu/assets/articlePDFs/v31/The-Artificial-Intelligence-Black-Box-and-the-Failure-of-Intent-and-Causation-Yavar-Bathaee.pdf> (Πρόσβαση: Ιανουάριος 2026).

πραγματικό χρόνο σε δημόσια προσβάσιμους χώρους για σκοπούς επιβολής του νόμου, καθώς και οι σχετικές εξαιρέσεις, νοούνται ως ειδικότερος νόμος (*lex specialis*) έναντι του Άρθρου 10 της LED. Το ανωτέρω συνεπάγεται ότι η χρήση και επεξεργασία βιομετρικών δεδομένων ρυθμίζεται κατά τρόπο εξαντλητικό από την Πράξη, αποκλείοντας τη δυνατότητα των αρμόδιων αρχών να θεμελιώσουν τη νομιμότητα της επεξεργασίας στις γενικότερες διατάξεις της Οδηγίας και ειδικότερα στο άρθρο 10 αυτής, εάν δεν πληρούνται οι αυστηρές προϋποθέσεις του Κανονισμού.

Εν αντιθέσει με όσα προεκτέθηκαν, η αρχή του *lex specialis* δεν σημαίνει ότι θα αποτελέσει τη νομική βάση για την επεξεργασία βιομετρικών δεδομένων, καταργώντας τον ρόλο της LED. Τουναντίον, η τελευταία εξακολουθεί να αποτελεί το βασικό νομικό πλαίσιο προστασίας, ωστόσο κρίθηκε αναγκαίο να θεσπιστούν ειδικοί κανόνες που να εισάγουν πρόσθετους, αυστηρότερους περιορισμούς σε συγκεκριμένα πλαίσια υψηλού κινδύνου. Έτσι, το Άρθρο 10 της LED εξακολουθεί και παραμένει η νομική βάση σε άλλες περιπτώσεις, που δεν εμπίπτουν στον στενό πυρήνα της ταυτοποίησης σε πραγματικό χρόνο, όπως η εγκληματολογική ταυτοποίηση (“forensic matching”), αλλά και σε περιπτώσεις όπου η χρήση βιομετρικών δεδομένων θα διενεργείται για σκοπούς επιβολής του νόμου^{110 111}.

Συμπερασματικά, μολονότι η Τεχνολογία Αναγνώρισης Προσώπου εμπίπτει στο πεδίο εφαρμογής τόσο της LED (ως προς την επεξεργασία δεδομένων για σκοπούς επιβολής του νόμου) όσο και της Πράξης για την TN (ως προς την τεχνολογική διάσταση), ανακύπτει η επιτακτική ανάγκη για ένα συνεκτικότερο νομικό πλαίσιο. Η άρση των ρυθμιστικών ασαφειών και των «γκρίζων ζωνών» καθίσταται κρίσιμη για την εμπέδωση της ασφάλειας δικαίου και τη θωράκιση των θεμελιωδών δικαιωμάτων κατά την άσκηση της αστυνομικής εξουσίας. Υπό το πρίσμα αυτό, σε περιπτώσεις κανονιστικής αλληλεπίδρασης, οι ειδικότερες

¹¹⁰ Αιτιολογική Σκέψη 39 Πράξης για την TN

¹¹¹ Συμβούλιο της Ευρωπαϊκής Ένωσης (2021) Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη θέσπιση εναρμονισμένων κανόνων σχετικά με την τεχνητή νοημοσύνη (Πράξη για την Τεχνητή Νοημοσύνη) και την τροποποίηση ορισμένων νομοθετικών πράξεων της Ένωσης - Έκθεση προόδου. 14278/21. Βρυξέλλες, 22 Νοεμβρίου. Διαθέσιμο στο: <https://data.consilium.europa.eu/doc/document/ST-14278-2021-INIT/en/pdf> (Πρόσβαση: Ιανουάριος 2026).

διατάξεις της Πράξης για την ΤΝ υπερισχύουν ως *lex specialis*, διασφαλίζοντας μία πιο στοχευμένη προσέγγιση στη βιομετρική επιτήρηση.

5.3.2 Σχέση ΓΚΠΔ – LED

Στον αντίποδα, η LED λειτουργεί ως ειδικότερο νομοθέτημα (*lex specialis*) έναντι του ΓΚΠΔ και απαιτεί νομική βάση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο της επιβολής του νόμου. Αξίζει να σημειωθεί ότι στο πλαίσιο της LED, σε αντίθεση με τον ΓΚΠΔ, η συγκατάθεση του υποκειμένου δεν δύναται, κατ' αρχήν, να θεμελιώσει νομική βάση επεξεργασίας, δεδομένης της εγγενούς ανισορροπίας ισχύος μεταξύ του πολίτη και της δημόσιας αρχής. Ως εκ τούτου, η επεξεργασία πρέπει να ερείδεται αποκλειστικά σε νομοθετική εξουσιοδότηση.

Ο εν λόγω νόμος πρέπει να είναι προσβάσιμος στο κοινό, σαφής και ακριβής, ώστε να παρέχει «επαρκείς εγγυήσεις έναντι του κινδύνου κατάχρησης και αυθαιρεσίας»¹¹², επιτρέποντας στους πολίτες να προβλέπουν τις συνέπειες της εφαρμογής του και να ρυθμίζουν αναλόγως τη συμπεριφορά τους¹¹³. Την αναγκαιότητα σαφούς οριοθέτησης και συμπληρωματικής λειτουργίας μεταξύ των δύο νομοθετημάτων αναδεικνύει η απόφαση της Σουηδικής Αρχής Προστασίας Δεδομένων¹¹⁴. Η εν λόγω απόφαση επιβεβαίωσε ότι δραστηριότητες που εμπίπτουν στους σκοπούς της επιβολής του νόμου διέπονται αποκλειστικά από το ειδικό κανονιστικό πλαίσιο της LED (άρθρο 1) και όχι από τον ΓΚΠΔ.

5.3.3 Σχέση AIA - ΓΚΠΔ

Η σχέση Τεχνητής Νοημοσύνης και προσωπικών δεδομένων είναι μία σχέση διπλής κατεύθυνσης: τα προσωπικά δεδομένα τροφοδοτούν την τεχνητή νοημοσύνη και αυτή παράγει περισσότερα δεδομένα. Το αυτό επιβεβαιώνεται και στις αιτιολογικές σκέψεις 45

¹¹² Αιτιολογική Σκέψη 33 και Άρθρο 8 LED

¹¹³ EDRI (2020) *Ban Biometric Mass Surveillance: A set of fundamental rights demands for the European Commission and Member States*. Brussels: European Digital Rights. Διαθέσιμο στο: <https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf> (Πρόσβαση: Φεβρουάριος 2026).

¹¹⁴ Ο.π. υποσημείωση 59

και 69 της Πράξης για την ΤΝ, όπου διευκρινίζεται ότι η χρήση συστημάτων ΤΝ θα πρέπει να εξακολουθεί να συμμορφώνεται με τη νομοθεσία για την προστασία των δεδομένων.

Όπως προαναφέρθηκε, η Πράξη για την ΤΝ εισάγει ένα οριζόντιο ρυθμιστικό πλαίσιο, το οποίο εφαρμόζεται με την επιφύλαξη του υφιστάμενου ενωσιακού δικαίου. Σύμφωνα με την αιτιολογική σκέψη 9, ο Κανονισμός λειτουργεί συμπληρωματικά (ως *lex specialis*) προς τις διατάξεις για τα προσωπικά δεδομένα, τα θεμελιώδη δικαιώματα, την προστασία των εργαζομένων και την ασφάλεια των προϊόντων. Χαρακτηριστικό της ανωτέρω σχέσης αποτελεί η διασφάλιση ότι η επεξεργασία προσωπικών δεδομένων στο πλαίσιο συστημάτων ΤΝ εξακολουθεί να υπόκειται στις αυστηρές επιταγές του GDPR και της Οδηγίας ePrivacy¹¹⁵. Η ρητή αυτή αναφορά εγγυάται ότι η νέα νομοθεσία θα συνεχίσει να διασφαλίζει το ευρωπαϊκό κεκτημένο αναφορικά με την προστασία των προσωπικών δεδομένων, όπως αυτά έχουν παγιωθεί μέσα από τη ευρωπαϊκή νομοθεσία, αλλά και από τη νομολογία του Δικαστηρίου της ΕΕ (ΔΕΕ) και τις αποφάσεις των εποπτικών αρχών¹¹⁶.

Παράλληλα, τα δύο νομοθετήματα αλληλοσυμπληρώνονται με αξιοσημείωτο παράδειγμα την εκτίμηση αντικτύπου. Η Εκτίμηση Αντικτύπου στα Θεμελιώδη Δικαιώματα (FRIA), που προβλέπεται στο Άρθρο 27(4) της Πράξης για την ΤΝ, δρα στοχευμένα για πτυχές που δεν καλύπτονται από την Εκτίμηση Αντικτύπου Προστασίας Δεδομένων (DPIA) βάσει GDPR. Παρόλο που η DPIA περιλαμβάνει παραδοσιακά την εξέταση κινδύνων για τα δικαιώματα και τις ελευθερίες, η FRIA στοχεύει στο να καλύψει το κενό εκείνο όπου η επίδραση της ΤΝ υπερβαίνει τη στενή έννοια της προστασίας δεδομένων, διασφαλίζοντας μια ολιστική εποπτεία των επιπτώσεων της τεχνολογίας στην κοινωνία.

Τέλος, όπως υπογραμμίζουν και το ΕΣΠΑ και ο ΕΕΠΑ, όταν τα συστήματα ΤΝ βασίζονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα, οι διατάξεις της Πράξης για την ΤΝ είναι άμεσα συνυφασμένες με το νομικό πλαίσιο προστασίας δεδομένων, πράγμα που θα ισχύει για τα περισσότερα συστήματα ΤΝ που εμπίπτουν στο πεδίο εφαρμογής του ΓΚΠΔ.

¹¹⁵ Άρθρο 2 παρ. 7 του AI ACT

¹¹⁶ ΕΣΠΑ και ΕΕΠΑ (2021) Κοινή γνωμοδότηση 5/2021 σχετικά με την πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη θέσπιση εναρμονισμένων κανόνων σχετικά με την τεχνητή νοημοσύνη (Πράξη για την Τεχνητή Νοημοσύνη). 18 Ιουνίου. Διαθέσιμο στο: https://edpb.europa.eu/our-work-tools/our-documents/edpb-edps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_el (Πρόσβαση: 26 Ιανουαρίου 2026).

Κατά συνέπεια, θα υπάρξουν διασυνδέσεις αρμοδιοτήτων μεταξύ των εποπτικών αρχών στο πλαίσιο της Πράξης για την ΤΝ¹¹⁷.

Ωστόσο, η Πράξη για την ΤΝ προβλέπει δύο εξαιρέσεις, όπου μπορεί να υπάρξει παρέκκλιση από τη νομοθεσία περί προστασίας δεδομένων. Το Άρθρο 2 (7) ορίζει ότι η Πράξη δεν θίγει την υφιστάμενη νομοθεσία (όπως τον GDPR ή την Οδηγία για την επιβολή του νόμου), με την επιφύλαξη όμως των ρυθμίσεων που προβλέπονται σε δύο άρθρα: το Άρθρο 10(5), το οποίο επιτρέπει κατ' εξαίρεση στους παρόχους συστημάτων υψηλού κινδύνου να επεξεργάζονται ειδικές κατηγορίες προσωπικών δεδομένων για τον σκοπό του εντοπισμού και της διόρθωσης περιπτώσεων μεροληψίας (bias), και το Άρθρο 59, το οποίο επιτρέπει την περαιτέρω επεξεργασία δεδομένων για την ανάπτυξη ορισμένων συστημάτων ΤΝ προς το δημόσιο συμφέρον εντός του «ρυθμιστικού δοκιμαστηρίου» (regulatory sandbox)¹¹⁸.

¹¹⁷ ΕΣΠΑ και ΕΕΠΑ (2021) Κοινή γνωμοδότηση 5/2021 σχετικά με την πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη θέσπιση εναρμονισμένων κανόνων σχετικά με την τεχνητή νοημοσύνη (Πράξη για την Τεχνητή Νοημοσύνη). Βρυξέλλες: Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων και Ευρωπαίος Επόπτης Προστασίας Δεδομένων. Διαθέσιμο στο: https://edpb.europa.eu/our-work-tools/our-documents/edpb-edps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_el (Πρόσβαση: Φεβρουάριος 2026).

¹¹⁸ Barkane, I. και Buka, L. (2023) 'Prohibited AI surveillance practices in the Artificial Intelligence Act: promises and pitfalls in protecting fundamental rights', στο McDaniel, J.L.M. και Peeters, K. (επιμ.) *Critical Perspectives on Predictive Policing*. Cheltenham: Edward Elgar Publishing, σσ. 110–129.

