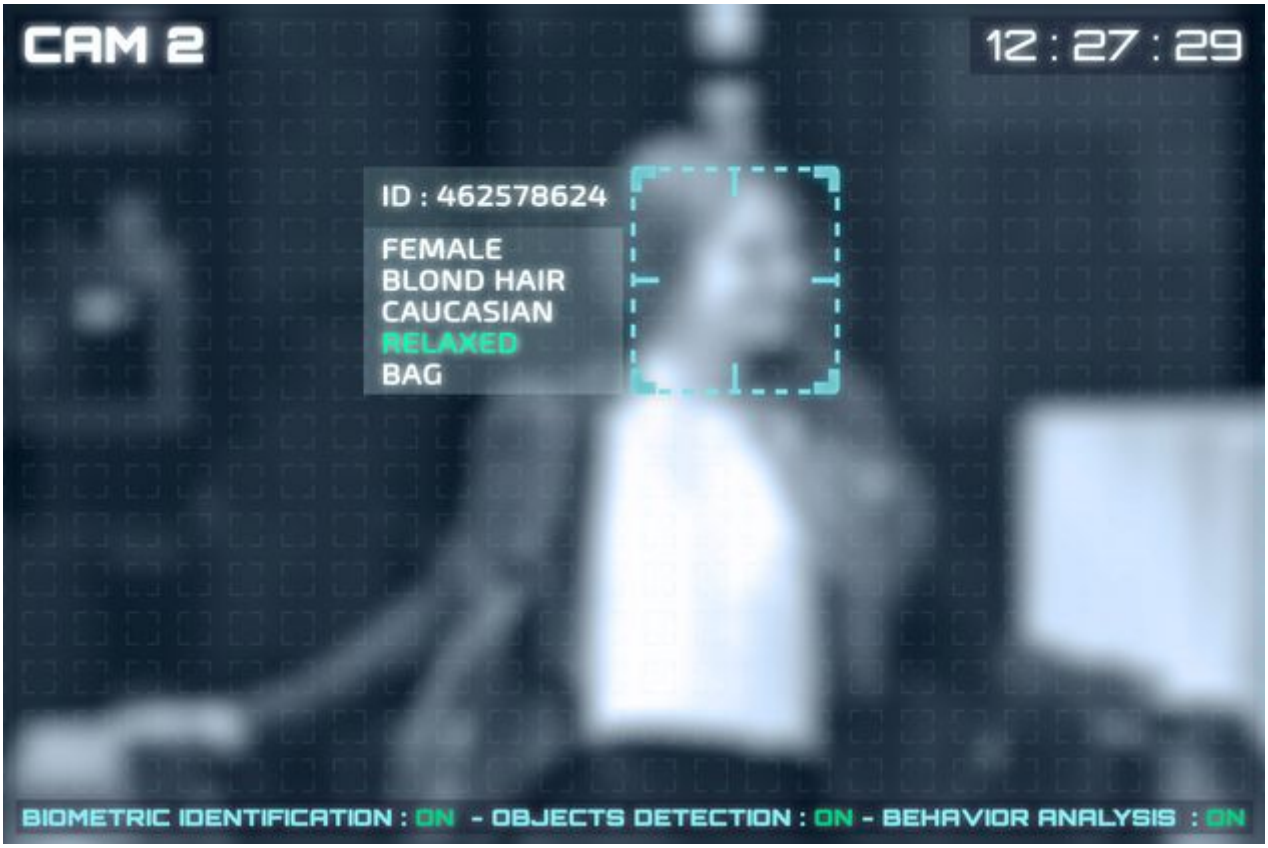
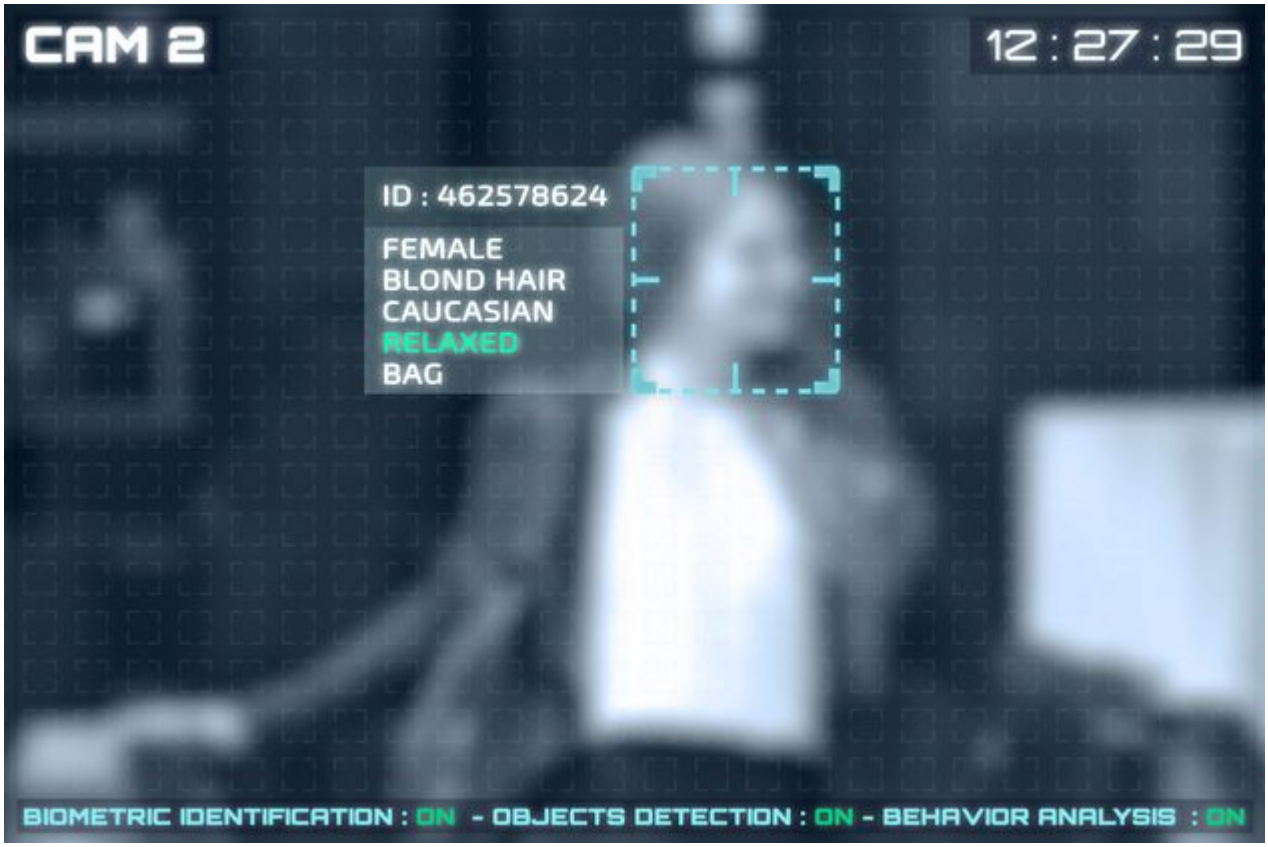
7 Σεπτεμβρίου 2020

