# τεχνολογίες διαχείρισης πλήθους

## Μία ακόμα πρόκληση ιδιωτικότητας στη ψηφιακή εποχή!

Ιωσήφ Αβραμίδης, Δικηγόρος

Διευθυντής Προστασίας Δεδομένων & Συμμόρφωσης

Διεθνής Αερολιμένας Αθηνών Α.Ε.

# Βασικές τεχνολογίες σε εφαρμογή

**Συστήματα μέτρησης και ανίχνευσης ταχύτητας/πυκνότητας** CCTV & CCTV + AI

**GPS Apps/Trackers**

**WiFi/Bluetooth Tracking**

**RFID**

**LiDAR (Light Detection And Ranging)**

**Συνδυασμός αυτών**

# Συστήματα μέτρησης και ανίχνευσης ταχύτητας/πυκνότητας με τη χρήση κάμερας CCTV/CCTV+AI (Video Analytics)

| Χαρακτηριστικά: | Εφαρμογές: | Ζητήματα Προστασίας Ιδιωτικότητας |
|---|---|---|
| ➢ Συνδυασμός μιας κάμερας (φακού) και ενός συνόλου οπτικών αλγόριθμων<br>➢ Σε πραγματικό χρόνο, η ροή βίντεο της κάμερας αναλύεται μέσω αυτών των αλγορίθμων στην πηγή<br>➢ Το αποτέλεσμα της ανάλυσης μεταδίδεται (ασύρματα, ή ενσύρματα) στο σύστημα διαχείρισης (dashboard)<br>➢ Σε τακτά χρονικά διαστήματα (π.χ. 1 λεπτού) αναλύεται η ροή των προσώπων, ο μέσος αριθμός κινούμενων προσώπων στο οπτικό πεδίο, ή η ταχύτητά τους στο οπτικό πεδίο. Η ίδια η ροή βίντεο πρέπει να διαγράφεται αμέσως μόλις αναλυθεί και δεν αποθηκεύεται στη μονάδα ανάλυσης στην πηγή ούτε σε καμία βάση δεδομένων του συστήματος<br>➢ Οι αλγόριθμοι μετατρέπουν επίσης τις συντεταγμένες των υποκειμένων που καταγράφονται από συντεταγμένες pixel σε πραγματικές συντεταγμένες απόστασης σε μέτρα κλπ. Ακολουθώντας την ακολουθία των συντεταγμένων κατά τη κίνηση καταγράφει κανείς και τη πορεία κάθε εποπτευόμενου προσώπου,<br>➢ Με τη χρήση κατάλληλης ψηφιακής επεξεργασίας είναι δυνατή η παραμόρφωση της εικόνας και η προβολή προσώπων σε μη αναγνωρίσιμη μορφή | ➢ Εποπτεία πυκνότητας/κίνησης/ροών/ταχύτητας, αλλά και συναισθημάτων προσώπων στον εποπτευόμενο χώρο, όπως σε εμπορικά κέντρα, επιβατικούς σταθμούς, εξωτερικούς χώρους (δρόμους, πλατείες, αθλητικές εγκαταστάσεις κ. ά.)<br>➢ Προσαρμογή υπηρεσιών, διαχείριση προσωπικού εξυπηρέτησης κοινού, διεύθυνση εγκαταστάσεων βάσει πυκνότητας και ροής κοινού – βελτιστοποίηση κόστους σχετικών συμβάσεων<br>➢ Ανάπτυξη τεχνικών δυνατοτήτων εκμάθησης υποδομών «smart city» κι αυτόνομης κίνησης οχημάτων, (αναγνώριση περιβάλλοντος, προσώπων, ανάπτυξη «αντίληψης» συστημάτων)<br>➢ Στοχευμένη προώθηση και προσαρμογή προσφερόμενων προϊόντων βάσει της κίνησης κοινού<br>➢ Παρακολούθηση συμπεριφοράς των πελατών και της αλληλεπίδρασής τους με προϊόντα ή προωθητικές ενέργειες<br>➢ Αναγνώριση προσώπου ή κατ' επιλογή απόκρυψη προσώπου (real time masking) | Τεχνικά:<br>➢ Κρίσιμη παράμετρος η επεξεργασία όχι μόνο των πρωτογενών δεδομένων (εικόνα/κίνηση), αλλά και των μεταδεδομένων τόσο σε αδράνεια (στο σύστημα διαχείρισης και τη βάση δεδομένων, όσο και σε μετάδοση (κατά την εκπομπή από τα σημεία συλλογής)<br>➢ Περίοδος διακράτησης (retention)<br>➢ Ψηφιακή επεξεργασία (αλγόριθμοι) με σκοπό την κρυπτογράφηση και την ψευδωνυμοποίηση, η οποία, ωστόσο δεν αποκλείει τη δυνατότητα αντιστροφής κρυπτογράφησης<br><br>Κανονιστικά:<br>➢ Βιομετρικά δεδομένα (άρθρο 9 ΓΚΠΔ),<br>➢ Δυνατότητα άρσης απόκρυψης προσώπου (real time masking)<br>➢ Δυνητική παρακολούθηση εργαζομένων<br>➢ Έλεγχος νομιμότητας σκοπού επεξεργασίας |
| | | |
| | | |

