

Τεχνολογία αναγνώρισης προσώπου στον τομέα της δημόσιας ασφάλειας: λειτουργία, εφαρμογές και προκλήσεις

Γεώργιος Μπορμπαντωνάκης

Εκπαιδευόμενος Δικαστικός Υπάλληλος, Σπουδαστής ΕΣΔι

ΜΔΕ Εγκληματολογίας και Αντεγκληματικής Πολιτικής, Νομική Σχολή ΕΚΠΑ



The New Yorker, του καλλιτέχνη Ibrahim Rayintakath

Εισαγωγή

Αδιαμφισβήτητο γεγονός είναι ότι τα συστήματα αναγνώρισης προσώπου (facial recognition) συνιστούν μια συνεχώς εξελισσόμενη τεχνολογία που συγκεντρώνει όλο και μεγαλύτερο ενδιαφέρον για την ενίσχυση της δημόσιας ασφάλειας και τη στήριξη του έργου των αρχών επιβολής του νόμου. Με αφορμή την αύξηση των ποσοστών εγκληματικότητας και της συνεπαγόμενης ανησυχίας των πολιτών ως προς το επαπειλούμενο αίσθημα ασφάλειας, ιδίως στα μεγάλα αστικά κέντρα, οι παγκόσμιες κυβερνήσεις προκρίνουν την υιοθέτηση συστημάτων παρακολούθησης και βιντεοεπιτήρησης, ικανών να αναγνωρίζουν γρήγορα και με ακρίβεια τα άτομα εκείνα που εμπλέκονται σε εγκληματικές δραστηριότητες.

Επί της ουσίας, η αναγνώριση προσώπου λειτουργεί με τη λήψη της εικόνας ενός ατόμου και την κατόπιν ταυτοποίησή του μέσω της ανάλυσης και χαρτογράφησης των καταγεγραμμένων χαρακτηριστικών. Οι εικόνες προσώπου και η επισταμένη ανάλυσή τους συνιστούν ένα βασικό εργαλείο για τις αρχές επιβολής του νόμου ήδη από τον 19^ο αιώνα. Περνώντας από τις άλλοτε χειροκίνητες τεχνικές σε εξελιγμένες τεχνολογίες του 21^{ου} αιώνα, καθίσταται πλέον εφικτή η αυτόματη εξαγωγή και σύγκριση των χαρακτηριστικών και κάθε μικρής διαφοροποίησης και απόκλισης χάρη στη συμβολή της τεχνικής νοημοσύνης, των αλγορίθμων και των μοντέλων βαθιάς μάθησης.¹ Ομολογουμένως, καταλύτης στη ραγδαία ανάπτυξη της εν λόγω τεχνολογίας υπήρξαν οι τρομοκρατικές επιθέσεις στη Νέα Υόρκη και την Ουάσιγκτον την 11^η Σεπτεμβρίου 2001. Με την αδήριτη πλέον ανάγκη για ασφάλεια στις διεθνείς αεροπορικές μεταφορές, οκ ολίγα αεροδρόμια έχουν εντάξει την τεχνολογία αναγνώρισης προσώπου στη φαρέτρα τους έναντι των τρομοκρατών.²

Το παρόν άρθρο επιχειρεί να διαφωτίσει τον αναγνώστη αναφορικά με τα στοιχειώδη τεχνικά χαρακτηριστικά της τεχνολογίας αναγνώρισης προσώπου (εφεξής ΤΑΠ χάριν συντομίας) και του τρόπου με τον οποίο λειτουργεί. Επιπλέον, εξετάζονται οι σημαίνουσες εφαρμογές και τα πλεονεκτήματά της στο πεδίο της δημόσιας ασφάλειας και της επιτήρησης δημόσιων χώρων, αντλώντας παραδείγματα από την παγκόσμια πρακτική. Τέλος, αναδεικνύονται μερικές εκ των αναδυόμενων τεχνικών, ηθικών και νομικών προκλήσεων της ΤΑΠ.

1. Almeida, D., Shmarko, K., & Lomas, E. (2021). The Ethics of Facial Recognition Technologies, Surveillance, and Accountability in An Age of Artificial Intelligence: A Comparative Analysis of US, EU, and UK Regulatory Frameworks. *AI and Ethics*, 2(3), 377-387, σ. 378.

2. Thornburg, R.H. (2002). Face Recognition Technology: The Potential Orwellian Implications and Constitutionality of Current Uses Under the Fourth Amendment. *John Marshall Journal of Computer & Information Law*, 20(2), 321-346, σ. 322.

Μερικά λόγια για την επιστήμη της βιομετρίας (biometrics)

Για χιλιάδες χρόνια, οι άνθρωποι χρησιμοποιούσαν χαρακτηριστικά του σώματος, λόγου χάρη το πρόσωπο, τη φωνή, το βάδισμα, ώστε να αναγνωρίζουν ο ένας τον άλλον. Περί τα μέσα του 19ου αιώνα, ο Alphonse Bertillon, επικεφαλής του τμήματος ταυτοποίησης εγκληματιών της αστυνομίας του Παρισιού, ανέπτυξε και εν συνεχεία εφάρμοσε την ιδέα της ανθρωπομετρίας, ήτοι της χρήσης διαφόρων μετρήσεων του σώματος (όπως ύψος, μήκος χεριών, ποδιών και δακτύλων) για την ταυτοποίηση εγκληματιών.³ Στα τέλη του 19ου αιώνα, ακριβώς όταν η ιδέα του γινόταν δημοφιλής, επισκιάστηκε από μια πολύ πιο σημαντική και πρακτική ανακάλυψη: τη μοναδικότητα των δακτυλικών αποτυπωμάτων του ανθρώπου.⁴ Σε σύντομο χρονικό διάστημα, μεγάλα αστυνομικά τμήματα υιοθέτησαν την ιδέα της καταχώρισης των δακτυλικών αποτυπωμάτων των εγκληματιών και της αποθήκευσής τους σε βάσεις δεδομένων (αρχικά σε καρτέλες). Αργότερα, η αστυνομία απέκτησε τη δυνατότητα να συλλέγει αποτυπώματα που είχαν απομείνει, συνήθως αποσπασματικά, σε σκηνές εγκλήματος και ακολούθως να τα συγκρίνει με τα αποτυπώματα στη βάση δεδομένων για να προσδιορίσει την ταυτότητα των εγκληματιών.⁵

Ορόσημο στην εξέλιξη της επιστήμης της βιομετρίας συνιστά η πρωτόλεια εφαρμογή της ΤΑΠ στον τραπεζικό κλάδο, με την αρχική ανάπτυξη της βιντεοεπιτήρησης μέσω ενός κλειστού κυκλώματος τηλεόρασης (CCTV). Η τεχνολογία της βιντεοεπιτήρησης, που εισήχθη στις ΗΠΑ για πρώτη φορά το 1956, έχει εξελιχθεί σε ευρέως διαδεδομένη μέθοδο προστασίας του αγαθού της δημόσιας ασφάλειας σε πολλούς δημόσιους χώρους, όπως εμπορικά κέντρα, τράπεζες, ΑΤΜ και σουπερμάρκετ.⁶ Με την επέλευση της εποχής της ψηφιακής απεικόνισης, αυτές οι συσκευές βιντεοεπιτήρησης έγιναν πιο αποτελεσματικές, λιγότερο δαπανηρές, και η χρήση τους παγιώθηκε σχεδόν παντού στον πλανήτη.

3. Prabhakar, S., Pankanti, S., & Jain, A. K. (2003). Biometric Recognition: Security and Privacy Concerns. *IEEE Security & Privacy*, 1(2), 33-42, σ. 39.

4. Η πρώτη ποινική υπόθεση που επιλύθηκε με τη χρήση δακτυλικών αποτυπωμάτων για την ταυτοποίηση ήταν στην Αργεντινή το 1892, χάρη στον αστυνομικό Juan Vucetich, ο οποίος χρησιμοποίησε ένα ματωμένο δακτυλικό αποτύπωμα για να ταυτοποιήσει τη Francisca Rojas ως δολοφόνο των δύο παιδιών της, αποδεικνύοντας την ενοχή της αφού είχε κατηγορήσει ψευδώς έναν γείτονα, τον Pedro Velázquez. Αυτή η πρωτοποριακή χρήση του συστήματος του Vucetich οδήγησε στην ομολογία της Rojas, καθιερώνοντας τα δακτυλικά αποτυπώματα ως κορυφαίο εργαλείο στην εγκληματολογική επιστήμη σε όλο τον κόσμο. Βλ. https://www.nlm.nih.gov/exhibition/visibleproofs/galleries/cases/vucetich_image_3.html.

5. Prabhakar, S., Pankanti, S., & Jain, A. K. (2003). Biometric recognition, ό. π., σ. 39.

6. Thornburg, R.H. (2002). Face Recognition Technology, ό. π., σ. 323.

Πώς λειτουργεί σε γενικές γραμμές η τεχνολογία αναγνώρισης προσώπου;

Προτού εμβαθύνουμε στα επιμέρους ζητήματα της εξεταζόμενης τεχνολογίας, η αναγνώριση προσώπου ορίζεται ως τεχνική για την ταυτοποίηση ή επαλήθευση⁷ ενός ατόμου από μια στατική ή κινούμενη εικόνα που πραγματοποιείται κατόπιν αντιπαραβολής αυτής προς μια βάση δεδομένων που εμπεριέχει ένα σύνολο εικόνων προσώπου.⁸

Η ΤΑΠ αποτελείται από δύο σημαντικά στοιχεία: αφενός τις κάμερες βιντεοεπιτήρησης που χρησιμοποιούνται για τη λήψη στιγμιότυπου του προσώπου ενός ατόμου και αφετέρου το λογισμικό ενός υπολογιστή που χρησιμοποιείται για την εξαγωγή και ανάλυση του προσώπου αυτού για τον σκοπό της ταυτοποίησης.⁹

Μολονότι το παρόν άρθρο δεν αποσκοπεί στην παρουσίαση ενός τεχνικού εγχειριδίου, για τη σφαιρική κατανόηση της φιλοσοφίας που διαπνέει την ΤΑΠ κρίνεται σκόπιμη μια ευσύνοπτη περιγραφή των επικρατέστερων προσεγγίσεων που αυτή εφαρμόζει. Η πρώτη είναι ευρέως γνωστή ως αναλυτική μέθοδος ή μέθοδος βασισμένη σε χαρακτηριστικά (feature-based), και επικεντρώνεται κυρίως στην ανίχνευση μεμονωμένων χαρακτηριστικών, όπως είναι τα μάτια, τα αυτιά, το περίγραμμα του κεφαλιού, το στόμα, καθώς και στη μέτρηση διαφορετικών γωνιών, αποστάσεων και μεγεθών μεταξύ των εν λόγω χαρακτηριστικών. Ακολουθεί η λεγόμενη ολιστική μέθοδος, η οποία εστιάζει σε μια συνολική αναπαράσταση του προσώπου, αντιμετωπίζοντας τις εικόνες ως διανύσματα στην κλίμακα του γκρι (grayscale). Εν ολίγοις, στηρίζεται στην εμφάνιση της εικόνας και όχι στη λεπτομερή γεωμετρία των μοντέλων προσώπου, όπως προκρίνει η αναλυτική μέθοδος. Τέλος, αναπτύχθηκε η υβριδική μέθοδος, όπου τα χαρακτηριστικά εξάγονται από τα μεμονωμένα όργανα του προσώπου (μάτια, μύτη, στόμα), ενώ παράλληλα ελέγχεται τόσο η απόσταση όσο και η σχέση μεταξύ τους. Πρόκειται επί της ουσίας για έναν συνδυασμό της ολιστικής και της αναλυτικής μεθόδου, επιτυγχάνοντας βέλτιστα αποτελέσματα δε-

