Η περίπτωση των Συστημάτων Απομακρυσμένης Βιομετρικής Αναγνώρισης και Ταυτοποίησης φυσικών προσώπων για σκοπούς δίωξης του εγκλήματος σύμφωνα με το σχέδιο πρότασης Κανονισμού Ε.Ε. για την Τεχνητή Νοημοσύνη

ΓΡΗΓΟΡΗ ΤΣΟΛΙΑ
Δικηγόρου-ΜΔ Ποινικών Επιστημών
Μέλους (αν.) Αρχής Προστασίας Δεδομένων
Εθνικού Εμπειρογνώμονα Working Group CDPC του Συμβουλίου της Ευρώπης
"Artificial Intelligence & Criminal Law"

Ι. Εισαγωγή.

1. Η εγκατάσταση και η ετοιμότητα προς λειτουργία κλειστών κυκλωμάτων βιντεοεπιτήρησης (CCTV) σε δημόσιους χώρους συνιστά από μόνη της έναν άμεσο κίνδυνο για τα προσωπικά δεδομένα και τις ατομικές ελευθερίες των πολιτών που εισέρχονται στο πεδίο λήψης – εμβέλειας του συστήματος. Εάν η τεχνική αυτή δυνατότητα συνδυαστεί επιπλέον με τη χρήση λογισμικών τεχνητής νοημοσύνης και συστημάτων αναγνώρισης- ταυτοποίησης προσώπου, τότε η επέμβαση στα ατομικά δικαιώματα καθίσταται βαθύτερη και άρα απαιτείται η λήψη διασφαλιστικών μέτρων τόσο για το ίδιο το γεγονός της κατασκευής και λειτουργίας των συστημάτων, όσο και για την πλήρωση των ουσιαστικών και διαδικαστικών εγγυήσεων ενεργοποίησης τους και εν συνεχεία επεξεργασίας προσωπικών δεδομένων.

Η τεχνολογία αναγνώρισης προσώπου (facial recognition) που αποσκοπεί στην ταυτοποίηση φυσικών προσώπων δια της επεξεργασίας βιομετρικών δεδομένων βασίζεται σε συστήματα, εφαρμογές και λογισμικά τεχνητής νοημοσύνης που εκπαιδεύονται με βάση συγκεκριμένα πρότυπα να παρέχουν κατ' αρχήν τις σχετικές πληροφορίες ταυτοποίησης. Τα συστήματα αυτά δύνανται ανάλογα με το λογισμικό τους να εξάγουν σε πραγματικό χρόνο επιπλέον αυτοματοποιημένα συμπεράσματα με βάση τη στάση του σώματος, τις κινήσεις, τις μικροεκφράσεις του προσώπου, ακόμη και την χροιά ή τον τόνο της φωνής ενός φυσικού προσώπου ανάλογα με τον επιδιωκόμενο σκοπό της επεξεργασίας π.χ. σε σχέση με τις πιθανότητές να εγκληματήσει ένα άτομο που στέκεται έξω από μια Τράπεζα.

Τα σχετικά λογισμικά βαρύνονται σε αρκετές περιπτώσεις με εσφαλμένα αποτελέσματα ταυτοποίησης προσώπων αλλά και συμπερασμάτων πρόβλεψης συμπεριφορών συνεπεία της επεξεργασίας/τροφοδοσίας με χαμηλής ποιότητάς δεδομένων αλλά και του τρόπου εκπαίδευσης των αλγορίθμων, παραβιάζοντας έτσι τελικά μια εκ των βασικών αρχών επεξεργασίας των προσωπικών δεδομένων και δη εκείνης της ακρίβειας, επιπλέον δε επέρχονται διακρίσεις και προκαταλήψεις, ιδίως σε σχέση με το χρώμα και την φυλετική ή εθνοτική καταγωγή. Οι Αρχές Προστασίας Δεδομένων (ΑΠΔ) της Γαλλίας και της Σουηδίας απαγόρευσαν τη λειτουργία συστημάτων αναγνώρισης προσώπων σε σχολεία, η ΑΠΔ του Βελγίου σταμάτησε την εγκατάσταση συστήματος στο αεροδρόμιο των Βρυξελλών ενώ τα διοικητικά δικαστήρια του Η.Β. και της Γαλλίας εξέδωσαν πρόσφατα σχετικές με το θέμα αποφάσεις.