# Αισθητήρες Wi-Fi & Bluetooth

| Χαρακτηριστικά: | Εφαρμογές: | Ζητήματα Προστασίας Ιδιωτικότητας |
|---|---|---|
| ➢ Κάθε συσκευή με δυνατότητα Wi-Fi/bluetooth, όπως τα smartphone, μεταδίδει μηνύματα για να προσδιορίσει τον πλησιέστερο πύργο κινητής τηλεφωνίας ή/και να επικοινωνεί με άλλες συσκευές.<br>➢ Αυτά τα μηνύματα περιέχουν, μεταξύ άλλων, πληροφορίες που σχετίζονται με την αναγνώριση της συσκευής με δυνατότητα Wi-Fi που στέλνει το μήνυμα και την ισχύ του σήματος που μεταδίδεται από τη συσκευή.<br>➢ Χρησιμοποιώντας αυτές τις πληροφορίες αναγνώρισης μπορεί κανείς να προσδιορίσει πόσες μοναδικές συσκευές υπάρχουν σε μια συγκεκριμένη τοποθεσία.<br>➢ Επιπλέον, όταν συγκρίνονται οι λίστες μοναδικών συσκευών περισσότερων τοποθεσιών, μπορεί να καθορίσει πόσες συσκευές μετακινήθηκαν από τη μια τοποθεσία στην άλλη.<br>➢ Ο αισθητήρας Wi-Fi/Bluetooth ανιχνεύει την επικοινωνία αυτών των συσκευών με δυνατότητα Wi-Fi και Bluetooth με τον πλησιέστερο πύργο κινητής τηλεφωνίας ή δρομολογητή Wi-Fi και φιλτράρει τις μοναδικές διευθύνσεις ελέγχου πρόσβασης πολυμέσων (MAC) αυτών των κινητών συσκευών.<br>➢ Παρακολούθηση της θέσης/κίνησης του κατόχου της κινητής συσκευής πραγματοποιείται και με τη μέτρηση της ισχύος του σήματος WiFi που εκπέμπει το access point προς την λαμβάνουσα συσκευή.<br>➢ Η διεύθυνση MAC, η οποία αποτελεί μέρος αυτού του μηνύματος, έχει κατηγοριοποιηθεί ως προσωπικό δεδομένο, (WP29: Opinion 247/4.4.2017) καθώς μπορεί να χρησιμοποιηθεί για τον προσδιορισμό μιας συγκεκριμένης συσκευής με δυνατότητα Wi-Fi που ανήκει σε ένα συγκεκριμένο άτομο. | ➢ **Λιανικό εμπόριο**: Παρακολούθηση συμπεριφοράς των πελατών και τις αλληλεπιδράσεις προϊόντων,<br>➢ **Έξυπνες πόλεις:** Άντληση δεδομένων και ειδοποιήσεων για πεζούς, οχήματα κλπ. και πληροφορίες για τη χρήση του δημόσιου χώρου για τη βελτιστοποίηση των δημόσιων υπηρεσιών.<br>➢ **Μεταφορές:** Παρέχει ειδοποιήσεις πληρότητας οχήματος, χρήσης σταθμού και κινδύνων σε πραγματικό χρόνο,<br>➢ **Αεροδρόμια:** Παρακολούθηση ροής και πυκνότητας κοινού σε αεροσταθμούς, εμπορικά κέντρα, χώρους υγιεινής, και άλλες κοινόχρηστες υποδομές, καλύτερη διαχείριση τεχνικών κι ανθρώπινων πόρων, βελτιστοποίηση εμπειρίας κι ασφάλειας στη διαχείριση των υποδομών<br>➢ Η τρισδιάστατη σάρωση της υποδομής εντοπίζει ελαττώματα, εμπόδια και φύλλωμα για την αποφυγή ζημιών ή ζητημάτων ασφάλειας. | **Τεχνικά:**<br>➢ Κρίσιμη παράμετρος η επεξεργασία τόσο των πρωτογενών δεδομένων (Διεύθυνση MAC/Bluetooth/I.P), αλλά και των μεταδεδομένων τόσο σε αδράνεια (στο σύστημα διαχείρισης και τη βάση δεδομένων, όσο και σε μετάδοση (κατά την εκπομπή από τα σημεία συλλογής)<br>➢ Ψηφιακή επεξεργασία (αλγόριθμοι) με σκοπό την κρυπτογράφηση και την **ψευδωνυμοποίηση /** ανωνυμοποίηση, η οποία, ωστόσο δεν αποκλείει τη δυνατότητα αντιστροφής κρυπτογράφησης<br>➢ Περίοδος διακράτησης δεδομένων (retention)<br><br>**Κανονιστικά:**<br>➢ Διαφανής ενημέρωση υποκειμένων<br>➢ Συγκατάθεση στην επεξεργασία των δεδομένων<br>➢ Έλεγχος υποβολής των δεδομένων και σε παράλληλη επεξεργασία σε συνδυασμό (π.χ. CCTV, GPS)<br>➢ Δυνητική παρακολούθηση εργαζομένων (μέσω της αναγνώρισης και καταχώρησης των διευθύνσεων MAC των συσκευών τους) |
| | | |
| | | |