7. Η ειδοποιός διαφορά μεταξύ ταυτοποίησης (identification) και επαλήθευσης (verification) έγκειται στο γεγονός ότι η ταυτοποίηση επιτυγχάνεται αναζητώντας όλα τα βιομετρικά δεδομένα που είναι αποθηκευμένα στη βάση δεδομένων. Στην περίπτωση αυτή, ένα σύστημα ταυτοποίησης πραγματοποιεί σύγκριση ενός προς πολλά για να αποδείξει την ταυτότητα ενός ατόμου. Αντίθετα, σε ένα σύστημα επαλήθευσης, οι βιομετρικές πληροφορίες ενός ατόμου που ισχυρίζεται ότι έχει συγκεκριμένη ταυτότητα συγκρίνονται με το δικό του βιομετρικό προφίλ που είναι αποθηκευμένο στη βάση δεδομένων. Στη δεύτερη αυτή περίπτωση, πρόκειται για σύγκριση ενός προς ένα. Saini, M., & Kumar Kapoor, A. (2016). Biometrics in Forensic Identification: Applications and Challenges. *Journal of Forensic Medicine*, 1(2), 1-6, σ. 2. Η ταυτοποίηση είναι πολύ πιο δυσχερής διαδικασία από την επαλήθευση, επειδή ένα σύστημα ταυτοποίησης θα πρέπει να εκτελέσει μεγαλύτερο αριθμό συγκρίσεων. Prabhakar, S., Pankanti, S., & Jain, A. K. (2003). Biometric Recognition, ό. π., σ. 40.

8. Arif, K. & Honi, D. (2015). Real-Time Secure System for Detection and Recognition the Face of Criminals. *International Journal of Computer Science and Mobile Computing*, 4(9), 58-83, σ. 66.

9. Thornburg, R.H. (2002). Face Recognition Technology, ό. π., σ. 325.

δομένης της ευμεταβλησίας των στοιχείων ενός προσώπου, κυρίως λόγω της στάσης του σώματος, των περιβαλλοντικών συνθηκών, του φωτισμού αλλά και της έκφρασης.¹⁰

Καίτοι η ΤΑΠ παρουσιάζει ιδιάζουσα ποικιλομορφία αναφορικά με τον τρόπο εφαρμογής κάθε προσέγγισης,¹¹ καθότι την τελευταία δεκαετία, και ιδίως μετά τη σαρωτική επέλευση της τεχνητής νοημοσύνης, έχουν αναπτυχθεί πλείστοι όσοι αλγόριθμοι και μοντέλα ταυτοποίησης,¹² όλα τα συστήματα αναγνώρισης προσώπου περιλαμβάνουν τα παρακάτω δομικά στάδια.¹³

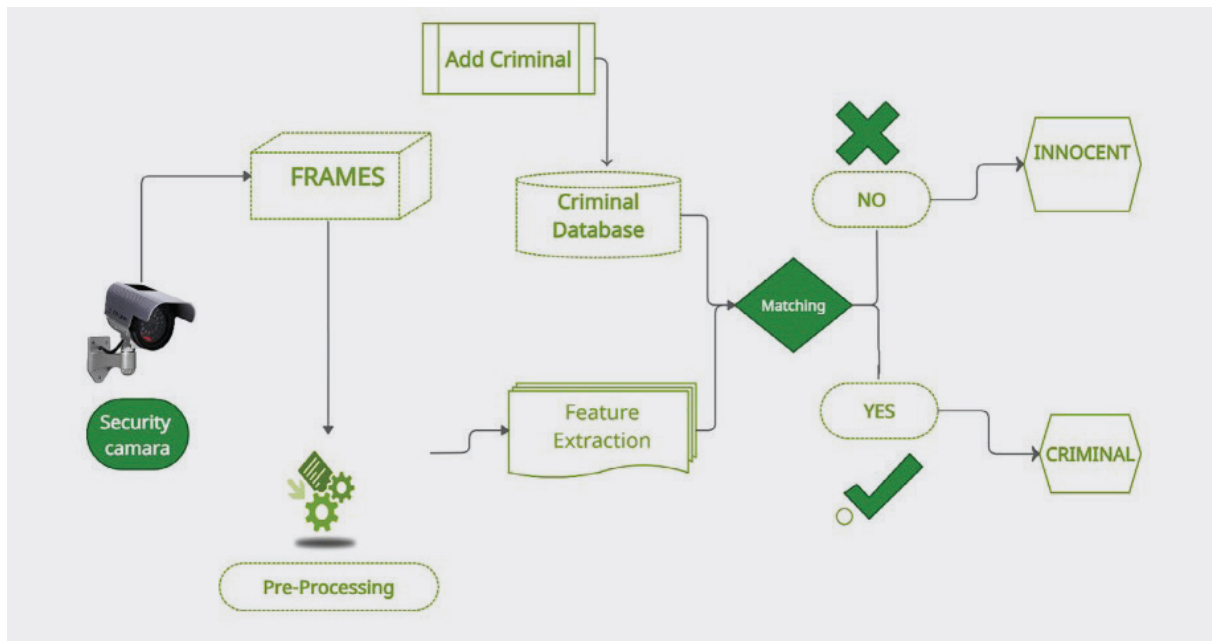
1. Στάδιο λήψης της εικόνας από κινούμενη εικόνα (βίντεο) ή στατικό καρέ (φωτογραφία).
2. Στάδιο ανίχνευσης της εικόνας του προσώπου από τη συνολική εικόνα και αφαίρεση της εικόνας φόντου.
3. Στάδιο ευθυγράμμισης και τυποποίησης της γωνίας του προσώπου με την κάμερα. Στο στάδιο αυτό γίνεται προεπεξεργασία των χαρακτηριστικών που πρόκειται να εξαχθούν για τη βελτίωση του ποσοστού αναγνώρισης. Η εικόνα του προσώπου περικόπτεται και αλλάζει μέγεθος σε μικρότερη τιμή pixel.
4. Στάδιο εξαγωγής σημαντικών χαρακτηριστικών από το πρόσωπο.
5. Στάδιο αντιπαραβολής της προκύπτουσας εικόνας με τις υπάρχουσες εικόνες στη βάση δεδομένων. Εάν βρεθεί αντιστοίχιση, εμφανίζονται τα δεδομένα που σχετίζονται με αυτήν την εικόνα από τη βάση δεδομένων.
6. Στάδιο ταυτοποίησης/επαλήθευσης της εικόνας από το σύστημα και αναφοράς για το εάν η αναγνώριση προσώπου ήταν επιτυχής ή όχι.

10. Jayaswal, R., & Dixit, M. (2020). Comparative Analysis of Human Face Recognition by Traditional Methods and Deep Learning in Real-Time Environment. *2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT)*, 66-71, σ. 68. Για μια αναλυτική ανασκόπηση των κλασικών και σύγχρονων προσεγγίσεων στον τομέα της αναγνώρισης προσώπου, βλ. Ali, W., Tian, W., Din, S.U., Iradukunda, D. & Khan, A.A. (2021). Classical and Modern Face Recognition Approaches: A Complete Review. *Multimedia Tools and Applications*, 80, 4825-4880.

11. Για μια ενδεικτική περιγραφή των κυριότερων τεχνικών αναγνώρισης προσώπου που στηρίζονται στις τρεις προαναφερθείσες μεθόδους, βλ. Chevelwalla, A., Gurav, A., Desai, S. & Sadhukhan, S. (2015). Criminal Face Recognition System. *International Journal of Engineering Research & Technology*, 4(3), 47-50.

12. Για μια συγκριτική ανάλυση των διαφόρων μοντέλων αναγνώρισης προσώπου που εφαρμόζονται σε σύνολα δεδομένων από βίντεο για την ανίχνευση εγκληματικών πράξεων (VGGFace, FaceNet, OpenFace και DeepFace, με το πρώτο να παρουσιάζει τη μεγαλύτερη ακρίβεια), βλ. Goyal, Gouri & Kumar, Vaibhav & Aggarwal, Piyush & Chugh, Gunjan & Lamba, Tripti (2024). Comparative Analysis of Face Recognition Models for Criminal Detection. Σε: Sharma, H., Chakravorty, A., Hussain, S. & Kumari, R. (επιμ.). *Artificial Intelligence: Theory and Applications*, 325-337.

13. Arif, K. & Honi, D. (2015). Real-Time Secure System for Detection and Recognition, ό. π., σ. 66.



Διαδικασία αναγνώρισης προσώπου.¹⁴

Πλεονεκτήματα και εφαρμογές της τεχνολογίας αναγνώρισης προσώπου

α. Η ΤΑΠ ως εργαλείο ελέγχου και πρόληψης του εγκλήματος

Από τους δημόσιους δρόμους έως τα αεροδρόμια, η ΤΑΠ προσφέρει έναν μη παρεμβατικό τρόπο παρακολούθησης και αναγνώρισης υπόπτων, επιτρέποντας στις αρχές επιβολής του νόμου να αποτρέπουν περιστατικά εγκληματικότητας και να συλλαμβάνουν τους παραβάτες. Σε αντίθεση με άλλες βιομετρικές μεθόδους που απαιτούν τη συνεργασία και την επίγνωση του ατόμου, ούτως ώστε να διεξαχθεί η ταυτοποίηση ή η επαλήθευση, όπως για παράδειγμα να κοιτάξει σε έναν σαρωτή ματιών ή να τοποθετήσει το χέρι του σε έναν αναγνώστη δακτυλικών αποτυπωμάτων, η αναγνώριση προσώπου μπορεί να ολοκληρωθεί άμεσα, ακόμη και χωρίς τη γνώση του ατόμου.¹⁵ Αυτοματοποιώντας τη διαδικασία αναγνώρισης υπόπτων, τα συστήματα αυτά ελαχιστοποιούν τα ανθρώπινα λάθη και επιτρέπουν στις αρμόδιες αρχές να διαχειρίζονται μεγάλους όγκους δεδομένων με μεγαλύτερη ακρίβεια.

Η δυνατότητα ανίχνευσης και αναγνώρισης σε πραγματικό χρόνο εικόνων προσώπου που ανήκουν σε εγκληματίες δύναται να αναβαθμίσει αισθητά τις αστυνομικές επιχειρήσεις, ιδίως σε

14. Kumar, K., Kasiviswanadham, Y., Indira, D., Palesetti, P. & Bhargavi, C. (2023). Criminal Face Identification System Using Deep Learning Algorithm Multi-Task Cascade Neural Network (MTCNN). *Materials Today: Proceedings*, 80, 2406-2410, σ. 2407.