6 Ο ΑΝΤΙΚΤΥΠΟΣ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΑΝΑΓΝΩΡΙΣΗΣ ΠΡΟΣΩΠΟΥ ΣΤΑ ΘΕΜΕΛΙΩΔΗ ΔΙΚΑΙΩΜΑΤΑ

6.1 Γενικά

Παρότι η Πράξη για την ΤΝ αναγνωρίζει τον πρωταρχικό ρόλο της προστασίας των θεμελιωδών δικαιωμάτων, το τελικό κείμενο της Πράξης έχει δεχθεί έντονη κριτική, καθώς διαφαίνεται ότι απέτυχε να ανταποκριθεί στα υψηλά πρότυπα προστασίας των δικαιωμάτων αυτών, ιδίως όσον αφορά τη διάταξη για τις απαγορευμένες πρακτικές ΤΝ¹¹⁹. Στο ίδιο πνεύμα κινείται και η κοινωνία των πολιτών, η οποία τάσσεται υπέρ της καθολικής απαγόρευσης της βιομετρικής επιτήρησης, π.χ. μέσω της εκστρατείας «Reclaim your face» και της Ευρωπαϊκής Πρωτοβουλίας Πολιτών που ξεκίνησε από την οργάνωση European Digital Rights, υποστηρίζοντας ότι η αδιάκριτη και αυθαίρετη χρήση βιομετρικών στοιχείων δύναται να οδηγήσει σε καθεστώς μαζικής επιτήρησης πλήττοντας -πέραν των άλλων- και την ψυχολογική ακεραιότητα και την ευημερία των ατόμων¹²⁰.

Το ερώτημα που ανακύπτει είναι κατά πόσον οι τεχνολογίες αναγνώρισης προσώπου, νοούμενες ως υποσύνολο των συστημάτων εξ αποστάσεως βιομετρικής ταυτοποίησης, οι οποίες αναπτύσσονται είτε σε πραγματικό χρόνο είτε εκ των υστέρων σε δημόσια προσβάσιμους χώρους για σκοπούς επιβολής του νόμου, είναι αναγκαίες σε μια δημοκρατική κοινωνία.

Για τη νομική αξιολόγηση, είναι σημαντικό να ληφθεί υπόψη ο τρόπος λειτουργίας αυτών των τεχνολογιών, καθώς και ποια δεδομένα τυγχάνουν επεξεργασίας. Όπως αναφέρθηκε και στο οικείο κεφάλαιο, οι εικόνες προσώπου συνιστούν δεδομένα προσωπικού χαρακτήρα, όπως έχει επιβεβαιωθεί τόσο από το ΔΕΕ όσο και από το ΕΔΔΑ. Το ΕΔΔΑ έχει επίσης δηλώσει ότι η εικόνα του προσώπου ενός ατόμου αποτελεί ένα από τα βασικά γνωρίσματα της προσωπικότητάς του, καθώς αποκαλύπτει τα μοναδικά χαρακτηριστικά του και το διακρίνει

¹¹⁹ CDT. (2024) 'Landmark EU AI Act Sets Benchmark for AI Regulation, but Fails to Meet the Bar on Human Rights Protection.' Διαθέσιμο στο: <https://cdt.org/press/landmark-eu-ai-act-sets-benchmark-for-ai-regulation-but-fails-to-meet-the-bar-on-human-rights-protection/> (Πρόσβαση: Φεβρουάριος 2026).

¹²⁰ EDRi (2021) *Civil society calls for AI Red Lines: A global call to action*. Brussels: European Digital Rights. Διαθέσιμο στο: <https://edri.org/wp-content/uploads/2021/11/Civil-society-calls-for-AI-Red-Lines.pdf> (Πρόσβαση: Φεβρουάριος 2026).

από τους ομοίους του. Ωστόσο, πρέπει να επισημανθεί ότι από μία εικόνα προσώπου δεν διακρίνεται πλέον μόνο η ταυτότητα του ατόμου, αλλά και τα βιολογικά και ψυχολογικά του χαρακτηριστικά, η εθνοτική καταγωγή, τα συναισθήματα κτλ. Ως εκ τούτου, η αξιοποίηση συστημάτων αναγνώρισης προσώπου για τη συλλογή, σύγκριση και αποθήκευση βιομετρικών δεδομένων συνιστά εν δυνάμει παρέμβαση τόσο στο δικαίωμα προστασίας των δεδομένων (Άρθρο 8 του Χάρτη της ΕΕ) όσο και στο δικαίωμα στην ιδιωτική ζωή (Άρθρο 7 του Χάρτη και Άρθρο 8 της ΕΣΔΑ).

6.2 Επέμβαση στο δικαίωμα της Ιδιωτικής Ζωής και της Προστασίας Δεδομένων

Τα δικαιώματα στον σεβασμό της ιδιωτικής ζωής και στην προστασία των δεδομένων κατέχουν κεντρική θέση στην εφαρμογή της τεχνολογίας αναγνώρισης προσώπου σε δημόσιους χώρους. Αν και συνδέονται στενά, αποτελούν διακριτά και αυτοτελή δικαιώματα. Και τα δύο επιδιώκουν την προστασία παρόμοιων αξιών, δηλαδή της αυτονομίας και της ανθρώπινης αξιοπρέπειας των ατόμων, διασφαλίζοντάς τους μια προσωπική σφαίρα εντός της οποίας μπορούν να αναπτύξουν ελεύθερα την προσωπικότητά τους, να σκεφτούν και να διαμορφώσουν τις απόψεις τους. Ως εκ τούτου, αποτελούν ουσιώδη προϋπόθεση για την άσκηση άλλων θεμελιωδών δικαιωμάτων, όπως η ελευθερία της σκέψης, της συνείδησης και της θρησκείας (Άρθρο 10 του Χάρτη), η ελευθερία έκφρασης και πληροφόρησης (Άρθρο 11 του Χάρτη) και η ελευθερία του συνέρχεσθαι και του συνεταιριζέσθαι (Άρθρο 12 του Χάρτη)¹²¹.

Η επεξεργασία εικόνων προσώπου σε βάσεις δεδομένων μεγάλης κλίμακας ενδέχεται, καθώς εξελίσσεται η τεχνολογία αναγνώρισης προσώπου, να εγείρει αχατογράφητα ζητήματα σχετικά με τα δικαιώματα προστασίας της ιδιωτικής ζωής καθώς και των προσωπικών δεδομένων. Δεδομένου ότι τα δύο αυτά δικαιώματα δεν είναι απόλυτα, μπορούν να υπόκεινται σε περιορισμούς, αλλά κάθε επέμβαση πρέπει να είναι επαρκώς

¹²¹ European Union Agency for Fundamental Rights (FRA) (2019) *Facial recognition technology: fundamental rights considerations in the context of law enforcement*. FRA Focus Paper. Vienna: FRA. Διαθέσιμο στο: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf (Πρόσβαση: Ιανουάριος 2026).

αιτιολογημένη και δεν μπορεί σε καμία περίπτωση να διακυβεύει τον ουσιώδη, αναπαλλοτρίωτο πυρήνα του δικαιώματος, όπως θα αναλυθεί στην επόμενη ενότητα.

6.2.1 Ιδιωτική Ζωή

Η έννοια της «ιδιωτικής ζωής» όπως αντιπαραβάλλεται με τη «δημόσια ζωή» είναι ευρύς όρος που δεν επιδέχεται εξαντλητικό ορισμό. Το δικαίωμα στην ιδιωτική ζωή κατοχυρώνεται με γενικούς όρους στο Άρθρο 8 της ΕΣΔΑ. «Οι συντάκτες της Σύμβασης προόριζαν το Άρθρο 8 της ΕΣΔΑ ως ένα κλασικό δικαίωμα στην ιδιωτικότητα, παρέχοντας ένα αρνητικό δικαίωμα στους πολίτες, να είναι ελεύθεροι από αυθαίρετες επεμβάσεις στην ιδιωτική και οικογενειακή τους ζωή, την κατοικία και τις επικοινωνίες τους, καθώς και μια αρνητική υποχρέωση για τα κράτη, να μην κάνουν κατάχρηση της εξουσίας τους επεμβαίνοντας αυθαίρετα στα δικαιώματα των πολιτών τους»¹²². Πέραν αυτής της αρνητικής υποχρέωσης, δημιουργείται επίσης μια «θετική υποχρέωση» για τη διασφάλιση του σεβασμού του δικαιώματος της ιδιωτικότητας.

Επιπλέον, έχουν διατυπωθεί και άλλες ερμηνείες σχετικά με την έννοια της ιδιωτικότητας. Στην πρώτη ερμηνεία, η έννοια της ιδιωτικότητας αναλύθηκε ως «το δικαίωμα του ατόμου να αφήνεται στην ησυχία του» (the right to be let alone) από τους Warren και Brandeis το 1890. Μετά από αυτό, το 1967, ο Westin την περιέγραψε ως «ένα συμφέρον στον έλεγχο των πληροφοριών σχετικά με τον εαυτό του». Τέλος, το 1980, ο Gavison την εξήγησε ως «μια κατάσταση περιορισμένης προσβασιμότητας: μυστικότητα, απομόνωση και ανωνυμία»¹²³.

Η ιδιωτικότητα καλύπτει τη σωματική και ψυχική ακεραιότητα ενός ατόμου και μπορεί, ως εκ τούτου, να περιλαμβάνει πολλαπλές πτυχές της φυσικής και κοινωνικής ταυτότητας του ατόμου. Υπάρχει επίσης μια ζώνη αλληλεπίδρασης του ατόμου με άλλους, ακόμη και σε δημόσιο πλαίσιο, η οποία μπορεί να εμπίπτει στο πεδίο της «ιδιωτικής ζωής». Το ΕΔΔΑ έχει χρησιμοποιήσει την έννοια της «εύλογης προσδοκίας ιδιωτικότητας» (reasonable expectation of privacy), αναφερόμενο στον βαθμό στον οποίο οι άνθρωποι μπορούν να αναμένουν ιδιωτικότητα σε δημόσιους χώρους χωρίς να υπόκεινται σε επιτήρηση, ως έναν από τους

¹²² Van der Sloot, B. (2015) 'Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of "Big Data"', *Utrecht Journal of International and European Law*, 31(80), σσ. 25-50. Διαθέσιμο στο: <http://dx.doi.org/10.5334/ujel.cp>. (Πρόσβαση: Ιανουάριος 2026).

¹²³ Liu, N.Y. (2011) *Bio-Privacy: Privacy Regulations and the Challenge of Biometrics*. London: Routledge.

παράγοντες, αν και όχι απαραίτητα τον καθοριστικό, για να αποφανθεί επί παραβίασης του δικαιώματος σεβασμού της ιδιωτικής ζωής. Αυτό εξηγείται από το γεγονός ότι τα άτομα έχουν το δικαίωμα να ελέγχουν την εικόνα τους και να αναπτύσσουν την «κοινωνική τους ταυτότητα».

Η διακήρυξη του απαραβίαστου της ιδιωτικής ζωής σημαίνει ότι στη ζωή καθενός ανθρώπου υπάρχει ένας πυρήνας στον οποίο κυριαρχεί αυτός και μόνο και στον οποίο δεν μπορεί να διεισδύσει το κράτος. Όρια και περιεχόμενο της ιδιωτικής του ζωής καθορίζει καταρχήν μόνο του κάθε άτομο. Η διακήρυξη του απαραβίαστου της ιδιωτικής ζωής σημαίνει δηλαδή την απαγόρευση της δημοσιοποιήσεως της ζωής του ανθρώπου, απαγορεύοντας επομένως κάθε κρατική επέμβαση¹²⁴. Από την άλλη πλευρά, εμπειρογνώμονες του ΟΗΕ, έχουν διατυπώσει ότι το γεγονός και μόνο ότι οι συμμετέχοντες σε συγκεντρώσεις βρίσκονται σε δημόσιο χώρο δεν σημαίνει ότι η ιδιωτικότητά τους δεν μπορεί να παραβιαστεί. Δεδομένου ότι το εν λόγω δικαίωμα δεν είναι απόλυτο, δύναται να υπόκεινται σε περιορισμούς, ωστόσο κάθε επέμβαση πρέπει να είναι επαρκώς αιτιολογημένη¹²⁵ και δεν δύναται σε καμία περίπτωση να θίγει τον ουσιώδη, πυρήνα του εν λόγω δικαιώματος, όπως θα αναλυθεί διεξοδικά.

Η ιδιωτικότητα είναι ένα σημαντικό ζήτημα ειδικά όταν σχετίζεται με την επεξεργασία βιομετρικών δεδομένων για την ταυτοποίηση του ατόμου. Όταν πρόκειται για την επεξεργασία βιομετρικών δεδομένων, παρατηρείται ότι η επεξεργασία εκτείνεται σε περισσότερες πληροφορίες από όσες πραγματικά είναι αναγκαίες για την ταυτοποίηση. Αυτό οφείλεται στο ότι τα βιομετρικά δεδομένα περιέχουν πολλές προσωπικές πληροφορίες, όπως η εθνικότητα και το φύλο. Αυτή η γνώση μπορεί να αποτελέσει προσβολή της ιδιωτικότητας, καθώς επιτρέπει στο κράτος να μάθει πολύ περισσότερα για τα άτομα από όσα είναι πρωτίστως απαραίτητα, ενώ ταυτόχρονα ανατρέπονται οι προσδοκίες, καθώς οι άνθρωποι δεν αναμένουν ότι οι άλλοι θα γνωρίζουν περισσότερα για αυτούς από όσα οι ίδιοι αποκαλύπτουν.

¹²⁴ Δαγτόγλου, Π.Δ. (2012) *Συνταγματικό Δίκαιο: Ατομικά Δικαιώματα*. 4η αναθ. έκδ. Αθήνα-Θεσσαλονίκη: Εκδόσεις Σάκκουλα.