# Εφαρμογές Κινητών και GPS trackers

| Χαρακτηριστικά: | Εφαρμογές: | Ζητήματα Προστασίας Ιδιωτικότητας |
|---|---|---|
| ➢ Η καταγραφή ίχνους GPS πραγματοποιείται από παρόχους/εφαρμογές που έχουν ζητήσει και λάβει ρητά άδεια από τους χρήστες τους να διανείμουν τα δεδομένα (ανώνυμα) σε τρίτους, σύμφωνα με την πολιτική απορρήτου της εφαρμογής.<br>➢ Τα δεδομένα αυτά κατακερματίζονται, αποκόπτονται και κατακερματίζονται εκ νέου πριν αποθηκευτούν στη βάση δεδομένων για τους σκοπούς της διαχείρισης πλήθους.<br>➢ Σύμφωνα με τις τεχνικές που ακολουθούνται στη πλειονότητά τους, τα ίχνη GPS μεμονωμένων smartphone χρησιμοποιούνται μόνο στην ανάλυση, αλλά ποτέ δεν απεικονίζονται με τρόπο που να μπορεί να εντοπιστεί ένα κομμάτι GPS σε ένα συγκεκριμένο άτομο.<br>➢ Γενικά, απεικονίζονται μόνο συνολικά δεδομένα (aggregated data), προσδιορίζοντας π.χ. τον αριθμό πεζών σε μια πλατεία, ή τη μέση ταχύτητα βάδισης. Μετά από αναλύσεις, όλα τα ακατέργαστα ίχνη GPS, συμπεριλαμβανομένων των κατακερματισμένων πληροφοριών ταυτοποίησής τους, διαγράφονται. Μόνο ανώνυμα δεδομένα GPS αποθηκεύονται μακροπρόθεσμα. Η ακριβής διαδικασία που χρησιμοποιείται για την περαιτέρω ανωνυμοποίηση του GPS εξαρτάται από το πλαίσιο στο οποίο καταγράφηκαν τα δεδομένα GPS. | ➢ **Crowdmapping:** Καθορισμός θέσης και κίνησης υποκειμένου – κατόχου κινητής συσκευής σε εγκαταστάσεις ή δημόσιους υπαίθριους χώρους (σε συνδυασμό κυρίως με Wi-Fi tracking)<br>➢ **Προώθηση Πωλήσεων- Marketing:** Virtual tour σε εμπορικά κέντρα – υπόδειξη ευκαιριών ανάλογα με τα σημεία διέλευσης | **Τεχνικά:**<br>➢ Κρίσιμη παράμετρος η επεξεργασία όχι μόνο των πρωτογενών δεδομένων γεωεντοπισμού, αλλά και των μεταδεδομένων τόσο σε αδράνεια (στο σύστημα διαχείρισης και τη βάση δεδομένων, όσο και σε μετάδοση (κατά την εκπομπή από τα σημεία συλλογής)<br>➢ Περίοδος διακράτησης δεδομένων (retention)<br>➢ Ψηφιακή επεξεργασία (αλγόριθμοι) με σκοπό την κρυπτογράφηση και την ανωνυμοποίηση, η οποία, ωστόσο δεν αποκλείει τη δυνατότητα αντιστροφής κρυπτογράφησης<br>**Κανονιστικά:**<br>➢ Διαφανής ενημέρωση υποκειμένων<br>➢ Συγκατάθεση στην επεξεργασία των δεδομένων<br>➢ Έλεγχος υποβολής των δεδομένων γεωεντοπισμού και σε παράλληλη επεξεργασία σε συνδυασμό (π.χ. CCTV, WiFi tracking)<br>➢ Δυνητική παρακολούθηση εργαζομένων |
| | | |
| | | |

