ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»

Ακαδημαϊκό έτος 2022-2023

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της Μιχαλοπούλου Ελένης - Μαρίας (Α.Μ.: ΜΔΙ 2130)

Smart cities και ζητήματα προστασίας προσωπικών δεδομένων

Επιβλέπουσα Καθηγήτρια :

κα Λίλιαν Μήτρου

Πειραιάς, Αύγουστος 2023

Ευχαριστίες

Θα ήθελα να ευχαριστήσω θερμά την επιβλέπουσα καθηγήτρια μου, κα Λίλιαν Μήτρου, για τη βοήθειά της στην υλοποίηση της διπλωματικής μου εργασίας.

Επίσης, θα ήθελα να ευχαριστήσω την οικογένειά μου και τους φίλους μου για την υποστήριξη και ηθική συμπαράσταση που μου πρόσφεραν καθ' όλη τη διάρκεια των μεταπτυχιακών μου σπουδών.

ΠΕΡΙΛΗΨΗ

Η παρούσα διπλωματική εργασία αποτελεί μια μελέτη του οικοσυστήματος της έξυπνης πόλης και των ζητημάτων που ενδέχεται να προκύψουν αναφορικά με την προστασία των προσωπικών δεδομένων των προσώπων που κατοικούν σε αυτήν. Αρχικά γίνεται μια παρουσίαση της έννοιας της έξυπνης πόλης, του τρόπου λειτουργίας της, των εμπλεκόμενων μερών, καθώς επίσης γίνεται μια παράθεση παραδειγμάτων έξυπνων πόλεων παγκοσμίως, προκειμένου να γίνει καλύτερα κατανοητό το πλαίσιο της παρούσας μελέτης. Εν συνεχεία γίνεται μια παρουσίαση της έννοιας του Διαδικτύου των Πραγμάτων και του τρόπου με τον οποίο συνδράμει στη λειτουργία της έξυπνης πόλης. Ακολούθως, παρουσιάζονται τα ζητήματα ασφαλείας και ιδιωτικότητας που μπορεί να προκύψουν στο πλαίσιο της έξυπνης πόλης από την συλλογή και επεξεργασία των δεδομένων των πολιτών, καθώς επίσης το νομοθετικό πλαίσιο που τα διέπει. Τέλος, παρουσιάζονται τα κύρια σημεία του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων (ΓΚΠΔ), τα προβλήματα εφαρμογής του στο οικοσύστημα της έξυπνης πόλης και τρόποι με τους οποίους μπορεί να επιτευχθεί η συμμόρφωση των έξυπνων πόλεων με αυτόν.

ABSTRACT

This diploma thesis is a study of the smart city's ecosystem and the issues that may arise from its operation regarding the protection of personal data of the people residing in it. Initially, there is a presentation of the concept of smart city, how it works, the parties involved, as well as examples of smart cities worldwide, in order to better understand the context of this study. Then, there is a presentation of the concept of Internet of Things and the ways it contributes to the operation of the smart city. Next, the security and privacy issues that may arise in the context of the smart city from the collection and processing of citizens' data are presented, as well as the legislative framework that governs them. Finally, the main points of the General Data Protection Regulation (GDPR) , the problems of its implementation in the smart city ecosystem and ways in which the compliance of smart cities with it can be achieved are presented .

SMART CITIES ΚΑΙ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ

ΠΕΡΙΕΧΟΜΕΝΑ

1. ΕΙΣΑΓΩΓΗ

Η ραγδαία ανάπτυξη της τεχνολογίας τις τελευταίες δεκαετίες έχει οδηγήσει στη μεταμόρφωση της ζωής που κάποτε ξέραμε και στη δημιουργία ενός νέου, τεχνολογικά εξελιγμένου, μέλλοντος. Στην ως άνω εξέλιξη έχουν συμβάλλει σημαντικά οι τεχνολογίες της πληροφορικής και των επικοινωνιών, οι οποίες έχουν συνδράμει στη δημιουργία έξυπνων λύσεων για τη διευκόλυνση της καθημερινότητας των ανθρώπων. Έχει ξεκινήσει, λοιπόν, μια μορφή τεχνολογικού μετασχηματισμού, στο επίκεντρο της οποίας έχουν βρεθεί οι πόλεις, δεδομένης της όλο και αυξανόμενης συγκέντρωσης του πληθυσμού της γης σε αυτές.

Σύμφωνα με μια πρόσφατη μελέτη των Ηνωμένων Εθνών, το παγκόσμιο μερίδιο του πληθυσμού των πόλεων, το οποίο ανερχόταν το 1950 σε ένα ποσοστό της τάξεως του 25%, διπλασιάστηκε, ανερχόμενο το 2020 στο 50%. Το φαινόμενο αυτό της αστικοποίησης υπολογίζεται ότι θα ενταθεί στα επόμενα πενήντα χρόνια με το ως άνω αναφερόμενο ποσοστό να αναμένεται να αυξηθεί σταδιακά στο 58% [1]. Σημειωτέον ότι η τάση αυτή της μετακίνησης του πληθυσμού από τις αγροτικές περιοχές προς τα μεγάλα αστικά κέντρα είχε ξεκινήσει πολύ πριν το 1950, από τον 18ο αιώνα, με την έναρξη της πρώτης βιομηχανικής επανάστασης, σε μία προσπάθεια εύρεσης καλύτερων συνθηκών ζωής και εργασίας. Το φαινόμενο αυτό της αστικοποίησης έδωσε μία νέα δυναμική στις πόλεις, καθιστώντας τες το επίκεντρο της οικονομικής και πολιτικής δραστηριότητας. Μολονότι η ανάπτυξη των πόλεων είχε πολλά σημαντικά οφέλη για την οικονομία και την καινοτομία, ερωτήματα άρχισαν να δημιουργούνται αναφορικά με την βιώσιμη διαβίωση των κατοίκων της. Ορισμένα από τα ζητήματα που ανέκυψαν αφορούσαν τομείς όπως οι δημόσιες συγκοινωνίες, η υγεία και το περιβάλλον. Στην προσπάθεια, λοιπόν, των πόλεων επίλυσης των διαφόρων ζητημάτων και διατήρησης παράλληλα της ανταγωνιστικότητας της, οι πόλεις στράφηκαν στην τεχνολογία.

Με τη χρήση τεχνολογιών της πληροφορικής και των επικοινωνιών οι υπηρεσίες μιας πόλης μετατρέπονται σε έξυπνες, μετατρέποντας με αυτό τον τρόπο και την ίδια την πόλη σε «έξυπνη πόλη», καθιστώντας βιώσιμη την περαιτέρω ανάπτυξή της. Κεντρικό ρόλο στην εξέλιξη των πόλεων διαδραματίζει η συλλογή των δεδομένων τόσο του περιβάλλοντος όσο και των πολιτών, τα οποία επεξεργάζονται και παρέχουν χρήσιμες πληροφορίες για τους φορείς της έξυπνης πόλης. Οι τεχνολογίες του Διαδικτύου των Πραγμάτων συμβάλλουν σημαντικά στην ως άνω συλλογή, καθώς και στην ελεύθερη διακίνηση των δεδομένων, καθιστώντας την έξυπνη πόλη διαρκώς συνδεδεμένη και ενήμερη. Μολονότι οι πληροφορίες που παρέχουν τα δεδομένα είναι καίριες για την ανάπτυξη και βελτιστοποίηση των παρεχόμενων υπηρεσιών της έξυπνης πόλης, ανακύπτουν ζητήματα σχετικά με το κατά πόσο υφίστανται κίνδυνοι ως προς την ασφάλεια και την ιδιωτικότητα των προσωπικών δεδομένων και κατά πόσο αυτοί μπορούν να εξαλειφθούν ή τουλάχιστον μετριαστούν.

Στην παρούσα μελέτη επιχειρείται η επισκόπηση των ανωτέρω ζητημάτων. Αρχικά, στο δεύτερο κεφάλαιο γίνεται μια παρουσίαση του μοντέλου της έξυπνης πόλης και ακολουθούν στο τρίτο κεφάλαιο ορισμένα παραδείγματα έξυπνων πόλεων τόσο του εξωτερικού όσο και της Ελλάδας. Εν συνεχεία, στο τέταρτο κεφάλαιο, αναδεικνύεται η σημασία και η συμβολή του Διαδικτύου των Πραγμάτων στη λειτουργία της έξυπνης πόλης και ακολουθούν στο πέμπτο και έκτο κεφάλαιο, αντιστοίχως, τα ζητήματα ασφάλειας και ιδιωτικότητας των δεδομένων των πολιτών που ανακύπτουν από την συλλογή και χρήση τους στο πλαίσιο της έξυπνης πόλης. Τέλος, στο έβδομο κεφάλαιο επιχειρείται μια σύντομη παρουσίαση του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων (ΓΚΠΔ) και εξετάζονται οι τρόποι με τους οποίους θα καταστεί εφικτή η συμμόρφωση των έξυπνων πόλεων με αυτόν με σκοπό την προστασία των προσωπικών δεδομένων των κατοίκων της.

2. Η ΕΞΥΠΝΗ ΠΟΛΗ

2.1. Έννοια και χαρακτηριστικά της έξυπνης πόλης

Η έννοια της «έξυπνης πόλης» έκανε την πρώτη της εμφάνιση κατά τις τελευταίες δεκαετίες του 20ου αιώνα. Δεν υπάρχει, ωστόσο, ένας ορισμός που να περιγράφει την «έξυπνη πόλη» αλλά στο διάστημα αυτό έχουν δοθεί πολλοί διαφορετικοί ορισμοί, οι οποίοι έχουν διαμορφωθεί και εξελιχθεί μαζί με την τεχνολογία και την εδραίωση αυτής στην κοινωνία. Ένας εκ των πρώτων ορισμών που αποσυνδέθηκε από τον καθαρά τεχνολογικό χαρακτήρα της έξυπνης πόλης ήταν ο ακόλουθος «*Πιστεύουμε ότι μια πόλη είναι έξυπνη όταν οι επενδύσεις σε ανθρώπινο και κοινωνικό κεφάλαιο, καθώς και οι παραδοσιακές μεταφορές και σύγχρονες υποδομές επικοινωνίας παρακινούν τη βιώσιμη οικονομική ανάπτυξη και μια υψηλή ποιότητα ζωής, με μια συνεχή διαχείριση των φυσικών πόρων, μέσω της συμμετοχικής διακυβέρνησης.*» [2]. Δίνοντας αυτό τον ορισμό, ο συγγραφέας ήθελε να τονίσει ότι μια έξυπνη πόλη περιλαμβάνει πολλές διαφορετικές πτυχές και διαστάσεις. Στο ίδιο πνεύμα κυμαίνεται και ο ορισμός που δόθηκε από το European Smart Cities Project σύμφωνα με το οποίο η έξυπνη πόλη ορίζεται ως η πόλη «*με καλές επιδόσεις σε 6 χαρακτηριστικά, που βασίζεται σε έναν «έξυπνο» συνδυασμό από δραστηριότητες ανεξάρτητων και ενημερωμένων πολιτών*» αναφερόμενο στην έξυπνη οικονομία, την έξυπνη κινητικότητα, το έξυπνο περιβάλλον, τους έξυπνους ανθρώπους, την έξυπνη διαβίωση και τέλος την έξυπνη διακυβέρνηση [3]. Αυτά τα ως άνω χαρακτηριστικά ή άλλως πυλώνες της έξυπνης πόλης, απαρτίζονται από επιμέρους δείκτες που μας βοηθάνε να μετρήσουμε το επίπεδο και το βαθμό ανάπτυξης μιας έξυπνης πόλης.

Ειδικότερα, οι πυλώνες της έξυπνης πόλης, οι οποίοι πρέπει να υπάρχουν και να εφαρμόζονται σε αυτήν προς επίτευξη της επιτυχημένης και ομαλούς λειτουργίας της και τα στοιχεία που τους απαρτίζουν είναι οι κάτωθι:

- Η «**έξυπνη οικονομία**», η οποία προσδιορίζεται από τον βαθμό της καινοτομίας και των επιχειρηματικών πρωτοβουλιών, τα εμπορικά

σήματα και τις δυνατότητες διείσδυσης και ένταξης στη διεθνή αγορά και οικονομία.

- Οι «**έξυπνοι άνθρωποι/πολίτες**», οι οποίοι προσδιορίζονται όχι από τα προσόντα τους ή το επίπεδο εκπαίδευσής τους αλλά από τις δυνατότητες που τους προσφέρει η ίδια η πόλη για ανάπτυξη της δημιουργικότητάς τους, ευκαιρίες σύγχρονης εκπαίδευσης, πλήρης προσβασιμότητας στις πληροφορίες και εκπαίδευση στις νέες τεχνολογίες, μια κοινωνία χωρίς αποκλεισμούς και άνιση μεταχείριση, δίνοντας τη δυνατότητα σε όλους τους πολίτες να συμμετέχουν στη λήψη αποφάσεων.

- Η «**έξυπνη διακυβέρνηση**», η οποία προσδιορίζεται από τη λειτουργία της διοίκησης και τη δημιουργία μέσων συμπερίληψης των πολιτών στο δημόσιο βίο με την συμμετοχή τους στη λήψη αποφάσεων επί θεμάτων και πολιτικών που τους αφορούν και επηρεάζουν την καθημερινότητά τους. Σημαντικό προσδιοριστικό στοιχείο της έξυπνης διακυβέρνησης είναι, επίσης, η ύπαρξη διαφάνειας, προσβασιμότητας στα δεδομένα και λογοδοσίας της δημόσιας διοίκησης.

- Το «**έξυπνο περιβάλλον**», το οποίο προσδιορίζεται από τη δημιουργία χώρων πρασίνου, την ορθολογική διαχείριση των φυσικών πόρων και τη χρήση ανανεώσιμων πηγών ενέργειας, τις προσπάθειες περιορισμού των εκπομπών ρύπων, τη διαχείριση των αποβλήτων και την εν γένει προστασία του περιβάλλοντος.

- Ο «**έξυπνος τρόπος ζωής / έξυπνη διαβίωση**», ο οποίος περιλαμβάνει διάφορους τομείς της ζωής των πολιτών, όπως η συμμετοχή σε πολιτιστικά δρώμενα, η τέχνη, η υγεία, η διασφάλιση της ασφάλειας, η επίλυση βασικών βιοτικών ζητημάτων όπως η στέγαση, ο τουρισμός, καθώς και άλλα ζητήματα που επηρεάζουν την ποιότητα διαβίωσης σε ένα αστικό περιβάλλον.

- Η «**έξυπνη κινητικότητα**», η οποία προσδιορίζεται από τις δυνατότητες μετακίνησης που δίνονται στους πολίτες μέσω καλά οργανωμένων συστημάτων μεταφοράς, που περιλαμβάνουν ηλεκτρικό, μετρό, λεωφορεία, αυτοκίνητα, ποδηλάτες, πεζούς, προωθώντας τις φιλικές προς το περιβάλλον και μη μηχανοκίνητες επιλογές. Ακόμη, την ενσωμάτωση τεχνολογιών πληροφορικής και επικοινωνιών στα Μέσα Μαζικής Μεταφοράς (Μ.Μ.Μ.), τον περιορισμό των ιδιωτικών οχημάτων στους δρόμους, τη διευκόλυνση της στάθμευσης μέσω αισθητήρων στους δρόμους και ειδικών εφαρμογών και τέλος, τη δημιουργία έξυπνων λύσεων για την επίλυση του κυκλοφοριακού προβλήματος που αντιμετωπίζουν τα αστικά κέντρα.

Εκ των ανωτέρω, καθίσταται κατανοητό ότι η ένταξη και χρήση Τεχνολογιών της Πληροφορικής και των Επικοινωνιών (ΤΠΕ) μέσα σε μια πόλη δεν θα την μετατρέψει αυτομάτως σε «έξυπνη», αλλά κλειδί στην επίτευξη του ως άνω σκοπού είναι να βρεθούν στο επίκεντρο της προσοχής οι ίδιοι οι πολίτες. Η ανάπτυξη ενός έξυπνου ανθρωπίνου κεφαλαίου μέσω της χρήσης ΤΠΕ, οι οποίες

καλούνται να αμβλύνουν προβλήματα που αντιμετωπίζουν οι κάτοικοι της πόλης σε σχέση με την εκπαίδευση, τον πολιτισμό, την κοινωνική ένταξη, τη μετακίνηση και λοιπά προβλήματα της διαβίωσης στην πόλη, θα βοηθήσει στην συμμετοχή των πολιτών στο δημόσιο βίο και στην εξεύρεση λύσεων για την επίλυση των ως άνω ζητημάτων από κοινού οι φορείς της έξυπνης πόλης και οι πολίτες της [5].

2.2. Η αρχιτεκτονική και οι τρόποι λειτουργίας της έξυπνης πόλης

Οι έξυπνες πόλεις ανά τον κόσμο διαφέρουν μεταξύ τους, ήδη από το επίπεδο σχεδιασμού τους, καθώς διαφέρουν οι ανάγκες, ο βαθμός ανάπτυξης, ο πολιτισμός και άλλα στοιχεία που έχουν σχέση με τους ανθρώπους που κατοικούν σε αυτές, οι οποίοι είναι και αυτοί που θα απολαύσουν τους καρπούς τους. Μολονότι, λοιπόν, φαίνεται ότι δεν υπάρχει μια καθολική αρχιτεκτονική για την ανάπτυξη μιας έξυπνης πόλης, θα μπορούσε να λεχθεί ότι υπάρχει μια βασική αρχιτεκτονική που εφαρμόζεται σε όλες τις έξυπνες ή εν δυνάμει έξυπνες πόλεις, η οποία συνδέεται στενά με τα εμπλεκόμενα μέρη της.

Ειδικότερα, κατά το σχεδιασμό και τη λειτουργία μιας έξυπνης πόλης είναι σημαντικό να συνδυάζονται αρμονικά κάποια επιμέρους στοιχεία της έξυπνης πόλης, όπως η κοινωνική υποδομή, η υλική υποδομή και τα συστήματα της πόλης, η υποδομή τεχνολογιών πληροφορικής και επικοινωνιών και η επιχειρηματική υποδομή [6]. Περαιτέρω, διακρίνουμε τις κάτωθι πτυχές της έξυπνης πόλης [7]:

- **Στόχοι, άνθρωποι και οικοσύστημα**

Κάθε έξυπνη πόλη βασίζεται σε ένα σύνολο στόχων που τίθενται προ της εκκίνησης υλοποίησης του σχεδίου της. Καθώς η έξυπνη πόλη δεν είναι παρά οι έξυπνοι άνθρωποι που ζουν σε αυτή, οι στόχοι που τίθενται πρέπει να είναι ανθρωποκεντρικοί και να αφορούν τη βελτιστοποίηση των λειτουργιών και των εφαρμογών της, προκειμένου να βελτιωθεί η ποιότητα ζωής των κατοίκων της. Κύριοι στόχοι, λοιπόν, της έξυπνης πόλης είναι η βιωσιμότητα, η κοινωνική ένταξη, η εξάλειψη των διακρίσεων, καθώς και η κοινωνική και οικονομική ανάπτυξη.

Λόγω του ανθρωποκεντρικού χαρακτήρα των στόχων και εν συνεπεία εφαρμογών της έξυπνης πόλης, κρίσιμη είναι η συμβολή των ίδιων των πολιτών στον προσδιορισμό των επιθυμητών στόχων και στον σχεδιασμό της στρατηγικής επίτευξής τους. Οι αισθητήρες, τα μεγάλα δεδομένα και το Διαδίκτυο των Πραγμάτων είναι εργαλεία για τη δημιουργία της έξυπνης πόλης, τα οποία θα πρέπει να χρησιμοποιούνται με γνώμονα τους τελικούς χρήστες και τις ανάγκες τους, οι οποίοι δεν είναι άλλοι από τους κατοίκους, τους εργαζομένους και τους επισκέπτες της έξυπνης πόλης [8].

- **Soft υποδομές**

Προκειμένου οι πολίτες να μπορούν να συμμετάσχουν και να επικοινωνήσουν τις ανάγκες τους στους υπεύθυνους σχεδιασμού και υλοποίησης της έξυπνης πόλης είναι απαραίτητο να δημιουργηθούν κάποιες soft (μαλακές) υποδομές. Στον όρο «soft υποδομές» περιλαμβάνονται οι μηχανισμοί εκείνοι που ρυθμίζουν τη ροή της πληροφορίας και την συνεργασία μεταξύ των μερών, όπως η δημιουργία συζήτησης και διαλόγου περί της υιοθέτησης μιας εφαρμογής. Άλλες soft υποδομές είναι πιο επίσημες όπως διαδικασίες μέτρησης της προόδου ανάπτυξης των επιμέρους έξυπνων συστημάτων της έξυπνης πόλης σε συνάρτηση με τους στόχους που έχουν τεθεί, καθώς και ο σχεδιασμός προτύπων διασύνδεσης των συστημάτων προκειμένου να επιτευχθεί η βιώσιμη ανάπτυξη και αρμονική λειτουργία της.

- **Συστήματα της έξυπνης πόλης**

Τα υπάρχοντα συστήματα μιας πόλης αποτελούν σημαντικό κομμάτι της έξυπνης πόλης και δεν πρέπει να παραβλέπονται καθώς ορισμένες φορές μπορεί να δημιουργήσουν περιορισμούς στην ανάπτυξη της. Εν προκειμένω, συστήματα που αφορούν τις βασικές υποδομές της, όπως το νερό, η ενέργεια, η υγεία, οι μεταφορές και η ενημέρωση, πολλές φορές μπορεί να είναι δύσκολο να συντηρηθούν ή να αναπτυχθούν περαιτέρω λόγω του κόστους και της ξεπερασμένης τεχνολογίας τους. Είναι, λοιπόν, σημαντικό τέτοιου είδους υποδομές να λαμβάνονται υπόψιν κατά τον σχεδιασμό της έξυπνης πόλης προκειμένου η υλοποίηση της και οι εφαρμογές αυτής να καταστούν βιώσιμες.

- **Hard Υποδομές**

Με τον όρο «hard (σκληρές) υποδομές» εννοούνται όλες εκείνες οι υποδομές από τις οποίες ξεκίνησε το όλο εγχείρημα της έξυπνης πόλης. Τέτοιου είδους υποδομές είναι τα συστήματα πληροφορικής και επικοινωνιών, τα δίκτυα 4G, 5G και 6G, τα μέσα κοινωνικής δικτύωσης, το υπολογιστικό νέφος και οι υποδομές σε αυτό, οι εφαρμογές λογισμικού που θα χρησιμοποιηθούν στα διάφορα συστήματα της έξυπνης πόλης κ.α. Αξίζει να αναφέρουμε ειδικά την σημασία ανάπτυξης δικτύων 5G και 6G, τα οποία θα αντικαταστήσουν σταδιακά τα δίκτυα 4G, παρέχοντας δυνατότητες ταχύτερης λήψης και αποστολής δεδομένων, εξασφαλίζοντας την άμεση και ανά πάσα στιγμή και τόπο συνδεσιμότητα στο δίκτυο της έξυπνης πόλης, οδηγώντας με αυτό τον τρόπο στη βελτίωση των υπηρεσιών της έξυπνης πόλης και κατ' επέκτασιν της ζωής των κατοίκων της [9]. Βασικό κριτήριο για τον σχεδιασμό όλων αυτών των σκληρών υποδομών θα πρέπει να είναι η εξυπηρέτηση των πολιτών και η διευκόλυνση της διαβίωσής τους μέσα στην έξυπνη πόλη, καθώς απώτερος στόχος τους πρέπει να είναι ακριβώς η εξυπηρέτηση του συνόλου της πόλης.

2.3. Εμπλεκόμενα Μέρη

Με την ολοένα αυξανόμενη μετατροπή των πόλεων σε «έξυπνων», κρίσιμο είναι να εξετάσουμε ποια μέρη εμπλέκονται σε αυτή τη διαδικασία, ποιων προσώπων τα δεδομένα συλλέγονται, ποιοι τα διαχειρίζονται και ποιος ο ρόλος του καθενός μέσα στην έξυπνη πόλη. Καθίσταται κατανοητό ότι τα εμπλεκόμενα μέρη στην ανάπτυξη μιας έξυπνης πόλης ποικίλλουν, τα σημαντικότερα εκ των οποίων αναλύονται κάτωθι [10].

2.3.1. Οι πολίτες

Όπως έχει αναφερθεί και ανωτέρω, ένας από τους κύριους λόγους ανάπτυξης μιας έξυπνης πόλης είναι η βελτίωση της ζωής των προσώπων που κατοικούν σε αυτήν. Συνεπώς, βασικό και αναπόσπαστο στοιχείο της έξυπνης πόλης δεν θα μπορούσε να είναι άλλο από τους ίδιους τους πολίτες της. Όντας στο επίκεντρο της δημιουργίας της έξυπνης πόλης, οι πολίτες αναλαμβάνουν ενεργό συμμετοχικό ρόλο στο δημόσιο βίο με την παροχή τόσο των απόψεών τους όσο και των δεδομένων τους. Ένα απλό παράδειγμα είναι η δυνατότητα του πολίτη να ενημερώσει π.χ. μέσω μιας εφαρμογής την αρμόδια δημοτική υπηρεσία για την ύπαρξη μιας λακκούβας στο οδόστρωμα, η οποία χρήζει επισκευής ή ενός επικίνδυνου δέντρου, τα κλαδιά του οποίου χρειάζονται κλάδεμα προκειμένου να αποφευχθεί ένα πιθανό ατύχημα. Ομοίως, η δυνατότητα των πολιτών μέσω ειδικά σχεδιασμένων εφαρμογών να συμμετέχουν ενεργά προτείνοντας ή/και αντιπροτείνοντας σε θέματα πολιτικής και εφαρμογών που αφορούν την πόλη τους και την καθημερινότητα τους. Τέλος, ένα ακόμη παράδειγμα είναι αυτό της έξυπνης στάθμευσης στην οποία ο πολίτης παρέχει τα δεδομένα της τοποθεσίας του μέσω μιας εφαρμογής και η εφαρμογή του εμφανίζει τις διαθέσιμες θέσεις στάθμευσης στην περιοχή.

2.3.2. Η κυβέρνηση και η δημόσια διοίκηση

Κινητήριος δύναμη της ανάπτυξης και υιοθέτησης πολιτικών και εφαρμογών που θα βοηθήσουν στην μετατροπή μιας πόλης σε «έξυπνη» είναι σε πρώτο βαθμό η κυβέρνηση και σε δεύτερο βαθμό η δημόσια διοίκηση. Οι κυβερνήσεις οφείλουν να λαμβάνουν τα αναγκαία μέτρα ώστε να καθίσταται δυνατή η μετατροπή των πόλεων σε «έξυπνες πόλεις» και η βελτίωση της καθημερινότητας των πολιτών, τόσο μέσω επιδοτήσεων ανάπτυξης έξυπνων λύσεων όσο και μέσω ένταξης σε διάφορα προγράμματα της Ευρωπαϊκής Ένωσης σχετικά με τις έξυπνες πόλεις.