¹²⁵ European Union Agency for Fundamental Rights (FRA), Council of Europe και European Data Protection Supervisor (EDPS) (2018) *Handbook on European data protection law*. 2018 edn. Luxembourg: Publications Office of the European Union.

Μια άλλη πτυχή του δικαιώματος σεβασμού της ιδιωτικής ζωής αφορά στη σύνδεσή του με τη μαζική επιτήρηση. Η Πράξη για την ΤΝ, μέσω της αιτιολογικής σκέψης 32, υπογραμμίζει τον ιδιαίτερα παρεμβατικό χαρακτήρα της RBI όταν αυτή εφαρμόζεται σε δημόσιους χώρους για σκοπούς επιβολής του νόμου. Και αυτό διότι η χρήση συστημάτων εξ αποστάσεως ταυτοποίησης σε μεγάλη έκταση δύναται να επιτρέψει ακόμα και τον εντοπισμό της τοποθεσίας ενός ατόμου σε συγκεκριμένες χρονικές στιγμές. Η εν λόγω δυνατότητα επιτρέπει την εξαγωγή συμπερασμάτων σχετικά με τον τόπο κατοικίας του ατόμου, τις κοινωνικές του σχέσεις και συνήθειες, το θρησκευμά του (π.χ. ανάλογα με την επισκεψιμότητα σε χώρο λατρείας), την υγεία του (εάν εισέρχεται σε ιατρική εγκατάσταση) και να αποκαλύψει πληθώρα άλλων δραστηριοτήτων¹²⁶. Συνέπεια των ανωτέρω είναι η δημιουργία ενός αισθήματος διαρκούς επιτήρησης στα άτομα¹²⁷, πλήττοντας την ιδιωτικότητα μεγάλου μέρους του κοινωνικού συνόλου και λειτουργώντας αποτρεπτικά (chilling effect) για την άσκηση άλλων θεμελιωδών ελευθεριών, όπως η ελευθερία του συνέρχεσθαι ή η ελευθερία της έκφρασης¹²⁸.

Οι επιπτώσεις στην ιδιωτικότητα καθίστανται ακόμη εντονότερες, εάν αναλογιστεί κανείς ότι η ψηφιακή καταγραφή της ανθρώπινης συμπεριφοράς επιτρέπει στα συστήματα ΤΝ να εξαγάγουν συμπεράσματα όχι μόνο για τις καταναλωτικές προτιμήσεις, αλλά και για ευαίσθητα προσωπικά δεδομένα, όπως ο σεξουαλικός προσανατολισμός, η ηλικία, το φύλο, καθώς και οι θρησκευτικές ή πολιτικές πεποιθήσεις. Επιπλέον, μπορεί να «αυξήσει την εξουσία που έχουν οι άλλοι επί των ατόμων» και να οδηγήσει σε στρεβλώσεις εάν χρησιμοποιηθεί στη λήψη αποφάσεων, δεδομένου ότι «τα δεδομένα είναι συχνά αποκομμένα από το αρχικό πλαίσιο συλλογής τους»¹²⁹. Όλες αυτές οι αρνητικές συνέπειες της παρακολούθησης οξύνονται κατά τον χρόνο που η τεχνολογία αναγνώρισης προσώπου

¹²⁶ Ο.π. υποσημείωση 14

¹²⁷ Opinion of Advocate General Bot (2015) *Maximillian Schrems v Data Protection Commissioner*, Case C-362/14, ECLI:EU:C:2015:627. Στην υπόθεση *Schrems*, ο Γενικός Εισαγγελέας Yves Bot δήλωσε ότι «μια τέτοια μαζική, αδιάκριτη επιτήρηση είναι εγγενώς δυσανάλογη και συνιστά αδικαιολόγητη επέμβαση στα δικαιώματα που κατοχυρώνονται στα άρθρα 7 και 8 του Χάρτη».

¹²⁸ Raposo, V.L. (2024) 'Look at the camera and say cheese': the existing European legal framework for facial recognition technology in criminal investigations, *Information & Communications Technology Law*, 33(1), σσ. 1–20. Διαθέσιμο στο: <https://doi.org/10.1080/13600834.2023.2239621> (Πρόσβαση: Φεβρουάριος 2026).

¹²⁹ Solove, D.J. (2006) 'A taxonomy of privacy', *University of Pennsylvania Law Review*, 154(3), pp. 477.

χρησιμοποιείται για την επιτήρηση δημόσιων χώρων, καθώς οι πολίτες αντιλαμβάνονται ότι χάνουν την ανωνυμία τους όταν βρίσκονται εκτός οικίας.

Αυτή είναι και η ερμηνεία του ΕΔΔΑ στην απόφαση Glukhin κατά Ρωσίας (πρώτη απόφαση διεθνούς Δικαστηρίου επί της τεχνολογίας αναγνώρισης προσώπου), όπου αναφέρεται ότι «η βιομετρική μαζική επιτήρηση, ιδίως με τη χρήση τεχνολογίας αναγνώρισης προσώπου, συνιστά μία από τις μεγαλύτερες απειλές για τα θεμελιώδη δικαιώματα στην ψηφιακή εποχή». Επιπροσθέτως, τα άτομα ενδέχεται να μην έχουν συγκατατεθεί σε τέτοιου είδους επεξεργασία δεδομένων προσωπικού χαρακτήρα. Ως εκ τούτου, ευλόγως θεωρούν ότι οι πληροφορίες αυτές παραμένουν άγνωστες σε τρίτους, συμπεριλαμβανομένων των ευφυνών συστημάτων, γεγονός που καταδεικνύει την παραβίαση του δικαιώματός τους στην ιδιωτικότητα.

Για όλους τους ανωτέρω λόγους, το ΕΣΠΔ και ο ΕΕΠΔ είχαν προτείνει την πλήρη απαγόρευση της χρήσης της τεχνητής νοημοσύνης για τον σκοπό της βιομετρικής ταυτοποίησης σε δημόσια προσβάσιμους χώρους, ανεξαρτήτως πλαισίου. Ειδικότερα, είχε υπογραμμιστεί ότι η εξ αποστάσεως βιομετρική ταυτοποίηση ενέχει υψηλό κίνδυνο εισβολής στην ιδιωτική ζωή των ατόμων και δεν έχει θέση σε μια δημοκρατική κοινωνία, καθώς αυτή μπορεί να οδηγήσει σε μαζική παρακολούθηση. Στο ίδιο πνεύμα, το ΕΣΠΔ εξέφρασε την άποψη ότι τα συστήματα αναγνώρισης προσώπου που κατηγοριοποιούν τα άτομα ανάλογα με την εθνικότητα, το φύλο, καθώς και τον πολιτικό ή σεξουαλικό προσανατολισμό, δεν είναι συμβατά με τον Χάρτη. Συμπερασματικά, κατά το ΕΣΠΔ, η χρήση βάσεων δεδομένων που προέρχονται από μαζική συλλογή προσωπικών στοιχείων για σκοπούς επιβολής του νόμου, προσκρούει στις απαιτήσεις αναγκαιότητας της ΕΕ¹³⁰.

Για να οικοδομηθεί ένα κλίμα εμπιστοσύνης, λοιπόν, είναι απαραίτητο να διασφαλίζεται ότι η συλλογή δεδομένων δεν θα διεισδύσει βαθύτερα στην ιδιωτικότητα των ατόμων και δεν θα αποτελέσει εφιαλτήριο για αθέμιτες διακρίσεις ή παράνομες πρακτικές εις βάρος των χρηστών¹³¹.

¹³⁰ Ο.π. υποσημείωση 14

¹³¹ Ευρωπαϊκή Επιτροπή (2019). Κατευθυντήριες γραμμές ηθικής για αξιόπιστη Τεχνητή Νοημοσύνη. Ανεξάρτητη ομάδα εμπειρογνομόνων υψηλού επιπέδου για την τεχνητή νοημοσύνη. [online] Βρυξέλλες: Ευρωπαϊκή Επιτροπή. Διαθέσιμο στο: <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai> (Πρόσβαση: Δεκέμβριος 2025).

6.2.2 Δικαίωμα στην προστασία προσωπικών δεδομένων

Το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα ορίζεται ως το δικαίωμα του υποκειμένου των δεδομένων να ασκεί έλεγχο, ακόμη και ενεργό, επί των εν λόγω δεδομένων. Το δικαίωμα αυτό εκτείνεται από την πρόσβαση έως τη διόρθωση. Αναγνωρίζεται ρητώς στο άρθρο 8 του Χάρτη ως μία από τις ουσιώδεις ελευθερίες του ατόμου. Ωστόσο, δεν περιλαμβάνεται ρητώς στην ΕΣΔΑ, αλλά η προστασία του συνδέεται συνήθως με το δικαίωμα στην ιδιωτική ζωή υπό την ευρύτερη έννοιά του. Στο ίδιο μήκος κύματος, το Συμβούλιο Ανθρωπίνων Δικαιωμάτων των Ηνωμένων Εθνών επεσήμανε το 2021 ότι η ΤΝ παρεμβαίνει στην ιδιωτική ζωή των ατόμων επεκτείνοντας, εντείνοντας ή ενθαρρύνοντας τις συνέπειες αυτής, ιδίως όσον αφορά τη συλλογή και χρήση προσωπικών δεδομένων¹³².

Η διατήρηση και χρήση δεδομένων από την αστυνομία αποτελεί ένα από τα ζητήματα που έχουν προκαλέσει το μεγαλύτερο ενδιαφέρον και αντιπαράθεση¹³³, ιδίως κατά τη χρήση μηχανισμών όπως η αναγνώριση προσώπου. Ιδιαίτερης σημασίας είναι η εικόνα του προσώπου, δεδομένου ότι πρόκειται για βιομετρικά και, ως εκ τούτου, προσωπικά δεδομένα, τα οποία αναγνωρίζονται ως ιδιαίτερα ευαίσθητης φύσης. Για τον λόγο αυτό, τα συστήματα FR στο πεδίο επιβολής του νόμου σε δημόσιους χώρους συνιστούν παρέμβαση στην προστασία των δεδομένων προσωπικού χαρακτήρα, από τη στιγμή που το υποκείμενο των δεδομένων έχει το δικαίωμα να ελέγχει την εικόνα του και τα δεδομένα που την αφορούν. Στην προκειμένη περίπτωση, αυτό που συμβαίνει είναι ότι λαμβάνεται μια εικόνα του ατόμου, η οποία μπορεί να είναι φωτογραφία ή βίντεο, και αποθηκεύεται σε μια βάση δεδομένων που υπόκειται σε αυτοματοποιημένη επεξεργασία από την αστυνομία, με αποτέλεσμα το άτομο να χάνει τον έλεγχο των προσωπικών του πληροφοριών.

Σε αυτό το σημείο αξίζει να επισημανθεί ότι για την λειτουργία των συστημάτων εξ αποστάσεως ταυτοποίησης δεν συλλέγονται μόνο τα δεδομένα του στοχευόμενου

¹³² United Nations Human Rights Council (2021) *The right to privacy in the digital age. Report of the United Nations High Commissioner for Human Rights*. A/HRC/48/31. Geneva: United Nations. Διαθέσιμο στο: <https://docs.un.org/en/a/hrc/48/31> (Πρόσβαση: Φεβρουάριος 2026).

¹³³ Coghlan, N. (2016) 'Gaughran [2015] UKSC 29 on police biometric data retention: Strasbourg unheard, Strasbourg unheard', *European Human Rights Law Review*, (1), σσ. 61–68.

προσώπου. Αντίθετα, τα εν λόγω συστήματα σαρώνουν πολλαπλά άτομα ταυτοχρόνως.

Κατά συνέπεια, η διαδικασία επηρεάζει το δικαίωμα προστασίας δεδομένων όχι μόνο ενός συγκεκριμένου ατόμου -όπως συμβαίνει, για παράδειγμα, στην άρση του απορρήτου των επικοινωνιών- αλλά και όλων όσων βρίσκονται στον περιβάλλοντα χώρο.

Σύμφωνα με το ΕΣΠΔ, η επεξεργασία βιομετρικών δεδομένων υπό οποιεσδήποτε περιστάσεις συνιστά αφ' εαυτής σοβαρή παρέμβαση. Ο χαρακτήρας αυτός δεν αναιρείται από το αποτέλεσμα της διαδικασίας, ήτοι από το εάν υπάρξει θετική ταύτιση ή εάν τα δεδομένα διαγραφούν αμελλητί κατόπιν αρνητικού αποτελέσματος¹³⁴. Η παρέμβαση στο θεμελιώδες δικαίωμα της προστασίας δεδομένων συντελείται ήδη από τη στιγμή που τα χαρακτηριστικά του προσώπου καταγράφονται για να μετασχηματιστούν, ανεξάρτητα από οποιαδήποτε αντιστοίχιση με άλλα βιομετρικά δεδομένα που είναι αποθηκευμένα σε μια υπάρχουσα βάση δεδομένων.