# LiDAR (Light Detection And Ranging)

| Χαρακτηριστικά: | Εφαρμογές: | Ζητήματα Προστασίας Ιδιωτικότητας |
|---|---|---|
| ➢ Ο ενεργητικός αυτός δέκτης εκπέμπει μερικές χιλιάδες παλμούς laser το δευτερόλεπτο.<br>➢ Κάθε παλμός ανακλάται στο αντικείμενο στόχευσης (π.χ. φυσικά πρόσωπα, κλπ.) κι επιστρέφει στον δέκτη, ενώ ο χρόνος της διαδρομής μετράται με χρονόμετρο ακριβείας και μετατρέπεται σε απόσταση.<br>➢ Αυτή η απόσταση καθώς και η θέση και ο προσανατολισμός του πομπού χρησιμοποιούνται για τον προσδιορισμό των συντεταγμένων του στοχευμένου αντικειμένου.<br>➢ Το LiDAR δεν χρησιμοποιεί φυσικό φως και δεν συλλαμβάνει προσωπικά αναγνωρίσιμες πληροφορίες (PII) σχετικά με την ταυτότητα των ατόμων στο οπτικό του πεδίο<br>➢ Τα στοχευόμενα πρόσωπα απεικονίζονται συνήθως με «τελείες» | ➢ **Εποπτεία πυκνότητας/κίνησης/ροών/ταχύτητας προσώπων στον εποπτευόμενο χώρο, όπως σε εμπορικά κέντρα, επιβατικούς σταθμούς, εξωτερικούς χώρους (δρόμους, πλατείες, αθλητικές εγκαταστάσεις κ. ά.)**<br>➢ **Προσαρμογή υπηρεσιών, διαχείριση προσωπικού εξυπηρέτησης κοινού, διεύθυνση εγκαταστάσεων σε χώρους υγιεινής, και άλλες κοινόχρηστες υποδομές βάσει πυκνότητας και ροής κοινού – βελτιστοποίηση κόστους σχετικών συμβάσεων**<br>➢ **Ανάπτυξη τεχνικών δυνατοτήτων εκμάθησης υποδομών «smart city» κι αυτόνομης κίνησης οχημάτων, (αναγνώριση περιβάλλοντος, προσώπων, ανάπτυξη «αντίληψης» συστημάτων)**<br>➢ **Στοχευμένη προώθηση και προσαρμογή προσφερόμενων προϊόντων βάσει της κίνησης κοινού**<br>➢ Παρέχει ειδοποιήσεις πληρότητας οχήματος, χρήσης σταθμού και κινδύνων σε πραγματικό χρόνο,<br>➢ Η τρισδιάστατη σάρωση της υποδομής εντοπίζει ελαττώματα, εμπόδια και επικίνδυνα αντικείμενα, για την αποφυγή ζημιών ή ζητημάτων ασφάλειας. | **Τεχνικά:**<br>➢ Αν και σύμφωνα με τις κοινά διαθέσιμες τεχνικές προδιαγραφές, δηλώνεται ότι δεν χρησιμοποιούνται κάμερες και δεν λαμβάνονται εικόνες ή βίντεο από τους εποπτευόμενους χώρους, δεν μπορεί κανείς ν' αποκλείσει τυχόν δυνητική ψηφιακή επεξεργασία, η οποία σε συνδυασμό και με άλλες μεθόδους και τεχνολογίες διαχείρισης πλήθους (π.χ. CCTV, WiFi tracking, crowdmapping) θα μπορούσαν δυνητικά να προσδιορίσουν υποκείμενα και τη κίνησή τους στον εποπτευόμενο χώρο<br>**Κανονιστικά:**<br>➢ Ανάλογα με την υλοποίηση της υπηρεσίας και τις τεχνικές παραμέτρους αυτής, ενδέχεται να παρουσιάζει ενδιαφέρον υπό το πλέγμα των διατάξεων προστασίας δεδομένων προσωπικού χαρακτήρα |
| | | |
| | | |

