ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»

Ακαδημαϊκό έτος 2021-2022

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Της Συμέλας Ατσαλάκη (Α.Μ.: ΜΔΙ2105)

Crowd monitoring - Wifi tracking και ζητήματα προστασίας θεμελιωδών ελευθεριών (προσωπικών δεδομένων κ.α.)

Επιβλέπουσα:

κα Ευαγγελία (Λίλιαν) Μήτρου

Πειραιάς, Σεπτέμβριος 2023

Στους γονείς μου.

Πίνακας περιεχομένων

ΠΕΡΙΛΗΨΗ

Η παρούσα διπλωματική εργασία, ασχολείται με τις έννοιες του «crowd monitoring» (παρακαλούθηση πλήθους) και του «WiFi tracking» (παρακολούθηση μέσω WiFi), τις εκφάνσεις αυτών των μεθόδων παρακολούθησης, την εφαρμογή τους στην καθημερινή ζωή των ανθρώπων και τον τρόπο με τον οποίο λειτουργούν. Εξετάζονται διάφορες πτυχές των ως άνω μορφών παρακολούθησης σε διαφορετικούς τομείς της κοινωνίας και της καθημερινότητας, ενώ περαιτέρω παρουσιάζεται και αναλύεται η έννοια της «έξυπνης πόλης» («smart city») που έχει ραγδαία εξέλιξη τα τελευταία χρόνια, καθώς αναπτύσσεται με γρήγορους ρυθμούς. Στην εργασία, ερευνώνται και τα τεχνολογικά εργαλεία που αναπτύχθηκαν στο πλαίσιο της επείγουσας και απρόβλεπτης ανάγκης αντιμετώπισης των αρνητικών συνεπειών λόγω της εμφάνισης του κορωνοϊού covid-19, και ειδικότερα στο πλαίσιο περιορισμού της διάδοσής του και λήψης συναφών αναγκαίων μέτρων και κατά πόσο οι τεχνολογίες που αναπτύχθηκαν και τα μέτρα που εφαρμόσθηκαν με σκοπό – μεταξύ άλλων – την ψηφιακή ιχνηλάτηση επαφών και τον έλεγχο τήρησης των κανόνων που ορίσθηκαν από τις εκάστοτε κυβερνήσεις ήταν συμμορφούμενα με τις προβλέψεις της νομοθεσίας προστασίας προσωπικών δεδομένων. Η διπλωματική εργασία ερευνά τα πλεονεκτήματα των ως άνω τεχνολογιών, τους τρόπους με τους οποίους διευκολύνουν και ωφελούν τη ζωή των ανθρώπων καθώς και τα μειονεκτήματα, αδυναμίες των σχετικών συστημάτων. Παράλληλα, εξετάζεται το επίπεδο προστασίας των προσωπικών δεδομένων και της ιδιωτικότητας των ατόμων στο πλαίσιο λειτουργίας των ανωτέρω συστημάτων "crowd monitoring" και η επιτακτική ανάγκη για ιδιωτικότητα που έχει προκύψει από τη ραγδαία εξέλιξη και εφαρμογή των νέων αυτών τεχνολογιών - σχεδόν - σε όλους τους τομείς της ζωής μας. Η αξιοποίηση των υφιστάμενων νομοθετικών εργαλείων στον τομέα της προστασίας των προσωπικών δεδομένων αποτελεί θεμελιώδους σημασίας προσέγγιση για την εφαρμογή και λειτουργία των ως άνω μορφών "crowd monitoring", ενώ παράλληλα είναι εξαιρετικά σημαντική Εκκινώντας από θεμελιώδεις διατάξεις της ευρωπαϊκής έννομης τάξης, αναπτύσσεται το ζήτημα της προστασίας των προσωπικών δεδομένων των ατόμων, ως πτυχή του δικαιώματος στον ιδιωτικό βίο, υπό το πρίσμα και του Γενικού Κανονισμού Προστασίας Δεδομένων.

ABSTRACT

This dissertation deals with the concepts of "crowd monitoring" and "WiFi tracking", the aspects of these monitoring methods, their application in people's daily lives and the way they work. Various aspects of the above forms of monitoring in different areas of society and everyday life are examined, while the concept of the 'smart city', which has been rapidly developing in recent years, is further presented, and analysed. The paper also explores the technological tools developed in the context of the urgent and unforeseen need to address the negative consequences of the emergence of the covid-19 coronavirus, and in particular in the context of limiting its spread and taking the necessary measures in this regard, and whether the technologies developed and the measures implemented to - inter alia - digitally track contacts and monitor compliance with the rules laid down by the respective governments were in compliance with the provisions of the data protection legislation. The dissertation explores the advantages of the above technologies, the ways in which they facilitate and benefit people's lives as well as the disadvantages and vulnerabilities of the relevant systems. At the same time, it examines the level of protection of personal data and privacy of individuals in the context of the operation of the above "crowd monitoring" systems and the urgent need for privacy that has arisen from the rapid development and application of these new technologies - almost - in all areas of our lives. The utilisation of existing legislative instruments in the field of personal data protection is a fundamental approach for the implementation and operation of the above forms of 'crowd monitoring', while at the same time it is extremely important Starting from fundamental provisions of the European legal order, the issue of the protection of personal data of individuals, as an aspect of the right to privacy, is developed in the light of the General Data Protection Regulation.

ΕΙΣΑΓΩΓΗ

Στη σύγχρονη εποχή η τεχνολογία εξελίσσεται ταχύτατα και παίζει ιδιαίτερα καθοριστικό ρόλο στην καθημερινή ζωή των ανθρώπων. Μια από τις μεγαλύτερες αλλαγές των τελευταίων ετών είναι η εμφάνιση του Διαδικτύου των Πραγμάτων ("Internet of Things- IoT") και των έξυπνων συσκευών που αποτελούν αναπόσπαστο κομμάτι της καθημερινής ζωής. Ο ρόλος τους είναι πολλαπλός, βελτιώνουν την ποιότητα ζωής των ανθρώπων ειδικά στις μεγάλες πόλεις, διευκολύνουν την καθημερινότητά τους με διάφορες εφαρμογές και λύσεις, ενημερώνουν και ψυχαγωγούν τους ανθρώπους συλλέγοντας δεδομένα μέσω αισθητήρων, μπορούν ακόμη και να δημιουργήσουν μια ολόκληρη έξυπνη πόλη με σπουδαίες εφαρμογές όπως η έξυπνη ενέργεια, το έξυπνο κτίριο, η έξυπνη κινητικότητα, η έξυπνη υγειονομική περίθαλψη, η έξυπνη διακυβέρνηση και η έξυπνη ασφάλεια. Καθίσταται σαφές σε όλους, ότι η σύγχρονη κοινωνία βρίσκεται στο επίκεντρο της ψηφιοποίησης. Σε όλους σχεδόν τους τομείς της κοινωνικής ζωής, συναντάμε ένα ευρύ φάσμα διαφορετικών πρακτικών που υπόκεινται σε ψηφιακές αλλαγές. Οι εφαρμογές και οι "έξυπνες" συσκευές έχουν σχεδιαστεί για να αξιοποιούν αυτά τα δεδομένα με σκοπό την αυτόματη κατανόηση μοτίβων ή τον έλεγχο των βιομηχανικών διεργασιών στο πλαίσιο της Βιομηχανίας 4.0 (τέταρτη βιομηχανική επανάσταση). Αλγόριθμοι, αυτόνομες ηλεκτρικές σκούπες, αυτοκίνητα ακόμα και ανθρωποειδή ρομπότ βρίσκονται σε διαφορετικά στάδια ανάπτυξης και υλοποίησης. Το Διαδίκτυο και οι πλατφόρμες κοινωνικής δικτύωσης έχουν αλλάξει τον τρόπο με τον οποίο λαμβάνουμε πληροφορίες και βιώνουμε την ψυχαγωγία, κοινωνικοποιούμαστε, ψωνίζουμε και παρουσιάζουμε τον εαυτό μας, ενώ παράλληλα ερχόμαστε αντιμέτωποι με νέα ψηφιακά επιχειρηματικά μοντέλα που αναπτύσσονται και τα οποία βασίζονται στο "νέο χρυσό", που θεωρούνται τα δεδομένα των ατόμων. Μία από τις τεχνολογίες που έχουν αναπτυχθεί ραγδαία τα τελευταία χρόνια είναι το crowd monitoring (παρακολούθηση πλήθους) και το WiFi tracking (παρακολούθηση μέσω WiFi). Όλες αυτές οι τεχνολογικές εξελίξεις και οι πρακτικές συνδέονται προφανώς με ζητήματα προστασίας του ιδιωτικού βίου, ψηφιακής ασφάλειας, δημοκρατίας καθώς και με τον τρόπο με τον οποίο η πολιτική και η νομοθεσία αντιμετωπίζουν αυτά τα νέα φαινόμενα ψηφιοποίησης.

.

1. CROWD MONITORING (ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΠΛΗΘΟΥΣ)

1.1 Έννοια και παραδείγματα crowd monitoring

Το crowd monitoring αναφέρεται στη διαδικασία παρακολούθησης, συλλογής, ανάλυσης και ερμηνείας δεδομένων των ανθρώπων σε συγκεκριμένους χώρους, που μπορεί να επιτευχθεί μέσω διαφόρων τεχνολογιών, όπως κάμερες, αισθητήρες κίνησης, αισθητήρες θερμοκρασίας, αισθητήρες ήχου και άλλα. Η μέθοδος αυτή, παρακολουθεί πρακτικά την παρουσία, τις δραστηριότητες και την κίνηση ατόμων στο χώρο, με τη συλλογή δεδομένων θέσης και συμπεριφοράς, περιλαμβάνοντας παραμέτρους όπως η κίνηση, ο χρόνος παραμονής και οι χώροι τους οποίους επισκέπτονται. Η παρακολούθηση μπορεί να γίνει για πολλούς σκοπούς, όπως η ασφάλεια, η βελτίωση της διοίκησης χώρων, η ανίχνευση συμπεριφορών κινδύνου. Οι τεχνολογίες crowd monitoring μπορεί να προσφέρει πολλά οφέλη στις πόλεις, παρέχοντας πολύτιμες εισηγήσεις και δεδομένα που συμβάλλουν στην αποτελεσματική αστική διαχείριση, τη βελτιωμένη ασφάλεια, τη βελτιωμένη παροχή υπηρεσιών και την καλύτερη συνολική ποιότητα ζωής των κατοίκων. Ορισμένοι τρόποι με τους οποίους το crowd monitoring μπορεί να συμβάλλει στην καλυτέρευση της καθημερινότητας των ανθρώπων στη σύγχρονη ζωή είναι ενδεικτικά οι ακόλουθοι. Μέσω της παρακολούθησης της κίνησης και της πυκνότητας του πλήθους, είναι εφικτή η διαχείριση της κυκλοφορίας και των μεταφορών με τη βελτιστοποίηση της ροής της κυκλοφορίας, τον εντοπισμό περιοχών με κυκλοφοριακή συμφόρηση. Η δυνατότητα παρακολούθησης της συγκέντρωσης πλήθους σε συγκεκριμένες γεωγραφικές περιοχές αποτελεί επίσης βασικό παράγοντα για την ανάπτυξη, μεταξύ άλλων, μέτρων ασφάλειας και προστασίας. Η επίγνωση της ροής ανθρώπων σε δρόμους, πλατείες, γειτονιές και κτίρια μπορεί να συμβάλλει στην πρόληψη και διαχείριση κρίσιμων καταστάσεων σε σημεία συμφόρησης, απρόσμενη συμφόρηση ή μη αναμενόμενες καταστάσεις μπορούν να ανιχνευθούν εγκαίρως, επιτρέποντας στις αρχές να λάβουν προληπτικά μέτρα για τη διατήρηση της δημόσιας ασφάλειας. Παράλληλα κατά τη διάρκεια φυσικών καταστροφών ή καταστάσεων έκτακτης ανάγκης, η παρακολούθηση των πληθυσμιακών ροών μπορεί να βοηθήσει στην εντοπισμό περιοχών με υψηλή πυκνότητα πληθυσμού, επιτρέποντας στις αρχές να κατανέμουν αποτελεσματικά πόρους και να εκκενώσουν ευάλωτες περιοχές πιο αποτελεσματικά.

Η ανίχνευση των στοιχείων πληρότητας ενός χώρου, όπως η αντίστοιχη ταχύτητα των ανθρώπων κατά τη διέλευσή τους από τον χώρο, ο ρυθμός άφιξης/αποχώρησης από/προς τον χώρο, καθώς και ο συνολικός αριθμός των ανθρώπων στον χώρο, μπορεί να είναι χρήσιμη σε πολλές εφαρμογές. Για παράδειγμα, τα καταστήματα λιανικής πώλησης μπορούν να μάθουν για τη δημοτικότητα των προϊόντων σε διάφορους διαδρόμους, αν γνωρίζουν την ταχύτητα/πυκνότητα των καταναλωτών σε διάφορα σημεία του καταστήματος. Σε έναν διάδρομο καταστήματος λιανικής πώλησης, στον οποίο διατίθεται ένας συγκεκριμένος τύπο προϊόντος, οι καταναλωτές που εισέρχονται σε αυτόν θα περπατήσουν με κανονικό ρυθμό, εάν τα προϊόντα στον διάδρομο δεν προσελκύουν την προσοχή τους. Από την άλλη πλευρά, μπορεί να επιβραδύνουν ή να σταματήσουν για να κοιτάξουν τα προϊόντα, αν τα βρουν ενδιαφέροντα. Επομένως, εκτιμώντας τη μέση ταχύτητα των αγοραστών σε έναν διάδρομο, μπορεί να συναχθεί η δημοτικότητα των προϊόντων στον εν λόγω διάδρομο. Οι πληροφορίες αυτές, με τη σειρά τους, μπορούν να βοηθήσουν σημαντικά στον επιχειρηματικό σχεδιασμό. Ομοίως, τα μουσεία μπορούν να εκτιμήσουν ποια από τα εκθέματά τους είναι πιο δημοφιλή, με βάση την ταχύτητα των επισκεπτών, καθώς και τον ρυθμό άφιξής τους σε διάφορες περιοχές. Οι έξυπνες πόλεις μπορούν περαιτέρω να σχεδιάσουν τον προγραμματισμό των φωτεινών σηματοδοτών για τις διαβάσεις πεζών με βάση τις ταχύτητές τους (*S. Depatla et al., 2018*). Επιπλέον, ο εντοπισμός των αργών περιοχών μπορεί να βοηθήσει στον πολεοδομικό σχεδιασμό με τη διάθεση νέων δρόμων και εγκαταστάσεων. Οι δημόσιοι χώροι, όπως ένας σιδηροδρομικός σταθμός, από την άλλη πλευρά, μπορούν να ανιχνεύσουν περαιτέρω μη συνήθεις ή μη αναμενόμενες καταστάσεις, εάν εντοπιστεί μια άτυπη επιβράδυνση σε μια συγκεκριμένη περιοχή.

Πολλοί ερευνητές, προτείνουν ένα πλαίσιο που μπορεί να αξιολογήσει ταχαρακτηριστικά πληρότητας μιας περιοχής, συμπεριλαμβανομένης της ταχύτητας του πλήθους κατά τη διέλευση από την περιοχή, του ρυθμού άφιξης/αναχώρησης προς/από την περιοχή ή του συνολικού αριθμού των ατόμων στην περιοχή, χρησιμοποιώντας μόνο την ισχύ του λαμβανόμενου σήματος (RSSI) δύο συνδέσεων WiFi στην περιοχή ενδιαφέροντος και χωρίς να βασίζεται σε άτομα που μεταφέρουν κάποια συσκευή (δηλαδή παθητικά). Δεδομένου ότι ένα άτομο μπορεί να μην έχει σταθερή ταχύτητα σε μια περιοχή, η "εκτίμηση της ταχύτητας" αναφέρεται στην εκτίμηση της μέσης ταχύτητας των ατόμων, όπου ο μέσος όρος είναι ο χωρικός μέσος όρος της ταχύτητας ενός ατόμου στη συγκεκριμένη περιοχή.

Οι διοργανωτές εκδηλώσεων έχουν επίσης εκδηλώσει το ενδιαφέρον τους για την αξιοποίηση των σύγχρονων τεχνολογιών καταμέτρησης προκειμένου να παρακολουθούν τις εκδηλώσεις σε πραγματικό χρόνο, να μπορούν να εκτιμούν τον αριθμό του κοινού και να πραγματοποιούν μεταγενέστερες αναλύσεις με σκοπό την ανάλυση των αιτιών τυχόν συνωστισμού, ώστε να αποφευχθούν μελλοντικά παρόμοια περιστατικά. Ειδικότερα, ο υπολογισμός της πυκνότητας του πλήθους σε πραγματικό χρόνο σε στρατηγικές περιοχές επιτρέπει στους υπευθύνους ασφαλείας να αποφανθούν εάν μια εκδήλωση έχει φθάσει στη μέγιστη χωρητικότητά της. Οι χρονοσειρές καταμέτρησης πλήθους μπορούν να χρησιμοποιηθούν σε αλγορίθμους για την πρόβλεψη του συνωστισμού, γεγονός που επιτρέπει στο προσωπικό ασφαλείας να λαμβάνει εκ των προτέρων τα κατάλληλα μέτρα.

1.2. Ανάλυση πλήθους και παρακολούθηση

Το πλήθος και η παρακολούθησή του, αποτελεί σημαντικό ερευνητικό ζήτημα στην εποχή της μηχανικής όρασης τα τελευταία χρόνια. Λόγω του ολοένα και αυξανόμενου πληθυσμού, η κατανόηση και η παρακολούθηση της συμπεριφοράς του πλήθους έχει πλέον καταστεί ουσιαστική άσκηση και πρόκληση για διάφορες πτυχές της καθημερινής ζωής παγκοσμίως. Κατά συνέπεια, διάφορες ομάδες ερευνητών και διανοητών έθεσαν ως στόχο την εξεύρεση κατάλληλης λύσης σε αυτόν τον τομέα, ώστε να ελέγχουν και να διαχειρίζονται το πλήθος με τον συγκεκριμένο τρόπο. Η παρακολούθηση μιας μεγάλης περιοχής πλήθους έχει παρουσιάσει αλματώδη αύξηση των καμερών παρακολούθησης που έχουν εγκατασταθεί σε όλο τον κόσμο, ενώ ο περιορισμένος αριθμός ανθρώπινων πόρων δεν επαρκεί για την ανάλυση αυτού του μεγάλου αριθμού καρέ βίντεο. Επομένως, απαιτείται ένας αυτοματοποιημένος τρόπος για την παρακολούθηση και την ταξινόμηση του πλήθους. Το ευφυές σύστημα επιτήρησης είναι μια από τις εξαιρετικά σημαντικές εφαρμογές της ανάλυσης πλήθους («Intelligent surveillance system»). Οι ερευνητές έχουν προτείνει διάφορες μεθόδους και τεχνικές για την κατανόηση της συμπεριφοράς του πλήθους για την ανάπτυξη ενός ασφαλούς περιβάλλοντος, προκειμένου να αποφευχθεί ο συνωστισμός του πλήθους, οι δημόσιες ταραχές και οι τρομοκρατικές επιθέσεις κ.λπ. Σε σκηνές συνωστισμού, οι συνήθεις τεχνικές όρασης υπολογιστών δεν είναι δυνατόν να εφαρμοστούν σε πρώτο χρόνο λόγω της εκτεταμένης απόκρυψης και των σύνθετων παρασκηνιακών σεναρίων. Στη βιβλιογραφία αναφέρονται πολλοί αλγόριθμοι υπολογιστικής όρασης για τον εντοπισμό, την ανίχνευση και την ανάλυση της συμπεριφοράς σε περιστατικά συνωστισμού. Αν και παρέχουν

ικανοποιητικά αποτελέσματα σε περιπτώσεις χαμηλής ή μέσης πυκνότητας πληθυσμού, η αντιμετώπιση μεγάλου πλήθους εξακολουθεί να αποτελεί πρόκληση. Είναι σκόπιμο να παρουσιαστεί μια ανασκόπηση της παρακολούθησης και ταξινόμησης του πλήθους. Οι περισσότερες από τις πρόσφατες έρευνες επικεντρώθηκαν στην ανάλυση της δραστηριότητας ενός ατόμου ή μιας μικρής ομάδας ανθρώπων, αντί να επικεντρωθούν σε ένα σενάριο με πλήθος ανθρώπων (Lamba S. and Nain N., 2017). Ένα πλήθος έχει τόσο δυναμικά όσο και ψυχολογικά χαρακτηριστικά, οπότε η ανάλυση της συμπεριφοράς είναι ένα πολύ σύνθετο έργο. Τα ανθρώπινα πλήθη είναι συχνά προσανατολισμένα σε διάφορους στόχους, συνεπώς, είναι πολύ δύσκολο να διαμορφωθεί η δυναμική ενός πλήθους σε επαρκές επίπεδο. Στις περισσότερες περιπτώσεις επιτήρησης υπάρχει ανάγκη ανίχνευσης, καταμέτρησης και ταξινόμησης της συμπεριφοράς του πλήθους.

Η μελέτη της ανάλυσης πλήθους διακρίνεται συνολικά σε τρία μέρη: παρακολούθηση ανθρώπων και κατανόηση της συμπεριφοράς ή ανίχνευση ανομοιομορφιών. Μια συστηματική αναπαράσταση της παρακολούθησης και ταξινόμησης πλήθους, αποτελείται από καταμέτρηση ατόμων ή εκτίμηση πυκνότητας («People Counting or Density Estimation»), παρακολούθηση ατόμων («People Tracking»), ανάλυση συμπεριφοράς πλήθους («Crowd Behavior Analysis»). Η καταμέτρηση των ανθρώπων επικεντρώνεται κυρίως σε περιοχές με υπερπληθυσμό, τόσο για λόγους ασφαλείας όσο και για λόγους προστασίας. Η καταμέτρηση ανθρώπων ή η εκτίμηση της πυκνότητας είναι ένα κυρίαρχο πρόβλημα για τον καθορισμό του επιπέδου ενός πλήθους ως πυκνού ή αραιού. Η καταμέτρηση ανθρώπων μπορεί να εφαρμοστεί σε στατικές εικόνες και αλληλουχίες βίντεο τόσο σε εξωτερικούς όσο και σε εσωτερικούς χώρους. Τα τελευταία χρόνια, η καταμέτρηση ανθρώπων μπορεί να διαμορφωθεί ως εξής: καταμέτρηση με ανίχνευση και καταμέτρηση με ομαδοποίηση. Η κατανόηση και η παρακολούθηση της συμπεριφοράς του πλήθους εξακολουθεί να αποτελεί πρόκληση, παρά τις διάφορες προόδους στην ανάλυση της ανθρώπινης συμπεριφοράς. Η μη συνηθισμένη συμπεριφορά μπορεί να οριστεί με διάφορους τρόπους λόγω της εξατομικευμένης φύσης της και έχει δημιουργήσει μεγάλη σύγχυση στη βιβλιογραφία. Ορισμένοι ερευνητές περιγράφουν τη μη συνηθισμένη συμπεριφορά με κριτήριο τη συχνότητα. Ως μη συνηθισμένο ονομάζεται το γεγονός που συμβαίνει σπάνια ή που συμβαίνει σπάνια. Το πλήθος μπορεί να κατηγοριοποιηθεί ως διαρθρωμένο ή μη διαρθρωμένο. Είναι εύκολο να αναλυθεί το διαρθρωμένο πλήθος, αλλά ένα μη διαρθρωμένο πλήθος είναι πολύ δύσκολο λόγω της συμπτωματικής κίνησης. Στην κατανόηση της

συμπεριφοράς επικεντρωνόμαστε κυρίως στις ταχύτητες, την κατεύθυνση της ροής και τα μη συνηθισμένα γεγονότα όπως οι συμπλοκές, το τρέξιμο κ.λπ. Η αξιολόγηση της συμπεριφοράς του πλήθους είναι και πάλι ένα απαιτητικό ζήτημα, επειδή το υλικό βίντεο που περιέχει συγκεκριμένες μη συνηθισμένες συμπεριφορές στο κοινό πλήθος δεν είναι εύκολα προσβάσιμο και διαθέσιμο.

1.3. Κατηγορίες συστημάτων crowd monitoring

1.3.1. Συμβατικά συστήματα

Τα συμβατικά συστήματα crowd monitoring βασίζονται στην τεχνολογία παρακολούθησης που έχει ως βάση την εικόνα, η πιο συχνά χρησιμοποιούμενη μέθοδος της οποίας είναι η παρακολούθηση μέσω κλειστού κυκλώματος τηλεόρασης (CCTV). Το CCTV είναι ένα σύστημα επικοινωνίας εικόνας που μπορεί να μεταδώσει ροή βίντεο από συγκεκριμένες περιοχές και βίντεο ευρείας κλίμακας σε συσκευές σταθερού κυκλώματος. Με άλλα λόγια, το σήμα μπορεί να μεταδοθεί από την πηγή δεδομένων σε μια προκαθορισμένη συγκεκριμένη συσκευή εκπομπής που είναι συνδεδεμένη με την πηγή. Με την ανάπτυξη της τεχνολογίας, η τεχνολογία crowd monitoring με βάση την εικόνα γνώρισε τα ακόλουθα στάδια εξέλιξης, (i) η παρακολούθηση "one-to-one', κατά την οποία η μία συσκευή οθόνης παρακολούθησης αντιστοιχεί σε ένα CCTV (ii) η μετατροπή κυκλωμάτων για παρακολούθηση, εδώ τόσο η καλωδίωση όσο και η λειτουργία του συστήματος είναι πολύπλοκες, ενώ η απόδοση επέκτασης του δικτύου είναι χαμηλή, και (iii) η παρακολούθηση πολυμέσων, κατά την οποία η εναλλαγή του βίντεο μπορεί να γίνει ομαλά, ενώ η απεικόνιση μπορεί να ελεγχθεί ικανοποιητικά.