Σε δεύτερο βαθμό, η δημόσια διοίκηση είναι αυτή που θα κληθεί να εφαρμόσει και να κάνει προσιτές στους πολίτες τις νέες τεχνολογικές λύσεις και τις νέες πολιτικές για την υλοποίηση του σχεδίου της έξυπνης πόλης. Οι δημοτικοί φορείς είναι αυτοί που θα επεξεργάζονται τα δεδομένα και τα αιτήματα των πολιτών και θα θέτουν σε εφαρμογή τις έξυπνες λύσεις. Πρώτος, ωστόσο, είναι ο δημόσιος τομέας αυτός που θα πρέπει να αφομοιώσει και να εξοικειωθεί με τις αλλαγές και τις νέες έξυπνες λύσεις, προκειμένου ολόκληρο το οικοσύστημα της έξυπνης πόλης να λειτουργήσει επιτυχώς και οι πολίτες να αισθάνονται ασφάλεια μέσα σε αυτό το νέο πλαίσιο.

2.3.3. Οι εταιρείες πληροφορικής και επικοινωνιών

Από την στιγμή όπου οι στόχοι έχουν τεθεί και οι αποφάσεις έχουν παρθεί από τα αρμόδια όργανα για την έναρξη της υλοποίησης του σχεδίου της έξυπνης πόλης, στο επίκεντρο έρχονται οι εταιρίες πληροφορικής και επικοινωνιών, οι οποίες είναι οι πλέον αρμόδιες να αναπτύξουν και να παρέχουν τις κατάλληλες τεχνολογικές λύσεις ανάλογα με τις ανάγκες τις εκάστοτε υπό διαμόρφωση έξυπνης πόλης. Δεδομένου του πλήθους των τομέων που καλύπτει η λειτουργία μιας έξυπνης πόλης γίνεται κατανοητό ότι η ανάγκη για παροχή τεχνολογικών λύσεων - ποικίλλου και ευρέως περιεχομένου - είναι επιτακτική. Η επιτυχία της μετάβασης μιας πόλης στη ψηφιακή εποχή και δη στην «έξυπνη» εποχή θα εξαρτηθεί από την ποιότητα και την καινοτομία των τεχνολογικών λύσεων που θα δοθούν από τις εν λόγω εταιρείες πληροφορικής και επικοινωνιών.

Κατόπιν των ανωτέρω, αξίζει να αναφερθούμε στο γεγονός ότι στο περιβάλλον της έξυπνης πόλης παρατηρούμε ότι εφαρμόζονται δύο αντίθετες δυνάμεις που έχουν σχέση με τα ως άνω εμπλεκόμενα μέρη και τα συμφέροντα αυτών. Από την μια πλευρά παρατηρούμε τη λεγόμενη «ώθηση της τεχνολογίας», η οποία συνεπάγεται ότι μια νέα υπηρεσία / προϊόν εισάγεται στην αγορά της έξυπνης πόλης, ως αποτέλεσμα της ανακάλυψης νέων τεχνολογικών λύσεων λόγω της διαρκώς αυξανόμενης τεχνολογικής ανάπτυξης, που οδηγείται από την προσφορά - ανεξάρτητα από τις εκφρασμένες ανάγκες της κοινωνίας - και από την άλλη πλευρά η λεγόμενη «έλξη της αγοράς», η οποία αναφέρεται σε μια υπηρεσία / προϊόν που αναπτύσσεται και διατίθεται στην αγορά της έξυπνης πόλης ως απάντηση σε μια αναγνωρισμένη ζήτηση από την πλευρά της κοινωνίας και των χρηστών των υπηρεσιών της έξυπνης πόλης. Προκειμένου να καταστεί επιτυχές το εγχείρημα της έξυπνης πόλης πρέπει να διασφαλιστεί η επικοινωνία και συνεργασία μεταξύ όλων των εμπλεκόμενων μερών, τοποθετώντας στην άκρη τα επιμέρους συμφέροντα του καθενός από αυτά προς επίτευξη ενός κοινού στόχου, ήτοι την υλοποίηση της έξυπνης πόλης. Απόρροια, δε, της ως άνω αμφίδρομης επικοινωνίας θα είναι η εξισορρόπηση των δύο ως άνω αναφερόμενων δυνάμεων που εφαρμόζονται στο οικοσύστημα της έξυπνης πόλης. Καταλήγοντας, όλα τα πρόσωπα, τα οποία εμπλέκονται στην υλοποίηση του εγχειρήματος της έξυπνης πόλης, είναι εξίσου σημαντικά και απαραίτητα για την επίτευξη της ανάπτυξής της και την πραγμάτωση των στόχων της και γι' αυτό το λόγο θα πρέπει να βρεθούν τρόποι αρμονικής συνύπαρξης όλων αυτών [11].

3. ΠΑΡΑΔΕΙΓΜΑΤΑ ΕΞΥΠΝΩΝ ΠΟΛΕΩΝ

Κατόπιν εξέτασης των ανωτέρω στοιχείων των έξυπνων πόλεων σε συνδυασμό με το βαθμό επίτευξης και ένταξης αυτών, μπορούμε να κατατάξουμε τις έξυπνες πόλεις σε τρεις κατηγορίες. Ειδικότερα, μπορεί να γίνει η διάκριση σε α) πρωτοπόρες έξυπνες πόλεις, οι οποίες αποτελούν και πρότυπα – έξυπνες πόλεις και έχουν καταφέρει να αναπτύξουν και υιοθετήσουν την όλη υποδομή μιας έξυπνης πόλης, β) αναδυόμενες έξυπνες πόλεις, οι οποίες έχουν κάνει τα πρώτα

βήματα, υιοθετώντας έξυπνες λύσεις και είναι στα όρια της καινοτομίας και τέλος γ) έξυπνες πόλεις της επόμενης φάσης, οι οποίες μελλοντικά και με ιδιαίτερη προσπάθεια ενδέχεται να βρεθούν στα πρόθυρα της καινοτομίας [10].

3.1. Βαρκελώνη, Ισπανία

Η Βαρκελώνη είναι η πόλη – πρότυπο όσον αφορά τις «έξυπνες πόλεις». Αξίζει να αναφερθεί ότι το 2014 ανακηρύχθηκε από την Ευρωπαϊκή Ένωση ως η πρωτεύουσα της καινοτομίας («iCapital») [12], καθώς επίσης έχει ανακηρυχθεί ως «Mobile World Capital» για μια δεκαετία, η οποία ολοκληρώνεται φέτος, ήτοι το έτος 2023 [13]. Δεν έχουν δοθεί άδικα αυτοί οι χαρακτηρισμοί στη Βαρκελώνη, η οποία κατάφερε να βελτιώσει την ποιότητα της ζωής των πολιτών της, υιοθέτησε τεχνολογικές λύσεις που εξασφαλίζουν την προστασία του περιβάλλοντος και προώθησε την επιχειρηματικότητα και την καινοτομία στο ευρύτερο οικονομικό περιβάλλον, αναβαθμίζοντας τις παρεχόμενες υπηρεσίες της.

Στο επίκεντρο της στρατηγικής σχεδιασμού της «έξυπνης πόλης της Βαρκελώνης» ήταν η σύνδεση των πολιτών με την ίδια την πόλη μέσω εγκαθίδρυσης διαδικασιών ανοιχτών δεδομένων, οι οποίες θα οδηγούσαν στην ανταλλαγή πολύτιμων πληροφοριών τόσο για τους πολίτες όσο και για τις εταιρείες που δραστηριοποιούνται μέσα στην έξυπνη πόλη. Ορισμένα παραδείγματα τέτοιων εφαρμογών στην έξυπνη πόλη της Βαρκελώνης είναι τα κάτωθι [14]:

- "**Smart Citizen**" : Στο πλαίσιο της έξυπνης διακυβέρνησης, έχει διαμορφωθεί μια πλατφόρμα ανοικτών δεδομένων ονομαζόμενη "Smart Citizen" μέσω της οποίας οι πολίτες της Βαρκελώνης έχουν τη δυνατότητα να «χτίσουν» μαζί με τις δημόσιες αρχές την έξυπνη πόλη συμμετέχοντας ενεργά. Σκοπός αυτής της πλατφόρμας είναι η ενθάρρυνση των πολιτών στην συλλογή δεδομένων σχετικών με το περιβάλλον τους και ύστερα κοινοποίησης τους μέσω της πλατφόρμας, φέρνοντας με αυτό τον τρόπο κοντά ανθρώπους, δεδομένα και γνώσεις που θα χρησιμεύσουν στην ανάπτυξη των έξυπνων εργαλείων και υπηρεσιών της πόλης [15].
- "**Social Innovation for Communities**": Μέσω του έργου με την ονομασία «Social Innovation for Communities», έχοντας ως στόχο την κοινωνική καινοτομία, το Δημοτικό Συμβούλιο της Βαρκελώνης κατάφερε να εμπλέξει οργανισμούς, επιχειρηματίες και επενδυτές στη δημιουργία και εφαρμογή διεθνώς επιτυχημένων έξυπνων λύσεων στην πόλη της Βαρκελώνης, οι οποίες σταδιακά ενσωματώθηκαν στην καθημερινότητα των πολιτών.

Επίσης, άξιες αναφοράς είναι οι κάτωθι τεχνολογικές λύσεις που εφάρμοσε η Βαρκελώνη και που της χάρισαν τον τίτλο της «έξυπνης πόλης – πρότυπο» [16]:

- **Έξυπνος φωτισμός**: Αντικαθιστώντας τους λαμπτήρες στους δημόσιους χώρους με λαμπτήρες τύπου «LED» και εγκαθιστώντας έξυπνους αισθητήρες, οι οποίοι καταγράφουν τις καιρικές συνθήκες, το θόρυβο, τη ρύπανση και ανιχνεύουν την κίνηση, επιτεύχθηκε η εξοικονόμηση της ηλεκτρικής ενέργειας ενώ

παράλληλα με τα δεδομένα που παράγονται έγινε δυνατός ο εντοπισμός της υψηλής κυκλοφοριακής κίνησης αλλά και η βελτίωση της ασφάλειας στους δημόσιους χώρους.

- **Έξυπνη στάθμευση**: Εγκαθιστώντας έξυπνους αισθητήρες σε χώρους στάθμευσης, οι οποίοι ανιχνεύουν την ύπαρξη φωτός και μετάλλου είναι δυνατή η έγκυρη και σε πραγματικό χρόνο ενημέρωση των πολιτών σχετικά με τις διαθέσιμες θέσεις στάθμευσης.

- **Έξυπνες συγκοινωνίες**: Στο πλαίσιο αναδιάρθρωσης του δικτύου των Μέσων Μαζικής Μεταφοράς της Βαρκελώνης δημιουργήθηκαν οι λεγόμενες «έξυπνες στάσεις» ή άλλως «Smart Bus Stops», στις οποίες έχουν εγκατασταθεί οθόνες αφής, οι οποίες τροφοδοτούνται με ηλιακή ενέργεια και παρέχουν πληροφορίες στους πολίτες τόσο σχετικά με τους αναμενόμενους χρόνους άφιξης των λεωφορείων όσο και πληροφορίες τουριστικού ενδιαφέροντος για την πόλη.

- **Έξυπνο σύστημα διαχείρισης απορριμμάτων** : Κατασκευάζοντας υπογείως ένα δίκτυο μεταφοράς των απορριμμάτων και εγκαθιστώντας ειδικούς αισθητήρες σε αυτό είναι δυνατή, κατόπιν εξέτασης των συλλεγόμενων πληροφοριών σχετικά με την πληρότητα του χώρου, η ενημέρωση των απορριμματοφόρων οχημάτων για την περισυλλογή των απορριμμάτων, εξοικονομώντας με αυτό τον τρόπο ενέργεια.

3.2. Άμστερνταμ, Ολλανδία

Το Άμστερνταμ βραβεύτηκε το 2016 από την Ευρωπαϊκή Επιτροπή ως «Ευρωπαϊκή Πρωτεύουσα Καινοτομίας» («iCapital») [17]. Ειδικότερα, το Άμστερνταμ ήδη από το 2009 με τη δημιουργία της πλατφόρμας «Amsterdam Smart City» έκανε τα πρώτα βήματα και έθεσε τους στόχους για τον εκσυγχρονισμό της πόλης. Μέσα από την πλατφόρμα αυτή έχει τεθεί σε εφαρμογή μια πληθώρα καινοτόμων προγραμμάτων με επίκεντρο τους πολίτες και την συμμετοχή τους σε αυτά. Μερικά εκ των ανωτέρω αναφερόμενων προγραμμάτων είναι τα εξής:

- **Έξυπνος φωτισμός**: Εγκαθιστώντας έξυπνους αισθητήρες που εξετάζουν τον καιρό, δίνεται η δυνατότητα εξ' αποστάσεως χειρισμού αλλά και αυτόματης ενεργοποίησης του φωτισμού σε δημοτικούς χώρους. Σημαντική εφαρμογή του έξυπνου φωτισμού είναι αυτή στο λιμάνι της πόλης («Atlas Park») όπου οι πολίτες κατά τη διέλευσή τους από την περιοχή είτε περπατώντας είτε τρέχοντας είτε διερχόμενοι από τον ποδηλατόδρομο, μπορούν να ρυθμίζουν την ένταση του φωτισμού, η οποία χαμηλώνει μετά τη διέλευσή τους βοηθώντας στην εξοικονόμηση ενέργειας. Λεκτέον δε ότι ο φωτισμός της πόλης αποτελείται από λαμπτήρες τύπου «LED», οι οποίοι τροφοδοτούνται από ηλιακούς συλλέκτες ενέργειας (panels) και ανεμογεννήτριες [18].

- **Έξυπνες μετακινήσεις**: Πολλά είναι τα προγράμματα που έχουν αναπτυχθεί αναφορικά με την έξυπνη κινητικότητα ορισμένα εκ των οποίων είναι το σύστημα «Car2Go», το οποίο αφορά τη μεταφορά προϊόντων και εμπορευμάτων στην πόλη μέσω μικρών ηλεκτροκίνητων οχημάτων [19] και το πρόγραμμα «Digital Road Authority» δυνάμει της οποίας είναι δυνατή η ενημέρωση των οδηγών για τις κυκλοφοριακές συνθήκες και την κίνηση στους δρόμους μέσω εφαρμογής στο κινητό τηλέφωνο και δίνεται η δυνατότητα στην ψηφιακή οδική αρχή να ρυθμίζει τα φανάρια κυκλοφορίας όταν υφίσταται αυξημένη κίνηση.
- **Έξυπνη διακυβέρνηση**: Όπως ειπώθηκε και ανωτέρω, το Άμστερνταμ έχει ως στόχο τη δημιουργία μιας έξυπνης πόλης με επίκεντρο τους πολίτες του. Σε αυτό το πλαίσιο, παρέχει στους πολίτες τη δυνατότητα ελέγχου και παρακολούθησης του κρατικού προϋπολογισμού, ενώ παράλληλα τους δίνει τη δυνατότητα να συναποφασίζουν με τη διοίκηση για την οικονομική και επιχειρηματική ανάπτυξη της πόλης.

3.3 Σόνγκντο, Νότια Κορέα

Μία από τις αναδυόμενες έξυπνες πόλεις, είναι η πόλη Σόνγκντο στη Νότια Κορέα. Πρόκειται για μία πόλη που δημιουργήθηκε από το μηδέν με σκοπό να γίνει μια πόλη του μέλλοντος, μια πόλη πρότυπο εισάγοντας την καινοτομία και την τεχνολογία σε κάθε πτυχή της πόλης. Με αυτούς τους στόχους δημιουργήθηκε μια πλήρως συνδεδεμένη πόλη όπου σχεδόν κάθε δρόμος, σπίτι και συσκευή φέρει αισθητήρες, οι οποίοι ανταλλάσσουν δεδομένα. Ειδικότερα [20] :

- **Έξυπνη κινητικότητα**: Στους δρόμους έχουν εγκατασταθεί αισθητήρες οι οποίοι μετράνε τη χρήση της ενέργειας και τη ροή της κυκλοφορίας, ενώ στα αυτοκίνητα έχουν, επίσης, εγκατασταθεί αισθητήρες κίνησης, οι οποίοι στέλνουν τις συντεταγμένες στην κεντρική μονάδα προκειμένου να ανιχνεύονται τα σημεία όπου υπάρχει κυκλοφοριακή συμφόρηση.
- **Έξυπνη διαβίωση**: Σε όλα τα σπίτια έχουν εγκατασταθεί αισθητήρες οι οποίοι δίνουν τη δυνατότητα στους πολίτες να χειρίζονται μέσω μιας πλατφόρμας στην κεντρική τους τηλεόραση τη θέρμανση, τον φωτισμό και λοιπές λειτουργίες του σπιτιού, μετατρέποντάς το σε ένα έξυπνο σπίτι. Επίσης, έχει δημιουργηθεί ένα παραθαλάσσιο πάρκο με αυτοσυντηρούμενα συστήματα άρδευσης προκειμένου να παρέχει άπλετο δημόσιο χώρο στους πολίτες.
- **Έξυπνο περιβάλλον**: Έχουν τοποθετεί μικροτσίπ στους κάδους απορριμμάτων με αποτέλεσμα όταν οι πολίτες πετούν τα απορρίμματά τους να δημιουργούνται δεδομένα, τα οποία συλλέγονται και βοηθούν στην καλύτερη διαχείριση των απορριμμάτων. Επίσης, σε επίπεδο μεμονωμένων κατοικιών, οι σωλήνες απορριμμάτων μεταφέρουν τα σκουπίδια σε ένα κεντρικό εργοστάσιο όπου διαχωρίζονται αυτόματα σε ανακυκλώσιμα και απόβλητα προς καύση.

3.4. Ελλάδα

Παραδείγματα έξυπνων πόλεων παρουσιάζει και η Ελλάδα, η οποία εξελίσσεται και αναπτύσσεται στον τομέα αυτό με την υιοθέτηση έξυπνων εφαρμογών και λοιπών στοιχείων των έξυπνων πόλεων, απολαμβάνοντας μάλιστα διεθνείς διακρίσεις. Ειδικότερα, σημειώνουμε ότι έχουν επιλεχθεί από την Ευρωπαϊκή Επιτροπή έξι ελληνικές πόλεις και ειδικότερα η Αθήνα, τα Ιωάννινα, η Καλαμάτα, η Κοζάνη, η Θεσσαλονίκη και τα Τρίκαλα προκειμένου να συμμετάσχουν στο πρόγραμμα της Ευρωπαϊκής Ένωσης για κλιματικά ουδέτερες και έξυπνες πόλεις μέχρι το έτος 2030 [21] [22]. Ενδεικτικά αναφέρουμε δύο εκ των ανωτέρω πόλεων:

- **Τρίκαλα**

Ο δήμος Τρικκαίων ήταν ο πρώτος στην Ελλάδα που άρχισε να υιοθετεί πρακτικές και εφαρμογές φιλικές προς τους πολίτες, το 2004 δε η πόλη των Τρικάλων ψηφίστηκε ως η «πρώτη ψηφιακή πόλη» της Ελλάδας. Ειδικότερα αναφέρουμε κάποιες από τις εφαρμογές που την ανέδειξαν ως «έξυπνη πόλη» [23]:

- **Έξυπνη διακυβέρνηση**: Στο πλαίσιο της έξυπνης διακυβέρνησης και της συμμετοχής των πολιτών στο δημόσιο βίο έχουν δημιουργηθεί διάφορες πλατφόρμες όπως η «e-dialogos», η οποία δίνει τη δυνατότητα στους δημότες και στους εργαζόμενους του δήμου να συμμετέχουν ενεργά στον σχεδιασμό των δράσεων στην πόλη τους, καθώς και το πρόγραμμα «ΔΗΜΟΣΘeΝΗΣ», στο οποίο οι πολίτες μπορούν να υποβάλλουν τα παράπονά τους. Εξειδικευμένο προσωπικό είναι διαθέσιμο για να συνομιλήσει με τους πολίτες και να δοθεί λύση στα προβλήματα που ανακύπτουν.
- **Έξυπνη μετακίνηση**: Πολλές ενέργειες έχουν λάβει χώρα στον τομέα αυτό μερικές εκ των οποίων, η πληροφόρηση σε πραγματικό χρόνο (real-time) της άφιξης των αστικών λεωφορείων με ειδικά τοποθετημένες ταμπέλες στις στάσεις, η δημιουργία εφαρμογής για διαμοιρασμό αυτοκινήτων (carsharing) και συνεπιβατισμό (carpooling) για μετάβαση σε κοντινές περιοχές, όπως και η εγκατάσταση συστήματος έξυπνης διάβασης πεζών, το οποίο προειδοποιεί τους οδηγούς όταν πλησιάζουν σε πεζοδιάβαση.

- **Ιωάννινα**

Σε έξυπνη πόλη μετατρέπονται και τα Ιωάννινα, τα οποία έχουν θέσει ως στόχο τη βελτίωση της μετακίνησης των πολιτών και των επισκεπτών της πόλης με τις κάτωθι τεχνολογικές λύσεις:

- **Έξυπνη μετακίνηση**: Στο πλαίσιο αυτό τα Ιωάννινα θα προμηθευτούν με αισθητήρες κίνησης, οι οποίοι θα τοποθετηθούν υπογείως σε 100 σημεία

στάθμευσης της πόλης και θα ενημερώνουν τους πολίτες και τους διερχομένους για τις διαθέσιμες θέσεις παροδικής στάθμευσης προκειμένου να εξυπηρετήσουν τις ανάγκες τους. Σημειωτέον δε ότι το σύστημα αυτό θα εξυπηρετεί και τα άτομα με ειδικές ανάγκες με την παροχή πληροφόρησης σε αυτά των διαθέσιμων ειδικών θέσεων [24].

- **Έξυπνη διακυβέρνηση**: Επίσης, έχει αναπτυχθεί στα Ιωάννινα ηλεκτρονική πλατφόρμα διαβούλευσης μέσω της οποίας οι πολίτες μπορούν να συμμετέχουν και να εκφράζουν τη γνώμη τους σχετικά με την υλοποίηση έργων στην πόλη τους (όπως π.χ. η εγκατάσταση του ανωτέρω συστήματος έξυπνης στάθμευσης) αλλά και να αντιπροτείνουν ή αντιτεθούν σε προτεινόμενα έργα και πολιτικές [25].

4. ΕΞΥΠΝΕΣ ΠΟΛΕΙΣ ΚΑΙ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ (ΔτΠ)

Το 2008 τα διασυνδεδεμένα στο διαδίκτυο «πράγματα» ξεπέρασαν σε αριθμό τους ανθρώπους, καθιστώντας εμφανή την εξάπλωση και την σημασία που θα αποκτούσαν μελλοντικά στη ζωή όλου του κόσμου. Σήμερα δε, πολλοί χαρακτηρίζουν το Διαδίκτυο των Πράγματων ως μία από τις τεχνολογίες που απαρτίζουν την 4η Βιομηχανική Επανάσταση (ή «Industry 4.0» ή «I 4.0» ή «4IR» ή «I.4») [26]. Το Διαδίκτυο των Πραγμάτων (Internet of Things ή IoT) αποτελεί βασικό στοιχείο και εργαλείο των έξυπνων πόλεων, δίνοντας τη δυνατότητα συλλογής δεδομένων και διασύνδεσης συσκευών σε πραγματικό χρόνο. Με αυτό τον τρόπο συμβάλλει στην βελτιστοποίηση και αυτοματοποίηση των υποδομών και των συστημάτων λειτουργίας μιας πόλης επιλύοντας ζητήματα όπως η αυξημένη κυκλοφορία, η διαχείριση των πόρων και η ασφάλεια των πολιτών, μειώνοντας ταυτόχρονα τις δημόσιες δαπάνες. Σε τί ακριβώς, όμως, συνίσταται και ποιες οι πιθανές εφαρμογές του στο περιβάλλον μιας έξυπνης πόλης;

4.1. Έννοια και χαρακτηριστικά του Διαδικτύου των Πραγμάτων

Το 1999 ένας Βρετανός πρωτοπόρος της τεχνολογίας, ο Kevin Ashton, εφηύρε τον όρο του Διαδικτύου των Πραγμάτων. Με αυτό τον όρο ήθελε να περιγράψει ένα σύστημα όπου ο φυσικός κόσμος και το διαδίκτυο μπορούν να συνδεθούν μέσω αισθητήρων χωρίς την ανάγκη παρέμβασης του ανθρώπου. Ένα σύστημα, δηλαδή, όπου συσκευές και αντικείμενα της καθημερινότητας μπορούν να συνδεθούν και να επικοινωνήσουν με τους υπολογιστές και το διαδίκτυο [27]. Σήμερα ο όρος αυτός χρησιμοποιείται ευρέως για να περιγράψουμε ένα δίκτυο επικοινωνίας μεταξύ έξυπνων συσκευών ή αντικειμένων, τα οποία έχουν ενσωματωμένη τεχνολογία που τους επιτρέπει μέσω αισθητήρων και ειδικού λογισμικού να λαμβάνουν πληροφορίες από το περιβάλλον τους και να μεταφέρουν αυτές τις πληροφορίες σε ένα δίκτυο (ή στο διαδίκτυο), έχοντας τη δυνατότητα να επικοινωνήσουν μεταξύ τους, χωρίς να είναι απαραίτητη η ανθρώπινη συνδρομή. Τέτοια παραδείγματα συσκευών που ανήκουν στο διαδίκτυο των πραγμάτων μπορεί να είναι οι αισθητήρες του αυτοκινήτου που μας

ειδοποιούν για την ύπαρξη κάποιου αντικειμένου κατά τη διάρκεια του παρκαρίσματος, το έξυπνο ρολόι που μετράει τους παλμούς και πόσα βήματα έχουμε κάνει, σε επίπεδο δε έξυπνης πόλης οι αισθητήρες που μπορεί να έχουν τοποθετηθεί για την μέτρηση της κίνησης στους δρόμους.

Σύμφωνα με έναν άλλο νεότερο ορισμό που δόθηκε το 2016 από τους Patel και Patel το Διαδίκτυο των Πραγμάτων είναι μια έννοια και ένα πρότυπο που έχει μια διάχυτη παρουσία στο περιβάλλον διαφόρων πραγμάτων / αντικειμένων, τα οποία μέσω ασύρματων και ενσύρματων συνδέσεων και μοναδικών συστημάτων δρομολόγησης έχουν τη δυνατότητα να επικοινωνούν μεταξύ τους και να συνεργάζονται με άλλα πράγματα/ αντικείμενα προκειμένου να δημιουργήσουν νέες εφαρμογές / υπηρεσίες και να πετύχουν κοινούς στόχους. Εκ των ανωτέρω ορισμών προκύπτει ότι κύρια χαρακτηριστικά του Διαδικτύου των Πραγμάτων είναι τα κάτωθι [28]:

- **Συνδεσιμότητα και διασυνδεσιμότητα**: Οι συσκευές έχουν τη δυνατότητα σύνδεσης τόσο μεταξύ τους όσο και με το διαδίκτυο δημιουργώντας με αυτό τον τρόπο ένα παγκόσμιο δίκτυο όπου καθίσταται δυνατή η διάχυση και ανταλλαγή της πληροφορίας. Η δυνατότητα της συνδεσιμότητας των συσκευών του Διαδικτύου των Πραγμάτων με την υποδομή του ΔτΠ πρέπει να είναι εφικτή κάθε στιγμή, σε οποιοδήποτε σημείο του κόσμου και από οποιοδήποτε πρόσωπο.