# Κάρτες και πομποδέκτες RFID

| Χαρακτηριστικά: | Εφαρμογές: | Ζητήματα Προστασίας Ιδιωτικότητας |
|---|---|---|
| ➢ Σε μια δεδομένη τοποθεσία δίνεται σε πρόσωπα που συμμετέχουν μια κάρτα RFID.<br>➢ Τα πρόσωπα αυτά καλούνται να συνεχίσουν τις δραστηριότητές τους, ενώ φέρουν την ετικέτα RFID για ορισμένο χρονικό διάστημα.<br>➢ Κατά τη διάρκεια αυτής της περιόδου, στρατηγικά τοποθετημένοι αισθητήρες RFID μπορούν να αντιληφθούν την παρουσία της ετικέτας RFID όποτε βρίσκεται κοντά της.<br>➢ Οι χρονικές σημάνσεις και οι πληροφορίες αναγνώρισης του ολοκληρωμένου δικτύου αισθητήρων RFID μπορούν να χρησιμοποιηθούν για την παρακολούθηση των κινήσεων των προσώπων που περπατούν με μια ετικέτα.<br>➢ Με την απόρριψη της κάρτας από τον κάτοχο οι αισθητήρες RFID δεν μπορούν να παρακολουθήσουν τις κινήσεις του ατόμου. | ➢ Ανάλογες με τις άλλες μεθόδους | **Κανονιστικά:**<br><br>Ένα κύριο πλεονέκτημα της παρακολούθησης ετικετών RFID έναντι της παρακολούθησης συσκευών με δυνατότητα Wi-Fi είναι ότι το άτομο που φέρει την ετικέτα, παραμένει ανώνυμο (εκτός αν συμμετέχει επώνυμα κι έχει δώσει τη συγκατάθεσή του) κι ελέγχει πλήρως τα δεδομένα κίνησής του.<br><br>Επιλέγει πότε θα τη κρατά και πότε θα την πετάξει. Κατά συνέπεια, μόνο οι πρόθυμοι πεζοί παρέχουν τις πληροφορίες που θέλουν να παράσχουν και οι απρόθυμοι πεζοί δεν μπορούν να εντοπιστούν. |
| | | |
| | | |

# MAC Address: Πόσο πραγματικά προσβάλει την ιδιωτικότητα μας; Λόγος και Αντίλογος

- **Το νομικό/κανονιστικό ζήτημα:**

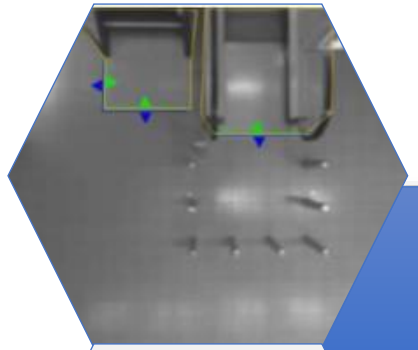
1. Η διεύθυνση MAC μιας συσκευής συνδεδεμένης στο διαδίκτυο, αποτελεί online identifier και εφόσον καταγράφεται κατά τη μετακίνηση της συσκευής σε εποπτευόμενους χώρους, σε συνδυασμό και με άλλες τεχνολογίες, με τη κατάλληλη ψηφιακή επεξεργασία, σε συνδυασμό και με άλλες μεθόδους και τεχνολογίες διαχείρισης πλήθους (π.χ. CCTV, LIDAR, στοιχεία ISP) θα μπορούσε δυνητικά να προσδιορίσει τους κατόχους των συσκευών και τη κίνησή τους στους εποπτευόμενους χώρους
2. Η δυνητική προσβολή της ιδιωτικότητας του κατόχου εντός του δικτύου WiFi, στο οποίο κινείται, δεν αντιμετωπίζεται αποτελεσματικά εν᾽ όψει όλων των διαθέσιμων τεχνολογιών
3. Κρίσιμα παραμένουν τα ζητήματα της νομικής βάσης, του σκοπού και της αναλογικότητας της επεξεργασίας