Επί του παρόντος, το ευρέως χρησιμοποιούμενο σύστημα παρακολούθησης βίντεο CCTV παρουσιάζει σημαντικά μειονεκτήματα, με βασικότερο το γεγονός ότι ο τύπος των αισθητήρων που χρησιμοποιούνται είναι απλός. Περαιτέρω, συνήθως, η τεχνολογία παρακολούθησης με βάση την εικόνα χρησιμοποιεί μόνο δεδομένα βίντεο ή εικόνας, πράγμα που σημαίνει ότι παραλείπονται ορισμένα δεδομένα του περιβάλλοντος χώρου (όπως η θερμοκρασία, η υγρασία, τα αέρια και τα ηχητικά κύματα), με αποτέλεσμα τα απλοποιημένα δεδομένα που συλλέγονται και υπόκεινται σε επεξεργασία να οδηγούν στις περισσότερες περιπτώσεις σε μη ασφαλείς αναλύσεις και συμπεράσματα (*X. Li et al., 2021*).

Η υποκειμενική τεχνητή κρίση και αξιολόγηση των δεδομένων ροής βίντεο που συλλέγονται από την κάμερα και την οθόνη απασχολούν υπερβολικά μεγάλο ανθρώπινο δυναμικό, με σκοπό την ανάλυσή του. Επιπλέον, δεν είναι εφικτή η ποσοτική ανάλυση σημαντικών δεικτών, όπως ο βαθμός πυκνότητας του πλήθους, η ταχύτητα ροής του πλήθους, η καταμέτρηση των ατόμων ή τα μη συνηθισμένα περιστατικά, ενώ παράλληλα υπάρχουν "τυφλές" περιοχές βιντεοεπιτήρησης (νεκρά σημεία). Συνήθως, για να αποφευχθεί η παρακώλυση των δραστηριοτήτων του πλήθους κατά την καταγραφή των καταστάσεων πλήθους σε μια συγκεκριμένη περιοχή, η κάμερα παρακολούθησης εγκαθίσταται σε υψηλό σημείο. Ωστόσο, όταν πρέπει να καταγραφεί η εικόνα της κατάστασης του πλήθους σε ένα συγκεκριμένο σημείο, η σταθερή εγκατάσταση και η ανάλυση της κάμερας το καθιστούν από δύσκολο έως μη εφικτό. Εξάλλου, σε περιπτώσεις κωλύματος ή δυσμενών καιρικών συνθηκών στην υπό παρακολούθηση περιοχή, μια κάμερα δεν μπορεί να καταγράψει με σαφήνεια μη συνηθισμένες συμπεριφορές ή περιστατικά στο πλήθος (ατυχήματα, διενέξεις κ.α.). Οι αισθητήρες επί του εδάφους (αισθητήρες υπερήχων, θερμοκρασίας, υγρασίας και καπνού) και του αέρα (κάμερες υπερύθρων, κάμερες UAV) μπορεί να είναι αποτελεσματικοί για την παρακολούθηση τυφλών περιοχών. Σε κάθε περίπτωση, τα συστήματα παρακολούθησης βίντεο CCTV δεν παρέχουν επαρκή χρονική ακρίβεια και πληροφορία ώστε να συμβάλλουν στη λήψη αποφάσεων. Ορισμένα μη συνηθισμένα περιστατικά, όπως συνωστισμός, ποδοπάτημα, καυγάδες, πυρκαγιά, χαλάζι και επιθέσεις βίας, προϋποθέτουν παρακολούθηση σε πραγματικό χρόνο καθώς και υιοθέτηση και εφαρμογή μηχανισμών εκκένωσης και διαχείρισης πλήθους υψηλής αποτελεσματικότητας με χρήση τεχνητής νοημοσύνης (AI) και τεχνολογιών επικοινωνίας *(B.Sirmacekand, P.Reinartz, 2011*). Γίνεται κατανοητό, συνεπώς, ότι βασικά στοιχεία των συστημάτων crowd monitoring, είναι η χρήση διαφόρων τύπων αισθητήρων, η λεπτομερής ανάλυση δεδομένων και η ταχεία λήψη αποφάσεων.

1.3.2. Ευφυή συστήματα παρακολούθησης και διαχείρισης πλήθους (intelligent crowd monitoring and management systems)

Οι ερευνητές καταλήγουν ότι τα ευφυή συστήματα παρακολούθησης και διαχείρισης πλήθους (intelligent crowd monitoring and management systems - ICMMS) είναι τα πλέον αποτελεσματικά μέσα για την ενίσχυση της δημόσιας ασφάλειας, την καινοτομία στην κοινωνική διακυβέρνηση, την αύξηση του επιπέδου διαχείρισης και την ανάπτυξη της ικανότητας έγκαιρης προειδοποίησης σε περιπτώσεις έκτακτης ανάγκης και την αναγνώρισή και ανάλυση της συμπεριφοράς του πλήθους σε διάφορες περιοχές με έξυπνο τρόπο. Τα ευφυή συστήματα παρακολούθησης και διαχείρισης πλήθους διαδραματίζουν σημαντικό ρόλο στην ανάπτυξη μιας έξυπνης πόλης, καθώς περιλαμβάνουν πολλούς αισθητήρες και συνεπώς συμβάλλουν στην ανάλυση μεγάλης ροής δεδομένων διαφόρων μορφών από πολλαπλές πηγές σε βάθος και με ακρίβεια σε πραγματικό χρόνο, καθιστώντας με αυτόν τον τρόπο εφικτή τη λήψη αποφάσεων σε σύντομο χρονικό διάστημα.

Σε ένα τέτοιο αυτόνομο σύστημα, είναι ιδιαίτερα σημαντική η επεξεργασία και η ανάλυση των δεδομένων. Η συγχώνευση δεδομένων ("data fusion") είναι ένα είδος τεχνολογίας συγχώνευσης πληροφοριών που συσχετίζει και συνδυάζει τις πληροφορίες που προέρχονται από πολλούς αισθητήρες προκειμένου να επιτευχθεί πιο άμεση και ορθή υποστήριξη στη λήψη αποφάσεων. Από τη συλλογή δεδομένων χαμηλής κλίμακας έως τις υπηρεσίες υψηλού επιπέδου, η συγχώνευση δεδομένων προσφέρει βιώσιμη και υψηλής απόδοσης υποστήριξη για συγχώνευση σε βάθος και εξαγωγή μαζικών δεδομένων πολλαπλών πηγών σε ετερογενή δίκτυα. Σε σύγκριση με ένα σύστημα που βασίζεται σε μία μόνο πηγή πληροφοριών, τα ευφυή συστήματα παρακολούθησης και διαχείρισης πλήθους με συγχώνευση δεδομένων έχουν μεγάλα πλεονεκτήματα σε πολλούς τομείς, όπως η κάλυψη του χώρου, η χρονική διάρκεια παρακολούθησης, τα πλεονασματικά δεδομένα, η εγκυρότητα των πηγών δεδομένων, η ανθεκτικότητα του συστήματος, η πολυπλοκότητα των δεδομένων, οι πόροι αποθήκευσης, οι απαιτήσεις υπολογιστικών επιδόσεων και οι υπηρεσίες εφαρμογών. Ωστόσο, οι υπάρχουσες αρχιτεκτονικές συγχώνευσης δεδομένων συστημάτων crowd monitoring, δεν είναι αρκετά ολοκληρωμένες, καθώς τα περισσότερα συστήματα που σχεδιάζονται επικεντρώνονται αποκλειστικά στην συγχώνευση αισθητήρων απλού τύπου, δηλαδή στη συγχώνευση δεδομένων χωρίς τη δυνατότητα αντίληψης των δεδομένων ή τη δυνατότητα λήψης αποφάσεων.

Η αρχιτεκτονική ενός ευφυούς συστήματος παρακολούθησης και διαχείρισης πλήθους περιλαμβάνει πολλαπλούς αισθητήρες, πολλαπλές λειτουργίες και διαδικασίες αλληλεπίδρασης ανθρώπου-μηχανής. Αυτό σημαίνει ότι η διαδικασία συγχώνευσης δεδομένων του συστήματος σε αυτό το σύστημα πρέπει να συμπράττει με την νοημοσύνη και την αυτοματοποίηση δεδομένων που προέρχονται από πολλές διαφορετικές πηγές και με διάφορους τρόπους, από τον κατώτερο αισθητήρα έως τις ανώτερες υπηρεσίες.

Ποιες είναι όμως οι απαιτήσεις και οι προκλήσεις της συγχώνευσης δεδομένων σε ένα ευφυές σύστημα παρακολούθησης και διαχείρισης πλήθους; Για να ενισχυθεί η ανθεκτικότητα ενός ευφυούς συστήματος παρακολούθησης και διαχείρισης πλήθους ολόκληρη η αρχιτεκτονική του δικτύου hardware πρέπει να ανταποκρίνεται στις λειτουργίες συλλογής κατανεμημένων και ιστορικών δεδομένων, η οποία απαιτεί συγχώνευση δεδομένων από διάφορες πηγές για την υποστήριξη της χωρικής επέκτασης ενός μεμονωμένου αισθητήρα. Επιπλέον, με βάση τον τρόπο με τον οποίο βελτιώνονται οι δυνατότητες αποθήκευσης του edge cloud και του cloud, η ενσωμάτωση όλων των ιστορικών δεδομένων επιτρέπει περαιτέρω τη χρονική επέκταση του συστήματος (Ansif Arooj et al. 2021). Σε ένα ευφυές σύστημα παρακολούθησης και διαχείρισης πλήθους, η αξιοπιστία των δεδομένων περιλαμβάνει την αξιοπιστία του κόμβου του αισθητήρα, την αυθεντικότητα των δεδομένων και την ασφάλεια του συστήματος. Η ασφάλεια του συστήματος μπορεί να διασφαλισθεί με τη λήψη μέτρων αποτροπής επιθέσεων και τον έλεγχο των αρμόδιων αρχών, για παράδειγμα. Τα μέτρα ασφάλειας δεδομένων συνήθως περιλαμβάνουν, ενδεικτικά την κρυπτογράφηση και αποκρυπτογράφηση δεδομένων από κοινού με την αποθήκευση, τη δημιουργία αντιγράφων ασφαλείας δεδομένων, τα ψηφιακά πιστοποιητικά. Ένα ευφυές σύστημα παρακολούθησης και διαχείρισης πλήθους χρησιμοποιεί κατανεμημένη ανίχνευση δεδομένων και κεντρική αποθήκευση και ανάλυση δεδομένων. Για την ακριβή ανάλυση των δεδομένων, είναι απαραίτητο να διασφαλιστεί η ενιαία αντίληψη των διαφορετικών πηγών δεδομένων αισθητήρων για το ίδιο συμβάν, η συνέπεια των δεδομένων κατά τη διαβίβαση από την πηγή δεδομένων στο edge cloud και η συνεκτικότητα ή η τυποποίηση των δεικτών αξιολόγησης των δεδομένων (J. K. Uhlmann, 2003). Υπό περιπτώσεις, τα δεδομένα που συλλέγονται από τους αισθητήρες ενδέχεται να είναι ελλιπή, περιττά και αταξινόμητα. Σε περίπτωση ελλιπών ή εσφαλμένων δεδομένων,

κρίνεται απαραίτητη η συμπλήρωση ή η αξιολόγησή τους μέσω άλλων πηγών δεδομένων ή πληροφοριών σχετικά με το περιβάλλον που συλλέγονται από τους αισθητήρες. Το υποσύνολο δεδομένων σε ένα κατανεμημένο σύστημα μπορεί να απεικονίζει ικανοποιητικά την κατάσταση του υποσυστήματος ή τους τύπους των συμβάντων σε μία συγκεκριμένη περιοχή. Ωστόσο, η περιγραφή των πληροφοριών είναι πολύ περιορισμένη από σφαιρική άποψη. Το ευφυές σύστημα παρακολούθησης και διαχείρισης πλήθους πρέπει να κατανέμει παγκόσμιες πηγές, να δίνει έγκαιρες προειδοποιήσεις και να λαμβάνει αποφάσεις σύμφωνα με την υπό παρακολούθηση δυναμική κατάσταση του πλήθους. Ως εκ τούτου, η συγχώνευση τοπικών χαρακτηριστικών στο στάδιο της ανάλυσης δεδομένων μπορεί να βοηθήσει στη διεξοδική αναζήτηση των κρυμμένων πληροφοριών στο επίπεδο λήψης αποφάσεων του συστήματος. Ως προς την ακρίβεια των αποφάσεων, η συγχώνευση δεδομένων που προαναφέρθηκε, συμβάλλει στην αναζήτηση πληροφοριών μεγάλης εμβέλειας, ενώ η συγχώνευση επιπέδων λήψης αποφάσεων συνδέεται με τις εφαρμογές και παρέχει ακριβείς και αποτελεσματικές αποφάσεις στους χρήστες. Σε ένα ευφυές σύστημα παρακολούθησης και διαχείρισης πλήθους, οι ακριβείς αποφάσεις περιλαμβάνουν ακριβείς προειδοποιήσεις για καταστροφές από πυρκαγιές, συστάσεις εκκένωσης, έγκαιρες προειδοποιήσεις για μη αναμενόμενα περιστατικά και καταστάσεις (*X. Li et al., 2021)*. Για τους χρήστες, εάν το σύστημα είναι προηγμένο, επηρεάζει άμεσα την εμπειρία της υπηρεσίας. Ο τρόπος παρουσίασης της ακριβούς απόφασης του ευφυούς συστήματος παρακολούθησης και διαχείρισης πλήθους με μεγαλύτερη νοημοσύνη είναι το πιο ουσιαστικό ζήτημα για υπηρεσίες και εφαρμογές προσανατολισμένες στις ανάγκες των χρηστών. Στο στάδιο της συγχώνευσης αποφάσεων, οι μέθοδοι οπτικοποίησης και προσομοίωσης, όπως η οθόνη παρακολούθησης βίντεο, η απεικόνιση διαγραμμάτων δεδομένων αισθητήρων, η τρισδιάστατη μοντελοποίηση του χώρου και του πλήθους, η πρόβλεψη του πλήθους στο μέλλον και ένα δυναμικό διάγραμμα προσομοίωσης, θα βελτιώσουν περαιτέρω την νοημοσύνη του συστήματος.

1.4 Mobile crowd sensing

Είναι κοινά΄ αποδεκτό πως οι έξυπνες συσκευές, οι οποίες συνήθως είναι εξοπλισμένες με μία σειρά αισθητήρων, εξελίσσονται σημαντικά στην εποχή μας και αποτελούν αναπόσπαστο κομμάτι της καθημερινότητας των ανθρώπων, καθιστώντας τις πόλο έλξης για πολλούς. Η πανταχού παρουσία τους φαίνεται φαίνεται να οδηγεί στην κυριαρχία τους,

ως το βασικό μέσο επικοινωνίας μεταξύ των χρηστών, ενισχύοντας, με αυτόν τον τρόπο τον ρόλο τους στη ζωή των ανθρώπων. Αυτό έχει ως αποτέλεσμα, οι κινητές συσκευές να δύναται να αποτελέσουν ανεξάντλητη πηγή πληροφοριών, καθώς, παρέχουν στους χρήστες τους τη δυνατότητα να συλλέξουν, να επεξεργαστούν και να μοιραστούν τεράστιους όγκους δεδομένων, μέσω του διαδικτύου. Αυτές οι δυνατότητες έδωσαν το έναυσμα για την ανάπτυξη και η υλοποίηση της ιδέας του Mobile Crowd Sensing, έναν όρο που αναπτύχθηκε πρόσφατα κι αποτελεί μια καινοτόμο εξέλιξη της ιδέας του Διαδικτύου των Πραγμάτων (Internet of Things). Το Mobile Crowd Sensing αποτελείται από τον συνδυασμό των λέξεων πλήθος (crowd) και ανίχνευση (sensing). Όπως υποδηλώνουν οι λέξεις από τις οποίες προέρχεται, αποτελεί μια μορφή ομαδικής δραστηριότητας που παρακινεί τους χρήστες οι οποίοι είναι διατεθειμένοι να συλλέξουν και να συνεισφέρουν πολύτιμες πληροφορίες να συμμετέχουν στη διαδικασία εκμεταλλευόμενοι την δυναμική των διαφόρων συσκευών, για τη συλλογή δεδομένων. Σκοπός είναι να για να αποκτηθεί γνώση για ένα συγκεκριμένο γεγονός κοινού ενδιαφέροντος στον πραγματικό κόσμο.

Ουσιαστικά το mobile crowd sensing είναι μια νέα τεχνική που συλλέγει δεδομένα από το περιβάλλον και την ευρύτερη κοινωνία μέσω μιας μεγάλης ομάδας ατόμων που διαθέτουν κινητές συσκευές με σκοπό τη συλλογή και την ανάλυση δεδομένων. Το mobile crowd sensing αφορά σε ένα μοντέλο συλλογικής ανίχνευσης όπου τα άτομα που διαθέτουν κινητές συσκευές, συμβάλλουν στον υπολογισμό κοινών δεδομένων με σκοπό τη μέτρηση και ανάλυση οποιωνδήποτε διεργασιών κοινού ενδιαφέροντος. Η μέθοδος αυτή προϋποθέτει μεγάλο αριθμό συμμετεχόντων για τη λήψη δεδομένων από το περιβάλλον με τη χρήση υποστηρικτικών συσκευών, όπως είναι τα smartphones ή τα tablets. Τα δεδομένα που ανιχνεύονται και παρέχονται από τους συμμετέχοντες μπορούν να βοηθήσουν στην ανάδειξη πολλών χρήσιμων πληροφοριών, όπως η ταυτότητα του χρήστη, οι προσωπικές δραστηριότητες, οι πολιτικές απόψεις και η κατάσταση της υγείας. Τέτοια δεδομένα μπορούν να συμβάλλουν στην εξιχνίαση εγκλημάτων, τον εντοπισμό κινδύνων και την αποτροπή δυνητικά επικίνδυνων για την κοινωνία περιστατικών. Χάρη σε αυτές τις καινοτομίες, η μέθοδος της συλλογικής ανίχνευσης εφαρμόζεται ευρέως σε πολλές εφαρμογές, όπως η υπηρεσία κλήσης ταξί σε πραγματικό χρόνο, π.χ. Uber, ο έλεγχος τοποθέτησης προϊόντων σε σούπερ μάρκετ, η υπηρεσία εντοπισμού πολιτών, η σημασιολογική επισήμανση χαρτών, η παρακολούθηση της κατάστασης των δρόμων, η παρακολούθηση του θορύβου, η παροχή

εικόνων από το πλήθος, η παρακολούθηση της ρύπανσης και άλλες. Για να ενθαρρυνθούν οι χρήστες να συγκεντρώσουν και να υποβάλουν τα δεδομένα σχετικά με το κοντινό τους περιβάλλον και να τα καταστήσουν διαθέσιμα σε εφαρμογές ευρείας κλίμακας, οι συμμετέχοντες ανταμείβονται για τα δεδομένα που εισάγουν (*Tu N. Nguyen et al., 2021*). Το mobile crowd-sensing είναι επίσης γνωστό ως ένα καινοτόμο κυβερνο-φυσικό σύστημα (Cyber-Physical System - CPS) που επιτρέπει στους ανθρώπους να διαθέτουν έξυπνες συσκευές με δυνατότητες ανίχνευσης και επικοινωνίας για να συλλέγουν και να παρέχουν δεδομένα σε ένα κέντρο CPS. Η συλλογή δεδομένων για την παρακολούθηση μιας κρίσιμης περιοχής είναι μια από τις τυπικές εφαρμογές του mobile crowd-sensing. Οι περισσότερες μελέτες για την συλλογή δεδομένων έχουν πραγματοποιηθεί με τη χρήση Ασύρματων Δικτύων Αισθητήρων (Wireless Sensor Networks - WSN) ή δικτύων αισθητήρων οχημάτων, ωστόσο, η χρήση Ασύρματων Δικτύων Αισθητήρων παρουσιάζει αρκετά μειονεκτήματα, όπως η κατανάλωση της μπαταρίας, η σταθερή θέση εγκατάστασης των αισθητήρων και, επιπλέον, τα έξοδα κατασκευής, τα οποία είναι σημαντικά υψηλότερα από το κόστος ανάπτυξης ενός δικτύου mobile crowd-sensing. Δεδομένου ότι τα παραδοσιακά ασύρματα δίκτυα αισθητήρων απαιτούν υψηλό κόστος για την ανάπτυξή τους και δεν μπορούν να παρέχουν έγκαιρα ολοκληρωμένη εικόνα της καίριας περιοχής, τα δίκτυα mobile crowd-sensing φαίνεται να είναι η καλύτερη λύση, διότι επιτρέπουν στον διαχειριστή του CPS να ενημερώνεται συνεχώς για την επίμαχη περιοχή, υπερνικώντας έτσι την πρόκληση της γεωγραφικής απόστασης.

1.4.1 Τα χαρακτηριστικά του Mobile Crowd Sensing

Το mobile crowd sensing βασίζεται στην ισχύ και στην ευφυΐα των διαφόρων συσκευών, όπως και στη δύναμη του πλήθους, με στόχο τη συγκέντρωση δεδομένων για ένα γεγονός που προσελκύει την προσοχή στον πραγματικό κόσμο. Τα συλλογικά δεδομένα που προσφέρονται από το πλήθος μπορούν να οδηγήσουν στη βέλτιστη λήψη αποφάσεων συγκριτικά με την περίπτωση που τα όποια δεδομένα προέρχονταν από μόνο ένα άτομο, του οποίου η συνεισφορά θα μπορούσε να θεωρηθεί αμελητέας σημασίας και σαφώς δε θα είχε τα ίδια αποτελέσματα

Χάρη στην αλματώδη εξέλιξη των δυνατότητων των συσκευών, δίνεται η δυνατότητα οι εργασίες του mobile crowd sensing να λαμβάνουν χώρα στις κινητές συσκευές των

ανθρώπων, οι οποίες, ωστόσο, πρέπει να πληρούν κάποιες προϋποθέσεις (θέση, χρόνο, ειδικούς αισθητήρες, κλπ.). Συνεπώς, ο ρόλος των χρηστών ενισχύεται στη διαδικασία συλλογής δεδομένων και η συμβολή τους κρίνεται ιδιαίτερα σημαντική. Οι χρήστες συμμετέχουν στο βρόχο για τη συλλογή των δεδομένων, την επεξεργασία τους, την ανάλυση τους καθώς και τη μετάδοση τους. Το χαρακτηριστικό αυτό προσφέρει πλεονεκτήματα στα συστήματα mobile crowd sensing, όπως ενδεικτικά η άμεση λήψη πληροφοριών, αλλά και σημαντικά μειονεκτήματα, καθώς επηρεάζει την ποιότητα των απαντήσεων και το χρόνο ανταπόκρισης των χρηστών.

Ο βαθμός συμμετοχής των χρηστών κατά τη διαδικασία συλλογής δεδομένων ποικίλλει ανά περιτώσεις και εξαρτάται από τις απαιτήσεις της κάθε εφαρμογής. Συγκεκριμένα το mobile crowd sensing επιτρέπει τόσο την άμεση όσο και την έμμεση συμμετοχή των χρηστών στο βρόχο συλλογής δεδομένων, αξιοποιώντας είτε τη συμμετοχική ανίχνευση (participatory sensing) είτε την ευκαιριακή ανίχνευση (opportunistic sensing). Ειδικότερα, στη συμμετοχική ανίχνευση, ο χρήστης εκδηλώνει τη συνειδητή επιλογή του να συμμετέχει στη διαδικασία και η παροχή των υπηρεσιών είναι απαραίτητη σε αυτόν, ενώ παράλληλα μπορεί να καθορίσει ο ίδιος το πλαίσιο στο οποίο επιθυμεί να παίρνει μέρος στη συλλογή πληροφοριών (πότε, πώς και πού). Αντίθετα, στην ευκαιριακή ανίχνευση, η συμμετοχή του χρήστη είναι ελάχιστη ή μηδενική και η συλλογή δεδομένων μπορεί να εξελίσσεται στο παρασκήνιο.

Παράλληλα αξιοποιώντας, τη συνεχή παρουσία των συσκευών στην καθημερινή ζωή των ανθρώπων και τον καθοριστικό ρόλο που αυτές διαδραματίζουν, το mobile crowd sensing συλλέγει δεδομένα από διαφορετικές ομάδες ανθρώπων και σε διαφορετικούς χώρους, παρέχοντας με αυτόν τον τρόπο μια ευρύτατη κάλυψη του ζητήματος με πολύ περιορισμένο κόστος και σε βέλτιστο χρόνο. Το mobile crowd sensing, μειώνει την εγκατάσταση δαπανηρών υποδομών, όπως π.χ. τα συστήματα αισθητήρων, επομένως, μειώνει το κόστος συλλογής δεδομένων, διατηρώντας, ωστόσο, σταθερή την ποιότητα των συλλεγόμενων δεδομένων και των αποτελεσμάτων. Θα μπορούσε να πει κάνεις, ότι το mobile crowd sensing μπορεί να παρέχει πληροφορίες για οποιοδήποτε θέμα, σε οποιαδήποτε γεωγραφική θέση και οποιαδήποτε χρονική στιγμή. Ένα επιπλέον χαρακτηριστικό του mobile crowd sensing είναι ότι εκμεταλλεύεται και συγκεντρώνει πολύτιμες πληροφορίες από ετερογενείς πηγές. Αρχικά, αξιοποιεί δεδομένα τόσο από τους πολυάριθμους αισθητήρες οι οποίοι βρίσκονται στις συσκευές των χρηστών όσο και από την άμεση, ουσιαστική παρέμβαση τους (σύνταξη

κειμένου, γνώμης) καθώς και από την ποσότητα πληροφοριών που οι ίδιοι οι χρήστες μοιράζονται στα μέσα κοινωνικής δικτύωσης. Λόγω του μεγάλου όγκου δεδομένων που προέρχονται από ετερογενείς πηγές το mobile crowd sensing μπορεί να αποκτήσει πρόσβαση σε προσωπικές πληροφορίες του χρήστη, όπως ενδεικτικά πληροφορίες σχετικά με τη θέση – τοποθεσία του, τις καθημερινές του συνήθειες, ακόμη και τις κοινωνικές αλληλεπιδράσεις του. Παράλληλα, συλλέγονται πληροφορίες αναφορικά με τη συσκευή του χρήστη, όπως πληροφορίες για τα επίπεδα μπαταρίας της συσκευής και τους διαθέσιμους πόρους της, ενώ είναι εφικτό να συλλεχθούν και πληροφορίες για μία συγκεκριμένη περιοχή και για τα επίπεδα κινητικότητας σε αυτή. Επισημαίνεται ότι για το σκοπό της βελτίωσης της ποιότητας και αξιοπιστίας των δεδομένων, συλλέγονται πολλές πληροφορίεςκαι από επίσημες πηγές (π.χ. κρατικές αρχές) (L. Pournajaf et al., 2015).