– **Υπηρεσίες που σχετίζονται με πράγματα**: Το Διαδίκτυο των Πραγμάτων είναι σε θέση να παρέχει υπηρεσίες που σχετίζονται με πράγματα υπό τους περιορισμούς των ιδίων των πραγμάτων όπως η προστασία της ιδιωτικής ζωής. Το Διαδίκτυο των Πραγμάτων εστιάζει στην επίτευξη ταυτότητας μεταξύ των πραγμάτων του φυσικού κόσμου και των πραγμάτων του εικονικού κόσμου.

– **Ετερογένεια**: Η αρχιτεκτονική του Διαδικτύου των Πραγμάτων εκ φύσεως δεν μπορεί να είναι ομοιογενής, αντιθέτως χαρακτηρίζεται από ετερογένεια. Τα πράγματα που αποτελούν το ΔτΠ είναι διαφορετικά κατασκευασμένα, ετερογενή μεταξύ τους και βασίζονται σε διαφορετικές υποδομές και δίκτυα. Βασικό χαρακτηριστικό, λοιπόν, του ΔτΠ είναι αυτές οι ετερογενείς συσκευές να μπορούν να συνδεθούν, να επικοινωνήσουν μεταξύ τους και να ανταλλάξουν δεδομένα.

– **Δυναμικές αλλαγές**: Οι συσκευές και τα αντικείμενα του Διαδικτύου των Πραγμάτων χαρακτηρίζονται από μια δυναμικότητα και προσαρμοστικότητα στις διάφορες συνθήκες. Η δυναμικότητα αυτή γίνεται εμφανής τόσο στην κατάσταση των συσκευών π.χ. ενεργοποιημένη/απενεργοποιημένη όσο και στο περιβάλλον στο οποίο βρίσκονται, π.χ. καταγραφή δεδομένων το πρωί / την νύχτα.

– **Μεγάλη κλίμακα συσκευών**: Ο αριθμός των διαφόρων συσκευών που συνδέονται καθημερινά στο διαδίκτυο αυξάνεται συνεχώς. Αυτό σημαίνει ότι ο αριθμός των συσκευών που επικοινωνούν μεταξύ τους στο Διαδίκτυο των Πραγμάτων θα είναι στο άμεσο μέλλον μεγαλύτερος από τον αριθμό των συσκευών που είναι συνδεδεμένες στο διαδίκτυο τώρα και ως αποτέλεσμα η αυξανόμενη πληροφορία που θα παράγεται θα πρέπει να μπορεί να χειρίζεται κατάλληλα.

– **Ασφάλεια**: Δεδομένου ότι οι συσκευές του Διαδικτύου των Πραγμάτων έχουν ως βασικό έργο την συλλογή και επεξεργασία δεδομένων, καθίσταται κρίσιμο να επιτευχθεί ένα σημαντικό επίπεδο ασφαλείας των δεδομένων αυτών. Η προστασία των προσωπικών δεδομένων και η ασφάλεια της ιδιωτικής ζωής θα πρέπει να είναι το κύριο μέλλημα των δημιουργών των συσκευών του ΔτΠ, ενώ δεν πρέπει να παραβλέπεται και η προστασία των δικτύων, μέσω των οποίων γίνεται η ανταλλαγή, επεξεργασία και αποθήκευση των δεδομένων.

4.2. Έξυπνες συσκευές – μοντέλα διασύνδεσης

Το 2015 εκδόθηκε από το Συμβούλιο Αρχιτεκτονικής του Διαδικτύου ((Internet Architecture Board «IAB») ένας κατευθυντήριος οδηγός σχετικά με τον τρόπο διασύνδεσης των έξυπνων συσκευών και το γενικότερο πλαίσιο αρχιτεκτονικής των μοντέλων επικοινωνίας που εφαρμόζονται σε αυτές [29]. Σημειώνεται ότι οι έξυπνες συσκευές χρησιμοποιούν προκαθορισμένα πρωτόκολλα επικοινωνίας προκειμένου να επικοινωνήσουν και συνδεθούν μεταξύ τους. Ανάμεσα στα κυριότερα χαρακτηριστικά του κάθε μοντέλου διασύνδεσης ανήκουν τα κάτωθι [30]:

α) Μοντέλο Διασύνδεσης Συσκευή με Συσκευή (Device-to-Device)

Το μοντέλο διασύνδεσης Συσκευή με Συσκευή (Device-to-Device) είναι ένα από τα πιο συνηθισμένα μοντέλα στη χρήση και έγκειται στην άμεση διασύνδεση και επικοινωνία μεταξύ δύο η περισσοτέρων συσκευών, χωρίς να είναι αναγκαία η παρεμβολή ενός ενδιάμεσου διακομιστή εφαρμογών. Οι διασυνδεόμενες συσκευές μπορούν να επικοινωνήσουν μεταξύ τους μέσω πολλών ειδών δικτύων, συμπεριλαμβανομένης της διεύθυνσης διαδικτυακού πρωτοκόλλου και το διαδίκτυο, συνήθως, όμως, για την μεταξύ τους επικοινωνία χρησιμοποιούν πρωτόκολλα επικοινωνίας όπως το Bluetooth[1], το Z-Wave[2] και το ZigBee[3].

β) Μοντέλο Διασύνδεσης Συσκευή με Νέφος (Device-to-Cloud)

Στο μοντέλο διασύνδεσης Συσκευή με Νέφος (Device-to-Cloud), η έξυπνη συσκευή συνδέεται απευθείας με μια διαδικτυακή υπηρεσία νέφους, όπως μια υπηρεσία

[1] Το Bluetooth είναι από τις πιο γνωστές μεθόδους ασύρματης επικοινωνίας, η οποία χρησιμοποιείται για την σύνδεση συσκευών χωρίς τη χρήση καλωδίων και την ανταλλαγή δεδομένων σε μικρές αποστάσεις.

[2] Το Z-Wave είναι ένα ασύρματο δίκτυο, το οποίο έχει σχεδιαστεί κυρίως για οικιακή χρήση και χρησιμοποιείται για την παροχή επικοινωνίας μεταξύ συσκευών σε ένα δίκτυο ελέγχου. Κύριο χαρακτηριστικό του Z-Wave είναι η δυνατότητα ενοποίησης πολλών συσκευών σε ένα ενιαίο δίκτυο.

[3] Το ZigBee είναι ένα πρωτόκολλο ασύρματης μετάδοσης δεδομένων που χρησιμοποιείται για αμφίδρομη επικοινωνία μεταξύ συσκευών και έχει αναπτυχθεί κυρίως για οικιακό δίκτυο. Τα κύρια χαρακτηριστικά του είναι η χαμηλή κατανάλωση ενέργειας και η απλή κατασκευή του, η οποία συνεπάγεται χαμηλό κόστος.

παροχής εφαρμογών, η οποία της επιτρέπει να ανταλλάσσει δεδομένα και ελέγχει την διαδρομή των μηνυμάτων. Το μοντέλο αυτό διασύνδεσης συνήθως εκμεταλλεύεται τους υπάρχοντες μηχανισμούς επικοινωνίας, όπως είναι το Ethernet[4] και το Wi-fi[5]. Το ανώτερο μοντέλο χρησιμοποιείται από αρκετούς δημοφιλείς καταναλωτές συσκευών διαδικτύου των πραγμάτων όπως η Samsung Smart TV, καθώς προσδίδει προσθετή αξία στην αρχική συσκευή επεκτείνοντας τις δυνατότητες της.

γ) Μοντέλο Διασύνδεσης Συσκευής με Πύλη (Device-to-Gateway)

Σε αυτό το μοντέλο διασύνδεσης, δεν έχουμε απευθείας σύνδεση μεταξύ της συσκευής με τη διαδικτυακή υπηρεσία νέφους αλλά για τον σκοπό αυτό (της σύνδεσης) χρησιμοποιείται μία ενδιάμεση συσκευή που εκτελεί αυτή τη λειτουργία. Αυτό το μοντέλο επικοινωνίας προσδίδει περισσότερη ασφάλεια και πρόσθετες λειτουργικότητες, όπως η μετάφραση δεδομένων ή πρωτοκόλλων. Το μοντέλο αυτό διασύνδεσης χρησιμοποιείται συνήθως σε καταναλωτικά είδη, όπως οι συσκευές μέτρησης φυσικής κατάστασης (fitness trackers), οι οποίες δεν δύνανται μόνες τους να έχουν απευθείας πρόσβαση στην υπηρεσία του νέφους και γι' αυτό χρειάζονται τη χρήση του λογισμικού εφαρμογών του έξυπνου τηλεφώνου, με το οποίο συνδέονται, προκειμένου να το χρησιμοποιήσουν ως ενδιάμεσο και να αποστείλουν τα δεδομένα στη διαδικτυακή υπηρεσία του νέφους.

δ) Μοντέλο Διασύνδεσης του Επιπέδου Πρόσβασης και Διαμοιρασμού Δεδομένων (Back-End Data Sharing)

Αυτό το μοντέλο διασύνδεσης συσκευών παρέχει τη δυνατότητα στους χρήστες να εξάγουν και να αναλύουν δεδομένα έξυπνων συσκευών και αντικειμένων διαδικτύου των πραγμάτων από μια διαδικτυακή υπηρεσία νέφους με άλλα δεδομένα τα οποία έχουν συλλέξει από άλλες πηγές. Το μοντέλο Back-End Data Sharing διευκολύνει τις ανάγκες φορητότητας των δεδομένων, ειδικότερα όταν ο χρήστης επιθυμεί να τα μεταφέρει μεταξύ υπηρεσιών του Διαδικτύου των Πράγματων που υπό άλλες συνθήκες (π.χ υπό τη μορφή του μοντέλου Device to Cloud) θα εφαρμόζονταν περιορισμοί και θα αδυνατούσε.

4.3. Εφαρμογές του Διαδικτύου των Πραγμάτων στις έξυπνες πόλεις

[4] Το Ethernet είναι μια μέθοδος ενσύρματης σύνδεσης συσκευών σε τοπικό δίκτυο ή σε δίκτυο ευρείας παροχής. Καθώς πρόκειται για ενσύρματο τύπο σύνδεσης, απαιτεί τη χρήση ενός καλωδίου Ethernet για την σύνδεση των συσκευών στο διαδίκτυο.

[5] Το Wi-Fi είναι μια μέθοδος ασύρματης επικοινωνίας, το οποίο επιτρέπει τη σύνδεση συσκευών σε ένα τοπικό δίκτυο και την ανταλλαγή δεδομένων ή σύνδεση στο διαδίκτυο μέσω της χρήσης ραδιοκυμάτων.

Όπως γίνεται αντιληπτό, το Διαδίκτυο των Πραγμάτων διαδραματίζει ουσιώδη ρόλο στην αναβάθμιση μιας πόλης σε «έξυπνη». Καθώς η τεχνολογία εξελίσσεται και οι ανάγκες των δυνητικών χρηστών πληθαίνουν, οι εφαρμογές του Διαδικτύου των Πραγμάτων καταλαμβάνουν όλο και μεγαλύτερο ρόλο στη λειτουργία μιας έξυπνης πόλης από τις μεταφορές και τη δημιουργία έξυπνων δικτύων κοινής ωφέλειας μέχρι την υγεία και τη διαχείριση των αποβλήτων. Παρέχοντας τη δυνατότητα εξ αποστάσεως παρακολούθησης διάφορων συνδεδεμένων συσκευών και ανάλυσης των δεδομένων και πληροφοριών που αυτές συλλέγουν, επιτυγχάνεται η ανάληψη των κατάλληλων ενεργειών προκειμένου να βελτιωθούν οι υποδομές της έξυπνης πόλης και να παρασχεθούν καλύτερες υπηρεσίες για τους πολίτες της. Εξετάζοντας, περαιτέρω, τις εφαρμογές του ΔτΠ σε μια έξυπνη πόλη μπορούν να διακρίνουμε τις κάτωθι.

4.3.1. Έξυπνη μεταφορά / κινητικότητα

Ένα από τα καίρια ζητήματα που καλείται να αντιμετωπίσει μια πόλη και οι πολίτες της είναι αυτό της μεταφοράς. Λαμβάνοντας υπόψιν την βαθμό ανάπτυξης των μεγαλουπόλεων λόγω της έντονης τάσης για αστικοποίηση που επικρατεί παγκοσμίως, η λύση του ζητήματος της μεταφοράς είναι ζωτικής σημασίας προκειμένου να καταστεί μια πόλη λειτουργική. Λύση σε αυτό το ζήτημα έρχονται να δώσουν διάφορες εφαρμογές του Διαδικτύου των Πραγμάτων καλύπτοντας πτυχές τόσο της δημόσιας όσο και της ιδιωτικής μεταφοράς.

- **Έξυπνη στάθμευση**

Το ζήτημα της στάθμευσης είναι ένα από τα μεγαλύτερα προβλήματα που αντιμετωπίζουν οι πολίτες των μεγαλουπόλεων και το οποίο διαρκώς θα χειροτερεύει με την αύξηση του πληθυσμού εάν δεν βρεθεί ένας τρόπος να αντιμετωπιστεί Την λύση στο πρόβλημα αυτό ή τουλάχιστον στην άμβλυνση του προβλήματος, έρχεται να δώσει το Διαδίκτυο των Πραγμάτων με την εγκατάσταση αισθητήρων σε όλους τους χώρους στάθμευσης της έξυπνης πόλης. Ο σκοπός είναι οι αισθητήρες να συλλέγουν τα δεδομένα, ήτοι τις πληροφορίες σχετικά με τη διαθεσιμότητα ή μη των εκάστοτε θέσεων στάθμευσης, οι οποίες θα συγκεντρώνονται σε μια πλατφόρμα, στην οποία θα μπορούν να έχουν πρόσβαση οι πολίτες και να εντοπίζουν τους διαθέσιμες θέσεις στάθμευσης κοντά τους [31].

- **Έξυπνο σύστημα δημόσιας συγκοινωνίας**

Όσον αφορά την μετατροπή των δημόσιων συγκοινωνιών σε «έξυπνων», με σκοπό τη διευκόλυνση της χρήσης τους από τους πολίτες, καθιστώντας παράλληλα αυτές τις υπηρεσίες ελκυστικές, υπάρχουν αρκετές δυνατότητες που προσφέρει το Διαδίκτυο των Πραγμάτων. Τέτοιου είδους εφαρμογές είναι η εγκατάσταση αισθητήρων στα μέσα μαζικής μεταφοράς με σκοπό την ενημέρωση των πολιτών μέσω ειδικά σχεδιασμένων εφαρμογών για όλες τις διαδρομές, τα μέσα τα οποία μπορούν να χρησιμοποιηθούν και τον ακριβή χρόνο άφιξης των μέσων σε έκαστη στάση. Επίσης, η ως άνω ενημέρωση για τον χρόνο άφιξης μπορεί να γίνεται μέσω της δημιουργίας ειδικών εγκαταστάσεων όπως π.χ. οθονών, οι οποίες θα ενημερώνονται συνεχώς και θα προσφέρουν ακριβή πληροφόρηση στους πολίτες.

Τέλος, στο πλαίσιο εκσυγχρονισμού των μέσων μαζικής μεταφοράς θα μπορούσαν να εξοπλιστούν οι δημόσιες συγκοινωνίες με τεχνολογίες ασύρματου δικτύου (Wi-Fi) και βελτίωση της ισχύος του σήματος στα υπογείως μετακινούμενα μέσα μαζικής μεταφοράς [32].

- **Αυτόνομη οδήγηση**

Η ανάπτυξη τεχνολογιών αυτόνομης οδήγησης είναι ένας ακόμη «έξυπνος» τρόπος μεταφοράς σε μια έξυπνη πόλη, ο οποίος θα οδηγήσει σε σημαντική εξοικονόμηση χρόνου για τον επιβάτη. Προκειμένου ένα τέτοιο σύστημα αυτόνομης οδήγησης να πετύχει, ειδικοί αισθητήρες, ραντάρ και φωτογραφικές μηχανές θα πρέπει να εγκατασταθούν στο αυτοκίνητο, προκειμένου εν συνεχεία το έξυπνο λογισμικό που θα είναι εγκατεστημένο σε αυτό να μπορεί αυτόνομα να επεξεργάζεται τις συλλεχθείσες πληροφορίες για να πλοηγεί με ασφάλεια (το αυτοκίνητο), καθώς σε περίπτωση κινδύνου θα υπάρχει η δυνατότητα αυτόνομης άμεσης ενεργοποίησης των φρένων για την πρόληψη τυχόν ατυχήματος. Μέσω του συστήματος αυτόνομης οδήγησης θα μπορούσε να επιλέγεται η κάθε φορά ταχύτερη και καλύτερη διαδρομή, η οποία θα ενημερώνεται διαρκώς κατά την μετακίνηση, ενώ επίσης ο επιβάτης θα δύναται να απωλέσει την ανάγκη αναζήτησης χώρου στάθμευσης, καθώς και το παρκάρισμα [33].

4.3.2. Έξυπνες υποδομές / κτίρια

Μέσω της εγκατάστασης αισθητήρων στα κτίρια της έξυπνης πόλης είναι δυνατή η αποτελεσματικότερη διαχείριση κάθε ενός από αυτά και η βελτίωση της ζωής των ενοίκων τους. Οι εφαρμογές του Διαδικτύου των Πραγμάτων μπορούν να βοηθήσουν σε πολλά διαχειριστικά θέματα μίας υποδομής από την διανομή της ηλεκτρικής ενέργειας, του νερού και της θέρμανσης μέχρι την καθαριότητα και την επίτευξη ενός σημαντικού βαθμού ασφάλειας. Μπορεί να γίνει, δε, ευκολότερη και απλούστερη η διαχείριση του κτιρίου και όποιων θεμάτων προκύπτουν, καθώς όλες οι σχετικές πληροφορίες συλλέγονται, αναλύονται και μέσω των έξυπνων εφαρμογών, μπορούν να ενημερώνουν κάθε φορά τους διαχειριστές ή/ και τους ενοικιαστές για όποιο ζήτημα προκύπτει [34].

4.3.3. Έξυπνη υγεία

Ο τομέας της υγείας μπορεί να βοηθηθεί σε μεγάλο βαθμό από τη χρήση εφαρμογών του Διαδικτύου των Πραγμάτων. Μέσω της εγκατάστασης ειδικών αισθητήρων μπορεί να γίνει δυνατή τόσο η εξ αποστάσεως παρακολούθηση ασθενών με την συλλογή και ανάλυση των φυσιολογικών δεδομένων τους από μια έξυπνη εφαρμογή για την υγεία, η οποία θα αποστέλλει τα αποτελέσματα στον θεράποντα ιατρό ή στους νοσηλευτές, όσο και η διάγνωση ασθενών που βρίσκονται σε απομακρυσμένες περιοχές ή έχουν αδυναμία μετάβασης σε κάποιο

νοσοκομείο ή ιατρείο. Μολονότι η παροχή ενός υψηλού επιπέδου υγείας είναι από τα μείζοντα ζητήματα σε μια πόλη, θα πρέπει να λαμβάνεται παράλληλα υπόψιν η διασφάλιση ενός αντίστοιχα υψηλού επιπέδου ασφάλειας, κατά την μεταχείριση τέτοιου είδους δεδομένων, καθώς τα ιατρικά δεδομένα δεν αποτελούν απλά προσωπικά δεδομένα αλλά ανήκουν στην ειδική κατηγορία των ευαίσθητων προσωπικών δεδομένων και χρήζουν μεγαλύτερης προστασίας [35].

4.3.4. Έξυπνη διαχείριση αποβλήτων

Η διαχείριση των αποβλήτων μιας πόλης έχει καταστεί ένα δύσκολο έργο, το οποίο αναμένεται να καταστεί ακόμη δυσκολότερο τα επόμενα έτη λόγω της συγκέντρωσης μεγάλου αριθμού ανθρώπων στα αστικά κέντρα. Ο τρόπος διαχείρισης, δε, των αποβλήτων είναι σημαντικός για την περιβαλλοντική βιωσιμότητα. Ένας τρόπος με τον οποίο οι εφαρμογές του Διαδικτύου των Πραγμάτων θα μπορούσαν να βοηθήσουν στην έξυπνη διαχείριση των αποβλήτων μίας πόλης είναι μέσω της εγκατάστασης ειδικών αισθητήρων μέσα στους κάδους απορριμμάτων. Αποτελέσματα σχετικά με την πληρότητα ή μη του κάδου μπορούν, εν συνεχεία, να αποστέλλονται στην σχετική υπηρεσία του δήμου, η οποία θα οργανώνει ανάλογα το δρομολόγιο του απορριμματοφόρου και θα επιτυγχάνει με αυτό τον τρόπο την αποτελεσματικότερη και γρηγορότερη συλλογή των απορριμμάτων [33].

4.3.5. Προστασία του περιβάλλοντος

Η προστασία του περιβάλλοντας αποτελεί ένα κύριο μέλημα της έξυπνης πόλης, καθώς αποτελεί και έναν από τους βασικούς πυλώνες της, ως αναφέρθηκε και ανωτέρω. Οι εφαρμογές του Διαδικτύου των Πραγμάτων παρέχουν τη δυνατότητα μέτρησης διαφόρων στοιχείων του περιβάλλοντος μέσω της εγκατάστασης ειδικών αισθητήρων. Ειδικότερα, με τους αισθητήρες αυτούς είναι δυνατή η μέτρηση της συγκέντρωσης του διοξειδίου του άνθρακα (CO_2) και διαφόρων αερίων στην ατμόσφαιρα της πόλης, καθώς και ο έλεγχος της θερμοκρασίας (π.χ. με ειδοποίηση σε περίπτωση αυξημένης θερμότητας, η οποία μπορεί να υποδηλώνει την εκδήλωση πυρκαγιάς), της συγκέντρωσης της υγρασίας στην ατμόσφαιρα και του επιπέδου του νερού για τις αποχετεύσεις και τα όμβρια ύδατα κλπ. Ύστερα, όλες αυτές οι πληροφορίες αναλύονται και βοηθάνε στην εφαρμογή των κατάλληλων μέτρων / λύσεων ή στην έγκαιρη επέμβαση, όπου χρειάζεται, προκειμένου να επιτευχθεί η προστασία του περιβάλλοντος της έξυπνης πόλης [33].

5. ΖΗΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΣΤΙΣ ΕΞΥΠΝΕΣ ΠΟΛΕΙΣ

Βασικό στοιχείο για τη λειτουργία μιας έξυπνης πόλης είναι η χρήση τεχνολογιών της πληροφορικής και επικοινωνιών (ΤΠΕ). Μέσω αυτών, καθώς και εφαρμογών του Διαδικτύου των Πραγμάτων, οι παρεχόμενες υπηρεσίες της έξυπνης πόλης εκσυγχρονίζονται με αποτέλεσμα την παροχή υψηλού επιπέδου υπηρεσιών στους πολίτες της. Με την τοποθέτηση, ωστόσο, των τεχνολογιών αυτών στον πυρήνα της λειτουργίας της έξυπνης πόλης, νέα ζητήματα και προκλήσεις ανακύπτουν τόσο ως προς την ιδιωτικότητα όσο και ως προς την ασφάλεια των δεδομένων. Ειδικότερα, με τη χρήση εφαρμογών των Διαδικτύου των Πραγμάτων, οι οποίες συλλέγουν και επεξεργάζονται τα δεδομένα των πολιτών, αυξάνεται ο κίνδυνος παραβίασης των συλλεχθέντων δεδομένων, ενώ μάλιστα, στην περίπτωση που οι χρησιμοποιούμενες τεχνολογίες δεν έχουν ισχυρά συστήματα ασφαλείας, αυξάνεται ο κίνδυνος υποκλοπής, αλλοίωσης και καταστροφής των δεδομένων. Αυξάνεται, λοιπόν, η δυνατότητα επίθεσης στα συστήματα αυτά και δημιουργούνται αμφιβολίες ως προς το βαθμό που μπορεί να επιτευχθεί η προστασία τους. Τέτοιου είδους επιθέσεις, οι οποίες μπορούν να χαρακτηριστούν ως συμβάντα ασφαλείας, συνήθως έχουν ως σκοπό να προκαλέσουν βλάβη στα λειτουργικά συστήματα της έξυπνης πόλης, να κλονίσουν την εμπιστοσύνη των πολιτών υποκλέπτοντας τα δεδομένα τους και εν γένει να προσβάλουν την ασφάλεια και ιδιωτικότητα της έξυπνης πόλης [36].

5.1. Οι παράγοντες της ασφάλειας των δεδομένων

Η ασφάλεια δεδομένων σχετίζεται με την ικανότητα προστασίας τους και ειδικότερα την ικανότητα διασφάλισης τριών παραγόντων, ήτοι 1) της εμπιστευτικότητας (Confidentiality), 2) της ακεραιότητας (Integrity) και 3) της διαθεσιμότητας (Availability), κοινώς γνωστών από τα αρχικά τους ως «C.I.A. triad». Τα βασικότερα είδη επιθέσεων κατά της ασφάλειας των συστημάτων πληροφορικής και επικοινωνιών σχετίζονται με τους τρεις ως άνω παράγοντες και χαρακτηρίζονται από τις κάτωθι ενέργειες [37]:

- **Μη εξουσιοδοτημένη πρόσβαση σε πληροφορίες (Confidentiality)**. Όταν προσωπικά δεδομένα και πληροφορίες αποκαλύπτονται σε ένα ή και περισσότερα μη εξουσιοδοτημένα πρόσωπα, προσβάλλοντας με αυτό τον τρόπο τον εμπιστευτικό χαρακτήρα των πληροφοριών.
- **Μη εξουσιοδοτημένη τροποποίηση των πληροφοριών (Integrity)**. Όταν ένα μη εξουσιοδοτημένο πρόσωπο αποκτά πρόσβαση σε προσωπικά δεδομένα και πληροφορίες και προβαίνει σε ενέργειες μεταβολής, αλλοίωσης ή ακόμη και διαγραφής των δεδομένων. Σημειώνεται ότι σε αυτή την περίπτωση δεν είναι απαραίτητο ο εισβολέας να βλέπει τις πληροφορίες που έχει τροποποιήσει / προσβάλλει. Η επίθεση κατά της ακεραιότητας των δεδομένων είναι μια μορφή σαμποτάζ.

- **Μη εξουσιοδοτημένη άρνηση χρήσης (Availability)**. Όταν ο εισβολέας καθιστά τις πληροφορίες και τα δεδομένα μη προσπελάσιμα από τις εξουσιοδοτημένες οντότητες, εμποδίζοντάς τες να αποκτήσουν πρόσβαση στις πληροφορίες, να τις τροποποιήσουν, διαγράψουν κλπ. Σε αυτού του είδους τις επιθέσεις συμπεριλαμβάνονται και αυτές που δημιουργούν αδικαιολόγητες καθυστερήσεις στην πρόσβαση των δεδομένων και συνεπώς προβλήματα άρνησης εξυπηρέτησης (Denial of Service, DoS). Σημειώνεται ότι σε αυτή την περίπτωση ο εισβολέας δε χρειάζεται να έχει ο ίδιος πρόσβαση στις πληροφορίες ή δυνατότητα τροποποίησης / αλλοίωσής τους.