2. Με το Π.Δ. υπ' αρ. 75/2020 (ΦΕΚ Α'173/10.9.2020) «*Χρήση συστημάτων επιτήρησης με λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους*» κατ'

εφαρμογή της εξουσιοδοτικής διάταξης του άρθρου 14 παρ. 4 ν. 3917/2011 ορίσθηκαν οι ειδικότεροι κανόνες για την εγκατάσταση και λειτουργία, σε δημόσιους χώρους, συστημάτων λήψης ή καταγραφής ήχου ή εικόνας, στο μέτρο που διενεργείται επεξεργασία προσωπικών δεδομένων κατά τρόπο ώστε να επιτυγχάνονται αποτελεσματικά οι σκοποί του νόμου, με ταυτόχρονη διασφάλιση των δικαιωμάτων των προσώπων που θίγονται από τη χρήση των συστημάτων αυτών. Στο άρθρο 2 του Π.Δ. ορίζεται ότι οι εφαρμοζόμενες διατάξεις που αφορούν τα εν λόγω συστήματα, στα οποία ανήκουν ιδίως τα κλειστά κυκλώματα τηλεόρασης, περιλαμβάνονται όσα διαθέτουν «*πρόσθετο εξοπλισμό για τη μετάδοση, αποθήκευση και* ***κάθε είδους περαιτέρω επεξεργασία*** *της εικόνας και του ήχου*». Από την διατύπωση αυτή δεν προκύπτει εναργώς εάν στην τελευταία έννοια είναι δυνατό να περιληφθούν και συστήματα επεξεργασίας βιομετρικών δεδομένων για την αναγνώριση και ταυτοποίηση φυσικών προσώπων, όπως επεσήμανε και η Αρχή Προστασίας Δεδομένων (ΑΠΔ) με την υπ' αρ. 3/2020 Γνωμοδότηση της, στην οποία θα γίνει αναλυτικότερη αναφορά στο τέλος της παρούσας.

ΙΙ. Η θέση του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων (ΕΣΠΔ) καθώς και του Ευρωπαίου Επόπτη Προστασίας Δεδομένων (ΕΕΠΔ).

Το ΕΣΠΔ, ήδη με τις υπ' αρ. 3/2019 Κατευθυντήριες Γραμμές σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω βιντεοσυσκευών έθεσε τις γενικές παραμέτρους για τη σύννομη συλλογή και επεξεργασία **βιομετρικών δεδομένων**, ήτοι προσωπικών δεδομένων τα οποία προκύπτουν από **ειδική τεχνική επεξεργασία** συνδεόμενη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου και τα οποία επιτρέπουν ή επιβεβαιώνουν την **αδιαμφισβήτητη ταυτοποίηση** του, όπως εικόνες προσώπου (βλ. αρ. 4 περ. 14 ΓΚΠΔ και αρ. 3 περ. 13 οδηγίας 680/16), διευκρινίζοντας ορθά ότι η απλή συλλογή υλικού βιντεοσκόπησης που απεικονίζει πρόσωπα δεν μπορεί να θεωρηθεί ότι αποτελεί καθεαυτό βιομετρικό δεδομένο. Προσφάτως, το ΕΣΠΔ εξέφρασε την ανησυχία του για τη χρήση τεχνολογιών αναγνώρισης προσώπου και την αμφιβολία του για τη νομιμότητά της χρήσης των σχετικών υπηρεσιών που παρέχονται από εταιρία που συλλέγει φωτογραφίες από κοινωνικά δίκτυα και φέρεται να τα διαθέτει για σκοπούς δίωξης τους εγκλήματος. Αντίστοιχες ανησυχίες εξέφρασε κατά το παρελθόν και ο ΕΕΠΔ για την χρήση τεχνολογιών αναγνώρισης προσώπου, ενώ πλέον πρόσφατα, μετά την ανακοίνωση της Ε.Ε. για το σχέδιο Κανονισμού Τεχνητής Νοημοσύνης, εξέφρασε ρητά την αντίθεση του στην χρήση συστημάτων βιομετρικής αναγνώρισης σε δημόσιους χώρους.

ΙΙΙ. Η πρόταση Κανονισμού Ε.Ε. για την Τεχνητή Νοημοσύνη.

Α. Εισαγωγή.

1. Με το προτεινόμενο σχέδιο Κανονισμού Τεχνητής Νοημοσύνης (DAE - Item (europa.eu)) η Ευρωπαϊκή Επιτροπή προτείνει την δημιουργία σχετικού νομικού πλαισίου ακολουθώντας μια προσέγγιση με βάση τον κίνδυνο (risk based approach) κατηγοριοποιώντας τα συστήματα ΤΝ ανάλογα με το επίπεδο κινδύνου που ενδέχεται να προκαλέσουν στην ασφάλεια και τα θεμελιώδη ατομικά δικαιώματα των πολιτών και των επιχειρήσεων διακρίνοντας μεταξύ συστημάτων i. «*μη αποδεκτού κινδύνου*», που απαγορεύονται πλήρως, ii. «*υψηλού κινδύνου*» των οποίων η κατασκευή και χρήση υπόκειται σε αυστηρές υποχρεώσεις προτού επιτραπεί η διάθεση και η

κυκλοφορία τους στην αγορά, iii. «*περιορισμένου κινδύνου*», των οποίων η χρήση επιτρέπεται υπό συγκεκριμένες υποχρεώσεις διαφάνειας και iv. «*ελαχίστου κινδύνου*», των οποίων η χρήση επιτρέπεται χωρίς την επιβολή υποχρεώσεων με βάση τη πρόταση σχεδίου Κανονισμού ΤΝ.