Από τα ανωτέρω γίνεται κατανοητό ότι το mobile crowd sensing αξιοποιεί δεδομένα που είναι διαθέσιμα τόσο εικονικά (virtual - online), δηλαδή δεδομένα που έχουν κοινοποιήσει οι χρήστες στα μέσα κοινωνικής δικτύωσης, όσο και φυσικά (physical - offline), δηλαδή δεδομένα που έχουν συνεισφέρει οι ίδιοι χρήστες ή που έχουν συλλεχθεί μέσω των αισθητήρων των κινητών συσκευών τους. Ωστόσο, αυτές οι πληροφορίες, παρουσιάζουν διαφορετικά χαρακτηριστικά μεταξύ τους και δημιουργούν μία νέα πρόκληση στο σχεδιασμό συστημάτων mobile crowd sensing, η οποία στοχεύει στην ορθή συγχώνευση των δεδομένων. Ως επακόλουθο, η εκτεταμένη συμμετοχή των χρηστών στο βρόχο συλλογής δεδομένων οδηγεί στο συνδυασμό της ανθρώπινης και της μηχανικής νοημοσύνης, η βελτιστοποίηση της οποίας αποτελεί καίριο ζήτημα στην ανάπτυξη των mobile crowd sensing συστημάτων (*B. Guo et al., 2014*). Από την μία, οι άνθρωποι έχουν τις ικανότητες να κατανοήσουν ποιες είναι οι ενέργειες στις οποίες πρέπει να προχωρήσουν, για να συλλέξουν τα απαραίτητα δεδομένα, ωστόσο είναι ελάχιστες οι δυνατότητες που έχουν από άποψη ταχύτητας, αποθήκευσης ενώ είναι συχνό φαινόμενο να εισάγουν λάθη στο σύστημα. Από την άλλη, οι μηχανές έχουν τις βέλτιστες ικανότητες για αποθήκευση και υπολογισμό, αλλά δεν έχουν δυνατότητα να κατανοήσουν. Συνεπώς, οι μηχανές μπορούν να χρησιμοποιηθούν για να αναθέτουν τις εργασίες στους χρήστες και αυτοί με τη σειρά τους να συλλέγουν τα δεδομένα που χρειόζονται ανά περίπτωση.

Η εμπλοκή των ανθρώπων - χρηστών στην ανταλλαγή δεδομένων προσφέρει πρωτοφανείς ευκαιρίες τόσο για την ανίχνευση όσο και για τη μετάδοση των δεδομένων (*Huadong MA et*

al., 2014). Όσον αφορά στη μετάδοση, υπάρχουν διάφορες τεχνικές που μπορούν να αξιοποιηθούν από τους χρήστες συμπεριλαμβανομένων των αυτοοργανώμενων (ad-hoc) δικτύων ή των ευκαιριακών (opportunistic) δικτύων καθώς και των δικτύων βασισμένων σε υποδομές (infrastructure-based). Επομένως, οι χρήστες μπορούν να υιοθετήσουν είτε την ευκαιριακή μετάδοση των δεδομένων μέσω επικοινωνιών μικρής εμβέλειας (Bluetooth, Wi-Fi) είτε τη μετάδοση βασισμένη σε υποδομές, κατά την οποία οι χρήστες ανεβάζουν δεδομένα μέσω του διαδικτύου από δίκτυα κινητής τηλεφωνίας.

Ένα ακόμη χαρακτηριστικό των συστημάτων mobile crowd sensing αποτελούν οι δυναμικές συνθήκες των κινητών συσκευών και η επαναχρησιμοποίηση των δεδομένων που έχουν συνεισφέρει οι χρήστες με στόχο την εξαγωγή πληροφοριών υψηλού επιπέδου (*B. Guo et al.,2014).* Αυτό σημαίνει ότι πολλά δεδομένα έχουν χρησιμοποιηθεί σε διαφορετικές εφαρμογές και έχουν αναλυθεί με διαφορετικό τρόπο καθώς διαφορετικές εργασίες ανίχνευσης μπορούν να ολοκληρωθούν από την ίδια συσκευή, ανάλογα με το σκοπό που πρέπει να επιτευχθεί (*Huadong MA et al., 2014*).

2. WI-FI TRACKING

2..1. Έννοια και τρόπος παρακολούθησης

Τα τελευταία χρόνια, έχουμε δει την αύξηση των λύσεων, προϊόντων και υπηρεσιών του Διαδικτύου των Πραγμάτων (IoT). Το Διαδίκτυο των πραγμάτων καταγράφει μεγάλο όγκο δεδομένων που αφορούν το περιβάλλον, καθώς και τους χρήστες τους. Η ουσιαστική αξία της συλλογής δεδομένων είναι αποτέλεσμα της επεξεργασίας και της συγκέντρωσης δεδομένων σε μεγάλη κλίμακα, από την οποία θα μπορούν να εξαχθούν νέες πληροφορίες, δεδομένα και συμπεράσματα. Μια σύγχρονη και νεότερη λύση crowd monitoring βασίζεται σε συστήματα παρακολούθησης WiFi. Τα συστήματα αυτά είναι σε αναμονή μέχρι οι συσκευές smartphones των ατόμων που βρίσκονται στο χώρο να συνδεθούν σε ένα δίκτυο ή να εγκαταστήσουν μια εφαρμογή (συνεργατική προσέγγιση), ή παρακολουθούν τα σήματα που αποστέλλονται από τις συσκευές smartphones (μη συνεργατική προσέγγιση). Αυτή η μέθοδος είναι νεότερη από τις προηγούμενες, καθώς πριν από δύο δεκαετίες κανείς δεν διέθετε ηλεκτρονικές συσκευές με δυνατότητα σύνδεσης σε Wi-Fi ή Bluetooth (*J. cois Determe et al.2022***).**

Γνωρίζουν όμως οι πολίτες για την παρακολούθηση μέσω Wi-Fi και πώς η γνώση αυτή επηρεάζει τις αντιδράσεις τους στους κινδύνους προστασίας της ιδιωτικής ζωής και της ασφάλειας; Τα αποτελέσματα των περισσότερων ερευνών δείχνουν ότι στις περισσότερες περιπτώσεις, υπάρχει έλλειψη ενημέρωσης των ατόμων σχετικά με την παρακολούθηση μέσω Wi-Fi, ενώ ταυτόχρονα τα περισσότερα άτομα είναι πρόθυμα να συμφωνήσουν στην παρακολούθηση Wi-Fi, παρά τις ανησυχίες για τον περιορισμό της ιδιωτικότητάς τους και την προστασία των προσωπικών τους δεδομένων, όσον αφορά τον τρόπο με τον οποίο συλλέγονται και αξιοποιούνται τα δεδομένα τους. Πρακτικά, κατά την παρακολούθηση μέσω Wi-Fi, οι συσκευές που εγκαθίστανται στους επιτηρούμενους χώρους, ανιχνεύουν σήματα που αποστέλλονται από τα κινητά τηλέφωνα (smartphones) των χρηστών όταν αναζητούν δίκτυο Wi-Fi, ώστε να συνδεθούν σε αυτό. Στη συνέχεια, αποσπάται η διεύθυνση διεύθυνση πρόσβασης υλικού (Media Access Control Address – MAC address) που είναι ένα αλφαριθμητικό αναγνωριστικό κάθε συσκευής που συνδέεται σε ένα δίκτυο. Η διεύθυνση MAC, είναι μοναδική για κάθε συσκευή και δεν τροποποιείται από καιρό σε καιρό όπως για παράδειγμα οι δυναμικές διευθύνσεις IP(dynamicIP), γι' αυτό το λόγο είναι και τόσο χρήσιμη. Οι πάροχοι, που χρησιμοποιούν μεθόδους παρακολούθησης μέσω Wi-FI και αποσπούν τη διεύθυνση MAC, εμμένουν ότι μέσω επεξεργασίας που πραγματοποιείται άμεσα και ταυτόχρονα κατά τη συλλογή της διεύθυνσης, κρυπτογραφείται η διεύθυνση MAC με την προσθήκη σε αυτήν κάποιων τυχαίων κάθε φορά ψηφίων, ώστε να μην είναι δυνατή η αντίστροφη διαδικασία και η εύρεση της πραγματικής διεύθυνσης MAC από τη μετέπειτα αποθηκευμένη πληροφορία. Ουσιαστικά δηλαδή, αφού εντοπισθούν οι συσκευές κινητών τηλεφώνων των ατόμων που βρίσκονται στο χώρο, συλλέγονται δεδομένα σε πραγματικό χρόνο, με βάση τη διαδρομή που ακολουθούν τα άτομα, το πού περνούν το χρόνο τους, τη διάρκεια που μένουν σε κάθε χώρο, τις περιοχές που επισκέπτονται καθώς και όσες δεν επισκέπτονται και προσπερνούν. Οι πληροφορίες συγκεντρώνονται από πολλές συσκευές κινητών τηλεφώνων, που βρίσκονται στον ελεγχόμενο χώρο και προσφέρει συγκεντρωτικές πληροφορίες, μέσω μεθόδων K-anonymity, με αποτέλεσμα να είναι αδύνατο να παρακολουθηθούν μεμονωμένες συσκευές. Στις περισσότερες περιπτώσεις, τα συστήματα παρακολούθησης μέσω Wi-Fi έχουν σχεδιασθεί με τέτοιο τρόπο ώστε σε περίπτωση που στον επιτηρούμενο χώρο ανιχνεύεται μία ή εν γένει μικρός αριθμός συσκευών κινητών τηλεφώνων, να μην αποθηκεύονται καθόλου δεδομένα, ώστε να μην καθίσταται εφικτή η ταυτοποίηση των ατόμων που βρίσκονται στο χώρο. Καθίσταται σαφές

ότι, οι πληροφορίες αυτές είναι πολύ σημαντικές τόσο για εμπορικά καταστήματα όσο και στο πλαίσιο μίας κοινότητας – πόλης.

2..2. Οι θέσεις των ευρωπαϊκών εποπτικών οργάνων

Η Ομάδα Εργασίας του άρθρου 29 στην υπ ' αριθμόν *01/2017 Γνώμη σχετικά με την πρόταση κανονισμού για τον κανονισμό για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες (2002/58/ΕΚ)*, που εκδόθηκε στις 4 Απριλίου 2017, ασχολήθηκε με τα ως άνω ζητήματα. Η Ομάδα Εργασίας του άρθρου 29 συστάθηκε βάσει του αντίστοιχου άρθρου της οδηγίας 95/46/ΕΚ, του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Οκτωβρίου 1995, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και ήταν ανεξάρτητο ευρωπαϊκό συμβουλευτικό όργανο για την προστασία των δεδομένων και της ιδιωτικής ζωής. Δυνάμει του άρθρου 68 του Γενικού Κανονισμού Προστασίας Δεδομένων συστάθηκε ως όργανο της Ευρωπαϊκής Ένωσης το Ευρωπαϊκό Συβούλιο Προστασίας Δεδομένων (ΕΣΠΔ), το οποίο αντικατέστησε την Ομάδα Εργασίας του άρθρου 29 και μεταξύ άλλων ανέλαβε την παρακολούθηση και τη διασφάλιση της ορθής εφαρμογής του νομοθετικού πλαισίου, με την επιφύλαξη των καθηκόντων των εποπτικών αρχών σε εθνικό επίπεδο.

Στην ανωτέρω Γνώμη, η Ομάδα Εργασίας του άρθρου 29, ασχολήθηκε με την πρόταση της Ευρωπαϊκής Επιτροπής, σχετικά με έναν κανονισμό για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες, η οποία υποβλήθηκε στις 10 Ιανουαρίου 2017, και διατύπωσε συγκεκριμένες προτάσεις για να διασφαλισθεί ότι ο – υπό τότε πρόταση – κανονισμός για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες θα εγγυάται το ίδιο ή υψηλότερο επίπεδο προστασίας με τον Κανονισμό για την Προστασία Δεδομένων, το οποίο να συνάδει με τον ιδιαίτερα ευαίσθητο χαρακτήρα των δεδομένων επικοινωνιών.

Σύμφωνα, με την ως άνω Γνώμη, αναφορικά με την παρακολούθηση μέσω Wi-Fi, ανάλογα με τις περιστάσεις και τους σκοπούς της συλλογής δεδομένων, βάσει του ΓΚΠΔ, η εν λόγω παρακολούθηση είναι πιθανό είτε να υπόκειται σε συγκατάθεση είτε να επιτρέπεται μόνον εφόσον τα δεδομένα προσωπικού χαρακτήρα που συλλέγονται είναι ανωνυμοποιημένα, καθώς σύμφωνα με την Ομάδα Εργασίας του άρθρου 29, οι διευθύνσεις MAC αποτελούν προσωπικά δεδομένα, ακόμη και μετά τη λήψη μέτρων ασφαλείας όπως ο κατακερματισμός. Η εν λόγω ανωνυμοποίηση θα πρέπει να εκτελείται αμέσως μετά τη συλλογή των

δεδομένων αυτών. Στην περίπτωση αυτή και πολύ περισσότερο εάν δεν είναι εφικτή η άμεση ανωνυμοποίηση των δεδομένων π.χ. λόγω των σκοπών για τους οποίους συλλέγονται τα δεδομένα, πρέπει περαιτέρω, σύμφωνα με τη Γνώμη της Ομάδας Εργασίας του άρθρου 29, να πληρούνται οι εξής προϋποθέσεις. Αρχικά, ο σκοπός συλλογής των δεδομένων από τον τερματικό εξοπλισμό θα πρέπει να περιορίζεται αυστηρά σε στατιστική καταμέτρηση. Ως προς την παρακολούθηση και στον βαθμό που είναι αυστηρά απαραίτητη για τον συγκεκριμένο σκοπό, αυτή θα πρέπει να περιορίζεται τόσο σε σχέση με το χρόνο όσο και σχέση με το χώρο. Τα δεδομένα θα πρέπει να διαγράφονται/καταστρέφονται ή να ανωνυμοποιούνται αμέσως μετά, ενώ παράλληλα θα πρέπει να υπάρχει πρόβλεψη για αποτελεσματικές δυνατότητες αυτοεξαίρεσης. Ειδικά, ως προς τις δυνατότητες αυτοεξαίρεσης, τα αρμόδια εποπτικά όργανα καλούνται να βρουν και να προωθήσουν ένα τεχνικό πρότυπο για τις κινητές συσκευές, ώστε οποιαδήποτε αντίρρηση σχετικά με την παρακολούθηση να είναι εφικτό να γνωστοποιείται αυτομάτως. Η Ομάδα Εργασίας επισημαίνει σχετικά με τη δυνατότητα ατομικής αυτοεξαίρεσης ανά οργανισμό που συλλέγει τα επίμαχα δεδομένα ότι είναι πολύ πιθανόν να δημιουργηθεί απαράδεκτη επιβάρυνση των ατόμων – υποκειμένων των δεδομένων, και για το λόγο αυτό καλεί τον νομοθέτη να προωθήσει την ανάπτυξη τεχνικών προτύπων ώστε οι συσκευές να γνωστοποιούν αυτομάτως την αντίρρηση στην επίμαχη παρακολούθηση και να είναι δυνατή η διασφάλιση της επιβολής της συμμόρφωσης των οργανισμών μέσω της γνωστοποίησης της αντίρρησης αυτής.

Περαιτέρω, η Ομάδα Εργασίας επικρίνει έντονα το γεγονός ότι οι προβλέψεις της πρότασης, όπως διατυπώνονται, δίνουν την εντύπωση ότι οι οργανισμοί έχουν τη δυνατότητα να συλλέγουν πληροφορίες που εκπέμπονται από τερματικό εξοπλισμό με σκοπό την παρακολούθηση της θέσης και των μετακινήσεων προσώπων, όπως η παρακολούθηση μέσω Wi-Fi ή παρακολούθηση μέσω Bluetooth, χωρίς να απαιτείται η συγκατάθεση του εκάστοτε ατόμου – υποκειμένου των δεδομένων, καθώς φαίνεται ότι ο εκάστοτε οργανισμός – υπεύθυνος για τη συλλογή των επίμαχων δεδομένων, υποχρεούται μόνο να ενημερώνει μέσω ανακοίνωσης την εφαρμογή μέτρων ασφάλειας προκειμένου να πραγματοποιεί συλλογή πληροφοριών που εκπέμπονται από τερματικό εξοπλισμό καθώς και για τυχόν δυνατότητα απενεργοποίησης των συσκευών, όταν τα εκάστοτε άτομα/υποκείμενα των δεδομένων δεν επιθυμούν να παρακολουθούνται. Σύμφωνα με την Ομάδα Εργασίας, μία τέτοια προσέγγιση του ζητήματος παρακολούθησης μέσω Wi-Fi και λοιπών τεχνολογιών,

θα αντέβαινε στον κύριαρχο στόχο της Ευρωπαϊκής Επιτροπής ο οποίος συνίσταται στην παροχή υψηλής ταχύτητας διασυνδεσιμότητας σε κινητό διαδίκτυο με παράλληλη διασφάλιση ισχυρής προστασίας της ιδιωτικής ζωής σε χαμηλό κόστος για όλους τους πολίτες της Ευρώπης, σε διασυνοριακό επίπεδο. Παράλληλα από την Ομάδα Εργασίας, δίνεται έμφαση στην επιβολή ρητών και συγκεκριμένων περιορισμών στο πεδίο εφαρμογής της συλλογής δεδομένων και των περαιτέρω πράξεων επεξεργασίας των δεδομένων αυτών, καθώς οι διευθύνσεις MAC, που συλλέγονται αποτελούν δεδομένα προσωπικού χαρακτήρα, ακόμη και μετά τη λήψη μέτρων ασφάλειας. Από τα ανωτέρω κατίθασταται σαφές ότι η θέση των ευρωπαϊκών εποπτικών οργάνων σε σχέση με ορισμένες λειτουργείες παρακολούθησης μέσω Wi-Fi είναι ότι πρόκειται για λειτουργίες που ενέχουν υψηλούς κινδύνου για την ιδιωτική ζωή. Συνεπώς, χωρίς την επιβολή περαιτέρω και συγκεκριμένων περιορισμών και τη θέσπιση συγκεκριμένου πλαισίου ως προς τις δραστηριότητες αυτές, η παρακολούθηση δεν θα είναι δίκαιη, σύννομη και διαφανής, ως επιβάλλεται και από τις αρχές επεξεργασίας του ΓΚΠΔ. Για παράδειγμα, ενδέχεται να απαιτείται η χορήγηση συγκατάθεσης βάσει του ΓΚΠΔ όταν ο υπεύθυνος επεξεργασίας δεδομένων συλλέγει και αποθηκεύει τις έμμεσα αναγνωρίσιμες (μέσω WiFi ή Bluetooth) διευθύνσεις MAC συσκευών και υπολογίζει τη θέση του χρήστη, προκειμένου να παρακολουθεί τη θέση του μακροπρόθεσμα, για παράδειγμα σε διάφορα καταστήματα. Αυτό συμβαίνει ιδίως όταν η παρακολούθηση λαμβάνει χώρα σε δημόσιους χώρους, όπου οι χρήστες έχουν τη θεμιτή προσδοκία ότι δεν θα αναγνωρίζονται ούτε θα παρακολουθούνται, αλλά συλλέγονται οι διευθύνσεις MAC περαστικών. Η συγκατάθεση αυτή μπορεί για παράδειγμα να εξασφαλίζεται με τη βοήθεια εφαρμογής η οποία καλεί τους χρήστες να επιτρέψουν την παρακολούθηση της θέσης τους σε συγκεκριμένους χώρους με αντάλλαγμα εμπορικές προσφορές, ή με την παροχή σημείων ελέγχου εντός συγκεκριμένων τοποθεσιών, ή μέσω δομοστοιχείου συγκατάθεσης σε σημεία πρόσβασης W-iFi.

Σε περιορισμένες μόνο περιπτώσεις μπορεί να επιτραπεί σε υπεύθυνους επεξεργασίας δεδομένων να επεξεργαστούν τις πληροφορίες που εκπέμπονται από τον τερματικό εξοπλισμό για τον σκοπό της παρακολούθησης των μετακινήσεών τους χωρίς τη συγκατάθεση του οικείου προσώπου. Για παράδειγμα, αυτό μπορεί να συμβαίνει όταν γίνεται καταμέτρηση του αριθμού των πελατών εντός μιας συγκεκριμένης τοποθεσίας ή όταν γίνεται συλλογή των δεδομένων που εκπέμπονται και στις δύο πλευρές ενός σημείου ελέγχου ασφαλείας για την εμφάνιση του χρόνου αναμονής. Ωστόσο, και στα δύο

παραδείγματα τα δεδομένα θα πρέπει να διαγράφονται ή να ανωνυμοποιούνται αμέσως μόλις επιτευχθεί ο στατιστικός σκοπός. Αυτό σημαίνει ότι οι διευθύνσεις MAC των συσκευών επισκεπτών εντός μιας συγκεκριμένης τοποθεσίας, όπως ένα κατάστημα, πρέπει να ανωνυμοποιούνται.

Τα δημόσια δίκτυα Wi-Fi είναι εξαιρετικά πρακτικά για τους χρήστες, αλλά εγείρουν πλήθος ζητημάτων αναφορικά με την διαφύλαξη της ιδιωτικότητας των χρηστών και του σεβασμού των προσωπικών τους δεδομένων. Οι προσωπικές πληροφορίες των χρηστών συλλέγονται πιο εύκολα, χωρίς να απαιτείται κάποια ενέργεια των χρηστών και πολλές φορές χωρίς καν οι ίδιοι να το αντιλαμβάνονται και μαζικά. Οι χρήστες φαίνεται να έχουν περιορισμένη επίγνωση και έλεγχο των προσωπικών δεδομένων που συλλέγονται, κατά τη σύνδεση τους σε τέτοιου είδους δίκτυα και φαίνεται να είναι διατεθειμένοι να «θυσιάσουν» την ιδιωτικότητά τους μπροστά σε ένα βραχυπρόθεσμο κέρδος (*K. ten Berg et al., 2019*). Ένας ενδεχόμενος λόγος για τον οποίο οι καταναλωτές είναι πρόθυμοι να ανταλλάξουν την ιδιωτική τους ζωή είναι επειδή δεν γνωρίζουν τον βαθμό παραβίασης της ιδιωτικότητας τους που διακινδυνεύεται. Επιπλέον, ακόμη και αν οι καταναλωτές είχαν επίγνωση της ενδεχόμενης παραβίασης της ιδιωτικότητας τους είναι εξαιρετικά πιθανό, να εξακολουθούσαν να επιδεικνύουν τέτοιου είδους συμπεριφορές και να αδιαφορούν για την παραβίαση της ιδιωτικότητας τους, καθώς είναι σύνηθες τα άτομα να υποτιμούν τον ενδεχόμενο κίνδυνο πρόκλησης ζημίας και να προτιμούν το βραχυπρόθεσμο κέρδος παρά το γεγονός ότι ελλοχεύει ένας μακροπρόθεσμος κίνδυνος (*L. Barkhuus & A. Dey, 2003*).

3. ΠΑΡΑΔΕΙΓΜΑΤΑ ΤΕΧΝΟΛΟΓΙΩΝ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ ΣΤΗΝ ΚΑΘΗΜΕΡΙΝΗ ΖΩΗ

3.1. Τεχνολογίες παρακολούθησης στο πλαίσιο διαχείρισης της πανδημίας του covid

Το 2020, στο πλαίσιο της εξαιρετικά επείγουσας και απρόβλεπτης ανάγκης αντιμετώπισης των αρνητικών συνεπειών λόγω της εμφάνισης του κορωνοϊού, covid-19, και ειδικότερα στο πλαίσιο περιορισμού της διάδοσής του και λήψης συναφών αναγκαίων μέτρων κατέστη αναγκαία η ανάπτυξη τεχνολογικών εργαλείων που θα μπορούσαν να αντιμετωπίσουν αυτό το φαινόμενο. Ως εκ τούτου, κρίθηκε ότι η πρωτόγνωρη αυτή κατάσταση απαιτούσε την κατανόηση των διαθέσιμων επιλογών και τεχνολογιών για να σταματήσει η εξάπλωση της πανδημίας. Για παράδειγμα, η αναγνώριση προσώπου, αντί της σάρωσης της ίριδας και

των δακτυλικών αποτυπωμάτων, και η χρήση θερμικών καμερών μείωσαν τις ευκαιρίες για σωματική επαφή (Gambino A. και Tuzzolino D., 2021), ενώ οι κυβερνήσεις και οι ιδιωτικοί φορείς στράφηκαν προς την υιοθέτηση λύσεων που βασίζονταν σε επεξεργασία δεδομένων υποκειμένων των δεδομένων σε μεγάλη κλίμακα, ως μέρος της απάντησης στην πανδημία covid-19. Στην παγκόσμια κατάσταση έκτακτης ανάγκης που σχετιζόταν με την εξάπλωση της πανδημίας covid-19, η κατανόηση και η ανακάλυψη μοτίβων που θα μπορούσαν να βοηθήσουν στην κατανόηση της ανθρώπινης συμπεριφοράς αποτέλεσε σημαντική πρόκληση για τον έλεγχο της πανδημίας. Ο συνδυασμός δεδομένων από τον φυσικό και τον διαδικτυακό κόσμο οδήγησε στην ανάπτυξη μοντέλων συμπεριφοράς που μελετούσαν την κυκλοφορία προσώπων, την κοινωνία, την οικονομία, καθώς και τον αντίκτυπο που είχε ο covid-19 σε αυτούς τους τομείς. Τα δεδομένα που αφορούσαν στην καθημερινή ζωή των χρηστών, την προσαρμοσμένη στις συνθήκες της περιόδου εκείνης συμπεριφορά τους και τις προβλέψεις για τις μετακινήσεις συνέβαλαν στη διαχείριση των πληροφοριών με σκοπό την απόκτηση αποτελεσμάτων που βοηθούσαν στην κατανόηση μεγάλων ομάδων χρηστών.