Τα ως άνω είδη επιθέσεων μπορούν να δημιουργήσουν πολύ μεγάλα προβλήματα στη λειτουργία της έξυπνης πόλης. Ειδικότερα, μια επίθεση κατά της εμπιστευτικότητας των δεδομένων θα είναι ιδιαίτερα κρίσιμη όταν π.χ. προσβάλλονται ιατρικά δεδομένα ασθενών τα οποία μάλιστα αποτελούν ευαίσθητα προσωπικά δεδομένα. Όταν, λοιπόν, χρησιμοποιούνται έξυπνες λύσεις τηλειατρικής, προκειμένου οι γιατροί να μπορούν να αποκτήσουν πρόσβαση στον ιατρικό φάκελο ασθενών που βρίσκονται σε απομακρυσμένες περιοχές, με σκοπό να παρέχουν την ιατρική τους διάγνωση, θα πρέπει να διασφαλίζεται πρώτον ότι πρόσβαση σε αυτές τις πληροφορίες μπορούν να έχουν μόνο εξουσιοδοτημένα πρόσωπα και δεύτερον ότι το σύστημα θα μπορεί να αναγνωρίζει αν ζητείται πρόσβαση από εξουσιοδοτημένο ή μη πρόσωπο.

Στην περίπτωση δε της επίθεσης κατά της ακεραιότητας των δεδομένων όταν π.χ. σε μια υπηρεσία της έξυπνης πόλης ο πολίτης παρέχει προσωπικά δεδομένα (όπως ο αριθμός του κινητού τηλεφώνου, της τραπεζικής κάρτας, η τοποθεσία κλπ) για να λάβει ακριβώς αυτή την υπηρεσία και τα δεδομένα του υποκλέπτονται και βρίσκονται στη διακριτική ευχέρεια κάποιου τρίτου, ο οποίος μπορεί να τα χρησιμοποιήσει προς δικό του όφελος ή προς βλάβη του υποκειμένου των δεδομένων, δημιουργείται ανασφάλεια και σοβαρές οικονομικές ζημίες στην έξυπνη πόλη.

Τέλος, στην περίπτωση μίας επίθεσης κατά της διαθεσιμότητας των δεδομένων είναι εμφανή τα προβλήματα που ανακύπτουν δεδομένου ότι στις περισσότερες υπηρεσίες της έξυπνης πόλης οι δημοτικές π.χ. υπηρεσίες που παρέχονται, βασίζονται στην αλληλεπίδραση με τους δημότες και στην περίπτωση πρόκλησης προβλημάτων στην εξυπηρέτηση και στο χρόνο αλληλεπίδρασης, δεν είναι δυνατή η παροχή των ίδιων των υπηρεσιών της έξυπνης πόλης όταν αυτές χρειάζονται.

5.2. Τρόποι επίτευξης της ασφάλειας των δεδομένων

Από τα ανωτέρω συνάγεται πόσο μεγάλος είναι ο βαθμός της αναγκαιότητας για προστασία των πληροφοριών και δη των προσωπικών δεδομένων που αποθηκεύονται στα συστήματα μιας έξυπνης πόλης. Η ως άνω προστασία ή έστω ο μετριασμός του κινδύνου από τις ανωτέρω επιθέσεις, μπορεί να επιτευχθεί μέσω

της διασφάλισης των ως βασικών παραγόντων που αναφέρθηκαν ανωτέρω, ήτοι της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων. Προκειμένου να προστατευθούν επαρκώς, ωστόσο, τα συστήματα πληροφορικής και επικοινωνιών μιας έξυπνης πόλης θα πρέπει πρώτα να γίνουν αντιληπτοί οι λόγοι οι οποίοι οδηγούν στην αποδυνάμωσή τους και τα καθιστούν ευπαθή σε κυβερνοεπιθέσεις.

Περαιτέρω, οι κυριότεροι λόγοι αδυναμίας της ασφάλειας των συστημάτων μιας έξυπνης πόλης είναι η ανεπαρκής ασφάλεια λόγω χρήσης είτε μηδαμινών πολιτικών ασφαλείας, εμπιστευόμενοι την προσφερόμενη ασφάλεια από τον πάροχο του έξυπνου συστήματος, είτε λόγω χρήσης ελλιπών τεχνικών ασφαλείας. Επίσης, η χρήση παλαιών σε τεχνολογία συστημάτων και εφαρμογών, τα οποία είτε δεν συντηρούνται επαρκώς/τακτικά είτε λόγω της παλαιότητας τους δεν είναι δυνατόν να αναβαθμιστούν, αποτελεί έναν ακόμη λόγο που καθιστά τα συστήματα μιας έξυπνης πόλης ευάλωτα σε επιθέσεις. Είναι λογικό ότι ένα σύστημα ασφαλείας το οποίο είχε σχεδιαστεί π.χ. πριν είκοσι χρόνια, λαμβάνοντας υπόψιν τα δεδομένα και τις απειλές εκείνης της χρονικής περιόδου, δεν θα μπορεί να ανταπεξέλθει επαρκώς και να προστατεύσει από τις σημερινές, πιο εξελιγμένες και νέες μορφές κυβερνοεπιθέσεων. Τέλος, δεν πρέπει να παραλειφθεί να αναφερθεί και η πιθανότητα του ανθρώπινου λάθους, ηθελημένου ή μη, η οποία μπορεί να οφείλεται πολλές φορές σε ανεπαρκή ή μηδαμινή ενημέρωση και εκπαίδευση του προσωπικού του χειριστή, το οποίο μπορεί να επιφέρει δυσμενείς συνέπειες, όπως η εξάπλωση ενός ιού ή η εγκατάσταση ενός κακόβουλου λογισμικού στο δίκτυο [10].

Προκειμένου να προστατευθούν οι έξυπνες πόλεις από τους άνω κινδύνους θα πρέπει να επενδύσουν σε προληπτικά μέτρα και να ενσωματώσουν στη λειτουργία τους μηχανισμούς και κώδικες ασφαλείας. Τέτοιου είδους μέτρα ασφαλείας θα μπορούσε να είναι [38]:

(α) η χρήση κωδικών και συνθηματικών ασφαλείας για την αυθεντικοποίηση της ταυτότητας των χρηστών πριν την παροχή εισόδου στις εφαρμογές της έξυπνης πόλης,

(β) η εγκατάσταση προγραμμάτων προστασίας (firewalls), των οποίων η ενημέρωση και αναβάθμιση δεν θα πρέπει να αμελείται και

(γ) η χρήση κρυπτογραφικών συστημάτων, προκειμένου να αποφευχθεί η προσπέλαση των δεδομένων από μη εξουσιοδοτημένα πρόσωπα

Όσον αφορά την τρίτη ως άνω μέθοδο, ως κρυπτογράφηση (encryption) ορίζεται η τεχνική με την οποία ο αποστολέας ενός μηνύματος τροποποιεί με τη χρήση ενός αλγορίθμου την αρχική πληροφορία σε ένα νέο κείμενο, το οποίο για να αποκωδικοποιηθεί και αποκρυπτογραφηθεί από τον παραλήπτη είναι απαραίτητη η χρήση ενός ορισμένου κλειδιού κρυπτογράφησης. Με αυτό τον τρόπο η πληροφορία / τα δεδομένα μεταδίδονται με ασφάλεια, καθώς ακόμη και αν τα υποκλέψει κάποιος τρίτος - μη εξουσιοδοτημένος χρήστης- δεν θα μπορεί να λάβει γνώση του περιεχομένου τους γιατί δεν θα έχει στην κατοχή του το κλειδί της κρυπτογράφησης. Από τα ανωτέρω, γίνεται κατανοητό ότι για τη διατήρηση

της ασφάλειας και της μυστικότητας των πληροφοριών δεν είναι τόσο σημαντικός ο αλγόριθμος κρυπτογράφησης που θα χρησιμοποιηθεί, αλλά το μέγεθος και η δυσκολία εύρεσης του κλειδιού που θα χρησιμοποιηθεί. Τα κλειδιά δε προέρχονται από έναν αλγόριθμο και αποτελούνται από μία τυχαία σειρά δυαδικών στοιχείων. Όσο περισσότερα είναι τα στοιχεία του κλειδιού, το μήκος δηλαδή αυτού, τόσο πιο ισχυρή είναι η κρυπτογράφηση [39].

Σε συνδυασμό με τα συστήματα κρυπτογραφίας, τα οποία βοηθάνε στην επίτευξη της ασφαλούς μετάδοσης των δεδομένων, σημαντικό είναι να χρησιμοποιούνται και ορισμένες τεχνικές ιδιωτικότητας, όπως η ψευδωνυμία και η ανωνυμία, προκειμένου να καθίσταται δυνατή η διασφάλιση και της ιδιωτικότητας των μεταδιδόμενων δεδομένων. Λεκτέον δε, ότι μόνο τα ψευδωνυμοποιημένα προσωπικά δεδομένα προστατεύονται από τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ), ενώ τέτοια πρόβλεψη δεν υπάρχει για τα ανωνυμοποιημένα, καθώς θεωρούνται τα πλέον ασφαλή για την οιαδήποτε επεξεργασία.

Ειδικότερα, στο άρθρο 4 στοιχ. 5 του ΓΚΠΔ ορίζεται η ψευδωνυμοποίηση ως «*η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο*» [40]. Εκ του ανωτέρω ορισμού σε συνδυασμό με την αιτιολογική σκέψη 26 του Κανονισμού προκύπτει η ειδοποιός διαφορά μεταξύ των ψευδωνυμοποιημένων και των ανωνυμοποιημένων δεδομένων, η οποία εδράζεται στο αν οι πληροφορίες αυτές μπορούν να οδηγήσουν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο. Στην πρώτη περίπτωση τα προσωπικά δεδομένα παραποιούνται, χρησιμοποιώντας συνήθως πλασματικές ή ψεύτικες πληροφορίες, με σκοπό την συγκάλυψη της πραγματικής ταυτότητας του υποκειμένου των δεδομένων, ενώ στη δεύτερη περίπτωση η ταυτότητα του υποκειμένου δεν μπορεί πλέον να εξακριβωθεί διότι στα ανωνυμοποιημένα δεδομένα τα αναγνωριστικά στοιχεία της ταυτότητας του υποκειμένου διαγράφονται και με αυτό τον τρόπο δεν παρέχεται οποιαδήποτε πληροφορία η όποια μπορεί να συνδέσει άμεσα ή έμμεσα τα δεδομένα με το υποκείμενο [10] [41].

Είναι πολύ σημαντική η εφαρμογή των ως άνω μηχανισμών ασφαλείας, προκειμένου να διασφαλιστεί η προστασία των δεδομένων των πολιτών και να ενισχυθεί η εμπιστοσύνη των τελευταίων προς τους φορείς της έξυπνης πόλης. Εάν, δε, τα ως άνω μέτρα χρησιμοποιηθούν συνδυαστικά, μπορούν να επιτύχουν την ελαχιστοποίηση των συμβάντων ασφαλείας και την επίτευξη της ομαλής λειτουργίας όλων των συστημάτων και υπηρεσιών της έξυπνης πόλης [10].

5.3. Νομοθετικό πλαίσιο για τη διασφάλιση της κυβερνοασφάλειας

Όπως αναφέρθηκε και ανωτέρω όλοι σχεδόν οι τομείς μιας έξυπνης πόλης, όπως

η μεταφορά, η υγεία και η ενέργεια, στηρίζονται σε τεχνολογίες πληροφορικής και επικοινωνιών (ΤΠΕ) προκειμένου να διατελέσουν τις βασικές λειτουργίες τους. Με αυτό τον τρόπο, ωστόσο, οι έξυπνες πόλεις καθίστανται εύκολος στόχος σε κυβερνοαπειλές και κυβερνοεπιθέσεις. Η ως άνω παραδοχή δεν πρέπει να αποτελεί φυσικά ανασταλτικό παράγοντα στην εξέλιξη των πόλεων σε «έξυπνων», καθώς η σημασία της κυβερνοασφάλειας έχει αναδειχθεί ιδιαίτερα τα τελευταία χρόνια, με την Ευρωπαϊκή Ένωση να έχει κάνει προσπάθειες και να έχει θέσει στόχους με σκοπό την ενίσχυση της.

Ειδικότερα, η Ε.Ε. είχε εν αρχή προβεί στην ψήφιση της Οδηγίας 2016/1148 σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση άλλως γνωστή ως «NIS Directive» [42]. Η Οδηγία αυτή στόχευε στην θέσπιση μιας εθνικής στρατηγικής από όλα τα κράτη μέλη για την αντιμετώπιση των απειλών κατά των συστημάτων δικτύου και πληροφοριών και τον μετριασμό των συμβάντων ασφαλείας, προκειμένου να καταστεί δυνατή η ομαλή λειτουργία της εσωτερικής αγοράς και η ανάπτυξη της οικονομίας[6]. Η χώρα μας, δε, εναρμονίστηκε με την Οδηγία και προέβη στην ενσωμάτωσή της με τον Ν. 4577/2018 και την υπ' αρ. 1027/Β/3739/08.10.2019 υπουργική απόφαση.

Εφόσον τέθηκε το βασικό πλαίσιο με την Οδηγία 2016/1148, δυνάμει του οποίου ενισχύθηκε η κυβερνοανθεκτικότητα της Ε.Ε., έξι χρόνια αργότερα, η Ένωση κλήθηκε να επανεξετάσει και να επικαιροποιήσει την Οδηγία δεδομένων των νέων τεχνολογικών εξελίξεων. Στις 14.12.2022, λοιπόν, δημοσιεύθηκε στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης η Οδηγία 2022/2555, άλλως γνωστή ως «NIS 2 Directive», σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του Κανονισμού (ΕΕ) αριθ. 910/2014 και της Οδηγίας (ΕΕ) 2018/1972 και για την κατάργηση της Οδηγίας (ΕΕ) 2016/1148 [43]. Είναι εμφανής η προσπάθεια της Ένωσης για αναβάθμιση του επιπέδου της ασφάλειας και συντονισμού με τις νέες εξελίξεις και τα νέα δεδομένα, δεδομένης της θέσης των δικτύων συστημάτων και πληροφοριών στο επίκεντρο της σύγχρονης κοινωνίας, η οποία ως επακόλουθο έχει οδηγήσει στην ανάπτυξη νέων κυβερνοαπειλών[7].

Ειδικότερα, με την Οδηγία 2022/2555 τίθενται αυστηρότερες υποχρεώσεις για τις επιχειρήσεις, τη δημόσια διοίκηση και τις «βασικές υποδομές». Στους βασικούς δε τομείς υψηλής κρισιμότητας περιλαμβάνονται μεταξύ άλλων στο Παράρτημα Ι της οδηγίας η ενέργεια, οι μεταφορές, οι τράπεζες, η υγεία, τα λύματα και οι ψηφιακές υποδομές. Οι νέοι κανόνες καλούνται να θέσουν τα μέτρα για τη διαχείριση των κινδύνων και την επίτευξη της κυβερνοασφάλειας και να δημιουργήσουν ένα πλαίσιο για αποτελεσματικότερη ανταλλαγή πληροφοριών και συνεργασία μεταξύ των διαφόρων αρχών των κρατών μελών σχετικά με την κυβερνοασφάλεια [44].

[6] Βλ. αρθρ. 1 της Οδηγίας (ΕΕ) 2016/1148

[7] Βλ. αιτιολογική σκέψη υπ' αριθμ. 3 της Οδηγίας (ΕΕ) 2022/2555

Κατόπιν των ανωτέρω, καθίσταται κατανοητό ότι έχουν αναπτυχθεί και συνεχίζουν να αναπτύσσονται διαρκώς, νέες στρατηγικές για την επίτευξη της κυβερνοασφάλειας και την προστασία των συστημάτων δικτύων και πληροφοριών. Οι φορείς δε των έξυπνων πόλεων, προκειμένου να προστατεύσουν τα συστήματά τους και τα δεδομένα των κατοίκων τους, δεν έχουν παρά να υιοθετήσουν και να συμμορφωθούν με τις ως άνω νομοθετικές στρατηγικές.

6. ΖΗΤΗΜΑΤΑ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΤΙΣ ΕΞΥΠΝΕΣ ΠΟΛΕΙΣ

6.1. Το δικαίωμα στην ιδιωτικότητα και το δικαίωμα στην προστασία των προσωπικών δεδομένων

Πολλοί έχουν προσπαθήσει να ορίσουν την ιδιωτικότητα, με πιο διαδεδομένους τους ορισμούς που δόθηκαν από τους Samuel D. Warren και Louis D. Brandeis, κατά τους οποίους ιδιωτικότητα είναι «*το δικαίωμα να μένει κανείς μόνος*» ("*the right to be let alone*") [45] και του ορισμού του Alan Westin, σύμφωνα με τον οποίο τόσο τα φυσικά πρόσωπα όσο και τα νομικά πρόσωπα (ομάδες και ιδρύματα) έχουν το δικαίωμα να προσδιορίζουν οι ίδιοι πότε, με ποιόν τρόπο και σε ποιο βαθμό οι πληροφορίες που αφορούν το πρόσωπό τους θα γνωστοποιηθούν σε κάποιον τρίτο [46].

Ως δικαίωμα, η ιδιωτικότητα εντοπίζεται στο άρθρο 9 του Συντάγματος και στο άρθρο 7 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ε.Ε. (Χ.Θ.Δ.Ε.Ε.). Με το δικαίωμα αυτό παρέχεται στον φορέα του η αμυντική δύναμη να προστατεύει τον ιδιωτικό του χώρο από κάθε εισβολή, παρέμβαση ή ελεγκτική ενέργεια, οι οποίες μπορεί να οδηγήσουν στον περιορισμό των νομοθετικώς κατοχυρωμένων ελευθεριών του να αναπτύσσει ελεύθερα την προσωπικότητα του, να συναναστρέφεται με τους οικείους του και να διαμορφώνει ελεύθερα το βίο και την ταυτότητά του [47]. Ως έννοια επηρεαζόμενη από τα κοινωνικά δρώμενα, η ιδιωτικότητα εξελίχθηκε μαζί με την κοινωνία και την ανάπτυξη της τεχνολογίας, με την τελευταία να συμβάλλει όχι στον επηρεασμό της ουσίας της αλλά στη δημιουργία νέων τρόπων παραβίασής της. Σήμερα μπορούμε να κάνουμε λόγο για τρείς μορφές ιδιωτικότητας [48]:

- την εδαφική ιδιωτικότητα (territorial privacy), που αφορά το φυσικό περιβάλλον που περιβάλλει ένα πρόσωπο (π.χ. η οικία, το εργασιακό περιβάλλον),
- την ιδιωτικότητα του ατόμου (privacy of the person), που αφορά την προστασία του προσώπου από εξωτερικές παρεμβάσεις (π.χ. ο σωματικός έλεγχος, δοκιμές φαρμάκων) και
- την πληροφοριακή ιδιωτικότητα (informational privacy), που αφορά τον έλεγχο του προσώπου σχετικά με το αν και πως οι προσωπικές του πληροφορίες μπορούν να συλλεχθούν, αποθηκευτούν, επεξεργαστούν και κοινοποιηθούν περαιτέρω.

Στο πλαίσιο των έξυπνων πόλεων, όπου γίνεται ευρεία χρήση τεχνολογιών της

πληροφορικής και των επικοινωνιών για την συλλογή και επεξεργασία πληροφοριών, διασπάται η έννοια της ιδιωτικότητας του προσώπου μεταμορφώνοντας το άτομο σε ένα ψηφιδωτό πληροφοριών, το λεγόμενο στην αμερικανική θεωρία «digital person» [49]. Γι' αυτό, λοιπόν, στην συγκεκριμένη περίπτωση η έννοια της ιδιωτικότητας πρέπει να εξετάζεται υπό το πρίσμα της πληροφοριακής ιδιωτικότητας, του δικαιώματος δηλαδή του ατόμου να εξετάζει τους κινδύνους που ελλοχεύουν για τον ιδιωτικό του βίο από την συλλογή και επεξεργασία των προσωπικών του δεδομένων και να λαμβάνει τα απαιτούμενα κατά την κρίση του μέτρα για την προστασία τους.

Με την έννοια «*προσωπικά δεδομένα*» ή άλλως «*δεδομένα προσωπικού χαρακτήρα*» εννοούμε όλες τις πληροφορίες που αφορούν ένα συγκεκριμένο πρόσωπο, το οποίο μέσω αυτών ταυτοποιείται ή δύναται να ταυτοποιηθεί. Ως δικαίωμα δε, το δικαίωμα στην προστασία των προσωπικών δεδομένων εντοπίζεται στο άρθρο 9Α του Συντάγματος και στο άρθρο 8 του Χ.Θ.Δ.Ε.Ε. και πρόκειται για ένα μεταγενέστερο δικαίωμα, η ανάγκη για το οποίο αναδείχθηκε υπό το πρίσμα της νέας ψηφιακής πραγματικότητας όπου η διάδοση, συλλογή και επεξεργασία των δεδομένων είναι αδιάκοπη και η προστασία της αυτονομίας και ελευθερίας του υποκειμένου από τις ως άνω ενέργειες κατέστη επιτακτική. Η «γέννηση» του δικαιώματος λοιπόν, ήταν απόρροια της ανάγκης προστασίας του δικαιώματος της προσωπικότητας και της ιδιωτικότητας από τις απειλές που εγκυμονούσε η τεχνολογία [47].

Κατόπιν των ανωτέρω, καθίσταται σαφές ότι το δικαίωμα στην προστασία των προσωπικών δεδομένων δεν ταυτίζεται με το δικαίωμα στην ιδιωτικότητα αλλά τα δύο δικαιώματα βρίσκονται σε μια σχέση αλληλεξάρτησης, με το δικαίωμα στην προστασία των προσωπικών δεδομένων να αναπαριστά ένα μόνο μέρος του δικαιώματος της ιδιωτικότητας, την πληροφοριακή ιδιωτικότητα που αναφέρθηκε ανωτέρω.

6.2. Ιδιωτικότητα και έξυπνες πόλεις

Το ερώτημα που επικρατεί είναι κατά ποσό μπορεί να εξασφαλισθεί η ιδιωτικότητα ενός προσώπου μέσα στο περιβάλλον της έξυπνης πόλης. Άλλοτε, πριν την τεχνολογική ανάπτυξη των πόλεων και την έναρξη της μετατροπής τους σε έξυπνες, ένα πρόσωπο μπορούσε να μετακινείται σε μια πόλη ελεύθερα, όντας ένας στους πολλούς, άγνωστος μεταξύ αγνώστων. Αυτή η κατάσταση έχει πλέον αλλάξει ριζικά και θα συνεχίσει να αλλάζει. Με την ενσωμάτωση τεχνολογιών της πληροφορικής και επικοινωνιών στις πόλεις, ο πολίτης πλέον, με κάθε του σχεδόν συναλλαγή ή ενέργεια, αφήνει το ψηφιακό του αποτύπωμα [50]. Το προσωποποιημένο για παράδειγμα ηλεκτρονικό εισιτήριο που κάποιος θα χρησιμοποιήσει για να μετακινηθεί μέσα στην έξυπνη πόλη με τα μέσα μαζικής μεταφοράς, το οποίο θα χρειαστεί να επικυρώσει στον σταθμό εισόδου και στον σταθμό εξόδου και η γνωστοποίηση της τοποθεσίας του σε μια εφαρμογή του δήμου για εντοπισμό

προβλημάτων (π.χ. ύπαρξη λακκούβας) είναι μερικά απλά καθημερινά παραδείγματα που αποδεικνύουν την μείωση του στοιχείου της ιδιωτικότητας στις έξυπνες πόλεις.

Ειδικότερα, η ύπαρξη ή μη και ο βαθμός της ιδιωτικότητας που έχει το υποκείμενο των δεδομένων στο πλαίσιο μιας έξυπνης πόλης, πρέπει να εξετάζεται υπό το πρίσμα πέντε διαστάσεων και εν προκειμένω (1) το απόρρητο της ταυτότητας, (2) το απόρρητο του ερωτήματος, (3) το απόρρητο της τοποθεσίας, (4) το απόρρητο του αποτυπώματος και (5) το απόρρητο του κατόχου. Αναλύοντας τις ως άνω διαστάσεις προκύπτουν τα κάτωθι [51]:

- **Το απόρρητο της ταυτότητας** σχετίζεται με την αποκάλυψη της ταυτότητας του πολίτη κάθε φορά που χρησιμοποιεί μια υπηρεσία της έξυπνης πόλης, όπως στο παράδειγμα της μεταφοράς που αναφέρθηκε ανωτέρω. Αν για τη χρήση της δημοτικής εφαρμογής ή υπηρεσίας απαιτείται η εξακρίβωση της ταυτότητας του χρήστη, τότε ο πάροχος της υπηρεσίας και τυχόν άλλα τρίτα μέρη θα μπορούν να συνδέσουν το συγκεκριμένο πρόσωπο – χρήστη με τη δραστηριότητά του. Μία λύση στην προστασία της ιδιωτικότητας του προσώπου και ειδικότερα του απορρήτου της ταυτότητας θα μπορούσε να είναι η χρήση τεχνικών ψευδωνυμοποίησης για την σύνδεση με τις εφαρμογές / υπηρεσίες προκειμένου να μην είναι δυνατή η συσχέτιση της χρήση της υπηρεσίας με συγκεκριμένο πρόσωπο.
- **Το απόρρητο του ερωτήματος** σχετίζεται με τη διατήρηση του απορρήτου των ερωτημάτων που υποβάλλουν οι πολίτες στις διάφορες υπηρεσίες της έξυπνης πόλης αλλά και στη διατήρηση της ανωνυμίας των προσώπων που υποβάλλουν τα συγκεκριμένα ερωτήματα. Η προστασία του ως άνω απορρήτου είναι σημαντική προκειμένου να μην δύνανται οι πάροχοι των υπηρεσιών ή τρίτοι να συλλέγουν πληροφορίες για τις συνήθειες των ως άνω προσώπων, οι οποίες (πληροφορίες) μπορούν να τους βοηθήσουν να καταρτίσουν το προφίλ των προσώπων - πολιτών. Το παράδειγμα της μεταφοράς που χρησιμοποιήθηκε ανωτέρω μπορεί να εφαρμοσθεί και σε αυτή την περίπτωση, όπου σε μια παραλλαγή αυτού, όπως στην αναζήτηση χώρου στάθμευσης, η συγκεκριμένη αναζήτηση μπορεί να συλλεχθεί και σε συνδυασμό με άλλες πληροφορίες να οδηγήσει στην κατάρτιση του προφίλ του ατόμου ανάλογα με τις συνήθειες του και π.χ. την περιοχή που τακτικά ψάχνει μέσω της δημοτικής υπηρεσίας να παρκάρει. Προκειμένου να προστατευθούν οι πολίτες της έξυπνης πόλης θα πρέπει να βρεθούν τρόποι με τους οποίους θα καθίσταται αδύνατος ο συσχετισμός μεταξύ των πολιτών και των ερωτημάτων που υποβάλουν κατά τη χρήση των διαφόρων υπηρεσιών της έξυπνης πόλης.
- **Το απόρρητο της τοποθεσίας** σχετίζεται με τη διασφάλιση της ιδιωτικοτήτας της φυσικής τοποθεσίας του πολίτη. Στο περιβάλλον της έξυπνης πόλης, ωστόσο, η γνωστοποίηση της τοποθεσίας από την πλευρά του πολίτη, προκειμένου να χρησιμοποιήσει τις έξυπνες υπηρεσίες, είναι σχεδόν πάντα απαραίτητη. Ένα απλό παράδειγμα είναι η χορήγηση της τοποθεσίας του χρήστη στη δημοτική εφαρμογή παρκαρίσματος, προκειμένου να τον οδηγήσει στην κοντινότερη θέση στάθμευσης. Για την προστασία της ιδιωτικότητας των πολιτών και της φυσικής τοποθεσίας τους θα μπορούσαν να εισαχθούν στις εφαρμογές που απαιτούν τη γνωστοποίηση της σε

πραγματικό χρόνο τοποθεσίας του χρήστη, κάποιες τεχνικές απόκρυψης της πραγματικής τοποθεσίας, ούτως ώστε να μην είναι δυνατή η παρακολούθηση του χρήστη από τον πάροχο ή τρίτα μέρη.