2. Στην περίπτωση των συστημάτων ΤΝ υψηλού κινδύνου, προ της κυκλοφορίας τους στην αγορά και χρήσης τους, θα πρέπει να έχει προηγηθεί αξιολόγηση της συμμόρφωσης προς τις απαιτήσεις του προτεινόμενου Κανονισμού ΤΝ που περιλαμβάνουν: εγκατάσταση και λειτουργία συστήματος εποπτείας και διαχείρισης κινδύνου καθ' όλο το κύκλο ζωής του ελεγχόμενου συστήματος ΤΝ, τήρηση κανόνων για τη χρήση δεδομένων αναγκαίων για την εκπαίδευση των αλγοριθμικών συστημάτων, τεχνική τεκμηρίωση του συστήματος ΤΝ προ της θέσης σε κυκλοφορία στην αγορά, σχεδιασμό και ανάπτυξη του συστήματος ΤΝ κατά τρόπο ώστε να διατηρεί αυτόματες καταγραφές συμβάντων (logs) με περαιτέρω δυνατότητα αναγνώρισης προτύπων ή κοινά αποδεκτών χαρακτηριστικών που θα καθιστούν εφικτή την ιχνηλάτηση του συστήματος, υποχρεώσεις διαφάνειας ώστε οι χρήστες των συστημάτων ΤΝ να μπορούν να ερμηνεύουν το εξαγόμενο αποτέλεσμα του συστήματος και να το χρησιμοποιούν συναφώς, υποχρέωση ανθρώπινης επίβλεψης κατά τη λειτουργία του συστήματος και σχεδιασμός του συστήματος ώστε να επιτυγχάνεται το κατάλληλο επίπεδο ακρίβειας, διαθεσιμότητας και κυβερνοασφάλειας (άρθρα 8-15 σχ Καν ΤΝ και περαιτέρω εξειδίκευση τους στα άρθρα 16-29 σχ Καν ΤΝ). Ο έλεγχος της πλήρωσης των απαιτούμενων υποχρεώσεων ανατίθεται σε ειδικές ελεγκτικές αρχές οι οποίες θα προβαίνουν στην σχετική επιβεβαίωση και η οποία μπορεί να συνίσταται και στην έκδοση πιστοποιητικών συμβατότητας (αρ. 44 σχ. Καν. ΤΝ) ή δήλωση συμμόρφωσης της ΕΕ με σήμανση CE (αρ. 48-49 σχ. Καν. ΤΝ). Προ της κυκλοφορίας στην αγορά, το σύστημα ΤΝ υψηλού κινδύνου, εφόσον έχει διέλθει επιτυχώς των προηγούμενων ελέγχων, καταχωρείται σε ειδική βάση δεδομένων της Ε.Ε. (αρ. 51 και 60 σχ Καν ΤΝ). Μετά την κυκλοφορία του συστήματος ΤΝ υψηλού κινδύνου στην αγορά, το σχ Καν ΤΝ περιλαμβάνει ένα δεύτερο στάδιο υποχρεώσεων συμμόρφωσης που περιλαμβάνουν την εγκατάσταση και λειτουργία συστήματος παρακολούθησης του συστήματος ΤΝ, την υποχρεωτική υποβολή αναφοράς σοβαρού συμβάντος ή δυσλειτουργίας τους συστήματος ΤΝ που οδηγεί σε παραβίαση υποχρεώσεων του δικαίου της Ε.Ε. για την προστασία ατομικών και θεμελιωδών δικαιωμάτων.

Β. Η περίπτωση των Συστημάτων Απομακρυσμένης Βιομετρικής Αναγνώρισης και Ταυτοποίησης φυσικών προσώπων για σκοπούς δίωξης του εγκλήματος.

1. Σύμφωνα με το σχ. Καν. ΤΝ ως σύστημα απομακρυσμένης βιομετρικής αναγνώρισης/ταυτοποίησης (Remote Biometric Identification-RBI) ορίζεται το σύστημα ΤΝ που αποσκοπεί στην εξ' αποστάσεως αναγνώριση φυσικών προσώπων δια της σύγκρισης των βιομετρικών δεδομένων ενός προσώπου σε σχέση προς τα βιομετρικά δεδομένα τα οποία περιλαμβάνονται σε μια βάση δεδομένων αναφοράς, **χωρίς να γνωρίζει εκ προοιμίου** ο χειριστής του συστήματος (π.χ. η Αστυνομία) εάν το υπό διερεύνηση πρόσωπο θα είναι παρόν και δύναται να ταυτοποιηθεί κατά τη λειτουργία του συστήματος (αρ. 3 περ. 36). Περαιτέρω, το σχ. Καν. ΤΝ διακρίνει μεταξύ συστήματος απομακρυσμένης βιομετρικής αναγνώρισης/ταυτοποίησης που λειτουργεί σε **πραγματικό χρόνο** (real-time RBI) και προβαίνει σε άμεση ή με ελάχιστη καθυστέρηση, ταυτοποίηση (αρ. 3 περ. 37) και συστήματος που λειτουργεί **ετεροχρονισμένα** (post RBI) και προβαίνει σε ταυτοποίηση όχι σε πραγματικό χρόνο

αλλά μεταγενέστερα (αρ. 3 περ. 38). Τέλος, το σχ. Καν. ΤΝ διακρίνει μεταξύ συστημάτων απομακρυσμένης βιομετρικής αναγνώρισης/ταυτοποίησης σε δημόσια προσβάσιμους χώρους (αρ. 3 περ. 39) και μη.