6.3 Επέμβαση στο δικαίωμα της μη διακριτικής μεταχείρισης

Η προκατάληψη και οι διακρίσεις συνιστούν κινδύνους σύμφυτους με κάθε μορφή κοινωνικής και οικονομικής δραστηριότητας. Ενώ η ανθρώπινη κρίση διέπεται αναπόφευκτα από υποκειμενικότητα, καθοδηγούμενη από την προσωπική αντίληψη του ατόμου για τον κόσμο, τα συστήματα ΤΝ περιβάλλονται συχνά από ένα τεκμήριο αυξημένης αντικειμενικότητας. Τούτο δικαιολογείται από το ότι λειτουργούν βάσει μαθηματικών συναρτήσεων και προκαθορισμένων παραμέτρων, γεγονός που δημιουργεί την προσδοκία της αμεροληψίας. Ωστόσο, παρά την υποτιθέμενη αυτή ουδετερότητα, τα εν λόγω συστήματα δύνανται να παραγάγουν μεροληπτικά και εσφαλμένα αποτελέσματα. Ως εκ τούτου, οδηγούν σε δυσμενή διακριτική μεταχείριση εις βάρος συγκεκριμένων ατόμων ή ομάδων, επιφέροντας σοβαρές επιπτώσεις στην καθημερινότητα και την κοινωνική τους υπόσταση.

Η διάκριση στην αλγοριθμική λήψη αποφάσεων των συστημάτων αναγνώρισης προσώπου δεν περιορίζεται σε μια μοναδική χρονική στιγμή, αλλά δύναται να λάβει χώρα κατά τον σχεδιασμό, τη δοκιμή και την εφαρμογή, λόγω των μεροληψιών που ενσωματώνονται στον ίδιο τον αλγόριθμο από το πρόσωπο ή την αρχή που είναι υπεύθυνη για την κατασκευή και/ή

¹³⁴ Ο.π. υποσημείωση 14

εφαρμογή του εν λόγω συστήματος. Υπό αυτή την έννοια, οι προγραμματιστές του συστήματος ενδέχεται να έχουν μεταφέρει εμμέσως τη διάκριση από τον αναλογικό στον ψηφιακό κόσμο.

Επιπροσθέτως, τα δεδομένα ενδέχεται να έχουν συλλεχθεί με εσφαλμένες ή ανακριβείς μεθοδολογίες που διακυβεύουν την αντιστοιχία μεταξύ της πραγματικότητας που περιγράφεται από τα εν λόγω δεδομένα και του πραγματικού κόσμου. Επιπλέον, ενδέχεται τα δεδομένα να έχουν ληφθεί μεν με κατάλληλο τρόπο, αλλά η πραγματικότητα να είναι καθαυτή (*per se*) μεροληπτική, με αποτέλεσμα τα δεδομένα να αναπαριστούν απλώς τις διακρίσεις που υφίστανται ήδη στην κοινωνία.

Σημειώνεται ότι η αλγοριθμική διάκριση, όπως και κάθε άλλη μορφή διάκρισης, διακρίνεται σε δύο είδη: την άμεση και την έμμεση. Η πρώτη υφίσταται «όταν ένα πρόσωπο υφίσταται μεταχείριση λιγότερο ευνοϊκή από αυτήν που τυγχάνει, έτυχε ή θα ετύγχανε άλλο πρόσωπο σε ανάλογη κατάσταση». Η δεύτερη λαμβάνει χώρα «όταν μια εκ πρώτης όψεως ουδέτερη διάταξη, κριτήριο ή πρακτική μπορεί να θέσει πρόσωπα συγκεκριμένης φυλετικής ή εθνοτικής καταγωγής σε μειονεκτική θέση συγκριτικά με άλλα πρόσωπα»¹³⁵.

Όπως έχει ήδη επισημανθεί, τα συστήματα ΤΝ και, κατ' επέκταση, τα συστήματα αναγνώρισης προσώπου, δεν αποδίδουν απόλυτα αποτελέσματα, αλλά αποτελέσματα βασισμένα σε πιθανολογική κρίση. Το γεγονός αυτό, σε συνδυασμό με την ύπαρξη μεροληψιών στις βάσεις δεδομένων οδηγεί σε εσφαλμένες ταυτοποιήσεις¹³⁶. Ένα επιπρόσθετο στοιχείο που καθιστά αυτά τα συστήματα εξαιρετικά επικίνδυνα είναι η αμεσότητα των αποτελεσμάτων τους, η οποία περιορίζει δραστικά τα χρονικά περιθώρια για διορθωτικές παρεμβάσεις ή ουσιαστικούς ελέγχους, εκθέτοντας τους πολίτες σε αυθαίρετες ή λανθασμένες επεμβάσεις των διωκτικών αρχών.

Όπως έχει αναφερθεί, τα σφάλματα που προκύπτουν από τα συστήματα αναγνώρισης διακρίνονται σε ψευδώς θετικά (*false positives*) και σε ψευδώς αρνητικά (*false negatives*). Υπό το πρίσμα των ανωτέρω, τα ψευδώς θετικά αποτελέσματα είναι πιο επικίνδυνα λόγω των

¹³⁵ Συμβούλιο της Ευρωπαϊκής Ένωσης (2000a) 'Οδηγία 2000/43/ΕΚ του Συμβουλίου της 29ης Ιουνίου 2000 περί εφαρμογής της αρχής της ίσης μεταχείρισης προσώπων ασχέτως φυλετικής ή εθνοτικής τους καταγωγής', *Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων*, L 180, σσ. 22–26.

¹³⁶ Brey, P. (2004) 'Ethical aspects of facial recognition systems in public places', *Journal of Information, Communication and Ethics in Society*, 2(2), σσ. 104.

νομικών τους επιπτώσεων που συνεπάγονται για όσους έχουν ταυτοποιηθεί εσφαλμένα ως επικίνδυνοι εγκληματίες ή τρομοκράτες ή ύποπτοι για τέλεση σοβαρού εγκλήματος, επειδή προέκυψε αντιστοίχιση με τις πληροφορίες που περιέχονται σε μια λίστα παρακολούθησης, με αποτέλεσμα να έχει ασκηθεί ποινική δίωξη εναντίον τους¹³⁷. Όπως γίνεται κατανοητό, μία εσφαλμένη ταυτοποίηση στον τομέα της επιβολής του νόμου μπορεί να οδηγήσει αφενός σε σύλληψη και σε δημόσια αποκάλυψη της ταυτότητας του συλληφθέντος και αφετέρου να επιφέρει τέτοια κοινωνική απαξίωση που να πληγεί ανεπανόρθωτα η φήμη του ατόμου και η κοινωνική του υπόληψη¹³⁸.

Το επίπεδο πιθανότητας επιτυχίας και αποτυχίας βασίζεται στην ακρίβεια του συστήματος, δηλαδή στον αριθμό των ψευδώς θετικών και αρνητικών αποτελεσμάτων που εκπέμπει, ο οποίος με τη σειρά του εξαρτάται τρεις κύριοι παράγοντες: τα δεδομένα εκπαίδευσης, την αρχιτεκτονική του συστήματος και τη συνάρτηση απώλειας, δηλαδή τον τρόπο που το σύστημα «εκπαιδεύεται» από τα λάθη του. Όπως στις περισσότερες εφαρμογές βαθιάς μάθησης, έτσι και στην FRT απαιτούνται μεγάλα σύνολα εκπαίδευσης για την αποφυγή της υπερπροσαρμογής (overfitting). Στην αναγνώριση προσώπου στόχος είναι η εξαγωγή χαρακτηριστικών που να μπορούν να γενικευτούν σε άτομα που δεν υπήρχαν στο αρχικό σύνολο εκπαίδευσης. Γι' αυτόν τον λόγο, μελέτες έχουν δείξει ότι τα «ευρύτερα» σύνολα δεδομένων (αυτά που περιέχουν χιλιάδες διαφορετικά άτομα, ακόμα και με λιγότερες φωτογραφίες για το καθένα) προσφέρουν μεγαλύτερη ακρίβεια και ικανότητα γενίκευσης σε σχέση με τα «βαθύτερα» σύνολα (που έχουν πολλές φωτογραφίες από λίγα άτομα). Ως εκ τούτου, τα άτομα που ανήκουν σε λιγότερο προβεβλημένες ομάδες ή υποαντιπροσωπεύονται καθίστανται σημαντικά πιο επιρρεπή σε εσφαλμένες ταυτοποιήσεις, μετατρέποντας ένα τεχνικό έλλειμμα (την απουσία δεδομένων) σε ζήτημα άνισης μεταχείρισης και διάκρισης¹³⁹.

¹³⁷ Zuiderveen Borgesius, F.J. (2020) 'Strengthening legal protection against discrimination by algorithms and artificial intelligence', *The International Journal of Human Rights*, 24(10), pp. 1572–1593.

¹³⁸ Raposo, V.L. (2022) 'Remote biometric identification for law enforcement in the EU: the end of anonymity in public spaces?', *European Public Law*, 28(4), σσ. 527–528.

¹³⁹ Buolamwini, J. and Gebru, T. (2018) 'Gender shades: Intersectional accuracy disparities in commercial gender classification', *Proceedings of Machine Learning Research*, 81, pp. 77–91. Διαθέσιμο στο: <https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf> (Πρόσβαση: Φεβρουάριος 2026).

Συμπερασματικά, λοιπόν, προκειμένου να αποφευχθούν εσφαλμένες ταυτοποιήσεις λόγω της ύπαρξης ανεπαρκών βάσεων δεδομένων εκπαίδευσης και κακής ποιότητας των δεδομένων σε αυτές, πρέπει να εφαρμοστούν υποχρεώσεις σχετικές με τη διαχείριση ποιότητας και τη διακυβέρνηση δεδομένων σε όλες τις φάσεις του συστήματος, με τις αρχές της διαφάνειας και της επεξηγησιμότητας να παίζουν κεντρικό ρόλο. Η εν λόγω διαδικασία καθίσταται ιδιαιτέρως δυσχερής, δεδομένου ότι τα συστήματα αυτά λειτουργούν εγγενώς ως «μαύρα κουτιά» (black boxes). Το γεγονός αυτό περιορίζει δραστικά τη δυνατότητα πλήρους ερμηνείας και κατανόησης του τρόπου με τον οποίο εξάγουν τα αποτελέσματά τους.

7 ΟΙ ΠΡΟΥΠΟΘΕΣΕΙΣ ΠΕΡΙΟΡΙΣΜΟΥ ΤΩΝ ΘΕΜΕΛΙΩΔΩΝ ΔΙΚΑΙΩΜΑΤΩΝ

Όπως διαφάνηκε από τα εκτεθέντα της προηγούμενης ενότητας, μολονότι η βιομετρική ταυτοποίηση σε δημόσιους χώρους δύναται να εξυπηρετήσει θεμιτούς σκοπούς (όπως ο εντοπισμός αγνοουμένων προσώπων), εντούτοις η λειτουργία της συνεπάγεται τη συρρίκνωση της ιδιωτικότητας των πολιτών και τη δημιουργία ενός καθεστώτος διαρκούς επιτήρησης, το οποίο κρίνεται μη ανεκτό σε μια δημοκρατία που διέπεται από ευρωπαϊκές αξίες¹⁴⁰. Σύμφωνα με το άρθρο 52 παράγραφος 1 του Χάρτη, κάθε περιορισμός στην άσκηση των θεμελιωδών δικαιωμάτων και ελευθεριών πρέπει να προβλέπεται από τον νόμο και να σέβεται τον «πυρήνα» των εν λόγω δικαιωμάτων και ελευθεριών. Τηρουμένης της αρχής της αναλογικότητας, περιορισμοί επιτρέπεται να επιβάλλονται μόνον εφόσον είναι αναγκαίοι και ανταποκρίνονται πραγματικά σε στόχους γενικού ενδιαφέροντος που αναγνωρίζει η ΕΕ ή στην ανάγκη προστασίας των δικαιωμάτων και ελευθεριών των τρίτων. Η τρίτη παράγραφος του ίδιου άρθρου παραπέμπει στην ΕΣΔΑ, υπό την έννοια ότι όταν τα δικαιώματα που προβλέπονται στον Χάρτη αντιστοιχούν σε εκείνα που περιέχονται σε αυτήν, η έννοια και η εμβέλειά τους είναι ταυτόσημες.

Υπό το πρίσμα των ανωτέρω, θα ακολουθήσει η ανάλυση των αρχών της **νομοθετικής πρόβλεψης**, της **αναλογικότητας** και της **αναγκαιότητας** σε μια δημοκρατική κοινωνία, οι οποίες συνδέονται στενά μεταξύ τους. Το ουσιώδες ερώτημα που πρέπει να απαντηθεί είναι: αποτελούν τα FRTs ένα αναλογικό και αναγκαίο μέτρο σε μια δημοκρατική κοινωνία;

7.1 Νομοθετική πρόβλεψη

Βάσει του Άρθρου 52(1) του Χάρτη, οιοσδήποτε περιορισμός θεμελιώδους δικαιώματος ή ελευθερίας δύναται να επιτραπεί μόνον εφόσον προβλέπεται εκ του νόμου. Η νομολογία του ΕΔΔΑ έχει διευκρινίσει ότι απλά και μόνο η ύπαρξη νόμου δεν αρκεί, ενώ παράλληλα απαιτείται η διασφάλιση της «ποιότητας του νόμου». Η έννοια αυτή προϋποθέτει ότι το κανονιστικό πλαίσιο είναι συμβατό με τις αρχές του κράτους δικαίου, προσβάσιμο και, κυρίως, προβλέψιμο για τους πολίτες. Όπως καταδείχθηκε στις υποθέσεις *Klass* κατά

¹⁴⁰ Sousa Silva, N. (2025) 'The artificial intelligence act: critical overview', *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 16(1), σσ. 2–23.