3.1.1. Ψηφιακή Ιχνηλάτηση επαφών

Για την καταπολέμηση της νόσου covid-19, χρησιμοποιήθηκαν τεχνολογίες που αποσκοπούσαν, μεταξύ άλλων, στην επεξεργασία δεδομένων θέσης με σκοπό την υποστήριξη της αντιμετώπισης της πανδημίας μέσω μοντελοποίησης της διασποράς του ιού, κατά τρόπο ώστε να αξιολογηθεί η συνολική αποτελεσματικότητα των μέτρων εγκλεισμού, όπως και στην ιχνηλάτηση επαφών, ώστε να ειδοποιούνται άμεσα πρόσωπα που είχαν έρθει σε επαφή με κάποιον που εν συνεχεία διαγνώστηκε επιβεβαιωμένα ως φορέας του ιού, ώστε να είναι εφικτό να διακοπεί το συντομότερο δυνατό η αλυσίδα μετάδοσης του ιού. Όπως, ανέφερε και το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ), στις υπ' αριθμ. 4/2020 Κατευθυντήριες Γραμμές που εξέδωσε, οι βασικές πηγές άντλησης δεδομένων θέσης, για τη μοντελοποίηση της διασποράς του covid-19 και της αποτελεσματικότητας των ληφθέντων μέτρων, είναι τα δεδομένα θέσης, που συλλέγονται από τους παρόχους ηλεκτρονικών επικοινωνιών, κατά την παροχή υπηρεσιών καθώς και τα δεδομένα θέσης που συλλέγονται από παρόχους υπηρεσιών της κοινωνίας των πληροφοριών, στο πλαίσιο εγκατάστασης και λειτουργίας εφαρμογών που χρησιμοποιούν τέτοιου είδους δεδομένα. Σε αυτό το πλαίσιο, οι εφαρμογές υγείας διαδραμάτισαν και εξακολουθούν να διαδραματίζουν σημαντικό ρόλο. Από τις εφαρμογές κινητών τηλεφώνων με στόχο την πρόληψη, τη

διάγνωση και την ιατρική βοήθεια εξ αποστάσεως έως τις εφαρμογές που χρησιμοποιούνται για συσκευές παρακολούθησης, η χρήση των εν λόγω εφαρμογών κατέστη χρήσιμη για την αντιμετώπιση της κρίσης. Ο εντοπισμός επαφών αποτελούσε ανέκαθεν σημαντικό μέσο για την πρόληψη και τον έλεγχο της εξάπλωσης των μεταδοτικών ασθενειών. Ο ψηφιακός εντοπισμός επαφών, χρησιμοποιώντας πρόσβαση σε βάσεις δεδομένων και τεχνολογίες εντοπισμού - όπως το GPS, το Wi-Fi ή το Bluetooth - είναι δυνατόν να συλλέξει δεδομένα για να εξάγει πληροφορίες σχετικά με την ταυτόχρονη παρουσία ατόμων σε ένα συγκεκριμένο μέρος. Πολλές χώρες επένδυσαν στην ανάπτυξη εφαρμογών ψηφιακής ανίχνευσης επαφών, αν και με διαφορετικές προσεγγίσεις η κάθε μία. Ωστόσο, αυτές οι εφαρμογές έχουν προκαλέσει αμφιβολίες και ανησυχίες, σχεδόν σε ολόκληρο τον κόσμο, σχετικά με τις επιπτώσεις στον ιδιωτικό βίο και την προστασία των προσωπικών δεδομένων εν γένει. Αναμφισβήτητα, η εφαρμογή των αρχών - όπως η αναλογικότητα της συλλογής, η προηγούμενη συγκατάθεση, η ελαχιστοποίηση, η διαφάνεια, η ανωνυμοποίηση και η λογοδοσία - συστήθηκε σε όλες τις έννομες τάξεις.

3.1.2. Παρακολούθηση τήρησης κανόνων αποστασιοποίησης

Ενδεικτικό της σημαντικής αναστάτωσης στην καθημερινή ζωή των ατόμων σε όλο τον κόσμο που προκάλεσε η πανδημία covid-19 είναι ότι μόλις έξι (6) μήνες μετά την εμφάνιση της πανδημίας, υπήρχαν ήδη 19,8 εκατομμύρια επιβεβαιωμένα κρούσματα παγκοσμίως με περισσότερες από 730 χιλιάδες θανάτους. Επιπλέον, η πανδημία αυτή επέφερε σημαντικές οικονομικές και κοινωνικές επιπτώσεις. Ένας από τους καλύτερους τρόπους για την πρόληψη της προσβολής από τον covid-19 θεωρήθηκε, ως ήταν λογικό, η αποφυγή έκθεσης στον ιό. Ο παγκόσμιος οργανισμός υγείας συνέστησε πολλές σχετικές οδηγίες, όπως η διατήρηση κοινωνικών αποστάσεων, η χρήση μάσκας ή άλλων καλυμμάτων προσώπου και το συχνό πλύσιμο των χεριών, ώστε να μειωθούν οι πιθανότητες μόλυνσης ή εξάπλωσης του ιού. Την περίοδο εκείνη, η διατήρηση των κανόνων κοινωνικής αποστασιοποίησης μεταξύ των ανθρώπων, δεν ήταν απλά ζητούμενο, είχε καταστεί απαραίτητο μέτρο προφύλαξης για την επιβράδυνση της μετάδοσης του covid-19. Σε γενικές γραμμές, η κοινωνική αποστασιοποίηση αναφέρεται στα μέτρα που λαμβάνονται για να μειωθεί η συχνότητα επαφής των ανθρώπων μεταξύ τους. Οι ερευνητικές ομάδες που είχαν προβεί σε προσομοίωση της εξάπλωσης του ιού κατέληξαν στο συμπέρασμα ότι η κοινωνική

αποστασιοποίηση μπορούσε να μειώσει σημαντικά τον συνολικό αριθμό των μολυσμένων κρουσμάτων.

Βασικό ζήτημα αποτέλεσε η ανάπτυξη κατευθυντήριων γραμμών και μεθόδων για την επιβολή αυτών των περιορισμών κοινωνικής απόστασης σε δημόσιες ή ιδιωτικές συγκεντρώσεις σε εσωτερικούς ή εξωτερικούς χώρους. Το γεγονός αυτό, δημιούργησε πολλές προκλήσεις, όπως ενδεικτικά, η διαμόρφωση εύλογων κανόνων που τα άτομα έπρεπε να ακολουθήσουν όταν χρησιμοποιούσαν δημόσιους χώρους και ο τρόπος με τον οποίο τα άτομα θα ενθαρρύνονταν για να ακολουθήσουν τους νέους αυτούς κανόνες. Ζήτημα ζωτικής σημασίας, θεωρήθηκε και ο εντοπισμός των περιπτώσεων παραβίασης των κανόνων αυτών, ώστε να μπορούν να εφαρμοστούν τα κατάλληλα αντίμετρα, δεδομένου ότι η ανίχνευση των παραβιάσεων της κοινωνικής απόστασης μπορούσε επίσης να βοηθήσει στον εντοπισμό επαφών.

Στο πλαίσιο, λοιπόν της διασφάλισης της κοινωνικής αποστασιοποίησης, παρουσιάστηκαν και χρησιμοποιήθηκαν ποικίλες μέθοδοι, για την αυτόματη ανίχνευση - σε σενάριο συνωστισμού - ζευγαριών ατόμων που δεν τηρούσαν τον περιορισμό της κοινωνικής απόστασης, δηλαδή περίπου 1,5 με 2 μέτρα (όσο περίπου είναι η έκταση των χεριών ενός ενήλικα), κατά τη συναναστροφή με όσους δεν ανήκαν στο στενό οικογενειακό περιβάλλον. Για την ανίχνευση υπερβολικού συνωστισμού ή την ανίχνευση επαφών προτάθηκαν πολλές τεχνολογίες οι περισσότερες εκ των οποίων αξιοποιούσαν το WiFi, το Bluetooth, ή τον εντοπισμό μέσω σύνδεσης κινητής τηλεφωνίας και άλλα. Οι περισσότερες από τις προαναφερόμενες τεχνολογίες λειτουργούν αποτελεσματικά μόνο σε εσωτερικούς χώρους, ενώ άλλες από αυτές απαιτούν πρόσθετη υποδομή ή συσκευές για τον εντοπισμό ατόμων σε εσωτερικούς χώρους. Σε άλλες περιπτώσεις, οι τεχνολογίες όπως το WiFi και το Bluetooth είναι χρήσιμες για την παρακολούθηση μόνο των ατόμων που είναι συνδεδεμένα με τις εν λόγω τεχνολογίες μέσω κινητών συσκευών και συγκεκριμένα smartphones. Το γεγονός αυτό περιορίζει τη χρήση τους για την παρακολούθηση πλήθους και των κανόνων κοινωνικής απόστασης σε ευρύ περιβάλλον ή δημόσιους χώρους και μπορεί να εμποδίσει τη χρήση οποιουδήποτε είδους αντιμέτρων. Ερευνητικές ομάδες (*Sathyamoorthy* 2020), παρουσίασαν ένα κινητό ρομπότ με οπτική καθοδήγηση (covid-robot) για την παρακολούθηση σεναρίων με πλήθος ανθρώπων χαμηλής ή υψηλής πυκνότητας και παρατεταμένη επαφή μεταξύ τους. Χρησιμοποιήθηκε ένας αλγόριθμος προηγμένης τεχνολογίας για την αυτόνομη

πλοήγηση του ρομπότ χωρίς συγκρούσεις σε αυθαίρετα σενάρια, ο οποίος χρησιμοποιούσε τον υβριδικό συνδυασμό μιας μεθόδου Βαθιάς Ενισχυτικής Μάθησης και μιας παραδοσιακής μεθόδου βασισμένης σε μοντέλα. Περαιτέρω χρησιμοποιήθηκαν αλγόριθμοι ανίχνευσης και παρακολούθησης πεζών κινούμενων στο χώρο με σκοπό την ανίχνευση ομάδων ανθρώπων που βρίσκονταν στο οπτικό πεδίο της κάμερας που είχαν απόσταση μικρότερη της προκαθορισμένης απόφασης - κανόνα (6 ft) μεταξύ τους.

Μόλις εντοπίζονταν παραβιάσεις της καθορισμένης απόστασης, το ρομπότ ταξινομούσε τις ομάδες με βάση το μέγεθός τους, κινούνταν στη σχετική ομάδα ατόμων και παρότρυνε την τήρηση των κανόνων κοινωνικής απόστασης με την εμφάνιση ενός μηνύματος προειδοποίησης σε μια τοποθετημένη οθόνη. Για τα άτομα που κινούνταν στο χώρο και δεν συμμορφώνονταν με την προκαθορισμένη απόσταση, το ρομπότ τους ακολουθούσε, ενώ παράλληλα εμφάνιζε προειδοποιήσεις για την μη τήρηση της απόστασης. Το ρομπότ χρησιμοποιούσε οπτικούς αισθητήρες μικρής χρηματικής αξίας, ώστε να πλοηγείται και να ταξινομεί τα περιφερόμενα άτομα που παραβιάζουν τους περιορισμούς κοινωνικής απόστασης ως μη συμμορφούμενους πεζούς. Σε σενάρια εσωτερικών χώρων, το ρομπότ χρησιμοποιούσε τη ρύθμιση της κάμερας CCTV (εφόσον ήταν διαθέσιμη) για να βελτιώσει περαιτέρω την ακρίβεια ανίχνευσης και να ελέγξει μια μεγαλύτερη ομάδα κινούμενων στο χώρο ατόμων σχετικά με τυχόν παραβιάσεις των κοινωνικών περιορισμών απόστασης. Χρησιμοποιούνταν επίσης μια θερμική κάμερα, η οποία ήταν τοποθετημένη στο ρομπότ με σκοπό την ασύρματη μετάδοση θερμικών εικόνων, που συνέβαλε στον εντοπισμό ατόμων που ενδέχεται να είχαν υψηλή θερμοκρασία χωρίς όμως να αποκαλύπτεται η ταυτότητά τους για να προστατεύονται οι ευαίσθητες πληροφορίες που τους αφορούν, ήτοι τα δεδομένα υγείας.

Ουσιαστικά δηλαδή, η μέθοδος που αναπτύχθηκε, περιελάμβανε το σύστημα κινητού ρομπότ που ανίχνευε παραβιάσεις των κανόνων κοινωνικής απόστασης, πλοηγείτο αυτόνομα προς ομάδες μη συμμορφούμενων ανθρώπων και τους ενθάρρυνε να διατηρούν την προκαθορισμένη απόσταση χωρίς να απαιτείτο τα συγκεκριμένα άτομα να φέρουν μαζί τους κάποια συσκευή εντοπισμού ή φορητές συσκευές, μία ενσωματωμένη στο ρομπότ εγκατάσταση CCTV ώστε να παρακολουθείται μεγαλύτερη περιοχή και να βελτιωθεί η ακρίβεια του εντοπισμού και της παρακολούθησης μη συμμορφούμενων με τον κανόνα ατόμων. Ο υβριδικός αυτός συνδυασμός στατικά τοποθετημένων καμερών και ενός κινητού

ρομπότ συνέβαλε σύμφωνα με τους ερευνητές στην επίτευξη μεγαλύτερου αριθμού εντοπιζόμενων παραβάσεων και επιβολών έως και 100%. Η συγκεκριμένη μέθοδος υπολογισμού των αποστάσεων μεταξύ των ανθρώπων σε πραγματικό χρόνο που βασίστηκε σε εικόνες που έχουν ληφθεί με τη χρήση κάμερας στο ρομπότ και κάμερας CCTV, σε εσωτερικούς χώρους έχει μέσο όρο σφάλματος 0,3 ft. Η ενσωμάτωση θερμικής κάμερας στο ρομπότ αποσκοπούσε στην εν συνεχεία ασύρματη μετάδοση των εικόνων στο κατάλληλο προσωπικό ασφαλείας/υγειονομικής περίθαλψης. Το ρομπότ δεν κατέγραφε θερμοκρασίες ούτε διενεργούσε οποιαδήποτε μορφή αναγνώρισης προσώπων, που οδηγούσε σε ταυτοποίηση των ατόμων.

3.1.3. Η θέση των ευρωπαϊκών οργάνων

Δεδομένης της επείγουσας κατάστασης και της μεγάλης κλίμακας επεξεργασίας δεδομένων στο πλαίσιο διαχείρισης της πανδημίας, στην Ευρώπη, τόσο η Ευρωπαϊκή Επιτροπή όσο και το ΕΣΠΔ διατύπωσαν τη θέση τους σχετικά με τις μεθόδους ψηφιακής ανίχνευσης επαφών.

Η πρώτη εξέδωσε σύσταση «*σχετικά με μια κοινή εργαλειοθήκη της Ένωσης για τη χρήση της τεχνολογίας και των δεδομένων με σκοπό την καταπολέμηση της κρίσης COVID-19 και την έξοδο από αυτή, ιδίως όσον αφορά εφαρμογές για φορητές συσκευές και τη χρήση ανωνυμοποιημένων δεδομένων κινητικότητας*», στην οποία η Επιτροπή εξέφρασε την προτίμησή της για τη συλλογή δεδομένων εγγύτητας αντί για δεδομένα θέσης σχετικά με τη θέση και τις κινήσεις ενός ατόμου. Η ίδια θέση εκφράστηκε και στις Κατευθυντήριες γραμμές του ΕΣΠΔ, που προαναφέρθηκαν, σχετικά με τις εφαρμογές που υποστηρίζουν την καταπολέμηση της πανδημίας covid-19 σε σχέση με την προστασία των δεδομένων, στην οποία εξέφρασε προτίμηση για τον εντοπισμό επαφών με τη χρήση Bluetooth Low Energy, αντί της χρήσης δεδομένων γεωγραφικού εντοπισμού.

Η θέση αυτή, είναι σε απόλυτη συμμόρφωση, με το πνεύμα και τις προβλέψεις της νομοθεσίας περί προστασίας προσωπικών δεδομένων, καθώς σύμφωνα με την αρχή της αναλογικότητας («ελαχιστοποίηση των δεδομένων») τα δεδομένα πρέπει να είναι κατάλληλα, συναφή και να περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία («ελαχιστοποίηση των δεδομένων»). Τα δεδομένα θέσης προσφέρουν μια συνολική εικόνα της κίνησης των προσώπων και οι πληροφορίες αυτές μπορούν να είναι χρήσιμες τόσο στην αξιολόγηση των μέτρων περιορισμού, όπως ο

εγκλεισμός και η μείωση των μετακινήσεων, όσο και στο πλαίσιο της ψηφιακής ανίχνευσης επαφών. Στον τομέα της ψηφιακής ανίχνευσης επαφών, τα δεδομένα εγγύτητας πρέπει να είναι διακριτά από τα δεδομένα γεωγραφικής θέσης. Τα δεδομένα εγγύτητας παράγονται από την ανταλλαγή Bluetooth Low Energy μεταξύ των πλησιέστερων συσκευών και αποκαλύπτουν τη σχετική θέση. Αντίθετα, τα δεδομένα γεωγραφικού εντοπισμού αξιοποιούν πληροφορίες σχετικά με τις γεωγραφικές συντεταγμένες που προκύπτουν μέσω GPS ή άλλων μεθόδων που αναφέρθηκαν παραπάνω, παρέχοντας την απόλυτη θέση ενός προσώπου σε έναν χάρτη. Το Bluetooth Low Energy αποτρέπει τη δυνατότητα εντοπισμού των ατόμων και εξετάζει την επαφή μόνο από επιδημιολογική άποψη, ενώ παράλληλα τα δεδομένα που συλλέγονται αποθηκεύονται απευθείας στη συσκευή. Αντίθετα, τα δεδομένα γεωγραφικού εντοπισμού μπορούν να προσφέρουν πρόσθετες πληροφορίες σχετικά με το πλαίσιο στο οποίο έλαβε χώρα η σχετική επαφή, παρέχοντας ενδείξεις σχετικά με την πιθανή διάδοση του ιού.

Περαιτέρω, το ΕΣΠΔ, στις κατευθυντήριες γραμμές που εξέδωσε σχετικά με τη χρήση δεδομένων θέσης και εργαλείων εντοπισμού επαφών στο πλαίσιο της έξαρσης της πανδημίας του covid-19 - εξέφρασε τις ανησυχίες του σχετικά με τις εφαρμογές ψηφιακής ανίχνευσης επαφών. Η χρήση του εν λόγω μέσων, σύμφωνα με το ΕΣΠΔ υπόκειται, στην τήρηση συγκεκριμένων κριτηρίων, όπως ενδεικτικά η μη υποχρεωτική χρήση τους, η διενέργεια μελέτης εκτίμησης αντίκτυπου (DPIA) πριν από την χρήση τους, η προτίμηση σε δεδομένα εγγύτητας, η αποκάλυψη πληροφοριών σχετικά με το με ποια άτομα έχει έρθει σε στενή επαφή το προσβεβλημένο από τον ιό πρόσωπο, την ελαχιστοποίηση των δεδομένων και την προστασία των δεδομένων από το σχεδιασμό, η χρήση κρυπτογραφημένων αναγνωριστικών που παράγονται από το Bluetooth Low Energy, η διατήρηση της ανωνυμίας των εμπλεκόμενων τρίτων χρηστών κ.α.. Από τη σκοπιά της προστασίας του ιδιωτικού βίου, η συνεχής επεξεργασία δεδομένων γεωγραφικού εντοπισμού αποδεικνύεται επεμβατική. Η μεγάλης κλίμακας παρακολούθηση και επεξεργασία των δεδομένων θέσης δημιουργεί το έδαφος για να ανοίξουν συζητήσεις σχετικά με τους προβληματισμούς αναφορικά με την ισορροπία μεταξύ της προστασίας της υγείας και της ιδιωτικής ζωής. Σε αυτές τις περιπτώσεις, απαιτείται αναλογικότητα των μέσων για την επίτευξη των επιδιωκόμενων στόχων. Λαμβάνοντας δεόντως υπ' όψιν τις ιδιαιτερότητες των δεδομένων θέσης, τη δυσκολία ανωνυμοποίησής τους και τον αποκαλυπτικό τους χαρακτήρα, η συντριπτική

πλειονότητα των αποφάσεων με γνώμονα την προστασία της ιδιωτικής ζωής κλίνει προς τη συλλογή δεδομένων εγγύτητας. Όμως, από συγκριτική άποψη, υπάρχουν παραδείγματα εφαρμογών γεωγραφικού εντοπισμού που δεν έχουν παρεμβατική επίδραση στη ζωή των ατόμων, που παρέχουν τη δυνατότητα ανάκλησης των δεδομένων γεωγραφικού εντοπισμού που έχουν καταγραφεί τοπικά εντός συγκεκριμένου χρονικού διαστήματος.

Όπως γίνεται κατανοητό, από τα ανωτέρω αναφερόμενα, στην περίοδο της πανδημίας του covid-19, εισήλθαμε σε ένα νέο στάδιο όπου μεγάλοι όμιλοι εταιρειών, είχαν τη δυνατότητα να συλλέξουν και συνέλλεξαν μεγάλο όγκο δεδομένων και απέκτησαν πρόσβαση στον παγκόσμιο έλεγχο του πλήθους και στη διαχείριση πληροφοριών. Η κατάσταση αυτή, θα μπορούσε να επηρεάσει σε μεγάλο βαθμό, τη σχέση των δημοκρατιών με τους μεγάλους ομίλους εταιρειών. Η διαχείριση των πληροφοριών σε κατάσταση έκτακτης ανάγκης, όπως ήταν αυτή του covid-19, πρέπει να καθίσταται η Νο 1 προτεραιότητα για τα θεσμικά όργανα που στοχεύουν στην επίλυση των προβλημάτων που αντιμετωπίζει η κοινωνία. Η κατάλληλη διαχείριση των πληροφοριών και των δεδομένων που συνδέονται με αυτές αποτελούν βασικά στοιχεία για την ανάπτυξη πρωτοκόλλων επικοινωνίας που σέβονται την ιδιωτική ζωή των χρηστών και ανταποκρίνονται στις ανάγκες υγειονομικών ή κοινωνικών κρίσεων. Συνεπώς, η κατάλληλη διαχείριση του σχηματισμού πρέπει να αναλύεται τόσο από την άποψη της ιδιωτικότητας των χρηστών όσο και από την άποψη της απόκτησης και του ελέγχου των πληροφοριών (*Wang et al. 2020*). Ως εκ τούτου, στο πλαίσιο της πανδημίας, οι χρήστες θα έπρεπε να γνωρίζουν τα όρια και τις διαθέσιμες επιλογές όσον αφορά τη χρήση των δεδομένων τους σε νέες προσεγγίσεις μαζικού ελέγχου, με την εφαρμογή νέων τεχνολογιών, που προτείνονταν από κυβερνήσεις και ιδιωτικούς φορείς. Ως εκ τούτου, οι τεχνολογίες αυτές μπορούν να προκαλέσουν δραματικές κοινωνικές, πολιτικές και οικονομικές αλλαγές παγκοσμίως. Στο συγκεκριμένο πλαίσιο, είναι σημαντικό να κατανοήσουμε ποιες τεχνολογίες μπορούν να βοηθήσουν στη συλλογή δεδομένων από κινητές εφαρμογές, smartphones και συνδεδεμένες συσκευές. Κάθε μία από αυτές τις τεχνολογίες μπορεί να παρέχει πληροφορίες στις εταιρείες και τα ιδρύματα για τη λήψη αποφάσεων σχετικά με την ιχνηλασιμότητα και το επίπεδο των πληροφοριών που συλλέγονται, τόσο για την παρακολούθηση του covid-19 όσο και για μελλοντικές πανδημίες. Οι πηγές των δεδομένων και το επίπεδο πολυπλοκότητας των τεχνολογιών κινητής τηλεφωνίας που χρησιμοποιούνται για την παρακολούθηση των χρηστών και τη λήψη

πληροφοριών αποτελεί προϋπόθεση για την ανάπτυξη κατάλληλων στρατηγικών που σέβονται την ιδιωτική ζωή των χρηστών. Με πρόφαση τις νέες συνθήκες που διευρύνουν τις δυνατότητες των εταιρειών να παρακολουθούν και να διαχειρίζονται τα προσωπικά δεδομένα των χρηστών, οι ανταποκρινόμενες τεχνικές μπορούν αργότερα να επεκταθούν και σε άλλους σκοπούς (*Ribeiro-Navarrete S., Saura J., Palacios-Marques D., 2021*). Βρισκόμαστε σε μια εποχή όπου οι ευαισθητοποιημένες κοινωνίες οφείλουν να δημιουργήσουν και να μοιραστούν ένα νομικό πλαίσιο που να καθορίζει τα οφέλη της τεχνολογίας για τη μαζική επιτήρηση με βάση τα δεδομένα. Η δημόσια υγεία μπορεί να αποτελέσει στοιχείο επιτήρησης για τον έλεγχο του covid-19 και μελλοντικών πανδημιών, με ή χωρίς τη συλλογή δεδομένων σε βάθος χρόνου.