2. Από τις διατάξεις του άρθρου 6 σε συνδυασμό με το Παράρτημα ΙΙΙ περ. 1 α' και περ. 6' του σχ Κ ΤΝ προκύπτει ότι τα συστήματα απομακρυσμένης βιομετρικής αναγνώρισης/ταυτοποίησης (και κατηγοριοποίησης) που λειτουργούν είτε σε πραγματικό χρόνο (real-time RBI) είτε ετεροχρονισμένα (post RBI) εμπίπτουν στην κατηγορία συστημάτων ΤΝ υψηλού κινδύνου, είτε χρησιμοποιούνται από ιδιώτες, είτε από αρμόδιες δημόσιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης και δίωξης ποινικών αδικημάτων (εφεξής «σκοπούς επιβολής του νόμου»).

Όταν όμως τα ανωτέρω συστήματα ΤΝ λειτουργούν σε **πραγματικό χρόνο** (real time RBI) σε **δημόσια προσβάσιμους χώρους** για σκοπούς επιβολής του νόμου, τότε εμπίπτουν κατά το άρθρο 5 παρ. 1 περ. δ' στην κατηγορία των συστημάτων «*μη αποδεκτού κινδύνου*» και η χρήση τους **απαγορεύεται**, εκτός αν είναι αυστηρά αναγκαία για έναν από τους ακόλουθους σκοπούς:

i. την στοχευμένη αναζήτηση πιθανών θυμάτων εγκλημάτων, περιλαμβανομένων εξαφανισμένων παιδιών

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

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

Εν συνεχεία, από τις διατάξεις της παραγράφου 2 του άρθρου 5 προβλέπονται τα κριτήρια λήψης αλλά και μεταγενέστερου ελέγχου της νομιμότητάς της απόφασης για τη χρήση του συστήματος: η φύση της κατάστασης που απαιτεί τη χρήση του συστήματος και ιδίως η σοβαρότητα, η πιθανότητα και το μέγεθος της βλάβης που μπορεί να προκληθεί από την μη χρήση του συστήματος, οι συνέπειες από τη χρήση στα δικαιώματα και τις ελευθερίες των ατόμων και ιδίως η σοβαρότητα, η πιθανότητα και το μέγεθος των συνεπειών. Επιπλέον, από τις ίδιες διατάξεις απαιτείται η χρήση των ανωτέρω συστημάτων να είναι σύμφωνη προς απαραίτητες και αναλογικές εγγυήσεις λαμβάνοντας υπόψη τους αναγκαίους χρονικούς, γεωγραφικούς και προσωπικούς περιορισμούς.

3. Η **σημαντικότερη εγγύηση** προβλέπεται από τις διατάξεις της παραγράφου 3 του άρθρου 5 με την οποία εισάγεται η υποχρέωση **προηγούμενης αδειοδότησης** της σε **πραγματικό χρόνο** λειτουργίας του συστήματος αναγνώρισης σε **δημόσια προσβάσιμους χώρους**, η οποία θα πρέπει να παρέχεται από ανεξάρτητη και αμερόληπτη δικαστική ή διοικητική αρχή, κατόπιν αιτιολογημένου αιτήματος της αρμόδιας αρχής που θα συνοδεύεται από αντικειμενικές αποδείξεις ή εναργείς ενδείξεις, εφόσον είναι αναγκαία και αναλογική για την επίτευξη των επιδιωκόμενων σκοπών, λαμβάνοντας υπόψη τα κριτήρια της παρ. 2 και εφόσον προβλέπονται από εναργείς και αναλυτικές ρυθμίσεις που περιλαμβάνονται σε διατάξεις της εθνικής νομοθεσίας («*ποιοτικός και προβλέψιμος νόμος*»), απηχώντας κατά τον τρόπο αυτό τις απαιτήσεις συμβατότητάς προς τις διατάξεις του ΧΘΔΕΕ και ΕΣΔΑ καθώς και την σχετική νομολογία τόσο του ΕΔΔΑ, όσο κυρίως του Δικαστηρίου της Ε.Ε. όπως

διαμορφώθηκε στο πλαίσιο εξέτασης της νομοθεσίας για την υποχρεωτική διατήρηση των δεδομένων από Παρόχους (ήδη ακυρωθείσα Οδηγία 2006/24/ΕΚ) και για την εφαρμογή των διατάξεων του άρ. 15 Οδηγίας 2002/58/ΕΚ, ήτοι από την απόφαση *Digital Rights Ireland Ltd* (C-293/12&C-594/12) έως την πρόσφατη *H.K. Prokuratuur* (C-746/18). Κατ' εξαίρεση, σε περίπτωση επείγοντος, οι σχετικές διασφαλίσεις μπορούν να λαμβάνονται μετά τη θέση σε λειτουργία του συστήματος.