Γερμανίας¹⁴¹, Shimonovos κατά Ρωσίας¹⁴², Uzun κατά Γερμανίας¹⁴³, ο νόμος οφείλει να καθορίζει με σαφήνεια τις συνθήκες και τις περιστάσεις υπό τις οποίες οι αρχές νομιμοποιούνται να προβαίνουν σε επεξεργασία βιομετρικών δεδομένων, ώστε να παρέχεται επαρκής προστασία έναντι της αυθαιρεσίας. Επισημαίνεται ότι, όσον αφορά τις αναγκαίες εγγυήσεις, η απαίτηση για την ποιότητα του νόμου και η αρχή της αναλογικότητας εξετάζονται συχνά από κοινού.

Στο πλαίσιο των συστημάτων αναγνώρισης προσώπου, η απαίτηση για σαφήνεια και ακρίβεια καθίσταται ακόμα πιο επιτακτική λόγω της φύσης των βιομετρικών δεδομένων και του κινδύνου μαζικής επιτήρησης. Η νομοθεσία πρέπει να θεσπίζει αυστηρές εγγυήσεις, προσδιορίζοντας τη φύση των αδικημάτων, τα οποία σύμφωνα με το ΔΕΕ πρέπει να αφορούν μόνο «σοβαρό έγκλημα», την κατηγορία των υποκειμένων, τη διάρκεια της διατήρησης των δεδομένων, καθώς και τις διαδικασίες εποπτείας και έννομης προστασίας¹⁴⁴. Ελλείψει τέτοιων ειδικών και λεπτομερών ρυθμίσεων, η χρήση FRT συνιστά ανεπίτρεπτη παραβίαση των δικαιωμάτων, ακόμη και αν ο επιδιωκόμενος σκοπός είναι θεμιτός¹⁴⁵.

Αναφορικά με την Πράξη για την Τεχνητή Νοημοσύνη (ΑΙΑ), παρόλο που θέτει αυστηρές προϋποθέσεις για τη χρήση συστημάτων βιομετρικής ταυτοποίησης εξ αποστάσεως σε πραγματικό χρόνο (π.χ. προηγούμενη δικαστική άδεια, εγγραφή σε βάση δεδομένων, εκτίμηση αντικτύπου), διευκρινίζεται ρητά ότι δεν αποτελεί από μόνη της τη νομική βάση για την επεξεργασία προσωπικών δεδομένων (Αιτιολογική Σκέψη 38). Συνεπώς, τα Κράτη Μέλη που επιθυμούν να κάνουν χρήση των εξαιρέσεων του ΑΙΑ για σκοπούς επιβολής του νόμου, υποχρεούνται να θεσπίσουν εθνική νομοθεσία ειδικά για την εν λόγω περίπτωση.

¹⁴¹ *Case of Klass and Others v. Germany* (1978) European Court of Human Rights, Application no. 5029/71.

¹⁴² *Case of Shimonovos v. Russia* (2011) European Court of Human Rights, Application no. 30194/09.

¹⁴³ *Case of Uzun v. Germany* (2010) European Court of Human Rights, Application no. 35623/05.

¹⁴⁴ ΔΕΕ (2014) *Συνεκδικασθείσες υποθέσεις C-293/12 και C-594/12, Digital Rights Ireland Ltd κατά Minister for Communications, Marine and Natural Resources* κ.λπ. Διαθέσιμο στο: https://infocuria.curia.europa.eu/tabs/jurisprudence?sort=DOC_DATE-DESC&searchTerm=%22c-293%2F12%22&publishedId=c-293%2F12 (Πρόσβαση: Φεβρουάριος 2026).

¹⁴⁵ *R (on the application of Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058. Διαθέσιμο στο: <https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf> (Πρόσβαση: Φεβρουάριος 2026).

7.2 Η Αρχή της Αναλογικότητας ως Κριτήριο Νομιμότητας

Το δεύτερο θεμελιώδες κριτήριο -και αναμφίβολα το πλέον κρίσιμο για τον περιορισμό των δικαιωμάτων- είναι η αρχή της αναλογικότητας, η οποία λειτουργεί ως κατευθυντήρια αρχή για τη στάθμιση μεταξύ του οφέλους από την προστασία ενός δημόσιου αγαθού και της βλάβης που προκαλείται στο ατομικό δικαίωμα. Ο έλεγχος αυτός διενεργείται σε τρία διακριτά στάδια: α) την καταλληλότητα (suitability) του μέτρου για την επίτευξη του επιδιωκόμενου σκοπού, β) την αναγκαιότητα (necessity), ήτοι την επιβεβαίωση ότι δεν υφίσταται άλλο ηπιότερο μέσο με την ίδια αποτελεσματικότητα και γ) την αναλογικότητα υπό στενή έννοια (stricto sensu), η οποία εξετάζει εάν το βάρος που επιβάλλεται στο υποκείμενο είναι ανάλογο σε σχέση με το επιδιωκόμενο σκοπό. Η αξιολόγηση της αναλογικότητας διενεργείται πάντοτε εκ των προτέρων (ex ante) σύμφωνα με τη σχετική νομοθεσία.

Συνεπώς, πρόκειται για μια διεργασία στάθμισης που στοχεύει στην εύρεση της ισορροπίας μεταξύ του κόστους (επέμβαση στα δικαιώματα) και του οφέλους (σημασία του επιδιωκόμενου στόχου σε ένα δεδομένο πλαίσιο). Ζητούμενο είναι η διασφάλιση ότι το μέτρο δεν είναι δυσανάλογο και μη ανεκτό, ώστε να υφίσταται μια δίκαιη ισορροπία (fair balance) μεταξύ του ληφθέντος μέτρου και του περιοριζόμενου δικαιώματος. Κατ' επέκταση, μπορεί να υποστηριχθεί ότι ένα μέτρο είναι αναλογικό εάν ο περιορισμός προάγει το δημόσιο συμφέρον περισσότερο από όσο επιβαρύνει («θυσιάζει») τα δικαιώματα. Εξ αυτού συνάγεται ότι ο περιορισμός των δικαιωμάτων πρέπει να διενεργείται κατά τρόπο απολύτως αναγκαίο (strictly necessary) για τη διασφάλιση της προστασίας των συμφερόντων χάριν των οποίων επιβάλλεται, με τα οφέλη να υπερτερούν της προκληθείσας βλάβης.

Η νομολογία του ΕΔΔΑ αναδεικνύει την κρισιμότητα των διαδικαστικών εγγυήσεων κατά την εφαρμογή της αρχής της αναλογικότητας. Στην υπόθεση Yefimov κατά Ρωσίας, η έλλειψη δικαστικού ελέγχου και η αυτοματοποιημένη συμπερίληψη σε λίστες υπόπτων κρίθηκαν δυσανάλογα μέτρα παραβιάζοντας καταφανώς τη Σύμβαση¹⁴⁶. Αντιθέτως, σε υποθέσεις μαζικής παρακολούθησης, το Δικαστήριο αναγνώρισε στα κράτη ευρύ

¹⁴⁶ Yefimov και Youth Human Rights Group κατά Ρωσίας (2021) Αρ. Προσφυγών 12385/15 και 51619/15, Ευρωπαϊκό Δικαστήριο Δικαιωμάτων του Ανθρώπου. Διαθέσιμο στο: [https://hudoc.echr.coe.int/eng/#{%22itemid%22:\[%22001-213913%22\]}](https://hudoc.echr.coe.int/eng/#{%22itemid%22:[%22001-213913%22]}) (Πρόσβαση: Φεβρουάριος 2026)

«περιθώριο εκτίμησης» για λόγους εθνικής ασφάλειας, υπό την προϋπόθεση όμως ότι υφίσταται ρητή νομική βάση και αυστηρές εγγυήσεις¹⁴⁷. Ωστόσο, όπως διατυπώθηκε στην υπόθεση *S. and Marper* κατά *H.B.*, η αδιάκριτη διατήρηση βιομετρικών δεδομένων μεταξύ καταδικασθέντων και υπόπτων υπερβαίνει το αποδεκτό περιθώριο εκτίμησης και παραβιάζει την ιδιωτική ζωή¹⁴⁸.

Ειδικότερα για τα συστήματα αναγνώρισης προσώπου, η εφαρμογή της αναλογικότητας απαιτεί αυστηρή στάθμιση λόγω της υψηλής παρεμβατικότητας της εν λόγω τεχνολογίας. Το μέτρο κρίνεται αναγκαίο μόνο εάν ο στόχος (π.χ. πρόληψη σοβαρού εγκλήματος) δεν μπορεί να επιτευχθεί με ηπιότερα μέσα, όπως η συμβατική βιντεοεπιτήρηση. Δεδομένου ότι η «χρησιμότητα» για τις αρχές επιβολής του νόμου δεν ταυτίζεται με την «αναγκαιότητα», και λαμβάνοντας υπόψη τον κίνδυνο ψευδών θετικών αποτελεσμάτων, η απλή νομοθετική πρόβλεψη δεν αρκεί. Απαιτείται *in concreto* αξιολόγηση ώστε να μην θυσιάζονται θεμελιώδη δικαιώματα στον βωμό μιας αβέβαιης ασφάλειας.

7.3 Αναγκαιότητα σε μία δημοκρατική κοινωνία

Η έκφραση «αναγκαίο σε μια δημοκρατική κοινωνία», όπως διατυπώθηκε στην υπόθεση του ΕΔΔΑ *Piechowicz* κατά Πολωνίας, σημαίνει ότι η επέμβαση στον νόμο πρέπει να ανταποκρίνεται σε μια πιεστική κοινωνική ανάγκη και, ειδικότερα, πρέπει να είναι ανάλογη προς τον επιδιωκόμενο θεμιτό σκοπό¹⁴⁹. Κατά την αξιολόγηση του εάν μια επέμβαση είναι αναγκαία, όπως και με το προηγούμενο κριτήριο, πρέπει να λαμβάνεται υπόψη το περιθώριο εκτίμησης που αφήνεται στις κρατικές αρχές για να αποφασίσουν πώς θα επιτύχουν καλύτερα τον θεμιτό σκοπό της προστασίας της ασφάλειας, με το Κράτος να φέρει επίσης το βάρος της απόδειξης της ύπαρξης αυτής της πιεστικής κοινωνικής ανάγκης που υποκρύπτεται στην επέμβαση.

¹⁴⁷ *Big Brother Watch and Others v. the United Kingdom* [GC] (2021) Application nos. 58170/13, 62322/14 and 24960/15, European Court of Human Rights. Διαθέσιμο στο: <https://hudoc.echr.coe.int/fre#%7B%22itemid%22%3A%22001-186048%22%7D> (Πρόσβαση: Φεβρουάριος 2026)

¹⁴⁸ *S. and Marper v. the United Kingdom* [GC] (2008) Application nos. 30562/04 and 30566/04, European Court of Human Rights.

¹⁴⁹ Βλ. παρ. 212 *Piechowicz v. Poland* (2012) Application no. 20071/07, European Court of Human Rights.

Το ΕΣΔΠ αποφαινεται επίσης επί του κριτηρίου του «αυστηρώς αναγκαίου» αναφορικά με την επεξεργασία ειδικών κατηγοριών δεδομένων, όπως τα βιομετρικά δεδομένα, όπου μπορεί να θεωρηθεί «απολύτως αναγκαίο» «μόνον εάν η παρέμβαση στην προστασία των δεδομένων προσωπικού χαρακτήρα και οι περιορισμοί της περιορίζονται σε ό,τι είναι απολύτως αναγκαίο, δηλαδή απαραίτητο, και αποκλείεται κάθε επεξεργασία γενικού ή συστηματικού χαρακτήρα». Υποστηρίζει περαιτέρω ότι ο όρος «αυστηρώς» αναγκάζει τον νομοθέτη να τηρεί ακόμη πιο αυστηρές προϋποθέσεις σε σχέση με την απλή αναγκαιότητα, ελαχιστοποιώντας έτσι το περιθώριο εκτίμησης των αρχών. Τέλος, η εφαρμογή του μέτρου πρέπει να βασίζεται σε αντικειμενικά κριτήρια που προσδιορίζουν συγκεκριμένες περιστάσεις, αποκλείοντας κατηγορηματικά κάθε μορφή γενικής ή συστηματικής παρακολούθησης¹⁵⁰.

7.4 Τελικές Σκέψεις εν είδει συμπερασμάτων

Όπως προαναφέρθηκε, η βιομετρική ταυτοποίηση συνιστά περιορισμό των θεμελιωδών δικαιωμάτων και πρέπει να υπόκειται σε έλεγχο αυστηρής αναγκαιότητας και αναλογικότητας, ο οποίος προϋποθέτει και την ύπαρξη σαφούς νομοθετικής πρόβλεψης. Ο έλεγχος αυτός πρέπει να λαμβάνει υπόψη το πλαίσιο και όλες τις υφιστάμενες περιστάσεις και παραμέτρους. Ως εκ τούτου, η ευαισθησία των δεδομένων ή ο τρόπος χρήσης τους αποτελούν σημαντικά στοιχεία για τον εν λόγω έλεγχο. Πέρα από τις εγγυήσεις θεμελιωδών δικαιωμάτων και τις βασικές αρχές προστασίας δεδομένων που απορρέουν από το Άρθρο 8 του Χάρτη, όπως ερμηνεύεται από το ΔΕΕ, ειδικές εγγυήσεις βάσει του κεκτημένου της ΕΕ για την προστασία δεδομένων ενισχύουν περαιτέρω τον έλεγχο αναγκαιότητας και αναλογικότητας.