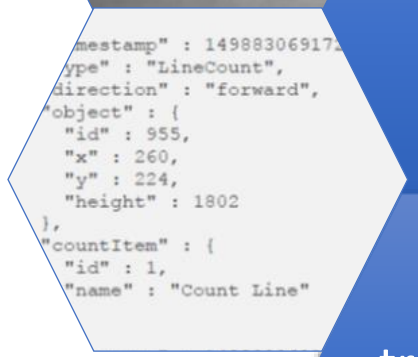
- **Τεχνική Ανάλυση:**

1. Η διεύθυνση MAC μιας συσκευής χρησιμοποιείται μόνο κατά την αρχική σύνδεση της συσκευής με ένα δίκτυο WiFi για να γίνει η αρχική σύνδεση στο σημείο πρόσβασης access point και δεν μεταδίδεται πέραν αυτού π.χ. στο διαδίκτυο. Με αυτήν προσδιορίζεται μόνο ο κατασκευαστής και ο τύπος του modem της συσκευής. Δεν προσδιορίζουν έναν συγκεκριμένο υπολογιστή από μόνοι τους, ούτε προσδιορίζουν έναν συγκεκριμένο χρήστη.
2. Με το κατακερματισμό σε τακτικά και σύντομα χρονικά διαστήματα (hashing) των διευθύνσεων MAC που συλλέγονται δίνεται η δυνατότητα απόκρυψης της πραγματικής διεύθυνσης σε ένα δεδομένο χώρο και χρόνο, ενώ με τη μετάδοση της λίστας των συντομευμένων διευθύνσεων στη βάση δεδομένων μέσω ασφαλούς σύνδεσης διασφαλίζεται η κρυπτογράφησή τους
3. Κάποιοι κατασκευαστές smartphone (π.χ. από το λειτουργικό IOS 14, Android 10 και μετά) κλπ. δίνουν τη δυνατότητα αλλαγής του MAC ID της συσκευής με τυχαία σειρά κατά την κάλυψη από ένα δίκτυο WiFi σε άλλο, διακόπτωντας με το τρόπο αυτό την ακολουθία ανίχνευσης

- **Τεχνική λύση**

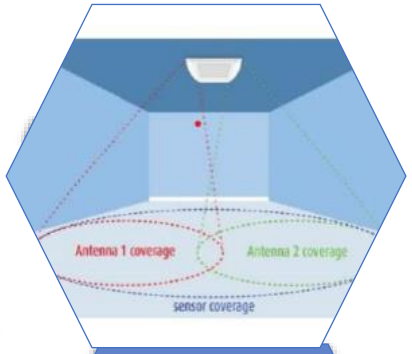
Ανωνυμοποίηση αυτών των δεδομένων, με κατακερματισμό, όσο το δυνατόν συντομότερα από την εγγραφή τους, ώστε η βάση δεδομένων να περιέχει μια λίστα κατακερματισμένων αναγνωριστικών που μπορούν να χρησιμοποιηθούν για την ανάλυση των κινήσεων του πλήθους, αλλά όχι για την αναγνώριση μιας συγκεκριμένης κινητής συσκευής ή ενός συγκεκριμένου ατόμου.





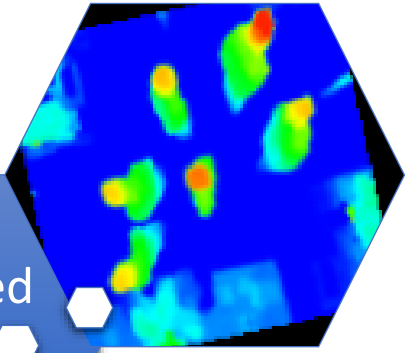

LiDAR

LiDAR transmission data




Wi-Fi tracking


CCTV/A.I.