Αναγνώριση προσώπου και ζητήματα προστασίας προσωπικών δεδομένων

/ Επιστήμες, Τέχνες & Πολιτισμός / Κοινωνιολογικά (κοινωνική πρόνοια & οικογενειακά θέματα)



Τι προβλέπει η ευρωπαϊκή νομοθεσία. Πόσο προστατεύονται οι πολίτες;



Simulation of a screen of cctv cameras with facial recognition. Facial recognition of a woman.

Το πρόσωπό μας είναι το πιο θεμελιώδες και αναγνωρίσιμο στοιχείο της ταυτότητάς μας. Μπορούμε να ταυτοποιηθούμε μόνο από μια φωτογραφία του προσώπου μας. Τα τελευταία χρόνια έχει παρατηρηθεί μεγάλη αύξηση στη χρήση, αποθήκευση και διάδοση εικόνων προσώπου με παράλληλη την «αυτόματη ταυτοποίηση του προσώπου». Αυτή η τεχνολογία χρησιμοποιείται σε κοινωνικά δίκτυα, εταιρικές βάσεις δεδομένων, ψηφιακά μέσα, κυβερνητικές εφαρμογές και σχεδόν όλες τις βάσεις δεδομένων.

Παράλληλα, οι νόμοι περί προστασίας του απορρήτου γίνονται όλο και πιο σκληροί σε ολόκληρο τον κόσμο και κυρίως στην Ευρωπαϊκή Ένωση, αναγκάζοντας τις εταιρείες που συλλέγουν και χρησιμοποιούν τέτοια δεδομένα να βελτιώσουν τις πολιτικές τους και να βρουν τρόπους να συμμορφωθούν με την εκάστοτε νομοθεσία.

Με την εμφάνιση αυτών των νέων εφαρμογών που επικεντρώνονται στην κοινή χρήση και αναγνώριση δεδομένων εικόνας, προκύπτουν σοβαρά ερωτήματα σχετικά με την προστασία της ιδιωτικής ζωής των ατόμων, ωστόσο οι ενέργειες για την θωράκιση των χαρακτηριστικών του προσώπου και ενδεχομένως και η πρόθεση προς ρύθμιση του σχετικού πλαισίου είναι ακόμα περιορισμένες.