Δυνάμει του Άρθρου 9 παράγραφος 2 στοιχείο ζ) του ΓΚΠΔ, η επεξεργασία βιομετρικών δεδομένων επιτρέπεται μόνο όταν 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». Το Άρθρο 10 της

¹⁵⁰ Ο.π. υποσημείωση 14

Οδηγίας για την επιβολή του νόμου (LED) θέτει παρόμοιες, αν και ελαφρώς πιο ελαστικές, προϋποθέσεις.

Η υιοθέτηση μιας προσέγγισης προσανατολισμένης στην προστασία των θεμελιωδών δικαιωμάτων συνεπάγεται ότι τα Κράτη Μέλη δεν πρέπει να εξετάζουν μεμονωμένα κάθε χρήση RBI, αρκούμενα σε έναν *ad hoc* έλεγχο αναλογικότητας. Αντιθέτως, οφείλουν να υιοθετήσουν μια ολιστική προσέγγιση, εξετάζοντας τον τρόπο με τον οποίο οι τεχνολογίες αυτές μπορούν να ενταχθούν ομαλά στο εθνικό νομικό πλαίσιο με απόλυτο σεβασμό στα ανθρώπινα δικαιώματα. Προς αυτή την κατεύθυνση, η θέσπιση λεπτομερούς εθνικής νομοθεσίας καθίσταται επιτακτική, δεδομένου ότι η ΕΕ διαθέτει περιορισμένες αρμοδιότητες στο ποινικό δικονομικό δίκαιο. Είναι χαρακτηριστικό ότι οι αυστηροί κανόνες για την κατ' εξαίρεση χρήση της FRT σε πραγματικό χρόνο θα ταίριαζαν περισσότερο σε εθνικούς κώδικες ποινικής δικονομίας, παρά σε έναν ευρωπαϊκό κανονισμό για την Τεχνητή Νοημοσύνη, ο οποίος εδράζεται κυρίως στους κανόνες της εσωτερικής αγοράς και της προϊόντικής ασφάλειας. Άλλωστε, οι ποινικές διαδικασίες -και ιδίως η συλλογή, η χρήση και το παραδεκτό των αποδεικτικών μέσων- ρυθμίζονται εγγενώς από το εθνικό δίκαιο. Επομένως, εάν τα Κράτη Μέλη προτίθενται να αξιοποιήσουν την FRT για την επιβολή του νόμου, υποχρεούνται να θεσπίσουν σαφείς κανόνες και περιορισμούς στην εθνική τους νομοθεσία. Καθώς η Πράξη για την TN παρέχει μεν κατευθυντήριες γραμμές, αλλά δεν συνιστά από μόνη της ένα αυτόνομο και πλήρες νομικό πλαίσιο, η ασφαλής χρήση τέτοιων συστημάτων απαιτεί τη δημιουργία συμπληρωματικών εθνικών ρυθμίσεων πέραν του ΑΙΑ. Λαμβάνοντας υπόψη το νομοθετικό παράδειγμα της Σουηδίας, γίνεται αντιληπτό ότι τα τελευταία χρόνια τα θεμελιώδη δικαιώματα περιορίζονται ολοένα και περισσότερο στο όνομα της καταπολέμησης του οργανωμένου εγκλήματος ή της προστασίας της ασφάλειας. Μέτρα μυστικής παρακολούθησης, οι λεγόμενες «ζώνες ασφαλείας», η αυξημένη βιντεοεπιτήρηση και οι περιορισμοί στην ελευθερία του συνέρχεσθαι είναι μερικά μόνο από τα μέτρα που προτάθηκαν την τελευταία πενταετία. Η άδεια χρήσης της RBI, ακόμη και

εντός των ορίων της Πράξης για την ΤΝ, αποτελεί ένα ακόμη βήμα προς αυτή την κατεύθυνση¹⁵¹.

Η ανησυχητική αυτή τάση εντείνεται από το γεγονός ότι, παρά τις φιλόδοξες στοχεύσεις της ίδιας της Πράξης για την Τεχνητή Νοημοσύνη, η κριτική ανάλυση του κειμένου αποκαλύπτει σημαντικά κανονιστικά κενά. Αρχικά, η απαγόρευση των συστημάτων RBI σε «πραγματικό χρόνο» περιορίζεται αποκλειστικά στις αρχές επιβολής του νόμου, αφήνοντας εκτός πλαισίου άλλους δημόσιους ή ιδιωτικούς φορείς. Αυτή η επιλογή φαίνεται να παραγνωρίζει το γεγονός ότι οι κίνδυνοι για τα δικαιώματα είναι εγγενείς στην τεχνολογία και δεν εξαρτώνται από τον εκάστοτε σκοπό χρήσης της. Επιπλέον, οι προβλεπόμενες εξαιρέσεις από την απαγόρευση εγκυμονούν τον κίνδυνο καταχρηστικής εκμετάλλευσης. Έννοιες όπως η «άμεση απειλή» ή η αποτροπή «τρομοκρατικής επίθεσης» παραμένουν εννοιολογικά ασαφείς, παρέχοντας ευρεία διακριτική ευχέρεια στην εκτελεστική εξουσία. Ακόμα και αν η προηγούμενη δικαστική ή διοικητική άδεια συνιστά την εγγυητική βάση του συστήματος, η δυνατότητα αναβολής της σε «επείγουσες περιπτώσεις» θέτει εν αμφιβόλω τον έλεγχο της αναλογικότητας, προλειαίνοντας το έδαφος για πρακτικές μαζικής επιτήρησης.

Από την άλλη πλευρά, η θέσπιση ενός άκαμπτου, εξαντλητικού καταλόγου αδικημάτων ενδέχεται να καταστεί γρήγορα παρωχημένη λόγω της ραγδαίας τεχνολογικής εξέλιξης, αφήνοντας αργύθμιστα νέα εγκλήματα, όπως η δημιουργία παιδικής πορνογραφίας μέσω ΤΝ^{152 153}. Για τον λόγο αυτό, προκρίνεται η ανάγκη για έναν ευέλικτο και δυναμικό (future-proof) κατάλογο αδικημάτων. Ένα επιπρόσθετο προβληματικό σημείο συνιστά η αδικαιολόγητη διαφοροποίηση μεταξύ της χρήσης RBIs σε «πραγματικό» και σε «μεταγενέστερο» χρόνο. Όπως έχει τονιστεί και από το Ευρωπαϊκό Κοινοβούλιο, η διάκριση αυτή είναι αμιγώς τεχνική, καθώς οι συνέπειες για την επιτήρηση των πολιτών παραμένουν

¹⁵¹ Walde, F. (2024) *Surveilling the surveillance: ensuring an effective protection of fundamental rights when using real-time remote biometric identification in EU Member States after the AI Act*. Μεταπτυχιακή Διπλωματική Εργασία. Lund University.

¹⁵² Niedbała, M. (2023) 'The Problem of Criminal Liability for Generating Pornography Using Artificial Intelligence', *Krytyka Prawa*, 15(4), σσ. 69–79. Διαθέσιμο στο: <https://doi.org/10.7206/kp.2080-1084.639> (Πρόσβαση: Ιανουάριος 2026).

¹⁵³ AllahRakha, N. (2024) 'Cybercrime and the Legal and Ethical Challenges of Emerging Technologies', *International Journal of Law and Policy*, 2(5), σσ. 28–36. Διαθέσιμο στο: <https://doi.org/10.59022/ijlp.191> (Πρόσβαση: Ιανουάριος 2026).

ακριβώς οι ίδιες. Εστιάζοντας μονομερώς στους «υπόπτους», ο Κανονισμός φαίνεται να παραγνωρίζει το γεγονός ότι η βιομετρική αναγνώριση προσώπων σε δημόσιο χώρο θίγει αδιακρίτως το σύνολο του πληθυσμού.

Συμπερασματικά, καθίσταται σαφές ότι η Πράξη για την TN δεν προορίζεται να λειτουργήσει ως θετική νομική βάση νομιμοποίησης της δράσης των διωκτικών αρχών, αλλά πρωτίστως ως ένας μηχανισμός χάραξης «κόκκινων γραμμών»¹⁵⁴. Συνεπώς, η αποτροπή της κανονικοποίησης της εξ αποστάσεως βιομετρικής ταυτοποίησης και η προστασία των δημοκρατικών κεκτημένων επαφίεται, εν τέλει, στην αυστηρότητα των εθνικών νομοθεσιών που θα κληθούν να εξειδικεύσουν αυτούς τους κανόνες. Ως εκ τούτου, κατά την άποψη της γράφουσας, κρίσιμο είναι τα Κράτη Μέλη να ερμηνεύουν τις εξαιρέσεις από την απαγόρευση της RBI υπό στενή έννοια. Τα θεμελιώδη δικαιώματα δεν μπορούν να θεωρηθούν ότι προστατεύονται επαρκώς, εάν αντιμετωπίζονται απλώς ως υστερόβουλη σκέψη ή ως τυπική προϋπόθεση (box to be checked off). Η στενή ερμηνεία των εξαιρέσεων αποτελεί τη λογική συνέπεια της ερμηνείας της Πράξης για την TN σύμφωνα με τον στόχο της για υψηλό επίπεδο προστασίας των δικαιωμάτων. Είναι επίσης η συνέπεια της αντιμετώπισης των εξαιρέσεων ως ακριβώς αυτό που είναι: μια προαιρετική εξαίρεση σε μια κατά τα άλλα απαγορευμένη πρακτική.

¹⁵⁴ Simmler, M. and Canova, G. (2020) 'Facial recognition technology in law enforcement: Regulating data analysis of another kind', *Computer Law & Security Review*, 39, p. 105481. Διαθέσιμο στο: <https://doi.org/10.1016/j.clsr.2020.105481> (Πρόσβαση: Φεβρουάριος 2026).

8 ΣΥΜΠΕΡΑΣΜΑΤΑ

Ολοκληρώνοντας την παρούσα μελέτη, καθίσταται σαφές ότι η ενσωμάτωση των συστημάτων Αναγνώρισης Προσώπου (FR) στο οπλοστάσιο των διωκτικών αρχών δεν συνιστά μια απλή τεχνική αναβάθμιση, αλλά μια θεμελιώδη πρόκληση για το ίδιο το κράτος δικαίου. Η μετατόπιση της τεχνολογίας από αυστηρά ελεγχόμενα περιβάλλοντα σε δημόσιους χώρους, σηματοδότησε την απαρχή μιας ανεξέλεγκτης επεξεργασίας δεδομένων. Η διαρκής ανάγκη εκπαίδευσης των αλγορίθμων οδήγησε σε μαζική άντληση (scraping) εικόνων από το διαδίκτυο και από συστήματα βιντεοεπιτήρησης, παρακάμπτοντας κατά κανόνα τη θεμελιώδη προϋπόθεση της συναίνεσης. Η πρακτική αυτή πυροδότησε μια βαθιά νομική και ηθική κρίση, καθώς τα δικαιώματα της ιδιωτικής ζωής και της προστασίας των προσωπικών δεδομένων υποχώρησαν μπροστά στην ταχύτητα της τεχνολογικής εξέλιξης. Επιπροσθέτως, η ευρεία διαθεσιμότητα των συστημάτων αυτών οδήγησε στην απώλεια ελέγχου εκ μέρους των ίδιων των δημιουργών τους αναφορικά με τον τελικό σκοπό και τρόπο χρήσης των μοντέλων¹⁵⁵.

Στο πλαίσιο αυτό, ο ΑΙΑ αποτελεί αναμφίβολα ένα ιστορικό βήμα της Ευρωπαϊκής Ένωσης προς τη δημιουργία ενός «ανθρωποκεντρικού» πλαισίου ψηφιακής διακυβέρνησης. Ωστόσο, η αποτελεσματικότητά του παραμένει υπό αίρεση. Η παρούσα εργασία κατέδειξε ότι, αφενός ο Κανονισμός φιλοδοξεί να περιορίσει τη μαζική επιτήρηση, αφετέρου όμως οι εκτεταμένες εξαιρέσεις που εισάγονται για λόγους εθνικής ασφάλειας και καταστολής σοβαρών εγκλημάτων δημιουργούν μια λεπτή γραμμή μεταξύ της προστασίας του πολίτη και της αδικαιολόγητης επέμβασης στην ιδιωτικότητά του. Ο κίνδυνος του «chilling effect», δηλαδή της αποτροπής των πολιτών από την άσκηση των ελευθεριών τους σε δημόσιους χώρους υπό τον φόβο της ταυτοποίησης, παραμένει υπαρκτός παρά τις προβλεπόμενες εγγυήσεις.

Συμπερασματικά, η «δίκαιη ισορροπία» που επιδιώκει ο νομοθέτης δεν μπορεί να επιτευχθεί μόνο μέσω της θέσπισης κανόνων, αλλά απαιτεί διαρκή δικαστικό και διοικητικό έλεγχο, διαφάνεια στις αλγοριθμικές διαδικασίες και, κυρίως, μια συνεκτική εφαρμογή σε όλα τα

¹⁵⁵ Raji, I.D. και Fried, G. (2021) 'About Face: A Survey of Facial Recognition Evaluation', *arXiv preprint arXiv:2102.00813*. Διαθέσιμο στο: <https://arxiv.org/abs/2102.00813> (Πρόσβαση: Φεβρουάριος 2026).