- **Το απόρρητο του αποτυπώματος** σχετίζεται με τον έλεγχο των πληροφοριών που μπορούν να ανακτηθούν ή να συναχθούν από σύνολα μικροδεδομένων. Αυτά τα μικροδεδομένα συλλέγονται με διάφορους τρόπους, όπως με τους αισθητήρες που είναι εγκατεστημένοι στα διάφορα σημεία της έξυπνης πόλης. Επομένως, το αποτύπωμα του χρήστη αφορά όλα τα σύνολα μικροδεδομένων που καταγράφουν πληροφορίες σχετικά με τη χρήση της εκάστοτε έξυπνης υπηρεσίας ή εφαρμογής από τον χρήστη. Τα σύνολα αυτά μικροδεδομένων, τα οποία περιέχουν πληροφορίες για τους χρήστες και δη ευαίσθητες πληροφορίες μερικές φορές, είθισται να δημοσιεύονται ή διατίθενται σε τρίτους, οι οποίοι (τρίτοι) μπορούν να τα χρησιμοποιήσουν για άλλους δευτερεύοντες σκοπούς. Επομένως, είναι σημαντικό να βρεθούν τρόποι διασφάλισης του απορρήτου του αποτυπώματος των χρηστών. Ειδικότερα, στα σύνολα των μικροδεδομένων θα πρέπει, πριν δημοσιευτούν ή διατεθούν σε οποιονδήποτε τρίτο, να χρησιμοποιούνται τεχνικές με τις οποίες αφενός θα προστατεύεται η ιδιωτικότητα του χρήστη και αφετέρου θα απελευθερώνονται οι απαιτούμενες μόνο πληροφορίες για τη δευτερεύουσα χρήση. Προκειμένου να συμβεί αυτό με τις τεχνικές αυτές θα πρέπει να επιτυγχάνεται η παραμόρφωση των δεδομένων σε τέτοιο βαθμό ώστε να αποφεύγεται η σύνδεση των δεδομένων με συγκεκριμένα πρόσωπα αλλά να διατηρείται ταυτόχρονα η χρησιμότητα των δεδομένων. Τέτοιου είδους τεχνικές είναι η ψευδωνυμοποίηση, ήτοι η αντικατάσταση των αναγνωριστικών στοιχείων από ψευδώνυμα ή η εξ ολοκλήρου διαγραφή τους. Τέλος, πέρα από τις τεχνικές αυτές θα πρέπει να εκτελούνται πριν την κοινοποίηση ορισμένες διαδικασίες επιμέτρησης του κινδύνου γνωστοποίησης των προσωπικών πληροφοριών των χρηστών, ο οποίος θα πρέπει να λαμβάνεται υπόψιν για τη διάθεση ή μη των δεδομένων στους τρίτους.
- Τέλος, **το απόρρητο του κατόχου** σχετίζεται με τον υπολογισμό και συσχετισμό των ερωτημάτων στις διάφορες βάσεις δεδομένων από διαφορετικές οντότητες και τη διαφύλαξη του απορρήτου των ερωτημάτων που αναφέρθηκε ανωτέρω. Ένα τέτοιό παράδειγμα θα μπορούσε να είναι η επιθυμία μιας εταιρείας που παρέχει ηλεκτρική ενέργεια να συσχετίσει τα δεδομένα κατανάλωσης της ηλεκτρικής ενέργειας με τα δεδομένα χρήσης άλλων υπηρεσιών, όπως το φυσικό αέριο. Με την παροχή, ωστόσο, των ως άνω πληροφοριών στην εταιρεία ηλεκτρισμού του παραδείγματός μας, τίθεται ο κίνδυνος χρήσης των δεδομένων των άλλων εταιρειών για άλλους σκοπούς, π.χ. στρατηγικούς ή εμπορικούς. Συνεπώς, οι πάροχοι δεν πρέπει να απελευθερώνουν ελεύθερα τα δεδομένα που έχουν συλλέξει σε άλλους παρόχους ή τρίτα μέρη εν γένει. Προκειμένου, να επιτευχθεί ένας έλεγχος των δεδομένων που μοιράζονται θα πρέπει να εφαρμοστούν ορισμένες τεχνικές στα ερωτήματα που υποβάλλονται σε όλες τις βάσεις δεδομένων προκειμένου να ελέγχονται τα εκάστοτε ερωτήματα και να περιορίζονται οι πληροφορίες που διαμοιράζονται στις απολύτως απαραίτητες.

Προκειμένου οι πόλεις να μετατραπούν επιτυχώς σε «έξυπνες πόλεις» θα πρέπει να βρεθούν τρόποι να διασφαλιστεί η ιδιωτικότητα των πολιτών, η οποία μπορεί να λάβει πολλές διαστάσεις, μερικές εκ των οποίων αναφέρθηκαν ανωτέρω. Σε πρώτη φάση θα πρέπει να διερευνηθούν οι πιθανοί κίνδυνοι για την ιδιωτικότητα των πολιτών από τη χρήση των έξυπνων υπηρεσιών και εφαρμογών που παρέχει η ίδια η πόλη και ύστερα να βρεθούν τρόποι να περιοριστούν και να μετριαστούν. Με τον τρόπο αυτό θα καταστεί εφικτό να παρέχονται καλύτερες υπηρεσίες για τον πολίτη, διευκολύνοντας την καθημερινότητα του και διασφαλίζοντας παράλληλα τον ιδιωτικό του βίο.

6.3. Συλλογή δεδομένων στις έξυπνες πόλεις

6.3.1. Η αξία των δεδομένων στην εξέλιξη της έξυπνης πόλης

Η ιδέα της έξυπνης πόλης είναι στενά συνδεδεμένη με την συλλογή δεδομένων, τόσο του περιβάλλοντος όσο και των πολιτών, προκειμένου τα δεδομένα αυτά να επεξεργαστούν και να χρησιμοποιηθούν για να δημιουργήσουν αξία προς τους πολίτες μέσω της καλυτέρευσης των παρεχόμενων σε αυτούς υπηρεσιών. Τα δεδομένα μπορούν να βοηθήσουν στη βελτίωση της λειτουργίας της έξυπνης πόλης και στην διευκόλυνση της ζωής των πολιτών με πολλούς τρόπους.

Κατ' αρχήν, δέον να λεχθεί ότι τα δεδομένα μπορούν να δημιουργήσουν αξία για τους πολίτες τους χωρίς να χρειαστεί η επεξεργασία τους αλλά π.χ. μέσω της ανάλυσης τους. Τα δεδομένα μπορούν να μοιράζονται ανάμεσα στους φορείς της έξυπνης πόλης, είτε ως ακατέργαστα δεδομένα είτε έχοντας ήδη υποστεί μια μορφή επεξεργασίας με σκοπό την περαιτέρω επεξεργασία τους. Με αυτό τον τρόπο η πόλη μπορεί να συλλέγει πληροφορίες για τους πολίτες της και να τις χρησιμοποιεί για τη βελτιστοποίηση των υπηρεσιών της σε αυτούς [52].

Ακόμη, τα δεδομένα μπορούν να βοηθήσουν στην βελτιστοποίηση της εσωτερικής οργάνωσης και λειτουργίας των διαδικασιών της έξυπνης πόλης. Με την παροχή λεπτομερέστερων πληροφοριών σχετικά με τις ως άνω διαδικασίες μπορεί να γίνει δυνατή η ανίχνευση και θεραπεία τυχόν ανεπαρκειών χωρίς να χρειάζεται ριζική αλλαγή στη ρουτίνα που ακολουθείται. Τα δεδομένα, δε, μπορούν να συνδράμουν στην αυτοματοποίηση - είτε μερικώς είτε ολικώς – ορισμένων διαδικασιών, η οποία θα οδηγήσει στη βελτιστοποίηση της διαχείρισης της έξυπνης πόλης. Προκειμένου π.χ. να ρυθμιστεί η κυκλοφορία στους δρόμους, τα δεδομένα που συλλέγονται από τις κάμερες και τους αισθητήρες στα φανάρια μπορούν να επεξεργάζονται προκειμένου να ρυθμίζουν αυτοματοποιημένα και σε πραγματικό χρόνο την κίνηση που δημιουργείται [53]. Από την επεξεργασία δε των δεδομένων αυτών ειδικοί αλγόριθμοι μπορούν να εντοπίζουν μοτίβα της κίνησης και να προβλέπουν τα σημεία και τις ώρες που μπορεί να προκύψει αυξημένη κυκλοφορία στους δρόμους. Ακόμη, τα δεδομένα μπορούν να βοηθήσουν τους φορείς της πόλης να λάβουν τις κατάλληλες αποφάσεις για τον σχεδιασμό και την ανάπτυξη της έξυπνης

πόλης, όπως με τη χρήση αλγοριθμικών συστημάτων για την πρόβλεψη αναγκών υγείας και φροντίδας των ηλικιωμένων. Η απόκτηση δε όλο και μεγαλύτερης γνώσης σχετικά με τη ζωή της πόλης και τις ανάγκες των πολιτών μπορεί να βοηθήσει στην ανάπτυξη νέων προϊόντων και υπηρεσιών προς εξυπηρέτηση των πολιτών [54].

Τέλος, η συγκέντρωση μεγάλων ποσοτήτων δεδομένων για τους πολίτες μπορεί να βοηθήσει τους φορείς της έξυπνης πόλης να τα χρησιμοποιήσουν προκειμένου να βρουν αποτελεσματικούς τρόπους σύνδεσης με τους πολίτες. Ως σύνδεση δε δεν νοείται μόνο η σύνδεση με τη μορφή δημοσίων σχέσεων αλλά μπορεί να επιτευχθεί και πραγματική εξατομικευμένη επικοινωνία [54]. Με όλους τους ανωτέρω τρόπους αλλά και με πολλούς άλλους ακόμη, η συλλογή των δεδομένων στην έξυπνη πόλη μπορεί να έχει θετικό αντίκτυπο στους πολίτες της και στον τρόπο ζωής τους μέσα σε αυτήν.

6.3.2. Ζητήματα από την συλλογή των δεδομένων στις έξυπνες πόλεις

Όπως έχει γίνει κατανοητό μέχρι τώρα, ο τρόπος με τον οποίο, κατά κύριο λόγο, συλλέγονται τα δεδομένα στις έξυπνες πόλεις είναι μέσω της χρήσης των τεχνολογιών του Διαδικτύου των Πραγμάτων. Αισθητήρες, άλλοι ορατοί και άλλοι αόρατοι, μονίμως συνδεδεμένοι με κάποιο δίκτυο, είναι εγκατεστημένοι σε κάθε σημείο της έξυπνης πόλης και συλλέγουν δεδομένα είκοσι τέσσερις ώρες το εικοσιτετράωρο. Από το έξυπνο κινητό μας τηλέφωνο, με το οποίο θα γνωστοποιήσουμε την τοποθεσία μας για να βρούμε μία θέση πάρκινγκ μέσω της δημοτικής εφαρμογής ως τους έξυπνους κάδους απορριμμάτων που ενημερώνουν την αρμόδια δημοτική υπηρεσία σχετικά με την συχνότητα που γεμίζει ο κάδος π.χ. έξω από το σπίτι μας, τα δεδομένα συλλέγονται, επεξεργάζονται και πολλές φορές συσχετίζονται μεταξύ τους δημιουργώντας το προφίλ του κάθε πολίτη. Ανακύπτει, λοιπόν, το ερώτημα, κατά πόσο ασκείται μια μορφή επιτήρησης μέσω των εφαρμογών του Διαδικτύου των Πραγμάτων υπό το πρόσχημα της ομαλής λειτουργίας των υπηρεσιών της έξυπνης πόλης. Πέρα, όμως, από τις δημοτικές αρχές, τις οποίες ο πολίτης γνωρίζει και έχει παράσχει την συγκατάθεσή του – στο βαθμό που αυτή επαρκή – για την επεξεργασία των δεδομένων του, δεν είναι απίθανο τα δεδομένα αυτά να μεταβιβάζονται στον κατασκευαστή των χρησιμοποιούμενων εφαρμογών του Διαδικτύου των Πραγμάτων ή σε άλλα τρίτα μέρη, τα οποία μπορούν να χρησιμοποιήσουν τις πληροφορίες αυτές προς ίδιο όφελος.
Το κύριο πρόβλημα, ωστόσο, έγκειται στη δυσκολία επίγνωσης από το άτομο – πολίτη όλων των εφαρμογών του Διαδικτύου των Πραγμάτων που υπάρχουν σε έναν χώρο και με τις οποίες ανταλλάσσει διαρκώς δεδομένα, χωρίς να γνωρίζει ορισμένες φορές ποια ακριβώς από τα δεδομένα του συλλέγονται και για ποιο λόγο. Ακόμη κι αν ήταν δυνατή η εκπαίδευση των πολιτών να γνωρίζουν με ποιόν τρόπο θα κοινοποιήσουν μόνο τα δεδομένα που οι ίδιοι θέλουν πραγματικά να μοιραστούν, φαντάζει σχεδόν ανέφικτο να μπορούν να διαφοροποιήσουν, ανάλογα με τις προτιμήσεις τους, την πολιτική απορρήτου που εφαρμόζουν οι εκάστοτε συσκευές του Διαδικτύου των Πραγμάτων, ειδικά την στιγμή που υπάρχουν

δυσκολίες στη γνώση και μόνο της εκάστοτε εφαρμοζόμενης πολιτικής [55]. Ο τρόπος αυτός δε ενημέρωσης των πολιτών για τα πιθανά ζητήματα από τη χρήση συσκευών του Διαδικτύου των Πραγμάτων κρίνεται ανεπαρκής όταν αυτές εφαρμόζονται σε δημόσια κλίμακα.

Όπως έχει λεχθεί απ' τον Peppet, υπάρχουν τέσσερις εγγενείς πτυχές των συσκευών που λειτουργούν με αισθητήρες, οι οποίες δημιουργούν πραγματικά προβλήματα διακρίσεων, ασφάλειας, ιδιωτικότητας και ζητήματα συγκατάθεσης. Οι πτυχές αυτές είναι (α) οι σύνθετες επιπτώσεις από τη χρήση πολλών διαφορετικών αισθητήρων, (β) η πλήρης σχεδόν αδυναμία αποταυτοποίησης των δεδομένων που έχουν συλλεχθεί μέσω των αισθητήρων, (γ) η πιθανότητα ότι οι συσκευές του Διαδικτύου των Πραγμάτων θα είναι εκ φύσεως επιρρεπείς σε ζητήματα ασφάλειας και (δ) η δυσκολία πραγματικής συγκατάθεσης του υποκειμένου στην επεξεργασία των δεδομένων του υπό αυτό το πλαίσιο [56]. Λαμβάνοντας υπόψιν τα ανωτέρω, γίνεται κατανοητό και επιβεβαιώνεται ότι η προσέγγιση ειδοποίησης και συναίνεσης δεν επαρκεί όσον αφορά την ιδιωτικότητα των δεδομένων. Αυτό συμβαίνει λόγω της εμφανούς αδυναμίας παροχής επαρκούς πληροφόρησης στο υποκείμενο σχετικά με την διαδικασία συλλογής (το πρόσωπο/φορέα που συλλέγει τα δεδομένα, τα δεδομένα που συλλέγονται, τον τρόπο χρήσης τους κλπ) καθιστώντας εξ αρχής άτοπη την εξέταση μιας συγκατάθεσης που έχει δοθεί σε αυτό το πλαίσιο [57].

Το 2018 διεξήχθη μια έρευνα στην Αγγλία αναφορικά με τα ζητήματα ιδιωτικότητας που προκύπτουν από τη δημόσια χρήση εφαρμογών του Διαδικτύου των Πραγμάτων στις έξυπνες πόλεις και την αντίληψη των πολιτών ως προς τους πιθανούς κινδύνους, την εμπιστοσύνη τους σε αυτά και τις επιθυμίες τους ως προς τον τρόπο με τον οποίο θα ήθελαν να λειτουργούν. Σύμφωνα με την έρευνα η ανάπτυξη των κατάλληλων μεθόδων για την ενημέρωση των πολιτών σχετικά με την συλλογή και επεξεργασία των δεδομένων είναι το κλειδί στην ανάπτυξη μιας έξυπνης πόλης δεδομένου ότι προκειμένου να ευδοκιμήσει το εγχείρημα της έξυπνης πόλης απαιτείται η συμμετοχή των πολιτών και η τελευταία μπορεί να διασφαλιστεί μόνο μέσω της δημιουργίας ενός αισθήματος εμπιστοσύνης και ασφάλειας της ιδιωτικότητας των δεδομένων τους από τους φορείς της έξυπνης πόλης. Όπως προέκυψε δε από την έρευνα, οι πολίτες επιθυμούν να έχουν πρόσβαση στις σχετικές πληροφορίες, συμπεριλαμβανομένου του προσώπου με το οποίο θα μπορούν να επικοινωνήσουν προκειμένου να λάβουν περισσότερες πληροφορίες σχετικά με τις συσκευές του Διαδικτύου των Πραγμάτων και την συλλογή των δεδομένων [57].

Το μόνο σίγουρο είναι ότι μέρα με τη μέρα, όσο οι τεχνολογίες της πληροφορικής και επικοινωνιών εξελίσσονται, τόσο περισσότερα δεδομένα συλλέγονται, επεξεργάζονται και αποθηκεύονται. Η μαζική δε και αδιάκοπη συλλογή και επεξεργασία των ως άνω δεδομένων μπορεί να έχει αρνητικές συνέπειες τόσο ως προς το απόρρητο των ίδιων των πληροφοριών όσο και ως προς την ιδιωτικότητα των πολιτών. Κατά πρώτον, η δυνατότητα μαζικής επιτήρησης και ελέγχου των πολιτών, καθώς και ο σχεδιασμός του ατομικού προφίλ κάθε πολίτη από τον συσχετι-

σμό των πληροφοριών που αναφέρθηκαν και ανωτέρω. Κατά δεύτερον, η αυξανόμενη διεισδυτικότητα των τεχνολογιών της πληροφορικής και επικοινωνιών στην καθημερινότητα των πολιτών με την σταδιακή μετατροπή όλων των συναλλαγών σε ψηφιακών και την ανάγκη χρήσης ειδικών μεθόδων ταυτοποίησης (π.χ. κωδικοί πρόσβασης, αριθμοί πιστωτικών καρτών, στοιχεία τηλεφώνου κλπ), γεγονός που καθιστά αδύνατη τη διαβίωση στην έξυπνη πόλη δίχως να αφήσεις το ψηφιακό σου αποτύπωμα σε κάθε ενέργεια. Τρίτον, η μαζική συλλογή, επεξεργασία και οργάνωση μεγάλων συνόλων δεδομένων για έναν συγκεκριμένο σκοπό / υπηρεσία μπορεί να αλλάξει τους σκοπούς για τους οποίους θα χρησιμοποιηθούν αυτά τα δεδομένα είτε προς το καλύτερο είτε προς το χειρότερο. Τέλος, η συλλογή και επεξεργασία πολλών και διαφορετικών ειδών δεδομένων μπορεί να οδηγήσει, κατόπιν συνδυασμού τους και παράλληλης επεξεργασίας, στην αποκάλυψη πρόσθετων πληροφοριών για τα πρόσωπα – πολίτες, οι οποίες ουδέποτε σκοπείτο να γνωστοποιηθούν [58].

6.4. Ζητήματα περιορισμού των ελευθεριών των πολιτών της έξυπνης πόλης

Η αδιάκοπη και ανέλεγκτη συλλογή και επεξεργασία των δεδομένων μέσα σε μια έξυπνη πόλη μπορεί να επιφέρει αρνητικές συνέπειες στην ίδια την συμπεριφορά και ψυχολογία των προσώπων που κατοικούν σε αυτή, εγείροντας με αυτόν τρόπο ερωτήματα ως προς την αξία και τον τρόπο συλλογής και επεξεργασίας των δεδομένων. Πολλές φαινομενικά μη επεμβατικές μέθοδοι συλλογής δεδομένων στις έξυπνες πόλεις μπορούν να χρησιμοποιηθούν από τα λάθος πρόσωπα ή για τα λάθος συμφέροντα προκειμένου να διεισδύσουν στη ζωή των πολιτών. Ένα τέτοιο παράδειγμα είναι οι κάμερες παρακολούθησης της κυκλοφορίας που είναι τοποθετημένες στους δρόμους για να παρακολουθούν, κατά κύριο λόγο, την σωστή τήρηση του κώδικα οδικής κυκλοφορίας και οι οποίες συλλέγουν πληροφορίες, όπως οι πινακίδες των οχημάτων και τυχόν δυνατοί ήχοι, όπως πυροβολισμοί ή ήχοι από συγκρούσεις αυτοκινήτων. Με την μετατροπή των πόλεων σε έξυπνων, σε πολλές από αυτές τις κάμερες δύνανται να προστεθούν τεχνολογίες τεχνητής νοημοσύνης, οι οποίες επιτρέπουν την αναγνώριση των προσώπων των διερχομένων σε πραγματικό ή μη χρόνο, καθώς επίσης οι ήχοι που αναγνωρίζουν αυτές οι κάμερες να επεκταθούν σε ομιλίες των διερχομένων καταγράφοντας τις σχετικές συζητήσεις [59]. Με την εγκατάσταση δε πληθώρας αισθητήρων σε όλα τα σημεία μιας πόλης, με τους οποίους θέλοντας και μη αλληλοεπιδρούν τα πρόσωπα που κατοικούν σε αυτή, καθίσταται εφικτή η παρακολούθηση των προσώπων, η οποία έχει ως αποτέλεσμα την πρόκληση του λεγόμενου «chilling effect».

Ως «chilling effect» περιγράφεται το φαινόμενο κατά το οποίο ένα πρόσωπο υπό τον φόβο της παρακολούθησης της δραστηριότητάς του ή κάποιας πιθανής νομικής κύρωσης που έχει σχέση με αυτήν, αλλάζει τον συνήθη τρόπο συμπεριφοράς του, αποφεύγοντας να μιλήσει ανοιχτά ή να συμμετάσχει σε διάφορες δραστηριότητες παρά το γεγονός ότι αυτές μπορεί να είναι εν τοις πράγμασι νόμιμες [60]. Στην ουσία, το πρόσωπο έχοντας σταθμίσει τις τυχόν αρνητικές συνέπειες που υπάρχει περίπτωση να υποστεί και την επιθυμία να δράσει όπως αισθάνεται,

μπαίνει σε μια διαδικασία αυτολογοκρισίας και επιλέγει να καταπιεστεί. Η παρακολούθηση, λοιπόν, των πολιτών λειτουργεί αποτρεπτικά, καταπατώντας τα συνταγματικώς κατοχυρωμένα δικαιώματα τους, όπως το δικαίωμα στην ελεύθερη ανάπτυξη της προσωπικότητας[8], το δικαίωμα του συνέρχεσθαι[9] και συνεταιρίζεσθαι [10] και το δικαίωμα στην ελευθερία της έκφρασης[11]. Μία από τις αιτίες που προκαλεί αυτό το συναίσθημα και την αλλαγή συμπεριφοράς στους πολίτες είναι η καχυποψία αφενός ως προς τα κίνητρα των αρχών και των προσώπων που είναι αρμόδια για την συλλογή και την επεξεργασία των δεδομένων και αφετέρου ο φόβος διαρροής των δεδομένων ή πρόσβασης σε αυτά από μη εξουσιοδοτημένα πρόσωπα ή ακόμη και κοινοποίησης των δεδομένων σε τρίτες ιδιωτικές εταιρείες, οι οποίες θα τα χρησιμοποιήσουν προς όφελός τους εις βάρος των ίδιων των υποκειμένων των δεδομένων. Ευαίσθητα προσωπικά δεδομένα, αξίες και συνήθειες των προσώπων μπορούν να αποκαλυφθούν και να συγκεντρωθούν σε βάσεις δεδομένων, παραμένοντας σε αδράνεια μέχρι την στιγμή που κάποιο από τα ανωτέρω αναφερόμενα πρόσωπα θα θελήσει να τα χρησιμοποιήσει. Μόνη η γνώση ύπαρξης αυτού του ενδεχόμενου είναι αρκετή για να αποτρέψει τους πολίτες να ασχοληθούν με νόμιμες δραστηριότητες, προκειμένου να κρατήσουν χαμηλό προφίλ και να αποφύγουν μια ενδεχόμενη λογοκρισία, περιθωριοποίηση ή ακόμη και τιμωρία [61].

Καταλήγοντας, τα ζητήματα περιορισμού των δικαιωμάτων που ανακύπτουν από τη μαζική συλλογή και επεξεργασία των δεδομένων των πολιτών πρέπει να ληφθούν σοβαρά υπόψιν και να σταθμισθούν διότι, ως αναλύθηκε ανωτέρω, τέτοιου είδους επεξεργασία έρχεται σε σύγκρουση με τα θεμελιώδη δικαιώματα των πολιτών. Η ελευθερία έκφρασης και ανάπτυξης της προσωπικότητας του ατόμου είναι άρρηκτα συνδεδεμένη με το απόρρητο και από την στιγμή που δεν μπορεί να διασφαλιστεί το δεύτερο, προσβάλλεται αυτομάτως η πρώτη. Κρίνεται αναγκαίο, λοιπόν, οι φορείς και τα λοιπά εμπλεκόμενα μέρη της έξυπνης πόλης να βρουν τρόπους ώστε να μετατρέψουν τις πόλεις σε έξυπνες, προστατεύοντας παράλληλα τις ατομικές ελευθερίες των πολιτών τους.

7. ΕΞΥΠΝΕΣ ΠΟΛΕΙΣ ΚΑΙ ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ (ΓΚΠΔ)

Η ραγδαία ανάπτυξη της τεχνολογίας και των υπηρεσιών του Διαδικτύου των Πραγμάτων έχουν ήδη αρχίσει να μεταμορφώνουν τις πόλεις σε «έξυπνες». Διαρκώς νέες εφαρμογές ανακαλύπτονται, καλύπτοντας όλα τα στοιχεία και τους τομείς που απαρτίζουν μια πόλη, με σκοπό να καταστούν όλα τα επιμέρους στοιχεία της «έξυπνα». Στο επίκεντρο αυτής της ανάπτυξης και εξελικτικής διαδικασίας

[8] Βλ. άρθρο 5 του Συντάγματος
[9] Βλ. άρθρο 11 του Συντάγματος
[10] Βλ. άρθρο 12 του Συντάγματος
[11] Βλ. άρθρο 14 του Συντάγματος

των πόλεων βρίσκεται ο άνθρωπος και δη τα δεδομένα που παρέχει. Επειδή, ωστόσο, ως αναφέρθηκε η τεχνολογία εξαπλώνεται σε όλους τους τομείς της έξυπνης πόλης, καθίσταται προφανές ότι τα δεδομένα και οι πληροφορίες που συλλέγονται και επεξεργάζονται ενδέχεται πολλές φορές να ενέχουν κινδύνους για την ιδιωτικότητα του σύγχρονου πολίτη. Ζητήματα, επομένως, έχουν γεννηθεί ως προς το βαθμό που η μετατροπή μιας πόλης σε «έξυπνη» είναι σύννομη με τον Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων (ΓΚΠΔ).