15. Chevelwalla, A., Gurav, A., Desai, S. & Sadhukhan, S. (2015). Criminal Face Recognition System, ό. π., 48.

περιοχές υψηλού κινδύνου, όπως οι συνοριακοί έλεγχοι, οι συγκοινωνιακοί κόμβοι και οι μεγάλες δημόσιες συγκεντρώσεις. Στο βαθμό που η χρήση της ΤΑΠ από τις αρχές επιβολής του νόμου διευκολύνει τις έγκαιρες συλλήψεις και καταδίκες, αυτό αναμένεται να αποτρέψει τους επίδοξους δράστες από το να παραβιάζουν το νόμο σε περιοχές όπου η συγκεκριμένη βιομετρική τεχνολογία είναι εγκατεστημένη και εμφανής.¹⁶

Συν τοις άλλοις, αξιολογώντας τις τάσεις και τα μοτίβα που προκύπτουν από τη χαρτογράφηση της εγκληματικότητας, οι αστυνομικές δυνάμεις μπορούν να διαθέσουν καλύτερα τους πόρους σε επικίνδυνες ζώνες και “hot spots” με βάση τα στοιχεία που συλλέγουν μέσω της ΤΑΠ (λ.χ. τη συχνότητα παρουσίας υπότροπων παραβατών και γνωστών υπόπτων εντός συγκεκριμένων περιοχών). Ως εκ τούτου, οι διωκτικές αρχές είναι σε θέση να αντιδράσουν άμεσα και με τον κατάλληλο προληπτικό σχεδιασμό σε επικείμενες απειλές εγκληματικών δραστηριοτήτων και να βελτιώσουν την επιχειρησιακή τους αποτελεσματικότητα και αποδοτικότητα.¹⁷



<https://news.sky.com/story/police-to-ramp-up-use-of-out-of-control-facial-recognition-technology-amid-privacy-warnings-13479217>

16. Johnson, T.L, Johnson, N.N., Topali, V., McCurdy, D. & Wallace, A. (2024). Police Facial Recognition Applications and Violent Crime Control in U.S. Cities. *Cities*, 155, 1-14, σ.1.

17. Σύμφωνα με τα πορίσματα έρευνας σχετικά με τις επιπτώσεις της ΤΑΠ στα εγκλήματα βίας και τη δυναμική των συλλήψεων σε 268 πόλεις των ΗΠΑ κατά το διάστημα 1997-2020, παρατηρήθηκε ότι η χρήση ΤΑΠ από την αστυνομία συνέβαλε στη μείωση των ποσοστών βίαιων εγκλημάτων και ανθρωποκτονιών, με τις μεγαλύτερες μειώσεις να εντοπίζονται σε πόλεις που υιοθέτησαν την εξεταζόμενη τεχνολογία νωρίτερα κατά την περίοδο της μελέτης, γεγονός που υποδηλώνει ότι τα οφέλη της για τη δημόσια ασφάλεια αυξάνονται με την πάροδο του χρόνου. Βλ. Johnson, T.L, Johnson, N.N., Topali, V., McCurdy, D. & Wallace, A. (2024). Police Facial Recognition Applications, ό. π.

Το γεγονός ότι η ΤΑΠ μπορεί να σαρώσει με ταχύτατους ρυθμούς πρόσωπα σε πραγματικό χρόνο και έπειτα να τα συγκρίνει με τις διαθέσιμες βάσεις δεδομένων βοηθά στην επιτάχυνση των διαδικασιών αναγνώρισης, και κατ' επέκτασιν τις αστυνομικές αρχές να συλλάβουν τυχόν υπόπτους για ποινικά αδικήματα. Μάλιστα, οι ΗΠΑ χρησιμοποιούν έναν ισχυρό αλγόριθμο βιομετρικής αναγνώρισης προσώπου για την ταυτοποίηση υπόπτων, ικανό να διατρέξει τρία δισεκατομμύρια εικόνες προσώπου από τα μέσα κοινωνικής δικτύωσης.¹⁸

Πέραν όμως της αναζήτησης υπόπτων, η τεχνολογία αυτή δύναται να αποδειχθεί εξαιρετικά χρήσιμη στην ταυτοποίηση και σύλληψη τρομοκρατών, κατ' επάγγελμα εγκληματιών και βίαιων ή μη δραστών που εμπλέκονται σε μορφές οργανωμένης εγκληματικότητας, στις περιπτώσεις δηλαδή όπου οι αστυνομικές έρευνες έρχονται πολύ συχνά αντιμέτωπες με τη δυσκολία συλλογής επαρκούς αποδεικτικού υλικού ή ανεύρεσης αυτοπτών μαρτύρων.¹⁹

Προς τον σκοπό αυτό, ομάδα ερευνητών ανέπτυξε ένα σύστημα ταυτοποίησης εγκληματιών που αξιοποιεί την ΤΑΠ, δίνοντας τη δυνατότητα στους αυτόπτες μάρτυρες να αναγνωρίζουν ευκολότερα τυχόν υπόπτους με τη χρήση εικόνων που έχουν ληφθεί σε προγενέστερο χρόνο. Οι μάρτυρες επιλέγουν μέσα από το σύστημα τα μεμονωμένα χαρακτηριστικά του φερόμενου υπόπτου και, αφού σχηματισθεί ολόκληρο το πρόσωπό του, διασταυρώνεται με τις εικόνες που είναι αποθηκευμένες στη βάση δεδομένων.²⁰ Συνακόλουθα, η ΤΑΠ δύναται να συνεισφέρει σημαντικά και στην εξιχνίαση εγκλημάτων.

Παράλληλα, η εξεταζόμενη τεχνολογία μπορεί να λειτουργήσει ως αρωγός των αστυνομικών αρχών στην αναγνώριση των θυμάτων σε περιπτώσεις εμπορίας ανθρώπων ή απαγωγών και των θυμάτων εκείνων που απεικονίζονται σε κατασχεθέν υλικό παιδικής πορνογραφίας.²¹ Συν τοις άλλοις, η ΤΑΠ έχει πρακτική αξία και στον τομέα των αγνοουμένων. Πράγματι, στην πολιτεία Michoacán του Μεξικού τέθηκε σε πιλοτική εφαρμογή ένα πρόγραμμα ζωντανής αναγνώρισης προσώπου για τον εντοπισμό ατόμων που έχουν δηλωθεί ως αγνοούμενοι ή για τα οποία η αστυνομία έχει εκδώσει ένταλμα σύλληψης. Προς τούτο, ειδικές κάμερες έχουν τοποθετηθεί τόσο σε αγροτικές όσο και σε αστικές περιοχές, αλλά και σε οδικές αρτηρίες σε ολόκληρη την πολιτεία.²²

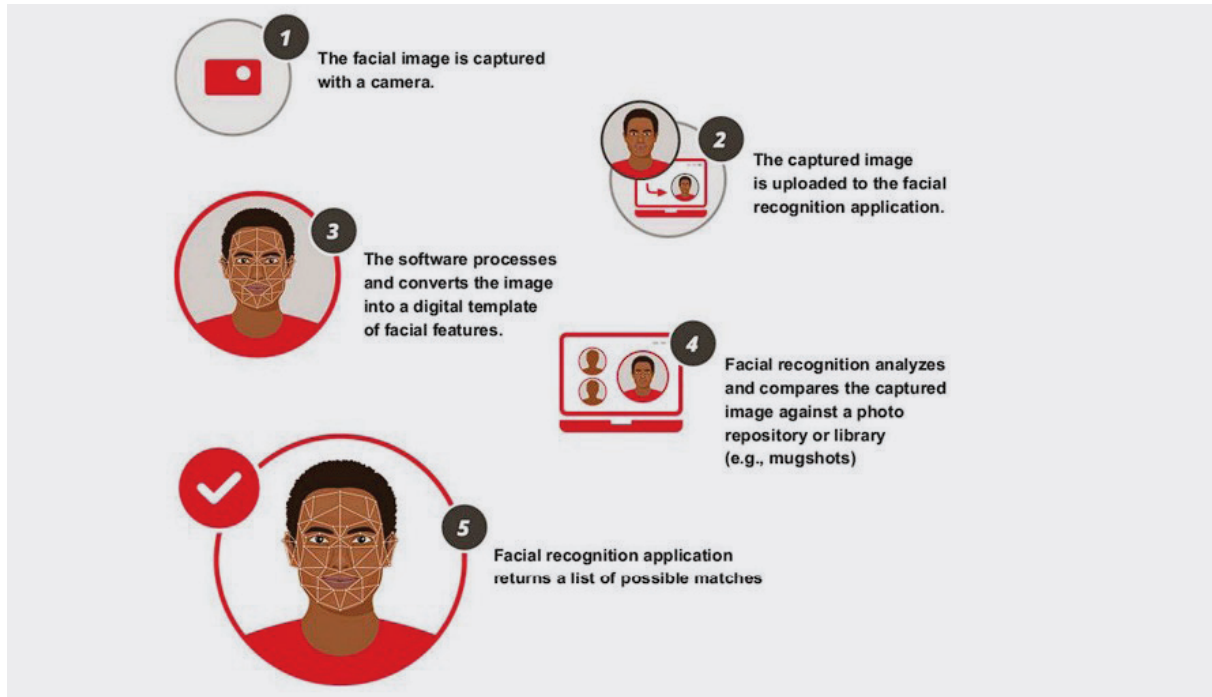
18. Smith, M., & Miller, S. (2021). The Ethical Application of Biometric Facial Recognition Technology. *AI & SOCIETY*, 37(1), 167-175, σ. 169.

19. Johnson, T.L, Johnson, N.N., Topali, V., McCurdy, D. & Wallace, A. (2024). Police Facial Recognition Applications, ό. π., σ. 3.

20. Βλ. Chevelwalla, A., Gurav, A., Desai, S. & Sadhukhan, S. (2015). Criminal Face Recognition, ό. π., 47-50.

21. Khan, Z.A. & Rizvi, A. (2021). AI Based Facial Recognition Technology and Criminal Justice: Issues and Challenges. *Turkish Journal of Computer and Mathematics Education*, 12(14), 3384-3392, σ. 3391.