Κράτη Μέλη ώστε να μην επιτραπεί ο κανονιστικός κατακερματισμός. Η αποτελεσματικότητα του ρυθμιστικού πλαισίου θα κριθεί στην πράξη: εκεί όπου η ανάγκη των αρχών για δημόσια ασφάλεια θα αναπτύσσεται με απόλυτο σεβασμό, και όχι εις βάρος, της ανθρώπινης αξιοπρέπειας και των ατομικών ελευθεριών.

9 ΠΗΓΕΣ ΚΑΙ ΑΝΑΦΟΡΕΣ

ΕΛΛΗΝΙΚΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

- Βασιλακοπούλου, Ε. (2021) Βιομετρικά και Γενετικά δεδομένα, Γενικός Κανονισμός για την Επεξεργασία Προσωπικών δεδομένων, Νομική διάσταση και πρακτική εφαρμογή. Αθήνα: Νομική Βιβλιοθήκη.
- Γεωργίου, Σ. (2021) *Αυτόματη αναγνώριση προσώπου στους δημόσιους χώρους: Μεταξύ πραγματικότητας και δυστοπίας*. Διαθέσιμο σε: https://www.syntagmawatch.gr/trending-issues/aytomati-anagnwrisi-proswpou-stous-dhmosious-xwrous-metaxy-pragmatikothtas-kai-dystopias/#_ftn4 (Πρόσβαση: Δεκέμβριος 2025).
- Δαγτόγλου, Π.Δ. (2012) *Συνταγματικό Δίκαιο: Ατομικά Δικαιώματα*. 4η αναθ. έκδ. Αθήνα-Θεσσαλονίκη: Εκδόσεις Σάκκουλα.
- Κανέλλος, Α. (επιμ.) (2023) *The GDPR Handbook: Η κανονιστική συμμόρφωση στο εργασιακό και επιχειρησιακό περιβάλλον*. 2η έκδ. Αθήνα: Νομική Βιβλιοθήκη.
- Λαζαράκος, Γ. (2016) «Τα συνταγματικά όρια της επεξεργασίας βιομετρικών δεδομένων (Κεφάλαιο 11ο)», στο Κοτσαλής, Α. και Λαζαράκος, Γ. (επιμ.) *Προσωπικά Δεδομένα*. Αθήνα: Νομική Βιβλιοθήκη.
- Σκόνδρα, Μ. (2020) *Συστήματα Βιντεοεπιτήρησης, αναγνώριση προσώπου και Προστασία Προσωπικών Δεδομένων, Μελέτες Γνωμοδοτήσεις*, σελ. 53 επ..
- Χαμπίδης, Κ. και Κιουμουρτζής, Γ. (2019) *Πρέπει να μπει φρένο στην αναγνώριση προσώπου; Εφημερίδα Καθημερινή*. Διαθέσιμο σε: <https://www.kathimerini.gr/opinion/1025741/prepei-na-mpei-freno-stin-anagnorisi-prosopoy/> (Πρόσβαση: Δεκέμβριος 2025).

ΞΕΝΟΓΛΩΣΣΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

Adler, A. and Schuckers, M. E. (2007) 'Comparing Human and Automatic Face Recognition Performance', *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, 37(5), pp. 1248–1255. Διαθέσιμο σε:

<https://sci2s.ugr.es/keel/pdf/specific/articulo/Comparing%20Human%20and%20Automatic%20Face%20Recognition%20Performance.pdf> (Πρόσβαση: Φεβρουάριος 2026).

Albrizio, A. (2007) 'Biometry and Anthropometry: from Galton to Constitutional Medicine', *Journal of Anthropological Sciences*, 85, pp. 101-123.

AllahRakha, N. (2024) 'Cybercrime and the Legal and Ethical Challenges of Emerging Technologies', *International Journal of Law and Policy*, 2(5), pp. 28–36. Διαθέσιμο στο: <https://doi.org/10.59022/ijlp.191> (Πρόσβαση: Ιανουάριος 2026).

Ammanath, B. (2022) *Trustworthy AI: A Business Guide for Navigating Trust and Ethics in AI*. Hoboken, New Jersey: John Wiley & Sons.

Barkane, I. and Buka, L. (2023) 'Prohibited AI surveillance practices in the Artificial Intelligence Act: promises and pitfalls in protecting fundamental rights', in McDaniel, J.L.M. and Peeters, K. (eds) *Critical Perspectives on Predictive Policing*. Cheltenham: Edward Elgar Publishing, pp. 110–129.

Bathae, Y. (2018) 'The Artificial Intelligence Black Box and the Failure of Intent and Causation', *Harvard Journal of Law & Technology*, 31(2), pp. 889-938. Διαθέσιμο στο:

<https://jolt.law.harvard.edu/assets/articlePDFs/v31/The-Artificial-Intelligence-Black-Box-and-the-Failure-of-Intent-and-Causation-Yavar-Bathae.pdf> (Πρόσβαση: Ιανουάριος 2026).

Belhumeur, P.N., Hespanha, J.P. and Kriegman, D.J. (1997) "Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 19(7), pp. 711–720.

Bennett, K. A. (2001) 'Can Facial Recognition Technology Be Used to Fight the New Way against Terrorism: Examining the Constitutionality of Facial Recognition Surveillance Systems', *North Carolina Journal of Law & Technology*, 3(1), pp. 151–178.

Bertuzzi, L. (2022) 'AI Act: Οι συζητήσεις του Ευρωπαϊκού Κοινοβουλίου εντείνονται για την αναγνώριση προσώπου και το πεδίο εφαρμογής', *Euractiv*, 6 Οκτωβρίου. Διαθέσιμο στο: <https://www.euractiv.com/section/digital/news/ai-act-eu-parliaments-discussions-heat-up-over-facial-recognition-scope/> (Πρόσβαση: 25 Ιανουαρίου 2026).

Bertuzzi, L. (2024) 'Η Ευρωπαϊκή Ένωση «τετραγωνίζει τον κύκλο» για το πρώτο ρυθμιστικό πλαίσιο παγκοσμίως σχετικά με την Τεχνητή Νοημοσύνη', *Euractiv*, 15 Φεβρουαρίου. Διαθέσιμο στο: <https://www.euractiv.com/section/artificial-intelligence/news/europeanunion-squares-the-circle-on-the-worlds-first-ai-rulebook/> (Πρόσβαση: 25 Ιανουαρίου 2026).

Bledsoe, W.W. (1966) *Man-Machine Facial Recognition: Report on a Large-Scale Experiment*, Technical Report PRI 22. Palo Alto, California: Panoramic Research, Inc..

Brey, P. (2004) 'Ethical aspects of facial recognition systems in public places', *Journal of Information, Communication and Ethics in Society*, 2(2), p. 104.

Buolamwini, J. and Gebru, T. (2018) 'Gender shades: Intersectional accuracy disparities in commercial gender classification', *Proceedings of Machine Learning Research*, 81, pp. 77–91. Διαθέσιμο στο: <https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf> (Πρόσβαση: Φεβρουάριος 2026).

CDT (2024) 'Landmark EU AI Act Sets Benchmark for AI Regulation, but Fails to Meet the Bar on Human Rights Protection.' Διαθέσιμο στο: <https://cdt.org/press/landmark-eu-ai-act-sets->

(Πρόσβαση: Φεβρουάριος 2026).

Coghlan, N. (2016) 'Gaughran [2015] UKSC 29 on police biometric data retention: Strasbourg unheard, Strasbourg unheeded', *European Human Rights Law Review*, (1), pp. 61–68.

Cotino Hueso, L. (2023) 'Automated facial recognition and biometric identification systems under the overlapping regulation of artificial intelligence and data protection', in Balaguer Callejón,

- F. and Cotino Hueso, L. (eds) *Derecho Público de la Inteligencia Artificial*. Zaragoza: Fundación Manuel Jiménez Abad de Estudios Parlamentarios y del Estado Autonómico, p. 353.
- Cupać, J. και Sienknecht, M. (2024) 'Regulate against the machine: how the EU mitigates AI harm to democracy', *Democratization*, 31(5), pp. 1067–1090.
- EDRi (2020) *Ban Biometric Mass Surveillance: A set of fundamental rights demands for the European Commission and Member States*. Brussels: European Digital Rights. Διαθέσιμο στο: <https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf>
- EDRi (2021) *Civil society calls for AI Red Lines: A global call to action*. Brussels: European Digital Rights. Διαθέσιμο στο: <https://edri.org/wp-content/uploads/2021/11/Civil-society-calls-for-AI-Red-Lines.pdf> (Πρόσβαση: Φεβρουάριος 2026).
- Fussey, P. and Murray, D. (2019) *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*. Colchester: Human Rights Centre, University of Essex. Διαθέσιμο στο: <https://repository.essex.ac.uk/24946/> (Πρόσβαση: Ιανουάριος 2026).
- Greens/EFA (n.d.) *Biometric surveillance*. Διαθέσιμο στο: <https://www.greens-efa.eu/biometricsurveillance/> (Πρόσβαση: Φεβρουάριος 2026).
- Guo, Z. and Kennedy, L. (2023) 'Policing based on facial recognition', *Artificial Intelligence and Law*, 31(4), pp. 741–769. Διαθέσιμο στο: <https://link.springer.com/article/10.1007/s10506-022-09330-x> (Πρόσβαση: Ιανουάριος 2026).
- Hopkins, R. (2010) 'An Introduction to Biometrics and Large Scale Civilian Identification', *International Review of Law, Computers & Technology*, 13(3), p. 337.
- Jain, A.K., Nandakumar, K. and Ross, A. (2016) "50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities," *Pattern Recognition Letters*, 79(3.2), pp. 80–105. Διαθέσιμο στο: <https://doi.org/10.1016/j.patrec.2015.12.013>.
- Jain, A.K., Ross, A. and Prabhakar, S. (2004) 'An Introduction to Biometric Recognition', *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1), pp. 4-20.

Jasserand, C. (2016) 'Legal Nature of Biometric Data: From 'Generic' Personal Data to Sensitive Data', *European Data Protection Law Review*, 2(3), pp. 297-311. University of Groningen Faculty of Law Research Paper No. 24/2018. Διαθέσιμο στο: <https://ssrn.com/abstract=3230342>.

Jasserand, C. (2025) 'Facial Recognition in Public Spaces and the Principle of Necessity', in Menéndez González, N. and Mobilio, G. (eds.) *Next Democratic Frontiers for Facial Recognition*

- Kanade, T. (1974) *Picture processing system by computer complex and recognition of human faces*, Tech. Rep. Kyoto University. Διαθέσιμο στο: https://repository.kulib.kyoto-u.ac.jp/dspace/bitstream/2433/162079/2/D_Kanade_Takeo.pdf.
- Kayser-Bril, N. (2019) *At least 11 police forces use face recognition in the EU, AlgorithmWatch reveals*. AlgorithmWatch, 11 December. Διαθέσιμο στο: <https://algorithmwatch.org/en/face-recognition-police-europe/> (Πρόσβαση: 8 Φεβρουαρίου 2026).
- Kim, M., Jain, A. and Liu, X. (2025) '50 Years of Automated Face Recognition', *arXiv preprint arXiv:2505.24247*. Διαθέσιμο στο: <https://arxiv.org/abs/2505.24247> (Πρόσβαση: Φεβρουάριος 2026).
- Koops, B.J. (2020/2021) 'The Concept of Function Creep', *Law, Innovation and Technology*, 13(1). Διαθέσιμο στο: <https://ssrn.com/abstract=3547903> (Πρόσβαση: Ιανουάριος 2026).
- Li, L., Mu, X., Li, S. and Peng, H. (2020) 'A Review of Face Recognition Technology', *IEEE Access*, 8, pp. 139110-139120. Διαθέσιμο στο: <https://doi.org/10.1109/ACCESS.2020.3011028> (Πρόσβαση: Φεβρουάριος 2026).
- Liu, J. (2017) *In Your Face: China's all-seeing state* [Video]. BBC News, 10 December. Διαθέσιμο στο: <https://www.bbc.com/news/av/world-asia-china-42248056> (Πρόσβαση: 24 Ιανουαρίου 2020).
- Liu, N.Y. (2011) *Bio-Privacy: Privacy Regulations and the Challenge of Biometrics*. London: Routledge.
- Mordini, E. et al. (2012) 'Introduction', in Mordini, E. and Tzovaras, D. (eds) *Second Generation Biometrics: The Ethical, Legal and Social Context*. Springer, p. 8.
- Naarttijärvi, M. *AI and Sensitive Personal Data Under the Law Enforcement Directive: Between Operational Efficiency and Legal Necessity*.