7.1. Ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ)

Στις 25 Ιανουαρίου 2012 η Επιτροπή της Ευρωπαϊκής Ένωσης παρουσίασε προς δημόσια διαβούλευση την Πρόταση Κανονισμού για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών [62]. Τέσσερα χρόνια αργότερα και ειδικότερα στις 14 Απριλίου 2016 ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) ψηφίσθηκε και λίγο αργότερα, στις 4 Μαΐου 2016, δημοσιεύθηκε στην εφημερίδα της Ευρωπαϊκής Ένωσης με αριθμό 2016/679 [40]. Έκτοτε ο Κανονισμός καθορίζει το γενικό πλαίσιο για την προστασία των προσωπικών δεδομένων στην Ευρωπαϊκή Ένωση.

Θεμελιώδης έννοια του Κανονισμού είναι αυτή των προσωπικών δεδομένων, η οποία όπως ορίζεται στο άρθρο 4 περ. 1 περικλείει «*κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)*». Ως ταυτοποιήσιμο δε φυσικό πρόσωπο ορίζει 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*» [40].

Επίσης, σημαντικό είναι να αναφερθεί εδώ και ο ορισμός που δίνεται στην περ. 2 του άρθρου 4 του Κανονισμού για την επεξεργασία ως «*κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή*» καθώς, επίσης, και η βασική έννοια της συγκατάθεσης του υποκειμένου των δεδομένων που περιγράφεται στην περ. 11 του ίδιου ως άνω άρθρου ως «*κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν*» [40].

Στην Ελλάδα υπήρχε νομοθετική πρόβλεψη για την ασφάλεια των προσωπικών δεδομένων των προσώπων ήδη από το 1997 με τον Ν. 2472/1997. Κατόπιν ψήφισης, ωστόσο, του Κανονισμού, το προϊσχύσαν νομοθετικό πλαίσιο αντικαταστάθηκε από τον Ν. 4624/2019, ο οποίος δημοσιεύθηκε στην επίσημη Εφημερίδα της Κυβέρνησης την 29.08.2019 (ΦΕΚ Α', 137/29.08.2019) και δυνάμει του οποίου διευρύνθηκε το πλαίσιο της προστασίας των δεδομένων και δη οι κατηγορίες των δεδομένων που προστατεύονται. Ειδικότερα, με το άρθρο 44 του νόμου αυτού προβλέπονται τα κάτωθι είδη δεδομένων και δίνονται οι κάτωθι ορισμοί [63]:

α) «**δεδομένα προσωπικού χαρακτήρα**»: 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 σε 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·[12]

β) «**γενετικά δεδομένα**»: τα δεδομένα προσωπικού χαρακτήρα που αφορούν στα γενετικά χαρακτηριστικά φυσικού προσώπου που κληρονομήθηκαν ή αποκτήθηκαν, όπως προκύπτουν, ιδίως, από ανάλυση βιολογικού δείγματος του εν λόγω φυσικού προσώπου και τα οποία παρέχουν μοναδικές πληροφορίες σχετικά με τη φυσιολογία ή την υγεία του εν λόγω φυσικού προσώπου·[13]
γ) «**βιομετρικά δεδομένα**»: δεδομένα προσωπικού χαρακτήρα τα οποία προκύπτουν από ειδική τεχνική επεξεργασία συνδεόμενη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου, και τα οποία επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου, όπως εικόνες προσώπου ή δακτυλοσκοπικά δεδομένα·[14]

δ) «**δεδομένα που αφορούν στην υγεία**»: δεδομένα προσωπικού χαρακτήρα τα οποία σχετίζονται με τη σωματική ή ψυχική υγεία ενός φυσικού προσώπου, περιλαμβανομένης της παροχής υπηρεσιών υγειονομικής φροντίδας, και τα οποία αποκαλύπτουν πληροφορίες σχετικά με την κατάσταση της υγείας του·[15]

ε) «**ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα**»: δεδομένα Προσωπικού Χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, γενετικά δεδομένα, βιομετρικά δεδομένα για την αδιαμφισβήτητη ταυτοποίηση ενός φυσικού προσώπου, δεδομένα που αφορούν την υγεία, δεδομένα που αφορούν τη σεξουαλική ζωή ή τον σεξουαλικό προσανατολισμό φυσικού προσώπου·[16]

---

[12] Βλ. περίπτωση 1 α) του αρ. 44 του Ν. Ν. 4624/2019
[13] Βλ. περίπτωση 1 ια) του αρ. 44 του Ν. Ν. 4624/2019
[14] Βλ. περίπτωση 1 ιβ) του αρ. 44 του Ν. Ν. 4624/2019
[15] Βλ. περίπτωση 1 ιγ) του αρ. 44 του Ν. Ν. 4624/2019
[16] Βλ. περίπτωση 1 ιδ) του αρ. 44 του Ν. Ν. 4624/2019

Επίσης, προβλέφθηκε για πρώτη φορά η προστασία από την κατάρτιση προφίλ, η οποία στο ίδιο ως άνω άρθρο ορίζεται ως «*οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που συνίσταται στη χρήση δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση ορισμένων προσωπικών πτυχών ενός φυσικού προσώπου, ιδίως για την ανάλυση ή την πρόβλεψη πτυχών που αφορούν την απόδοση στην εργασία, στην οικονομική κατάσταση, στην υγεία, στις προσωπικές προτιμήσεις, στα ενδιαφέροντα, στην αξιοπιστία, στη συμπεριφορά, στη θέση ή στις μετακινήσεις τού εν λόγω φυσικού προσώπου*»[17].

7.2. Βασικές αρχές και προϋποθέσεις του ΓΚΠΔ

7.2.1. Η αρχή της ελαχιστοποίησης

Σύμφωνα με την αρχή της ελαχιστοποίησης, η οποία θεσπίζεται στην περ. γ του άρθρου 5 του Κανονισμού τα δεδομένα προσωπικού χαρακτήρα που συλλέγονται και επεξεργάζονται πρέπει να είναι «*κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία*». Συνεπώς, η αναγκαιότητα αποτελεί βασικό στοιχείο της αρχής της ελαχιστοποίησης και της νομιμότητας επεξεργασίας των δεδομένων αυτών. Εκ των ανωτέρω προκύπτει, όπως σαφώς αναφέρεται και στις αιτιολογικές σκέψεις του Κανονισμού, ότι τα δεδομένα θα πρέπει να περιορίζονται στα απολύτως αναγκαία για τον εκάστοτε σκοπό της επεξεργασίας, καθώς επίσης ότι ο χρόνος διατήρησής τους θα πρέπει να περιορίζεται στον ελάχιστα δυνατό. Ακόμη, τα δεδομένα θα πρέπει να υπόκεινται επεξεργασίας μόνο εάν ο επιθυμητός σκοπός δεν μπορεί να επιτευχθεί με άλλα μέσα [40][18].

7.2.2. Privacy by design / by default

Στην προσπάθεια διασφάλισης ενός υψηλού επιπέδου προστασίας των δεδομένων προσωπικού χαρακτήρα των πολιτών της Ένωσης, συνεκτιμώντας παράλληλα το ραγδαίο βαθμό ανάπτυξης της τεχνολογίας και την ένταση του βαθμού αυτοματοποίησης όλων των καθημερινών διεργασιών, ο Κανονισμός εισήγαγε δύο πολύ καινοτόμες έννοιες. Ειδικότερα, στο άρθρο 25 του Κανονισμού εντοπίζουμε την έννοια της προστασίας των δεδομένων από τον σχεδιασμό, το λεγόμενο «privacy by design» και την έννοια της προστασίας των δεδομένων εξ ορισμού, άλλως γνωστό ως «privacy by default».

Όσον αφορά την προστασία δεδομένων από τον σχεδιασμό (privacy by design), ο Κανονισμός εναποθέτει την ευθύνη στον υπεύθυνο επεξεργασίας να εφαρμόσει

[17] Βλ. περίπτωση 1 δ) του αρ. 44 του Ν. Ν. 4624/2019
[18] Βλ. αιτιολογ. Σκέψη 39 του ΓΚΠΔ

ήδη από την στιγμή του καθορισμού των μέσων επεξεργασίας αλλά και κατά την στιγμή της ίδιας της επεξεργασίας των προσωπικών δεδομένων, έναν συνδυασμό τεχνικών και οργανωτικών μέτρων, κατάλληλα επιλεγμένων ανάλογα με τον εκάστοτε σκοπό επεξεργασίας, τα οποία θα έχουν σχεδιαστεί για την «*εφαρμογή των αρχών προστασίας των δεδομένων*», όπως αυτές ορίζονται στο άρθρο 5 του Κανονισμού και την «*ενσωμάτωση των απαραίτητων εγγυήσεων στην επεξεργασία*» προκειμένου να πληρούνται οι απαιτήσεις του Κανονισμού [40][19].

Σύμφωνα με τον Κανονισμό, προκειμένου να εφαρμοστούν τα κατάλληλα μέτρα για τη διασφάλιση της τήρησης των απαιτήσεων του, ο υπεύθυνος επεξεργασίας θα πρέπει να λαμβάνει υπ' όψιν του μία πληθώρα παραγόντων. Ειδικότερα, θα πρέπει κάθε φορά να εξετάζει και να συνεκτιμά τις εξελίξεις της τεχνολογίας, το κόστος εφαρμογής των επιβαλλόμενων μέτρων, τη φύση και το πεδίο εφαρμογής των μέτρων, το πλαίσιο και τους σκοπούς επεξεργασίας, καθώς και τους κινδύνους που ελλοχεύουν για τα δικαιώματα και τις ελευθερίες των υποκειμένων από την σκοπούμενη επεξεργασία.

Ως προς τα τεχνικά και οργανωτικά μέτρα που θα πρέπει να λαμβάνει ο υπεύθυνος, αυτά θα πρέπει να διακρίνονται από τεχνολογίες και εφαρμογές που ενισχύουν την ιδιωτικότητα. Τέτοιου είδους μέτρα θα μπορούσαν να είναι η ελαχιστοποίηση της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, η χρήση τεχνικών ψευδωνυμοποίησης των δεδομένων[20], η κρυπτογράφηση των δεδομένων και η ύπαρξη διαφάνειας αναφορικά με την επεξεργασία και τη ροή των προσωπικών δεδομένων, προκειμένου το υποκείμενο των δεδομένων να μπορεί να παρακολουθεί τα στάδια της επεξεργασίας [40][21].

Από την αιτιολ. σκέψη 78 του Κανονισμού απορρέει η επιθυμία εφαρμογής της προστασίας των προσωπικών δεδομένων εκ του σχεδιασμού ήδη από τους παραγωγούς των διαφόρων προϊόντων, υπηρεσιών και εφαρμογών προκειμένου να διευκολύνεται το έργο των υπευθύνων και εκτελούντων την επεξεργασία και να επιτυγχάνεται η επιτυχής προστασία των δεδομένων προσωπικού χαρακτήρα. Αυτό σημαίνει ότι η ιδέα της προστασίας των προσωπικών δεδομένων θα πρέπει να «εισάγεται» από το πρώιμο στάδιο της επιλογής, του σχεδιασμού και της ανάπτυξης μιας εφαρμογής ή υπηρεσίας προκειμένου να εξασφαλιστεί η νομιμότητα λειτουργίας της εφαρμογής ή της υπηρεσίας που επεξεργάζεται προσωπικά δεδομένα με τον Κανονισμό.

Όσον αφορά δε την προστασία δεδομένων εξ' ορισμού (privacy by default), ο

---

[19] Βλ. άρθρο 25 παρ. 1 του ΓΚΠΔ

[20] Σύμφωνα με το άρθρο 4 περ. 5 του ΓΚΠΔ ως ψευδωνυμοποίηση ορίζεται «η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο». Στις τεχνικές ψευδωνυμοποίησης περιλαμβάνονται το data masking, το tokenization, το blurring κλπ.

[21] Βλ. αιτιολ. σκέψη 78 του ΓΚΠΔ

Κανονισμός προβλέπει ότι ο υπεύθυνος επεξεργασίας θα πρέπει να εφαρμόζει τα «*κατάλληλα τεχνικά και οργανωτικά μέτρα*» προκειμένου να διασφαλίζει ότι επεξεργάζονται εξ' ορισμού μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι απολύτως αναγκαία για τον εκάστοτε σκοπό της επεξεργασίας. Αυτή η υποχρέωση, σύμφωνα με τον Κανονισμό, περιλαμβάνει το εύρος των προσωπικών δεδομένων που συλλέγονται, τον βαθμό της επεξεργασίας τους, τη διάρκεια αποθήκευσης τους και το βαθμό προσβασιμότητάς τους, έτσι ώστε να μην είναι δυνατή η πρόσβαση σε αυτά εξ ορισμού από αόριστο αριθμό προσώπων.

7.3. Ζητήματα εφαρμογής και περιορισμοί του ΓΚΠΔ στις έξυπνες πόλεις

7.3.1. Εμπλεκόμενα μέρη και κατανομή ευθύνης

Μολονότι οι ως άνω αναφερθείσες έννοιες και προβλέψεις του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ) είναι κοινώς γνωστές και αποδεκτές, ένα από τα ζητήματα που δημιουργείται στο πλαίσιο της έξυπνης πόλης, είναι ποιος είναι υπεύθυνος να τις εφαρμόσει και γενικότερα να θέσει το γενικό πλαίσιο όσον αφορά την επεξεργασία των προσωπικών δεδομένων των πολιτών, που ως είδαμε αποτελούν ακρογωνιαίο λίθο στη λειτουργία της έξυπνης πόλης. Τα μέρη που εμπλέκονται είναι πολλά και με διαφορετικούς σκοπούς και στόχους το κάθε ένα. Από τους παραγωγούς των έξυπνων λύσεων και εφαρμογών του Διαδικτύου των Πραγμάτων στις δημόσιες αρχές που μεταχειρίζονται τα δεδομένα και τους ίδιους τους πολίτες που τα παρέχουν, οι απόψεις διίστανται ως προς τον σωστό τρόπο συλλογής και επεξεργασίας των προσωπικών δεδομένων και το βαθμό ευθύνης καθενός από αυτά. Καθίσταται κρίσιμο δε να γίνεται ξεκάθαρο κάθε φορά ποιος είναι ο υπεύθυνος και ποιος ο εκτελών την επεξεργασία, έννοιες που εισάγονται στο άρθρο 4 του ΓΚΠΔ.

Ειδικότερα, σύμφωνα με τον ΓΚΠΔ ως υπεύθυνος επεξεργασίας ορίζεται «*το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα*»[22] και ως εκτελών την επεξεργασία «*το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας*» [40][23]. Τα λοιπά δε εμπλεκόμενα μέρη σύμφωνα με τον Κανονισμό είναι ο αποδέκτης, ήτοι «*το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας, στα οποία κοινολογούνται τα δεδομένα προσωπικού χαρακτήρα, είτε πρόκειται για τρίτον είτε όχι. Ωστόσο, οι δημόσιες αρχές που ενδέχεται να λάβουν δεδομένα προσωπικού χαρακτήρα στο πλαίσιο συγκεκριμένης έρευνας σύμφωνα με το δίκαιο*

[22] Βλ. άρθρο 4 στοιχ. 7 του ΓΚΠΔ
[23] Βλ. άρθρο 4 στοιχ. 8 του ΓΚΠΔ

της Ένωσης ή κράτους μέλους δεν θεωρούνται ως αποδέκτες»[24] και ο τρίτος, ο οποίος ορίζεται ως «*οποιοδήποτε φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία ή φορέας, με εξαίρεση το υποκείμενο των δεδομένων, τον υπεύθυνο επεξεργασίας, τον εκτελούντα την επεξεργασία και τα πρόσωπα τα οποία, υπό την άμεση εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα*»[40][25].

Τα ως άνω πρόσωπα είναι υπεύθυνα για την εφαρμογή των διατάξεων του ΓΚΠΔ και την τήρηση ορισμένων αρχών. Εν προκειμένω, ο υπεύθυνος επεξεργασίας οφείλει να τηρεί την αρχή της λογοδοσίας σύμφωνα με την οποία πρέπει να αιτιολογεί τις αποφάσεις που λαμβάνει σχετικά με την επεξεργασία των προσωπικών δεδομένων και να είναι σε θέση κάθε φορά να αποδείξει ότι συμμορφώνεται με τις διατάξεις και τις αρχές του Κανονισμού [40][26]. Ειδικότερα, ο υπεύθυνος επεξεργασίας είναι το πρόσωπο που θα εξετάσει ποια δεδομένα είναι αναγκαίο να συλλεχθούν και να επεξεργαστούν, τον τρόπο επεξεργασία τους, τους κινδύνους που ενδέχεται να ενέχει η επεξεργασία αυτή και τη λήψη των κατάλληλων τεχνικών και οργανωτικών μέτρων κατόπιν στάθμισης των συμφερόντων του υποκειμένου των δεδομένων και των συμφερόντων της υπηρεσίας του. Τα εν λόγω δε μέτρα πρέπει να τα επανεξετάζει και να τα επικαιροποιεί κάθε φορά που αλλάζουν τα δεδομένα και ο σκοπός της επεξεργασίας [40][27].

Ευθύνη ως προς την τήρηση των διατάξεων του Κανονισμού έχει και ο εκτελών την επεξεργασία, ο οποίος επεξεργάζεται τα δεδομένα σύμφωνα με τις εντολές που του έχει δώσει ο υπεύθυνος επεξεργασίας. Ειδικότερα, ο εκτελών την επεξεργασία οφείλει να τηρεί αρχεία των δραστηριοτήτων επεξεργασίας[28], να λαμβάνει τα κατάλληλα μέτρα προκειμένου να διασφαλίζεται η ασφάλεια της επεξεργασίας των δεδομένων[29] , να γνωστοποιεί αμελλητί στον υπεύθυνο επεξεργασίας την ύπαρξη παραβίασης των προσωπικών δεδομένων[30] και εν γένει να συμμορφώνεται με τις οδηγίες του υπεύθυνου επεξεργασίας.

Τέλος, στον Κανονισμό προβλέπεται ότι μπορεί να υπάρχουν περισσότεροι του ενός υπεύθυνοι επεξεργασίας, οι οποίοι καθορίζουν από κοινού τους σκοπούς και τα μέσα της επεξεργασίας και αποτελούν από κοινού υπεύθυνους επεξεργασίας[31]. Στα πλαίσια της λειτουργίας της έξυπνης πόλης είναι συχνά δυσδιάκριτα τα όρια και ποιο αποτελεί από τα εμπλεκόμενα μέρη τον υπεύθυνο επεξεργασίας, τον εκτελούντα την επεξεργασία ή πότε έχουμε από κοινού υπεύθυνους επεξεργασίας.

Συνεπώς, δημιουργούνται προβλήματα ως προς την εφαρμογή των διατάξεων

---

[24] Βλ. άρθρο 4 στοιχ. 9 του ΓΚΠΔ
[25] Βλ. άρθρο 4 στοιχ. 10 του ΓΚΠΔ
[26] Βλ. άρθρο 5 παραγρ. 2 του ΓΚΠΔ
[27] Βλ. άρθρο 24 του ΓΚΠΔ
[28] Βλ. άρθρο 30 του ΓΚΠΔ
[29] Βλ. άρθρο 32 του ΓΚΠΔ
[30] Βλ. άρθρο 33 του ΓΚΠΔ
[31] Βλ. άρθρο 26 του ΓΚΠΔ

του ΓΚΠΔ διότι δεν καθίσταται σαφές ποιο είναι το πρόσωπο ή ο φορέας που έχει την ευθύνη, ποιος είναι αρμόδιος να αποδείξει την συμμόρφωση με τον Κανονισμό και σε ποιον θα μπορεί να στραφεί το υποκείμενο των δεδομένων για πληροφορίες σχετικά με την επεξεργασία των προσωπικών δεδομένων του. Συνήθως, στις έξυπνες πόλεις τον ρόλο του εκτελούντος την επεξεργασία τον έχουν οι εταιρείες παροχής τεχνολογικών λύσεων (εφαρμογών, συσκευών, λογισμικών κλπ), οι οποίες παρέχουν έξυπνες λύσεις κατ' εντολήν του υπευθύνου επεξεργασίας και επεξεργάζονται τα προσωπικά δεδομένα των πολιτών σύμφωνα με τις οδηγίες του. Διευκρινίζεται, ωστόσο, ότι αυτές οι εταιρείες δεν υπάγονται πάντοτε στις διατάξεις του ΓΚΠΔ, καθώς πολλές φορές δεν καταχωρούνται ως εκτελούντες την επεξεργασία ή αναλαμβάνουν μόνο την παροχή των έξυπνων προϊόντων (π.χ. αισθητήρων) και δεν εμπλέκονται στην συλλογή και επεξεργασία των προσωπικών δεδομένων. Σε κάθε περίπτωση, δεν θα πρέπει να παραβλέπεται η ανάγκη ελέγχου από τους φορείς της έξυπνης πόλης και υπεύθυνους επεξεργασίας των εταιρειών αυτών, καθώς το μονοπώλιο που έχουν στην αγορά των έξυπνων λύσεων σε συνδυασμό με την αυξημένη οικονομική τους ισχύ, τους καθιστά σε πλεονεκτική σχέση σε συνάρτηση με τους φορείς της δημόσιας εξουσίας κάτι το οποίο πολλές φορές προσπαθούν να το εκμεταλλευτούν, επιβάλλοντας τους δικούς τους κανόνες στην επεξεργασία των δεδομένων [54].

Κατόπιν των ανωτέρω, καθίσταται σαφές ότι εάν βρίσκονται σε μειονεκτική θέση οι φορείς την έξυπνης πόλης σε ακόμη μειονεκτικότερη θέση βρίσκονται οι πολίτες της, που αποτελούν εν προκειμένων τα υποκείμενα των δεδομένων. Μολονότι οι πολίτες πρέπει να ενημερώνονται επαρκώς και σαφώς για τα δεδομένα τους που κάθε φορά συλλέγονται και επεξεργάζονται, προκειμένου να έχουν τον έλεγχο επί αυτών, είθισται, ακόμη και όταν υπάρχει η απαιτούμενη πληροφόρηση, να μην ασκούν τα δικαιώματά που τους παρέχει ο ΓΚΠΔ διότι έχει γεννηθεί η πεποίθηση ότι δεν πρόκειται να ικανοποιηθούν. Το φαινόμενο αυτό είναι γνωστό σήμερα ως παραίτηση από την ιδιωτικότητα (privacy designation). Προκειμένου, ωστόσο, να λειτουργήσει το μοντέλο της έξυπνης πόλης, πρέπει να δοθεί βάσει στον πολίτη, ο οποίος αποτελεί και το πρωταρχικό στοιχείο της και να καταστεί βέβαιη η δυνατότητα άσκησης των δικαιωμάτων του. Ειδικότερα, ο ΓΚΠΔ προβλέπει τα εξής δικαιώματα για τα υποκείμενα των δεδομένων, ήτοι το δικαίωμα σε διαφανή ενημέρωση[32], το δικαίωμα πρόσβασης στα προσωπικά του δεδομένα[33], το δικαίωμα πρόσβασης του υποκειμένου των δεδομένων[34], το δικαίωμα διόρθωσης[35], το δικαίωμα διαγραφής («το δικαίωμα στη λήθη»)[36], το δικαίωμα περιορισμού της

[32] Βλ. άρθρο 12 του ΓΚΠΔ
[33] Βλ. άρθρο 13 του ΓΚΠΔ
[34] Βλ. άρθρο 15 του ΓΚΠΔ
[35] Βλ. άρθρο 16 του ΓΚΠΔ
[36] Βλ. άρθρο 17 του ΓΚΠΔ

επεξεργασίας[37], το δικαίωμα στη φορητότητα των δεδομένων[38] και το δικαίωμα εναντίωσης.[39] Υποχρέωση των φορέων, λοιπόν, της έξυπνης πόλης είναι να γνωστοποιήσουν στα υποκείμενα των δεδομένων τα κατοχυρωμένα δικαιώματα τους και να προβούν σε κάθε απαιτούμενη ενέργεια για την προώθηση και διευκόλυνση της άσκησής τους.

7.3.2. Αυτοματοποιημένη λήψη αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ

Ένα από τα δικαιώματα του υποκειμένου των δεδομένων είναι το δικαίωμα στη μη αυτοματοποιημένη ατομική λήψη αποφάσεων. Ειδικότερα, στο άρθρο 22 παρ. 1 του Κανονισμού προβλέπεται ρητά ότι «*το υποκείμενο των δεδομένων έχει το δικαίωμα να μην υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης προφίλ, η οποία παράγει έννομα αποτελέσματα που το αφορούν ή το επηρεάζει σημαντικά με παρόμοιο τρόπο*». Ως κατάρτιση προφίλ δε νοείται σύμφωνα με την αιτιολογική σκέψη 71 του Κανονισμού «*οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση προσωπικών πτυχών σχετικά με ένα φυσικό πρόσωπο, ιδίως την ανάλυση ή την πρόβλεψη πτυχών που αφορούν τις επιδόσεις στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις ή συμφέροντα, την αξιοπιστία ή τη συμπεριφορά, τη θέση ή κινήσεις του υποκειμένου των δεδομένων, στον βαθμό που παράγει νομικά αποτελέσματα έναντι του προσώπου αυτού ή το επηρεάζει σημαντικά κατά ανάλογο τρόπο*». Υπεύθυνος προκειμένου να καταστεί δυνατή η άσκηση του ως άνω δικαιώματος δεν είναι άλλος από τον υπεύθυνο επεξεργασίας, ο οποίος σύμφωνα με την παράγραφο 3 του ίδιου ως άνω άρθρου «*εφαρμόζει κατάλληλα μέτρα για την προστασία των δικαιωμάτων, των ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων, τουλάχιστον του δικαιώματος εξασφάλισης ανθρώπινης παρέμβασης από την πλευρά του υπευθύνου επεξεργασίας, έκφρασης άποψης και αμφισβήτησης της απόφασης*»[40].