22. Burt, C. (September 2025). Mexican State Selects SAFR Live Facial Recognition to ID Missing Persons, Suspects, *Biometric Update*, προσβάσιμο στο: <https://www.biometricupdate.com/202509/mexican-state-selects-safr-live-facial-recognition->



Η χρήση της ΤΑΠ από τις αρχές επιβολής του νόμου.²³

Ωστόσο, η πιο ολοκληρωμένη κυβερνητική πρωτοβουλία κράτους μέλους της Ευρωπαϊκής Ένωσης για τη χρήση της ΤΑΠ ανήκει ίσως στη Σουηδία. Και μολονότι το σκανδιναβικό αυτό κράτος είναι συνυφασμένο με τις έννοιες την κοινωνικής συνοχής και συμπερίληψης, η άλλη όψη του νομίσματος την κατατάσσει σε μια από τις υψηλότερες θέσεις στην ΕΕ σε ποσοστά ένοπλης βίας τα τελευταία χρόνια.²⁴ Συγκεκριμένα, το προταθέν νομοσχέδιο που βρίσκεται επί του παρόντος σε περίοδο διαβούλευσης θα επιτρέψει στις αστυνομικές αρχές να τοποθετούν κάμερες τεχνητής νοημοσύνης σε δημόσιους χώρους για την ταυτοποίηση και τον εντοπισμό υπόπτων εγκληματικών πράξεων και καταζητούμενων σε πραγματικό χρόνο. Στο δίκτυο αυτού του νόμου θα εντάσσονται σοβαρά εγκλήματα που επισύρουν ποινές φυλάκισης από τεσσάρων ετών και άνω, όπως ανθρωποκτονίες, βιασμοί και αδικήματα που σχετίζονται με τη νομοθεσία περί όπλων. Στόχος, σύμφωνα με κρατικές πηγές, είναι η ΤΑΠ να συμβάλει και στην πρόληψη τρομοκρατικών επιθέσεων και τον εντοπισμό αγνοουμένων θυμάτων.²⁵

to-id-missing-persons-suspects.

23. Johnson, T.L., Johnson, N.N., Topali, V., McCurdy, D. & Wallace, A. (2024). Police Facial Recognition, ό. π., σ. 3.

24. Το 2023 κατέλαβε το υψηλότερο ποσοστό ένοπλης βίας ανά κάτοικο στην ΕΕ, καθώς σκοτώθηκαν με όπλο 55 άτομα σε 363 διαφορετικές υποθέσεις πυροβολισμών σε μια χώρα μόλις 10 εκατομμυρίων πολιτών. Η αύξηση της βαριάς εγκληματικότητας αποδίδεται κυρίως στα δίκτυα οργανωμένου εγκλήματος (συμμορίες) που στρατολογούν ανήλικους για να εκμεταλλευτούν την ηπιότερη ποινική μεταχείριση που τους επιφυλάσσεται. Βλ. Ahlander, J. (June 2024). How Sweden's Youth Homes Nurtured Killers, Creating Europe's Gun Crime Capital, Reuters, προσβάσιμο στο: <https://www.reuters.com/world/europe/how-swedens-youth-homes-nurtured-killers-creating-europes-gun-crime-capital-2024-06-24/>.

25. Μάλιστα, ο Σουηδός Υπουργός Δικαιοσύνης Gunnar Strömmer υποστήριξε ότι «με την άμεση αναγνώριση των ατόμων

Αναφορικά με το πεδίο της σωφρονιστικής πολιτικής, η ΤΑΠ μπορεί να είναι κι εδώ αρκετά ωφέλιμη. Ένα τέτοιο αντιπροσωπευτικό παράδειγμα έρχεται από την Ινδία, όπου η διοίκηση του σωφρονιστικού καταστήματος στην πόλη Gurugram χρησιμοποίησε την αναβαθμισμένη μέσω της τεχνικής νοημοσύνης αναγνώριση προσώπου προκειμένου να διαχειριστεί το πλήθος των κρατουμένων και να εξασφαλίσει την τήρηση των κανόνων κοινωνικής αποστασιοποίησης κατά την περίοδο της πανδημίας του Covid-19.²⁶

β. Η ΤΑΠ ως εργαλείο επιτήρησης δημόσιων χώρων

Τα συστήματα αναγνώρισης προσώπου μέσω κλειστού κυκλώματος τηλεόρασης έχουν πλέον καταστεί αναντικατάστατο εργαλείο στην επιτήρηση ποικίλων σημαντικών περιοχών, όπως αεροδρόμια, λιμάνια, σιδηροδρομικοί σταθμοί, αστυνομικά τμήματα, κυβερνητικά κτίρια, στρατιωτικές εγκαταστάσεις, τράπεζες και εμπορικά καταστήματα, καθώς και σε μέρη που υποδέχονται υψηλή συγκέντρωση ανθρώπων, φέρ' ειπείν μεγάλες αθλητικές διοργανώσεις, συναυλίες, ακόμη και σε κεντρικούς δρόμους. Ακολουθώς, παρατίθενται μερικά ενδεικτικά παραδείγματα χρήσης της εξεταζόμενης τεχνολογίας σε δημόσιους χώρους.

Πρωτίστως, αξίζει να σημειωθεί ότι η Κίνα κρατά τα πρωτεία στον τομέα της ανάπτυξης και εφαρμογής της ΤΑΠ, καθώς χρησιμοποιεί ένα ευρύτατο σύστημα επιτήρησης με περισσότερες από 626 εκατομμύρια κάμερες αναγνώρισης προσώπου. Οι εφαρμογές της ΤΑΠ στην Κίνα καλύπτουν διαφορετικούς τομείς της δημόσιας ζωής, όχι μόνο τη δημόσια ασφάλεια αλλά και καθημερινές καταστάσεις, λ.χ. την είσοδο σε ζωολογικό κήπο ή την παράνομη διάσχιση του δρόμου από πεζούς (το λεγόμενο jaywalking).²⁷

Επιπλέον, η ΤΑΠ έχει καταστεί συνήθης πρακτική ασφαλείας σε πολλά διεθνή αεροδρόμια, με την υιοθέτηση του λεγόμενου βιομετρικού διαβατηρίου, που επιτρέπει στους επιβάτες να περνούν πιο γρήγορα από την πύλη δίχως να υποβάλλονται σε έλεγχο.²⁸ Ειδικότερα, η Emirates

αυτών όταν περνούν μπροστά από μια κάμερα, η ικανότητα της αστυνομίας να παρεμβαίνει για την πρόληψη πυροβολισμών και εκρήξεων θα αυξηθεί σημαντικά». Kennedy, C. (Μάρτιος 2025). Sweden Plans AI Face Scanning Law to Let Police Track Criminal Suspects, *FRT*, προσβάσιμο στο: https://ft.idtechwire.com/post/sweden-plans-ai-face-scanning-law-to-let-police-track-criminal-suspects?_gl=1*60y7ak*_ga*MTcyNzQ4NjQ3Ni4xNzY2MDU3NDc1*_ga_ZH90WR2WFY*czE3NjYzNTczMzckbzMkZzAkDE3NjYzNTczMzckajYwJGwwJGgw

26. Khan, Z.A. & Rizvi, A. (2021). AI Based Facial Recognition Technology, ό. π., σ. 3391.

27. Fontes, C. & Perrone, C. (2021). *Ethics of Surveillance: Harnessing the Use of Live Facial Recognition Technologies in Public Spaces for Law Enforcement*. Research Brief, Institute for Ethics in Artificial Intelligence, σ. 3, προσβάσιμο στο: https://ieai.mcts.tum.de/wp-content/uploads/2021/12/ResearchBrief_December_Fontes-1.pdf.

28. Virgil Petrescu, R. V. (2019). Face Recognition as a Biometric Application. *Journal of Mechatronics and Robotics*, 3(1), 237-257, σ. 238.

Airlines έχει προχωρήσει στην εγκατάσταση περισσότερων από 200 καμερών στο πλαίσιο ενός συστήματος αναγνώρισης προσώπου για την απλοποίηση των διαδικασιών αερομεταφοράς επιβατών στο Διεθνές Αεροδρόμιο του Ντουμπάι.²⁹ Επιπλέον, η Κίνα πρόκειται να επεκτείνει τον βιομετρικό εκτελωνισμό σε όλα τα λιμάνια της ηπειρωτικής χώρας που συνδέονται με το Χονγκ Κονγκ, το Μακάο και την Ταϊβάν. Για να χρησιμοποιήσουν την ταχεία διαδικασία βιομετρικών ελέγχων, οι ταξιδιώτες οφείλουν αρχικά να συναινέσουν στη συλλογή και επαλήθευση βιομετρικών στοιχείων προσώπου, δακτυλικών αποτυπωμάτων και άλλων βιομετρικών δεδομένων κατά τον διασυνοριακό έλεγχο.³⁰

Επιπροσθέτως, η Βρετανική Αστυνομία Μεταφορών εξήγγειλε εξάμηνη πιλοτική εφαρμογή της ΤΑΠ. Συγκεκριμένα, ειδικές κάμερες θα εγκατασταθούν προσωρινά στους χώρους των σιδηροδρομικών σταθμών, καταγράφοντας ζωντανά πλάνα των περαστικών πολιτών και συγκρίνοντας τα πρόσωπά τους με μια προκαθορισμένη λίστα παρακολούθησης υπόπτων και παραβατών. Σύμφωνα με τις σχετικές εξαγγελίες, τα πρόσωπα εκείνα που δεν θα ταυτίζονται με όσα βρίσκονται στη λίστα παρακολούθησης (watchlist), και συνεπώς δεν θα αποστέλλεται αναφορά γι' αυτά στις αστυνομικές αρχές, θα διαγράφονται αυτόματα.³¹

Αξιοσημείωτο είναι ότι το 2024 ο τότε εν ενεργεία πρωθυπουργός του Ηνωμένου Βασιλείου, Rishi Sunak, ανακοίνωσε δημόσια ότι θα δαπανηθούν 55,5 εκατομμύρια λίρες για εφαρμογή της ΤΑΠ κατά τα επόμενα τέσσερα έτη. Η επένδυση αυτή είχε ως στόχο τη μείωση της εγκληματικότητας στον τομέα του λιανικού εμπορίου, ιδίως των κλοπών σε καταστήματα. Μάλιστα, περίπου 4 εκατομμύρια λίρες από την επένδυση αυτή προορίζονταν για την αγορά ειδικά σχεδιασμένων κινητών μονάδων (βλ. εικόνα 5) που θα χρησιμοποιούνται σε δημόσια προσβάσιμους χώρους ή δρόμους με δυνατότητα αναγνώρισης προσώπου σε πραγματικό χρόνο. Οι μονάδες αυτές συγκρίνουν τις εικόνες που καταγράφουν σε πραγματικό χρόνο μέσω κάμερας σε πολυσύχναστα μέρη με τις βάσεις δεδομένων της αστυνομίας, προκειμένου να αναγνωρίσουν τυχόν ύποπτους εγκληματίες και καταζητούμενους, ιδίως υπότροπους κλέφτες καταστημάτων, οι οποίοι έχουν συμπεριληφθεί στη λίστα παρακολούθησης.³²

29. Macdonald, A. (Νοέμβριος 2025). Emirates unveils \$23M facial recognition deployment with 200 cameras at Dubai Int'l, *Biometric Update*, προσβάσιμο στο: <https://www.biometricupdate.com/202511/emirates-unveils-23m-facial-recognition-deployment-with-200-cameras-at-dubai-intl>.

30. Liang, L. (Νοέμβριος 2025). China expands biometric customs clearance for ports to Hong Kong, Macao, Taiwan, *Biometric Update*, προσβάσιμο στο: <https://www.biometricupdate.com/202511/china-expands-biometric-customs-clearance-for-ports-to-hong-kong-macao-taiwan>.