4. Απολύτως σύμφωνα προς το πεδίο εφαρμογής του δικαίου της Ε.Ε., στην παράγραφο 4 του ίδιου άρθρου προβλέπεται ότι εναπόκειται στην διακριτική ευχέρεια του κάθε κράτους μέλους να επιτρέψει ή μη (αιτ. σκ. 22) , την εν όλω ή εν μέρει χρήση συστημάτων απομακρυσμένης βιομετρικής ταυτοποίησης σε δημόσια προσβάσιμους χώρους σε πραγματικό χρόνο (real time RBI), σύμφωνα όμως με τους όρους και εγγυήσεις που αναφέρονται στις προηγούμενες παραγράφους που θα περιληφθούν στον εθνικό νόμο και επιπλέον θα προσδιορίζεται η αρμόδια αρχή που θα παρέχει την άδεια για τη χρήση των συστημάτων αυτών για λόγους επιβολής του νόμου. Τα ανωτέρω φαίνεται ότι δεν καλύπτουν τις περιπτώσεις χρήσης συστημάτων ΤΝ ετεροχρονισμένης λειτουργίας (post RBI).

Γ. Η σχέση των διατάξεων του σχ Καν ΤΝ προς εκείνες της Οδηγίας 680/16 για την επεξεργασία δεδομένων προσωπικού χαρακτήρα για λόγους επιβολής του νόμου.

1. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης και δίωξης ποινικών αδικημάτων (ήδη «σκοπούς επιβολής του νόμου») προβλέπονται από την Οδηγία 680/16, όπως ενσωματώθηκε με το κεφάλαιο Δ' του ν. 4624/2019.

Όπως προεκτέθηκε, τα εν λόγω συστήματα απομακρυσμένης βιομετρικής ταυτοποίησης σε δημόσια προσβάσιμους χώρους σε πραγματικό χρόνο (real time RBI), κατ' αρχήν υπάγονται στην κατηγορία των συστημάτων ΤΝ «*μη αποδεκτού κινδύνου*» και άρα απαγορεύεται η χρήση τους, εκτός αν εξαιρετικά συντρέχουν οι ουσιαστικές και διαδικαστικές προϋποθέσεις που επίσης προεκτέθηκαν. Εάν συντρέχουν οι τελευταίες, τότε τα εν λόγω συστήματα, προκειμένου να είναι σύμφωνα με τις κατασκευαστικές και λοιπές απαιτήσεις και υποχρεώσεις του σχ Καν. ΤΝ, υπάγονται στις διατάξεις που αφορούν τις οικείες σχεδιαστικές, κατασκευαστικές και λειτουργικές υποχρεώσεις των συστημάτων ΤΝ «*υψηλού κινδύνου*» σύμφωνα με τη ρητή πρόβλεψη του άρθρου 6 παρ. 2 σχ. Καν. ΤΝ και επιπλέον σε εκείνες του άρθρου 43 παρ. 1 για τον έλεγχο της αξιολόγησης της συμμόρφωσης από αρμόδια αρχή. Εξαιρέσεις από τις υποχρεώσεις διαφάνειας των προμηθευτών και χρηστών συστημάτων ΤΝ για σκοπούς επιβολής του νόμου προβλέπονται από τις διατάξεις του άρ. 52 σχ Καν ΤΝ.

Οι ανωτέρω απαιτήσεις/υποχρεώσεις αφορούν το πρώτο στάδιο σχεδιασμού, κατασκευής και λειτουργίας του συστήματος ΤΝ προ της κυκλοφορίας του στην αγορά και της χρήσης του. Εάν οι απαιτήσεις/υποχρεώσεις εκείνες δεν πληρούνται, το σύστημα ΤΝ δεν μπορεί να κυκλοφορήσει στην αγορά και άρα να τεθεί σε λειτουργία. Υπενθυμίζεται ότι κατά την τελευταία φάση του πρώτου σταδίου συμμόρφωσης προς τις απαιτήσεις και ελέγχου τους, το σύστημα ΤΝ καταχωρείται σε ειδική βάση δεδομένων της Ε.Ε.

Εν όψει των ανωτέρω, προτού καταφύγει κανείς στον έλεγχο των προϋποθέσεων νομιμότητας της επεξεργασίας των βιομετρικών δεδομένων, θα πρέπει

σε ένα πρώτο στάδιο να έχει διασφαλιστεί η συμμόρφωση προς τις απαιτήσεις και την πλήρωση των υποχρεώσεων του Σχ Κ ΤΝ.