Ειδικά, ως προς την επεξεργασία δεδομένων θέσης κατά την περίοδο της πανδημίας του covid-19, το ΕΣΠΔ, επεσήμανε ότι τα δεδομένα θέσης που συλλέγονται από παρόχους ηλεκτρονικών επικοινωνιών εμπίπτουν στο πεδίο εφαρμογής των άρθρων 6 και 9 της Οδηγίας 2002/58/ΕΚ, και πρέπει να υποβάλλονται σε επεξεργασία σύμφωνα με τις προβλέψεις των άρθρων αυτών. Στο πλαίσιο των διατάξεων αυτών, η διαβίβαση των δεδομένων που υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού ενός χρήστη, χωρίς να περιλαμβάνονται σε αυτά δεδομένα μετακίνησης, σε τρίτα μέρη, μεταξύ των οποίων και οργανισμοί και αρχές, πραγματοποιείται κατόπιν παροχής προηγούμενης συγκατάθεσης από τους χρήστες. Αναφορικά με τις πληροφορίες και τα δεδομένα θέσης, που συλλέγονται απευθείας από τον τερματικό εξοπλισμό, πρέπει να εφαρμόζεται το άρθρο 5 παράγραφος 3 της Οδηγίας 2002/58/ΕΚ και συνεπώς, τυχόν αποθήκευση πληροφοριών στη συσκευή ενός χρήστη, όπως και τυχόν πρόσβαση σε πληροφορίες που έχουν αποθηκευθεί στη συσκευή του χρήστη επιτρέπεται εφόσον, ο εκάστοτε χρήστης έχει παράσχει τη συγκατάθεσή του σχετικά ή εφόσον η πρόσβαση στις πληροφορίες αυτές ή/και η αποθήκευσή τους είναι απολύτως αναγκαία για την παροχή της υπηρεσίας της κοινωνίας των πληροφοριών την οποία ο χρήστης ρητά έχει αιτηθεί. Σημειώνεται ότι στην Οδηγία 2002/58/ΕΚ, προβλέπονται παρεκκλίσεις ως προς τα δικαιώματα και τις υποχρεώσεις. Ειδικά, ως προς την εκ νέου χρήση δεδομένων θέσης, τα οποία έχουν συλλεχθεί από παρόχους υπηρεσιών της κοινωνίας των πληροφοριών, π.χ. από ήδη εγκατεστημένες εφαρμογές, πρέπει να πληρούνται περαιτέρω προϋποθέσεις.

Εν κατακλείδι, το ΕΣΠΔ κατέληγε στο συμπέρασμα ότι τα δεδομένα και η τεχνολογία που χρησιμοποιούνται για να βοηθήσουν στην καταπολέμηση της νόσου COVID-19 θα πρέπει να χρησιμοποιούνται με σκοπό να προσφέρουν δυνατότητες για τη διαχείριση της πανδημίας, και όχι με σκοπό τον έλεγχο, τον περιορισμό ή ακόμα και τον στιγματισμό των ατόμων και επεσήμανε την ανάγκη ανάπτυξης. Το νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων έχει σχεδιασθεί με γνώμονα να είναι ευέλικτο και να μπορεί να συμβάλλει στη διαχείριση και τον περιορισμό των εκάστοτε κρίσεων διασφαλίζοντας παράλληλα των θεμελιωδών δικαιώματων και ελευθεριών των ανθρώπων. Καθίσταται σαφές ότι, παρότι τα δεδομένα και η τεχνολογία μπορούν να αποτελέσουν χρήσιμα εργαλεία, ενέχουν εγγενείς περιορισμούς. Κατά την επεξεργασία προσωπικών δεδομένων, σε περιόδους διαχείρισης κρίσεων, πόσω μάλλον δεδομένων θέσης, οδηγός πρέπει να είναι οι αρχές της αποτελεσματικότητας, της αναγκαιότητας και της αναλογικότητας, καθώς η προστασία των δεδομένων είναι απολύτως απαραίτητη «*για την οικοδόμηση εμπιστοσύνης, τη δημιουργία των προϋποθέσεων για την κοινωνική αποδοχή οποιασδήποτε λύσης και, συνεπώς, για την εγγύηση της αποτελεσματικότητας των εν λόγω μέτρων*».

3.2. Η περίπτωση των «έξυπνων πόλεων»

Μια από τις μεγαλύτερες αλλαγές των τελευταίων ετών είναι η εμφάνιση του Διαδικτύου των Πραγμάτων (Internet of Things - IoT) και των έξυπνων συσκευών που αποτελούν αναπόσπαστο κομμάτι της καθημερινής ζωής. Ο ρόλος τους είναι πολλαπλός, βελτιώνουν την ποιότητα ζωής των ανθρώπων ειδικά στις μεγάλες πόλεις, διευκολύνουν την καθημερινότητά τους με διάφορες εφαρμογές και λύσεις, συλλέγοντας δεδομένα μέσω αισθητήρων, μπορούν ακόμη και να δημιουργήσουν μια ολόκληρη έξυπνη πόλη με σπουδαίες εφαρμογές. Με το 54% του παγκόσμιου πληθυσμού να ζει σε αστικές περιοχές, η έννοια της έξυπνης πόλης έχει καταστεί απολύτως απαραίτητη για την ανθρωπότητα.

Ο τρόπος με τον οποίο λειτουργούν τα συστήματα IoT βασίζεται σε αισθητήρες και συσκευές που συλλέγουν δεδομένα και τα μεταφέρουν στο cloud ή στο διαδίκτυο μέσω κάποιου είδους συνδεσιμότητας. Μόλις τα δεδομένα φτάσουν στο cloud, το λογισμικό τα επεξεργάζεται και στη συνέχεια μπορεί να αποφασίσει να δράσει, όπως η αποστολή μιας ειδοποίησης ή η αυτόματη ρύθμιση των αισθητήρων/συσκευών χωρίς να χρειάζεται ο χρήστης. Γίνεται

κατανοητό ότι οι συσκευές IoT δεν έχουν καμία χρησιμότητα χωρίς δεδομένα, οπότε τα δεδομένα είναι ιδιαίτερα σημαντικά για τη λειτουργία των συσκευών αυτών. Πόσο ασφαλής όμως είναι αυτός ο τρόπος ζωής; Γνωρίζουν οι άνθρωποι ότι υπάρχουν περιπτώσεις όπου θυσιάζουν την ιδιωτικότητά τους για να έχουν έναν - θεωρητικά - καλύτερο τρόπο ζωής;

3.2.1. Έννοια και αρχιτεκτονική «έξυπνης πόλης»

Μετά από αυτή την εισαγωγή, παρουσιάζεται η έννοια της έξυπνης πόλης καθώς και το δικαίωμα στην πόλη, ενώ ακολουθεί συζήτηση για τη συμμετοχή του κοινού στις έξυπνες πόλεις (ή τη συμμετοχική δημιουργία πόλεων) και τις εννοιολογικές προκλήσεις όσον αφορά τα δικαιώματα προστασίας δεδομένων στο πλαίσιο της Ευρωπαϊκής Ένωσης. Είναι σχεδόν αδύνατο να δοθεί ένας εξαντλητικός, καθολικά αποδεκτός ορισμός για την έξυπνη πόλη. Η παροχή μιας υπηρεσίας έξυπνης πόλης μπορεί να χαρακτηριστεί ως μία λύση για ένα κοινωνικό πρόβλημα που βασίζεται σε τεχνολογία που αλληλεπιδρά με τον φυσικό κόσμο, όπου η συλλογή και η χρήση δεδομένων είναι καίριας σημασίας και στην οποία εμπλέκονται διάφοροι παράγοντες, δημόσιοι και ιδιωτικοί. Υπάρχουν διάφοροι ορισμοί για το τι κάνει μια πόλη "έξυπνη", εν συντομία η έξυπνη πόλη, χρησιμοποιεί ένα πλαίσιο τεχνολογιών πληροφορικής και επικοινωνιών για τη δημιουργία, την ανάπτυξη και την προώθηση αναπτυξιακών πρακτικών για την αντιμετώπιση των αστικών προκλήσεων και τη δημιουργία μιας τεχνολογικά ενεργοποιημένης και βιώσιμης υποδομής. Επιπλέον, οι έξυπνες πόλεις συνδυάζουν την αυτοματοποίηση, την εκμάθηση μηχανών (machine learning) και το IoT για την προσαρμογή των τεχνολογιών σε ποικίλες εφαρμογές. Ωστόσο, εξακολουθεί να είναι δύσκολο να διατυπωθεί ένας ορισμός της ορολογίας "έξυπνη πόλη". Ο καθηγητής Mark Deakin σε σχετικό άρθρο του απαριθμεί τέσσερις παράγοντες που συμβάλλουν στον ορισμό μιας έξυπνης πόλης, οι οποίοι είναι οι ακόλουθοι: (i) η εφαρμογή ενός ευρέος φάσματος ηλεκτρονικών και ψηφιακών τεχνολογιών στις κοινότητες και τις πόλεις, (ii) η χρήση των Τεχνολογιών Πληροφοριών και Επικοινωνιών (ΤΠΕ) για τον μετασχηματισμό της ζωής και του εργασιακού περιβάλλοντος στην περιοχή, (iii) η ενσωμάτωση αυτών των τεχνολογιών πληροφορικής και επικοινωνιών (ΤΠΕ) στα κρατικά συστήματα και (iv) η εδαφιοποίηση των πρακτικών που φέρνει σε επαφή τις ΤΠΕ και τους ανθρώπους για την ενίσχυση της καινοτομίας και της γνώσης που προσφέρουν. Οι έξυπνες πόλεις σχετίζονται πάντα με την ύπαρξη συσκευών IoT. Λόγω της πολυπλοκότητας της

αρχιτεκτονικής τους, είναι δύσκολο να δημιουργηθεί μια ενιαία δομή που θα ταιριάζει σε κάθε σύστημα που περιλαμβάνει συσκευές IoT.

Ποια είναι όμως η αρχιτεκτονική μίας έξυπνης πόλης; Είναι σημαντικό να κατανοήσουμε τι σημαίνει πρακτικά μια έξυπνη πόλη και πώς λειτουργεί. Είναι δύσκολο να συλλάβει κανείς μια γενική αρχιτεκτονική για τις έξυπνες πόλεις λόγω του εξαιρετικά ποικίλου φάσματος συσκευών, τεχνολογιών και υπηρεσιών που μπορεί να συνδέονται σε ένα τέτοιο σύστημα, καθώς και λόγω του υψηλού βαθμού αλληλεξάρτησης μεταξύ των διαφόρων στοιχείων (Jalali et al., 2015). Ως εκ τούτου, υπάρχουν πολλά διαφορετικά μοντέλα που εξετάζουν ποια στοιχεία και υποδομές χρειάζεται μια έξυπνη πόλη (Gaur, Scotney, Parr, & McClean, 2015). Η έξυπνη πόλη αποτελείται από τα εξής επίπεδα, το επίπεδο ανίχνευσης (sensing layer), το επίπεδο δικτύου (network layer), το επίπεδο εφαρμογών (application layer) και το επιχειρηματικό επίπεδο (business layer). Το επίπεδο ανίχνευσης (sensing layer) είναι το χαμηλότερο επίπεδο της αρχιτεκτονικής και χρησιμοποιείται κυρίως για δεδομένα που συλλέγονται από συσκευές όπως αισθητήρες, κάμερες κ.λπ. Μετά τη συλλογή, τα δεδομένα πρόκειται να μεταφερθούν για περαιτέρω επεξεργασία στο επόμενο επίπεδο, το οποίο είναι το επίπεδο δικτύου (network layer). Αυτό το επίπεδο μπορεί να περιγραφεί ως ο πυρήνας της αρχιτεκτονικής IoT, επειδή μπορεί να διαβιβάσει τα αρχικά δεδομένα στις συσκευές που είναι συνδεδεμένες στο δίκτυο, είτε η σύνδεση είναι ενσύρματη είτε ασύρματη. Για να λειτουργήσει σωστά το επίπεδο δικτύου, χρειάζεται υποστήριξη, η οποία είναι το επόμενο επίπεδο και ονομάζεται επίπεδο ενδιάμεσου λογισμικού (middleware layer) και περιλαμβάνει τεχνικές ευφυούς υπολογισμού, όπως η διεπαφή προγραμματισμού εφαρμογών (API) και βάσεις δεδομένων. Το επόμενο είναι το επίπεδο εφαρμογών (application layer), το οποίο παρέχει εφαρμογές ή υπηρεσίες στους χρήστες που βασίζονται στις εξατομικευμένες ανάγκες τους. Πάνω απ' όλα είναι το επιχειρηματικό επίπεδο (business layer), το οποίο είναι επιφορτισμένο με την ανάπτυξη στρατηγικών και τη διαμόρφωση πολιτικών που βοηθούν στη διαχείριση του συνολικού συστήματος. Ωστόσο, πέρα από αυτά τα πέντε επίπεδα, η αρχιτεκτονική των έξυπνων πόλεων βασίζεται σε τρεις τύπους λειτουργιών, οι οποίες αφορούν το επίπεδο του IoT πλαισίου στο οποίο μπορεί να πραγματοποιηθεί η επεξεργασία των δεδομένων, και οι οποίες είναι το Cloud Computing, το Fog Computing και το Edge Computing. Ο κύριος σκοπός κάθε σχεδιαστή συστήματος IoT

είναι να συνδυάσει με ισορροπία και τα τρία επίπεδα, λαμβάνοντας υπόψη το κόστος και τις απαιτήσεις του εκάστοτε συστήματος.

Το cloud ("υπολογιστικό νέφος") είναι ο χώρος που φιλοξενεί όλη την επεξεργασία των δεδομένων από τα επιμέρους στοιχεία του συστήματος IoT. Το πλεονέκτημα του cloud είναι η δυνατότητα αποακρυσμένης πρόσβασης σε αδιάλειπτες διαμοιραζόμενες πηγές, όπως υπολογιστές, αποθηκευτικό χώρο και υπηρεσίες μέσω δικτύου, από διάφορες πλατφόρμες. Επί της ουσίας, πρόκειται για συγκεντρωτικά συστήματα, τα οποία φιλοξενούν τόσο υπηρεσίες hardware όσο και υπηρεσίες software και παρέχουν κεντρικές πλατφόρμες διαχείρισης για τον έλεγχο του όγκου των δεδομένων που λαμβάνουν, ενώ παράλληλα επιτρέπουν στα συστήματα cloud να διαθέτουν επαρκώς μεγάλες υπολογιστικές και αποθηκευτικές ικανότητες, γεγονός που τους δίνει τη δυνατότητα να εκτελούν σύνθετες εργασίες εξαγωγής δεδομένων, προτύπων και συμπερασμάτων από τα στοιχεία αισθητήρων στις έξυπνες πόλεις, ώστε να αξιοποιούνται με τον καλύτερο δυνατό τρόπο. Ωστόσο, το cloud εμφανίζει κάποια μειονεκτήματα τις περισσότερες φορές λόγω της διαβίβασης μεγάλου όγκου δεδομένων. Η διαβίβαση όλων των δεδομένων που συλλέγονται από διάφορες εφαρμογές στο cloud αυξάνει την επισκεψιμότητα του δικτύου και επιβαρύνει άμεσα το κόστος του. Επιπλέον, λόγω των πολλών εφαρμογών, αισθητήρων και δεδομένων, εμφανίζεται Επιπλέον, λόγω των πολλών εφαρμογών, αισθητήρων και δεδομένων, εμφανίζεται χρονική υστέρηση στη ροή των δεδομένων, ιδίως όταν πολλές συσκευές αρχίζουν να αποστέλλουν ταυτόχρονα δεδομένα στο cloud, επειδή οι μονάδες ανίχνευσης υπάρχουν στο επίπεδο ανίχνευσης και η λήψη αποφάσεων/επεξεργασία δεδομένων πραγματοποιείται στο cloud.

Το fog computing προσφέρει μια πιο διαφοροποιημένη κατανομή αρμοδιοτήτων από ό,τι υπαγορεύεται από την αρχιτεκτονική του cloud computing, μεταφέροντας μέρος της επεξεργασίας σε συσκευές στο τοπικό δίκτυο. Λόγω των αυξημένων υπολογιστικών δυνατοτήτων που προσφέρει το fod computing, είναι παρέχει λειτουργίες όπως η συγκέντρωση και η συλλογή δεδομένων αισθητήρων, απλές λειτουργίες επεξεργασίας και λήψη αποφάσεων που μπορεί να πραγματοποιηθεί για τη μείωση της ροής πληροφοριών προς το ανώτερο επίπεδο cloud. Επιπλέον, το fog computing μπορεί να παρέχει στα ανώτερα επίπεδα εναλλακτικές αποφάσεις και όχι απλώς δεδομένα, παρέχοντας έτσι καλύτερη ποιότητα πληροφοριών στο επίπεδο cloud, με αποτέλεσμα την καλύτερη αξιοποίηση των

πηγών cloud. Επίσης, έχει πρόσβαση στην τοπική εικόνα της κατάστασης μιας συγκεκριμένης περιοχής, οπότε μπορεί να συνδράμει στη λήψη αποφάσεων. Θα πρέπει να σημειωθεί ότι το fog computing, επιλύει τα ζητήματα του cloud που προαναφέρθηκαν, διότι μειώνει το κόστος ανάπτυξης των συστημάτων IoT, ενισχύει την ανθεκτικότητα, καθώς περιορίζεται η χρονική υστέρηση στη ροή των δεδομένων, η υπερφόρτωση και τα σφάλματα μετάδοσης. Με τον τρόπο αυτό είναι δυνατή η βελτίωση της αποδοτικότητας των εφαρμογών, καθώς μπορεί να ληφθεί μια γρήγορη απόφαση βάσει των δεδομένων, γεγονός που είναι σημαντικό σε κρίσιμες καταστάσεις λήψης αποφάσεων.

Και τέλος, υπάρχει το μοντέλο edge computing, το οποίο επίσης μπορεί να μειώσει τα ζητήματα που εμφανίζονται σε χαμηλότερο επίπεδο, όπως η περαιτέρω μείωση του κόστους του δικτύου και των συσκευών. Η κύρια διαφορά μεταξύ του edge coputing και του fog computing είναι ότι οι κόμβοι άκρης του πρώτου λειτουργούν ως μονάδες συγκέντρωσης και λήψης αποφάσεων σε μικρότερη κλίμακα σε σύγκριση με το δεύτερο, και ενεργούν για να εξασφαλίσουν απρόσκοπτη συνδεσιμότητα και ακεραιότητα δεδομένων σε όλο το δίκτυο IoT.

3.2.2. Το δικαίωμα στην πόλη & Ζητήματα προστασίας προσωπικών δεδομένων

Στην έξυπνη πόλη, τα δεδομένα και οι πολίτες διαδραματίζουν πρωταγωνιστικό ρόλο. Το δικαίωμα στην πόλη είναι μια θεμελιώδης ιδέα που θέτει τους πολίτες στο επίκεντρο της αστικής ανάπτυξης μέσω της ενεργού, άμεσης και ουσιαστικής συμμετοχής τους στη λήψη αποφάσεων. Η συμμετοχική διαμόρφωση της πόλης και «το δικαίωμα στην πόλη» είναι στην πραγματικότητα αυτό που μας προτρέπει να σκεφτούμε την πόλη ως μια διαδικασία συλλογικού συν-σχεδιασμού και κοινής παραγωγής" (Breuer J. and Pierson J., 2019).

Η παντοδυναμία των συνδεδεμένων συσκευών που συλλέγουν δεδομένα σε δημόσιους χώρους φέρνει στο προσκήνιο ζητήματα προστασίας θεμελιωδών δικαιωμάτων της ιδιωτικότητας και της προστασίας των δεδομένων. Η καινοτομία της έξυπνης πόλης βασίζεται συχνά σε δεδομένα που μπορεί να χαρακτηριστούν προσωπικά δεδομένα καινά οδηγήσουν σε ταυτοποίηση των ατόμων που αφορούν. Στην Ευρωπαϊκή Ένωση, ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) που υιοθετήθηκε το 2016 ρυθμίζει την επεξεργασία προσωπικών δεδομένων σε συνδυασμό με θεμελιώδη δικαιώματα και

ελευθερίες που κατοχυρώνονται σε άλλα νομικά κείμενα. Η έμφαση που δίνει ο ΓΚΠΔ στα "υποκείμενα των δεδομένων" υποδεικνύει αλληλεπιδράσεις μεταξύ των δικαιωμάτων στην προστασία των δεδομένων και της ουσιαστικής συμμετοχής των πολιτών στις κοινωνικο-τεχνολογικές διεργασίες που διαμορφώνουν τις (έξυπνες) πόλεις, όπως εισηγείται το δικαίωμα στην πόλη.

Καταρχάς, ο ΓΚΠΔ εφαρμόζεται μόνο όταν πραγματοποιείται επεξεργασία προσωπικών δεδομένων δηλαδή πληροφορίες που μπορούν να συνδεθούν με μια μοναδική ταυτότητα. Από τη στιγμή που συντρέχει αυτή η περίπτωση, τα άτομα έχουν θεμελιώδες δικαίωμα στην προστασία των δεδομένων τους. Ο έλεγχος, η ενδυνάμωση και ο πληροφοριακός αυτοκαθορισμός κρίνονται ως βασικές προϋποθέσεις για να καταστεί δυνατή η εν λόγω προστασία. Οι έννοιες αυτές συμπίπτουν με το δικαίωμα στην πόλη, το οποίο στοχεύει στην ενίσχυση της επιρροής των πολιτών. Περαιτέρω στον ΓΚΠΔ προβλέπονται συγκεκριμένα δικαιώματα, όπως το δικαίωμα ενημέρωσης, πρόσβασης, διόρθωσης, διαγραφής και περιορισμού της επεξεργασίας. Αυτά εξασφαλίζουν στα υποκείμενα των δεδομένων πρακτικά μέσα για να μπορούν να ασκήσουν επιρροή στην επεξεργασία των προσωπικών τους δεδομένων. Στα εγχειρήματα έξυπνων πόλεων, οι πολίτες θα μπορούσαν, για παράδειγμα, να ζητήσουν πρόσβαση σε όλα τα προσωπικά τους δεδομένα και να αιτηθούν τη διαγραφή τους. Μια τρίτη δυνητική αλληλεπίδραση μεταξύ των δικαιωμάτων προστασίας των δεδομένων και του δικαιώματος στην πόλη μπορεί να βρεθεί στις γενικές αρχές του ΓΚΠΔ όπως "νομιμότητα, δικαιοσύνη και διαφάνεια", "ελαχιστοποίηση των δεδομένων" και "ικανότητα λογοδοσίας". Η ενίσχυση της διαφάνειας, για παράδειγμα, όσον αφορά πολύπλοκα, δυσνόητα συστήματα, μπορεί να βοηθήσει στην προσπάθεια μετάδοσης της γνώσης μεταξύ ειδικών και μη ειδικών, έτσι ώστε οι πολίτες να μπορούν να συμμετέχουν ενεργά και ουσιαστικά. Η διαφάνεια και η λογοδοσία, που συνεπάγεται ότι ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και πρέπει να είναι σε θέση να αποδείξει τη συμμόρφωσή του, αποτελούν ήδη βασικές αρχές για τις κρατικές αρχές. Για την ανάπτυξη πρωτοβουλιών στο πλαίσιο της έξυπνης πόλης, η εφαρμογή των αρχών αυτών και η συνεκτίμηση των αναγκών των πολιτών συμβαδίζουν. Τέταρτον, το άρθρο 35 παράγραφος 9 του κανονισμού απαιτεί ρητά - υπό περιπτώσεις – και όπου απαιτείται, ο υπεύθυνος επεξεργασίας να "*ζητά τη γνώμη των υποκειμένων των δεδομένων ή των εκπροσώπων τους για τη σχεδιαζόμενη επεξεργασία, με την επιφύλαξη της προστασίας εμπορικών ή δημόσιων συμφερόντων ή της*

ασφάλειας των πράξεων επεξεργασίας" στις λεγόμενες εκτιμήσεις αντικτύπου σχετικά με την προστασία των δεδομένων (DPIA). Η διάταξη αυτή, θα μπορούσε να ερμηνευθεί ως απαίτηση για δημοκρατική νομιμοποίηση με τη συμμετοχή των υποκειμένων των δεδομένων σε αποφάσεις που ενδέχεται να προκαλέσουν συγκρούσεις μεταξύ διαφορετικών ερμηνειών και θεμελιωδών δικαιωμάτων. Η καθοριστική σημασία των δραστηριοτήτων συμμετοχής δεν είναι προφανής, και οι αφηρημένες διατάξεις του ΓΚΠΔ (ιδίως το άρθρο 35 παράγραφος 9) δεν παρέχουν κίνητρα. Οι διατάξεις αυτές χρήζουν ερμηνείας κυρίως από τους ΥΠΔ που κατέχουν βασικό ρόλο στον κανονισμό και θα μπορούσαν να προωθήσουν το άνοιγμα των διαδικασιών υπέρ των πολιτών. Στη θεωρία, αυτές οι πτυχές φαίνεται να είναι καθοριστικές για την ανάπτυξη και τη χρήση υπηρεσιών έξυπνης πόλης που απευθύνονται στους πολίτες. Ωστόσο, η προστασία της ιδιωτικής ζωής και των δεδομένων ως αξίωση για πληροφοριακό αυτοκαθορισμό εστιάζουν στο άτομο και στα ατομικά του συμφέροντα και στον έλεγχό του και όχι στη συλλογική ενδυνάμωση. Στην έξυπνη πόλη, όπου η επεξεργασία δεδομένων μπορεί να πραγματοποιείται στο όνομα του συμφέροντος της πόλης και των κατοίκων της, ο ατομικός έλεγχος μπορεί να είναι δύσκολο να επιτευχθεί. Όπως, έχει επισημανθεί, στη διαμόρφωση των πρωτοβουλιών της έξυπνης πόλης, συχνά κυριαρχούν τα επιχειρηματικά συμφέροντα, ενώ οι θέσεις των πολιτών είναι λιγότερο παρούσες και αισθητές κατά τη διαδικασία λήψης αποφάσεων. Ο ΓΚΠΔ παρέχει σημαντικές εξουσίες λήψης αποφάσεων στους λεγόμενους υπεύθυνους επεξεργασίας δεδομένων, οι οποίοι είναι ως επί το πλείστον ήδη ισχυρές εταιρείες και κρατικές διοικήσεις, και αφήνει μεγάλο περιθώριο για τις αποφάσεις τους λόγω ασαφών και αφηρημένων διατάξεων.