31. Borak, M. (Νοέμβριος 2025). British Transport Police to Trial Live Facial Recognition on Railway Stations, *Biometric Update*, προσβάσιμο στο: <https://www.biometricupdate.com/202511/british-transport-police-to-trial-live-facial-recognition-on-railway-stations>.

32. McConvey, J. (Απρίλ 2024). UK Police Fully Embrace the Potential of Facial Recognition With £55.5M to Spend, *Biometric Update*, προσβάσιμο στο: <https://www.biometricupdate.com/202404/uk-police-fully-embrace-the-potential-of-facial>.

Ειδικά σχεδιασμένη κινητή μονάδα³³

Στη Δανία, χώρα που μαστίζεται από επαναλαμβανόμενα επεισόδια οπαδικής βίας και άλλες εγκληματικές συμπεριφορές σε διοργανώσεις ποδοσφαίρου, η κυβέρνηση ανακοίνωσε την εφαρμογή νομοθετικών μεταρρυθμίσεων που θα περιλαμβάνουν την υποχρεωτική χρήση συστημάτων αυτοματοποιημένης αναγνώρισης προσώπου για τον εντοπισμό βίαιων οπαδών, στους οποίους θα επιβάλλεται απαγόρευση εισόδου στα γήπεδα. Στην ίδια κατεύθυνση έχουν κινηθεί η Ισπανία και η Ιταλία, με την υιοθέτηση αντίστοιχων συστημάτων σε συνεργασία με τις ποδοσφαιρικές ομάδες και τους διοργανωτές των πρωταθλημάτων.³⁴

Όσον αφορά τις συναυλίες, η αστυνομία του Leicestershire στο Ηνωμένο Βασίλειο προχώρησε στη χρήση αυτοματοποιημένης ΤΑΠ το 2015 κατά τη διάρκεια του Download Festival. Κατά τη συγκεκριμένη εκδήλωση, 90.000 άτομα ελέγχθηκαν ως προς μια λίστα παρακολούθησης της Europol, ενώ η αστυνομία δήλωσε ότι οι εικόνες που καταγράφηκαν διαγράφηκαν στη συνέχεια. Αντίστοιχα, η αστυνομία της Νότιας Ουαλίας εφαρμόζει την ΤΑΠ στο πλαίσιο δημόσιων επιχειρήσεων επιτήρησης σε μεγάλες συγκεντρώσεις, όπως υπαίθρια φεστιβάλ, αθλητικές εκδηλώσεις ή δημόσιες διαδηλώσεις.³⁵

recognition-with-55-5m-to-spend.

33. <https://www.bbc.com/news/articles/c4gvn7r7m4vo>.

34. MacDonald, A. (Σεπτέμβριος 2025). Denmark Mandates Facial Recognition to Keep Violent Fans Out of Football Stadiums, *Biometric Update*, προσβάσιμο στο: <https://www.biometricupdate.com/202509/denmark-mandates-facial-recognition-to-keep-violent-fans-out-of-football-stadiums>.

35. Fontes, C. & Perrone, C. (2021). *Ethics of Surveillance*, ό. π., σ. 3.

Αναδυόμενες προκλήσεις και σημεία κριτικής

α) Τεχνικά ζητήματα

Παρότι η τεχνολογία αναγνώρισης προσώπου παρουσιάζει ανοδική εξέλιξη, δεν παύει να εμφανίζει τεχνικές αδυναμίες. Οι διακυμάνσεις στον φωτισμό, οι εκφράσεις του προσώπου και οι μεταμφιέσεις που μπορεί να χρησιμοποιούν οι εν δυνάμει εγκληματίες για να αποφύγουν την ταυτοποίηση είναι μερικοί από τους περιορισμούς της ΤΑΠ που περιπλέκουν το έργο των δικτυικών αρχών και απαιτούν την ανάπτυξη ακόμη πιο εξελιγμένων αλγορίθμων, ικανών να διαχειριστούν ποικιλόμορφα χαρακτηριστικά και εμφανίσεις προσώπων.³⁶

Επιπροσθέτως, το ανθρώπινο πρόσωπο αποτελεί ένα δυναμικό αντικείμενο, με την εμφάνισή του να παρουσιάζει υψηλό βαθμό μεταβλητότητας. Τούτο γεννά προσκόμματα στην ακριβή του αναγνώριση. Το γεγονός δε ότι το ανθρώπινο πρόσωπο είναι πιο ευαίσθητο τόσο σε περιβαλλοντικές αλλαγές όσο και σε τεχνικές διαφοροποίησης ή απόκρυψης, όπως έγχρωμοι φακοί επαφής, μουστάκι ή γενειάδα, έντονο μακιγιάζ κ.ά., δημιουργεί μια πρόσθετη εγγενή αδυναμία της κρινόμενης τεχνολογίας. Ως εκ τούτου, υποστηρίζεται ότι το ποσοστό ακριβείας είναι εν τέλει χαμηλότερο σε σύγκριση με άλλα βιομετρικά δεδομένα ενός ατόμου, όπως τα δακτυλικά αποτυπώματα, η φωνή, η γεωμετρία της παλάμης, ο αμφιβληστροειδής και η ίριδα.³⁷

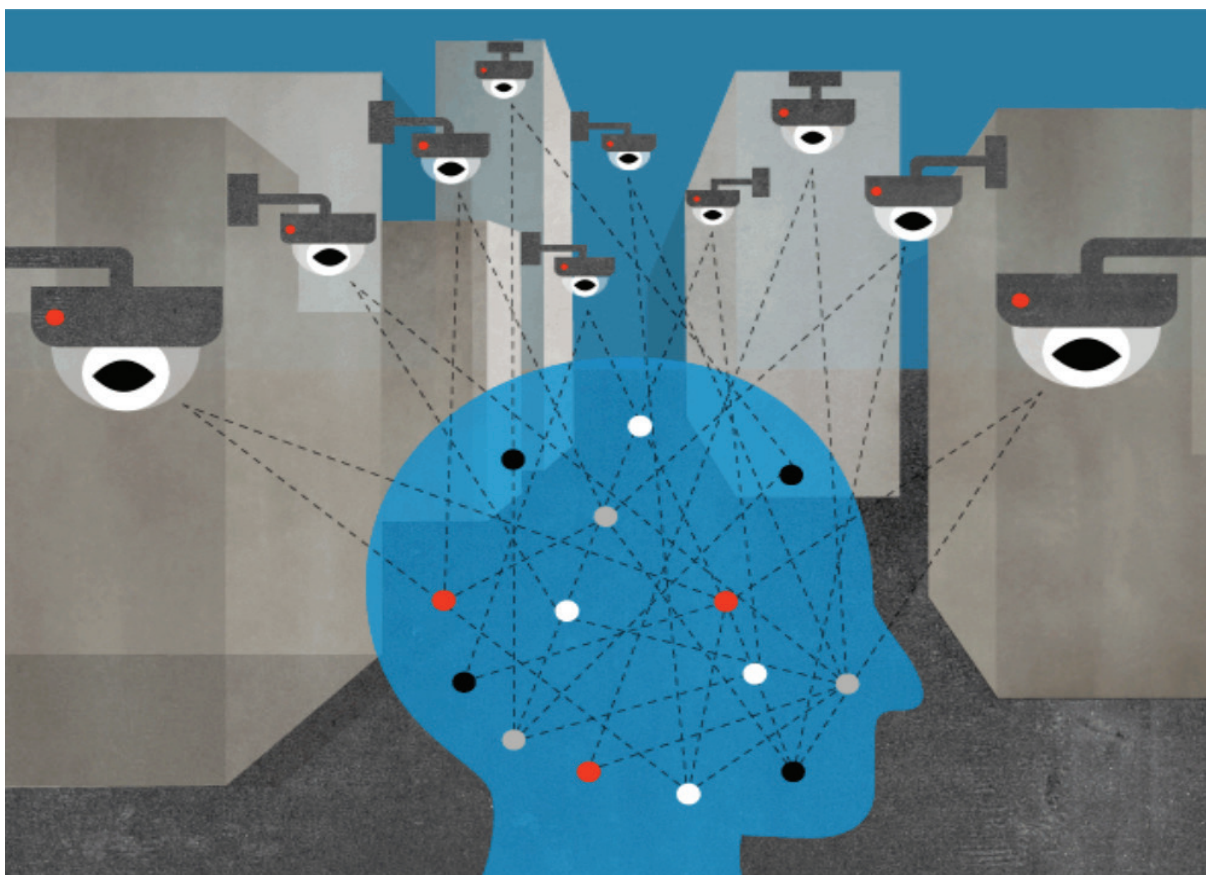
Επεξηγηματικά, η ΤΑΠ μπορεί να παραγάγει λανθασμένα αποτελέσματα, όπως η εσφαλμένη αντιστοίχιση δύο διαφορετικών εικόνων, το λεγόμενο ψευδώς θετικό αποτέλεσμα, ή η αποτυχία αντιστοίχισης του ίδιου προσώπου σε δύο διαφορετικές φωτογραφίες, το γνωστό ως ψευδώς αρνητικό αποτέλεσμα. Μάλιστα, και οι δύο τύποι σφαλμάτων έχουν τη δυνατότητα να επιδράσουν αρνητικά στην αποτελεσματικότητα των αστυνομικών ερευνών, στην εμπέδωση της εμπιστοσύνης των πολιτών προς τις αρχές επιβολής του νόμου και στην εν γένει ασφάλεια της κοινότητας.³⁸

Αφενός, τα ψευδώς θετικά αποτελέσματα μπορεί να οδηγήσουν αθώους ανθρώπους στο να αντιμετωπίζονται ως ύποπτοι ή καταζητούμενοι και να υφίστανται περιττό τραύμα. Αφετέρου, τα ψευδώς αρνητικά αποτελέσματα δύνανται να οδηγήσουν στην παράλειψη σημαντικών αποδεικτικών στοιχείων και σε άδικες κατηγορίες, καθότι το σύστημα αναγνώρισης προσώπου είναι πιθανό να εξακολουθεί να παράγει μια λίστα πιθανών υπόπτων που μπορεί να είναι όλοι ψευδώς θετικοί, μειώνοντας έτσι την πιθανότητα να αναγνωριστεί και να συλληφθεί ο πραγ-

36. Βλ. Sangeetha, K., Raja, P., Poornashree, T., Sanjay, B. & Sanjeev, M. (2025). Criminal Face Detection Using Deep Learning Algorithms. *Grenze International Journal of Engineering and Technology*, 1, 4731-4737.

37. Arif, K. & Honi, D. (2015). Real-Time Secure System for Detection and Recognition, ό. π., σ. 66.

38. Johnson, T.L., Johnson, N.N., Topali, V., McCurdy, D. & Wallace, A. (2024). Police Facial Recognition Applications, ό. π., σ. 2



The New Yorker, illustration by Chad Hagen

ματικός δράστης.³⁹ Για τον λόγο αυτό προτείνεται η τελική διαπίστωση της αναγνώρισης να γίνεται από ανθρώπινο χέρι και να μην επαφίεται η κρίση αποκλειστικά στον αλγόριθμο.