2. Από την αιτιολογική σκέψη 23 του σχ Καν ΤΝ προκύπτει ότι οι διατάξεις του για τη χρήση των συστημάτων RBI σε πραγματικό χρόνο σε δημόσια προσβάσιμους χώρους από αρμόδιες αρχές για σκοπούς επιβολής του νόμου, η οποία συνεπάγεται την επεξεργασία βιομετρικών δεδομένων, βασίζεται στο άρθρο 16 της Συνθήκης Λειτουργίας της ΕΕ (ΣΛΕΕ) για την προστασία προσωπικών δεδομένων και επομένως εφαρμόζονται ως ειδικότερες ("lex specialis") εκείνων του άρθρου 10 της Οδηγίας 680/16 που ρυθμίζουν το ίδιο αντικείμενο, ήτοι την επεξεργασία βιομετρικών δεδομένων. Επισημαίνεται δε από την ίδια αιτιολογική σκέψη ότι η χρήση και η επεξεργασία των βιομετρικών δεδομένων στην περίπτωση των συγκεκριμένων συστημάτων ΤΝ θα είναι δυνατή μόνο εφόσον είναι σύμφωνη αποκλειστικά προς το πλαίσιο που ορίζεται από τον Κανονισμό ΤΝ χωρίς να παρέχεται άλλο ουσιαστικό πεδίο εφαρμογής (εκτός του παρόντος) στις αρμόδιες αρχές για λόγους επιβολής του νόμου που προβλέπονται στο πλαίσιο του άρθρου 10 της Οδηγίας 680/16.

Τέλος, επισημαίνεται από την ίδια αιτιολογική σκέψη ότι στο πλαίσιο αυτό ο εν λόγω Κανονισμός ΤΝ δεν αποσκοπεί στο να παρέχει τη νομική βάση για την επεξεργασία των προσωπικών δεδομένων υπό το άρθρο 8 της Οδηγίας 680/16, εννοώντας πιθανώς ότι ο Κανονισμός ΤΝ δεν εμπίπτει στην περίπτωση του εξουσιοδοτικού δικαίου της Ε.Ε. που αναφέρεται στην παράγραφο 2 του άρθρου 8 της Οδηγίας 680/16 και επομένως η νομική βάση θα διαπλασθεί με βάση το εθνικό δίκαιο κατ' εξουσιοδότηση του Κανονισμού ΤΝ. Στην περίπτωση εκείνη, η όποια εθνική ρύθμιση για την χρήση του συστήματος απομακρυσμένης βιομετρικής ταυτοποίησης σε πραγματικό χρόνο σε δημόσια προσβάσιμους χώρους καθώς και η επεξεργασία των βιομετρικών δεδομένων θα βασίζεται στις διατάξεις του Κανονισμού ΤΝ και όχι σε εκείνες των άρθρων 8 και 10 της Οδηγίας 680/16.

Εξ' αντιδιαστολής, η επεξεργασία προσωπικών δεδομένων δια της χρήσης (β' στάδιο του σχ. Καν ΤΝ) απομακρυσμένων βιομετρικών συστημάτων ταυτοποίησης σε πραγματικό χρόνο (real time-rt RBI) σε δημόσια προσβάσιμους χώρους που **δεν αποσκοπούν** στην επιβολή του νόμου (LE) ή βιομετρικών συστημάτων **ετεροχρονισμένης** ταυτοποίησης (post RBI) σε δημόσια προσβάσιμους χώρους που αποσκοπούν στην επιβολή του νόμου ή η χρήση τους σε μη δημόσια προσβάσιμους χώρους θα εξακολουθήσουν να διέπονται από το άρθρο 9 Γενικού Κανονισμού Προστασίας Δεδομένων υπ' αρ. 697/16 (GDPR) και το άρθρο 10 της Οδηγίας 680/16 (Law Enforcement Directive – LED). Σχηματικά θα μπορούσε να παρουσιαστεί ως εξής:

Real Time	RBI	LEA	Καν ΤΝ
Real Time	RBI	Non LEA	GDPR
Post	RBI	LEA	LED
Post	RBI	Non LEA	GDPR

3. Από τις διατάξεις του άρθρου 10 της Οδηγίας 680/2016 προκύπτουν οι προϋποθέσεις επεξεργασίας των βιομετρικών δεδομένων για την αποκλειστική ταυτοποίηση ενός φυσικού προσώπου εν γένει, χωρίς να προσδιορίζονται ειδικότερες ουσιαστικές και διαδικαστικές προϋποθέσεις στην περίπτωση λειτουργίας συστημάτων βιομετρικής ταυτοποίησης **σε πραγματικό χρόνο** και σε **δημόσια προσβάσιμους χώρους** για τους σκοπούς επιβολής του νόμου. Εν όψει των όσων

έχουν προπαρατεθεί πιθανολογείται ότι η Ε.Ε. θέλησε να ρυθμίσει αυτοτελώς, εξειδικευμένα και διακριτά προς τις διατάξεις του άρθρου 10 της Οδηγίας 680/16, αντίστοιχα προς τη θεσμοθέτηση των εξειδικευμένων ειδικών ανακριτικών τεχνικών [πρβλ. Recommendation CM/Rec (2017)6 of the Committee of Ministers to member States on "special investigation techniques" in relation to serious crimes including acts of terrorism], όπως τις γνωρίζουμε στο εθνικό δίκαιο από τις διατάξεις του άρθρου 254 επ. ΚΠΔ, την περίπτωση της χρήσης των ανωτέρω συστημάτων όταν λειτουργούν **σε πραγματικό χρόνο** και σε **δημόσια προσβάσιμους χώρους** κρίνοντας ότι όταν συντρέχουν οι δυο (2) αυτές συνθήκες σωρευτικά απαιτούνται ειδικότερες ρυθμίσεις για τη προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων των οποίων τα βιομετρικά δεδομένα υποβάλλονται σε επεξεργασία με σκοπό την ταυτοποίηση μετά από ειδική επεξεργασία δοθέντος ότι η συγκεκριμένη επέμβαση είναι ιδιαιτέρως επαχθής και διεισδυτική.