Λαμβάνοντας υπ' όψιν ένα μικρό αλλά ουσιαστικό δείγμα διαφόρων εγχειρημάτων έξυπνων πόλεων που έχουν υλοποιηθεί, τα σχετικά ευρήματα καταδεικνύουν ότι κάτι τέτοιο δεν συμβαίνει. Το ποσοστό και το είδος της συμμετοχής των πολιτών που έχει διαπιστωθεί ότι στις περισσότερες περιπτώσεις, απέχει ακόμη πολύ από το να έχουν οι πολίτες δικαίωμα στην πόλη (*Breuer J. and Pierson J., 2019*) Τα ευρήματα καταδεικνύουν ότι, πρώτον, το δύσκολο ζήτημα των πολύπλοκων τεχνικών συστημάτων, του δικαίου και των θεμελιωδών δικαιωμάτων, καθώς και η έλλειψη γνώσης κατανόησης όλων των εμπλεκόμενων μερών αποτελεί σημαντικό εμπόδιο για την ουσιαστική συμμετοχή. Από την άποψη αυτή, η ευαισθητοποίηση και η συνεχής εκπαίδευση όχι μόνο για των πολιτών, αλλά και λοιπών εμπλεκομένων, όπως οι Υπεύθυνοι Προστασίας Δεδομένων (ΥΠΔ), οι προγραμματιστές και

άλλοι φορείς καθοριστικοί στη λήψη αποφάσεων κατά τη διαδικασία ,είναι ουσιαστικής σημασίας. Δεύτερον, η λήψη αποφάσεων είναι ήδη αρκετά περίπλοκη, ενώ παράλληλα δεν υπάρχουν επίσης επαρκή κίνητρα για την καταβολή επιπρόσθετων προσπαθειών. Ακόμα και οι πιο φιλόδοξοι, όταν έρχονται αντιμέτωποι με τις προκλήσεις της σκοπιμότητας και της αντιπροσωπευτικότητας καθώς και το σχετικό κόστος μπορεί να αποθαρρυνθούν. Τρίτον, οι αφηρημένες και - ανά περιπτώσεις - αόριστες διατάξεις του ΓΚΠΔ δεν βοηθούν. Επομένως, όσοι συμμετέχουν ήδη στις διαδικασία λήψεως αποφάσεων βρίσκονται σε κύριες θέσεις για να επηρεάσουν τις εξελίξεις στις έξυπνες πόλεις. Ο ρόλος του υπεύθυνου επεξεργασίας δεδομένων είναι τόσο κεντρικός, ώστε η όποια απόφαση για τη συμμετοχή των πολιτών εξακολουθεί να εξαρτάται από τον ίδιο. Στην έξυπνη πόλη συνήθως οι διοικήσεις ή οι εταιρείες καταλαμβάνουν τον ρόλο του υπεύθυνου επεξεργασίας. Οι τελευταίοι μπορούν να αποδεχθούν την άσκηση των δικαιωμάτων των πολιτών μόνο για όσο διάστημα είναι οικονομικά εφικτό γι' αυτούς. Το να ερωτηθούν οι θιγόμενοι κάτοικοι των πόλεων για τη γνώμη τους, για τις ανάγκες τους και για το κατά πόσον ένα εγχείρημα στο πλαίσιο της έξυπνης πόλης θα ήταν πράγματι πολύτιμο γι' αυτούς πριν από την υλοποίησή του, θα μπορούσε ήδη να είναι ένα βήμα προς ένα δικαίωμα στην πόλη, αλλά ο ΓΚΠΔ δεν απαιτεί μια τέτοια εκ των προτέρων διαβούλευση.

Ορισμένες από αυτές τις ελλείψεις μπορούν να βελτιωθούν από τους νομικούς και τους δικαστές μέσω της νομολογίας και από τους ερευνητές που μπορούν να εντοπίσουν και να αναδείξουν αυτά τα ζητήματα. Άλλες ελλείψεις θα μπορούσαν να τροποποιηθούν με την παρουσία πιο ενεργών εποπτικών αρχών που θα παρέχουν σαφέστερες κατευθυντήριες γραμμές, καθοδήγηση και υποστήριξη. Και τα δύο είναι πιθανό να επιτευχθούν με την πάροδο του χρόνου, αλλά παρόλα αυτά, ο νόμος εξακολουθεί να παραμένει το πιο καθοριστικό, ίσως, εργαλείο η αξιοποίηση του οποίου όμως είναι πιο ευχερής για ορισμένες κοινωνικές ομάδες απ' ό,τι για άλλες, οι οποίες δεν έχουν τα μέσα, τις γνώσεις ή τη θέση στην κοινωνία για να τον χρησιμοποιήσουν προς όφελός τους. Παρόλα αυτά, τα δικαιώματα προστασίας δεδομένων, όπως επικαιροποιούνται από τον ΓΚΠΔ, αποτελούν ένα σημαντικό βήμα προς τη σωστή κατεύθυνση. Σε κάθε περίπτωση, οι έντονες συζητήσεις, επιστημονικές και άλλες, ενισχύουν την ευαισθητοποίηση. είναι σημαντικό να τονιστεί ότι η συμμετοχή του κοινού δεν αναμένεται ούτε απαιτείται να επιφέρει άμεσα σημαντικές αλλαγές στον τρόπο οργάνωσης της κοινωνίας. Σε αυτό το πλαίσιο του εγχειρήματος, κάθε συμμετοχή που

είναι διαφανής, με σαφείς προθέσεις, με πραγματικά δυναμικό αντίκτυπο στις αποφάσεις, είναι καλύτερη από τη μη συμμετοχή και μπορεί να προκαλέσει αξιόλογες σταδιακές αλλαγές.Τέλος, είναι σημαντικό να τονιστεί ο ρόλος της έρευνας, η οποία συμβάλλει στη διαμόρφωση του πλαισίου προστασίας δεδομένων στην ανάπτυξη των έξυπνων πόλεων. Θέτοντας τις σωστές ερωτήσεις, ενισχύοντας την ενημέρωση, υποστηρίζοντας τους φορείς μέσω μεθόδων και τεχνικών συμμετοχής, μπορεί να επιτευχθεί η αλλαγή και να προωθηθεί η ανάπτυξη ψηφιακών πόλεων με επίκεντρο τον πολίτη.

Το ερώτημα παραμένει αν η χρήση τέτοιων τεχνολογιών θα υπονομεύσει μακροπρόθεσμα τις ατομικές ανάγκες προστασίας του ιδιωτικού βίου. Ορισμένοι συγγραφείς αναφέρουν ότι «*οι τεχνολογίες επιτήρησης αποτελούν βασικό συστατικό στοιχείο των έξυπνων και δικτυωμένων πόλεων που αποτρέπουν ή ανιχνεύουν το έγκλημα και δίνουν στους κατοίκους την αίσθηση της ασφάλειας*» (*van Heek, Aming, & Ziefle, 2016).* Ωστόσο, ενώ πολλές καινοτομίες μπορεί να δημιουργούν πιο αποτελεσματικές υπηρεσίες πόλης ή να μειώνουν αποτελεσματικά την εγκληματικότητα, μπορεί ταυτόχρονα να κάνουν τους ανθρώπους να αισθάνονται λιγότερο ασφαλείς, επειδή έχουν την αίσθηση ότι συνεχώς παρακολουθούνται. Ιδιαίτερα σε καθεστώτα αυταρχικά (ή τουλάχιστον όχι πλήρως δημοκρατικά), η εφαρμογή αυτών των μέτρων ασφαλείας μπορεί να αυξήσει εκθετικά την κρατική εξουσία και τον έλεγχο των πολιτών. Συνεπώς, υπάρχει έντονος διάλογος και διαφωνίες, που δεν έχουν επιλυθεί ακόμη σε σχέση με αυτές τις νέες τεχνολογίες, ιδίως όσον αφορά την προστασία του ιδιωτικού βίου και πλαισίου προστασίας προσωπικών δεδομένων, καθώς και τη μεγάλη σημασία της υποδομής αστικής επιτήρησης και ασφάλειας για την παροχή προστασίας και ασφάλειας στην πόλη του 21ου αιώνα (*J. Laufs et al., 2020).*

4. ΔΕΔΟΜΕΝΑ ΘΕΣΗΣ

4.1. Η επεξεργασία δεδομένων θέσης μέσω εφαρμογών

Από τα ανωτέρω αναφερόμενα, προκύπτει με σαφήνεια ότι μέσω των τεχνολογιών παρακολούθησης και εντοπισμού είναι πολύ πιθανό να παραβιάζεται το δικαίωμα ιδιωτικότητας των ατόμων με επεξεργασία δεδομένων θέσης και κίνησης εντός του επιτηρούμενου χώρου σε μεγάλη κλίμακα, ειδικά όταν πρόκειται για τεχνολογίες εντοπισμού σε κινητά τηλέφωνα, αυτοκίνητα και υπηρεσίες που παρέχονται με βάση την τοποθεσία του χρήστη. Με τη χρήση τεχνολογιών που βασίζονται στην τοποθεσία, μία από

τις μεγαλύτερες ανησυχίες είναι ότι μπορεί να είναι δυνατή η συλλογή μιας πολύ λεπτομερούς εικόνας των κινήσεων κάποιου, εάν αυτός φέρει μια ασύρματη συσκευή που επικοινωνεί τη θέση της στους φορείς παροχής του δικτύου. Η πιθανότητα καταχρηστικής επεξεργασίας αυτών των πληροφοριών περιλαμβάνει διάφορες μορφές, από ανεπιθύμητη διαφήμιση σε καταστήματα όταν τα πλησιάζει ένας χρήστης κινητού τηλεφώνου, μέχρι πιο σοβαρές περιπτώσεις, όπως επιχειρήσεις που χρησιμοποιούν πληροφορίες θέσης για τους εργαζόμενους στο χώρο για να επιβάλλουν αυστηρά κριτήρια αποδοτικότητας, ακόμη και εγκληματίες που με τη χρήση τέτοιου είδους παρακολούθησής, γνωρίζουν την κατάλληλη στιγμή για να εισβάλουν στο σπίτι ενός ατόμου, ή μια αδικαιολόγητη καταδικαστική απόφαση με βάση περιστασιακές πληροφορίες θέση. Ωστόσο, η σχετικά μεγάλη επιτυχία ορισμένων εφαρμογών που βασίζονται στον εντοπισμό θέσης του χρήστη καταδεικνύει ότι μία ικανοποιητική μερίδα του κόσμου δείχνει να αισθάνεται ασφαλής με την αποστολή των δεδομένων της θέσης του σε τρίτους.

Τα δεδομένα θέσης, λοιπόν, χρησιμοποιούνται για την παροχή διαφόρων υπηρεσιών και για την εκτέλεση του βασικού σκοπού ορισμένων εφαρμογών κινητής τηλεφωνίας, οι οποίες αναπτύσσονται βάσει λογισμικού ώστε να λειτουργούν σε κινητές συσκευές. Τα δεδομένα θέσης είναι δυνατόν να αποκαλύψουν ιδιωτικές πληροφορίες που, λόγω της παρουσίας των συσκευών νέας γενιάς παντού, θα μπορούσαν να αφορούν δεδομένα υγείας, οικονομικά δεδομένα, δεδομένα καταναλωτικής συμπεριφοράς, προσωπικές συνήθειες και θρησκευτικές πεποιθήσεις του κατόχου τους, επιτρέποντας έτσι να εξαχθεί ένα ευρύ φάσμα πληροφοριών σχετικά με τη ζωή του ατόμου. Η δυνατότητα ενός πολύ μεγάλου φάσματος συσκευών να επεξεργάζονται προσωπικά και μη προσωπικά δεδομένα δημιουργεί όλο και περισσότερες ανησυχίες σχετικά με την εν λόγω επεξεργασία, τόσο από νομικής όσο και από ηθικής πλευράς.

Η χρήση εφαρμογών έχει γίνει ένας από τους κύριους παράγοντες που οδηγούν στην γνωστοποίηση προσωπικών δεδομένων και στην μετέπειτα επεξεργασία τους. Η αύξηση της συλλογής δεδομένων τοποθεσίας κατά την τελευταία εικοσιπενταετία μαρτυρά τη ραγδαία εξάπλωση των νέων συσκευών στον ευρύτερο πληθυσμό, ανεξάρτητα από την ηλικία, το επάγγελμα και τα ενδιαφέροντά του εκάστοτε ατόμου. Αυτό οφείλεται εν μέρει στο γεγονός ότι οι εφαρμογές είναι εύκολο να αποκτηθούν, χάρη στα ηλεκτρονικά καταστήματα εφαρμογών που είναι διαθέσιμα στα κινητά (app stores), και μέσω των οποίων οι χρήστες

μπορούν να περιηγηθούν στις εφαρμογές, που ταξινομούνται ανά κατηγορίες, και να τις μεταφορτώσουν στο κινητό τους με ένα απλό "κλικ". Στην ουσία, ορισμένες συσκευές θα μπορούσαν να χαρακτηριστούν ως ένα εργαλείο παγκόσμιας και μοναδικής χρήσης, ικανό να διαμορφώνεται ανάλογα με τις επιθυμίες και τα ενδιαφέροντα του χρήστη. Υπάρχουν διάφορες κατηγορίες εφαρμογών - που μπορούν να μεταφορτωθούν εύκολα από τα καταστήματα εφαρμογών στη συσκευή του χρήστη - για κάθε κατηγορία ενδιαφερόντων ενός ατόμου, όπως η εργασία, η ψυχαγωγία, τα κοινωνικά δίκτυα, ο ελεύθερος χρόνος, οι ειδήσεις, ο αθλητισμός, η γυμναστική κ.α.

Η πρόσβαση σε διάφορες κατηγορίες προσωπικών δεδομένων και μεταδεδομένων επιβάλλεται από τα χαρακτηριστικά του hardware στο εσωτερικό της συσκευής, γεγονός που ενισχύει τη δυνατότητά της συσκευής να συλλέγει προσωπικά δεδομένα. Κάθε κινητό τηλέφωνο, για παράδειγμα, είναι εξοπλισμένο με μια σειρά από αισθητήρες (μικρόφωνο, κάμερα, υπέρυθρες, GPS, Bluetooth, μετρητή επιτάχυνσης, Wi-Fi, αισθητήρα δακτυλικών αποτυπωμάτων κ.λπ.), που έχουν τη δυνατότητα ανάκτησης προσωπικών πληροφοριών σχετικά με τον κάτοχο της συσκευής. Τα χαρακτηριστικά του hardware αυξάνουν επίσης τις δυνατότητες του λειτουργικού συστήματος, το οποίο συνήθως σχεδιάζεται έτσι ώστε να ταιριάζει απόλυτα με τα χαρακτηριστικά της συσκευής. Το λειτουργικό σύστημα επικοινωνεί με τους εν λόγω αισθητήρες χρησιμοποιώντας μια διεπαφή που λειτουργεί ως ενδιάμεσος για τη ροή δεδομένων μεταξύ των υπηρεσιών. Αυτός ο ενδιάμεσος ονομάζεται διεπαφή προγραμματισμού εφαρμογών, οι εφαρμογές χρησιμοποιούν τη διεπαφή αυτή, για να διαβάζουν πληροφορίες από τους αισθητήρες και να αλληλεπιδρούν μεταξύ αυτών και του λειτουργικού συστήματος.

Σχεδόν ανεξαιρέτως, το hardware των νέων συσκευών περιλαμβάνει chip GPS, συνδέσεις Wi-Fi ή Bluetooth, τις οποίες σε πολλές περιπτώσεις εκμεταλλεύονται τόσο το λειτουργικό σύστημα όσο και οι εφαρμογές που έχουν μεταφορτωθεί στη συσκευή, συλλέγοντας με αυτόν τον τρόπο δεδομένα τοποθεσίας προκειμένου να διασφαλιστεί η πλήρης αξιοποίηση της λειτουργικότητας των συσκευών.

Τα νομικά ζητήματα που σχετίζονται με τη συλλογή δεδομένων θέσης μέσω εφαρμογών βρίσκονται πάντα στο επίκεντρο του ενδιαφέροντος των ευρωπαϊκών και εθνικών εποπτικών οργάνων, λόγω της απρόβλεπτης και συνεχούς εξέλιξης της τεχνολογίας. Ποιο είναι όμως το νομικό πλαίσιο επεξεργασίας των δεδομένων αυτών; Λόγω του ιδιαίτερα "αποκαλυπτικού" τους χαρακτήρα, τα δεδομένα θέσης, εντάσσονται στην κατηγορία των προσωπικών δεδομένων. Ο ΓΚΠΔ, αποτελεί το κύριο νομικό σημείο αναφοράς για την επεξεργασία προσωπικών δεδομένων, συνεπώς η ανάπτυξη και η λειτουργία των εφαρμογών θα πρέπει να υπόκειται στις αρχές του ΓΚΠΔ. Από τον ορισμό των προσωπικών δεδομένων στο άρθρο 4 εδ. 1 του ΓΚΠΔ, ο οποίος έχει ως εξής «*κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου*», προκύπτει ξεκάθαρα ότι τα δεδομένα θέσης εμπίπτουν στον ως άνω ορισμό και συνακόλουθα στο πεδίο εφαρμογής του ΓΚΠΔ, δεδομένου ότι μπορούν να αποκαλύψουν προσωπικές πληροφορίες για τα πρόσωπα που αφορούν.

Αυτό συνεπάγεται ότι η επεξεργασία των δεδομένων θέσης πρέπει να είναι σύμφωνη με τις προβλέψεις του ΓΚΠΔ, στο βαθμό που αποκαλύπτουν προσωπικές πληροφορίες. Το πεδίο εφαρμογής του ΓΚΠΔ περιλαμβάνει επίσης τα μεταδεδομένα.

Ωστόσο, το ευρωπαϊκό νομικό πλαίσιο σχετικά με τις εφαρμογές κινητών τηλεφώνων είναι ευρύτερο και περιλαμβάνει την οδηγία 2002/58/ΕΚ για την προστασία των δεδομένων προσωπικού χαρακτήρα στον τομέα των ηλεκτρονικών επικοινωνιών, όπως τροποποιήθηκε από την οδηγία 2009/136/ΕΚ. Η οδηγία υπόκειται σήμερα σε επικαιροποίηση μέσω του νέου κανονισμού για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, ο οποίος εξετάζεται επί του παρόντος από το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο.

Ο ΓΚΠΔ συμπληρώνεται και εξειδικεύεται με αυτόν τον τρόπο από ειδικές ρυθμίσεις. Η οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες θεσπίζει κανόνες για τη διασφάλιση της ιδιωτικής ζωής και της προστασίας των δεδομένων

προσωπικού χαρακτήρα στον προαναφερθέντα τομέα. Τα θέματα που δεν εμπίπτουν στο πεδίο εφαρμογής της οδηγίας, αλλά αφορούν την επεξεργασία δεδομένων προσωπικού χαρακτήρα, ρυθμίζονται από τον ΓΚΠΔ.

Η αλληλεπίδραση μεταξύ της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες και του ΓΚΠΔ αποτέλεσε αντικείμενο ενδιαφέροντος σε σχετική γνωμοδότηση του ΕΣΠΔ. Σύμφωνα με το ΕΣΠΔ, μια σειρά από διατάξεις της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες αφορούν τον ΓΚΠΔ. Πράγματι, μεταξύ των δύο αυτών νόμων εφαρμόζεται η αρχή lex specialis derogat legi generali . Με τον τρόπο αυτό, η παρέκκλιση του γενικού κανόνα που προβλέπει ο ΓΚΠΔ πραγματοποιείται στο μέτρο που η οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες περιέχει ειδικούς κανόνες, με την επιφύλαξη ότι η αναφερόμενη αλληλεπίδραση εμπλέκει το εθνικό δίκαιο μεταφοράς της οδηγίας. Βεβαίως, η τελευταία καθορίζει μόνο τον εκάστοτε σκοπό που πρέπει να επιτύχουν τα κράτη μέλη και για την επίτευξη των στόχων αυτών απαιτείται εσωτερικό νόμος.

Στο πλαίσιο της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, ως δεδομένα θέσης, σύμφωνα με το άρθρο 2 στοιχείο γ), "νοούνται όλα τα δεδομένα που επεξεργάζονται σε δίκτυο ηλεκτρονικών επικοινωνιών ή από υπηρεσία ηλεκτρονικών επικοινωνιών, τα οποία υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού ενός χρήστη δημόσια διαθέσιμης υπηρεσίας ηλεκτρονικών επικοινωνιών".

Επιπλέον, η αιτιολογική σκέψη 14 διευκρινίζει ότι τα δεδομένα αυτά "μπορούν να αναφέρονται στο γεωγραφικό πλάτος, στο γεωγραφικό μήκος και στο υψόμετρο του τερματικού εξοπλισμού του χρήστη, στην κατεύθυνση της κίνησης, στο επίπεδο ακρίβειας των πληροφοριών θέσης, στον προσδιορισμό της κυψέλης του δικτύου στην οποία βρίσκεται ο τερματικός εξοπλισμός σε μια συγκεκριμένη χρονική στιγμή και στην ώρα που καταγράφηκαν οι πληροφορίες θέσης". Η οδηγία λαμβάνει υπόψη το ιδιόμορφο χαρακτηριστικό των ηλεκτρονικών επικοινωνιών να αποκαλύπτουν προσωπικές πληροφορίες για τους εμπλεκόμενους χρήστες. Η πρόταση του κανονισμού για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες ερμηνεύει την έννοια των μεταδεδομένων, "*δεδομένα που υποβάλλονται σε επεξεργασία σε δίκτυο ηλεκτρονικών επικοινωνιών για τους σκοπούς της μετάδοσης, της διανομής ή της ανταλλαγής περιεχομένου*

ηλεκτρονικών επικοινωνιών· συμπεριλαμβάνονται τα δεδομένα που χρησιμοποιούνται για την παρακολούθηση και την ταυτοποίηση της πηγής και του προορισμού μιας επικοινωνίας, τα δεδομένα τοποθεσίας της συσκευής που παράγονται στο πλαίσιο της παροχής υπηρεσιών ηλεκτρονικών επικοινωνιών και της ημερομηνίας, της ώρας, της διάρκειας και του είδους της επικοινωνίας·". Λαμβάνοντας υπόψη το σενάριο αναφοράς, είναι δυνατόν να καθοριστεί η γενική αρχή της προστασίας των δεδομένων θέσης που εφαρμόζεται στην επεξεργασία μέσω εφαρμογών. .

Στο πλαίσιο της επεξεργασίας δεδομένων θέσης από μια συσκευή κινητού τηλεφώνου, ο ρόλος του υπεύθυνου επεξεργασίας δεδομένων - ο οποίος καθορίζει τους σκοπούς και τα μέσα της επεξεργασίας - θα μπορούσε να εκληφθεί από διαφορετικούς φορείς και συγκεκριμένα τον προγραμματιστή του λειτουργικού συστήματος, εάν το εν λόγω λογισμικό συλλέγει δεδομένα θέσης για τη βελτίωση των παρεχόμενων υπηρεσιών, τον πάροχο εφαρμογών που επεξεργάζεται δεδομένα θέσης (π.χ. χάρτες, μετεωρολογική υπηρεσία, υπηρεσία παράδοσης φαγητού) μόλις εγκατασταθούν στη συσκευή ή αποκτήσουν πρόσβαση μέσω ενός προγράμματος περιήγησης, και τους υπευθύνους επεξεργασίας δεδομένων της υποδομής γεωγραφικού εντοπισμού, όπως οι φορείς εκμετάλλευσης τηλεπικοινωνιών ή τα σημεία πρόσβασης Wi-Fi. Επιπλέον, κάθε άλλο μέρος που πραγματοποιεί περαιτέρω επεξεργασία των δεδομένων θέσης που συλλέγονται θεωρείται υπεύθυνος επεξεργασίας δεδομένων, δεδομένου ότι καθορίζει τους σκοπούς και τα μέσα των εν λόγω πράξεων.

Τα δεδομένα θέσης συλλέγονται και υποβάλλονται σε επεξεργασία όταν η συσκευή επιτρέπει την αλληλεπίδραση μεταξύ του αισθητήρα και των εφαρμογών ή του λειτουργικού συστήματος, ακόμη και όταν τα δεδομένα αυτά υποβάλλονται σε επεξεργασία στη συσκευή ή μέσω του διαδικτύου.

Η συλλογή των δεδομένων αυτών πρέπει να είναι σύμφωνη με τις γενικές αρχές που θεσπίζει ο ΓΚΠΔ και οι οποίες μπορεί να συνοψισθούν ως εξής: τα προσωπικά δεδομένα υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο, συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασυμβίβαστο με τους σκοπούς αυτούς, υποβάλλονται σε επεξεργασία με ακρίβεια, επάρκεια και περιορίζονται στους σκοπούς, διατηρούνται σε

μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων για χρονικό διάστημα όχι μεγαλύτερο από το αναγκαίο- και προστατεύονται από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και από τυχαία απώλεια, καταστροφή και ζημία, με την υιοθέτηση κατάλληλων τεχνικών ή οργανωτικών μέτρων.

Σύμφωνα με τα παραπάνω, οι εφαρμογές θα πρέπει να συλλέγουν μόνο εκείνα τα δεδομένα που είναι απολύτως απαραίτητα για την εκτέλεση της λειτουργίας που έχει σχεδιασθεί και προγραμματιστεί. Οποιαδήποτε περαιτέρω και μη συμβατή επεξεργασία θα θεωρείται υπέρμετρη και, ως εκ τούτου, παράνομη.

Ο ΓΚΠΔ περιλαμβάνει επίσης τις προϋποθέσεις για την επεξεργασία ευαίσθητων δεδομένων προσωπικού χαρακτήρα, σύμφωνα με τις προβλέψεις του άρθρου 9 του ΓΚΠΔ. Τα δεδομένα αυτά αφορούν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, τα γενετικά βιομετρικά δεδομένα και τα δεδομένα υγείας ή τα δεδομένα που αφορούν τη σεξουαλική ζωή ή τον γενετήσιο προσανατολισμό ενός φυσικού προσώπου. Τα δεδομένα θέσης ενδέχεται να αποκαλύπτουν πληροφορίες που είναι εγγενείς σε εκείνες που περιλαμβάνονται στην ειδική κατηγορία δεδομένων προσωπικού χαρακτήρα, επομένως στην περίπτωση αυτή, η επεξεργασία τους απαιτεί ιδιαίτερη προσοχή ως προς την αναλογικότητα επεξεργασίας δεδομένων αλλά και την ελαχιστοποίηση επεξεργασίας των δεδομένων αυτών, γεγονός που οδηγεί στην ανάγκη διενέργειας εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων από τον υπεύθυνο επεξεργασίας.