β) Ηθικά ζητήματα

Η αυξανόμενη χρήση της βιομετρικής αναγνώρισης προσώπου εγείρει μια σειρά από σοβαρές ηθικές προκλήσεις για τις φιλελεύθερες δημοκρατίες. Πρώτα απ' όλα, η χρήση τεχνολογιών βιντεοεπιτήρησης, όπως η ΤΑΠ, υπονομεύει το θεμελιώδες δικαίωμα στην ιδιωτική ζωή. Η ιδιωτικότητα παρέχει στους πολίτες έναν προσωπικό και κατ' αρχήν απαραβίαστο χώρο, εντός του οποίου μπορούν να ασκήσουν την αυτονομία τους, να αισθανθούν ελεύθεροι στις σκέψεις και τις πράξεις τους, πράγμα που δεν θα ήταν φυσικά δυνατό υπό τον κίνδυνο της συνεχούς παρακολούθησης.⁴⁰

39. Ο. π.

40. Guo, Z. & Kennedy, L. (2023). Policing Based on Automatic Facial Recognition. *Artificial Intelligence and Law*, 31, 397-443, σ. 417.

Η παραβίαση της ιδιωτικής σφαίρας των πολιτών ενδέχεται να αποτελεί σοβαρό πλήγμα για την προσωπική ακεραιότητά τους και την ανθρώπινη αξιοπρέπείά τους, εμποδίζοντας έτσι την ελεύθερη ανάπτυξη της προσωπικότητάς τους. Ας μην λησμονούμε άλλωστε ότι σχεδόν πάντα συμπεριφερόμαστε διαφορετικά όταν κάποιος μας παρατηρεί. Εξαιτίας αυτού, περιστέλλεται η αυτονομία, με αποτέλεσμα οι άνθρωποι να αυτολογοκρίνονται και να αυτοπεριορίζονται. Πρόκειται για το λεγόμενο «πάγωμα του λόγου» (chilling effect), το οποίο σταδιακά διαχέεται σε όλη τη δημόσια ζωή και παραλύει τη δημοκρατική συμμετοχή των πολιτών.⁴¹

Βεβαίως, δεν θα πρέπει να παραλειφθεί η εξέχουσα κριτική που σχετίζεται με την υπέρβαση των δηλωμένων σκοπών επιβολής του νόμου και τη συνεπαγόμενη αρνητική επίδραση στις πολιτικές και ατομικές ελευθερίες, συμπεριλαμβανομένης της ελευθερίας του συνεταιρίζεσθαι και της έκφρασης (ειδικότερη έκφανση της ελεύθερης ανάπτυξης της προσωπικότητας). Επί παραδείγματι, στην Ουγγαρία η αστυνομία προέβη στη χρήση της τεχνολογίας αναγνώρισης προσώπου σε πραγματικό χρόνο ώστε να καταστείλει εκδηλώσεις της ΛΟΑΤΚΙ κοινότητας. Υπενθυμίζεται ότι η ουγγρική κυβέρνηση απαγόρευσε με νόμο του 2025 τις παρελάσεις υπερηφάνειας (Pride), επιβάλλοντας χρηματικά πρόστιμα στους συμμετέχοντες και πιθανή φυλάκιση για τους διοργανωτές. Επομένως, ελλοχεύει σοβαρός κίνδυνος εργαλειοποίησης της ΤΑΠ έναντι ευάλωτων κοινωνικών ομάδων, όπως η ΛΟΑΤΚΙ κοινότητα, που αγωνίζονται για κοινωνική ορατότητα αλλά αντιμετωπίζονται με βιντεοεπιτήρηση και τιμωρητικότητα.⁴²

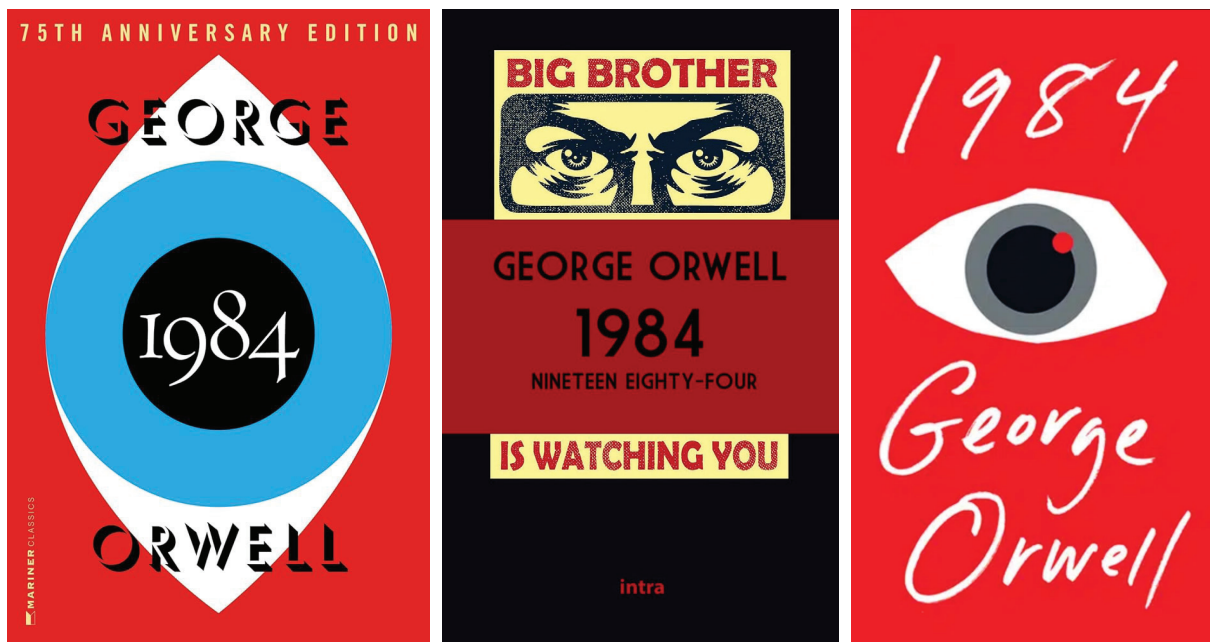
Παράλληλα με την απειλή στα θεμελιώδη δικαιώματα,⁴³ υφίσταται το φλέγον ζήτημα της μεροληπτικής προδιάθεσης των αλγορίθμων, η οποία δύναται να οδηγήσει σε προκατάληψη και διακρίσεις σε βάρος ορισμένων ομάδων ή ατόμων. Η απόδοση και τα αποτελέσματα των συστημάτων τεχνητής νοημοσύνης εξαρτώνται σημαντικά από την ποιότητα των συνόλων δεδομένων, στα οποία όμως αρκετές φορές εμφοιλοχωρούν προκαταλήψεις, ανακρίβειες και σφάλματα κατά τη διαδικασία συλλογής των δεδομένων.⁴⁴

41. Murray, D. (2024). Facial Recognition and the End of Human Rights as We Know Them?. *Netherlands Quarterly of Human Rights*, 42(2), 145-152, σ. 149.

42. McConvey, J.R. (October 2025). Hungary Law Permitting Live Facial Recognition at Outlawed Pride Event Challenged, *Biometric Update*, προσβάσιμο στο: <https://www.biometricupdate.com/202510/hungary-law-permitting-live-facial-recognition-at-outlawed-pride-event-challenged>.

43. Για μια επισκόπηση των θεμελιωδών δικαιωμάτων που προσβάλλονται από τη χρήση ΤΑΠ βλ. την αναφορά του Οργανισμού Θεμελιωδών Δικαιωμάτων της Ε.Ε. FRA (2020). *Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement*, προσβάσιμο στο: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf.

44. Nesterova, I. (2020). Mass Data Gathering and Surveillance: The Fight Against Facial Recognition Technology In the Globalized World. *SHS Web of Conferences*, 74, 1-8, σ. 2.



Στο δυστοπικό μυθιστόρημα 1984, ο George Orwell περιγράφει μια ολοκληρωτική κοινωνία όπου κάθε δωμάτιο έχει από μια ενσωματωμένη οθόνη-κάμερα και όπου ο Μεγάλος Αδελφός, δηλαδή η κυβέρνηση, παρακολουθεί τους πολίτες.

Ειδικότερα, η ΤΑΠ εκδηλώνει μεροληψία μέσω ενός σημαντικά καλύτερου ποσοστού αναγνώρισης για πρόσωπα με ανοιχτόχρωμο δέρμα και πρόσωπα που παρουσιάζουν παραδοσιακά ανδρικά χαρακτηριστικά σε σύγκριση με πρόσωπα με σκουρόχρωμο δέρμα και πρόσωπα που παρουσιάζουν παραδοσιακά γυναικεία χαρακτηριστικά.⁴⁵ Συνακόλουθα, παρατηρείται το φαινόμενο στις ΗΠΑ να είναι πιο πιθανό ένα σύστημα ΤΑΠ να αναγνωρίσει εσφαλμένα ή να αποτύχει να αναγνωρίσει Αφροαμερικανούς πολίτες συγκριτικά με λευκούς. Αυτή η εγγενής μεροληψία δύναται να οδηγήσει στον χαρακτηρισμό αθώων πολιτών ως υπόπτων για εγκλήματα.⁴⁶

Μολονότι μπορεί να είναι ηθικά δικαιολογημένη η δημιουργία μιας εθνικής βάσης δεδομένων αναγνώρισης προσώπου για την αντιμετώπιση της σοβαρής ή βίαιης εγκληματικότητας, η χρήση δισεκατομμυρίων εικόνων από λογαριασμούς κοινωνικών μέσων για τον

45. Schuetz, P. (2021). Fly in the Face of Bias: Algorithmic Bias in Law Enforcement's Facial Recognition Technology and the Need for an Adaptive Legal Framework. *Minnesota Journal of Law & Inequality*, 39(1), 221-254, σ. 223.

46. Garvie, C. & Frankle J. (April 2016). Facial-Recognition Software Might Have a Racial Bias Problem, *The Atlantic*, προσβάσιμο στο: <https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991/>. Βλ. επίσης σχετ. Haddad, G. (2021). Confronting the Biased Algorithm: The Danger of Admitting Facial Recognition Technology Results in the Courtroom. *Vanderbilt Journal of Entertainment & Technology Law*, 23(4), 891-918.