Anonymized CCTV footage

# Ολλανδική Αρχή ΠΔΠΧ κατά ΔήμουEnschede

- Το 2021 η Ολλανδική Αρχή Προστασίας Δεδομένων (DPA) επέβαλε πρόστιμο 600.000 ευρώ στον δήμο του Enschede για χρήση της παρακολούθησης Wi-Fi στο κέντρο της πόλης με τρόπο που απαγορεύεται. Η παρακολούθηση Wi-Fi κατέστησε δυνατή την τη μέτρηση του συνωστισμού του δρόμου μετρώντας πόσα τηλέφωνα βρίσκονται κοντά σε έναν αισθητήρα σε μια συγκεκριμένη στιγμή. Εάν, ωστόσο, παρακολουθείται για μεγαλύτερο χρονικό διάστημα ποιο τηλέφωνο περνάει κοντά σε ποιον αισθητήρα, αυτή η «μέτρηση» γίνεται παρακολούθηση αγοραστών και ατόμων που ζουν ή εργάζονται στο κέντρο της πόλης.
- *«Το απόρρητο των ανθρώπων πρέπει να προηγείται»*
- *«Αν οι άνθρωποι μπορούν να παρακολουθούνται μέσω των τηλεφώνων τους, αυτό είναι κακή κατάσταση»*, δήλωσε η αναπληρώτρια πρόεδρος του DPA Monique Verdier. *«Καθένας έχει το δικαίωμα να κάνει τις δουλειές του έξω ελεύθερα και χωρίς να τον κατασκοπεύουν. Χωρίς η κυβέρνηση ή οποιοδήποτε άλλο κόμμα να μπορεί να σας παρακολουθεί ή να παρακολουθεί τι κάνετε. Αυτό είναι μέρος της ελεύθερης και ανοιχτής κοινωνίας μας»*.
- Η χρήση της παρακολούθησης Wi-Fi υπόκειται σε αυστηρούς όρους και στις περισσότερες περιπτώσεις απαγορεύεται, είπε η η αναπληρώτρια πρόεδρος του DPA κ. Monique Verdier. *«Επειδή αυτή η τεχνολογία μπορεί να επηρεάσει τόσο βαθιά την καθημερινή ζωή των ανθρώπων, πρέπει να χρησιμοποιείται μόνο σε εξαιρετικές περιπτώσεις»*
- https://edpb.europa.eu/news/national-news/2021/dutch-dpa-fines-municipality-wi-fi-tracking_en

# Συμπεράσματα:

- Η τεχνολογική, αλλά και οικονομική πίεση για την μεγιστοποίηση της χρήσης δεδομένων που σχετίζονται με τον πολίτη και τον καταναλωτή είναι πραγματικά μεγάλη και ωθεί στην υιοθέτηση εφαρμογών περαιτέρω ανάλυσης προσωπικών δεδομένων
- Επιπλέον η τεχνητή νοημοσύνη και το διαδίκτυο των πραγμάτων, όπως υλοποιούνται σε «έξυπνες συσκευές» οδηγούν στην απόλυτη ψηφιακή εμπειρία
- Στη πορεία αυτή κρίσιμη παράμετρος είναι η επεξεργασία, όχι μόνο των πρωτογενών προσωπικών δεδομένων (εικόνα/κίνηση), αλλά και των μεταδεδομένων τόσο σε αδράνεια (στο σύστημα διαχείρισης και τη βάση δεδομένων), όσο και σε μετάδοση (κατά την εκπομπή από τα σημεία συλλογής)
- Ως αντίβαρο στις επιφυλάξεις των Ρυθμιστικών Αρχών, η Αγορά προσφέρει ψηφιακές λύσεις κατακερματισμού (hashing), ανωνυμοποίησης και κρυπτογράφησης δεδομένων, οι οποίες ωστόσο παραμένουν εκτεθειμένες σε αντιστροφή προγραμματισμού και δυνητική άρση της προστασίας των υποκειμένων ιδιαίτερα, σε συνδυασμό με άλλες τεχνολογίες επεξεργασίας
- Το ζήτημα αυτό περιπλέκεται με δεδομένη την εμπλοκή σε αυτές τις εφαρμογές περισσότερων Εκτελούντων την Επεξεργασία, με εφαρμογές και βάσεις δεδομένων στο cloud και πιθανόν εκτός Ευρωπαϊκού Οικονομικού Χώρου
- Η επιβολή των Αρχών του ΓΚΠΔ, αλλά και η αυτορρύθμιση της αγοράς στην ανάπτυξη αλγορίθμων, οι οποίοι δεν θα παραβιάζουν τις ατομικές ελευθερίες και τα ατομικά δικαιώματα των πολιτών, αποτελούν το μόνο εχέγγυο συνετής και ανάπτυξης των τεχνολογιών αυτών.

Ευχαριστώ για τη προσοχή σας