- Μεταπτυχιακή Διπλωματική Εργασία:
«ΣΥΣΤΗΜΑΤΑ ΑΝΑΓΝΩΡΙΣΗΣ ΠΡΟΣΩΠΟΥ ΣΕ ΔΗΜΟΣΙΟΥΣ ΧΩΡΟΥΣ ΓΙΑ ΣΚΟΠΟΥΣ ΕΠΙΒΟΛΗΣ
ΤΟΥ ΝΟΜΟΥ: ΚΙΝΔΥΝΟΙ ΣΤΟ ΠΛΑΙΣΙΟ ΤΟΥ ΚΑΝΟΝΙΣΜΟΥ ΓΙΑ ΤΗΝ ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ»
- National Academies of Sciences, Engineering, and Medicine (2024) *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance*. Washington, DC: The National Academies Press. Διαθέσιμο στο: <https://doi.org/10.17226/62>.
- Niedbała, M. (2023) 'The Problem of Criminal Liability for Generating Pornography Using Artificial Intelligence', *Krytyka Prawa*, 15(4), pp. 69–79. Διαθέσιμο στο: <https://doi.org/10.7206/kp.2080-1084.639> (Πρόσβαση: Ιανουάριος 2026).
- O'Flaherty, M. (2020) 'Facial recognition technology and fundamental rights'. *European Data Protection Law Review (EDPL)*, 6(2), pp. 170-173.
- Oosterhof, N. N. and Todorov, A. (2008) 'The functional basis of face evaluation', *Proceedings of the National Academy of Sciences (PNAS)*, 105(32), pp. 11087–11092. Διαθέσιμο στο: <https://pubmed.ncbi.nlm.nih.gov/18685089/> (Πρόσβαση: Δεκέμβριος 2025).
- O'Toole, A.J. and Castillo, C.D. (2021) 'Face Recognition by Humans and Machines: Three Fundamental Advances from Deep Learning', *Annual Review of Vision Science*, 7, pp. 543-570.
- Paolucci, F. (2025) 'Constitutional safeguards in the age of AI: a study on the fundamental rights impact assessment of facial recognition technology'. Διδακτορική Διατριβή. Università Commerciale 'Luigi Bocconi'. Διαθέσιμο στο: https://iris.unibocconi.it/retrieve/65105e19-f61b-44e0-8972-cb69394c1359/PAOLUCCI_Revised%20Thesis_vf.pdf (Πρόσβαση: Ιανουάριος 2026).
- Partnership on AI (2020) *Understanding Facial Recognition Systems*. Διαθέσιμο στο: <https://partnershiponai.org/paper/understanding-facial-recognition-systems/> (Πρόσβαση: Φεβρουάριος 2026).
- Petrescu, R.V. (2019) 'Face Recognition as a Biometric Application', *Journal of Mechatronics and Robotics*, 3, pp. 237-257. Διαθέσιμο στο: <https://ssrn.com/abstract=3417325>. (Πρόσβαση: Ιανουάριος 2026).

- Phillips, P.J. et al. (2018) 'Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms', *Proceedings of the National Academy of Sciences (PNAS)*, 115(24), pp. 6171-6176. Διαθέσιμο στο: <https://doi.org/10.1073/pnas.1721355115>.
- Raji, I.D. and Fried, G. (2021) 'About Face: A Survey of Facial Recognition Evaluation', *arXiv preprint arXiv:2102.00813*. Διαθέσιμο στο: <https://arxiv.org/abs/2102.00813> (Πρόσβαση: Φεβρουάριος 2026).
- Raposo, V.L. (2022) 'Remote biometric identification for law enforcement in the EU: the end of anonymity in public spaces?', *European Public Law*, 28(4), pp. 527-528.
- Raposo, V.L. (2023) Look at the camera and say cheese: the existing European legal framework for facial recognition technology in criminal investigations, *Information & Communications Technology Law*, 33(1), σσ. 1-20.
- Riera, A. et al. (2012) Electrophysiological Biometrics: Opportunities and Risks, in Mordini, E. and Tzovaras, D. (eds) *Second Generation Biometrics: The Ethical, Legal and Social Context*. Springer, p. 152.
- Sachoulidou, A. (2024) 'Harnessing AI for law enforcement: solutions and boundaries from the forthcoming AI Act', *New Journal of European Criminal Law*, 15(2), pp. 117-125.
- Sáez Trigueros, D. and Meng, L. (2018) Face Recognition: From Traditional to Deep Learning Methods. Διαθέσιμο στο: <https://arxiv.org/abs/1811.00116> (Πρόσβαση: Ιανουάριος 2026).
- Salami, E. (2017) The Impact of Directive (EU) 2016/680 on the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences. Διαθέσιμο στο: <https://ssrn.com/abstract=2912449>.
- Sanchez del Rio, J. et al. (2016) Automated Border Control E-Gates and Facial Recognition Systems, *Computers & Security*, 62, p. 49. Διαθέσιμο στο: <https://www.sciencedirect.com/science/article/pii/S0167404816300736?via%3Dihub>.

Simmler, M. and Canova, G. (2020) Facial recognition technology in law enforcement: Regulating data analysis of another kind, *Computer Law & Security Review*, 39, article 105494. Διαθέσιμο στο: <https://doi.org/10.1016/j.clsr.2020.105481> (Πρόσβαση: Φεβρουάριος 2026).

Solove, D.J. (2006) A taxonomy of privacy, *University of Pennsylvania Law Review*, 154(3), p. 477.

Sousa Silva, N. (2025) 'The artificial intelligence act: critical overview', *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 16(1), pp. 2–23.

Spearman, E. (1869) *Crime and Punishment in England: A Sourcebook*. London: Routledge.

Taigman, Y., Yang, M., Ranzato, M.A. and Wolf, L. (2014) 'Deepface: Closing the gap to human-level performance in face verification', in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 1701–1708.

Turk, M. and Pentland, A. (1991) "Eigenfaces for Recognition," *Journal of Cognitive Neuroscience*, 3(1), pp. 71–86.

Van der Sloot, B. (2015) 'Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of "Big Data"', *Utrecht Journal of International and European Law*, 31(80), pp. 25-50. Διαθέσιμο στο: <http://dx.doi.org/10.5334/ujiel.cp> (Πρόσβαση: Ιανουάριος 2026).

Viola, P. and Jones, M.J. (2004) "Robust Real-Time Face Detection," *International Journal of Computer Vision*, 57(2), pp. 137–154. Διαθέσιμο στο:

Wörsdörfer, M. (2023) Mitigating the adverse effects of AI with the European Union's Artificial Intelligence Act: hype or hope?, *SSRN Electronic Journal*. Διαθέσιμο στο: <https://doi.org/10.2139/ssrn.4630087>.

Wachter, S. (2024) Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond. Διαθέσιμο στο: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4743200 (Πρόσβαση: Ιανουάριος 2026).

Walde, F. (2024) Surveilling the surveillance: ensuring an effective protection of fundamental rights when using real-time remote biometric identification in EU Member States after the AI Act. Μεταπτυχιακή Διπλωματική Εργασία. Lund University.

Wang, M. and Deng, W. (2021) 'Deep face recognition: A survey', *Neurocomputing*, 429, p. 216.

Wang, W. et al. (2014) 'Face recognition based on deep learning,' in Proc. Int. Conf. Hum. Centered Comput., pp. 812–820.

Zuiderveen Borgesius, F.J. (2020) 'Strengthening legal protection against discrimination by algorithms and artificial intelligence', *The International Journal of Human Rights*, 24(10), pp. 1572–1593.

NΟΜΟΘΕΤΙΚΑ ΚΕΙΜΕΝΑ & ΕΠΙΣΗΜΑ ΕΓΓΡΑΦΑ

Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης (2016) 'Κανονισμός (ΕΕ) 2016/679 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)', *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*, L 119, 4 Μαΐου, σσ. 1–88.

Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης (2016) 'Οδηγία (ΕΕ) 2016/680 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών

κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου', Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, L 119, 4 Μαΐου, σσ. 89–131.

Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης (2024) 'Κανονισμός (ΕΕ) 2024/1689 για τη θέσπιση εναρμονισμένων κανόνων σχετικά με την τεχνητή νοημοσύνη (Πράξη για την τεχνητή νοημοσύνη)', Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, L, 12 Ιουλίου.

Ευρωπαϊκή Επιτροπή (2019). Κατευθυντήριες γραμμές ηθικής για αξιόπιστη Τεχνητή Νοημοσύνη. Ανεξάρτητη ομάδα εμπειρογνομόνων υψηλού επιπέδου για την τεχνητή νοημοσύνη. Διαθέσιμο στο: <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai> (Πρόσβαση: Δεκέμβριος 2025).

ΕΣΠΑ (2022) Κατευθυντήριες γραμμές 05/2022 σχετικά με τη χρήση της τεχνολογίας αναγνώρισης προσώπου στον τομέα της επιβολής του νόμου.

ΕΣΠΑ (2019) / EDPB (2020) Κατευθυντήριες γραμμές 3/2019 σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω βιντεοσυσκευών.

ΕΣΠΑ και ΕΕΠΑ (2021) Κοινή γνωμοδότηση 5/2021 σχετικά με την πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη θέσπιση εναρμονισμένων κανόνων σχετικά με την τεχνητή νοημοσύνη (Πράξη για την Τεχνητή Νοημοσύνη). Βουξέλλες. Διαθέσιμο στο: https://edpb.europa.eu/our-work-tools/our-documents/edpb-edps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_el (Πρόσβαση: Φεβρουάριος 2026).

Ομάδα Εργασίας του Άρθρου 29 (2003) Εγγραφο εργασίας WP80/2003 σχετικά με τα στοιχεία βιομετρίας. Διαθέσιμο σε: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_el.pdf.

Ομάδα Εργασίας του Άρθρου 29 (2012) Γνωμοδότηση 02/2012 σχετικά με την αναγνώριση προσώπου στις διαδικτυακές υπηρεσίες και στις υπηρεσίες κινητής τηλεφωνίας (WP 192). 22 Μαρτίου. Διαθέσιμο στο: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_el.pdf (Πρόσβαση: Δεκέμβριος 2025).

Ομάδα Εργασίας του Άρθρου 29 (2012) Γνωμοδότηση 3/2012 σχετικά με τις εξελίξεις στις βιομετρικές τεχνολογίες (WP193). 27 Απριλίου. Διαθέσιμο στο:

[https://ec.europa.eu/justice/article-29/documentation/opinion-](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_el.pdf)

[recommendation/files/2012/wp193_el.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_el.pdf) (Πρόσβαση: Ιανουάριος 2026).

Ομάδα Εργασίας του Άρθρου 29 (2014) Γνώμη 6/2014 σχετικά με την έννοια των εννόμων συμφερόντων του υπευθύνου επεξεργασίας κατ' άρθρο 7 της Οδηγίας 95/46, σελ. 14.

Διαθέσιμο σε: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_el.pdf.

Ομάδα Εργασίας του Άρθρου 29 (n.d.) Γνώμη σχετικά με ορισμένα βασικά ζητήματα της οδηγίας (ΕΕ) 2016/680 για την επιβολή του νόμου. Διαθέσιμο σε: <https://ec.europa.eu/newsroom/article29/items/610178> (Πρόσβαση: Ιανουάριος 2026

European Union Agency for Fundamental Rights (FRA) (2019) *Facial recognition technology: fundamental rights considerations in the context of law enforcement*. FRA Focus Paper. Vienna: FRA. Διαθέσιμο στο: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf (Πρόσβαση: Ιανουάριος 2026).

ΝΟΜΟΛΟΓΙΑ

ΔΕΕ (2014) Συνεκδικασθείσες υποθέσεις C-293/12 και C-594/12, *Digital Rights Ireland Ltd κατά Minister for Communications, Marine and Natural Resources* κ.λπ. Απόφαση της 8ης Απριλίου 2014.

ΔΕΕ (2015) Υπόθεση C-362/14, *Maximillian Schrems*. Απόφαση της 6ης Οκτωβρίου 2015.

ΔΕΕ (2021) Απόφαση της 22ας Ιουνίου 2021, B κατά *Latvijas Republikas Saeima*, C-439/19, EU:C:2021:504, σκέψη 87.

Opinion of Advocate General Bot (2015) *Maximillian Schrems v Data Protection Commissioner*, Case C-362/14, ECLI:EU:C:2015:627.

R (on the application of Bridges) v Chief Constable of South Wales Police [2020] EWCA Civ 1058.

Διαθέσιμο στο: <https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf> (Πρόσβαση: Φεβρουάριος 2026).

ΕΔΔΑ (1978) *Case of Klass and Others v. Germany*. Application no. 5029/71, European Court of Human Rights.

ΕΔΔΑ (2008) *S. and Marper v. the United Kingdom* [GC]. Application nos. 30562/04 and 30566/04, European Court of Human Rights.

ΕΔΔΑ (2010) *Case of Uzun v. Germany*. Application no. 35623/05, European Court of Human Rights.

ΕΔΔΑ (2011) *Case of Shimovolos v. Russia*. Application no. 30194/09, European Court of Human Rights.

ΕΔΔΑ (2012) *Piechowicz v. Poland*. Application no. 20071/07, European Court of Human Rights.

ΕΔΔΑ (2021) *Big Brother Watch and Others v. the United Kingdom* [GC]. Application nos. 58170/13, 62322/14 and 24960/15, European Court of Human Rights. Διαθέσιμο στο: <https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%22001-186048%22%5D%7D> (Πρόσβαση: Φεβρουάριος 2026).

ΕΔΔΑ (2021) *Yefimov και Youth Human Rights Group κατά Ρωσίας*. Αρ. Προσφυγών 12385/15 και 51619/15. Διαθέσιμο στο: <https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-213913%22%5D%7D> (Πρόσβαση: Φεβρουάριος 2026).

ΕΔΔΑ (2023) *Υπόθεση Glukhin κατά Ρωσίας*. Προσφυγή αριθ. 11519/20, Απόφαση της 4ης Ιουλίου 2023. Στρασβούργο: Ευρωπαϊκό Δικαστήριο Δικαιωμάτων του Ανθρώπου. Διαθέσιμο σε: <https://hudoc.echr.coe.int/#%7B%22itemid%22:%5B%22001-225655%22%5D%7D> .