εντοπισμό και την αποτροπή μικρών αδικημάτων, πολλώ δε μάλλον η δημιουργία ενός κράτους επιτήρησης (π.χ. στο βαθμό που έχει επιτευχθεί στην Κίνα⁴⁷), είναι σαφώς απαράδεκτη.⁴⁸

Έρεισμα των ηθικών αυτών αδυναμιών συνιστά η έλλειψη διαφάνειας ως προς τη χρήση της ΤΑΠ από τις εκάστοτε κυβερνήσεις. Επί παραδείγματι, αστυνομικές αρχές στην Αυστραλία αρνούνταν τη χρήση της ΤΑΠ έως ότου απεδείχθη το αντίθετο από τα μέσα ενημέρωσης.⁴⁹ Άλλες αντίστοιχες αρχές παρέχουν πολύ περιορισμένες πληροφορίες σχετικά με το πού, για ποιο σκοπό και πώς χρησιμοποιείται η ΤΑΠ και ποια μέτρα προστασίας έχουν θεσπιστεί. Οι κατηγορούμενοι συχνά δεν γνωρίζουν ότι η ΤΑΠ οδήγησε στην ταυτοποίησή τους ως υπόπτων.⁵⁰ Η αρχή της διαφάνειας έχει λοιπόν ως στόχο να διασφαλίσει ότι η αστυνομία δεν θα κάνει κατάχρηση της τεχνολογίας ή των εξουσιών της, ενώ παράλληλα λειτουργεί και ως ασφαλιστική δικλείδα έναντι αδικαιολόγητων παραβιάσεων των ανθρώπινων δικαιωμάτων, καθιερώνοντας αναγκαίους μηχανισμούς λογοδοσίας.

γ) Νομικά ζητήματα

Για την ελαχιστοποίηση των ανωτέρω ηθικών προκλήσεων, η χρήση της ΤΑΠ δεν θα πρέπει να είναι αλόγιστη, αλλά να καθορίζεται μέσα σε σαφές νομοθετικό και ρυθμιστικό πλαίσιο. Εν ολίγοις, κρίνεται αναγκαία η θέσπιση εθνικών νόμων και συναφών μηχανισμών λογοδοσίας, ώστε να διασφαλίζεται ότι μια βάση δεδομένων με βιομετρικές εικόνες προσώπου που έχει δημιουργηθεί για νόμιμους και δικαιολογημένους σκοπούς είναι μεν προσβάσιμη από τους υπαλλήλους των αρχών επιβολής του νόμου προκειμένου να μπορούν να προλαμβάνουν και να εντοπίζουν σοβαρά εγκλήματα, αλλά δεν χρησιμοποιείται για την ταυτοποίηση λ.χ. διαδηλωτών σε πολιτικές συγκεντρώσεις.⁵¹

Δεδομένου ότι τα βιομετρικά δεδομένα, όπως το αποτύπωμα προσώπου (faceprint), λογίζονται ως προσωπικά δεδομένα, η εφαρμογή της ΤΑΠ σε κράτη μέλη της Ευρωπαϊκής Ένωσης. οριο-

47. Στην Κίνα, εθντικές μειονότητες όπως οι Ουιγούροι φαίνεται να υπόκεινται σε εκτεταμένη παρακολούθηση και διακρίσεις μέσω της χρήσης ΤΑΠ και άλλων βιομετρικών μεθόδων. Wakefield, J. (Μάιος 2021). AI Emotion-Detection Software Tested on Uyghurs, *BBC News*, προσβάσιμο στο: <https://www.bbc.com/news/technology-57101248>.

48. Smith, M., & Miller, S. (2021). The Ethical Application of Biometric Facial Recognition, ό. π., σ. 172.

49. Hickey, S. (March 2020). Police Accused of Lying About Use of Ineffective Facial Recognition Software, *Mondaq*, προσβάσιμο στο: <https://www.mondaq.com/australia/crime/902056/police-accused-of-lying-about-use-of-ineffective-facial-recognition-software>.

50. Matulionyte, R. (2023). Increasing Transparency Around Facial Recognition Technologies in Law Enforcement: Towards a Model Framework. *Journal of Information and Communications Technology Law*, 33(1), 66-84.

51. Smith, M., & Miller, S. (2021). The Ethical Application of Biometric Facial Recognition, ό. π., σ. 172.

θετείται κανονιστικά από το Γενικό Κανονισμό Προστασίας Δεδομένων (εφεξής ΓΚΠΔ χάριν συντομίας).⁵² Μάλιστα, ο ΓΚΠΔ στο άρθρο 9 παρ. 1 χαρακτηρίζει ως ευαίσθητα τα βιομετρικά δεδομένα που έχουν σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, καθώς ενέχουν αυξημένο κίνδυνο για τα δικαιώματα των φυσικών προσώπων, επιφυλάσσοντας γι' αυτά ρητή απαγόρευση επεξεργασίας, με εξαίρεση όταν την επιβάλλουν λόγοι δημόσιου συμφέροντος και εφόσον η χρήση της ΤΑΠ σέβεται την αρχή της αναλογικότητας.⁵³

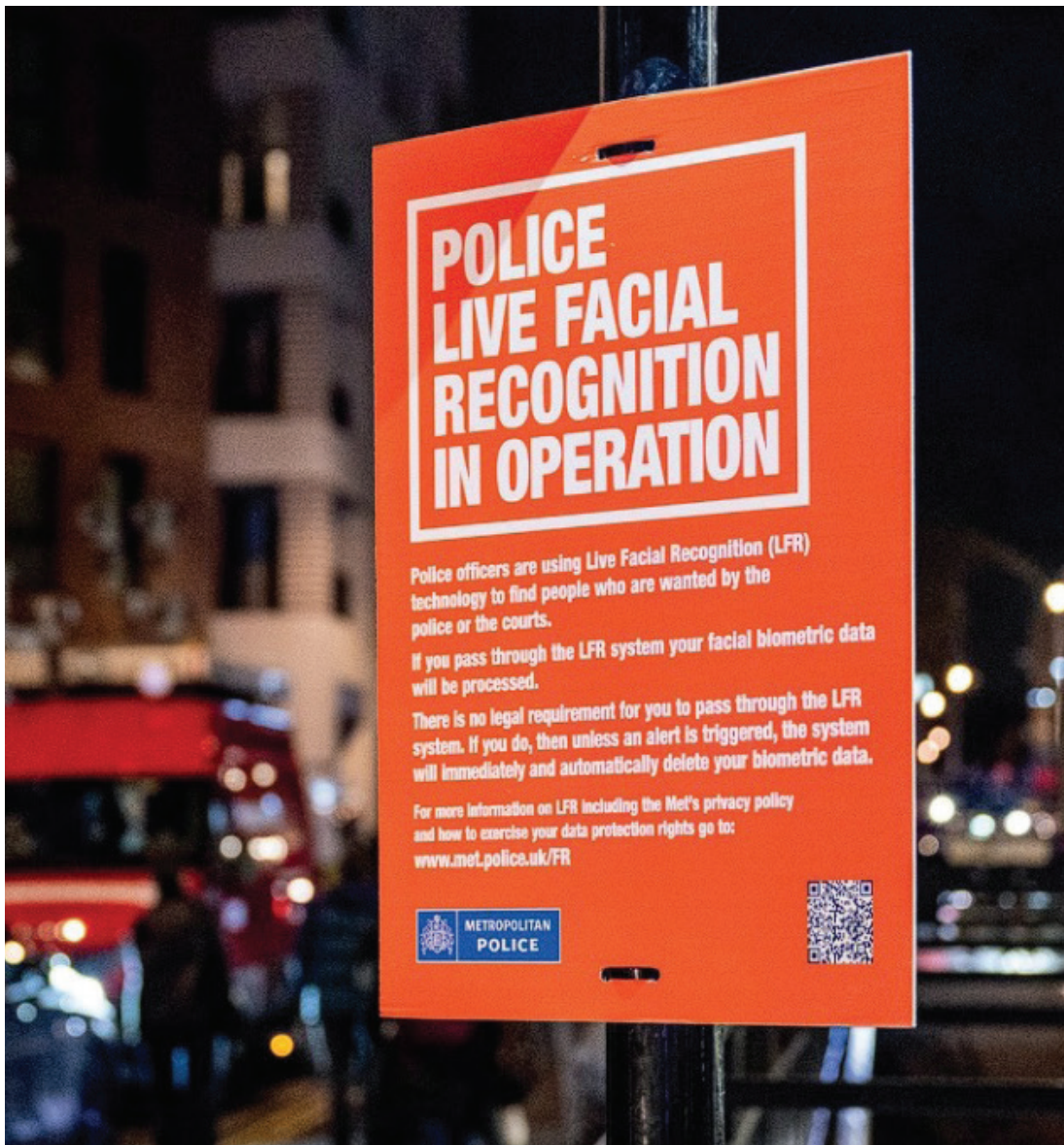
Κατά την επεξεργασία βιομετρικών δεδομένων, είναι ιδιαίτερα σημαντικό να τηρούνται όλες οι βασικές αρχές επεξεργασίας δεδομένων προσωπικού χαρακτήρα που ορίζονται στο άρθρο 5 ΓΚΠΔ.⁵⁴ Μια από τις σημαντικότερες είναι η αρχή του περιορισμού του σκοπού. Επιβάλλει την υποχρέωση να αξιολογείται εάν η επεξεργασία των δεδομένων είναι απολύτως απαραίτητη και αναλογική και εάν υπάρχουν άλλοι, λιγότερο περιοριστικοί τρόποι για την επίτευξη του συγκεκριμένου σκοπού. Επιπροσθέτως, η χρήση ΤΑΠ πρέπει να συμμορφώνεται με τις άλλες απαιτήσεις που ορίζονται στον ΓΚΠΔ, όπως η υποχρέωση παροχής πληροφοριών ως προς τη χρήση αυτών των τεχνολογιών και την επεξεργασία δεδομένων, η λήψη συναίνεσης (βλ. εικόνα 7) και η διασφάλιση της προστασίας έτερων δικαιωμάτων των υποκειμένων των δεδομένων, η εφαρμογή κατάλληλων μέτρων ασφαλείας καθώς και η διενέργεια Εκτίμησης Αντικτύπου σχετικά με την Προστασία Δεδομένων.⁵⁵

52. Σύμφωνα με το άρθρο 4 παράγραφος 14 του ΓΚΠΔ, τα βιομετρικά δεδομένα ορίζονται ως «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 δακτυλοσκοπικά δεδομένα». Βλ. Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων), προσβάσιμο στο: <https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679>.

53. Nesterova, I. (2020). Mass Data Gathering and Surveillance, ό. π., σ. 4-5. Για τη σχέση μεταξύ αναλογικότητας και χρήσης ΤΑΠ στο πλαίσιο του ΓΚΠΔ, βλ. Mobilio, G. (2023). Your Face is Not New to Me – Regulating the Surveillance Power of Facial Recognition Technologies. *Internet Policy Review*, 12(1), 1-31, σ. 10-18.

54. Οι αρχές είναι οι εξής: α) νομιμότητα, αντικειμενικότητα και διαφάνεια, β) περιορισμός του σκοπού, γ) ελαχιστοποίηση των δεδομένων, δ) ακρίβεια, ε) περιορισμός της περιόδου αποθήκευσης, στ) ακεραιότητα και εμπιστοσύνη, ζ) λογοδοσία.

55. Tical, G.M. (2025). Facial Recognition and Biometric Systems: Benefits and Challenges for Law Enforcement, *Land Forces Academy Review*, 30(2), 249-259, σ. 253.