Επιπλέον, σύμφωνα με την αιτιολογική σκέψη 67 του Κανονισμού, όταν η αρχειοθέτηση των προσωπικών δεδομένων γίνεται με αυτοματοποιημένο τρόπο, ο υπεύθυνος επεξεργασίας θα πρέπει να διασφαλίζει, σε πρώτο βαθμό, με τεχνικά μέσα τον περιορισμό της επεξεργασίας των δεδομένων έτσι ώστε τα προσωπικά δεδομένα να μην τύχουν περαιτέρω επεξεργασίας και να μην μπορούν να πραγματοποιηθούν αλλαγές ή αλλοιώσεις σε αυτά. Το δε υποκείμενο των δεδομένων θα πρέπει να μπορεί να λαμβάνει από τον υπεύθυνο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που έχει παράσχει σε αυτόν και που έχουν επεξεργαστεί με

---

[37] Βλ. άρθρο 18 του ΓΚΠΔ
[38] Βλ. άρθρο 20 του ΓΚΠΔ
[39] Βλ. άρθρο 21 του ΓΚΠΔ
[40] Βλ. άρθρο 22 παρ. 1 και 3 του ΓΚΠΔ

αυτοματοποιημένα μέσα.[41] Σε κάθε περίπτωση τα προσωπικά δεδομένα δεν πρέπει να επεξεργάζονται για σκοπούς εμπορικής προώθησης και τα υποκείμενα των δεδομένων θα πρέπει να έχουν τη δυνατότητα να αντιταχθούν στην επεξεργασία αυτή, συμπεριλαμβανομένης της κατάρτισης προφίλ που μπορεί να συνδέεται με αυτή είτε πρόκειται για αρχική είτε για περαιτέρω επεξεργασία των δεδομένων. Ο υπεύθυνος επεξεργασίας θα πρέπει να ενημερώνει το υποκείμενο των δεδομένων για το ως άνω δικαίωμά του και η ενημέρωση αυτή να είναι σαφής, ρητή και ξεχωριστή από οποιαδήποτε άλλη πληροφορία που θα παράσχει στο υποκείμενο των δεδομένων [40][42].

Περαιτέρω, από την αιτιολογική σκέψη 71 του ΓΚΠΔ γίνεται σαφής η επιταγή να προστατεύονται τα υποκείμενα των δεδομένων από τη λήψη αυτοματοποιημένων αποφάσεων, οι οποίες έχουν παρθεί κατόπιν αξιολόγησης προσωπικών πτυχών που τα αφορούν και απορρέουν από την πραγματοποίηση αυτοματοποιημένης επεξεργασίας. Η ως άνω απόφαση δε έχει ως επακόλουθο την παραγωγή εννόμων αποτελεσμάτων για τα υποκείμενα των δεδομένων ή τον επηρεασμό της καθημερινότητάς τους με οποιοδήποτε τρόπο. Όταν δε ο Κανονισμός αναφέρεται σε αυτοματοποιημένη επεξεργασία, εννοεί την επεξεργασία και συνακόλουθα την απόφαση που λαμβάνεται χωρίς ανθρώπινη παρέμβαση. Η ως άνω αιτιολογική σκέψη προβλέπει ρητά ότι προκειμένου να διασφαλιστούν τα δικαιώματα του υποκειμένου των δεδομένων και να προστατευθούν τα δεδομένα του, ο υπεύθυνος θα πρέπει «*να χρησιμοποιεί κατάλληλες μαθηματικές ή στατιστικές διαδικασίες για την κατάρτιση του προφίλ, να εφαρμόζει τεχνικά και οργανωτικά μέτρα, ώστε να διορθώνονται οι παράγοντες που οδηγούν σε ανακρίβειες σε δεδομένα προσωπικού χαρακτήρα και να ελαχιστοποιείται ο κίνδυνος σφαλμάτων, να καθιστά ασφαλή τα δεδομένα προσωπικού χαρακτήρα κατά τρόπο που να λαμβάνει υπόψη τους πιθανούς κινδύνους που συνδέονται με τα συμφέροντα και τα δικαιώματα του υποκειμένου των δεδομένων και κατά τρόπο που να προλαμβάνει, μεταξύ άλλων, τα αποτελέσματα διακρίσεων σε βάρος φυσικών προσώπων βάσει της φυλετικής ή εθνοτικής καταγωγής, των πολιτικών φρονημάτων, της θρησκείας ή των πεποιθήσεων, της συμμετοχής σε συνδικαλιστικές οργανώσεις, της γενετικής κατάστασης ή της κατάστασης της υγείας ή του γενετήσιου προσανατολισμού, ή μέτρων ισοδύναμου αποτελέσματος.*»[40].

Εκ των ανωτέρω συνάγεται ότι όσο η τεχνολογία εξελίσσεται και τα όρια αναφορικά με την συλλογή και επεξεργασία των δεδομένων γίνονται πιο δυσδιάκριτα, τόσο μεγαλύτερη είναι η ανάγκη και υποχρέωση ενημέρωσης του υποκειμένου των δεδομένων, με τον πιο εύληπτο δυνατό τρόπο, σχετικά με τις πράξεις που διενεργούνται, προκειμένου να καταφέρει (το υποκείμενο των δεδομένων) να ασκήσει τα δικαιώματα του. Στην περίπτωση δε αυτή, η υποχρέωση του υπεύθυνου επεξεργασίας να τηρεί την αρχή της λογοδοσίας μεταμορφώνεται σε μια ειδικότερη υποχρέωση, αυτής της αλγοριθμικής λογοδοσίας, δυνάμει της οποίας θα πρέπει να δίνει όλες τις απαιτούμενες πληροφορίες στα υποκείμενα των δεδομένων προκειμένου να έχουν πλήρη επίγνωση και κατανόηση κάθε φορά που δίνουν ή

[41] Βλ. αιτιολογική σκέψη 68 του ΓΚΠΔ

[42] Βλ. αιτιολογική σκέψη 70 του ΓΚΠΔ

όχι την συναίνεση τους [64].

7.4. Τρόποι συμμόρφωσης των έξυπνων πόλεων με τον ΓΚΠΔ

Στο ίδιο το κείμενο του Κανονισμού εντοπίζουμε τους τρόπους με τους οποίους μπορούμε να ξεπεράσουμε τα προβλήματα εφαρμογής του στο πλαίσιο της έξυπνης πόλης. Αυτό που πρέπει να κάνουν τα μέρη της έξυπνης πόλης είναι να εξοικειωθούν με τις διατάξεις του Κανονισμού και να καταστρώσουν τις κατάλληλες στρατηγικές προκειμένου να συμμορφωθούν με αυτόν. Κατωτέρω εξετάζονται μερικοί τρόποι με τους οποίους οι έξυπνες πόλεις μπορούν να επιτύχουν την συμμόρφωση με τον ΓΚΠΔ και συνακόλουθα την προστασία των προσωπικών δεδομένων των κατοίκων τους.

7.4.1. Η συναίνεση του υποκειμένου των δεδομένων

Ένας τρόπος με τον οποίο θα μπορούσε να διασφαλιστεί η συμμόρφωση ως ένα βαθμό της λειτουργίας μιας έξυπνης πόλης με τον ΓΚΠΔ, είναι μέσω της χορήγησης συγκατάθεσης από τα υποκείμενα των δεδομένων, ήτοι τους πολίτες της. Όπως έχει αναφερθεί και ανωτέρω, στο επίκεντρο της έξυπνης πόλης βρίσκεται ο πολίτης, ο οποίος βοηθάει στη λειτουργία και στην ανάπτυξή της μέσω των δεδομένων που παρέχει.

Στο άρθρο 6 παρ. 1 του Κανονισμού τίθεται ως πρώτη προϋπόθεση νομιμότητας (νομική βάση) της συλλογής και επεξεργασίας προσωπικών δεδομένων με τον ΓΚΠΔ η συγκατάθεση του υποκειμένου των δεδομένων στην επεξεργασία των προσωπικών δεδομένων του για έναν ή περισσότερους συγκεκριμένους σκοπούς[43]. Στο άρθρο 4 δε ως συγκατάθεση ορίζεται «*κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν*»[44]. Από τις αιτιολογικές σκέψεις του Κανονισμού συνάγεται ότι η «*δήλωση ή σαφής θετική ενέργεια*» μπορούν να δοθούν από το υποκείμενο των δεδομένων είτε με γραπτή δήλωση, η οποία μπορεί να γίνει με χρήση ηλεκτρονικών μέσων είτε με προφορική δήλωση. Η γραπτή δήλωση – σαφής θετική ενέργεια θα μπορούσε να περιλαμβάνει την συμπλήρωση ενός τετραγωνιδίου, την επιλογή των επιθυμητών τεχνικών ρυθμίσεων ή με οποιονδήποτε άλλο τρόπο τη ρητή δήλωση ότι το υποκείμενο αποδέχεται την συλλογή και επεξεργασία των δεδομένων του. Εκ των ανωτέρω συνάγεται ότι η σιωπή ή η εξακολούθηση χρήσης της εφαρμογής / ιστοσελίδας δεν μπορεί να νοηθεί ως συγκατάθεση του υποκειμένου. Επίσης, η συγκατάθεση θα πρέπει να δίνεται για έναν ή περισσότερους συγκεκριμένους σκοπούς

[43] Βλ. άρθρο 6 παρ. 1 στοιχ. α) του ΓΚΠΔ
[44] Βλ. άρθρο 4 στοιχ. 11 του ΓΚΠΔ

επεξεργασίας και όχι για ένα μη ορισμένο σύνολο δραστηριοτήτων που εκφεύγουν των ορίων του ορισθέντος σκοπού [40][45].

Η συλλογή των δεδομένων στις έξυπνες πόλεις γίνεται μέσω έξυπνων συσκευών και εφαρμογών του Διαδικτύου των Πραγμάτων. Για την συλλογή δε των δεδομένων για τους σκοπούς της έξυπνης πόλης, απαιτείται πληθώρα έξυπνων συσκευών, οι οποίες συλλέγουν και επεξεργάζονται πληθώρα πληροφοριών και προσωπικών δεδομένων των πολιτών – χρηστών. Γίνεται αντιληπτό ότι πολλές φορές τα δεδομένα αυτά συλλέγονται και επεξεργάζονται χωρίς καν οι ίδιοι οι χρήστες να έχουν γνώση επ' αυτών ή να έχουν γνώση ποιος είναι ο σκοπός της επεξεργασίας τους. Είναι σημαντικό και σκόπιμο, λοιπόν, προκειμένου οι εν λόγω πράξεις επεξεργασίας να είναι σύννομες με τον Κανονισμό να διασφαλίζεται η εν πλήρη επιγνώσει συγκατάθεση των πολιτών – χρηστών. Προκειμένου να επιτευχθεί η ως άνω συγκατάθεση θα πρέπει να βρεθούν τρόποι με τους οποίους θα ενημερώνεται το υποκείμενο με απλό και περιεκτικό τρόπο, ώστε να γίνονται εύκολα αντιληπτοί οι σκοποί της επεξεργασίας, η κίνηση των δεδομένων του και τα ρίσκα που ενέχει η παροχή συναίνεσης στην συλλογή και επεξεργασία τους. Συνεπώς, οι όροι συλλογής και επεξεργασίας θα πρέπει να είναι σε απλή γλώσσα, σαφείς, περιεκτικοί, εύκολα προσβάσιμοι και μη προδιατυπωμένοι, με την έννοια ότι θα πρέπει να παρέχεται στους χρήστες η δυνατότητα διαμόρφωσής τους μέσω αυτοματοποιημένων διαπραγματευτικών τεχνικών. Μέσα για την επίτευξη της αληθούς και ρητής συγκατάθεσης είναι μεταξύ άλλων η δημιουργία όρων και προϋποθέσεων επεξεργασίας με τα ως άνω χαρακτηριστικά, οι ενημερώσεις σχετικά με τη χρήση cookies και επιλογής του είδους αυτών και οι πολιτικές απορρήτου των δεδομένων. Ειδικά στο έξυπνο δίκτυο της έξυπνης πόλης ο χρήστης θα πρέπει να λαμβάνει γνώση πότε διασυνδέονται οι συσκευές και μεταβιβάζονται τα δεδομένα του, καθώς επίσης για ποιο λόγο συλλέγονται και πως χρησιμοποιούνται. Για όλα τα ανωτέρω το πιο σημαντικό είναι ο χρήστης να ενημερώνεται επαρκώς και να παρέχει τη ρητή εν επιγνώσει συναίνεσή του [65].

7.4.2. Η ανάγκη διενέργειας εκτίμησης αντικτύπου (DPIA) για την προστασία των προσωπικών δεδομένων

Ο Κανονισμός προκειμένου να διασφαλίσει το επιθυμητό επίπεδο προστασίας των προσωπικών δεδομένων, εισάγει στο άρθρο 35, ως πρόσθετη υποχρέωση προς τον υπεύθυνο επεξεργασίας, τη διενέργεια εκτίμησης αντικτύπου, άλλως γνωστή ως Data Protection Impact Assessment (DPIA). Η υποχρέωση αυτή συνδέεται στενά με την αρχή της λογοδοσίας, που επιβάλλει ο Κανονισμός, ήτοι την υποχρέωση του υπεύθυνου επεξεργασίας να μπορεί να αποδεικνύει την συμμόρφωσή του με τις αρχές επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που περιγράφονται στον Κανονισμό. Προκειμένου δε να αποδείξει την συμμόρφωση του με τον Κανονισμό ο υπεύθυνος επεξεργασίας θα πρέπει να λαμβάνει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την αντιμετώπιση των πιθανών κινδύνων. Ανάγκη διενέργειας, λοιπόν, της ως άνω εκτίμησης αντικτύπου υφίσταται όταν μία

[45] Βλ. αιτιολ. Σκέψη 32 του ΓΚΠΔ

πράξη επεξεργασίας - ιδίως όταν αυτή γίνεται με χρήση νέων τεχνολογιών - ενδέχεται να έχει ως απόρροια τη δημιουργία υψηλού κινδύνου για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Θα πρέπει, λοιπόν, ο υπεύθυνος επεξεργασίας να αξιολογήσει και να συνεκτιμήσει ένα σύμπλεγμα παραγόντων, όπως η φύση, το πεδίο εφαρμογής, το πλαίσιο, τους σκοπούς της επεξεργασίας, την σοβαρότητα και την πιθανότητα επέλευσης του κινδύνου. Η εκτίμηση αντικτύπου θα πρέπει να διενεργείται πριν από την σκοπούμενη πράξη επεξεργασίας και τα αποτελέσματά της να λαμβάνονται υπόψιν κατά τον καθορισμό των μέτρων που θα πρέπει να ληφθούν προκειμένου η επεξεργασία των προσωπικών δεδομένων να είναι σύννομη με τον Κανονισμό. Περαιτέρω, η εκτίμηση αντικτύπου θα πρέπει να περιλαμβάνει πέρα από τα προβλεπόμενα μέτρα, τις εγγυήσεις αλλά και τους τρόπους με τους οποίους θα μετριαστεί ο κίνδυνος και θα εξασφαλισθεί η προστασία των προσωπικών δεδομένων .

Σύμφωνα με το άρθρο 35 παρ. 3 του Κανονισμού η εκτίμηση αντικτύπου για την προστασία των προσωπικών δεδομένων θα πρέπει να διενεργείται κυρίως στην περίπτωση μεγάλης κλίμακας και συστηματικής επεξεργασίας προσωπικών δεδομένων, η οποία μπορεί να επηρεάσει αρνητικά μεγάλο αριθμό φυσικών προσώπων (π.χ. λόγω του ευαίσθητου χαρακτήρα των δεδομένων) και ειδικά όταν η επεξεργασία γίνεται με αυτοματοποιημένο τρόπο και λαμβάνει χώρα σε περιφερειακό, εθνικό ή υπερεθνικό επίπεδο. Στην περίπτωση αυτή, ο κίνδυνος για το υποκείμενο των δεδομένων όχι μόνο είναι υψηλός αλλά έχει και ως αποτέλεσμα την αδυναμία του υποκειμένου να ασκήσει τα δικαιώματα του και να διατηρήσει τις συνταγματικά κατοχυρωμένες ελευθερίες του. Ακόμη, εκτίμηση αντικτύπου απαιτείται όταν η πράξη της επεξεργασίας αφορά την συστηματική παρακολούθηση δημόσια προσβάσιμων χώρων σε μεγάλη κλίμακα και ιδίως όταν χρησιμοποιούνται οπτικοακουστικές συσκευές για την επιτήρηση του χώρου, στερώντας με αυτό τον τρόπο από τα φυσικά πρόσωπα τη δυνατότητα άσκησης των ελευθεριών και δικαιωμάτων τους.

Σημειώνεται, επιπλέον, ότι σε μία εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα είναι δυνατό να εξετάζονται περισσότερες της μίας πράξεις επεξεργασίας, οι οποίες διακρίνονται από μια συνάφεια και ελλοχεύουν παρόμοιους υψηλούς κινδύνους. Τέτοια περίπτωση θα μπορούσε να είναι η εγκαθίδρυση από ένα δημόσιο φορέα μιας κοινής πλατφόρμας ή εφαρμογής για μια δραστηριότητα, η οποία σκοπείται να εφαρμοσθεί και χρησιμοποιηθεί ευρέως .

Κατόπιν των ανωτέρω, γίνεται σαφές ότι στο πλαίσιο μιας έξυπνης πόλης, όπου προκειμένου να λειτουργήσουν οι υπηρεσίες της γίνεται χρήση νέων τεχνολογιών και η επεξεργασία των δεδομένων είναι ευρεία και περίπλοκη, καθίσταται αναγκαίο οι εκάστοτε υπεύθυνοι επεξεργασίας να προβαίνουν στη διενέργεια εκτίμησης αντικτύπου προκειμένου να αξιολογούν κάθε φορά τους πιθανούς κινδύνους προτού προβούν στην συλλογή και επεξεργασία των προσωπικών δεδομένων των πολιτών. Τεχνολογίες όπως οι εφαρμογές του Διαδικτύου των Πραγμάτων, που αποτελούν θεμελιώδες στοιχείο για την εύρυθμη λειτουργία της έξυπνης πόλης,

υποκρύπτουν πολλούς πιθανούς κινδύνους για τα δεδομένα των πολιτών και καθιστούν αναγκαία τη διενέργεια εκτίμησης αντικτύπου προκειμένου να βρεθούν οι κατάλληλοι τρόποι για τον αποτελεσματικό μετριασμό των κινδύνων [66].

Ωστόσο, η διενέργεια εκτίμησης αντικτύπου για τις υπηρεσίες της έξυπνης πόλης δεν είναι ένα εύκολο εγχείρημα αλλά, αντιθέτως, συνεπάγεται πληθώρα προκλήσεων για τους εκάστοτε υπεύθυνους επεξεργασίας, οι οποίες έχουν σχέση με το ίδιο το σύστημα της έξυπνης πόλης. Ως υπηρεσίες, δε, της έξυπνης πόλης μπορούμε να ορίσουμε γενικά τις υπηρεσίες που δίνουν λύση σε ένα κοινωνικό ζήτημα με τεχνολογικό τρόπο, ο οποίος αλληλοεπιδρά με το φυσικό περιβάλλον της έξυπνης πόλης και στην οποία έξυπνη υπηρεσία συμμετέχουν τόσο δημόσιοι όσο και ιδιωτικοί φορείς [67]. Όσον αφορά τις δυσκολίες που εμφανίζονται κατά τη διενέργεια εκτίμησης αντικτύπου σε μια έξυπνη πόλη μπορούμε να διακρίνουμε την συσχέτισή τους:
(α) με την ανάγκη στάθμισης των δικαιωμάτων των πολιτών και του σκοπού του υπεύθυνου επεξεργασίας, δεδομένου ότι από μια εφαρμογή της έξυπνης πόλης δεν διακινδυνεύεται μόνο το δικαίωμα στην προστασία των προσωπικών δεδομένων των πολιτών αλλά και άλλα θεμελιώδη δικαιώματα αυτών, όπως το δικαίωμα στην ελεύθερη ανάπτυξη της προσωπικότητας, το δικαίωμα στη χρηστή διοίκηση και άλλα δικαιώματα τα οποία πρέπει να ληφθούν υπόψιν κατά τη διενέργεια της εκτίμησης αντικτύπου,
(β) με τη δυσκολία εκτίμησης των πιθανών κινδύνων και των επιπτώσεων στα προσωπικά δεδομένα των πολιτών, δεδομένου ότι οι εφαρμογές της έξυπνης πόλης πολλές φορές αλληλοεπιδρούν και αλληλεπικαλύπτονται με αποτέλεσμα να καθίσταται δύσκολη η διερεύνηση και αποτύπωση όλων των πιθανών κινδύνων,
(γ) με την έλλειψη διαφάνειας και δυνατότητας συμμετοχής των πολιτών στον σχεδιασμό και στην ανάπτυξη των εφαρμογών της έξυπνης πόλης προκειμένου να μπορούν να προτάσσουν και αυτοί τη γνώμη τους και τα δικαιώματα τους προς μια πιο ανθρωποκεντρική λειτουργία της έξυπνης πόλης και
(δ) με την άμεση ή έμμεση συμμετοχή ιδιωτικών εταιρειών στην ανάπτυξη, τον σχεδιασμό και την καθημερινή λειτουργία των έξυπνων εφαρμογών της έξυπνης πόλης, η οποία ελλοχεύει κινδύνους χρήσης των δεδομένων των πολιτών όχι μόνο για τους σκοπούς της λειτουργίας της έξυπνης πόλης αλλά και προς εξυπηρέτηση ιδιωτικών και εμπορικών συμφερόντων των εταιρειών αυτών [68].

Προκειμένου οι υπεύθυνοι επεξεργασίας της έξυπνης πόλης να αντιμετωπίσουν τις ως άνω προκλήσεις και να δημιουργήσουν ένα περιβάλλον εμπιστοσύνης ανάμεσα στους φορείς και στους πολίτες της έξυπνης πόλης μπορούν να προβούν σε μια σειρά ενεργειών που θα αποσκοπούν στο μετριασμό των ως άνω αναφερθέντων ζητημάτων. Ειδικότερα, ένα πρώτο βήμα θα ήταν η δημοσίευση των εκθέσεων εκτίμησης αντικτύπου, η οποία μολονότι δεν εγκαθιδρύεται ως νομική υποχρέωση από τον ΓΚΠΔ, θα μπορούσε να συνδράμει στην ενίσχυση της διαφάνειας των ενεργειών επεξεργασίας του εκάστοτε υπεύθυνου επεξεργασίας και στη δημιουργία του επιθυμητού κλίματος εμπιστοσύνης με τους πολίτες [66]. Ειδικότερα, μια τέτοια ενέργεια θα έπρεπε να καθίσταται υποχρεωτική στο πλαίσιο της έξυπνης πόλης όπου οι εφαρμογές και τα προσωπικά δεδομένα συλλέγονται και επε-

ξεργάζονται από δημόσιες αρχές, προκειμένου οι πολίτες να μπορούν να γνωρίζουν ποια ακριβώς είναι τα προσωπικά δεδομένα τους που επεξεργάζονται, με ποιόν τρόπο, για ποιο σκοπό και πως σκοπεύει ο εκάστοτε υπεύθυνος επεξεργασίας – αρχή της έξυπνης πόλης να τα προστατέψει [69].

Ακόμη, ένα δεύτερο βήμα θα ήταν η παροχή δυνατότητας στους πολίτες να συμμετέχουν στις διαβουλεύσεις και στον σχεδιασμό των εφαρμογών της έξυπνης πόλης, δημιουργώντας με αυτό τον τρόπο ένα κλίμα συμπερίληψης και συνεργασίας. Η ως άνω ενέργεια δίνεται ως σύσταση από τον ίδιο τον GDPR στο άρθρο 35 παρ. 9 του οποίου, όπου προβλέπεται ότι «Όπου ενδείκνυται, ο υπεύθυνος επεξεργασίας ζητεί 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». Ο δήμος Τρικκαίων, όπως έχει αναφερθεί σε άλλη ενότητα της παρούσας, έχει ακολουθήσει την σύσταση του Κανονισμού με τη δημιουργία διαφόρων πλατφορμών, οι οποίες παρέχουν τη δυνατότητα στους δημότες και στους κατοίκους της πόλης να συμμετέχουν ενεργά στον σχεδιασμό των δράσεων και των έξυπνων εφαρμογών της πόλης τους [23].

Σε μια έρευνα που έγινε σε μία από τις τρεις κύριες περιοχές του Βελγίου, την Φλαμανδία και ειδικότερα στις φλαμανδικές έξυπνες πόλεις, εξετάστηκε ένας άλλος παράγοντας που ενδιαφέρει τους φορείς της έξυπνης πόλης και τους παρόχους των υπηρεσιών και εν προκειμένω το κόστος που συνεπάγεται η προστασία των προσωπικών δεδομένων από την επεξεργασία που απαιτείται να λάβει χώρα στο πλαίσιο της έξυπνης πόλης και τους τρόπους με τους οποίους η εκτίμηση αντικτύπου μπορεί να γίνει πιο αποτελεσματική και λιγότερο κοστοβόρα για αυτούς. Σύμφωνα με την έρευνα αυτή, βασικός παράγοντας εκτίμησης του κόστους είναι η πολυπλοκότητα και ειδικότερα το κόστος της εκτίμησης αντικτύπου ποικίλλει ανάλογα με τον βαθμό πολυπλοκότητας του αστικού περιβάλλοντος, στο οποίο θα γίνει η παροχή της έξυπνης υπηρεσίας και της πολυπλοκότητας της ίδιας της υπηρεσίας. Σύμφωνα με την έρευνα η πολυπλοκότητα του αστικού περιβάλλοντος επηρεάζεται κυρίως από α) το μέγεθος της πόλης, β) την ποικιλομορφία των συμφερόντων των εμπλεκόμενων μερών και γ) τον συνολικό αριθμό των έξυπνων υπηρεσιών που παρέχονται στην έξυπνη πόλη. Παρομοίως, η πολυπλοκότητα της υπηρεσίας της έξυπνης πόλης διαμορφώνεται από α) τον αριθμό των διαφορετικών ροών δεδομένων, β) την σαφήνεια του ιδιοκτησιακού καθεστώτος των δεδομένων, γ) την ποσότητα των περιπτώσεων χρήσης της υπηρεσίας, δ) τον βαθμό παραβίασης της ιδιωτικής ζωής των πολιτών και ε) τη διαφάνεια της ίδιας της έξυπνης υπηρεσίας [70].

Με βάση τα αποτελέσματα της έρευνας η ποικιλομορφία των εμπλεκόμενων μερών, ο συνολικός αριθμός των υπηρεσιών που παρέχονται στην συγκεκριμένη περιοχή, το μέγεθος του αριθμού των ροών των δεδομένων, η σαφήνεια του ιδιοκτησιακού καθεστώτος, ο βαθμός χρήσης της υπηρεσίας και οι πιθανότητες παραβίασης της ιδιωτικότητας των πολιτών είναι οι βασικοί παράγοντες για τον προσδιορισμό του κόστους της εκτίμησης αντικτύπου σε μια έξυπνη πόλη, το οποίο (κόστος) είναι στενά συνδεδεμένο με τους πιθανούς κινδύνους για την ιδιωτικότητα.

Όσο η πολυπλοκότητα του αστικού περιβάλλοντος και της έξυπνης υπηρεσίας αυξάνεται τόσο αυξάνεται και το κόστος διενέργειας μιας ικανοποιητικής - για τις ανάγκες που προκύπτουν - εκτίμησης αντικτύπου. Προκειμένου, λοιπόν, να καταστεί πιο αποτελεσματική και λιγότερο κοστοβόρα η εκτίμηση αντικτύπου, σύμφωνα με την έρευνα συστήνεται η δημιουργία υπηρεσιών ομαδοποίησης των έξυπνων υπηρεσιών βάσει των αναγκών προστασίας προσωπικών δεδομένων κάθε μίας, οι οποίες θα καθιστούν εύκολη την σύγκριση με άλλου, παρόμοιου είδους υπηρεσιών, η οποία θα βοηθήσει στη διαμόρφωση καλύτερων επιλογών κατά τη διενέργεια μιας εκτίμησης αντικτύπου.