Επομένως, η επεξεργασία βιομετρικών δεδομένων δια της χρήσης απομακρυσμένων συστημάτων βιομετρικής ταυτοποίησης σε πραγματικό χρόνο σε δημόσια προσβάσιμους χώρους για σκοπούς επιβολής του νόμου επιτρέπεται με βάση το σχ. Καν. ΤΝ εφόσον:

i. προβλέπεται ρητά, εναργώς και αναλυτικά από εθνικό νόμο,

ii. ο οποίος περιλαμβάνει τις απαιτούμενες ουσιαστικές και διαδικαστικές εγγυήσεις του σχ Κ ΤΝ,

iii. περιλαμβανομένης της προηγούμενης αδειοδότησης για τη χρήση του συστήματος από ανεξάρτητη και αμερόληπτη δικαστική ή διοικητική αρχή

iv. έτι περιλαμβανομένων αναλυτικών και εναργών διατάξεων που ρυθμίζουν τις προϋποθέσεις εφαρμογής του άρθρου 10 Οδηγίας 680/16 (βλ. αιτ. σκ. 33, 35 και 37) στο μέτρο που συμπληρώνουν τις διατάξεις του σχ. Κ ΤΝ και

v. εφόσον πληρούνται οι απαιτούμενες προϋποθέσεις/απαιτήσεις/υποχρεώσεις που περιγράφονται στο α' στάδιο εφαρμογής του σχ Κ ΤΝ που απευθύνονται κυρίως στους προμηθευτές του συστήματος και έχει εγκριθεί η χρήση του συστήματος και έχει καταχωρηθεί στη βάση δεδομένων της Ε.Ε. του άρθρου 60 σχ. Κ ΤΝ.

Δ. Η λειτουργία συστημάτων απομακρυσμένης βιομετρικής ταυτοποίησης σε πραγματικό χρόνο σε δημόσια προσβάσιμους χώρους για σκοπούς επιβολής του νόμου de lege lata.

1. Από τις διατάξεις του άρθρου 10 Οδηγίας 680/16 προκύπτουν οι προϋποθέσεις επεξεργασίας **των βιομετρικών δεδομένων για την αποκλειστική ταυτοποίηση ενός φυσικού προσώπου** μόνο όταν είναι απολύτως αναγκαία με την επιφύλαξη των κατάλληλων διασφαλίσεων για τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων και εφόσον επιτρέπονται από το δίκαιο των κρατών μελών της Ε.Ε. ή επιβάλλονται για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου ή η επεξεργασία αυτή αφορά σε δεδομένα τα οποία έχουν προδήλως δημοσιοποιηθεί από το υποκείμενο των δεδομένων.

Η διάταξη αυτή ενσωματώθηκε στην εθνική νομοθεσία με το άρθρο 46 του ν. 4624/2019. Από την ανάγνωση της διάταξης του άρθρου 46 ν. 4624/2019 που τιτλοφορείται «*επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα*», προκύπτει ότι γίνεται αναφορά εν γένει στην επεξεργασία «*ειδικών κατηγοριών δεδομένων*», η έννοια των οποίων παρέχεται από τις διατάξεις του άρθρου 44 περ. ιδ' καθώς και ιβ' για τα βιομετρικά δεδομένα, χωρίς όμως να προσδιορίζεται ρητά η υπό

εξέταση **επεξεργασία των βιομετρικών δεδομένων <u>για την αποκλειστική ταυτοποίηση ενός φυσικού προσώπου.</u>** Η επιλογή αυτή υπήρξε ορθή δοθέντος ότι εναπόκειται στον εθνικό νομοθέτη ανάλογα προς το εκάστοτε ειδικότερο ζήτημα (ιδίως τομεακού δικαίου), όπως εν προκειμένω, να προβεί σε ειδικότερες νομοθετικές προβλέψεις, όπως εξάλλου προτείνεται και με το σχ. Καν. ΤΝ. Ούτως ή άλλως, η διάταξη του άρθρου 46 ν. 4624/2019 δεν φαίνεται να παρέχει τη νομική βάση (εξάλλου ο εθνικός νομοθέτης παρέλειψε να ενσωματώσει το άρθρο 8 της Οδηγίας 680/16), άλλα ούτε τις ουσιαστικές και διαδικαστικές προϋποθέσεις για την ad hoc επεξεργασία σε πραγματικό χρόνο βιομετρικών δεδομένων για την ταυτοποίηση φυσικού προσώπου σε δημόσιους χώρους από αρμόδιες αρχές για τη δίωξη του εγκλήματος. Η εν λόγω διάταξη φαίνεται να λειτουργεί περισσότερο ως διάταξη «ομπρέλα», όχι άμεσης εφαρμογής, αλλά παραπομπής σε αυτήν (δοθέντος ότι περιλαμβάνει μια σειρά εγγυήσεων) από έτερη ειδικότερη διάταξη, όπως π.χ. των οικείων διατάξεων του Π.Δ. 75/2020, κατά το πνεύμα και του σχ. Κανονισμού ΤΝ.