Ενημερωτική πινακίδα για χρήση ΤΑΠ σε δημόσιους χώρους στο Ηνωμένο Βασίλειο:

«Οι αστυνομικοί χρησιμοποιούν τεχνολογία Ζωντανής Αναγνώρισης Προσώπου (ΖΑΠ)

για να εντοπίζουν άτομα που καταζητούνται από την αστυνομία ή τα δικαστήρια.

Εάν περάσετε από το σύστημα ΖΑΠ, τα βιομετρικά δεδομένα του προσώπου σας θα υποβληθούν σε επεξεργασία. Δεν υπάρχει νομική υποχρέωση να περάσετε από το σύστημα ΖΑΠ.

Εάν το κάνετε, εκτός εάν ενεργοποιηθεί κάποιος συναγερμός,

το σύστημα θα διαγράψει αμέσως και αυτόματα τα βιομετρικά σας δεδομένα.

Για περισσότερες πληροφορίες σχετικά με το ΖΑΠ, συμπεριλαμβανομένης της πολιτικής απορρήτου της Met και του τρόπου άσκησης των δικαιωμάτων σας για την προστασία των δεδομένων,

επισκεφθείτε τη διεύθυνση: www.met.police.uk/FR».⁵⁶

56. <https://policinginsight.com/feature/opinion/live-facial-recognitions-defining-moment-why-its-now-time-for-a-national-co-ordination-capability-for-lfr/>.

Νομικές προκλήσεις εγείρει και ο νέος ευρωπαϊκός κανονισμός του 2024 για την καθιέρωση εναρμονισμένων κανόνων σχετικά με την τεχνητή νοημοσύνη, ο οποίος θέτει αυστηρότερους όρους για την αναλογική χρήση της ΤΑΠ.⁵⁷ Ο λεγόμενος Νόμος για την Τεχνητή Νοημοσύνη (AI Act) κατηγοριοποιεί τα διάφορα συστήματα τεχνητής νοημοσύνης με βάση το επίπεδο κινδύνου, κατατάσσοντας τα βιομετρικά συστήματα στα «υψηλού κινδύνου». Σύμφωνα με το άρθρο 5 παρ. 1 στοιχείο η', απαγορεύεται η χρήση συστημάτων εξ αποστάσεως βιομετρικής ταυτοποίησης «σε πραγματικό χρόνο», σε δημόσια προσβάσιμους χώρους για τους σκοπούς της επιβολής του νόμου, εκτός εάν και στον βαθμό που η χρήση αυτή είναι απολύτως αναγκαία για έναν από τους ακόλουθους στόχους:

α) τη στοχευμένη αναζήτηση συγκεκριμένων θυμάτων απαγωγής, εμπορίας ανθρώπων ή σεξουαλικής εκμετάλλευσης ανθρώπων, καθώς και την αναζήτηση εξαφανισθέντων προσώπων·

β) την πρόληψη συγκεκριμένης, ουσιαστικής και επικείμενης απειλής κατά της ζωής ή της σωματικής ακεραιότητας φυσικών προσώπων ή πραγματικής και υπαρκτής ή πραγματικής και προβλέψιμης απειλής τρομοκρατικής επίθεσης· γ) τον εντοπισμό ή την ταυτοποίηση προσώπου ύποπτου για την τέλεση αξιόποινης πράξης, για τον σκοπό της διεξαγωγής ποινικής έρευνας ή δίωξης ή εκτέλεσης ποινικής ποινής για αξιόποινες πράξεις που τιμωρούνται στο οικείο κράτος μέλος με στερητική της ελευθερίας ποινή ή στερητικό της ελευθερίας μέτρο ασφάλειας ανώτατης διάρκειας τουλάχιστον τεσσάρων ετών.

Επίσης, η χρήση συστημάτων εξ αποστάσεως βιομετρικής ταυτοποίησης «σε πραγματικό χρόνο» θα πρέπει σύμφωνα με την παρ. 2 του άρθρου 5 να συμμορφώνεται με το εθνικό δίκαιο και δη τους χρονικούς, γεωγραφικούς και προσωπικούς περιορισμούς. Συμπληρωματικά, θα πρέπει η χρήση τους να συνοδεύεται από εκτίμηση επιπτώσεων στα θεμελιώδη δικαιώματα και καταχώριση του συστήματος στην αρμόδια βάση δεδομένων της ΕΕ. Κάθε χρήση απαιτεί προηγούμενη άδεια από δικαστική ή ανεξάρτητη διοικητική αρχή, η οποία τη χορηγεί μόνο αν αποδεικνύεται ότι η χρήση είναι απολύτως αναγκαία και αναλογική για την επίτευξη ενός από τους στόχους που καθορίζονται στο άνωθεν στοιχείο η', και, ιδίως, περιορίζεται σε ό,τι είναι απολύτως αναγκαίο όσον αφορά τη χρονική περίοδο, καθώς και το γεωγραφικό και προσωπικό πεδίο εφαρμογής (άρθρο 5 παρ. 3).

57. Βλ. Κανονισμός (ΕΕ) 2024/1689 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Ιουνίου 2024, για τη θέσπιση εναρμονισμένων κανόνων σχετικά με την τεχνητή νοημοσύνη και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 300/2008, (ΕΕ) αριθ. 167/2013, (ΕΕ) αριθ. 168/2013, (ΕΕ) 2018/858, (ΕΕ) 2018/1139 και (ΕΕ) 2019/2144 και των οδηγιών 2014/90/ΕΕ, (ΕΕ) 2016/797 και (ΕΕ) 2020/1828 (κανονισμός για την τεχνητή νοημοσύνη) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ). Προσβάσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=OJ:L_202401689.

Τέλος, είναι αξιομνημόνευτο πως ο νέος αυτός κανονισμός υπογραμμίζει ρητά ότι: «θα πρέπει να απαγορεύεται η διάθεση στην αγορά, η θέση σε λειτουργία για τον συγκεκριμένο αυτό σκοπό ή η χρήση συστημάτων ΤΝ [τεχνητής νοημοσύνης] που δημιουργούν ή επεκτείνουν βάσεις δεδομένων αναγνώρισης προσώπου μέσω της μη στοχευμένης εξαγωγής εικόνων προσώπου από το διαδίκτυο ή από βίντεο CCTV, καθώς η πρακτική αυτή αυξάνει το αίσθημα μαζικής παρακολούθησης και μπορεί να οδηγήσει σε κατάφωρες παραβιάσεις των θεμελιωδών δικαιωμάτων, συμπεριλαμβανομένου του δικαιώματος στην ιδιωτική ζωή».

Αντί επιλόγου

Στην τρέχουσα ψηφιακή εποχή, οι βιομετρικές τεχνολογίες, όπως η αναγνώριση προσώπου, έχουν καταστεί απαραίτητα εργαλεία για τις αρχές επιβολής του νόμου για την εξιχνίαση όσο και για την πρόληψη εγκληματικών δραστηριοτήτων. Οι τεχνολογίες αυτές επιτρέπουν την ταχεία και ακριβή αναγνώριση ατόμων, διευκολύνοντας έτσι την άμεση και αποτελεσματική παρέμβαση των διωκτικών αρχών. Πληθώρα ερευνητών και πολιτικών ιθυνόντων έχουν στρέψει με ζήλο το βλέμμα τους προς την ΤΑΠ, ιδίως μάλιστα μετά την ενσωμάτωση της τεχνητής νοημοσύνης, η οποία προσφέρει βελτιωμένη ακρίβεια και αξιοσημείωτη αποτελεσματικότητα. Η επί σειρά ετών δοκιμασμένη αναγνώριση προσώπου, αναβαθμισμένη τώρα με προηγμένους αλγόριθμους και εξελιγμένα μοντέλα βαθιάς μάθησης εκπαιδευμένα στη διαχείριση τεράστιου όγκου δεδομένων, έχει εμπλουτίσει ποικιλοτρόπως το πεδίο της ποινικής, σωφρονιστικής και αντεγκληματικής πολιτικής, προσφέροντας ελπιδοφόρες προοπτικές για την καταπολέμηση και πρόληψη του εγκλήματος.

Παρά ταύτα, η δυνατότητα που προσφέρει η εν λόγω τεχνολογία στις κυβερνήσεις και τις αστυνομικές αρχές να γνωρίζουν τις καθημερινές δραστηριότητες των πολιτών ενισχύει τον κίνδυνο δημιουργίας ενός καθεστώτος διαρκούς επιτήρησης, μιας κοινωνίας που δεν διαφέρει πολύ από αυτή που οραματίστηκε ο συγγραφέας George Orwell. Η ΤΑΠ δεν μπορεί να αντιμετωπίζεται ως ουδέτερη τεχνολογία, διότι εγείρει εξόχως σημαντικούς ηθικούς προβληματισμούς. Συνακόλουθα, δεν θα πρέπει επ' ουδενί να θεωρηθεί πανάκεια στο ζήτημα της δημόσιας ασφάλειας, ούτε να υιοθετείται ασυνειδήτως στο πλαίσιο ενός άκριτου μιμητισμού του παραδείγματος άλλων χωρών.

Προκειμένου να κριθεί η ΤΑΠ ως αξιόπιστη, είναι ζωτικής σημασίας να καθοριστεί με σαφήνεια εάν, τότε και πώς μπορεί να εφαρμοσθεί, διακρίνοντας μεταξύ της στοχευμένης επιτήρησης για συγκεκριμένους ηθικά και κανονιστικά δικαιολογημένους σκοπούς και της μαζικής επιτήρησης. Η αναγνώριση προσώπου με τη χρήση δημόσιων καμερών πρέπει να συμμορφώνεται με τις κατευθυντήριες γραμμές της Ε.Ε. που διέπουν την προστασία των

προσωπικών δεδομένων, την προσεκτική εφαρμογή της τεχνητής νοημοσύνης και την άμβλυνση τυχόν παράπλευρων συνεπειών.

Πρέπει να υφίσταται σαφές νομοθετικό πλαίσιο που να εγγυάται ότι η ΤΑΠ χρησιμοποιείται μόνον όταν είναι πρόσφορη, αναγκαία και αναλογική για την επίτευξη των επιδιωκόμενων σκοπών της. Το παρόν διακύβευμα είναι επίκαιρο και για την χώρα μας, καθώς πριν από μερικές εβδομάδες τέθηκαν σε χρήση οι πρώτες έξυπνες κάμερες τεχνητής νοημοσύνης για τον εντοπισμό παραβατικών οδηγών που δεν συμμορφώνονται με τον αυστηροποιημένο νέο ΚΟΚ,⁵⁸ ενώ ενδέχεται μελλοντικά να επιχειρηθεί και πιο γενικευμένη εφαρμογή της ΤΑΠ.

58. Χρήστου, Σ. (Νοέμβριος 2025). Πρώτες ΑΙ κάμερες σε Συγγρού και Πανεπιστημίου - Ο χάρτης με τα έξι σημεία στην Αθήνα, *Η Καθημερινή*, προσβάσιμο στο: <https://www.kathimerini.gr/society/reportaz/563929309/protes-ai-kameres-se-syggroy-kai-panepistimioy-o-chartis-me-ta-exi-simeia-stin-athina/>.