Από νομική πλευρά, τα δεδομένα που συλλέγει η τεχνολογία αναγνώρισης

προσώπου ταξινομούνται στα βιομετρικά δεδομένα, καθώς συλλέγονται πληροφορίες σχετικά με τα χαρακτηριστικά του προσώπου, τα οποία κατηγοροποιούνται ως «ευαίσθητα προσωπικά δεδομένα».

Ο Γενικός Κανονισμός Προσωπικών Δεδομένων διαχωρίζει τις βιομετρικές πληροφορίες σε δύο κατηγορίες, στα φυσικά χαρακτηριστικά και στα χαρακτηριστικά συμπεριφοράς. Τα φυσικά χαρακτηριστικά είναι τα χαρακτηριστικά του προσώπου, δακτυλικά αποτυπώματα, χαρακτηριστικά ίριδας, βάρος κ.λπ., ενώ τα χαρακτηριστικά συμπεριφοράς είναι συνήθειες, ενέργειες, χαρακτηριστικά προσωπικότητας, ιδιοτροπίες κ.λπ.
Ήδη με βάση την πρόβλεψη του άρθρου 6 του ΓΚΠΔ τίθενται τα εχέγγυα και οι όροι με τους οποίους μπορούν να υποστούν νομική επεξεργασία και συλλογή τα χαρακτηριστικά του προσώπου, με εννοούμενες τις εξαιρέσεις στον κανόνα ως προς τα θέματα δημόσιας ασφάλειας.

Επιπλέον, το νομοθετικό ευρωπαϊκό πλαίσιο δίνει τη δυνατότητα στα κράτη μέλη να προσθέτουν περιορισμούς στη χρήση και διαχείριση των ευαίσθητων δεδομένων, όπως κρίνουν κατάλληλο.

Σε ευρωπαϊκό επίπεδο, η Αντιπρόεδρος της Επιτροπής Margrethe Vestager δηλώνει πως σύμφωνα με το παρόν καθεστώς προστασίας δεδομένων της ΕΕ η αυτόματη αναγνώριση μέσω της τεχνολογίας αναγνώρισης προσώπου είναι παράνομη. Σε συνέντευξη τύπου που παραχώρησε στις 13 Φεβρουαρίου τόνισε πως «όπως ισχύει τώρα, θα έλεγα μην την χρησιμοποιείτε (την αυτόματη αναγνώριση προσώπων), επειδή δεν μπορείτε να λάβετε τη συγκατάθεσή από τα υποκείμενα».

Περαιτέρω, μεγάλες εταιρίες δεδομένων έχουν ξεκινήσει να αποχαρακτηρίζουν τις εικόνες που διατηρούν στις βάσεις δεδομένων τους ώστε να μην είναι αυτομάτως αναγνωρίσιμες ή επαναξιολογούν τις πολιτικές τους. Επιπλέον αναπτύσσονται συνεχώς τεχνικές και διαδικασίες απο-ταυτοποίησης που καθίστανται διαθέσιμες στο κοινό. Καθίστανται γνωστές ωστόσο; Επιπλέον, μεγάλο ζήτημα παραμένει η συνεχιζόμενη χρήση αλγορίθμων τεχνητής νοημοσύνης, που καθιστά την αυτόματη αναγνώριση ως κάτι σχετικά απλό, καθώς και το γεγονός ότι η «δημόσια» επεξεργασία διαθέσιμων φωτογραφιών συνιστά αρκετά συχνό φαινόμενο.

Είναι αναγκαίο οι εταιρίες δεδομένων να επαναξιολογήσουν τις στάσεις τους και να αλλάξουν κατεύθυνση ειδικά στις «δημόσιες» ευκαιρίες επεξεργασίας και ταυτοποιήσεις προσώπων. Από την μια πλευρά η υπερ-ρύθμιση της κατάστασης ενέχει κινδύνους, ωστόσο η κατεύθυνση που παίρνει συνεχώς η Ευρωπαϊκή Νομοθεσία δεν έχει ως γνώμονα την επικαιροποίηση δικλείδων ασφαλείας από τις

λεγόμενες εταιρίες συλλογής δεδομένων, αλλά αντιθέτως δίνεται η προτίμηση στην ενημέρωση των χρηστών για τυχόν ευθύνες από παραβιάσεις, με ουσιαστική της μετακύλιση της ευθύνης στους χρήστες.

Πηγή: huffingtonpost.gr