Επομένως, η διάταξη του άρθρου 46 ν. 4624/2019 φαίνεται κατ' αρχήν ότι δεν επαρκεί για την απευθείας – άμεση εγκατάσταση και λειτουργία συστημάτων ΤΝ απομακρυσμένης βιομετρικής ταυτοποίησης σε πραγματικό χρόνο σε δημόσια προσβάσιμους χώρους ακόμη και στην παρούσα περίσταση κατά την οποία δεν υφίσταται Κανονισμός ΤΝ, καθώς μια τέτοια εθνική διάταξη θα πρέπει να παρέχει τα εχέγγυα του «*ποιοτικού*» και «*εναργούς*» νόμου που απαιτείται από τη νομολογία του ΕΔΔΑ και του Δ.Ε.Ε. κατ' εφαρμογή των διατάξεων του ΧΘΔΕΕ και ΕΣΔΑ.

Πάντως, η Αρχή Προστασίας Δεδομένων (ΑΠΔ) με την υπ' αρ. 3/2020 Γνωμοδότηση επί του σχεδίου Π.Δ. υπ' αρ. 75/2020 (ΦΕΚ Α'173/10.9.2020) «*Χρήση συστημάτων επιτήρησης με λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους* χώρους», επεσήμανε ότι «*τυχόν εγκατάσταση και χρήση πρόσθετου εξοπλισμού στην οποία περιλαμβάνεται και λογισμικό που αποσκοπεί στην περαιτέρω επεξεργασία της εικόνας και του ήχου, ενδέχεται να αφορά διαφορετική, αυτοτελή και διακριτή επεξεργασία σε σχέση με την αρχική συλλογή, αποθήκευση και διατήρηση του υλικού, όπως π.χ. σε περίπτωση χρήσης* ***λογισμικού αναγνώρισης και ταυτοποίησης προσώπου (facial recognition) ή και ενδεχομένως σε περίπτωση χρήσης τεχνητής νοημοσύνης.*** *Σε εκείνη την περίπτωση θα πρέπει να τηρούνται επίσης όλες οι αρχές επεξεργασίας και νομιμότητάς καθώς και οι απαιτήσεις σεβασμού των υποχρεώσεων που απορρέουν από τις διατάξεις των άρθρων 7, 8. 52 ΧΘΔΕΕ και 8 ΕΣΔΑ*», πρωτίστως δηλαδή η αναλυτική και εναργής πρόβλεψη των ουσιαστικών και διαδικαστικών εγγυήσεων σε ειδική εθνική διάταξη, ενώ συνεχίζοντας κατωτέρω, προσέθεσε ότι θα πρέπει να περιλαμβάνεται στις οικείες διατάξεις του Π.Δ. νομοθετική πρόβλεψη ορισμού ενός εκπροσώπου ανεξάρτητης και αμερόληπτης αρχής (δικαστικής ή διοικητικής) με αδειοδοτικό και εγγυητικό ρόλο, ιδίως στις περιπτώσεις στόχευσης συγκεκριμένου προσώπου. Οι ανωτέρω επισημάνσεις της ΑΠΔ βασίσθηκαν ιδίως στην πάγια νομολογία του Δικαστηρίου της Ε.Ε. αλλά και συναφή νομολογία του ΕΔΔΑ, την οποία προφανώς ακολουθεί και το σχέδιο Καν. ΤΝ.

Τέλος, θα πρέπει να επισημανθεί ότι η σχέση της νομοθεσίας που αφορά την εγκατάσταση και λειτουργία τέτοιων συστημάτων τεχνητής νοημοσύνης που συνίσταται στην επεξεργασία βιομετρικών δεδομένων σε πραγματικό χρόνο σε δημόσια προσβάσιμους χώρους για την διακρίβωση εγκλημάτων, θα πρέπει να εξετασθεί και στο ειδικότερο πλαίσιο της ειδικής εθνικής ποινικοδικονομικής νομοθεσίας για την διενέργεια ειδικών ανακριτικών πράξεων σε βάρος στοχευμένων – συγκεκριμένων φυσικών προσώπων σε αντιδιαστολή προς την σκόπευση του σχ. Καν. ΤΝ που αφορά την ταυτοποίηση προσώπων **χωρίς να γνωρίζει εκ προοιμίου** ο

χειριστής του συστήματος εάν το υπό διερεύνηση πρόσωπο θα είναι παρόν και δύναται να ταυτοποιηθεί κατά τη λειτουργία του συστήματος.