4.2. Ανωνυμοποίηση και ψευδωνυμοποίηση δεδομένων θέσης

Το ΕΣΠΔ, στις σχετικές κατευθυντήριες γραμμές που έχει εκδόσει σχετικά με τα δεδομένα θέσης επισημαίνει ότι κατά την επεξεργασία τέτοιου είδους δεδομένων πρέπει να προτιμάται η χρήση ανωνυμοποιημένων δεδομένων και όχι προσωπικών δεδομένων. Σύμφωνα με την αιτιολογική σκέψη 26 ΓΚΠΔ, οι αρχές προστασίας δεδομένων πρέπει να εφαρμόζονται σε κάθε πληροφορία η οποία αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο. Ως προς τα προσωπικά δεδομένα έχουν υποστεί ψευδωνυμοποίηση, θα πρέπει να θεωρούνται πληροφορίες σχετικά με ταυτοποιήσιμο φυσικό πρόσωπο και συνεπώς να εμπίπτουν στο πεδίο εφαρμογής του ΓΚΠΔ. Σύμφωνα με την ως άνω αιτιολογική σκέψη «*για*

να κριθεί κατά πόσον ένα φυσικό πρόσωπο είναι ταυτοποιήσιμο, θα πρέπει να λαμβάνονται υπόψη όλα τα μέσα τα οποία είναι ευλόγως πιθανό ότι θα χρησιμοποιηθούν, όπως για παράδειγμα ο διαχωρισμός του, είτε από τον υπεύθυνο επεξεργασίας είτε από τρίτο για την άμεση ή έμμεση εξακρίβωση της ταυτότητας του φυσικού προσώπου». Περαιτέρω, για τη διαπίστωση εάν και σε ποιο βαθμό ορισμένα μέσα είναι εύλογα πιθανό να χρησιμοποιηθούν για την εξακρίβωση της ταυτότητας ενός φυσικού προσώπου, θα πρέπει να λαμβάνονται υπόψη όλοι οι αντικειμενικοί παράγοντες, όπως ενδεικτικά έξοδα και χρόνος που απαιτούνται ώστε να πραγματοποιηθεί η ταυτοποίηση, λαμβάνοντας υπ' όψιν την τεχνολογία που είναι διαθέσιμη κατά τον χρόνο της επεξεργασίας. Συνεπώς, στο πεδίο εφαρμογής του ΓΚΠΔ, δεν εμπίπτουν ανώνυμες πληροφορίες που δεν είναι εφικτό να συσχετισθούν με ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο, όπως και επίσης σε προσωπικά δεδομένα που έχουν καταστεί ανώνυμα, με τέτοιο τρόπο, με αποτέλεσμα η ταυτότητα των φυσικών προσώπων να είναι πλέον εφικτό να εξακριβωθεί.

Όπως γίνεται κατανοητό, οι δύο όροι, ανωνυμοποίηση και ψευδονυμοποίηση είναι σαφώς διαφορετικοί και, ως εκ τούτου, πρέπει να γίνουν κατανοητοί ώστε να παρέχονται εγγυήσεις σύμφωνες με τον ΓΚΠΔ για τα προσωπικά δεδομένα ενός υποκειμένου που έχουν συλλεχθεί. Ως ανωνυμοποίηση θα μπορούσε να ορισθεί η προστασία των δεδομένων με την υιοθέτηση μιας μη αναστρέψιμης αυτοματοποιημένης μεθόδου. Ο όρος μη αναστρέψιμος είναι σημαντικό να γίνει κατανοητός, καθώς τα ανώνυμα δεδομένα δεν μπορούν να επανέλθουν στην αρχική τους μορφή ή να χρησιμοποιηθούν για την ταυτοποίηση του υποκειμένου των δεδομένων με την ανάπτυξη οποιασδήποτε πρακτικής μεθόδου. Από την άλλη ως ψευδωνυμοποίηση θα μπορούσε να ορισθεί η προστασία των δεδομένων με την αντικατάσταση των πραγματικών προσωπικών πληροφοριών με ένα αναγνωριστικό ψευδώνυμο μέσω μιας αυτοματοποιημένης μεθόδου, έτσι ώστε το υποκείμενο των δεδομένων να μην μπορεί να καταστεί άμεσα αντιληπτό μέσω ενός ψευδωνύμου.

Οι προηγούμενοι ορισμοί καταδεικνύουν τη διάκριση μεταξύ ανωνυμοποιημένων και ψευδωνυμοποιημένων δεδομένων. Ο χαρακτηριστικός ορισμός από την Επιτροπή Προστασίας Δεδομένων της Ιρλανδίας έχει ως εξής:

«Αν και η ψευδωνυμοποίηση έχει πολλές χρήσεις, θα πρέπει να διακρίνεται από την ανωνυμοποίηση, καθώς σε πολλές περιπτώσεις παρέχει μόνο περιορισμένη προστασία της

ταυτότητας των υποκειμένων των δεδομένων, καθώς εξακολουθεί να επιτρέπει την ταυτοποίηση με έμμεσους τρόπους. Στις περιπτώσεις που χρησιμοποιείται ένα ψευδώνυμο, είναι συχνά δυνατό να ταυτοποιηθεί το υποκείμενο των δεδομένων της ανάλυσης των υποκείμενων ή σχετικών δεδομένων.».

Ο παραπάνω ορισμός της ψευδωνυμοποίησης καταδεικνύει ότι σε ορισμένες περιπτώσεις τα στοιχεία που έχουν ψευδωνυμοποιηθεί, μπορούν να οδηγήσουν σε ταυτοποίηση του εκάστοτε υποκειμένου των δεδομένων, το υποκείμενο των δεδομένων μπορεί να αναγνωριστεί με τη χρήση οποιασδήποτε άλλης σχετικής πληροφορίας ή αυτοματοποιημένης μεθόδου, ακόμη και όταν τα δεδομένα δεν επανέρχονται στην αρχική τους μορφή. Συνεπώς, σε γενικές γραμμές, μπορεί κανείς να διακρίνει τους δύο όρους λέγοντας ότι, η ψευδωνυμοποίηση μπορεί να είναι μια τεχνική διασφάλισης που μπορεί να είναι αναστρέψιμη, αλλά η ανωνυμοποίηση είναι μια μη αναστρέψιμη τεχνική για την εξασφάλιση της προστασίας των δεδομένων. Τα αμετάκλητως ανωνυμοποιημένα δεδομένα δεν εμπίπτουν στο πεδίο εφαρμογής του κανονισμού και οι υπεύθυνοι επεξεργασίας μπορούν να διατηρούν αυτή τη μορφή δεδομένων για απεριόριστο χρονικό διάστημα (για μελλοντική στατιστική ανάλυση) χωρίς να προκύπτουν ζητήματα συμμόρφωσης με τον ΓΚΠΔ.

Τώρα τίθεται λογικά το ερώτημα ότι εάν οι υπεύθυνοι επεξεργασίας διατηρούν την ανώνυμη μορφή των δεδομένων, τότε ποιος είναι ο σκοπός της διατήρησης των δεδομένων αυτών; Οι υπεύθυνοι επεξεργασίας δεν μπορούν να επαναφέρουν τα δεδομένα στην πραγματική τους μορφή για οποιοδήποτε είδους επεξεργασία, ακόμη και αν αυτή ήταν νόμιμη. Ως εκ τούτου, η διατήρηση των δεδομένων σε αυτή τη μορφή, που προορίζονται για παράδειγμα για μελλοντική στατιστική ανάλυση, θα μπορούσε να θεωρηθεί απλώς σπατάλη αποθηκευτικού χώρου από την πλευρά των υπευθύνων επεξεργασίας

Ο ΓΚΠΔ, στις προβλέψεις των άρθρων 6 και 32, δίνει έμφαση «*στην ψευδωνυμοποίηση ή κρυπτογράφηση*»[1] και «*στην ψευδωνυμοποίηση και κρυπτογράφηση*»[2], αντίστοιχα. Στο άρθρο 6, η λέξη «*ή*» και στο άρθρο 32, η χρήση της λέξης «και» μεταξύ αυτών των δύο διαδικασιών δεν έχουν επιλεχθεί τυχαία. Οι υπεύθυνοι επεξεργασίας μπορούν να θεωρήσουν ότι οι δύο

[1] Άρθρο 6 παράγραφος 4 στοιχείο ε) ΓΚΠΔ
[2] Άρθρο 32 παράγραφος 1 στοιχείο α) ΓΚΠΔ

αυτές διαδικασίες είναι εξίσου κατάλληλες ως μέτρο προστασίας των προσωπικών δεδομένων. Ωστόσο, αξίζει να σημειωθεί ότι η κρυπτογράφηση είναι πάντοτε αναστρέψιμη και συνεπώς μπορεί να οδηγήσει στην ταυτοποίηση του υποκειμένου, ενώ η ψευδωνυμοποίηση μπορεί είτε να είναι είτε να μην είναι αναστρέψιμη. Παρόλο που η κρυπτογράφηση και η ψευδωνυμοποίηση μπορούν να χρησιμοποιηθούν ταυτόχρονα ή και χωριστά, δεν αποτελούν εναλλακτικές μεταξύ τους που μπορούν να αξιολογηθούν ανάλογα με τα πλεονεκτήματα και τα μειονεκτήματά τους.

Η ανωνυμοποίηση πραγματοποιείται με τη χρήση πλήθους τεχνικών ώστε να καθίσταται εφικτή η σύνδεση των δεδομένων με φυσικό πρόσωπο και συνεπώς η ταυτοποίησή του με «εύλογες» προσπάθειες. Κατά τον έλεγχο του ευλόγου χαρακτήρα, οι υπεύθυνοι επεξεργασίας πρέπει να λαμβάνουν υπ ' όψιν τους τόσο αντικειμενικές πτυχές (χρόνος, τεχνικά μέσα κ.λπ.) όσο και συγκυριακά στοιχεία που μπορεί να διαφοροποιούνται ανά περίσταση. Σε περίπτωση που ο έλεγχος αυτός δεν ικανοποιηθεί τότε συνάγεται ότι τα δεδομένα δεν έχουν ανωνυμοποιηθεί και οι διατάξεις του ΓΚΠΔ πρέπει να εφαρμόζονται. Σύμφωνα με το ΕΣΠΔ, « *η αξιολόγηση της αρτιότητας της ανωνυμοποίησης βασίζεται σε τρία κριτήρια, ήτοι την απομόνωση της ταυτότητας ενός φυσικού προσώπου (από μία μεγαλύτερη ομάδα με βάση τα δεδομένα ξεχωρίζεται ένα άτομο), τη διασυνδεσιμότητα (διασύνδεση δύο στοιχείων που αφορούν το ίδιο άτομο) και την επαγωγή (συνάγονται, με σημαντική πιθανότητα, άγνωστες πληροφορίες για ένα άτομο).*»

Οι διεργασίες ανωνυμοποίησης και οι επιθέσεις εκ νέου ταυτοποίησης είναι ενεργά πεδία έρευνας. Για έναν υπεύθυνο επεξεργασίας που υλοποιεί λύσεις ανωνυμοποίησης έχει ζωτική σημασία να παρακολουθεί τις πρόσφατες εξελίξεις σ' αυτόν τον τομέα, ιδίως όσον αφορά τα δεδομένα θέσης (που προέρχονται από τηλεπικοινωνιακούς φορείς εκμετάλλευσης και/ή υπηρεσίες της κοινωνίας των πληροφοριών) τα οποία είναι γνωστό ότι είναι εξαιρετικά δύσκολο να ανωνυμοποιηθούν.

4.3. Προστασία των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού

Σε πολλές περιπτώσεις, έχει αποδειχθεί ότι δεδομένα θέσης που θεωρείτο ότι είχαν ανωνυμοποιηθεί ίσως να μην είχαν ανωνυμοποιηθεί στην πραγματικότητα και να μπορούσαν να οδηγήσουν σε ταυτοποίηση του ατόμου στο οποίο αδορούσαν. Τα ίχνη των

μετακινήσεων των ατόμων από τη φύση τους συσχετίζονται μεταξύ τους και είναι μοναδικά. Ως εκ τούτου, μπορούν, υπό ορισμένες προϋποθέσεις, να είναι ευάλωτα σε προσπάθειες εκ νέου ταυτοποίησης.

Το άρθρο 25 του ΓΚΠΔ επικεντρώνεται στην προστασία δεδομένων από το σχεδιασμό και - εξ ορισμού Η προστασία δεδομένων εξ ορισμού διασφαλίζει την ελαχιστοποίηση των δεδομένων κατά την επεξεργασία. Δηλαδή, μόνο οι απαραίτητες πληροφορίες που αφορούν ένα υποκείμενο των δεδομένων συλλέγονται και διατηρούνται. Εάν η προστασία δεδομένων κατά τον σχεδιασμό εφαρμόζεται με κατάλληλα τεχνικά μέτρα, θα εξασφαλίσει αυτόματα το σεβασμό και την προστασία των δεδομένων εξ ορισμού. Η προστασία των δεδομένων από τον σχεδιασμό είναι μια θεμελιώδης τεχνική έννοια που πρέπει να λαμβάνεται υπόψη από τους υπευθύνους επεξεργασίας. Πρόκειται ουσιαστικά για «*εγγυήσεις που παρέχονται στα προσωπικά δεδομένα μέσω του τεχνολογικού σχεδιασμού*». Η αποτελεσματικότητα βρίσκεται στο επίκεντρο της έννοιας της προστασίας των δεδομένων ήδη από τον σχεδιασμό. Η απαίτηση περί εφαρμογής των αρχών με αποτελεσματικό τρόπο σημαίνει ότι οι υπεύθυνοι επεξεργασίας πρέπει να εφαρμόζουν τα αναγκαία μέτρα και εγγυήσεις ώστε να προστατεύουν αυτές τις αρχές, προκειμένου να διασφαλίζονται τα δικαιώματα των υποκειμένων των δεδομένων. Κάθε εφαρμοζόμενο μέτρο θα πρέπει να παράγει τα επιδιωκόμενα αποτελέσματα για την επεξεργασία που προβλέπεται από τον υπεύθυνο επεξεργασίας. Αυτό συνεπάγεται, ότι η διάταξη του άρθρου 25 του ΓΚΠΔ, δεν απαιτεί εφαρμογή συγκεκριμένων τεχνικών και οργανωτικών μέτρων, αλλά ότι τα επιλεγόμενα από τον υπεύθυνο επεξεργασίας μέτρα και εγγυήσεις θα πρέπει να αφορούν ειδικά την εφαρμογή των αρχών προστασίας των δεδομένων στο πλαίσιο της εκάστοτε επεξεργασίας. Ως εκ τούτου, τα μέτρα και οι εγγυήσεις θα πρέπει να σχεδιάζονται με τρόπο ώστε να είναι άρτια και ο υπεύθυνος επεξεργασίας θα πρέπει να μπορεί να εφαρμόζει περαιτέρω μέτρα ώστε να έχει τη δυνατότητα να προσαρμόζεται σε τυχόν αύξηση του κινδύνου. Ο βαθμός αποτελεσματικότητας των μέτρων εξαρτάται, κατά συνέπεια, από το πλαίσιο της εκάστοτε επεξεργασίας και από μια αξιολόγηση ορισμένων στοιχείων που πρέπει να λαμβάνονται υπόψη κατά τον προσδιορισμό των μέσων επεξεργασίας

Τα εφαρμοζόμενα μέτρα και εγγυήσεις θα πρέπει να επιτυγχάνουν το επιθυμητό αποτέλεσμα από πλευράς προστασίας δεδομένων και ο υπεύθυνος επεξεργασίας θα πρέπει να διαθέτει τεκμηρίωση των εφαρμοζόμενων τεχνικών και οργανωτικών μέτρων. Για να το

επιτύχει αυτό, ο υπεύθυνος επεξεργασίας μπορεί να καθορίζει τους κατάλληλους δείκτες επιδόσεων για την απόδειξη της αποτελεσματικότητας. Ένας δείκτης επίδοσης συνιστά μετρήσιμη τιμή που επιλέγεται από τον υπεύθυνο επεξεργασίας, η οποία καταδεικνύει το πόσο αποτελεσματικά επιτυγχάνει ο υπεύθυνος επεξεργασίας τον στόχο του σε ό,τι αφορά την προστασία των δεδομένων. Οι δείκτες επιδόσεων μπορούν να είναι ποσοτικοί, όπως το ποσοστό των ψευδώς θετικών ή ψευδώς αρνητικών αποτελεσμάτων, η μείωση των καταγγελιών, η μείωση του χρόνου απάντησης όταν τα υποκείμενα των δεδομένων ασκούν τα δικαιώματά τους, ή να είναι ποιοτικοί, όπως αξιολογήσεις επιδόσεων, χρήση κλιμάκων βαθμολόγησης ή αξιολόγηση από εμπειρογνώμονες. Εναλλακτικά προς τους δείκτες επιδόσεων, οι υπεύθυνοι επεξεργασίας μπορούν ενδεχομένως να αποδεικνύουν την αποτελεσματική εφαρμογή των αρχών δηλώνοντας το σκεπτικό τους πίσω από την αξιολόγηση της αποτελεσματικότητας των επιλεγόμενων μέτρων και εγγυήσεων.

Επί του παρόντος, για τη διαχείριση των μεγάλων δεδομένων, τα χειροκίνητα συστήματα αντικαθίστανται από αυτόματα συστήματα. Οι διαδικασίες επεξεργασίας και χειρισμού των δεδομένων εφαρμόζονται με καλύτερο τρόπο όταν ενσωματώνονται στην τεχνολογία.

5. ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΙΔΙΩΤΙΚΟΥ ΒΙΟΥ & ΠΕΡΙΟΡΙΣΜΟΙ

Η προστασία του ιδιωτικού και οικογενειακού βίου κατοχυρώνεται τόσο στο άρθρο 9 παρ.1 του Συντ. όσο και στο άρθρο 7 του ΧΘΔΕΕ και 8 της ΕΣΔΑ. Φορείς του δικαιώματος είναι κατ' αρχήν τα φυσικά πρόσωπα, Έλληνες και αλλοδαποί. Το δικαίωμα δεν φαίνεται να προσιδιάζει στα νομικά πρόσωπα, αφού αυτά δεν διαθέτουν «ιδιωτική ζωή». Αποδέκτης είναι η κρατική εξουσία, που οφείλει να μην προσβάλλει με πράξεις της τον ιδιωτικό ή οικογενειακό βίο, αλλά και να λαμβάνει θετικά μέτρα για την προστασία του δικαιώματος αυτού από προσβολές τρίτων. Παρά την κανονιστική «συστέγαση» του δικαιώματος αυτού με το δικαίωμα στο άσυλο της κατοικίας, το ίδιο αποτελεί έννοια γένους, αφού καλύπτει ευρύτερο πεδίο προστασίας (Γεωργόπουλος Γ., Μπουκουβάλα Β. 2021).

Ο ιδιωτικός και οικογενειακός βίος αντιδιαστέλλεται από τον δημόσιο βίο και καλύπτει μία σφαίρα απορρήτου κάθε προσώπου, ένα σύνολο σχέσεων ή δραστηριοτήτων που θέλει να κρατήσει κρυφά από τη δημοσιότητα ή εντός ενός στενού κύκλου προσώπων. Υπάρχει

μάλιστα ένας απαραβίαστος πυρήνας του δικαιώματος ο οποίος δεν μπορεί κατ' αρχήν να προσβληθεί. Έτσι, σε ζητήματα που αφορούν στην υγεία, την ερωτική ζωή, τις οικογενειακές σχέσεις, τη σωματική και ψυχική κατάσταση του ανθρώπου δεν μπορεί να διεισδύσει κανείς, χωρίς τη ρητή συγκατάθεση του φορέα του δικαιώματος. Ωστόσο, το δικαίωμα αυτό υπόκειται σε περιορισμούς, οι οποίοι, όμως, πρέπει να προβλέπονται από τον νόμο, να επιδιώκουν την εξυπηρέτηση ενός σκοπού δημοσίου συμφέροντος ή άλλου θεμιτού στόχου και να τηρείται η αρχή της αναλογικότητας. Εξάλλου, περιορισμοί μπορεί να προκύψουν εν τοις πράγμασι από τη σύγκρουση του δικαιώματος αυτού με το δικαίωμα ενός τρίτου προσώπου.

Μετά την αναθεώρηση του 2001 βρίσκει πλέον ρητή συνταγματική κατοχύρωση στο άρθρο 9Α του Συντ. το δικαίωμα της πληροφορικής αυτοδιάθεσης ή προστασίας των προσωπικών δεδομένων, αφού, πλέον, είναι δυνατή, στην κοινωνία της πληροφορίας, με τις σύγχρονες τεχνολογικές εξελίξεις, η ηλεκτρονική παρακολούθηση, καταχώρηση και επεξεργασία των προσωπικών πληροφοριών των προσώπων. Το ίδιο δικαίωμα κατοχυρώνεται στο άρθρο 8 του ΧΘΔΕΕ. Το άρθρο αυτό αφορά τη συλλογή, καταχώρηση και επεξεργασία προσωπικών δεδομένων μέσω κυρίως των ηλεκτρονικών υπολογιστών (ιδίως με ηλεκτρονικά μέσα), αν και μπορεί να εφαρμοστεί και στην περίπτωση της προβολής προσωπικών πληροφοριών μέσω των ραδιοτηλεοπτικών μέσων. Προσωπικό δεδομένο, ως αναφέρθηκε και ανωτέρω, είναι «κάθε πληροφορία που αφορά ένα φυσικό πρόσωπο, του οποίου η ταυτότητα είναι γνωστή ή μπορεί να προσδιοριστεί άμεσα ή έμμεσα ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός ή περισσοτέρων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική». Ως εκ τούτου, το δικαίωμα αυτό δεν προστατεύει αποκλειστικά την πληροφοριακή ιδιωτικότητα, αφού στο πεδίο προστασίας του υπάγονται όχι μόνον οι απόρρητες πληροφορίες, αλλά και κάθε πληροφορία που αφορά ένα πρόσωπο, ακόμη κι αν προορίζεται προς εξωτερίκευση στη δημόσια σφαίρα . Σε ό,τι δε αφορά τα καλούμενα ευαίσθητα προσωπικά δεδομένα, ήτοι την κατηγορία εκείνη των προσωπικών δεδομένων που αποτελούν τον σκληρό πυρήνα της ιδιωτικότητας του ατόμου (λόγου χάρη στοιχεία ερωτικής ζωής, ιατρικά δεδομένα και πληροφορίες υγείας , κοκ) γίνεται δεκτό ότι η πάσης φύσεως επεξεργασία τους υπόκειται σε εντονότερους περιορισμούς και απαιτείται προς τούτο άδεια εκ μέρους της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Η συνταγματική διάταξη δεν ιδρύει μία

απόλυτη απαγόρευση συλλογής, χρήσης, επεξεργασίας και δημοσιοποίησης των προσωπικών δεδομένων, αλλά επιτάσσει στο κράτος να θεσπίσει το αναγκαίο θεσμικό πλαίσιο για την προστασία τους. Σύμφωνα με το ισχύον πάντως θεσμικό πλαίσιο η συλλογή και επεξεργασία προσωπικών δεδομένων είναι νόμιμη υπό συγκεκριμένες προϋποθέσεις, ενώ το άτομο διαθέτει, υπό περιπτώσεις, την εξουσία να ορίζει και να καθορίζει τη ροή των προσωπικών του πληροφοριών προς τους τρίτους.Η συνταγματική διάταξη δεν ιδρύει μία απόλυτη απαγόρευση συλλογής, χρήσης, επεξεργασίας και δημοσιοποίησης των προσωπικών δεδομένων, αλλά επιτάσσει στο κράτος να θεσπίσει το αναγκαίο θεσμικό πλαίσιο για την προστασία τους. Σύμφωνα με το ισχύον πάντως θεσμικό πλαίσιο κάθε συλλογή και επεξεργασία προσωπικών δεδομένων είναι κατ' αρχήν μη νόμιμη, εκτός αν συγκατατεθεί προς τούτο ο φορέας τους. Το άτομο δηλαδή διαθέτει την εξουσία να ορίζει και να καθορίζει τη ροή των προσωπικών του πληροφοριών προς τους τρίτους. Το εν λόγω συνταγματικό δικαίωμα στην προστασία των προσωπικών δεδομένων μπορεί να αναλυθεί κατά τα πρότυπα του αντίστοιχου άρθρου του Χάρτη (8 παρ. 2), από το οποίο συνάγονται τρεις βασικοί κανόνες ως προς τη σύννομη επεξεργασία τους: α) πρέπει αυτή να προβλέπεται σε ρητή διάταξη νόμου ή να έχει συγκατατεθεί προς τούτο το υποκείμενο του δικαιώματος, β) θα πρέπει να υφίσταται ένας νόμιμος και θεμιτός σκοπός της τοιαύτης επεξεργασίας, όπως η άσκηση δικαιωμάτων τρίτων (έννομη προστασία, δικαίωμα πληροφόρησης, ελευθερία της έρευνας) ή η επιδίωξη σκοπού υπέρτερου δημοσίου συμφέροντος (εθνική ασφάλεια, διακρίβωση εγκλημάτων, δημόσια υγεία, φορολογικοί και συναφείς έλεγχοι) και γ) το άτομο οφείλει να ασκεί πλήρως τα σχετικά του δικαιώματα, κυρίως, δε, το δικαίωμα πρόσβασης και διόρθωσης των προσωπικών του πληροφοριών.