Σε κάθε περίπτωση, οι φορείς και υπεύθυνοι επεξεργασίας της έξυπνης πόλης πρέπει να βρίσκουν κάθε φορά τους κατάλληλους και οικονομικά συμβατούς τρόπους διενέργειας των εκτιμήσεων αντικτύπου, προκειμένου να διασφαλίσουν ότι οι παρεχόμενες υπηρεσίες τους προστατεύουν τα δεδομένα των πολιτών και είναι σύννομες με τον Κανονισμό. Μόλις δε επιτευχθεί η ως άνω συμμόρφωση, θα καταστεί παράλληλα δυνατή η δημιουργία αισθήματος ασφάλειας και εμπιστοσύνης στους πολίτες της έξυπνης πόλης, η οποία θα συνδράμει στην επιτυχή ανάπτυξη της τελευταίας.

8. ΕΠΙΛΟΓΟΣ

Εάν οι πόλεις, αυτές καθ' αυτές, αποτελούν ένα σύνθετο οικοσύστημα, με την εισαγωγή των τεχνολογιών της πληροφορικής και επικοινωνιών και την εξέλιξή τους σε έξυπνες, το ως άνω οικοσύστημα καθίσταται ακόμη πιο σύνθετο. Η μετατροπή, ωστόσο, των πόλεων σε έξυπνες έχει ήδη εκκινήσει και σύντομα θα είναι η νέα πραγματικότητα μέσα στην οποία θα πρέπει να ζήσουν οι πολίτες τους. Κλειδί στην επιτυχία του ως άνω εγχειρήματος, όπως έχει αναδειχθεί στην παρούσα εργασία, είναι οι ίδιοι οι κάτοικοι των πόλεων και η διασφάλιση της ιδιωτικότητας και της ασφάλειας των δεδομένων τους. Στο πλαίσιο αυτό, οι φορείς της έξυπνης πόλεις καλούνται να εξισορροπήσουν τον εκσυγχρονισμό των υπηρεσιών τους με την προστασία των δεδομένων των πολιτών τους.

Κάθε φαινομενικά θετική ενέργεια προς τη δημιουργία «έξυπνων υπηρεσιών» υποκρύπτει πιθανούς κινδύνους και προκλήσεις που πρέπει να ληφθούν υπ' όψιν. Με τη θέση των εφαρμογών του Διαδικτύου των Πραγμάτων στο επίκεντρο της ανάπτυξης της έξυπνης πόλης, υιοθετώντας τις εφαρμογές αυτές σε όλους τους επιμέρους τομείς της (από την συγκοινωνία έως την υγεία), τίθενται υπό απειλή τα ίδια τα δεδομένα που αφορούν τις ως άνω υπηρεσίες. Αυτό συμβαίνει διότι παράλληλα με τις εφαρμογές του Διαδικτύου των Πραγμάτων εξελίσσονται και οι μορφές των κυβερνοαπειλών και κυβερνοεπιθέσεων κατά αυτών, γεγονός που ασκεί επιπλέον πίεση στους κατασκευαστές των εφαρμογών και στους φορείς της έξυπνης πόλης. Επιδεικνύοντας, όμως, την απαιτούμενη προσοχή κατά την κατασκευή και υιοθετώντας στρατηγικές επίτευξης ενός υψηλού επιπέδου ασφάλειας των υπηρεσιών της έξυπνης πόλης, η ανάπτυξη με τη διασφάλιση της ασφάλειας μπορεί να καταστεί δυνατή.

Όσον αφορά δε την ιδιωτικότητα των πολιτών της έξυπνης πόλης και την προστασία των δεδομένων τους, σε ένα περιβάλλον που φαίνεται αυτή (η ιδιωτικότητα) κατά φύση να προσβάλλεται, λόγω της μαζικής συλλογής και επεξεργασίας δεδομένων, είναι στην αρμοδιότητα των φορέων της έξυπνης πόλης να αποδείξουν το αντίθετο. Σύμμαχος τους σε αυτό το εγχείρημα είναι ο Γενικός Κανονισμός Προστασίας Δεδομένων, ο οποίος μολονότι μπορεί να χαρακτηρίζεται από πολλούς ως τροχοπέδη στην ανάπτυξη των έξυπνων πόλεων, στην πραγματικότητα αποτελεί το εργαλείο για την επιτυχημένη εξέλιξή τους. Τα εμπλεκόμενα μέρη της έξυπνης πόλης καλούνται να εφαρμόσουν και να ενσωματώσουν τις διατάξεις του Κανονισμού στις διάφορες λειτουργίες τους, αναλαμβάνοντας το καθένα από αυτά τις υποχρεώσεις και τα δικαιώματα που του αναλογεί.

Ειδικότερα, προκειμένου να επιτευχθεί ο στόχος της βιώσιμης ανάπτυξης των έξυπνων πόλεων με την συμμόρφωση αυτών με τον Κανονισμό, προτείνονται οι εξής λύσεις. Αρχικά, οι πολίτες θα πρέπει να ενημερώνονται από τις αρχές της έξυπνης πόλης αλλά και από τους κατασκευαστές των έξυπνων υπηρεσιών σχετικά α) με τους τρόπους με τους οποίους λειτουργούν αυτές οι υπηρεσίες (π.χ. πως γίνεται η συλλογή των δεδομένων τους, για ποιο σκοπό, τι είδους επεξεργασία θα υποστούν κλπ), β) τα δικαιώματα τους αναφορικά με τα δεδομένα τους και ειδικότερα τα δικαιώματα που τους παρέχει στα άρθρα 12, 13, 15, 16, 17 και 18 ο Κανονισμός και γ) τα πρόσωπα τα οποία είναι υπεύθυνα για την συλλογή και επεξεργασία των δεδομένων, στα οποία θα μπορούν να στραφούν για περαιτέρω πληροφορίες αλλά και για την άσκηση των δικαιωμάτων τους. Επίσης, είναι σημαντικό να δημιουργηθεί μια γενικότερη ευαισθητοποίηση γύρω από τα δεδομένα και τις πληροφορίες που συλλέγονται προκειμένου οι πολίτες να αντιλαμβάνονται πραγματικά τους πιθανούς κινδύνους που ελλοχεύουν από την συλλογή και επεξεργασία τους. Μέσω της ουσιαστικής ενημέρωσης των πολιτών θα μπορούν μετεπείτα αυτοί να χορηγήσουν την εν πλήρει επιγνώσει συγκαταθεσή τους δίνοντας στους φορείς της έξυπνης πόλης νόμιμη βάση για την επεξεργασία των δεδομένων τους και τη λειτουργία των έξυπνων υπηρεσιών. Ακόμη, οι φορείς της έξυπνης πόλης θα πρέπει να δίνουν την οδηγία στους κατασκευαστές των έξυπνων εφαρμογών και υπηρεσιών να εισάγουν την αρχή της προστασία των προσωπικών δεδομένων ήδη από τον σχεδιασμό των εκάστοτε εφαρμογών / υπηρεσιών, διευκολύνοντας με αυτό τον τρόπο το έργο τους ως υπευθύνων ή/και εκτελούντων την επεξεργασία, επιτυγχάνοντας ταυτόχρονα την προστασία των προσωπικών δεδομένων των πολιτών. Τέλος, δεδομένου ότι στο οικοσύστημα της έξυπνης πόλης πραγματοποιείται μαζική συλλογή και επεξεργασία δεδομένων, η οποία ενέχει σοβαρούς κινδύνους προσβολής της ιδιωτικότητας και των δικαιωμάτων των πολιτών, καθίσταται απαραίτητο οι φορείς της έξυπνης πόλης, ως υπεύθυνοι της επεξεργασίας, να ενεργούν πριν από κάθε επεξεργασία ή δημιουργία νέας υπηρεσίας εκτίμηση αντικτύπου, τη λεγόμενη στον Κανονισμό «DPIA». Θα πρέπει, λοιπόν, να εξετάζονται οι πιθανοί κίνδυνοι και να λαμβάνονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την αντιμετώπιση τους, αποδεικνύοντας με αυτό τον τρόπο την συμμόρφωση των εκάστοτε έξυπνων υπηρεσιών με τον Κανονισμό.

Καθώς η τεχνολογία εξελίσσεται και μέρα με τη μέρα νέες τεχνολογικές λύσεις ανακαλύπτονται, καινούριες ευκαιρίες βελτίωσης της ζωής των πολιτών δημιουργούνται. Προκειμένου, ωστόσο, η ανάπτυξη των έξυπνων πόλεων να λάβει ένα θετικό πρόσημο στην ιστορία, αποφεύγοντας ένα δυστοπικό μέλλον μιας κοινωνίας επιτήρησης, θα πρέπει ήδη από τώρα, από το ξεκίνημα του εγχειρήματος, να τεθεί στο επίκεντρο ο άνθρωπος. Αυτό, δε, θα επιτευχθεί μέσω της υιοθέτησης μιας ανθρωποκεντρικής στρατηγικής στη διαμόρφωση της έξυπνης πόλης, αναπτύσσοντας υπηρεσίες και εφαρμογές γύρω από τον άνθρωπο και για τον άνθρωπο, αποφεύγοντας παγίδα της ανάπτυξης απλά και μόνον χάριν της ραγδαίας τεχνολογικής ανάπτυξης που επικρατεί.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] UN Habitat (2022) 'World Cities Report 2022: *Envisaging the Future of Cities'* https://unhabitat.org/sites/default/files/2022/06/wcr_2022.pdf (ελεύθερα προσβάσιμο την 12.08.2023)

[2] Caragliu, A., Del Bo, C. and Nijkamp, P. (2011) 'Smart cities in Europe', *Journal of Urban Technology*, 18(2), pp. 65–82. doi:10.1080/10630732.2011.601117, https://degree.ubvu.vu.nl/repec/vua/wpaper/pdf/20090048.pdf (ελεύθερα προσβάσιμο την 12.08.2023)

[3] Giffinger, R. and Pichler-Milanović, N. (2007) in *Smart cities: Ranking of European medium-sized cities*. Vienna: Centre of Regional Science, Vienna University of Technology, http://www.smart-cities.eu/download/smart_cities_final_report.pdf) (ελεύθερα προσβάσιμο την 12.08.2023)

[4] Manville et al. (2014) '*Mapping Smart Cities in the EU*'. European Parliamentary Research Service, https://op.europa.eu/en/publication-detail/-/publication/78882e80-fc4a-4a86-9c39-2ad88ab89f9b (ελεύθερα προσβάσιμο την 10.08.2023)

[5] Hollands, R.G. (2008) 'Will the real Smart City Please Stand up?', *City*, 12(3), pp. 303–320. doi:10.1080/13604810802479126.

[6] Harrison, C. and Donnelly, I. A. (2011). 'A Theory of Smart Cities'. Proceedings of the 55th Annual Meeting of the ISSS, Hull, UK. pp. 123-136

[7] 'The new architecture of Smart Cities', Smartcities dive, https://www.smartcitiesdive.com/ex/sustainablecitiescollective/new-architecture-smart-cities/68921/ (ελεύθερα προσβάσιμο την 12.08.2023)

[8] Trivedi, A. (2021) *Architecture and the smart cities*, *RTF | Rethinking The Future*. https://www.re-thinkingthefuture.com/2021/10/26/a5683-architecture-and-the-smart-cities/ (ελεύθερα προσβάσιμο την 12.08.2023)

[9] Car, Tomislav; Pilepić Stifanich, Ljubica; Kovačić, Nataša (2022) *The Role of 5G and IoT in Smart Cities*, In: Proceedings of the ENTRENOVA - ENTerprise REsearch InNOVAtion Conference, Hybrid Conference, Opatija, Croatia, 17-18 June 2022, IRENET - Society for Advancing Innovation and Research in Economy, Zagreb, pp. 377-389, https://doi.org/10.54820/entrenova-2022-0032 (ελεύθερα προσβάσιμο την 12.08.2023)

[10] Μπούα, Ε.Α. (2017) «Θέματα ασφάλειας, ιδιωτικότητας και χρηματοδότησης στις έξυπνες πόλεις», Διπλωματική, Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών, https://pergamos.lib.uoa.gr/uoa/dl/frontend/file/lib/default/data/1518971/theFile (ελεύθερα προσβάσιμο την 12.08.2023)

[11] Carbonnell, J. (2019) *Smart-city: Stakeholders roles and needs*, *Medium*. Available at: https://juliencarbonnell.medium.com/smart-city-stakeholders-roles-and-needs-8e3679764d2a (ελεύθερα προσβάσιμο την 12.08.2023)

[12] European Commission (2014), press release , Barcelona is "iCapital" of Europe,

https://ec.europa.eu/commission/presscorner/detail/en/IP_14_239 (ελεύθερα προσβάσιμο την 12.08.2023)

[13] Luka (2015) *Barcelona to remain mobile world capital and host of GSMA Mobile World Congress through 2023*, *GSMA*. Available at: https://www.gsma.com/newsroom/press-release/barcelona-to-remain-mobile-world-capital-and-host-of-gsma-mobile-world-congress-through-2023/ (ελεύθερα προσβάσιμο την 12.08.2023)

[14] Ferrer, J. R. (2017) "*Barcelona's Smart City vision: an opportunity for transformation*", Field Actions Science Reports [Online], Special Issue 16 | 2017, URL: http://journals.openedition.org/factsreports/4367 (ελεύθερα προσβάσιμο την 12.08.2023)

[15] Smart Citizen – Fan Lab Barcelona | Research, education, innovation Center https://fablabbcn.org/projects/smart-citizen (ελεύθερα προσβάσιμο την 12.08.2023)

[16] Smith, L. (2022) *Smart city portrait: Barcelona, The Global Smart City Knowledge Center*. https://www.beesmart.city/city-portraits/smart-city-portrait-barcelona (ελεύθερα προσβάσιμο την 12.08.2023)

[17] European Commission (2016) European Capital of Innovation (iCapital), https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/prizes/icapital/icapital-2016_en (ελεύθερα προσβάσιμο την 12.08.2023)

[18] Eduardo, B. (2019) *Amsterdam launches a modular urban lighting system Tomorrow.City - The biggest platform about urban innovation*. https://tomorrow.city/a/amsterdam-launches-a-modular-urban-lighting-system (ελεύθερα προσβάσιμο την 12.08.2023)

[19] Παρίσης, Ι. (2019), «Έξυπνες πόλεις: εστιασμένα παραδείγματα χερσαίων και παραθαλάσσιων περιοχών», Ερευνητική Εργασία, Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, http://ikee.lib.auth.gr/record/305729/files/PARISISIOANNIS661_EE.pdf (ελεύθερα προσβάσιμο την 12.08.2023)

[20] Overstreet, K. (2021) *Building a city from scratch: The story of Songdo, Korea*, *ArchDaily*. https://www.archdaily.com/962924/building-a-city-from-scratch-the-story-of-songdo-korea (ελεύθερα προσβάσιμο την 12.08.2023)

[21] European Commission, EU Mission: Climate-Neutral and Smart Cities https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/eu-missions-horizon-europe/climate-neutral-and-smart-cities_en (ελεύθερα προσβάσιμο την 12.08.2023)

[22] *Six greek cities to become EU climate-neutral and smart cities by 2030* (2022) *Greek News Agenda*. https://www.greeknewsagenda.gr/topics/business-r-d/7685-six-greek-cities-to-become-eu-climate-neutral-and-smart-cities-by-2030 (ελεύθερα προσβάσιμο την 12.08.2023)

[23] Smartcity.gr, Εφαρμογές Έξυπνης Πόλης Δήμου Τρικκαίων, https://www.smartiscity.gr/dimos-trikkaion/ (ελεύθερα προσβάσιμο την 12.08.2023)

[24] Smartcity.gr, Εφαρμογές Έξυπνης Πόλης Δήμου Ιωαννιτών, https://www.smartiscity.gr/dimos-ioanniton/ (ελεύθερα προσβάσιμο την 12.08.2023)

[25] Diavouleusi.eu, http://www.diavouleusi.eu/ (ελεύθερα προσβάσιμο την 12.08.2023)

[26] Negahban, N. (2019) *Kinetica Brandvoice: The internet of things is powering the data-driven Fourth Industrial Revolution*, *Forbes*. Available at: https://www.forbes.com/sites/kinetica/2019/05/31/the-internet-of-things-is-powering-the-data-driven-fourth-industrial-revolution/ (ελεύθερα προσβάσιμο την 12.08.2023)

[27] Schoder, D. (2018) 'Introduction to the internet of things', *Internet of Things A to Z*, pp. 1–50. doi:10.1002/9781119456735.ch1.

[28] Patel, K. K., & Patel, S. M. (2016). Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges. International Journal of Engineering Science and Computing, 6(5), 6122-6131

[29] Tschofenig, H. et al. (2015, March). Architectural Considerations in Smart Object Networking, https://www.rfc-editor.org/rfc/rfc7452.txt (ελεύθερα προσβάσιμο την 12.08.2023)

[30] Kulkarni, S., & Kulkarni, S.G. (2017). Communication Models in Internet of Things: A Survey. *International Journal For Science Technology And Engineering, 3*, 87-91.

[31] Arasteh, H., Hosseinnezhad, V., Loia, V., Tommasetti, A., Troisi, O., Shafie-khah, M., & Siano, P. (2016). Iot-based smart cities: A survey. *2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC)*, 1-6.

[32] Jin, J., Gubbi, J., Marusic, S. and Palaniswami, M. (2014) An Information Framework for Creating a Smart City through Internet of Things. IEEE Internet of Things Journal, 1, 112-121. https://doi.org/10.1109/JIOT.2013.2296516

[33] Ιωαννίδου Κ. (2020), Ζητήματα ιδιωτικότητας στο Διαδίκτυο των Πραγμάτων (Internet of Things), Διπλωματική εργασία, Πανεπιστήμιο Μακεδονίας, https://dspace.lib.uom.gr/handle/2159/24160 (ελεύθερα προσβάσιμο την 12.08.2023)

[34] Τζιούφα Π. (2019), Internet of Things – RFID και προσωπικά δεδομένα: Θέματα ασφάλειας και απορρήτου στο Διαδίκτυο των Πραγμάτων (IoT), Διπλωματική Εργασία, Πανεπιστήμιο Μακεδονίας https://dspace.lib.uom.gr/handle/2159/22795 (ελεύθερα προσβάσιμο την 12.08.2023)

[35] Talari, Saber, et al. (2017) "A review of smart cities based on the internet of things concept." *Energies* 10.4: 421, https://doi.org/10.3390/en10040421 (ελεύθερα προσβάσιμο την 12.08.2023)

[36] Ι. Ιγγλεζάκης (2021) Δίκαιο πληροφορικής, 4η έκδ., Εκδόσεις Σάκκουλα

[37] Samonas, S., & Coss, D. (2014). The CIA strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, *10*(3). https://www.semanticscholar.org/paper/The-CIA-Strikes-Back%3A-Redefining-

Confidentiality%2C-Samonas-Coss/d0a5f110b0f46c52211c98ab852ddb8de1e082a3 (ελεύθερα προσβάσιμο την 12.08.2023)

[38] Ma, C. (2021). Smart city and cyber-security; technologies used, leading challenges and future recommendations. *Energy Reports*.https://doi.org/10.1016/j.egyr.2021.08.124 (ελεύθερα προσβάσιμο την 12.08.2023)

[39] Αραμπατζής Α. (2019), *Κρυπτογράφηση και Αποκρυπτογράφηση*, Homo Digitalis https://www.homodigitalis.gr/posts/4305 (ελεύθερα προσβάσιμο την 12.08.2023)

[40] ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων), L 119/1, http://data.europa.eu/eli/reg/2016/679/oj (ελεύθερα προσβάσιμο την 12.08.2023)

[41] Ντόκας Β. (2019), Είναι τα ανωνυμοποιημένα δεδομένα πραγματικά ανώνυμα, Ntokas, https://ntokas.gr/anonymous-data/ (ελεύθερα προσβάσιμο την 12.08.2023)

[42] Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 6ης Ιουλίου 2016, σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση, http://data.europa.eu/eli/dir/2016/1148/oj (ελεύθερα προσβάσιμο την 12.08.2023)

[43] Οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 14ης Δεκεμβρίου 2022 σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972, και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148 (οδηγία NIS 2), http://data.europa.eu/eli/dir/2022/2555/oj (ελεύθερα προσβάσιμο την 12.08.2023)

[44] *Κυβερνοασφάλεια: Δημοσιεύθηκε η Οδηγία NIS 2 της Ευρωπαϊκής Ένωσης*, (2022) Lawspot, https://www.lawspot.gr/nomika-nea/kyvernoasfaleia-dimosieythike-i-odigia-nis-2-tis-eyropaikis-enosis (ελεύθερα προσβάσιμο την 12.08.2023)

[45] Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, *4*(5), 193–220. https://doi.org/10.2307/1321160 (ελεύθερα προσβάσιμο την 12.08.2023)

[46] Westin, A. (1967). Privacy and Freedom. New York, Atheneum

[47] Ακριβοπούλου Χ., (2011). Το δικαίωμα στην προστασία των προσωπικών δεδομένων μέσα από το φακό του δικαιώματος στην ιδιωτική ζωή, Θεωρία & Πράξη Δημοσίου Δικαίου 7/2011, https://www.constitutionalism.gr/2213-to-dikaiwma-stin-prostasia-twn-proswpikwn-dedomenw/ (ελεύθερα προσβάσιμο την 12.08.2023)

[48] Καρανικόλα Χ. (2013), Πληροφοριακή Ιδιωτικότητα: Κίνδυνοι & Τεχνολογίες για την αντιμετώπισή τους, Διπλωματική Εργασία, Πανεπιστήμιο Αιγαίου https://hellanicus.lib.aegean.gr/bitstream/handle/11610/8732/file0.pdf?sequence=2&is

Allowed=y (ελεύθερα προσβάσιμο την 12.08.2023)

[49] Solove, D. (2004). The digital person: technology and privacy in the information age , New York University Press, https://ssrn.com/abstract=2899131 (ελεύθερα προσβάσιμο την 12.08.2023)

[50] Arne Hintz, Lina Dencik, Karin Wahl-Jorgensen (2017), Digital Citizenship and Surveillance Society, International Journal of Communication 11, 731–739, Digital Citizenship and Surveillance Society: Introduction (cardiff.ac.uk) (ελεύθερα προσβάσιμο την 12.08.2023)

[51] Ballesté, Antoni & Pérez-Martínez, Pablo & Solanas, Agusti. (2013). The Pursuit of Citizens' Privacy: A Privacy-Aware Smart City Is Possible. IEEE Communications Magazine. 51. 10.1109/MCOM.2013.6525606.

[52] Eckhoff, David, & Wagner, Isabel (2018). 'Privacy in the smart city—applications, technologies, challenges, and solutions. IEEE Communications Surveys & Tutorials, 20 (1), 489–516.

[53] Coletta, Claudio, & Kitchin, Rob (2017). Algorhythmic governance: Regulating the "heartbeat" of a city using the Internet of Things. Big Data & Society, 4(2), 1–16.

[54] König, Pascal. (2021). Citizen-centered data governance in the smart city: From ethics to accountability. Sustainable Cities and Society. 75. 103308. 10.1016/j.scs.2021.103308.

[55] Γκλεζάκου Ε. (2022), Διαδίκτυο των Πραγμάτων - Ζητήματα προστασίας Προσωπικών Δεδομένων στην Έξυπνη Πόλη (Smart City), Διπλωματική Εργασία, Πανεπιστήμιο Πειραιώς, https://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/15069/Gklezakou_mdi2011.pdf?sequence=1 (ελεύθερα προσβάσιμο την 12.08.2023)

[56] Peppet, S. R. (2014). Regulating the internet of things: first steps toward managing discrimination, privacy, security and consent. Tex. L. Rev., 93, 85–178.

[57] Cottrill, Caitlin & Jacobs, Naomi & Markovic, Milan & Edwards, Pete. (2020). Sensing the City: Designing for Privacy and Trust in the Internet of Things. Sustainable Cities and Society. 63. 102453. 10.1016/j.scs.2020.102453.

[58] Kitchin, Rob. (2016). Getting smarter about smart cities: Improving data privacy and data security. https://www.researchgate.net/publication/293755608_Getting_smarter_about_smart_cities_Improving_data_privacy_and_data_security (ελεύθερα προσβάσιμο την 12.08.2023)

[59] Ahmad, W., & Dethy, E. (2019). Preventing Surveillance Cities: Developing a Set of Fundamental Privacy Provisions. https://www.semanticscholar.org/paper/Preventing-Surveillance-Cities%3A-Developing-a-Set-of-Ahmad-Dethy/49db87c399dad097a5cf71c35b58177b1e13db7d (ελεύθερα προσβάσιμο την 12.08.2023)

[60] Penney, Jonathon, Understanding Chilling Effects (May 28, 2021). 106 Minnesota

(2022), https://ssrn.com/abstract=3855619 or http://dx.doi.org/10.2139/ssrn.3855619, (ελεύθερα προσβάσιμο την 12.08.2023)

[61] Andersen L, Human rights in the age of artificial intelligence, https://www.accessnow.org/wp-content/uploads/2018/11/AI-and-Human-Rights.pdf (ελεύθερα προσβάσιμο την 12.08.2023)

[62] Πρόταση ΚΑΝΟΝΙΣΜΟΣ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (γενικός κανονισμός για την προστασία δεδομένων), COM (2012) 11 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52012PC0011 (ελεύθερα προσβάσιμο την 12.08.2023)

[63] Νόμος υπ' αρ. 4624/2019 Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις, ΦΕΚ Α', 137/29.08.2019.

[64] Mitrou, Lilian. (2018). Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'?. SSRN Electronic Journal. 10.2139/ssrn.3386914.

[65] Τσάνη Σ. (2021), Μελέτη και ανάλυση παραβιάσεων ιδιωτικότητας σε περιβάλλοντας έξυπνων σπιτιών και έξυπνων πόλεων, Διπλωματική Εργασία, Πανεπιστήμιο Μακεδονίας https://dspace.lib.uom.gr/handle/2159/25766 (ελεύθερα προσβάσιμο την 12.08.2023)

[66] European Commission (2017), Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, ARTICLE 29 DATA PROTECTION WORKING PARTY, https://ec.europa.eu/newsroom/article29/items/611236 (ελεύθερα προσβάσιμο την 12.08.2023)

[67] Neirotti, P., De Marco, A., Cagliano, A. C., Mangano, G., & Scorrano, F. (2014). Currenttrends in Smart City initiatives: Some stylised facts.Cities, 38, 25–36, https://doi.org/10.1016/j.cities.2013.12.010 (ελεύθερα προσβάσιμο την 12.08.2023)

[68] Jonas Breuer, Ellen Wauters, Ine van Zeeland, Athena Christofi, Identifying GDPR enforcement problems and requirements in Smart Cities, SPECTRE, https://spectreproject.be/ (ελεύθερα προσβάσιμο την 12.08.2023)

[69] Smart Cities Onderzoeksrapport bescherming van persoonsgegevens in de ontwikkeling van Nederlandse Smart Cities (2021) https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/onderzoeksrapport_smart_cities_def.pdf (ελεύθερα προσβάσιμο την 12.08.2023)

[70] Vandercruysse, L., Buts, C., & Dooms, M. (2020). A typology of Smart City services: The case of Data Protection Impact Assessment. *Cities*, *104*, 1-15. [102731]. https://doi.org/10.1016/j.cities.2020.102731