Από τη θέση σε ισχύ της Συνθήκης της Λισαβόνας, η νομική φύση του δικαιώματος στην προστασία προσωπικών δεδομένων έχει αναγνωριστεί στο πρωτογενές Ενωσιακό δίκαιο, καθώς το άρθρου 8 του ΧΘΔΕΕ κατοχυρώνει την προστασία των δεδομένων προσωπικού χαρακτήρα ως γενικά ισχύον θεμελιώδες δικαίωμα. Η ανάπτυξη ενός αυτοτελούς, ανεξάρτητου δικαιώματος προστασίας των δεδομένων στο άρθρο 8 του Χάρτη αντανακλά μια μάλλον ασυνήθιστη πορεία, διότι του δικαιώματος προηγήθηκε λεπτομερής δευτερογενής νομοθεσία που ρυθμίζει την επεξεργασία δεδομένων. Οι αιτιολογικές εκθέσεις που συνοδεύουν τον Χάρτη αναφέρουν ότι το δικαίωμα βασίστηκε μεταξύ άλλων στην οδηγία για την προστασία των δεδομένων, υποδηλώνοντας έτσι ότι το δευτερογενές

νομικό πλαίσιο είναι κατά κάποιο τρόπο σχετικό με την έννοια του δικαιώματος. Αυτή η αναφορά στο παράγωγο δίκαιο εγείρει ωστόσο σημαντικά ερωτήματα, σχετικά με τη σχέση μεταξύ του δικαιώματος και του παράγωγου νομικού πλαισίου: θα πρέπει το δικαίωμα να ερμηνεύεται υπό το πρίσμα του παράγωγου νομικού πλαισίου, δεδομένου ότι το τελευταίο υπήρξε μία από τις πηγές έμπνευσης του δικαιώματος, ή θα πρέπει το παράγωγο νομικό πλαίσιο να ερμηνεύεται υπό το πρίσμα του δικαιώματος; Δεδομένου ότι τα θεμελιώδη δικαιώματα έχουν υψηλότερη κανονιστική αξία, θα ήταν παράδοξο να επιτραπεί στο παράγωγο δίκαιο να προσδώσει νόημα στο θεμελιώδες δικαίωμα. Ταυτόχρονα, η ερμηνεία του παράγωγου δικαίου υπό το πρίσμα του δικαιώματος θα απαιτούσε σαφή κατανόηση της ουσίας του δικαιώματος.

Πολλές είναι οι προκλήσεις για την προστασία του δικαιώματος αυτού στις μέρες μας. Ιδίως με την εξέλιξη του διαδικτύου και των ψηφιακών τεχνολογιών ενημέρωσης και επικοινωνίας, η επεξεργασία προσωπικών δεδομένων αποτελεί συστατικό στοιχείο του επιχειρηματικού μοντέλου πολλών επιχειρήσεων. Κατά συνέπεια το αίτημα για την προστασία των δεδομένων που είναι το «νέο νόμισμα» για πολλούς τομείς της οικονομίας δεν τίθεται μόνο ως προς τη διάσταση προστασίας του πολίτη από παρεμβάσεις εκ μέρους του κράτους ή τρίτων, αλλά είναι και ζήτημα ανταγωνιστικότητας της οικονομίας μας.

Η αναγνώριση της προστασίας των δεδομένων ως θεμελιώδους δικαιώματος στον Χάρτη της ΕΕ έχει νομικές συνέπειες, ιδίως όσον αφορά τον τρόπο με τον οποίο θα πρέπει πλέον να γίνει κατανοητή η σχέση μεταξύ του δικαιώματος και του παράγωγου νομικού πλαισίου της ΕΕ για την προστασία των δεδομένων. Κατ' αρχάς, πρέπει να σημειωθεί ότι τα θεμελιώδη δικαιώματα παραδοσιακά αποσκοπούν στην προστασία των πολιτών έναντι των κρατών: η ΕΣΔΑ, για παράδειγμα, αναγνωρίζει πρώτα και κύρια αρνητικές υποχρεώσεις ("negative obligations"[3]) για τα κράτη, με σκοπό να απέχουν από αδικαιολόγητες παρεμβάσεις στα θεμελιώδη δικαιώματα. Για ορισμένα δικαιώματα μπορεί επίσης να υπάρχουν θετικές υποχρεώσεις ('positive obligations'[4]), οι οποίες απαιτούν από τα κράτη να αναλάβουν δράση

[3] Οι αρνητικές υποχρεώσεις (negative obligations) υποχρεώνουν τις αρχές ενός Κράτους να μην ενεργούν κατά τρόπο που να αποτελεί αδικαιολόγητη παρέμβαση στα δικαιώματα της Σύμβασης. Τα περισσότερα δικαιώματα της Σύμβασης διατυπώνονται κατ΄ αυτόν τον τρόπο.

[4] Οι θετικές υποχρεώσεις (positive obligations) υποχρεώνουν τις αρχές ενός Κράτους να λάβει ενεργά μέτρα προκειμένου να διασφαλίσει τα δικαιώματα της Σύμβασης. Στις περισσότερες περιπτώσεις, τα μέτρα αυτά δεν αναφέρονται ρητά στο κείμενο αλλά έχουν υπονοηθεί σε αυτό από το Δικαστήριο.

για να διασφαλίσουν ότι τα άτομα απολαμβάνουν αποτελεσματικά τα δικαιώματά τους. Οι Συνθήκες της ΕΕ αναμφισβήτητα πυροδοτούν μια τέτοια θετική υποχρέωση σε σχέση με την προστασία των δεδομένων, καθώς το άρθρο 16 ΣΛΕΕ, αφού διακηρύσσει ότι όλοι έχουν δικαίωμα στην προστασία των προσωπικών τους δεδομένων, απαιτεί από τον νομοθέτη της ΕΕ να "θεσπίσει τους κανόνες" που αφορούν την προστασία αυτή. Δεύτερον, τα περισσότερα θεμελιώδη δικαιώματα -συμπεριλαμβανομένου του δικαιώματος στην προστασία των δεδομένων- δεν είναι απόλυτα, αλλά μπορούν να περιοριστούν για λόγους γενικού συμφέροντος του κοινού ή για την προστασία των δικαιωμάτων άλλων.

Οι προϋποθέσεις για τους περιορισμούς των θεμελιωδών δικαιωμάτων παρατίθενται στο άρθρο 52 παράγραφος 1 του Χάρτη και περιλαμβάνουν την ανάγκη σεβασμού της ουσίας του δικαιώματος, την αναγκαιότητα και την αναλογικότητα. Σε μεγάλο βαθμό αυτές αντικατοπτρίζουν τις προϋποθέσεις για τους δικαιολογημένους περιορισμούς που υπάρχουν και στην ΕΣΔΑ. Τρίτον, ο δικαστικός έλεγχος για την επαλήθευση της συμμόρφωσης με τις υποχρεώσεις των θεμελιωδών δικαιωμάτων δεν είναι, τουλάχιστον στο πλαίσιο της ΕΣΔΑ, ταυτόσημος σε περιπτώσεις που αφορούν αρνητική υποχρέωση ή θετική υποχρέωση. Ενώ και για τους δύο τύπους υποχρεώσεων ο στόχος είναι να επιτευχθεί δίκαιη ισορροπία μεταξύ των αντικρουόμενων συμφερόντων, για τις αρνητικές υποχρεώσεις εφαρμόζεται αυστηρότερος έλεγχος των προϋποθέσεων σχετικά με τους δικαιολογημένους περιορισμούς και κατά πόσον έχει επιτευχθεί δίκαιη ισορροπία. Στην περίπτωση των θετικών υποχρεώσεων αναγνωρίζεται ένα ευρύτερο περιθώριο εκτίμησης, καθώς τα δικαστήρια μπορεί να διστάζουν να αντικαταστήσουν με τη δική τους κρίση τη στάθμιση που πραγματοποιούν τα κράτη. Για τις θετικές υποχρεώσεις το ΕΔΔΑ φαίνεται ότι προχωρά "με έναν βαθμό επιφυλακτικότητας που σπάνια συναντάται στο πλαίσιο του ελέγχου των αρνητικών υποχρεώσεων".

Υπό το πρίσμα των ανωτέρω, ο ΓΚΠΔ θα μπορούσε να θεωρηθεί ότι αντανακλά την θετική υποχρέωση. Στην πραγματικότητα, ενώ το δικαίωμα στην προστασία των δεδομένων πρέπει να προστατεύεται ειδικότερα, ο ΓΚΠΔ αποσκοπεί στην προστασία όλων των θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων που ενδέχεται να εμπλέκονται στο πλαίσιο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Για να διασφαλιστεί η προστασία αυτή, ο ΓΚΠΔ θέτει ουσιαστικά μια τέτοια βάση για τη δίκαιη στάθμιση, η οποία στο σύνολό της παρέχει μια λεπτομερή πραγμάτωση των προϋποθέσεων για τους

δικαιολογημένους περιορισμούς που περιέχονται στο άρθρο 52 παράγραφος 1 του Χάρτη. Αυτό το σύστημα δίκαιης στάθμισης στον ΓΚΠΔ καθορίζει ωστόσο κυρίως τον τρόπο με τον οποίο πρέπει να επιτευχθεί η ισορροπία, αντί να επιτυγχάνεται οριστικά η ίδια η ισορροπία μεταξύ των ανταγωνιστικών δικαιωμάτων και συμφερόντων. Ερωτήματα όπως το κατά πόσον μια πράξη επεξεργασίας είναι δίκαιη, ή νόμιμη, ή αναλογική είναι ανοικτά και επαφίενται στην κρίση του υπευθύνου επεξεργασίας (*A. Christofidi et al, 2020*). Οι υπεύθυνοι επεξεργασίας διαθέτουν σημαντικά περιθώρια διακριτικής ευχέρειας και εξουσίας λήψης αποφάσεων όταν πρόκειται για τέτοιου είδους αποφάσεις.

Αυτή η διακριτική ευχέρεια που παρέχεται στους υπευθύνους επεξεργασίας είναι κατανοητή, ιδίως για την επεξεργασία που αφορά ιδιωτικά συμφέροντα και τον ιδιωτικό τομέα. Υπάρχει μια "εύλογη οικονομική ανησυχία" ότι "οι ιδιωτικές επιχειρήσεις δεν θα πρέπει να επιβαρύνονται υπερβολικά από τις υποχρεώσεις προστασίας των δεδομένων". Επιπλέον, οι ιδιωτικοί φορείς δεν είναι οι αποδέκτες των υποχρεώσεων θεμελιωδών δικαιωμάτων. Αν και η άσκηση θετικών υποχρεώσεων μπορεί να απαιτεί από τα κράτη να παρεμβαίνουν και να ρυθμίζουν τις οριζόντιες σχέσεις μεταξύ ιδιωτών, ώστε να διασφαλίζουν ότι τα άτομα προστατεύονται από παραβιάσεις των δικαιωμάτων τους από ιδιωτικές οντότητες, τα κράτη έχουν διακριτική ευχέρεια ως προς τον τρόπο επίτευξης της προστασίας αυτής. Στην ουσία, ο ΓΚΠΔ αντικατοπτρίζει την επιλογή του νομοθέτη της ΕΕ να καταστήσει υπεύθυνο τον υπεύθυνο επεξεργασίας παρέχοντας ένα σύστημα έλεγχου και στάθμισης που θα πρέπει τελικά να τον καθοδηγεί προς τη δίκαιη εξισορρόπηση. Εντούτοις, αυτός ο βαθμός διακριτικής ευχέρειας μπορεί να είναι πιο προβληματικός για τις δημόσιες αρχές που επεξεργάζονται δεδομένα για σκοπούς δημοσίου συμφέροντος. Εκεί, αυτό που μπορεί να διακυβεύεται δεν είναι μόνο η θετική υποχρέωση προστασίας, αλλά και η αρνητική υποχρέωση των δημόσιων αρχών να μην παρεμβαίνουν στα δικαιώματα. Λαμβάνοντας υπόψη τη θέση του ΔΕΕ ότι το δικαίωμα στην προστασία των δεδομένων θίγεται κάθε φορά που γίνεται επεξεργασία δεδομένων προσωπικού χαρακτήρα, θα μπορούσε να υποστηριχθεί ότι με την επεξεργασία προσωπικών δεδομένων εξ ορισμού οι κρατικές αρχές παραβιάζουν την αρνητική τους υποχρέωση να μην παρεμβαίνουν στο δικαίωμα. Ομολογουμένως, η παρέμβαση αυτή μπορεί να δικαιολογηθεί μέσω της προσφυγής στο άρθρο 52 παράγραφος 1 και στο άρθρο 8 παράγραφοι 2 και 3 του Χάρτη, ωστόσο ο έλεγχος της δίκαιης εξισορρόπησης είναι αναμφισβήτητα αυστηρότερος στο

πλαίσιο των αρνητικών υποχρεώσεων. Δεν είναι βέβαιο ότι η ευρεία δομή δίκαιης εξισορρόπησης που καθιερώνει ο ΓΚΠΔ μπορεί να ανταποκριθεί στις αυστηρότερες απαιτήσεις που ισχύουν συνήθως για τους κρατικούς φορείς στο δίκαιο των θεμελιωδών δικαιωμάτων. Στην πραγματικότητα, με το να καθιστά πρόσθετες νομικές βάσεις απαραίτητες για την επεξεργασία προς το δημόσιο συμφέρον, ο ΓΚΠΔ υποδηλώνει το αντίθετο: ο νομοθέτης θα πρέπει να προκαθορίσει και να επιτύχει τη δίκαιη εξισορρόπηση σε αυτές τις περιπτώσεις, λαμβάνοντας δεόντως υπόψη τις προϋποθέσεις για τους περιορισμούς των θεμελιωδών δικαιωμάτων που θεσπίζονται στον Χάρτη, την ΕΣΔΑ και τη νομολογία του ΔΕΕ και του ΕΔΔΑ.

ΣΥΜΠΕΡΑΣΜΑ

Τα πλεονεκτήματα που μπορούν να προσφέρουν οι τεχνολογίες crowd monitoring και Wi-Fi στην σύγχρονη ζωή και την καθημερινότητά μας είναι αμέτρητα. Προκειμένου, όμως να πληρούνται οι προϋποθέσεις της νομοθεσίας προστασίας προσωπικών δεδομένων και να προστατεύεται ουσιαστικά η ιδιωτική ζωή των ατόμων, έμφαση πρέπει να δοθεί σε λιγότερο παρεμβατικές τεχνικές crowd monitoring οι οποίες προστατεύουν την ιδιωτικότητα των ατόμων. Τόσο σε εθνικό όσο και σε ευρωπαϊκό επίπεδο, έχει θεσμοθετηθεί ένα σύνολο νομοθετημάτων που εξετάζει και ορίζει το πλαίσιο και τις αρχές που πρέπει να διέπουν, τη συλλογή και επεξεργασία προσωπικών δεδομένων. Από τα ως άνω νομοθετήματα, καθίσταται σαφές ότι στο επίκεντρο της προστασίας των διατάξεών τους τίθεται το ίδιο το άτομο – υποκείμενο των δεδομένων από κινδύνους που σχετίζονται με τη μη νόμιμη χρήση και επεξεργασία των προσωπικών τους δεδομένων και παραβίαση της ιδιωρτικότητάς τους.

Τόσο οι τεχνικές crowd monitoring με βάση την εικόνα όσο και οι υπόλοιπες τεχνικές μπορούν να θέσουν σε κίνδυνο την ιδιωτικότητα ενός ατόμου, είτε μέσω της αναγνώρισης προσώπου είτε μέσω της παρακολούθησης των σημάτων της συσκευής που φέρει μαζί του.. Η χρήση αισθητήρων έχει μεγάλες δυνατότητες, καθώς η συνένωση διαφορετικών τεχνολογιών μπορεί να χρησιμοποιηθεί για την ανάπτυξη ενός προηγμένου και ισχυρού συστήματος crowd monitoring. Για παράδειγμα, τα πλεονεκτήματα και τα μειονεκτήματα του WiFi και των κυψελοειδών δικτύων (κόστος, κάλυψη και ποιότητα δεδομένων) αλληλοσυμπληρώνονται. Επομένως, η χρήση της συγχώνευσης αισθητήρων και των δικτύων πολλαπλής πιστότητας πρέπει να ληφθεί υπόψη κατά την ανάπτυξη μελλοντικών

συστημάτων παρακολούθησης. Με τον τρόπο αυτό θα διασφαλιστεί ότι η όποια αδυναμία, αστοχία, ανεπάρκεια του ενός συστήματος θα καλυφθεί από το άλλο. Το crowd monitoring αποτελεί σημαντικό ερευνητικό πεδίο και για την ανάπτυξη αποτελεσματικών τεχνολογιών, είναι απαραίτητο να γίνονται δοκιμές των νέων προτεινόμενων τεχνικών σε διαφορετικά σενάρια πλήθους.

Όπως έγινε αντιληπτό ανωτέρω, η προστασία της ιδιωτικής ζωής αποτελεί μεγάλη πρόκληση για τον τομέα του crowd monitoring. Είναι προφανές ότι δεν έχει καταβληθεί μεγάλη προσπάθεια για τη διαφύλαξη της ιδιωτικής ζωής και τη μη παρεμβατική παρακολούθηση του πλήθους. Με την εφαρμογή των πρόσφατων και πιο αυστηρών κατευθυντήριων γραμμών, όπως αποτυπώνονται στον ΓΚΠΔ, αναμένεται ότι οι αναδυόμενες τεχνικές παρακολούθησης πλήθους θα είναι υποχρεωμένες να λαμβάνουν μέτρα προστασίας της ιδιωτικής ζωής των ατόμων. Παρόλο που αυτό σημαίνει ότι οι υπάρχουσες τεχνικές παρακολούθησης ενδεχομένως να καταστούν παρωχημένες, οι εξελίξεις στο πεδίο της νομοθεσίας, θα επισπεύσουν την επιστημονική έρευνα στον τομέα του crowd monitoring. Οι διάφορες τεχνικές crowd monitoring έχουν ποικίλες απαιτήσεις σε δεδομένα και, συνεπώς, διαφορετικές ανησυχίες για την προστασία της ιδιωτικής ζωής. Οι διάφορες τεχνικές crowd monitoring εμφανίζουν διαφορετικές δυνατότητες επεξεργασίας δεδομένων και, συνεπώς, ποικίλες προκλήσεις όσον αφορά την προστασία της ιδιωτικής ζωής ανακύπτουν.

Αυτό επιφέρει ερωτήματα σχετικά, μεταξύ άλλων, με τη συγκατάθεση του κόσμου, όταν παρακολουθείται. Ειδικότερα η χρήση καμερών και τεχνολογιών αναγνώρισης προσώπου, μπορεί να θέσει σε κίνδυνο την ιδιωτικότητα των ατόμων. Ωστόσο, αυτού του είδους η εντατική παρακολούθηση είναι γενικά απαραίτητη για τους υπεύθυνους ασφαλείας. Από τη σκοπιά της ερευνητικής δεοντολογίας, το να αποφεύγει κάποιος τις κάμερες αποτελεί ένδειξη ότι ασκεί το δικαίωμά του να μην είναι μέρος μιας συγκεκριμένης δοκιμής ή ότι προστατεύει το δικαίωμά του στην ιδιωτική ζωή. Από την άποψη της αστυνόμευσης, η ίδια συμπεριφορά μπορεί να αποκτήσει διαφορετικό νόημα και να χρησιμεύσει ως ένδειξη ύποπτης συμπεριφοράς. Στην περίπτωση της παρακολούθησης μέσω WiFi και Bluetooth, οι διευθύνσεις MAC των συσκευών προκαλούν προβληματισμό σχετικά με την προστασία της ιδιωτικής ζωής. Από ερευνητική σκοπιά, μπορεί να διασφαλιστεί ότι η ταυτότητα των ατόμων προστατεύεται μέσω της κρυπτογράφησης δεδομένων πριν από την αποθήκευση

δεδομένων. Σε κάθε περίπτωση, θα πρέπει να παρέχεται προηγούμενη ενημέρωση των ατόμων σχετικά με την εγκατάσταση και λειτουργία του συστήματος. Από τα ανωτέρω εκτιθέμενα γίνεται σαφές, ότι τα συστήματα crowd monitoring, στην πλειονότητά τους παραβιάζουν το δικαιώμα στην ιδωτική ζωή και δεν συμμορφώνονται με το ευρωπαϊκό πλαίσιο προστασίας προσωπικών δεδομένων.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Ribeiro-Navarrete S., Saura J.R., Palacios-Marques D.,2021. Towards a new era of mass data collection: Assessing pandemic surveillance technologies to preserve user privacy.
Available at: *https://www.sciencedirect.com/science/article/pii/S004016252100113X?via%3Dihub*
[Accessed 30 July 2023]

Habibzadeh H., Nussbaum B., Anjomshoa F., Kantarci B. Soyata T., 2019. A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities.
Available at:
https://www.sciencedirect.com/science/article/abs/pii/S2210670718316883?via%3Dihub
[Accessed 11 July 2023]

K. ten Berg, Ton A. M. Spil, and Effing R., 2019. The Privacy Paradox of Utilizing the Internet of Things and Wi-Fi Tracking in Smart Cities. IFIP International Federation for Information Processing 2019, Published by Springer Nature Switzerland AG 2019, pp. 364–381, 2019.

Gambino A. M. and Tuzzolino D., 2021. Location Data and Privacy. Springer Nature Singapore Pte Ltd. 2022, R. Senigaglia et al. (eds.), Privacy and Data Protection in Software Services,

Sathyamoorthy A. J., Patel U., Savle Y.A., Paul M. and Manocha D., 2020. COVID-Robot: Monitoring Social Distancing Constraints in Crowded Scenarios
Available at:
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8635356/
[Accessed August 12 2023]

Pournajaf L., Garcia-Ulloa D.A.,Xiong L.,Sunderam V, 2015. Participant Privacy in Mobile Crowd Sensing Task Management: A survey of Methods and Challenges. Newsletter on ACM SIGMOD Record, vol.44, issue.4, pp.23-24
Available at:
https://dl.acm.org/doi/10.1145/2935694.2935700
[Accessed 25 August 2023]

Xiao Y., Simoens P., Padmanabhan P., Ha K., Satyanarauanan M., 2013. Lowering the barriers to large-scale mobile crowdsensing, in Proc. of the 14th Workshop on Mobile Computing Systems and Applications, pp.1-6, Jekyll Island.
Available at:
https://elijah.cs.cmu.edu/DOCS/xiao-hotmobile-crowd-2013.pdf
[Accessed 17 August 2023]

B.Guo, Z. Yu, D. Zhang, X. Zhou, 2014.From Participatory Sensing to Mobile Crowd Sensing.in Proc. of the 12th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshop), pp.593-598.

Available at:
http://www.guob.org/research/MCS_Guo.pdf
[Accessed 2 August 2023]

Nguyen T.N., Zeadally S.,2021. Mobile Crowd-sensing Applications: Data Redundancies, Challenges, and Solutions. ACM Transactions on Internet Technology, Vol. 22, No. 2, Article 48.

Breuer J., Zeeland I.V., Pierson J., Heyman R., 2019. The Social Construction of Personal Data Protection in Smart Cities.

Singh U., Determe J. F., Horlin F., Doncker P. D., 2020. Crowd Monitoring: State-of-the-Art and Future Directions.

Li, X., Yu Q., Alzahrani B., Barnawi A., Alhindi A. Alghazzawi A., Miao Y. 2021, Data Fusion for Intelligent Crowd Monitoring and Management Systems: A Survey

Singh U., Determe J. F., Horlin F., Doncker P. D., Azzagnuni S, 2022, Monitoring Large Crowds With WiFi: A Privacy-Preserving Approach.

Laufs J. Borrion H., Bradford B., 2020. Security and the Smart City: A Systematic Review.

Depatla S. and Mostofi Y., 2018. Passive Crowd Speed Estimation and Head Counting Using WiFi.

Christofi A., 2019, Smart cities and the data protection framework in context

Tyagi A. K., Shamilab M., 2019. Spy in the Crowd: How User's Privacy is getting affected with the Integration of Internet of Thing's Devices. International Conference on Sustainable Computing in Science, Technology & Management.

Breuer J. and Pierson J., 2021, The right to the city and data protection for developing citizen-centric digital cities.

Asghar M. N., Kanwal N., Lee B., Fleury M., Herbst M. and Qiao Y., 2019. Visual Surveillance Within the EU General Data Protection Regulation: A Technology Perspective.

Wang et al. 2020, Response to COVID-19 in Taiwan Big Data Analytics, New Technology, and Proactive Testing.
Available at:
https://jamanetwork.com/journals/jama/fullarticle/2762689
[Accesed 5 August 2023]
Barkhuus L. and Dey A., 2003, Location-Based Services for Mobile Telephony: a study of users' privacy concerns.
Available at:

https://www.researchgate.net/publication/221054646_Location-Based_Services_for_Mobile_Telephony_a_Study_of_Users'_Privacy_Concerns/link/02bfe50f0ca2cb22af000000/download
[Accessed 25 July 2023]

Huadong MA, Zhao D., Yuan P., 2014. Opportunities in mobile crowd sensing. IEEE Communications Magazine, vol.52, issue.8, pp. 29-35.

Sirmacekand B, Reinartz P., 2011. Automatic crowd density and motion analysis in airborne image sequences based on a probabilistic framework. in Proc. IEEE Int. Conf. Comput. Vis. Workshops (ICCV Workshops), pp. 898–905.

Lamba S. and Nain N., 2017. Crowd Monitoring and Classification: A Survey.
Available at:
https://www.researchgate.net/publication/318134478_Crowd_Monitoring_and_Classification_A_Survey
[Accessed 20 July 2023]

Duives D., T Oijen and Hoogendoorn S., 2020. Enhancing Crowd Monitoring System Functionality through Data Fusion: Estimating Flow Rate from Wi-Fi Traces and Automated Counting System Data.
Available at:
https://www.mdpi.com/1424-8220/20/21/6032?type=check_update&version=1
[Accessed 23 July 2023]

Uhlmann J. K., 2002. Covariance consistency methods for fault-tolerant distributed data fusion,'' Inf. Fusion, vol. 4, no. 3, pp.201–215, S
Available at:
https://www.researchgate.net/publication/220338378_Covariance_consistency_methods_for_fault-tolerant_distributed_data_fusion
[Accessed 1 August 2023]

Γεωργόπουλος Γ., Μπουκουβάλα Β., 2021. Συνταγματικα Δικαιωματα και Ελευθεριες, Από τη θεωρία στην πράξη. Νομικη Βιβλιοθηκη,σελ 48-51